de de de de de de parceiro

AWS Security Hub

AWS Security Hub: de de de de de de parceiro

Table of Contents

Visão geral da integração de terceiros comAWS Security Hub

Este guia é destinado aAWSPartner Network (APN) Parceiros que gostariam de criar uma integração comAWS Security Hub.

Como um parceiro da APN, você pode integrar o Security Hub de uma ou mais das maneiras a seguir.

- Enviar descobertas ao Security Hub
- Consumir descobertas do Security Hub
- Ambos enviam descobertas e consomem descobertas do Security Hub
- Use o Security Hub como o centro de uma oferta de provedor de serviços de segurança gerenciada (MSSP)
- Consulta com oAWSclientes sobre como implantar e usar o Security Hub

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

Tópicos

Por que integrar com oAWS Security Hub?

AWS Security HubFornece 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 clientes informações sobre as descobertas de segurança geradas por você.

Uma integração com o Security Hub pode agregar valor das seguintes maneiras.

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

- Fornece aos clientes uma visão única de seus clientesAWSDescobertas relacionadas 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 seus motivos para a integração. É mais provável que uma integração seja bem-sucedida se seus clientes quiserem uma integração do Security Hub com seu produto. Você pode construir uma integração puramente por motivos de marketing ou para adquirir novos clientes. No entanto, se você construir a integração sem qualquer entrada atual do cliente e não considerar as necessidades de seus clientes, a integração pode não produzir os resultados esperados.

Preparando o envio de descobertas aoAWS Security Hub

Como um parceiro da APN, você não pode enviar informações para o Security Hub para seus clientes até que a equipe do Security Hub o permita como provedor de busca. Para ser habilitado como provedor de descoberta, você deve concluir as seguintes etapas de integração. Isso garante uma experiência positiva Security Hub para você e seus clientes.

Ao concluir as etapas de integração, siga as diretrizes emthe section called “Princípio para criar e atualizar descobertas”,the section called “Diretrizes para mapeamento do ASFF”, ethe section called “Diretrizes para usar o`BatchImportFindings`API”.

1. Mapeie suas descobertas de segurança para oAWSFormato de descoberta de segurança da (ASFF).
2. Crie sua arquitetura de integração para enviar descobertas para o endpoint correto do Regional Security Hub. Para fazer isso, você define se enviará descobertas da sua próprioAWSconta ou de dentro das contas do cliente.
3. Peça aos clientes que assinem o produto em sua conta. Para fazer isso, eles podem usar o console do ou o`EnableImportFindingsForProduct`Operação da API. Consulte Gerenciar integrações de produtosnoAWS Security HubGuia do usuário do.

   Você também pode assinar o produto para eles. Para fazer isso, use uma função entre contas para acessar o`EnableImportFindingsForProduct`Operação da API em nome do cliente.

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

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

- Anunciando a integração do Cloud Custodian comAWS Security Hub
- Usar oAWS Fargatee Prowler para enviar descobertas de configuração de segurança sobreAWSServiços para Security Hub
- Como importarAWS ConfigAvaliações de regras como descobertas no Security Hub

Preparando-se para receber descobertas deAWS Security Hub

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

- Peça a seus clientes enviarem automaticamente todas as descobertas paraCloudWatchEvents (Eventos). Um cliente pode criar específicoCloudWatchregras de evento para enviar descobertas para destinos específicos, como um SIEM ou um bucket do S3.
- Peça aos clientes que selecionem descobertas ou grupos específicos de descobertas dentro do 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 tickets, 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.

Eles são chamados de ações personalizadas. Quando um usuário executa uma ação personalizada, umCloudWatchevento é criado para essas descobertas específicas. Como parceiro, você pode aproveitar esse recurso e criarCloudWatchregras de evento ou metas 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 paraCloudWatchEvents (Eventos). Esse recurso serve para um usuário agir sobre descobertas específicas.

As publicações de blog a seguir descrevem soluções que usam a integração com o Security Hub eCloudWatchEventos para ações personalizadas.

- Como integrarAWS Security HubAções personalizadas comPagerDuty
- Como habilitar ações personalizadas noAWS Security Hub
- Como importarAWS ConfigAvaliações de regras como descobertas no Security Hub

Recursos para aprender sobre oAWS Security Hub

Os seguintes materiais podem ajudá-lo a entender melhor oAWS Security HubSolução e comoAWSos clientes podem usar o serviço.

- Introdução aoAWS Security Hubvídeo
- Guia do usuário Security Hub
- Referência da Security Hub
- Webinar de integração

Também recomendamos que você ative o Security Hub em um dos seusAWScontas e obtenha alguma experiência prática com o serviço.

Pré-requisitos para parceiros

Antes que você possa iniciar uma integração comAWS Security Hub, você deve atender a um dos seguintes critérios:

- Você é umAWSSelecione Parceiro de nível ou superior.
- Você se juntou aoAWSCaminho do parceiro do ISV, e o produto que você usa para a integração do Security Hub concluiu umAWSAnálise Técnica Fundacional (FTR). Em seguida, o produto recebe um “Avaliado porAWS“distintivo.

Você também deve ter um contrato de confidencialidade mútua em vigor comAWS.

Casos de uso da integração e permissões necessárias

AWS Security HubpermiteAWSclientes para receber descobertas de parceiros da APN. Os produtos do parceiro podem ser executados dentro ou fora do clienteAWSconta. 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 permissões de um parceiro a qualquer momento.

Para permitir que um parceiro envie descobertas de segurança para sua conta, o cliente primeiro se inscreve no 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, consulteGerenciar integrações de produtosnoAWS Security HubGuia do usuário do.

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

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

Parceiro hospedado: descobertas enviadas da conta de parceiro

Este caso de uso abrange parceiros que hospedam um produto por conta próprioAWSconta. Para enviar descobertas de segurança para umAWScliente, o parceiro chama o`BatchImportFindings`Operação da API da conta do produto de parceiro.

Para esse caso de uso, a conta do cliente só precisa das permissões estabelecidas quando o cliente se inscreve no produto parceiro.

Na conta do parceiro, o diretor do IAM que chama o`BatchImportFindings`A operação da API deve ter uma política do IAM que permita que o diretor chame`BatchImportFindings`.

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

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

Para enviar descobertas de segurança relacionadas à conta do cliente, o produto parceiro usa suas próprias credenciais para chamar oBatchImportFindingsOperação da API.

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

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

Parceiro hospedado: descobertas enviadas da conta do cliente

Este caso de uso abrange parceiros que hospedam um produto por conta próprialAWSconta, mas use uma função entre contas para acessar a conta do cliente. Eles chamam oBatchImportFindingsOperação da API da conta do cliente.

Para este caso de uso, para chamar oBatchImportFindingsOperação da API, a conta de parceiro assume uma função 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 para a conta do produto parceiro seja usado na chamada. A política de recursos gerenciados do Security Hub concede permissão para a conta do produto de parceiro e o ARN do produto parceiro. O ARN do produto é o identificador exclusivo do parceiro como provedor. Como a chamada não vem da conta do produto parceiro, o cliente deve conceder explicitamente permissão para que o produto parceiro envie descobertas para o Security Hub.

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

concederAWSAcesso à conta a um parceiro. O identificador exclusivo garante que o parceiro use a conta de cliente correta.

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 que trabalham em nome do cliente, inicia a assinatura de um produto no Security Hub.
2. O Security Hub gera a política de recursos gerenciados correta com a confirmação do cliente.
3. O cliente configura a função entre contas manualmente ou usando o uso doAWS CloudFormation. Para obter informações sobre funções entre contas, consulteComo fornecer acesso aAWSContas de propriedade de terceirosnoManual do usuário do IAM.
4. O produto armazena com segurança a função do cliente e a ID externa.

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

1. O produto chama oAWS Security Token Service(AWS STS) assumir a função do cliente.
2. O produto chama o`BatchImportFindings`Operação de API 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 para a 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"
        }
    ]
}
```

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

Cliente hospedado: descobertas enviadas da conta do cliente

Este caso de uso abrange parceiros que têm um produto implantado noAWSconta. O`BatchImportFindings`A API é chamada a partir da solução executada na conta do cliente.

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

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

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

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 parceiro em seusAWSconta usando manualmenteAWS CloudFormationou outra ferramenta de implantação.
2. O cliente define a política do IAM necessária para o produto parceiro usar quando enviar descobertas para o Security Hub.
3. O cliente anexa a política aos componentes necessários do produto parceiro, como uma instância do EC2, um contêiner ou uma função do Lambda.

Agora o produto pode enviar descobertas para o Security Hub:

1. O produto parceiro usa oAWSSDK ouAWS CLIPara chamar o`BatchImportFindings`Operação da API no Security Hub. Ele faz a chamada do componente na conta do cliente em que a política está anexada.
2. Durante a chamada de API, as credenciais temporárias necessárias são geradas para permitir que o`BatchImportFindings`Chamar para ter sucesso.

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 inclusão de parceiros

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

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

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

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

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

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

   Mapeando descobertas para ASFF

   Para enviar descobertas para o Security Hub, você deve mapear suas descobertas para oAWSFormato de descoberta de segurança (ASFF).

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

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

ASFF é o formato de protocolo de fio necessário para usar para enviar descobertas paraAWS Security Hub. As descobertas são representadas como documentos JSON que aderem ao Esquema JSON ASFF e RFC-7493 O Formato de Mensagem I-JSON. Para obter detalhes sobre o esquema ASFF, consulteAWSFormato de descoberta de segurança da (ASFF)noAWS Security HubGuia do usuário do.

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

Construindo e testando a integração

Você pode concluir todos os testes para sua integração usando umAWSConta própria. Isso lhe dá 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 o`BatchImportFindings`Operação da API para enviar descobertas novas e atualizadas para o Security Hub.

Ao longo da compilação de uma integração do Security Hub,AWSincentiva você a manter seus contatos de parceiros da APN informados sobre o progresso de sua integração. Você também pode pedir ajuda aos contatos do parceiro da APN com perguntas de integração.

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

7. Você demonstra a integração com a equipe de produtos Security Hub. Essa integração deve ser demonstrada usando uma conta que a equipe do Security Hub possui.

   Se eles estiverem confortáveis com a integração, a equipe do Security Hub dá aprovação para avançar para listá-lo como provedor.

8. Você forneceAWScom um manifesto final para revisão.
9. A equipe do Security Hub cria a integração do provedor no console do Security Hub. Os clientes podem descobrir e habilitar a integração.
10. (Opcional) Você se envolve em esforços de marketing adicionais para promover a integração do Security Hub. Consulte Go-to-marketatividades.

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

    - Um vídeo de demonstração (no máximo 3 minutos) da integração de trabalho. O vídeo é usado para fins de marketing e é postado noAWS YouTubeChannel.

- Um diagrama de arquitetura de um slide para adicionar ao slide deck de primeira chamada do Security Hub.

Go-to-marketatividades

Os parceiros também podem se envolver em atividades de marketing opcionais para ajudar a explicar e promover seusAWS Security HubIntegração do.

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

AWSOs parceiros da Rede de Parceiros (APN) podem usar a Central de Marketing de Parceiros da APN e o programa de Fundos de Desenvolvimento de Mercado (MDF) para criar campanhas e obter suporte de financiamento. 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 naAWS Security HubPágina de parceiros.

Para ser listado nesta página, forneça os seguintes detalhes aos contatos do parceiro da APN. Isso 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 fornece aos clientes. Essa descrição é limitada a 700 caracteres, incluindo espaços.
- O URL para uma página que descreve sua solução. Este site deve ser específico para o seuAWSintegração e, mais especificamente, 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 de alta resolução do seu logotipo que é de 600 x 300 pixels. Para obter detalhes sobre os requisitos para este logotipo, consultethe section called “Logotipo para página de parceiros”.

Press Releases

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

Antes de publicar o comunicado de imprensa, você deve enviá-lo paraAWSpara análise por marketing de parceiros da APN, liderança do Security Hub eAWSServiços de segurança externos (ESS). O comunicado de imprensa pode incluir uma proposta de cotação para o vice-presidente da ESS.

Para iniciar esse processo, trabalhe com seu PDM. Temos um Contrato de Nível de Serviço (SLA) de 10 dias úteis para revisar os comunicados à imprensa.

AWSBlog da Rede de Parceiros (APN)

Também podemos ajudá-lo a publicar uma entrada de blog que você cria no blog da APN. A entrada do blog deve se concentrar em uma história do cliente e caso de uso. Ele não pode ser posicionado apenas em torno de ser 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 8 semanas ou mais para aprovação e publicação finais.

Principais coisas a saber sobre o blog da APN

Ao criar uma postagem do blog, lembre-se dos seguintes itens.

O que se passa em uma postagem no blog?

- As postagens de parceiros devem ser educacionais e fornecer conhecimento profundo sobre um tópico relevante paraAWSclientes.
- O comprimento ideal não é superior a 1.500 palavras. Os leitores valorizam conteúdo educacional profundo que lhes ensina o que é possível emAWS.
- O conteúdo deve ser original para o blog da APN. Não reutilize o conteúdo de fontes, como postagens de blog ou whitepapers existentes.

Quais são outros limites para postar no blog da APN?

- Somente parceiros de nível Avançado ou Premier podem postar no blog da APN. Há exceções para parceiros selecionados que têm uma designação do programa da APN, como a prestação de serviços.
- Cada parceiro é limitado a três postagens por ano. Com dezenas de milhares de parceiros da APN,AWSdeve ser equitativo em sua cobertura.

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

Quanto tempo demora para editar uma postagem de blog antes de ser publicada?

Depois de enviar o primeiro rascunho completo da postagem do blog, leva de quatro a seis semanas para ser editado.

Por que escrever para o blog da APN?

Um blog do APN pode fornecer os seguintes benefícios.

- Credibilidade— Para parceiros da APN, ter uma história publicada porAWSpode influenciar os clientes globalmente.
- Visibilidade— O blog da APN é um dos blogs mais lidos emAWScom 1,79 milhões de visualizações de página em 2019, incluindo tráfego influenciado.
- Business— As postagens do Parceiro da APN têm botões de conexão que podem gerar leads por meio do programa APN Customer Engagements (ACE).

Que tipo de conteúdo é o melhor ajuste?

Os seguintes tipos de conteúdo são mais adequados para uma postagem no blog da APN.

- O conteúdo técnico é o tipo de história mais popular. Isso inclui holofotes da solução e informações de instruções. Mais de 75% dos leitores analisam esse conteúdo técnico.
- Os clientes valorizam histórias de nível 200 ou acima que demonstram como algo funcionaAWSou como um parceiro da APN resolveu um problema de negócios para os clientes.
- As postagens escritas por especialistas técnicos ou especialistas no assunto têm o melhor desempenho de longe.

Folha lisa ou folha de marketing

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

Se você criar uma planilha lisa para sua integração, envie uma cópia para a equipe do Security Hub. Eles o adicionarão à página do parceiro.

Whitepaper ou ebook

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

Webinário do

Se você realizar um webinar sobre sua integração, envie uma gravação do webinar para a equipe do Security Hub. A equipe vinculará a ele na página do parceiro.

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

Vídeo de demonstração

Para fins de marketing, você pode produzir um vídeo de demonstração da integração de trabalho. Publique esse vídeo na sua conta da plataforma de vídeo, e a equipe do Security Hub será vinculada a ele na página do parceiro.

Manifesto

Cada parceiro deAWS Security Hub integração deve preencher um manifesto de integração de produtos 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 a placa 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 usathe section called “Lista de verificação de prontidão” o. Essa lista de verificação determina se sua integração está pronta para ser lançada.

Todas as informações técnicas fornecidas por você 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 deAWS Security Hub parceiros. Observe que a página de parceiros não está disponível nas regiões China (Pequim) e China (Ningxia).

Índice

Caso de uso e informações de marketing

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

Caso de uso de encontrar fornecedores e consumidores

Necessário para fornecedores independentes de software (ISV).

Para descrever seu caso de uso em torno de sua integração comAWS Security Hub, responda às seguintes perguntas. Se você não planeja enviar nem receber descobertas, anote isso nesta seção e, em seguida, conclua a próxima seção.

As informações a seguir devem estar 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 de descobertas?
- Se você planeja receber descobertas, o que fará com essas descobertas? Que tipos de descobertas você receberá? Por exemplo, você receberá todas as descobertas, descobertas de um determinado tipo ou apenas 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 busca dos clientes.

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

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

Caso de uso do Consulting Partner (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 privados. A equipe do Security Hub não os anuncia em nenhum lugar. Eles devem descrever uma ou ambas as seguintes:

- Como você ajuda os clientes a inicializar o Security Hub? Por exemplo, você ajudou os clientes a usar serviços profissionais, um módulo Terraform ou umAWS 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 seguintes informações.

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

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

Arquitetura

Obrigatório se você enviar descobertas ou receber descobertas do 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 os diagramas de arquitetura, considere o seguinte:

- QuaisAWS serviços, agentes do sistema operacional e assim por diante você usará?
- Se você enviar descobertas para o Security Hub, você enviará descobertas daAWS conta do cliente ou da sua próprioAWS conta?

- Se você receber descobertas, como você 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 limitação?

Configuração

Obrigatório se você enviar descobertas ou receber descobertas do Security Hub.

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

No mínimo, você deve usarAWS CloudFormation modelos ou uma infraestrutura semelhante, 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 busca 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 você vai agrupar e enviar descobertas para o Security Hub? Em outras palavras, qual é a latência de quando a descoberta é criada em seu produto até quando ela é enviada ao Security Hub?

Essas informações devem ser refletidas na documentação do produto para sua integração. 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 sua 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, você pode fornecer uma descrição separada para cada produto, mas nós os combinaremos em uma única entrada na página do parceiro.

Cada descrição pode ter no máximo 700 caracteres com espaços.

Ativos

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 com o 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 documentos técnicos. O Security Hub também vinculará aqueles da página de seus parceiros.

Logotipo para página de parceiros

Obrigatório 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
- Corte: apertado, sem acolchoamento
- Plano de de de de de de
- Formato: PNG

Logotipos para o console do Security Hub

Necessário para todas as integrações.

Forneça URLs para os logotipos do modo claro e escuro para exibição 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: apertado, sem acolchoamento
- Plano de de de de de de

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

Encontrando tipos

Obrigatório se você enviar descobertas para o Security Hub.

Forneça uma tabela que documente os tipos de busca no formato ASFF que você usa e como eles se alinham aos seus tipos de busca nativos. Para obter detalhes sobre como encontrar tipos no ASFF, consulte Taxonomia de tipos para ASFF no GuiaAWS Security Hub do usuário.

Recomendamos que você também inclua 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 funciona mais.

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

Detecção do batimento cardíaco

Recomendado se você estiver enviando descobertas para o Security Hub.

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

Se você puder, faça isso usando o tipo de descobertaHeartbeat.

AWS Security Hubinformações do console

Forneça um texto JSON para aAWS Security Hub equipe que contenha as informações a seguir. O Security Hub usa essas informações para criar o ARN do seu produto, exibir a lista de fornecedores 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 em todas as empresas. Provavelmente é o mesmo ou semelhante`name` a. Tipo: String Tamanho mínimo: 5 caracteres Tamanho máximo: 24 caracteres Caracteres permitidos: letras minúsculas, números e números e hifens Devem começar com uma letra minúscula. Devem terminar com uma letra minúscula ou um número.

Campo	Obrigatório	Descrição
`name`	Sim	O nome da empresa do provedor a ser exibido no console do Security Hub. Tipo: String Tamanho máximo: 16 caracteres
`description`	Sim	A descrição da empresa do provedor a ser exibida no console do Security Hub. Tipo: String Tamanho máximo: 200 caracteres

Informações do produto

Esta seção fornece informações sobre o seu 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 enviam e recebem descobertas. Caso você seja um parceiro de consultoria, deixe este 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. Eles devem ser exclusivos dentro de uma empresa. Eles não precisam ser exclusivos 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 números e hifens Devem começar com uma letra minúscula. Devem terminar com uma letra minúscula ou um número.
`regionsNotSupported`	Sim	Quais das seguintesAWS regiões você não apoia? Em outras palavras, em quais regiões o Security Hub não deve mostrar você como

Campo	Obrigatório	Descrição
		uma opção em nossa página de parceiros no console do Security Hub? Tipo: String Forneça somente o código da região. Por exemplo, `us-west-1` . Para obter uma lista das regiões, consulte Endpoints regionais no Referência geral da AWS. Os códigos de região para oAWS GovCloud (US) são`us-gov-west-1` (paraAWS GovCloud (Oeste dos EUA)) e`us-gov-east-1` (paraAWS GovCloud (Leste dos EUA)). Os códigos de região das regiões da China são`cn-north-1` (para a China (Pequim)) e`cn-northwest-1` (para a China (Ningxia)).

Campo	Obrigatório	Descrição
`commercialAccountNumber`	Sim	O númeroAWS da conta principal do produto para asAWS regiões. Se você enviar descobertas para o Security Hub, a conta fornecida será baseada em onde você envia as descobertas. • Da suaAWS conta. Nesse caso, forneça o número da conta que você usa para enviar descobertas. • DaAWS 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 é obrigatório. Tipo: String

Campo	Obrigatório	Descrição
`govcloudAccountNumber`	Não	O número daAWS conta principal do produto paraAWS GovCloud (US) regiões (se seu produto estiver disponível emAWS GovCloud (US)). Se você enviar descobertas para o Security Hub, a conta fornecida será baseada em onde você envia as descobertas. • Da suaAWS conta. Nesse caso, forneça o número da conta que você usa para enviar descobertas. • DaAWS 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 asAWS GovCloud (US) 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 é obrigatório. Tipo: String

Campo	Obrigatório	Descrição
`chinaAccountNumber`	Não	O número daAWS 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 em onde você envia as descobertas. • Da suaAWS conta. Nesse caso, forneça o número da conta que você usa para enviar descobertas. • DaAWS 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 da China. Se isso não for possível, entre em contato com a equipe do Security Hub. Se você receber apenas descobertas do Security Hub, pode ser qualquer conta que você possua em uma região da China. Tipo: String
`name`	Sim	O nome do produto do fornecedor a ser exibido no console do Security Hub. Tipo: String Tamanho máximo: 24 caracteres

Campo	Obrigatório	Descrição
`description`	Sim	A descrição do produto do fornecedor 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 parceiros, você pode especificar uma das políticas de recursos a seguir ou você pode especificar uma das políticas de recursos a seguir`NEITHER`. • Com`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, você só pode enviar descobertas para o Security Hub a partir 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 para 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 faltando, 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 oAWS Marketplace destino do seu produto. O URL é exibido no console do Security Hub. Tipo: String Isso deve ser umAWS Marketplace URL. Caso você não tenha umAWS Marketplace anúncio, deixe este campo em branco.

Campo	Obrigatório	Descrição
`configurationUrl`	Sim	O URL da documentação do 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 • Links paraAWS CloudFormation modelos (se necessário) • Informações sobre seu caso de uso para a integração • Latência • Mapeamento do ASFF • Tipos de descobertas • Arquitetura

Diretrizes e listas de verificação

À medida que você prepara os materiais necessários para o seuAWS Security Hubintegração, 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 que o logotipo seja exibido naAWS Security Hubconsole

Para que o logotipo seja exibido noAWS Security HubConsole, siga estas diretrizes.

Modos claro e escuro

Você deve fornecer um modo claro e uma versão em modo escuro do logotipo.

Formato

Formato de arquivo SVG

Background color (Cor de fundo)

Transparente

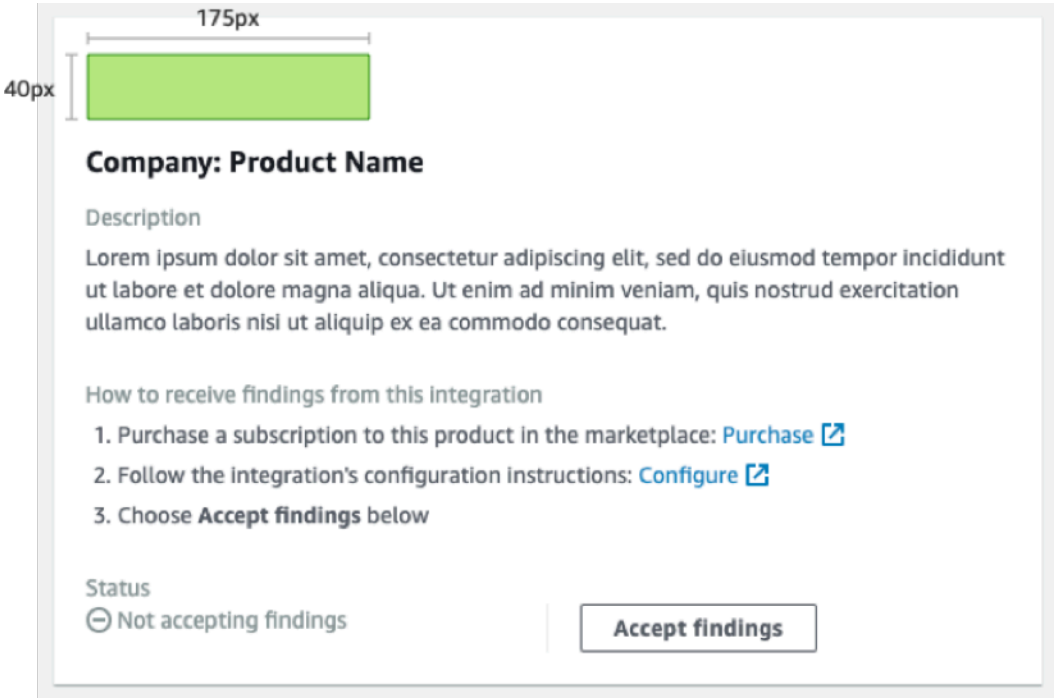
Tamanho

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

A altura mínima é de 40 px.

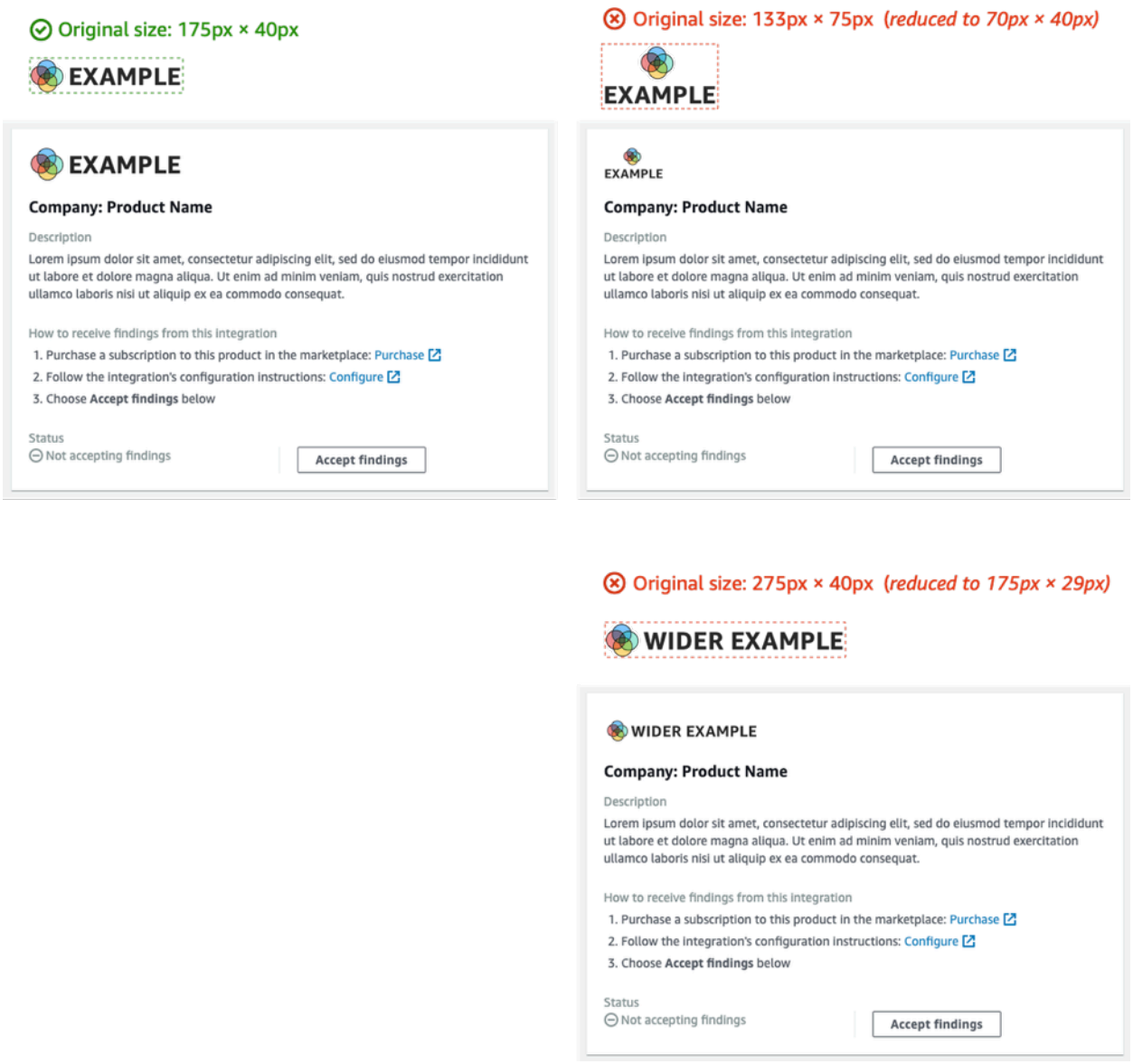
Logotipos retangulares funcionam melhor.

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



Se o seu logotipo não corresponder a essas dimensões, o Security Hub reduz 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.

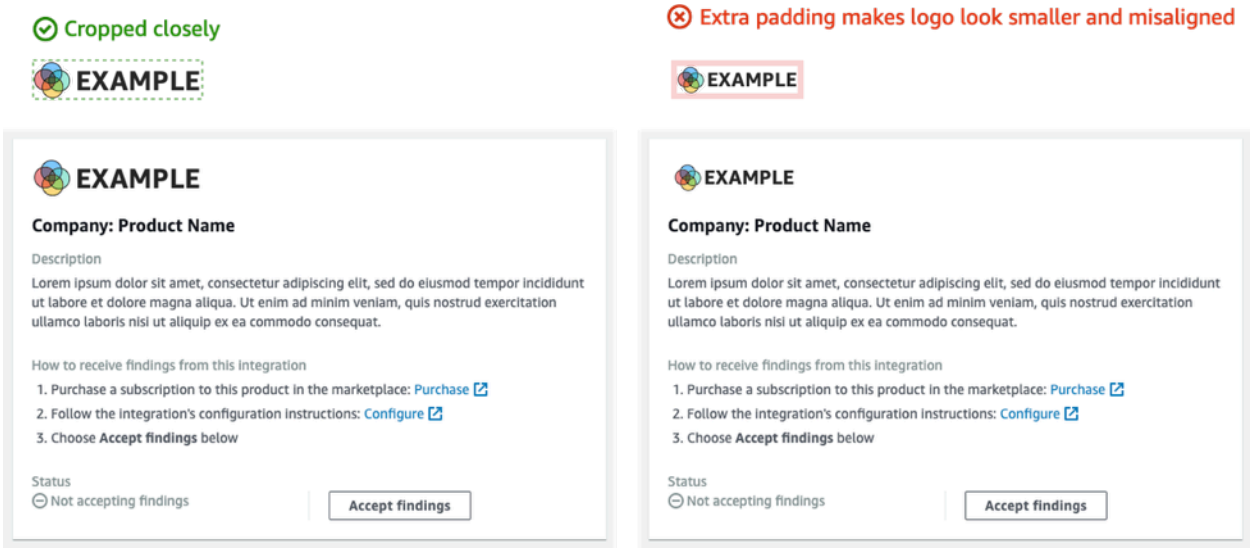
A imagem a seguir compara a exibição de um logotipo que usou o tamanho ideal para logotipos mais largos ou mais altos.



Cortando

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

A imagem a seguir mostra a diferença entre um logotipo que é cortado de perto e um logotipo com preenchimento extra.



Princípio para criar e atualizar descobertas

Conforme você planeja como você criará e atualizará descobertas noAWS Security Hub, tenha os seguintes princípios em mente.

Torne as descobertas específicas para que os clientes possam agir facilmente sobre elas.

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

- Eles geralmente devem lidar com um único ou principal recurso.
- Eles devem ter um único tipo de descoberta.
- Eles devem lidar com um único evento de segurança.

Quando uma descoberta contém dados para vários eventos de segurança, é mais difícil para os clientes tomarem medidas sobre a descoberta.

Mapeie todos os seus campos de descoberta para oAWSFormato de descoberta de segurança (ASFF). Permita que os clientes confiem no Security Hub como fonte de verdade.

Os clientes esperam que todos os campos que estão em seu formato de descoberta nativo também sejam representados no Security Hub ASFF.

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

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

O Security Hub não é uma ferramenta geral de gerenciamento de registros. Você deve enviar descobertas para o Security Hub altamente acionáveis e que os clientes podem responder diretamente, corrigir ou correlacionar com outras descobertas.

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

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

Por exemplo, criar descobertas para varreduras de portas individuais em tempo real não é altamente acionável. Como a varredura de portas pode acontecer continuamente, ela produziria um grande volume de descobertas. É muito mais atraente e preciso simplesmente atualizar o último tempo de varredura e contar a verificação em uma única descoberta para uma varredura de porta em uma porta MongoDB a partir de um nó TOR.

Permita que os clientes personalizem suas descobertas para torná-los mais significativos.

Os clientes querem ser capazes de ajustar determinados campos de descoberta para torná-los mais relevantes para seu ambiente ou requisitos.

Por exemplo, os clientes desejam adicionar notas, tags 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 noAWSFormato de descoberta de segurança da (ASFF)

Use as diretrizes a seguir para mapear suas descobertas para o ASFF. Para obter descrições detalhadas de cada campo e objeto ASFF, consulteAWSFormato de descoberta de segurança da (ASFF)noAWS Security HubGuia do usuário do.

Identificando informações

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

`ProductArn`é o ARN queAWS Security Hubatribui a você.

`Id`é o valor que o Security Hub usa para indexar descobertas. O identificador de 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 que`Id`ou pode se referir a uma unidade de lógica discreta, como uma AmazonGuardDutyID do detector,AWS ConfigID do gravador ou ID do analisador de acesso IAM.

Title e Description

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

Adicione informações detalhadas mais longas ao`Description`.`Description`está limitado a 1024 caracteres, incluindo espaços. Você pode considerar adicionar truncamento 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 de tipo de descoberta em`FindingProviderFields.Types`.

`Types`Deve corresponder aoTipos de taxonomia para ASFF.

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

Timestamps

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

`CreatedAt` e **`UpdatedAt`**

Você deve enviar`CreatedAt`e`UpdatedAt`toda vez que você liga`BatchImportFindings`para cada achado.

Os valores devem corresponder ao formato ISO8601 no Python 3.8.

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

`FirstObservedAt` e `LastObservedAt`

`FirstObservedAt`e `LastObservedAt`deve corresponder quando seu sistema observou a descoberta. Se você não registrar essas informações, não precisará enviar esses carimbos de data/hora.

Os valores correspondem ao formato ISO8601 no Python 3.8.

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

Severity

Você fornece informações de gravidade na`FindingProviderFields.Severity`objeto, que contém os campos a seguir.

`Original`

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

`Label`

O indicador Security Hub necessário da gravidade de descoberta. Os valores permitidos são os seguintes.

- `INFORMATIONAL`— Nenhum problema foi encontrado.
- `LOW`— O problema não requer ação por conta própria.
- `MEDIUM`— O problema deve ser tratado, mas sem caráter urgente.
- `HIGH`— O problema deve ser tratado como uma prioridade.
- `CRITICAL`— O problema deve ser corrigido imediatamente para evitar danos adicionais.

As descobertas que estão em conformidade sempre devem ter`Label`Defina como`INFORMATIONAL`. Exemplos de`INFORMATIONAL`descobertas são descobertas de verificações de segurança que passaram eAWS Firewall Managerdescobertas que são corrigidas.

Os clientes geralmente classificam as descobertas por sua gravidade para dar às equipes de operações de segurança uma lista de tarefas. Seja conservador ao definir a gravidade da descoberta como`HIGH`ou`CRITICAL`.

Sua documentação de integração deve incluir sua lógica de mapeamento.

Remediation

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

`Remediation.Recommendation.Text`aparece nocorreçãoseção dos detalhes de descoberta. Ele está com hiperlink para o valor de`Remediation.Recommendation.Url`.

Atualmente, apenas 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 uma URL vinculada ao console para essa descoberta específica. Caso contrário, omita-o do mapeamento.

O Security Hub não oferece suporte a hiperlinks desse campo, mas é 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 malware que faz uma conexão de saída com um comando conhecido e nó de controle, forneça os detalhes para a instância do EC2 em`Resource.Details.AwsEc2Instance`. Forneça o relevante`Malware`,`Network`, e`ThreatIntelIndicator`Objetos para essa instância do EC2.

Malware

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

Cada entrada tem os seguintes campos.

`Name`

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

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

`Path`

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

- Se você digitalizar objetos em um bucket do S3 ou em um compartilhamento EFS 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 caminho do clone.

`State`

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

No título e na descrição da descoberta, certifique-se de fornecer contexto para o que aconteceu com o malware.

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

Se`Malware.State`é`OBSERVED`e, em seguida, o título e a descrição da descoberta devem 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|POTEN`

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 fonte

O destino e a origem são fáceis de mapear logs de fluxo TCP ou VPC ou logs WAF. Eles são mais difíceis de usar quando você está descrevendo informações de rede para uma descoberta sobre um ataque.

Normalmente, a fonte é de onde o ataque se originou, mas pode ter 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 DDoS em uma instância do EC2, a origem é o invasor, embora um ataque DDoS real possa usar milhões de hosts. O destino é o endereço IPv4 público da instância EC2.`Direction`está IN.
- Para malware observado se comunicando de uma instância do EC2 para um nó de comando e controle conhecido, a origem é o endereço IPV4 da instância do EC2. O destino é o nó de comando e controle.`Direction`é`OUT`. Você também forneceria`MalwareeThreatIntelIndicators`.

`Protocol`

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

`Protocol`é independente das informações de origem e destino. Apenas forneça quando fizer sentido fazê-lo.

`Direction`

`Direction`é sempre relativo ao*AWS*Limites de rede.

- `IN`significa que está entrando*AWS*(VPC, serviço).
- `OUT`significa que está saindo do*AWS*Limites de rede.

Process

`Process`é um único objeto. Você não pode 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 Linux (PID) ou ao ID de evento do Windows. Para diferenciar, use Imagens de máquina da Amazon do EC2 (AMIs) para fornecer as informações. Os clientes provavelmente podem 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 para o milissegundo, não as forneça.

Se um cliente depende de carimbos de data/hora para investigação forense, então não ter carimbo de data/hora é melhor do que ter o carimbo de data/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 sã`DOMAIN`|`EMAIL_ADDRESS`|`HASH_MD5`|`HASH_SHA1`|`HASH_SHA256`|`HASH_SHA512`|`IPV4_ADDRESS`|`IPV6_`

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

- Você encontrou um processo que você sabe que está associado ao Cobalt Strike. Você aprendeu isso comFireEye.

  Defina `Type` para `PROCESS`. Crie também um`Process`objeto para o processo.

- Seu filtro de e-mail encontrou alguém enviando um pacote hash bem conhecido de um domínio malicioso conhecido.

  Criar dois`ThreatIntelIndicator`objetos. Um objeto é para o`DOMAIN`. O outro é para o`HASH_SHA1`.

- Você encontrou malware com uma regra Yara (Loki, Fenrir, Awss3VirusScan,BinaryAlert).

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

Resources

para o`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 registro mensal das alterações no ASFF, entre em contato`<securityhub-partners@amazon.com>`.

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

Para um recurso que não é modelado em ASFF, defina`Type`para`Other`. Para obter informações detalhadas, use`Details.Other`.

Você também pode usar o`Other`tipo de recurso para não-AWSDescobertas.

ProductFields

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

Se você usar`ProductFields`, você deve fornecer uma lógica rigorosa para essa decisão.

Compliance

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

Usar o Security Hub`Compliance`para as descobertas que ele gera com base em controles.

Usar Firewall Manager`Compliance`por suas descobertas porque estão relacionadas à conformidade.

Campos restritos

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

Não mapeie para esses campos ou objetos.

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

- `Workflow`

Para esses campos, mapeie para os campos que estão na`FindingProviderFields`objeto. Não mapeie para os campos de nível superior.

- `Confidence`— Inclua apenas uma pontuação de confiança (0-99) se o seu serviço tiver uma funcionalidade semelhante ou se você ficar 100% por sua descoberta.
- `Criticality`— O escore de criticidade (0-99) destina-se a expressar a importância do recurso associado ao achado.
- `RelatedFindings`— Forneça apenas descobertas relacionadas 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 descoberta de uma descoberta que já está no Security Hub.

Diretrizes para usar o**`BatchImportFindings`**API

Ao usar o`BatchImportFindings`Operação da API para enviar descobertas aoAWS Security Hub, use as seguintes diretrizes.

- Você deve ligar`BatchImportFindings`usando a conta associada às descobertas. O identificador da conta associada é o valor do`AwsAccountId`atributo 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 de taxa de aceleração é de 10 TPS por conta por região, com um burst de 30 TPS.
- Você deve implementar um mecanismo para manter o estado das descobertas se existirem problemas de limitação ou rede. Você também precisa do estado de descoberta para que você possa enviar atualizações de busca à medida que uma descoberta entra e sai da conformidade.
- Para obter informações sobre os comprimentos máximos de strings e outras limitações, consulteAWSFormato de descoberta de segurança da (ASFF)noAWS Security HubGuia do usuário do.

Lista de verificação de prontidão

OAWS Security Hube as equipes de parceiros da APN usam essa lista de verificação para validar se a integração está pronta para ser iniciada.

Mapeamento do ASFF

Essas perguntas estão relacionadas ao mapeamento de sua descoberta para oAWSFormato de descoberta de segurança (ASFF).

Todos os dados de descoberta do parceiro estão mapeados para o ASFF?

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

O parceiro usa**`Resource.Details`**campos, como**`AwsEc2instance`**,**`AwsS3Bucket`**, e**`Container`**?

O parceiro usa**`Resource.Details.Other`**para definir detalhes do recurso que não são modelados no ASFF?

- Sempre que possível, use os campos fornecidos para recursos selecionados como instâncias do EC2, buckets do S3 e security groups em suas descobertas.
- Mapeie outras informações relacionadas a recursos para`Resource.Details.Other`somente quando não há correspondência direta.

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

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

As informações do mapa do parceiro**`ProductFields`**que poderiam ser mapeados para outros campos ASFF?

- Use somente`ProductFields`para informações específicas do produto, como informações de controle de versão, descobertas de gravidade específicas do produto ou outras informações que não podem ser mapeadas em um campo com curadoria ou`Resources.Details.Other`.

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

- O`FirstObservedAt`timestamp destina-se a registrar o horário em que um achado foi observado no produto. Mapeie esse campo, se possível.

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

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

Você também deve manter o estado do identificador de descoberta com a finalidade de atualizar as descobertas.

O parceiro fornece um valor que mapeia 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 descobertas pelo que as gerou.

Isso pode ser um subcomponente dentro de um produto (Produto A - Vulnerabilidade vs Produto A - EDR) ou algo semelhante.

O parceiro usa os namespaces de tipos de descoberta necessários de uma forma relevante para o produto? O parceiro usa as categorias de tipo de descoberta recomendadas ou classificadores em seus tipos de descoberta?

A taxonomia do tipo de descoberta deve mapear de perto as descobertas geradas pelo produto.

Os namespaces de primeiro nível descritos naAWSFormato de descoberta de segurança é necessário.

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

O parceiro captura informações de fluxo de rede na**`Network`**campos, se eles tiverem dados de rede?

Se o produto capturarNetFlowinformações, mapeie-as para o`Network`campo.

As informações do processo de captura do parceiro (PID) no**`Process`**campos, se eles tiverem dados de processo?

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

O parceiro captura informações de malware na**`Malware`**campos, se eles tiverem dados de malware?

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

O parceiro captura informações de inteligência contra ameaças no**`ThreatIntelIndicators`**campos, se eles tiverem dados de inteligência contra ameaças?

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

O parceiro fornece uma classificação de confiança para as descobertas? Se o fizerem, um raciocínio é fornecido?

Sempre que você usar esse campo, forneça uma lógica na documentação e no manifesto.

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

Ao identificarAWSrecursos, 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 eday-to-dayfunção da integração.

O parceiro fornece uminfrastructure-as-codeModelo (iAC) para implantar a integração com o Security Hub, como o Terraform,AWS CloudFormation, ouAWS Cloud Development Kit (AWS CDK)?

Para integrações que enviarão descobertas da conta do cliente ou usarãoCloudWatchEventos para consumir descobertas, alguma forma de modelo IAC é necessária.

AWS CloudFormationÉ preferido, masAWS CDKou Terraform também pode ser usado.

O produto parceiro tem uma configuração com um clique no console para integração com o Security Hub?

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

O parceiro só envia descobertas de valor?

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

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

O parceiro forneceu uma estimativa de quantas descobertas enviarão por dia por cliente e em 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 for preenchida apenas`ThreatIntelIndicators`e outro povoado apenas`Resources.Details.AWSEc2Instance`, essas são duas descobertas únicas.

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

Atualmente, há uma taxa de intermitência de 30 a 50 TPS no`BatchImportFindings`Operação da API. Se forem retornados erros 4xx ou 5xx, você deverá manter o estado dessas descobertas com falha para que possa repeti-las na totalidade posteriormente. Você pode fazer isso por meio de uma fila de letras mortas ou outraAWSserviços de mensagens, como Amazon SNS ou Amazon SQS.

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

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

Se você fornecer descobertas, não use o`BatchUpdateFindings`operação para atualizar descobertas. Esta operação só deve ser usada pelos clientes. Você só usa`BatchUpdateFindings`Quando você investiga e toma medidas sobre 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 as IDs de descoberta originais no caso de erros para que você não duplique ou substitua descobertas bem-sucedidas por engano.

O parceiro atualiza as descobertas ligando para o**`BatchImportFindings`**operação com o ID de descoberta dos achados existentes?

Para atualizar uma descoberta, você deve substituir a descoberta existente enviando o mesmo ID de descoberta.

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

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

Se você tomar medidas em relação às descobertas, você pode usar o`BatchUpdateFindings`operação para atualizar campos específicos.

O parceiro fornece informações sobre a quantidade de latência entre quando uma descoberta é criada e quando ela é enviada de seu produto para o Security Hub?

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

Essas informações são necessárias no manifesto.

Se a arquitetura do parceiro for enviar descobertas para o Security Hub a partir de uma conta de cliente, eles demonstraram isso com sucesso? Se a arquitetura do parceiro for enviar descobertas para o Security Hub a partir de sua própria conta, eles demonstraram isso com sucesso?

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

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

O parceiro fornece uma descoberta de pulsação para o Security Hub?

Para mostrar que sua integração está funcionando corretamente, você deve enviar uma descoberta de pulsação. A descoberta de 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 com a conta da equipe de produtos Security Hub durante o teste?

Durante a validação de pré-produção, você deve enviar exemplos de descoberta para a equipe de produtos do Security HubAWSconta. 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, Leia os documentos ou outro formato dedicado.

Documentação de hospedagem emGitHubnão satisfaz o requisito do site dedicado.

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

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

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

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 o raciocínio para os tipos de descobertas que você envia.

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

A documentação do parceiro fornece uma justificativa de como o parceiro mapeia suas descobertas para o ASFF?

Você deve fornecer a lógica 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 orientações sobre como o parceiro atualiza as descobertas, se eles atualizarem as descobertas?

Forneça aos clientes informações sobre como você mantém o estado, garante a idempotência e substitui descobertas comup-to-dateInformações.

A documentação do parceiro descreve encontrar latência?

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

Essas informações são necessárias no manifesto.

A documentação do parceiro descreve como a pontuação de gravidade deles mapeia para a pontuação de gravidade ASFF?

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

Por exemplo, se seu valor de gravidade for uma nota de letra (A, B, C), você deverá fornecer informações sobre como mapear a nota da letra para o rótulo de gravidade.

A documentação do parceiro fornece uma justificativa para as classificações de confiança?

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

Se você usar pontuações de confiança estaticamente preenchidas ou mapeamentos derivados de inteligência artificial ou aprendizado de máquina, você deve fornecer contexto adicional.

A documentação do parceiro observa quais regiões o parceiro suporta e não?

Observação Regiões que são ou não têm suporte para que os clientes saibam em quais regiões não tentar uma integração.

Informações do cartão

Essas perguntas estão relacionadas ao cartão do produto exibido noIntegraçõespágina do console do Security Hub.

É o fornecidoAWSID da conta válido e contém 12 dígitos?

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

A descrição do produto contém 200 ou menos caracteres?

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

O link de configuração leva à documentação para a integração?

O link de configuração deve levar à documentação online. Ele não deve levar ao seu site principal ou a páginas de marketing.

O link de compra (se fornecido) leva aoAWS Marketplacelistagem para o produto?

Se você fornecer um link de compra, ele deve ser para umAWS MarketplaceEntrada. O Security Hub não aceita links de compra que não são hospedados porAWS.

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 dos produtos são válidos e corretos?

O nome da empresa deve ter 16 ou menos caracteres.

O nome do produto deve ter 24 ou menos caracteres.

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

Informações de marketing

Essas perguntas estão relacionadas ao marketing para a integração.

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

A página de parceiros do Security Hub aceita apenas 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 acessível ao público com um 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 dedicada do parceiro sobre a integração?

OSaiba maislink 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 instrucional sobre como usar sua integração?

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

É umAWSPublicação do blog da Partner Network sendo lançada com o parceiro e seu gerente de desenvolvimento de parceiros ou representante de desenvolvimento de parceiros?

AWSAs postagens do blog da Partner Network devem ser coordenadas antes do tempo com o gerente de desenvolvimento de parceiros ou representante de desenvolvimento de parceiros.

Eles são separados de qualquer postagem de blog que você mesmo criar.

Aguarde o prazo de 4 a 6 semanas. Esse esforço deve ser iniciado após a conclusão do teste com o ARN do produto privado.

Um comunicado de imprensa liderado por parceiros 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 cotação em seu comunicado de imprensa.

Uma postagem de blog liderada por parceiros está sendo lançada?

Você pode criar suas próprias postagens de blog para mostrar a integração fora doAWSBlog do Partner Network.

Um webinar liderado 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 do produto depois de concluir o teste com o ARN do produto privado.

O parceiro solicitou suporte para redes sociais deAWS?

Após o lançamento, você pode trabalhar com oAWSO marketing de segurança leva ao usoAWScanais oficiais de mídia social para compartilhar detalhes sobre seus webinars.

AWS Security HubPerguntas frequentes sobre parceiros

A seguir, são perguntas comuns sobre como configurar e manter uma integração comAWS Security Hub.

1. Quais são os benefícios da integração com o Security Hub?
   - Meeting satisfaction do— O motivo número um para se integrar ao Security Hub é porque você tem solicitações de clientes para fazê-lo.

     O Security Hub é o centro de segurança e conformidade paraAWSclientes. Ele é projetado como a primeira parada ondeAWSprofissionais de segurança e conformidade vão todos os dias para entender seu estado de segurança e conformidade.

     Ouça seus clientes. Eles informarão se querem ver suas descobertas no Security Hub.
   - Oportunidades do— Promovemos parceiros com integrações certificadas dentro do console do Security Hub, incluindo links para seusAWS Marketplacelistagens. Esta é uma ótima maneira de os clientes descobrirem novos produtos de segurança.
   - Oportunidades de— Os fornecedores com integrações aprovadas podem participar de webinars, emitir comunicados à imprensa, criar planilhas e demonstrar suas integrações paraAWSclientes.
2. Que tipos de parceiros existem?
   - Parceiros que enviam descobertas para o 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 em seu ambiente
3. Como a integração de um parceiro com o Security Hub funciona em alto nível?

   Você reúne descobertas de dentro de uma conta de cliente ou de sua própriaAWSconta e transforme o formato das descobertas para oAWSFormato de descoberta de segurança da (ASFF) da. Em seguida, você envia essas descobertas para o endpoint regional apropriado do Security Hub.

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

a. Envie as informações sobre o manifesto do parceiro.

b. Receba ARNs de produtos para usar com o Security Hub, se você enviar descobertas para o Security Hub.

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

d. Defina sua arquitetura para enviar descobertas e receber descobertas do Security Hub. Siga os princípios descritos emthe section called “Princípio para criar e atualizar descobertas”.

e. Crie uma estrutura de implantação para clientes. Por exemplo,AWS CloudFormationscripts podem servir a esse propósito.

f. Documente sua configuração e forneça instruções de configuração para os clientes.

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

h. Demonstre sua integração com a equipe do Security Hub.

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

5. Qual é o processo para enviar o manifesto do parceiro? E paraAWSServiços para enviar descobertas para o Security Hub?

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

   Você recebe ARNs de produto dentro de sete dias corridos.

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

   O preço do Security Hub é parcialmente baseado no número de descobertas ingeridas. Por isso, você deve abster-se de enviar descobertas que não fornecem valor aos clientes.

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

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

   Estas são as principais abordagens:

   - Você envia descobertas de seus próprios designadosAWSconta usando o`BatchImportFindings`operação.

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

Para obter diretrizes gerais sobre o uso`BatchImportFindings`, consultethe section called “Diretrizes para usar o`BatchImportFindings`API”.

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

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

   Por exemplo, alguns parceiros criam um aplicativo Python que pode ser implantado como umAWS CloudFormationscript. O script reúne as descobertas do parceiro do ambiente do cliente, as transforma em 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 levar descobertas para o Security Hub.

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

   O Security Hub oferece suporte à autorização parcial em lote para o`BatchImportFindings`Operação da API, para que você possa enviar todas as suas descobertas para o 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 só ingere descobertas autorizadas que estão no lote.

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

    a. Certifique-se de que as políticas do IAM corretas estejam em vigor.

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

    c. Verifique se o`ProductArn`da descoberta é o ARN público do seu produto.

    d. Verifique se o`AwsAccountId`da descoberta é o ID da conta do cliente.

    e. Certifique-se de que suas descobertas não tenham dados mal formados de acordo com aAWSFormato de descoberta de segurança da (ASFF) da. 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 eu enviar descobertas?

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

O teste mais fácil é fazer isso a partir de uma conta de administrador. Você pode restringi-los `aaction: 'securityhub:BatchImportFindings'eresource:` *`<productArn and/or productSubscriptionArn>`*.

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

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

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

Certifique-se de verificar se não há `Deny` Políticas para o chamador. Depois de trabalhar com isso, 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 de parceiro específico, o cliente (ou o parceiro com funções entre contas trabalhando em nome do cliente) deve estabelecer uma assinatura de

produto. Para fazer isso no console, eles usam oIntegrações. Para fazer isso a partir da API, eles usam o`EnableImportFindingsForProduct`Operação da API.

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

O Security Hub tem os seguintes tipos de políticas 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 ambos os tipos de políticas.

com`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, você só pode enviar descobertas para o Security Hub a partir da conta listada no ARN do produto.

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

13. Suponha que um cliente tenha criado uma conta de administrador e tenha adicionado algumas contas de membro. O cliente precisa assinar cada conta de membro para mim? Ou o cliente assina apenas a partir da conta de administrador e, em seguida, posso enviar descobertas sobre recursos em todas as contas de membro?

    Esta pergunta pergunta se as permissões são criadas para todas as contas de membro com base no registro da conta de administrador.

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

14. Qual é o meu produto ARN?

    O ARN do 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 integrado ao Security Hub. O ARN correto do produto deve fazer parte de cada descoberta enviada para o Security Hub. As descobertas sem o ARN do produto são descartadas. O ARN do produto usa o seguinte formato:

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

Aqui está um 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 é implantado. O ID da conta, a empresa e os nomes do produto são ditados pelos envios do manifesto do parceiro. Você nunca altera nenhuma das informações associadas ao ARN do produto, exceto pelo código da região. O código da região deve corresponder à Região para a qual você envia descobertas.

Um erro comum é alterar o ID da conta para corresponder à conta de onde 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 produto.

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

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

15. Qual formato deve ser usado para enviar descobertas para o Security Hub?

    As descobertas devem ser fornecidas naAWSFormato de descoberta de segurança da (ASFF) da. Para obter mais detalhes, consulte .AWSFormato de descoberta de segurança da (ASFF)noAWS Security HubGuia do usuário do.

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

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

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

17. Onde posso encontrar a lista de endpoints regionais?

    Consulte oLista de pontos de extremidade do Security Hub.

18. Posso enviar descobertas entre regiões?

O Security Hub ainda não oferece suporte ao envio entre regiões de descobertas para o nativoAWSserviços, como a AmazonGuardDuty, Amazon Macie e Amazon Inspector. Se o cliente permitir, o Security Hub não impedirá 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,`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`. Enfileirar e colocar 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 no lote não estiver inscrita no Security Hub, o lote inteiro falhará. Essa é uma limitação do modelo de autorização de linha de base do API Gateway.

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

20. Posso enviar atualizações para descobertas que criei?

Sim, se você enviar uma descoberta com o mesmo ARN do produto e o mesmo ID de descoberta, ele substituirá os dados anteriores dessa descoberta. Observe que todos os dados são substituídos, portanto, você deve enviar uma descoberta completa.

Os clientes são medidos e cobrados pelas novas descobertas e pela descoberta de atualizações.

21. Posso enviar atualizações para descobertas que outra pessoa criou?

Sim, se o cliente conceder acesso ao`BatchUpdateFindings`Operação da API, você pode atualizar determinados campos usando essa operação. Esta operação foi projetada para ser usada por clientes, SIEMs, sistemas de emissão de bilhetes e plataformas de Orquestração, Automação e Resposta de Segurança (SOAR).

22. Como as descobertas envelhecem?

O Security Hub envelhece as descobertas 90 dias após a última data da atualização. Após esse período, as descobertas envelhecidas são removidas do Security HubOpenSearchCluster.

Se você atualizar uma descoberta com o mesmo ID de descoberta e ela tiver sido envelhecida, uma nova descoberta será criada no Security Hub.

Os clientes podem usarCloudWatchEventos para mover descobertas do Security Hub. Isso permite que todas as descobertas sejam enviadas para metas de escolha do cliente.

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

23. Que aceleradores o Security Hub implementa?

aceleradores do Security Hub`GetFindings`Chamadas de API, pois a abordagem recomendada para acessar descobertas está usandoCloudWatchEvents (Eventos).

O Security Hub não implementa nenhuma outra limitação em serviços internos, parceiros ou clientes além do imposto pelas invocações do API Gateway e do Lambda.

24. Quais são os SLAs de pontualidade ou latência ou expectativas para descobertas que são enviadas ao Security Hub a partir dos serviços de origem?

O objetivo é ser o mais próximo possível em tempo real para descobertas iniciais e atualizações das descobertas. Você deve enviar descobertas para o Security Hub dentro de cinco minutos após elas serem criadas.

25. Como posso receber descobertas do Security Hub?

Para receber descobertas, use um dos métodos a seguir.

- Todas as descobertas são enviadas automaticamente paraCloudWatchEvents (Eventos). Um cliente pode criar específicoCloudWatchRegras de eventos para enviar descobertas a destinos específicos, como um SIEM ou um bucket do S3. Esse recurso substituiu o legado`GetFindings`Operação da API.
- Usar oCloudWatchEventos para ações personalizadas. O Security Hub permite que os clientes selecionem descobertas ou grupos específicos de descobertas dentro do console e tomem medidas sobre elas. Por exemplo, eles podem enviar descobertas para um SIEM, sistema de emissão de tickets, 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. Eles são chamados de ações personalizadas.

  Quando um usuário seleciona uma ação personalizada, umCloudWatchevento é criado para essas descobertas específicas. Você pode aproveitar esse recurso e construirCloudWatchRegras de eventos e metas 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 paraCloudWatchEvents (Eventos). Cabe a um usuário agir sobre descobertas específicas.

Você pode usar as operações da API de ação personalizada, como`CreateActionTarget`, para criar automaticamente ações disponíveis para seu produto (como usarAWS CloudFormationModelos do). Você também usariaCloudWatchOperações de API de regras de eventos para criar o correspondenteCloudWatchRegras de eventos associadas à ação personalizada. O uso doAWS CloudFormationmodelos, você também pode criarCloudWatchRegras de 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 de segurança gerenciado (MSSP) se torne um parceiro do Security Hub?

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

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

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

Se o MSSP receber apenas descobertas do Security Hub, eles devem, no mínimo, ter umAWS CloudFormationModelo para configurar o apropriadoCloudWatchRegras de eventos.

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

Se você for um parceiro de consultoria da APN, você pode se tornar um parceiro do Security Hub. Você deve enviar dois estudos de caso privados sobre como ajudou um cliente específico a fazer o seguinte.

- Configure o Security Hub com permissões do IAM que o cliente precisa.
- Ajude a conectar soluções ISV (fornecedor independente de software) já integradas ao Security Hub usando as instruções de configuração na página do parceiro no console.
- Ajude os clientes com integrações de produtos personalizadas.
- Crie insights personalizados relevantes para as necessidades e conjuntos de dados do cliente.
- Crie ações personalizadas.
- Crie playbooks de correção.

- Crie Quickstarts alinhados aos padrões de conformidade do Security Hub. Eles devem ser validados pela equipe do Security Hub.

Estudos de caso não precisam ser compartilháveis publicamente.

28. Quais são os requisitos sobre 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 para a integração não leve mais que 15 minutos.

Se você estiver implantando software de integração noAWSambiente, você deve aproveitarAWS CloudFormationmodelos para simplificar a integração. Alguns parceiros criaram uma integração com um clique, o que é altamente incentivado.

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 deAWS CloudFormationModelos do.

Essa documentação também deve incluir informações sobre o uso do ASFF. Especificamente, isso deve listar os tipos de descoberta ASFF que você está usando para suas diferentes descobertas. Se você tiver alguma definição de insight padrão, recomendamos que também as inclua aqui.

Considere incluir outras informações em potencial:

- Seu caso de uso para integração com o Security Hub
- Volume médio de descobertas enviadas
- Sua arquitetura de integração
- As regiões que você faz e não oferece suporte
- Latência entre quando as descobertas são criadas e quando elas são enviadas para o Security Hub
- Se você atualiza descobertas

30. O que são insights personalizados?

Você é incentivado a definir insights personalizados para suas descobertas. Insights são regras de correlação leves que ajudam um cliente a priorizar quais descobertas e recursos mais exigem atenção e ação.

O Security Hub tem um`CreateInsight`Operação da API. Você pode criar insights personalizados dentro de uma conta de cliente como parte de suaAWS CloudFormationTemplate Template Esses insights aparecem no console do cliente.

31. Posso enviar widgets de painel?

Não neste momento. Você só pode criar insights gerenciados.

32. Qual é o seu modelo de preços?

Consulte oInformações sobre preços do Security Hub.

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

Envie descobertas para a conta de demonstração do Security Hub usando o ARN do produto fornecido, usando`us-west-2`como a Região. As descobertas devem incluir o número da conta demo na`AwsAccountId`campo de ASFF. Para obter o número da conta demo, entre em contato com a equipe do Security Hub.

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

34. Que mensagens de erro ou sucesso fazem**`BatchImportFindings`**Forneça?

O Security Hub fornece uma resposta para autorização e uma resposta para`BatchImportFindings`. Mensagens de sucesso, falha e erro mais nítidas 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, limitação e alarmante. Eles também devem lidar com feedback ou mensagens de erro enviadas por meio do mecanismo de feedback do Security Hub.

36. Quais são algumas resoluções para problemas comuns?

UmaAuthorizerConfigurationExceptioné causada por um malformadoAwsAccountIdouProductArn.

Ao solucionar problemas, observe o seguinte:

- AwsAccountIddeve ter 12 dígitos exatamente.
- ProductArnDeve estar no seguinte formato: arn:aws:securityHub:*<us-west-2 or us-east-1>*:*<accountId>*:product/*<company-id>*/*<product-id>*

  O ID da conta não muda daquele que a equipe do Security Hub incluiu nos ARNs do produto que eles forneceram a você.

AccessDeniedExceptioné causado quando uma descoberta é enviada para ou da conta errada, ou quando a conta não tem umProductSubscription. A mensagem de erro conterá um ARN com um tipo de recurso deproductouproduct-subscription. Esse erro ocorre somente durante chamadas entre contas. Se você ligarBatchImportFindingscom sua própria conta para a mesma conta emAwsAccountIdeProductArn, a operação usa políticas do IAM e não tem nada a ver comProductSubscriptions.

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

37 Para onde envio perguntas, comentários e bugs?

<securityhub-partners@amazon.com>

38 Para qual região eu envio descobertas para itens relacionados ao globalAWSServiços? Por exemplo, para onde envio descobertas relacionadas ao IAM?

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

Se o cliente executar o Security Hub em três regiões e o mesmo problema do IAM for detectado em todas as três regiões, envie a descoberta para todas as três regiões.

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

Histórico de documentos do Guia de integração de parceiros

A tabela a seguir descreve as atualizações da documentação para este guia.

Alteração	Descrição	Data
Requisitos atualizados para o logotipo do console	As diretrizes do logotipo e do manifesto 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 que parceiros que se juntaram aoAWSCaminho de parceiro ISV e que usam um produto de integração que concluiu umaAWSRevisão Técnica Fundacional (FTR). Anteriormente, era necessário que todos os parceiros de integração fossemAWS Selecione Parceiros de nível.	29 de abril de 2021
NovoFindingProviderFields objeto em ASFF	Atualizou as informações sobre o mapeamento dos resultados para o ASFF. ParaConfidence ,Criticality ,RelatedFindings ,Severity, eTypes, os parceiros mapeiam seus valores para os campos	18 de março de 2021

	`emFindingProviderFields` .	
Novos princípios para criar e atualizar descobertas	Foi adicionado um novo conjunto de diretrizes para criar novas descobertas e atualizar descobertas existentes no Security Hub.	4 de dezembro de 2020
Versão inicial do guia	IssoGuia de integração de parceirosforneceAWSparceiros com informações sobre como estabelecer uma integração comAWS 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.