Guide d'intégration de partenaire

AWS Security Hub

AWS Security Hub: Guide d'intégration de partenaire

Table of Contents

Vue d'ensemble de l'intégration tierce avecAWS Security Hub

Ce guide est destiné auxAWSPartenaires du réseau de partenaires (APN) qui souhaitent créer une intégration avecAWS Security Hub.

En tant que partenaire APN, vous pouvez intégrer Security Hub d'une ou plusieurs des manières suivantes.

- Envoi des résultats à Security Hub
- Utilisation des résultats de Security Hub
- Les deux envoient des résultats à Security Hub et consomment les résultats de Security Hub
- Utiliser Security Hub comme centre d'une offre de fournisseurs de services de sécurité gérés (MSSP)
- Consulté avecAWSclients sur la façon de déployer et d'utiliser Security Hub

Ce guide d'intégration se concentre principalement sur les partenaires qui envoient des résultats à Security Hub.

Rubriques

Pourquoi intégrer avecAWS Security Hub?

AWS Security Huboffre une vue complète des alertes de sécurité haute priorité et l'état de sécurité sur les comptes Security Hub. Security Hub permet à des partenaires comme vous d'envoyer des résultats de sécurité à Security Hub pour fournir à vos clients des informations sur les résultats de sécurité que vous générez.

Une intégration avec Security Hub peut apporter de la valeur ajoutée des manières suivantes.

- Satisfait vos clients qui ont demandé une intégration Security Hub

- Offre à vos clients une vue unique de leurAWSRésultats liés à la sécurité
- Permet aux nouveaux clients de découvrir votre solution lorsqu'ils recherchent des partenaires qui fournissent des résultats liés à des types spécifiques d'événements de sécurité

Avant de créer une intégration avec Security Hub, examinez les raisons de l'intégration. Une intégration est plus susceptible d'être couronnée de succès si vos clients souhaitent une intégration de Security Hub avec votre produit. Vous pouvez créer une intégration uniquement pour des raisons marketing ou pour acquérir de nouveaux clients. Toutefois, si vous créez l'intégration sans aucune intervention client actuelle et que vous ne tenez pas compte des besoins de vos clients, l'intégration peut ne pas donner les résultats attendus.

Préparation à envoyer des résultats àAWS Security Hub

En tant que partenaire APN, vous ne pouvez pas envoyer d'informations à Security Hub pour vos clients tant que l'équipe Security Hub ne vous autorise pas en tant que fournisseur de recherche. Pour être activé en tant que fournisseur de recherche, vous devez suivre les étapes d'intégration suivantes. Cela garantit une expérience positive de Security Hub pour vous et vos clients.

Lorsque vous terminez les étapes d'intégration, assurez-vous de suivre les instructions dethe section called “Principes de création et de mise à jour des résultats”,the section called “Consignes pour la cartographie ASFF”, etthe section called “Instructions relatives à l'utilisation duBatchImportFindingsAPI”.

1. Mappez vos résultats de sécurité à laAWSFormat ASFF (Security Finding Format).
2. Créez votre architecture d'intégration pour transmettre les résultats vers le point de terminaison Regional Security Hub approprié. Pour ce faire, vous définissez si vous allez envoyer des résultats à partir des vôtresAWSou depuis les comptes de vos clients.
3. Demandez à vos clients d'abonner le produit à leur compte. Pour ce faire, ils peuvent utiliser la console ou le`EnableImportFindingsForProduct`Opération d'API. Voir[Gestion des intégrations de produits](#)dans leAWS Security HubGuide de l'utilisateur.

   Vous pouvez également vous abonner au produit pour eux. Pour ce faire, vous utilisez un rôle entre comptes pour accéder à`EnableImportFindingsForProduct`Opération d'API pour le compte du client.

   Cette étape établit les stratégies de ressources nécessaires pour accepter les résultats de ce produit pour ce compte.

Les articles de blog suivants traitent de certaines des intégrations de partenaires existantes avec Security Hub.

- Annonce de l'intégration Cloud Custodian avecAWS Security Hub
- UtiliserAWS Fargateet Prowler pour envoyer des résultats de configuration de sécuritéAWSServices à Security Hub
- Comment importerAWS ConfigÉvaluations des règles comme résultats dans Security Hub

Se préparer à recevoir les résultats deAWS Security Hub

Pour recevoir les résultats deAWS Security Hub, utilisez l'une des options suivantes :

- Demandez à vos clients d'envoyer automatiquement tous les résultats àCloudWatchÉvénements. Un client peut créer des données spécifiquesCloudWatchrègles d'événement pour envoyer des résultats à des cibles spécifiques, telles qu'un compartiment SIEM ou S3.
- Demandez à vos clients de sélectionner des résultats ou des groupes de résultats spécifiques à partir de la console Security Hub, puis de prendre des mesures à leur sujet.

Par exemple, vos clients peuvent envoyer des résultats à un SIEM, à un système de billetterie, à une plateforme de discussion ou à un workflow de correction. Cela ferait partie d'un processus de triage des alertes effectué par un client dans Security Hub.

Ces actions sont appelées actions personnalisées. Lorsqu'un utilisateur effectue une action personnalisée, unCloudWatchest créé pour ces résultats spécifiques. En tant que partenaire, vous pouvez tirer parti de cette capacité et développerCloudWatchrègles ou cibles d'événements que le client peut utiliser dans le cadre d'une action personnalisée. Notez que cette fonctionnalité n'envoie pas automatiquement tous les résultats d'un type ou d'une classe particulier àCloudWatchÉvénements. Cette fonctionnalité permet à un utilisateur de prendre des mesures sur des résultats spécifiques.

Les articles de blog suivants présentent des solutions utilisant l'intégration avec Security Hub etCloudWatchÉvénements pour les actions personnalisées.

- Comment intégrerAWS Security HubActions personnalisées avecPagerDuty
- Procédure pour activer les actions personnalisées dansAWS Security Hub
- Comment importerAWS ConfigÉvaluations des règles comme résultats dans Security Hub

Ressources pour en savoir plus surAWS Security Hub

Les documents suivants peuvent vous aider à mieux comprendre laAWS Security Hubsolution et commentAWSles clients peuvent utiliser le service.

- Introduction àAWS Security Hubvidéo
- Guide de l'utilisateur Security Hub
- Référence d'API Security Hub
- Webinaire d'intégration

Nous vous encourageons également à activer Security Hub dans l'un de vosAWSet bénéficiez d'une expérience pratique avec le service.

Conditions préalables partenaires

Avant de commencer une intégration avecAWS Security Hub, vous devez répondre à l'un des critères suivants :

- Vous êtes unAWSSélectionnez Partenaire de niveau ou supérieur.
- Vous avez rejoint leAWSParcours partenaires, et le produit que vous utilisez pour l'intégration de Security Hub a terminé uneAWSRevue technique fondamentale (FTR). Le produit reçoit ensuite un « Revu parAWS« badge.

Vous devez également avoir mis en place un accord de non-divulgation mutuelle avecAWS.

Cas d'utilisation de l'intégration et autorisations requises

AWS Security HubpermetAWSles clients doivent recevoir les résultats des partenaires APN. Les produits du partenaire peuvent être exécutés à l'intérieur ou à l'extérieur duAWS. La configuration des autorisations dans le compte du client diffère en fonction du modèle utilisé par le produit partenaire.

Dans Security Hub, le client contrôle toujours quels partenaires peuvent envoyer des résultats sur le compte du client. Les clients peuvent révoquer les autorisations d'un partenaire à tout moment.

Pour permettre à un partenaire d'envoyer des résultats de sécurité sur son compte, le client s'abonne d'abord au produit partenaire dans Security Hub. L'étape d'abonnement est nécessaire pour tous les cas d'utilisation décrits ci-dessous. Pour plus d'informations sur la façon dont les clients gèrent les intégrations de produits, consultezGestion des intégrations de produitsdans leAWS Security HubGuide de l'utilisateur.

Une fois qu'un client s'est abonné à un produit partenaire, Security Hub crée automatiquement une stratégie de ressources gérées. La stratégie accorde au produit partenaire l'autorisation d'utiliser l'option`BatchImportFindings`Opération d'API permettant d'envoyer les résultats à Security Hub pour le compte du client.

Voici les cas courants pour les produits partenaires qui s'intègrent à Security Hub. Les informations incluent les autorisations supplémentaires requises pour chaque cas d'utilisation.

Partenaire hébergé : résultats envoyés depuis un compte partenaire

Ce cas d'utilisation couvre les partenaires qui hébergent eux-mêmes un produit.AWS. Pour envoyer des résultats de sécurité pour unAWSclient, le partenaire appelle le`BatchImportFindings`Octroi d'une opération d'API depuis le compte produit partenaire.

Dans ce cas d'utilisation, le compte client n'a besoin que des autorisations établies lorsque le client s'abonne au produit partenaire.

Dans le compte partenaire, le principal IAM qui appelle le`BatchImportFindings`L'opération d'API doit avoir une stratégie IAM permettant à l'agent principal d'appeler`BatchImportFindings`.

Permettre à un produit partenaire d'envoyer des résultats au client dans Security Hub est un processus en deux étapes :

1. Le client crée un abonnement à un produit partenaire dans Security Hub.
2. Security Hub génère la stratégie de ressources gérées correcte avec la confirmation du client.

Pour envoyer des résultats de sécurité liés au compte du client, le produit partenaire utilise ses propres informations d'identification pour appeler leBatchImportFindingsOpération d'API.

Voici un exemple de stratégie IAM qui accorde au principal du compte partenaire les autorisations nécessaires au 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"
        }
    ]
}
```

Partenaire hébergé : résultats envoyés depuis le compte client

Ce cas d'utilisation couvre les partenaires qui hébergent eux-mêmes un produit.AWSmais utilisez un rôle entre comptes pour accéder au compte du client. Ils appellent l'intentionBatchImportFindingsOpération d'API à partir du compte du client.

Pour ce cas d'utilisation, appelez leBatchImportFindingsOpération API, le compte partenaire assume un rôle IAM géré par le client dans le compte du client.

Cet appel est effectué depuis le compte du client. Par conséquent, la stratégie de ressources gérées doit permettre l'utilisation de l'ARN du produit pour le compte du produit partenaire lors de l'appel. La stratégie de ressources gérées Security Hub accorde l'autorisation pour le compte de produit partenaire et l'ARN du produit partenaire. L'ARN du produit est l'identifiant unique du partenaire en tant que fournisseur. Étant donné que l'appel ne provient pas du compte de produit partenaire, le client doit explicitement accorder au produit partenaire l'autorisation d'envoyer des résultats à Security Hub.

La meilleure pratique pour les rôles entre comptes entre les comptes partenaires et clients consiste à utiliser un identificateur externe fourni par le partenaire. Cet identifiant externe fait partie de la définition de stratégie inter-comptes dans le compte du client. Le partenaire doit fournir l'identifiant lorsqu'il assume le rôle. Un identifiant externe offre une couche de sécurité supplémentaire lors de l'octroiAWSun accès à un partenaire. L'identifiant unique garantit que le partenaire utilise le bon compte client.

L'autorisation d'un produit partenaire d'envoyer des résultats au client dans Security Hub avec un rôle entre comptes se déroule en quatre étapes :

1. Le client, ou le partenaire utilisant des rôles entre comptes travaillant pour le compte du client, démarre l'abonnement à un produit dans Security Hub.
2. Security Hub génère la stratégie de ressources gérées correcte avec la confirmation du client.
3. Le client configure le rôle entre comptes soit manuellement, soit en utilisantAWS CloudFormation. Pour plus d'informations sur les rôles entre comptes, consultezOctroi d'un accèsAWScomptes appartenant à des tiersdans leIAM User Guide.
4. Le produit stocke en toute sécurité le rôle client et l'ID externe.

Le produit envoie ensuite les résultats à Security Hub :

1. Le produit appelle leAWS Security Token Service(AWS STS) pour assumer le rôle de client.
2. Le produit appelle le`BatchImportFindings`Opération API sur Security Hub avec les informations d'identification temporaires du rôle assumé.

Voici un exemple d'une stratégie IAM accordant les Security Hub nécessaires au rôle entre comptes du partenaire.

```
{
    "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"
        }
    ]
```

```
}
```

Le`Resource`de la stratégie identifie l'abonnement spécifique au produit. Cela garantit que le partenaire ne peut envoyer des résultats que pour le produit partenaire auquel le client est abonné.

Hébergé par le client : résultats envoyés depuis le compte client

Ce cas d'utilisation couvre les partenaires disposant d'un produit déployé dans leAWS. Le`BatchImportFindings`L'API est appelée à partir de la solution exécutée dans le compte du client.

Pour ce cas d'utilisation, le produit partenaire doit bénéficier d'autorisations supplémentaires pour appeler le`BatchImportFindings`API. La façon dont cette autorisation est accordée diffère selon la solution partenaire et la façon dont elle est configurée dans le compte du client.

Un exemple de cette approche est un produit partenaire exécuté sur une instance EC2 dans le compte du client. Cette instance EC2 doit être associée à un rôle d'instance EC2 qui lui confère la possibilité d'appeler le`BatchImportFindings`Opération d'API. Cela permet à l'instance EC2 d'envoyer des résultats de sécurité au compte du client.

Ce cas d'utilisation est fonctionnellement équivalent à un scénario dans lequel un client charge les résultats dans son compte pour un produit qu'il possède.

Le client permet au produit partenaire d'envoyer les résultats du compte du client au client dans Security Hub :

1. Le client déploie le produit partenaire dans sonAWScompte manuellement en utilisantAWS CloudFormation, ou un autre outil de déploiement.
2. Le client définit la stratégie IAM nécessaire pour le produit partenaire à utiliser lorsqu'il envoie des résultats à Security Hub.
3. Le client attache la stratégie aux composants nécessaires du produit partenaire, tels qu'une instance EC2, un conteneur ou une fonction Lambda.

Le produit peut désormais envoyer les résultats à Security Hub :

1. Le produit partenaire utilise leAWSkit SDK ouAWS CLIpour appeler l'intention`BatchImportFindings`Opération d'API dans Security Hub. Il effectue l'appel depuis le composant du compte du client sur lequel la stratégie est attachée.

2. Au cours de l'appel d'API, les informations d'identification temporaires nécessaires sont générées pour autoriser le`BatchImportFindings`appelle à réussir.

Voici un exemple de stratégie IAM qui accorde les autorisations Security Hub nécessaires au produit partenaire dans le compte client.

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

Processus d'inscription partenaires

En tant que partenaire, vous pouvez vous attendre à effectuer plusieurs étapes de haut niveau dans le cadre de votre processus d'intégration. Vous devez effectuer ces étapes avant de pouvoir envoyer des résultats de sécurité àAWS Security Hub.

1. Vous initiez un engagement avec l'équipe Partenaire APN ou l'équipe Security Hub et manifestez votre intérêt à devenir partenaire de Security Hub. Vous identifiez les adresses e-mail à ajouter aux canaux de communication Security Hub.
2. AWSvous fournit le matériel d'intégration des partenaires Security Hub.
3. Vous êtes invité sur le canal Slack, partenaire de Security Hub, où vous pouvez poser des questions relatives à votre intégration.
4. Vous fournissez aux contacts partenaires APN un brouillon de manifeste d'intégration de produit pour révision.

   Le manifeste d'intégration du produit contient des informations utilisées pour créer le produit partenaire Amazon Resource Name (ARN) pour l'intégration avecAWS Security Hub.

   Il fournit à l'équipe Security Hub des informations qui apparaissent sur la page du fournisseur partenaire dans la console Security Hub. Il est également utilisé pour proposer de nouvelles informations gérées liées à l'intégration à ajouter à la bibliothèque d'informations Security Hub.

   Cette version initiale du manifeste d'intégration du produit ne doit pas avoir tous les détails. Mais il doit au moins contenir le cas d'utilisation et les informations du jeu de données.

   Pour de plus amples informations sur le manifeste et les informations requises, consultezmanifeste d'intégration de produit.
5. L'équipe Security Hub vous fournit un ARN produit pour votre produit. Vous utilisez l'ARN pour envoyer les résultats à Security Hub.
6. Vous créez votre intégration pour envoyer des résultats à Security Hub ou en recevoir des résultats.

   Cartographie des résultats avec ASFF

   > Pour envoyer des résultats à Security Hub, vous devez mapper vos résultats avec leAWSFormat ASFF (Security Finding Format).

L'ASFF fournit une description cohérente des résultats qui peuvent être partagés entreAWSles services de sécurité, les partenaires et les systèmes de sécurité des clients. Cela réduit les efforts d'intégration, encourage un langage commun et fournit un plan directeur aux implémenteurs.

ASFF est le format de protocole filaire requis pour envoyer les résultats àAWS Security Hub. Les résultats sont représentés sous la forme de documents JSON conformes au schéma JSON ASFF et au format de message I-JSON RFC-7493. Pour plus de détails sur le schéma ASFF, voirAWSFormat ASFF (Security Finding Format)dans leAWS Security HubGuide de l'utilisateur.

Consultez the section called “Consignes pour la cartographie ASFF”.

Construire et tester l'intégration

Vous pouvez effectuer tous les tests de votre intégration à l'aide d'unAWSque vous possédez. Cela vous donne une visibilité complète sur la façon dont les résultats apparaissent dans Security Hub. Il vous aide également à comprendre l'expérience du client avec vos résultats de sécurité.

Vous utilisez le logiciel`BatchImportFindings`Opération API pour envoyer les résultats nouveaux et les résultats mis à jour à Security Hub.

Tout au long de la création d'une intégration Security Hub,AWSvous encourage à tenir vos contacts partenaires APN informés de la progression de votre intégration. Vous pouvez également demander de l'aide à vos contacts partenaires APN pour des questions d'intégration.

Consultez the section called “Instructions relatives à l'utilisation du`BatchImportFindings`API”.

7. Vous démontrez l'intégration à l'équipe produit Security Hub. Cette intégration doit être démontrée à l'aide d'un compte appartenant à l'équipe Security Hub.

   S'ils sont à l'aise avec l'intégration, l'équipe Security Hub donne l'autorisation d'aller de l'avant pour vous répertorier en tant que fournisseur.

8. Vous fournissezAWSavec un manifeste final pour examen.
9. L'équipe Security Hub crée l'intégration du fournisseur dans la console Security Hub. Les clients peuvent ensuite découvrir et activer l'intégration.

10. (Facultatif) Vous déployez des efforts marketing supplémentaires pour promouvoir l'intégration de votre Security Hub. Consultez G.o-to-marketactivités.

    Au minimum, Security Hub vous recommande de fournir les ressources suivantes.

    - Une vidéo de démonstration (3 minutes au maximum) de l'intégration fonctionnelle. La vidéo est utilisée à des fins de marketing et est publiée sur leAWS YouTubeChannel.
    - Diagramme d'architecture à une diapositive à ajouter au diaporama de premier appel de Security Hub.

G.o-to-marketactivités

Les partenaires peuvent également s'engager dans des activités marketing optionnelles pour expliquer et promouvoir leursAWS Security HubIntégration d'.

Si vous souhaitez créer votre propre contenu marketing lié à Security Hub, avant de publier le contenu, envoyez un brouillon à votre gestionnaire de partenaires APN pour révision et approbation. Cela garantit que tout le monde est aligné sur la messagerie.

AWSLes partenaires du réseau de partenaires (APN) peuvent utiliser APN Partner Marketing Central et le programme Market Development Funds (MDF) pour créer des campagnes et obtenir un soutien financier. Pour plus d'informations sur ces programmes, contactez votre responsable partenaire.

Entrée sur la page des partenaires Security Hub

Une fois que vous avez été approuvé en tant que partenaire Security Hub, votre solution peut être affichée sur leAWS Security Hubpage partenaires.

Pour être répertorié sur cette page, fournissez les informations suivantes à vos contacts partenaires APN. Il peut s'agir de votre gestionnaire de développement de partenaires (PDM), d'architecte de solutions partenaires (PSA) ou d'un e-mail à`<securityhub-pms@amazon.com>`.

- Une brève description de votre solution, de son intégration à Security Hub et de la valeur que l'intégration avec Security Hub apporte aux clients. Cette description est limitée à 700 caractères, espaces compris.
- URL vers une page qui décrit votre solution. Ce site doit être spécifique à votreAWSl'intégration et plus particulièrement votre intégration Security Hub. Il doit se concentrer sur l'expérience client et la valeur que les clients reçoivent lorsqu'ils utilisent l'intégration.
- Une copie haute résolution de votre logo de 600 x 300 pixels. Pour plus de détails sur les exigences relatives à ce logo, voirthe section called “Logo pour la page des partenaires”.

Communiqués de presse

En tant que partenaire agréé, vous pouvez éventuellement publier un communiqué de presse sur votre site Web et les canaux de relations publiques. Le communiqué de presse doit être approuvé parAWS.

Avant de publier le communiqué de presse, vous devez le soumettre àAWSpour examen par le marketing des partenaires APN, la direction de Security Hub etAWSServices de sécurité externes (ESS). Le communiqué de presse peut inclure une proposition de devis pour le vice-président d'ESS.

Pour lancer ce processus, travaillez avec votre PDM. Nous disposons d'un accord de niveau de service (SLA) de 10 jours ouvrables pour passer en revue les communiqués de presse.

AWSBlog du réseau de partenaires (APN)

Nous pouvons également vous aider à publier une entrée de blog que vous créez sur le blog APN. L'entrée de blog doit se concentrer sur un article client et un cas d'utilisation. Il ne peut pas être positionné uniquement sur le fait d'être un partenaire de lancement d'intégration.

Si vous êtes intéressé, contactez votre PDM ou votre PSA pour commencer le processus. L'approbation finale et la publication des blogs APN peuvent prendre 8 semaines ou plus.

Principales choses à savoir sur le blog APN

Lorsque vous créez un article de blog, n'oubliez pas les éléments suivants.

Qu'est-ce qui se trouve dans un article de blog ?

- Les postes de partenaires doivent être éducatifs et fournir une expertise approfondie sur un sujet pertinentAWSclients.
- La longueur idéale ne dépasse pas 1 500 mots. Les lecteurs apprécient le contenu éducatif approfondi qui leur enseigne ce qui est possible surAWS.
- Le contenu doit être original sur le blog APN. Ne réutilisez pas le contenu provenant de sources telles que des articles de blog ou des livres blancs existants.

Quelles sont les autres limites de publication sur le blog APN ?

- Seuls les partenaires de niveau Advanced ou Premier peuvent publier sur le blog APN. Il existe des exceptions pour les partenaires sélectionnés qui ont une désignation de programme APN, telle que la prestation de services.
- Chaque partenaire est limité à trois postes par an. Avec des dizaines de milliers de partenaires APN,AWSdoit être équitable dans sa couverture.

Chaque publication doit avoir un sponsor technique capable de valider la solution ou le cas d'utilisation.

Combien de temps faut-il pour modifier un article de blog avant d'être publié ?

Après avoir soumis le premier brouillon complet du billet de blog, il faut compter de quatre à six semaines pour le modifier.

Pourquoi écrire pour le blog APN ?

Un article de blog APN peut offrir les avantages suivants.

- Crédibilité— Pour APN Partners, avoir une histoire publiée parAWSpeuvent influencer les clients du monde entier.
- Visibility— Le blog APN est l'un des blogs les plus lus surAWSavec 1,79 million de pages vues en 2019, y compris le trafic influencé.
- Entreprise— Les publications des partenaires APN possèdent des boutons de connexion qui peuvent générer des pistes via le programme APN Customer Engagements (ACE).

Quel type de contenu convient-il le mieux ?

Les types de contenus suivants conviennent le mieux à un article de blog APN.

- Le contenu technique est le type d'histoire le plus populaire. Cela inclut des projecteurs de solution et des informations pratiques. Plus de 75 % des lecteurs consultent ce contenu technique.
- Les clients apprécient les histoires de 200 ou plus qui démontrent comment quelque chose fonctionneAWSou comment un partenaire APN a résolu un problème commercial pour les clients.
- Les publications écrites par des experts techniques ou des experts en la matière sont de loin les meilleurs résultats.

Fiche Slick ou fiche marketing

Une feuille slick est un document d'une page qui décrit votre produit, son architecture d'intégration et les cas d'utilisation communs des clients.

Si vous créez une feuille détaillée pour votre intégration, envoyez-en une copie à l'équipe Security Hub. Ils l'ajouteront à la page des partenaires.

Livre blanc ou ebook

Si vous créez un livre blanc ou un livre électronique décrivant votre produit, son architecture d'intégration et les cas d'utilisation communs des clients, envoyez-en une copie à l'équipe Security Hub. Ils l'ajouteront à la page des partenaires Security Hub.

Webinaire

Si vous organisez un webinaire sur votre intégration, envoyez un enregistrement du webinaire à l'équipe Security Hub. L'équipe y affichera un lien à partir de la page des partenaires.

L'équipe peut également fournir un expert en matière de Security Hub pour participer à votre webinaire.

Vidéo de démonstration

À des fins de marketing, vous pouvez produire une vidéo de démonstration de l'intégration opérationnelle. Publiez une telle vidéo sur votre compte de plateforme vidéo, et l'équipe Security Hub va y accéder depuis la page partenaire.

manifeste d'intégration de produit

Chaque partenaireAWS Security Hub d'intégration doit remplir un manifeste d'intégration du produit fournissant les informations requises pour l'intégration proposée.

L'équipe Security Hub utilise ces informations de différentes manières :

- Pour créer la liste de votre site Web
- Pour créer la carte produit pour la console Security Hub
- Informer l'équipe produit de votre cas d'utilisation.

Pour évaluer la qualité de l'intégration proposée et des informations fournies, l'équipe Security Hub utilise lethe section called “Liste de contrôle de préparation des produits”. Cette liste de contrôle détermine si votre intégration est prête à être lancée.

Toutes les informations techniques que vous fournissez doivent également figurer dans votre documentation.

Vous pouvez télécharger une version PDF du manifeste d'intégration du produit dans la section Ressources de la page desAWS Security Hub partenaires. Notez que la page partenaires n'est pas disponible dans les régions de Chine (Beijing) et de Chine (Ningxia).

Table des matières

  - Logos pour la console Security Hub
  - Types de résultats
  - Hotline
  - Détermination du rythme cardiaque
- AWS Security Hubinformations sur la console
  - Informations sur la société
  - Informations sur le produit

Informations sur le cas d'utilisation et le marketing

Les cas d'utilisation suivants peuvent vous aider à effectuerAWS Security Hub des configurations à des fins différentes.

Cas d'utilisation de la recherche de fournisseurs et de consommateurs

Obligatoire pour les éditeurs de logiciels indépendants (ISV).

Pour décrire votre cas d'utilisation concernant votre intégration avecAWS Security Hub, répondez aux questions suivantes. Si vous n'avez pas l'intention d'envoyer ou de recevoir des résultats, notez-le dans cette section, puis complétez la section suivante.

Les informations suivantes doivent figurer dans votre documentation.

- Allez-vous envoyer des résultats, recevoir des résultats, ou les deux ?
- Si vous prévoyez d'envoyer des résultats, quels types de résultats enverrez-vous ? Allez-vous envoyer tous les résultats ou un sous-ensemble spécifique de résultats ?
- Si vous prévoyez de recevoir des résultats, que ferez-vous de ces résultats ? Quels types de résultats recevrez-vous ? Par exemple, recevrez-vous tous les résultats, les résultats d'un certain type ou uniquement les résultats spécifiques sélectionnés par le client ?
- Prévoyez-vous de mettre à jour les résultats ? Dans l'affirmative, quels champs allez-vous mettre à jour ? Security Hub vous recommande de mettre à jour les résultats au lieu de toujours en créer de nouveaux. La mise à jour des résultats existants permet de réduire le bruit des clients.

  Pour mettre à jour une constatation, vous envoyez une constatation avec un numéro de recherche attribué à une constatation que vous avez déjà envoyée.

Pour obtenir rapidement des commentaires sur votre cas d'utilisation et vos ensembles de données, contactez le partenaire APN ou l'équipe Security Hub.

Cas d'utilisation de Consulting Partner (CP)

Obligatoire si vous êtes un partenaire consultant de Security Hub.

Fournissez deux cas d'utilisation client pour votre travail avec Security Hub. Il peut s'agir de cas d'utilisation privés. L'équipe de Security Hub n'en fait la publicité nulle part. Ces noms doivent décrire l'une des actions suivantes ou les deux.

- Comment aidez-vous les clients à démarrer Security Hub ? Par exemple, avez-vous aidé des clients à utiliser des services professionnels, un module Terraform ou unAWS CloudFormation modèle ?
- Comment aidez-vous les clients à opérationnaliser et à étendre Security Hub ? Par exemple, avez-vous fourni des modèles de réponse ou de correction, créé des intégrations personnalisées ou utilisé des outils de business intelligence pour créer un tableau de bord exécutif ?

Jeux de données

Obligatoire si vous envoyez les résultats à Security Hub.

Pour les résultats que vous enverrez à Security Hub, fournissez les informations suivantes.

- Les résultats dans leur format natif, tel que JSON ou XML
- Un exemple de la façon dont vous allez convertir les résultats au formatAWS Security Finding Format (ASFF)

Informez l'équipe de Security Hub si vous avez besoin de mises à jour de l'ASFF pour faciliter votre intégration.

Architecture

Obligatoire si vous envoyez des résultats à Security Hub.

Décrivez comment vous allez vous intégrer à Security Hub. Ces informations doivent également figurer dans votre documentation.

Vous devez fournir des schémas d'architecture. Tenez compte des éléments suivants lorsque vous préparez vos schémas d'architecture :

- QuelsAWS services, agents du système d'exploitation, etc. utiliserez-vous ?
- Si vous envoyez des résultats à Security Hub, les enverrez-vous depuis leAWS compte client ou depuis votre propreAWS compte ?
- Si vous recevez des résultats, comment utiliserez-vous l'intégration CloudWatch des événements ?
- Comment allez-vous convertir les résultats en ASFF ?
- Comment allez-vous regrouper les résultats, suivre l'état des résultats et éviter les limites de limitation ?

Configuration

Obligatoire si vous envoyez des résultats à Security Hub.

Décrivez la configuration de votre intégration avec Security Hub

Vous devez au minimum utiliser desAWS CloudFormation modèles ou une infrastructure similaire, telle que des modèles de code. Certains partenaires ont fourni une interface utilisateur permettant une intégration en un clic.

La configuration ne devrait pas prendre plus de 15 minutes. La documentation de votre produit doit également fournir des conseils de configuration pour votre intégration.

Nombre moyen de résultats par jour et par client

Obligatoire si vous envoyez les résultats à Security Hub.

Combien de mises à jour de recherche par mois (moyenne et maximale) prévoyez-vous d'envoyer à Security Hub à l'ensemble de votre clientèle ? Les estimations d'ordres de grandeur sont acceptables.

Latence

Obligatoire si vous envoyez les résultats à Security Hub.

En combien de temps comptez-vous regrouper et envoyer les résultats à Security Hub ? En d'autres termes, quelle est la latence entre le moment où le résultat est créé dans votre produit et celui où il est envoyé à Security Hub ?

Ces informations doivent être reflétées dans la documentation de votre produit pour votre intégration. C'est une question fréquemment posée par les clients.

Description de l'entreprise et du produit

Requis pour toutes les intégrations avec Security Hub.

Décrivez brièvement votre entreprise et votre produit, en insistant particulièrement sur la nature de votre intégration au Security Hub. Nous l'utilisons sur la page des partenaires de Security Hub.

Si vous intégrez plusieurs produits à Security Hub, vous pouvez fournir une description distincte pour chaque produit, mais nous les combinerons en une seule entrée sur la page partenaire.

Chaque description ne peut pas comporter plus de 700 caractères avec des espaces.

Ressources du site Web partenaire

Requis pour toutes les intégrations avec Security Hub.

Vous devez au minimum fournir une URL à utiliser pour le lien hypertexte En savoir plus sur la page des partenaires de Security Hub. Il doit s'agir d'une page d'accueil marketing décrivant l'intégration entre votre produit et Security Hub.

Si vous intégrez plusieurs produits à Security Hub, vous pouvez disposer d'une seule page d'accueil pour chacun d'entre eux. Security Hub recommande d'inclure un lien vers vos instructions de configuration sur cette page d'accueil.

Vous pouvez également fournir des liens vers d'autres ressources telles que des blogs, des webinaires, des vidéos de démonstration ou des livres blancs. Security Hub proposera également des liens vers ceux-ci depuis la page de leurs partenaires.

Logo pour la page des partenaires

Requis pour toutes les intégrations de Security Hub.

Fournissez l'URL d'un logo à afficher sur la page des partenaires de Security Hub. Le logo doit répondre aux critères suivants :

- Taille : 600 x 300 pixels
- Recadrage : serré sans rembourrage
- Fond : transparent

- Format : PNG

Logos pour la console Security Hub

Requis pour toutes les intégrations.

Fournissez les URL des logos du mode clair et du mode sombre à afficher sur la console Security Hub.

Les logos doivent répondre aux critères suivants :

- Format : SVG
- Taille : 175 x 40 pixels. Si elle est plus grande, l'image doit utiliser ce ratio.
- Recadrage : serré, sans rembourrage
- Fond : transparent

Pour obtenir des instructions détaillées concernant le petit logo, reportez-vous à la sectionthe section called “Directives concernant le logo de la console”.

Types de résultats

Obligatoire si vous envoyez les résultats à Security Hub.

Fournissez un tableau qui décrit les types de recherche au format ASFF que vous utilisez et la façon dont ils s'alignent sur vos types de recherche natifs. Pour plus de détails sur la recherche de types dans ASFF, consultez la section Taxonomie des types pour ASFF dans le Guide deAWS Security Hub l'utilisateur.

Nous vous recommandons d'inclure également ces informations dans la documentation de votre produit.

Hotline

Requis pour toutes les intégrations avec Security Hub.

Fournissez une adresse e-mail et un numéro de téléphone ou un numéro de téléavertisseur pour un point de contact technique. Security Hub communiquera avec ce contact en cas de problème technique, par exemple lorsqu'une intégration ne fonctionne plus.

Fournissez également un point de contact 24 heures sur 24, 7 jours sur 7 pour les problèmes techniques les plus graves.

Détermination du rythme cardiaque

Recommandé si vous envoyez les résultats à Security Hub.

Pouvez-vous envoyer à Security Hub un « battement de cœur » toutes les cinq minutes indiquant que votre intégration à Security Hub est fonctionnelle ?

Si vous le pouvez, faites-le en utilisant le type de recherche`Heartbeat`.

AWS Security Hubinformations sur la console

Fournissez à l'AWS Security Hubéquipe un texte JSON contenant les informations suivantes. Security Hub utilise ces informations pour créer l'ARN de votre produit, afficher la liste des fournisseurs dans la console et inclure les informations gérées que vous proposez dans la bibliothèque d'informations de Security Hub.

Informations sur la société

Les informations sur l'entreprise fournissent des informations sur votre entreprise. Voici un exemple:

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

Les informations sur la société comprennent les champs suivants :

Champ	Obligatoire	Description
`id`	Oui	L'identifiant unique de la société L'identifiant de société doit être unique pour les entreprises. C'est probablement le même ou similaire à`name`. Type : String

Champ	Obligatoire	Description
		Longueur minimale : 5 caractères Longueur maximale : 24 caractères Caractères autorisés : lettres minuscules, chiffres et traits d'union Ils doivent commencer par une minuscule. Ils doivent terminer par une minuscule ou un chiffre.
`name`	Oui	Le nom de la société du fournisseur à afficher sur la console Security Hub. Type : String Longueur maximale : 16 caractères
`description`	Oui	Description de la société du fournisseur à afficher sur la console Security Hub. Type : String Longueur maximale : 200 caractères

Informations sur le produit

Cette section fournit des informations sur votre produit. Voici un exemple:

```
{
    "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"
}
```

Les informations sur le produit contiennent les champs suivants.

Champ	Obligatoire	Description
`IntegrationType`	Oui	Indique si votre produit envoie des résultats à Security Hub, reçoit des résultats de Security Hub, ou à la fois envoie et reçoit des résultats. Si vous êtes un partenaire de conseil, laissez ce champ vide. Type : tableau de chaînes Valeurs valides : `SEND_FINDINGS_TO_SECURITY_HUB` | `RECEIVE_FINDINGS_FROM_SECURITY_HUB`
`id`	Oui	L'identifiant unique du produit Ces noms doivent être uniques dans une entreprise. Ces noms ne doivent pas nécessairement être uniques d'une entreprise à l'autre. C'est probablement le même ou similaire à`name`. Type : String Longueur minimale : 5 caractères Longueur maximale : 24 caractères Caractères autorisés : lettres minuscules, chiffres et traits d'union Ils doivent commencer par une minuscule. Ils doivent terminer par une minuscule ou un chiffre.

Champ	Obligatoire	Description
`regionsNotSupported`	Oui	Parmi lesAWS régions suivantes, laquelle ne soutenez-vous pas ? En d'autres termes, dans quelles régions Security Hub ne devrait-il pas vous proposer en option sur la page de nos partenaires de la console Security Hub ? Type : String Indiquez uniquement le code de région. Par exemple, `us-west-1` . Pour obtenir la liste des régions, consultez la section Points de terminaison régionaux dans le Références générales AWS. Les codes de région pour leAWS GovCloud (US) sont`us-gov-west-1` (pourAWS GovCloud (US-Ouest)) et`us-gov-east-1` (pourAWS GovCloud (US-Est)). Les codes de région pour la Chine sont`cn-north-1` (pour la Chine (Pékin)) et`cn-northwest-1` (pour la Chine (Ningxia)).

Champ	Obligatoire	Description
`commercialAccountNumber`	Oui	Numéro deAWS compte principal du produit pour lesAWS régions. Si vous envoyez des résultats à Security Hub, le compte que vous fournissez dépend de l'endroit d'où vous envoyez les résultats. • Depuis votreAWS compte. Dans ce cas, indiquez le numéro de compte que vous utilisez pour soumettre vos résultats. • Depuis leAWS compte du client. Dans ce cas, Security Hub vous recommande de fournir le numéro de compte principal que vous utilisez pour tester l'intégration. Idéalement, vous utiliserez le même compte pour tous vos produits dans toutes les régions. Si cela n'est pas possible, contactez l'équipe du Security Hub. Si vous ne recevez des résultats que de Security Hub, ce numéro de compte n'est pas requis. Type : String

Champ	Obligatoire	Description
`govcloudAccountNumber`	Non	Numéro deAWS compte principal du produit pour lesAWS GovCloud (US) régions (si votre produit est disponible dansAWS GovCloud (US)). Si vous envoyez des résultats à Security Hub, le compte que vous fournissez dépend de l'endroit d'où vous envoyez les résultats. • Depuis votreAWS compte. Dans ce cas, indiquez le numéro de compte que vous utilisez pour soumettre vos résultats. • Depuis leAWS compte du client. Dans ce cas, Security Hub vous recommande de fournir le numéro de compte principal que vous utilisez pour tester l'intégration. Idéalement, vous utilisez le même compte pour tous vos produits dans toutes lesAWS GovCloud (US) régions. Si cela n'est pas possible, contactez l'équipe du Security Hub. Si vous ne recevez des résultats que de Security Hub, ce numéro de compte n'est pas requis. Type : String

Champ	Obligatoire	Description
`chinaAccountNumber`	Non	Numéro deAWS compte principal du produit pour les régions de Chine (si votre produit est disponible dans les régions de Chine). Si vous envoyez des résultats à Security Hub, le compte que vous fournissez dépend de l'endroit d'où vous envoyez les résultats. • Depuis votreAWS compte. Dans ce cas, indiquez le numéro de compte que vous utilisez pour soumettre vos résultats. • Depuis leAWS compte du client. Dans ce cas, Security Hub vous recommande de fournir le numéro de compte principal que vous utilisez pour tester l'intégration du produit. Idéalement, vous utilisez le même compte pour tous vos produits dans toutes les régions de Chine. Si cela n'est pas possible, contactez l'équipe du Security Hub. Si vous ne recevez des résultats que de Security Hub, il peut s'agir de n'importe quel compte que vous possédez dans une région chinoise. Type : String
`name`	Oui	Nom du produit du fournisseur à afficher sur la console Security Hub. Type : String Longueur maximale : 24 caractères

Champ	Obligatoire	Description
`description`	Oui	Description du produit du fournisseur à afficher sur la console Security Hub. Type : String Longueur maximale : 200 caractères
`importType`	Oui	Type de politique de ressources pour le partenaire. Au cours du processus d'intégration de partenaire, vous pouvez spécifier l'une des politiques de ressources suivantes ou vous pouvez les spécifier`NEITHER`. • Avec`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, vous ne pouvez envoyer des résultats à Security Hub qu'à partir du compte indiqué dans l'ARN de votre produit. • Avec`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, vous ne pouvez envoyer des résultats qu'à partir du compte client auquel vous êtes abonné. Type : String Valeurs valides : `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` |`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` | `NEITHER`

Champ	Obligatoire	Description
`category`	Oui	Les catégories qui définissent votre produit. Vos sélections s'affichent sur la console Security Hub. Choisissez jusqu'à trois catégories. Les sélections personnalisées ne sont pas autorisées. Si vous pensez que votre catégorie est manquante, contactez l'équipe du Security Hub. Type : Array Catégories disponibles : • `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 Management` • `Configuration and Patch Management` • `Configuration Management Database (CMDB)` • `Consulting Partner` • `Container Security` • `Cyber Range` • `Data Access Management`

Champ	Obligatoire	Description
		• 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

Champ	Obligatoire	Description
		• `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`	Non	L'URL deAWS Marketplace destination de votre produit. L'URL s'affiche dans la console Security Hub. Type : String Il doit s'agir d'uneAWS Marketplace URL. Si vous n'avez pas d'AWS Marketplaceannonce , laissez ce champ vide.

Champ	Obligatoire	Description
`configurationUrl`	Oui	L'URL de la documentation de votre produit sur l'intégration avec Security Hub. Ce contenu est hébergé sur votre site Web ou sur une page Web que vous gérez, telle qu'une GitHub page. Type : String Votre documentation doit inclure les informations suivantes. • Instructions de configuration • Liens versAWS CloudFormation des modèles (si nécessaire) • Informations sur votre cas d'utilisation pour l'intégration • Latence • Cartographie ASFF • Types de résultat inclus • Architecture

Consignes et listes de contrôle

Au fur et à mesure que vous préparez le matériel requis pour votreAWS Security Hubintégration, utilisez ces directives.

La liste de contrôle de préparation est utilisée pour effectuer un examen final de l'intégration avant que Security Hub ne la mette à la disposition des clients Security Hub.

Rubriques

Directives relatives à l'affichage du logo sur leAWS Security Hubconsole

Pour que le logo s'affiche sur leAWS Security Hub, suivez ces instructions.

Modes Clair et Sombre

Vous devez fournir à la fois un mode clair et une version en mode sombre du logo.

Format

SVG - Format de fichier

Background color

Transparent

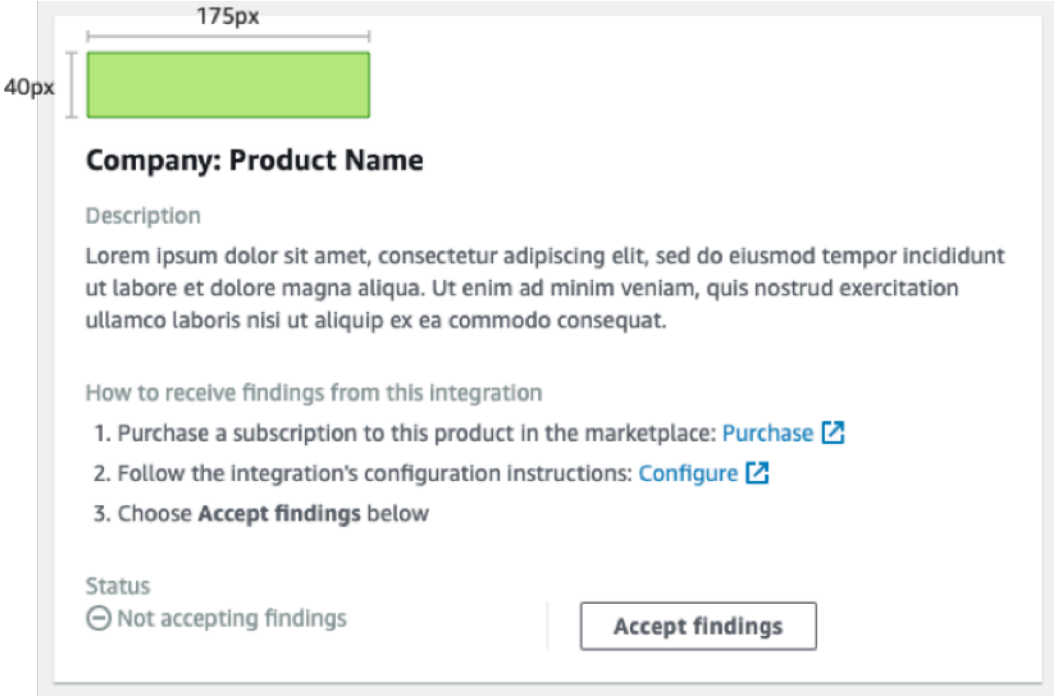
Size

Le rapport idéal est de 175 px de large sur 40 px de haut.

La hauteur minimale est de 40 px.

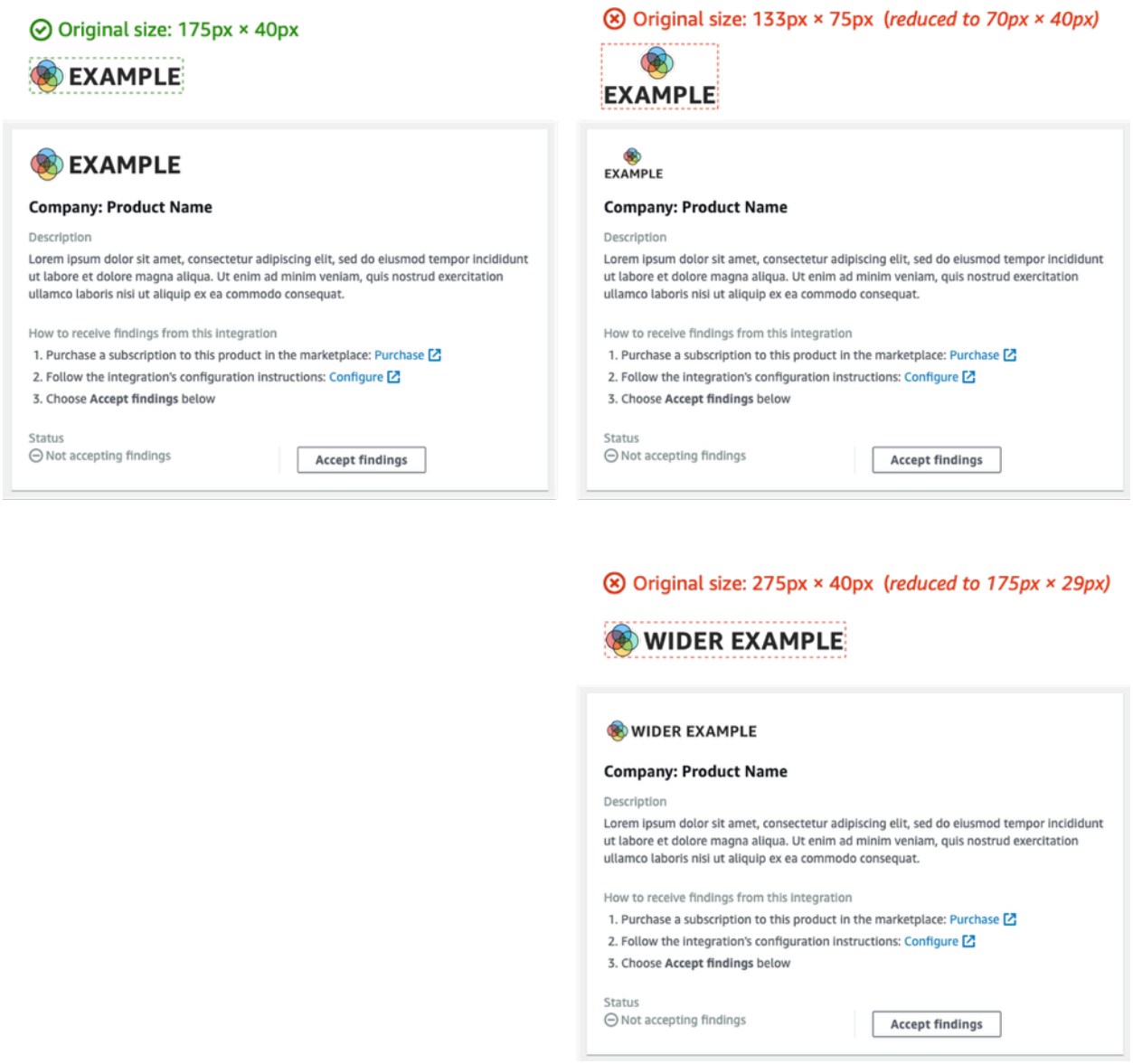
Les logos rectangulaires fonctionnent le mieux.

L'image suivante montre comment un logo idéal est affiché sur la console Security Hub.



Si votre logo ne correspond pas à ces dimensions, Security Hub réduit la taille à une hauteur maximale de 40 px et à une largeur maximale de 175 px. Cela affecte la façon dont le logo est affiché sur la console Security Hub.

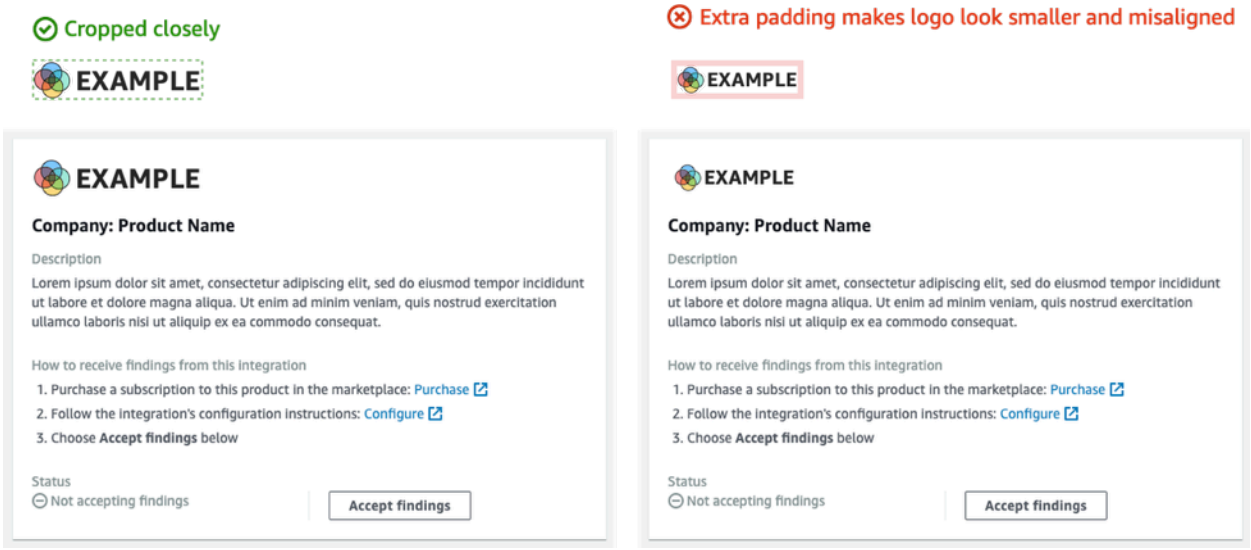
L'image suivante compare l'affichage d'un logo ayant la taille idéale à des logos plus larges ou plus grands.



Recadrage

Recadrez l'image du logo le plus près possible. Ne pas fournir de rembourrage supplémentaire.

L'image suivante montre la différence entre un logo recadré de près et un logo doté d'un rembourrage supplémentaire.



Principes de création et de mise à jour des résultats

Lorsque vous planifiez comment créer et mettre à jour les résultats dansAWS Security Hub, gardez à l'esprit les principes suivants.

Définissez des résultats spécifiques afin que les clients puissent facilement agir à cet égard.

Les clients souhaitent automatiser les actions de réponse et de correction et mettre en corrélation les résultats avec d'autres résultats. Pour étayer cela, les résultats doivent présenter les caractéristiques suivantes :

- Ils doivent généralement s'occuper d'une ressource unique ou principale.
- Ils devraient avoir un seul type de recherche.
- Ils doivent faire face à un seul événement de sécurité.

Lorsqu'une recherche contient des données pour plusieurs événements de sécurité, il est plus difficile pour les clients d'agir sur la recherche.

Mappez tous vos champs de recherche à laAWSFormat ASFF (Security Finding Format). Permettez aux clients de se fier à Security Hub comme source de vérité.

Les clients s'attendent à ce que chaque champ de votre format de recherche natif soit également représenté dans le Security Hub ASFF.

Les clients souhaitent que toutes les données soient présentes dans la version Security Hub de la recherche. Les données manquantes font perdre confiance à Security Hub en tant que source centrale d'informations de sécurité.

Minimisez la redondance des résultats. Ne submergez pas les clients en trouvant des volumes.

Security Hub n'est pas un outil général de gestion des journaux. Vous devez envoyer des résultats à Security Hub qui sont hautement exploitables et que les clients peuvent directement répondre aux autres résultats, les corriger ou les corréler.

Lorsqu'il n'y a qu'une modification mineure apportée à la recherche, mettez-la à jour au lieu d'en créer une nouvelle.

Lorsqu'il y a un changement majeur dans la recherche, par exemple le score de gravité ou l'identificateur de ressource, créez une nouvelle recherche.

Par exemple, créer des résultats pour des analyses de ports individuels en temps réel n'est pas très exploitable. Étant donné que l'analyse des ports peut se faire en continu, elle produirait un volume important de résultats. Il est beaucoup plus convaincant et précis de simplement mettre à jour la dernière heure d'analyse et de compter le nombre d'analyses sur une seule recherche pour une analyse de port sur un port MongoDB à partir d'un nœud TOR.

Permettez aux clients de personnaliser leurs résultats pour les rendre plus significatifs.

Les clients souhaitent pouvoir ajuster certains champs de recherche pour les rendre plus pertinents à leur environnement ou à leurs exigences.

Par exemple, les clients souhaitent pouvoir ajouter des notes, des balises et ajuster les scores de gravité en fonction du type de compte ou du type de ressource auquel la recherche est associée.

Lignes directrices pour la cartographie des résultats dans leAWSFormat ASFF (Security Finding Format)

Suivez les recommandations suivantes pour associer vos résultats à l'ASFF. Pour obtenir une description détaillée de chaque champ et objet ASFF, voirAWSFormat ASFF (Security Finding Format)dans leAWS Security HubGuide de l'utilisateur.

Informations d'identification

`SchemaVersion` est toujours `2018-10-08`.

`ProductArn`est l'ARN quiAWS Security Hubvous attribue.

`Id`est la valeur utilisée par Security Hub pour indexer les résultats. L'identificateur de recherche doit être unique, pour s'assurer que les autres résultats ne sont pas écrasés. Pour mettre à jour une recherche, soumettez à nouveau la recherche avec le même identifiant.

`GeneratorId`peut être identique à`Id`ou peut faire référence à une unité de logique discrète, telle qu'AmazonGuardDutyID de détecteur,AWS ConfigID de l'enregistreur ou ID IAM Access Analyzer.

Title et Description

`Title`devrait contenir des informations sur la ressource affectée.`Title`est limité à 256 caractères, espaces compris.

Ajoutez des informations détaillées plus longues à`Description`.`Description`est limité à 1 024 caractères, espaces compris. Vous pouvez envisager d'ajouter une troncature aux descriptions. Voici un exemple:

```
"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.",
```

Types de résultats

Vous fournissez vos informations de type de recherche dans`FindingProviderFields.Types`.

`Types`doit correspondre à la valeurTaxonomie des types pour ASFF.

Si nécessaire, vous pouvez spécifier un classificateur personnalisé (le troisième espace de noms).

Horodatages

Le format ASFF inclut quelques horodatages différents.

`CreatedAt` et **`UpdatedAt`**

Vous devez soumettre`CreatedAt`et`UpdatedAt`chaque fois que vous appelez`BatchImportFindings`pour chaque constatation.

Les valeurs doivent correspondre au format ISO8601 dans Python 3.8.

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

`FirstObservedAt` et `LastObservedAt`

`FirstObservedAt`et`LastObservedAt`doit correspondre lorsque votre système a observé le résultat. Si vous n'enregistrez pas ces informations, vous n'avez pas besoin de soumettre ces horodatage.

Les valeurs correspondent au format ISO8601 dans Python 3.8.

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

Severity

Vous fournissez des informations de gravité dans le`FindingProviderFields.Severity`objet, qui contient les champs suivants.

`Original`

La valeur de gravité de votre système.`Original`peut être n'importe quelle chaîne, pour s'adapter au système que vous utilisez.

`Label`

Indicateur Security Hub requis de la gravité de la recherche. Les valeurs autorisées sont les suivantes.

- `INFORMATIONAL`— Aucun problème n'a été identifié.
- `LOW`— Le problème ne nécessite pas d'action en soi.
- `MEDIUM`— Le problème doit être traité, mais n'est pas urgent.
- `HIGH`— Le problème doit être traité en priorité.
- `CRITICAL`— Le problème doit être résolu immédiatement pour éviter d'autres dommages.

Les résultats conformes devraient toujours avoir`Label`défini sur`INFORMATIONAL`. Exemples de`INFORMATIONAL`les résultats sont des résultats des contrôles de sécurité qui ont été passés etAWS Firewall Managerles résultats qui sont corrigés.

Les clients trient souvent les résultats en fonction de leur gravité pour donner à leurs équipes des opérations de sécurité une liste de choses à faire. Soyez prudent lorsque vous définissez la gravité de la recherche sur`HIGH`ou`CRITICAL`.

Votre documentation d'intégration doit inclure votre justification cartographique.

Remediation

`Remediation`compte deux éléments. Ces éléments sont combinés sur la console Security Hub.

`Remediation.Recommendation.Text`s'affiche dans le fichier*Correction*section des détails de la recherche. Il est hyperlié à la valeur de`Remediation.Recommendation.Url`.

Actuellement, seuls les résultats des normes Security Hub, IAM Access Analyzer et Firewall Manager affichent des hyperliens vers la documentation sur la façon de remédier à la recherche.

SourceUrl

Utiliser uniquement`SourceUrl`si vous pouvez fournir une URL profondément liée à votre console pour ce résultat spécifique. Sinon, omettez-le dans le mappage.

Security Hub ne prend pas en charge les liens hypertexte de ce champ, mais il est exposé sur la console Security Hub.

Malware, Network, Process, ThreatIntelIndicators

Le cas échéant, utilisez`Malware`,`Network`,`Process`, ou`ThreatIntelIndicators`. Chacun de ces objets est exposé dans la console Security Hub. Utilisez ces objets dans le contexte de la recherche que vous envoyez.

Par exemple, si vous détectez des logiciels malveillants qui établissent une connexion sortante à un nœud de commande et de contrôle connu, indiquez les détails de l'instance EC2 dans`Resource.Details.AwsEc2Instance`. Fournir les éléments pertinents`Malware`,`Network`, et`ThreatIntelIndicator`objets pour cette instance EC2.

Malware

`Malware`est une liste qui accepte jusqu'à cinq baies d'informations sur les logiciels malveillants. Rendez les entrées de logiciels malveillants pertinentes pour la ressource et la recherche.

Chaque entrée contient les champs suivants.

`Name`

Nom du programme malveillant. La valeur est une chaîne comportant jusqu'à 64 caractères.

`Name`devraient provenir d'une source de renseignements sur les menaces ou d'un chercheur vérifié.

`Path`

Chemin vers le malware. La valeur est une chaîne comportant jusqu'à 512 caractères.`Path`doit être un chemin d'accès au fichier système Linux ou Windows, sauf dans les cas suivants.

- Si vous analysez des objets dans un compartiment S3 ou un partage EFS par rapport aux règles YARA, alors`Path`est le chemin d'accès à l'objet S3 ://ou HTTPS.
- Si vous analysez des fichiers dans un référentiel Git, alors`Path`est l'URL Git ou le chemin du clone.

`State`

Statut du programme malveillant. Les valeurs autorisées sont :`OBSERVED`| `REMOVAL_FAILED`|`REMOVED`.

Dans le titre et la description de recherche, assurez-vous de fournir le contexte de ce qui s'est passé avec le logiciel malveillant.

Par exemple, si`Malware.State`est`REMOVED`, le titre et la description de recherche doivent indiquer que votre produit a supprimé le logiciel malveillant situé sur le chemin d'accès.

Si`Malware.State`est`OBSERVED`, alors le titre et la description de recherche doivent indiquer que votre produit a rencontré ce logiciel malveillant situé sur le chemin d'accès.

`Type`

Indique le type de programme malveillant. Les valeurs autorisées sont :`ADWARE`|`BLENDED_THREAT`|`BOTNET_AGENT`|`COIN_MINER`|`EXPLOIT_KIT`|`KEYLOGGER`|`MACRO`|`POTE`

Si vous avez besoin d'une valeur supplémentaire pour`Type`, contactez l'équipe Security Hub.

Network

`Network`est un seul objet. Vous ne pouvez pas ajouter plusieurs détails liés au réseau. Lorsque vous mappez les champs, suivez les recommandations suivantes.

Informations sur la destination et la source

La destination et la source sont faciles à mapper les journaux de flux TCP ou VPC ou les journaux WAF. Ils sont plus difficiles à utiliser lorsque vous décrivez des informations réseau pour trouver une attaque.

En règle générale, la source est d'origine de l'attaque, mais elle peut avoir d'autres sources comme indiqué ci-dessous. Vous devez expliquer la source dans votre documentation et la décrire dans le titre de recherche et la description.

- Pour une attaque DDoS sur une instance EC2, la source est l'attaquant, bien qu'une attaque DDoS réelle puisse utiliser des millions d'hôtes. La destination est l'adresse IPv4 publique de l'instance EC2.`Direction`est IN.
- Pour les logiciels malveillants observés qui communiquent depuis une instance EC2 vers un nœud de commande et de contrôle connu, la source est l'adresse IPV4 de l'instance EC2. La destination est le nœud de commande et de contrôle.`Direction`est`OUT`. Vous fourniriez également`Malware`et`ThreatIntelIndicators`.

`Protocol`

`Protocol`est toujours associé à un nom enregistré IANA (Internet Assigned Numbers Authority), à moins que vous ne puissiez fournir un protocole spécifique. Vous devez toujours l'utiliser et fournir les informations de port.

`Protocol`est indépendant des informations sur la source et la destination. Ne le fournissez que lorsqu'il est logique de le faire.

`Direction`

`Direction`est toujours relatif à la*AWS*limites de réseau.

- `IN`signifie qu'il entre*AWS*(VPC, service).
- `OUT`signifie qu'il quitte le*AWS*limites de réseau.

Process

`Process`est un seul objet. Vous ne pouvez pas ajouter plusieurs détails liés au processus. Lorsque vous mappez les champs, suivez les recommandations suivantes.

`Name`

`Name`doit correspondre au nom de l'exécutable. Il accepte jusqu'à 64 caractères.

`Path`

`Path`est le chemin d'accès au système de fichiers vers l'exécutable du processus. Il accepte jusqu'à 512 caractères.

`Pid`, **`ParentPid`**

`Pid`et`ParentPid`doit correspondre à l'identificateur de processus Linux (PID) ou à l'ID d'événement Windows. Pour différencier, utilisez EC2 Amazon Machine Images (AMI) pour fournir les informations. Les clients peuvent probablement faire la différence entre Windows et Linux.

Horodatages (**`LaunchedAt`**et**`TerminatedAt`**)

Si vous ne pouvez pas récupérer ces informations de manière fiable et qu'elles ne sont pas exactes à la milliseconde, ne les fournissez pas.

Si un client s'appuie sur des horodatages pour les enquêtes médicolégales, il vaut mieux ne pas avoir d'horodatage que d'avoir un horodatage erroné.

ThreatIntelIndicators

`ThreatIntelIndicators`accepte un tableau contenant jusqu'à cinq objets de détection des menaces.

Pour chaque entrée,`Type`est dans le contexte de la menace spécifique. Les valeurs autorisées sont :`DOMAIN`|`EMAIL_ADDRESS`|`HASH_MD5`|`HASH_SHA1`|`HASH_SHA256`|`HASH_SHA512`|`IPV4_ADDRESS`|`IPV`

Voici des exemples de cartographie des indicateurs de détection des menaces :

- Vous avez trouvé un processus dont vous savez qu'il est associé à Cobalt Strike. Vous avez appris cela deFireEyesur le blog.

  Définissez `Type` sur `PROCESS`. Créez également un`Process`objet pour le processus.
- Votre filtre de messagerie a détecté que quelqu'un envoyait un paquet haché bien connu à partir d'un domaine malveillant connu.

  Créer deux`ThreatIntelIndicator`objets. L'un des objets est destiné au`DOMAIN`. L'autre est destinée à l'`HASH_SHA1`.
- Vous avez trouvé un logiciel malveillant avec une règle Yara (Loki, Fenrir, Awss3)VirusScan,BinaryAlert).

  Créer deux`ThreatIntelIndicator`objets. L'un concerne le logiciel malveillant. L'autre est destinée à l'`HASH_SHA1`.

Resources

Pour`Resources`, utilisez les types de ressources et les champs de détails fournis chaque fois que possible. Security Hub ajoute constamment de nouvelles ressources à l'ASFF. Pour recevoir un journal mensuel des modifications apportées à ASFF, contactez`<securityhub-partners@amazon.com>`.

Si vous ne pouvez pas insérer les informations dans les champs de détails pour un type de ressource modélisé, mapper les détails restants sur`Details.Other`.

Pour une ressource qui n'est pas modélisée dans ASFF, définissez`Type`pour`Other`. Pour plus d'informations, utilisez`Details.Other`.

Vous pouvez également utiliser l'option`Other`type de ressource pour les non -AWSrésultats.

ProductFields

Utiliser uniquement`ProductFields`si vous ne pouvez pas utiliser un autre champ réservé pour`Resources`ou un objet descriptif tel que`ThreatIntelIndicators`,`Network`, ou`Malware`.

Si vous utilisez`ProductFields`, vous devez fournir une justification stricte de cette décision.

Conformité

Utiliser uniquement`Compliance`si vos résultats sont liés à la conformité.

Security Hub utilise`Compliance`pour les résultats qu'il génère sur la base de contrôles.

Firewall Manager utilise`Compliance`pour ses résultats parce qu'ils sont liés à la conformité.

Champs restreints

Ces champs sont destinés à permettre aux clients de suivre leur enquête sur un constat.

Ne pas mapper ces champs ou objets.

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

Pour ces champs, mapper les champs qui se trouvent dans la zone`FindingProviderFields`objet. Ne pas mapper les champs de niveau supérieur.

- `Confidence`— N'incluez un score de confiance (0-99) que si votre service dispose d'une fonctionnalité similaire ou si vous êtes à 100 % de votre recherche.
- `Criticality`— Le score de criticité (0-99) vise à exprimer l'importance de la ressource associée à la découverte.
- `RelatedFindings`— Ne fournissez des résultats associés que si vous pouvez suivre les résultats liés à la même ressource ou au même type de recherche. Pour identifier une recherche associée, vous devez vous référer à l'identifiant de recherche d'une recherche déjà présente dans Security Hub.

Instructions relatives à l'utilisation du**`BatchImportFindings`**API

Lorsque vous utilisez l'option`BatchImportFindings`Opération d'API pour envoyer des résultats àAWS Security Hub, utilisez les directives suivantes.

- Vous devez appeler`BatchImportFindings`en utilisant le compte associé aux résultats. L'identificateur du compte associé est la valeur de la`AwsAccountId`attribut de la recherche.
- Envoyez le lot le plus volumineux possible. Security Hub accepte jusqu'à 100 résultats par lot, jusqu'à 240 Ko par recherche et jusqu'à 6 Mo par lot.
- La limite de vitesse d'accélération est de 10 TPS par compte et par région, avec une rafale de 30 TPS.
- Vous devez implémenter un mécanisme pour conserver l'état des résultats en cas de problèmes de limitation ou de réseau. Vous avez également besoin de l'état de recherche pour pouvoir soumettre des mises à jour de recherche au fur et à mesure qu'une recherche passe à l'entrée et à la sortie de la conformité.
- Pour plus d'informations sur les longueurs maximales de chaînes et sur d'autres limitations, consultezAWSFormat ASFF (Security Finding Format)dans leAWS Security HubGuide de l'utilisateur.

Liste de contrôle de préparation des produits

LeAWS Security Hubet les équipes partenaires APN utilisent cette liste de contrôle pour vérifier que l'intégration est prête à être lancée.

Mappage ASFF

Ces questions sont liées au mappage de votre découverte avec leAWSFormat ASFF (Security Finding Format).

Toutes les données de recherche du partenaire sont-elles mappées dans ASFF ?

- Mappez toutes vos conclusions à l'ASFF d'une manière ou d'une autre.
- Utiliser des champs curés tels que des types de ressources modélisés,`Network`,`Malware`, ou`ThreatIntelIndicators`.
- Cartographiez tout autre élément dans`Resource.Details.Other`ou`ProductFields`selon les besoins.

Le partenaire utilise-t-il**`Resource.Details`**champs, tels que**`AwsEc2instance`**,**`AwsS3Bucket`**, et**`Container`**? Le partenaire utilise-t-il**`Resource.Details.Other`**pour définir les détails des ressources qui ne sont pas modélisés dans l'ASFF ?

- Dans la mesure du possible, utilisez les champs fournis pour les ressources sélectionnées telles que des instances EC2, des compartiments S3 et des groupes de sécurité dans vos résultats.
- Cartographiez d'autres informations relatives aux ressources à`Resource.Details.Other`uniquement lorsqu'il n'y a pas de correspondance directe.

Le partenaire fait-il correspondre les valeurs à**`UserDefinedFields`**?

- N'utilisez pas `UserDefinedFields`.
- Envisagez d'utiliser un autre champ organisé, tel que`Resource.Details.Other`ou`ProductFields`.

Le partenaire fait-il correspondre les informations dans**`ProductFields`**qui pourraient être mappés dans d'autres champs ASFF ?

- Utiliser uniquement`ProductFields`pour des informations spécifiques au produit telles que des informations de versionnement, des résultats de gravité spécifiques au produit ou d'autres informations qui ne peuvent pas être mappées dans un champ organisé ou`Resources.Details.Other`.

Le partenaire importe-t-il ses propres horodatages pour**`FirstObservedAt`**?

- Le`FirstObservedAt`l'horodatage est destiné à enregistrer l'heure à laquelle un constat a été observé dans le produit. Si possible, cartographiez ce champ.

Le partenaire fournisse-t-il des valeurs uniques générées pour chaque identifiant de recherche, à l'exception des résultats qu'il souhaite mettre à jour ?

Tous les résultats de Security Hub sont indexés sur l'identifiant de recherche (`Id`attribut). Cette valeur doit toujours être unique pour garantir que les résultats ne sont pas mis à jour accidentellement.

Vous devez également conserver l'état de l'identifiant de recherche dans le but de mettre à jour les résultats.

Le partenaire fournit-il une valeur qui associe les résultats à un identifiant de générateur ?

`GeneratorID`ne doit pas avoir la même valeur que l'ID de recherche.

`GeneratorID`devraient être en mesure de lier logiquement les résultats en fonction de ce qui les a générés.

Il peut s'agir d'un sous-composant d'un produit (produit A - Vulnérabilité vs produit A - EDR) ou quelque chose de similaire.

Le partenaire utilise-t-il les espaces de noms des types de recherche requis d'une manière pertinente pour son produit ? Le partenaire utilise-t-il les catégories de types de recherche recommandés ou les classificateurs dans ses types de recherche ?

La taxonomie du type de recherche doit correspondre étroitement aux résultats générés par le produit.

Les espaces de noms de premier niveau décrits dans leAWSLe format des conclusions de sécurité est requis.

Vous pouvez utiliser des valeurs personnalisées pour les espaces de noms de deuxième et troisième niveaux (catégories ou classificateurs).

Le partenaire capte-t-il les informations de flux réseau dans le**`Network`**, s'ils ont des données réseau ?

Si votre produit est capturéNetFlowinformations, mapper le fichier à la`Network`.

Est-ce que les informations du processus de capture des partenaires (PID) dans le**`Process`**, s'ils ont des données de traitement ?

Si votre produit capture des informations sur le processus, mapper les informations sur le`Process`.

Le partenaire capte-t-il les informations relatives aux logiciels malveillants dans le**`Malware`**, s'ils ont des données de logiciels malveillants ?

Si votre produit capture des informations sur les logiciels malveillants, mapez-les au`Malware`.

Le partenaire capte-t-il les informations relatives à l'intelligence des menaces dans le**`ThreatIntelIndicators`**, s'ils ont des données d'intelligence sur les menaces ?

Si votre produit capture des informations relatives à l'intelligence des menaces, mapez-le à la`ThreatIntelIndicators`.

Le partenaire fournit-il une cote de confiance pour les résultats ? Si c'est le cas, une justification est-elle fournie ?

Chaque fois que vous utilisez ce champ, fournissez une justification dans votre documentation et votre manifeste.

Le partenaire utilise-t-il un ID canonique ou un ARN pour l'ID de ressource dans la recherche ?

Lors de l'identificationAWSressources, la meilleure pratique consiste à utiliser l'ARN. Si aucun ARN n'est disponible, utilisez l'ID de ressource canonique.

Configuration et fonction de l'intégration

Ces questions sont liées à la configuration etday-to-dayfonction de l'intégration.

Est-ce que le partenaire fournit uninfrastructure-as-code(iAC) pour déployer l'intégration avec Security Hub, tel que Terraform,AWS CloudFormation, ouAWS Cloud Development Kit (AWS CDK)?

Pour les intégrations qui enverront des résultats à partir du compte client ou utiliserontCloudWatchÉvénements pour consommer des résultats, une forme de modèle iAC est requise.

AWS CloudFormationest préférable, maisAWS CDKou Terraform peut également être utilisée.

Le produit partenaire dispose-t-il d'une configuration en un clic sur sa console pour son intégration à Security Hub ?

Certains produits partenaires utilisent une bascule ou un mécanisme similaire dans leur produit pour activer l'intégration. Cela peut nécessiter un provisionnement automatique des ressources et des autorisations. Si vous envoyez des résultats à partir d'un compte produit, la configuration en un clic est la méthode préférée.

Le partenaire n'envoie-t-il que des résultats de valeur ?

En règle générale, vous ne devez envoyer des résultats qui présentent une valeur de sécurité qu'aux clients de Security Hub.

Security Hub n'est pas un outil général de gestion des journaux. Vous ne devez pas envoyer tous les journaux possibles à Security Hub.

Le partenaire a-t-il fourni une estimation du nombre de résultats qu'il enverra par jour et par client et à quelle fréquence (moyenne et rafale) ?

Le nombre de résultats uniques permet de calculer la charge sur Security Hub. Une découverte unique est définie comme une découverte avec une cartographie ASFF différente d'une autre découverte.

Par exemple, si une seule recherche est peupléeThreatIntelIndicatorset un autre peuplé seulementResources.Details.AWSEc2Instance, ce sont deux résultats uniques.

Le partenaire a-t-il une façon gracieuse de gérer les erreurs 4xx et 5xx de sorte qu'elles ne soient pas limitées et que toutes les conclusions puissent être envoyées ultérieurement ?

Il existe actuellement un taux de rafale de 30 à 50 TPS sur leBatchImportFindingsOpération d'API. Si des erreurs 4xx ou 5xx sont renvoyées, vous devez conserver l'état de ces résultats échoués afin de pouvoir les réessayer ultérieurement. Vous pouvez le faire via une file d'attente de lettres mortes ou une autreAWSservices de messagerie tels qu'Amazon SNS ou Amazon SQS.

Le partenaire maintient-il l'état de ses résultats afin qu'il sache archiver les résultats qui ne sont plus présents ?

Si vous envisagez de mettre à jour les résultats en écrasant l'ID de recherche d'origine, vous devez disposer d'un mécanisme permettant de conserver l'état afin que les informations correctes soient mises à jour pour la recherche correcte.

Si vous fournissez des résultats, n'utilisez pas leBatchUpdateFindingsopération de mise à jour des résultats. Cette opération ne doit être utilisée que par les clients. Vous n'utilisez queBatchUpdateFindingslorsque vous enquêtez sur les résultats et prenez des mesures à cet égard.

Le partenaire gére-t-il les nouvelles tentatives d'une manière qui ne compromet pas les résultats obtenus précédemment ?

Vous devez disposer d'un mécanisme permettant de conserver les identifiants de recherche d'origine en cas d'erreur afin de ne pas dupliquer ou écraser les résultats réussis par erreur.

Est-ce que le partenaire met à jour ses résultats en appelant le**`BatchImportFindings`**opération avec l'identifiant de recherche des résultats existants ?

Pour mettre à jour une recherche, vous devez remplacer la recherche existante en soumettant le même ID de recherche.

Le`BatchUpdateFindings`ne doit être utilisée que par les clients.

Le partenaire mette-t-il à jour les résultats à l'aide du**`BatchUpdateFindings`**API ?

Si vous prenez des mesures sur les résultats, vous pouvez utiliser le`BatchUpdateFindings`opération de mise à jour de champs spécifiques.

Le partenaire fournisse-t-il des informations sur la quantité de latence entre le moment où une recherche est créée et le moment où elle est envoyée de son produit à Security Hub ?

Vous devez minimiser la latence pour vous assurer que les clients voient les résultats dès que possible dans Security Hub.

Ces informations sont requises dans le manifeste.

Si l'architecture du partenaire doit envoyer des résultats à Security Hub à partir d'un compte client, l'a-t-il démontré avec succès ? Si l'architecture du partenaire doit envoyer des résultats à Security Hub depuis son propre compte, l'a-t-il démontré avec succès ?

Pendant les tests, les résultats doivent être envoyés avec succès à partir d'un compte que vous possédez différent du compte fourni pour l'ARN du produit.

L'envoi d'une recherche à partir du compte du propriétaire de l'ARN du produit peut contourner certaines exceptions d'erreur des opérations de l'API.

Le partenaire offre-t-il une recherche battue à Security Hub ?

Pour montrer que votre intégration fonctionne correctement, vous devez envoyer une recherche de battements de cœur. La recherche de battements de cœur est envoyée toutes les cinq minutes et utilise le type de recherche`Heartbeat`.

Cela est important si vous envoyez des résultats à partir d'un compte produit.

Le partenaire s'est-il intégré au compte de l'équipe produit Security Hub pendant les tests ?

Lors de la validation de la préproduction, vous devez envoyer des exemples de recherche à l'équipe produit Security HubAWS. Ces exemples démontrent que les résultats sont envoyés et cartographiés correctement.

Documentation

Ces questions concernent la documentation de l'intégration que vous fournissez.

Le partenaire héberge-t-il sa documentation sur un site Web dédié ?

La documentation doit être hébergée sur votre site Web sous forme de page Web statique, de wiki, de lecture des documents ou d'un autre format dédié.

Documentation d'hébergement surGitHubne satisfait pas aux exigences du site Web dédié.

La documentation des partenaires fournisse-t-elle des instructions sur la façon de configurer l'intégration Security Hub ?

Vous pouvez configurer l'intégration à l'aide d'un modèle iAC ou d'une intégration « en un clic » basée sur une console.

La documentation du partenaire fournisse-t-elle une description de leur cas d'utilisation ?

Le cas d'utilisation que vous fournissez dans le manifeste doit également être décrit dans la documentation

La documentation du partenaire fournisse-t-elle une justification des résultats qu'ils envoient ?

Vous devez fournir la justification des types de résultats que vous envoyez.

Par exemple, votre produit peut générer des résultats de vulnérabilités, de logiciels malveillants et d'antivirus, mais vous n'envoyez que des résultats de vulnérabilité et de logiciels malveillants à Security Hub. Dans ce cas, vous devez expliquer pourquoi vous n'envoyez pas de résultats antivirus.

La documentation du partenaire explique-t-elle comment le partenaire associe ses résultats à ASFF ?

Vous devez fournir la justification du mappage des résultats natifs d'un produit avec ASFF. Les clients veulent savoir où rechercher des informations spécifiques sur les produits.

La documentation du partenaire fournit-elle des conseils sur la façon dont le partenaire met à jour les résultats, s'il met à jour les résultats ?

Donnez aux clients des informations sur la façon dont vous conservez l'état, garantissez l'impotence et remplacez les résultats parup-to-dateinformations.

La documentation du partenaire décrive-t-elle la recherche de latence ?

Minimisez la latence pour garantir que les clients voient les résultats dès que possible dans Security Hub.

Ces informations sont requises dans le manifeste.

La documentation du partenaire décrive-t-elle comment leur score de gravité correspond au score de gravité ASFF ?

Fournissez des informations sur la façon dont vous effectuez`Severity.Original`pour`Severity.Label`.

Par exemple, si votre valeur de gravité est une note de lettre (A, B, C), vous devez fournir des informations sur la façon dont vous mapper la note de lettre à l'étiquette de gravité.

La documentation du partenaire fournit-elle une justification pour les cotes de confiance ?

Si vous indiquez des scores de confiance, ces scores doivent être classés.

Si vous utilisez des scores de confiance statiques ou des mappages dérivés de l'intelligence artificielle ou de l'apprentissage automatique, vous devez fournir un contexte supplémentaire.

La documentation du partenaire indique-t-elle quelles régions le partenaire prend en charge ou non ?

Remarque : Régions prises en charge ou non, afin que les clients sachent dans quelles régions ne doivent pas tenter d'intégration.

Informations sur la fiche produit

Ces questions concernent la fiche du produit affichée sur leIntégrationsde la console Security Hub.

Est-ce que le produit est fourniAWSID de compte valide et contient 12 chiffres ?

Les identifiants de compte comptent 12 chiffres. Si un ID de compte contient moins de 12 chiffres, l'ARN du produit ne sera pas valide.

La description du produit contient-elle 200 caractères ou moins ?

La description du produit fournie dans le JSON dans le manifeste ne doit pas dépasser 200 caractères, espaces compris.

Le lien de configuration mène-t-il à la documentation pour l'intégration ?

Le lien de configuration doit conduire à votre documentation en ligne. Il ne doit pas conduire à votre site Web principal ni à des pages marketing.

Le lien d'achat (s'il est fourni) mène-t-il à laAWS Marketplacela mise en vente du produit ?

Si vous fournissez un lien d'achat, il doit s'agir d'unAWS Marketplaceentrée. Security Hub n'accepte pas les liens d'achat qui ne sont pas hébergés parAWS.

Les catégories de produits décrivent-elles correctement le produit ?

Dans le manifeste, vous pouvez fournir jusqu'à trois catégories de produits. Ils doivent correspondre au JSON et ne peuvent pas être personnalisés. Vous ne pouvez pas fournir plus de trois catégories de produits.

Les noms de l'entreprise et des produits sont-ils valides et corrects ?

Le nom de l'entreprise doit comporter 16 caractères ou moins.

Le nom du produit doit comporter 24 caractères ou moins.

Le nom du produit figurant dans la fiche produit JSON doit correspondre au nom figurant dans le manifeste.

Informations marketing

Ces questions sont liées au marketing pour l'intégration.

La description du produit de la page des partenaires Security Hub est-elle contenue dans 700 caractères, espaces compris ?

La page des partenaires Security Hub n'accepte que 700 caractères maximum, espaces compris.

L'équipe modifiera les descriptions plus longues.

Le logo de la page des partenaires Security Hub ne dépasse-t-il pas 600 x 300 px ?

Fournissez une URL accessible au public avec un logo d'entreprise en PNG ou JPG ne dépassant pas 600 x 300 pixels.

Le lien hypertexte En savoir plus sur la page des partenaires Security Hub mène-t-il à la page Web dédiée du partenaire sur l'intégration ?

LeEn savoir pluslien ne doit pas conduire au site Web principal du partenaire ni aux informations de documentation.

Ce lien doit toujours accéder à une page Web dédiée contenant des informations marketing sur l'intégration.

Le partenaire propose-t-il une démonstration ou une vidéo didactique expliquant comment utiliser son intégration ?

Une vidéo de démonstration ou d'intégration est facultative, mais recommandée.

C'est unAWSUn billet de blog Partner Network est publié avec le partenaire et son responsable du développement de partenaires ou son représentant du développement des partenaires ?

AWSLes billets de blog Partner Network doivent être coordonnés à l'avance avec le responsable du développement des partenaires ou le représentant du développement des partenaires.

Ils sont séparés de tout article de blog que vous créez vous-même.

Prévoyez un délai de 4 à 6 semaines. Cet effort doit être lancé une fois le test effectué avec l'ARN du produit privé.

Un communiqué de presse dirigé par un partenaire est-il en cours de publication ?

Vous pouvez travailler avec votre responsable du développement de partenaires ou votre représentant du développement de partenaires pour obtenir un devis du vice-président des services de sécurité externes. Vous pouvez utiliser cette citation dans votre communiqué de presse.

Un billet de blog dirigé par un partenaire est-il publié ?

Vous pouvez créer vos propres articles de blog pour présenter l'intégration en dehors duAWSBlog Partenaire Network.

Un webinaire dirigé par des partenaires est-il publié ?

Vous pouvez créer vos propres webinaires pour présenter l'intégration.

Si vous avez besoin de l'aide de l'équipe Security Hub, travaillez avec l'équipe produit après avoir terminé le test avec l'ARN du produit privé.

Le partenaire a-t-il demandé de l'aide sur les réseaux sociaux auprès deAWS?

Après votre sortie, vous pouvez travailler avec leAWSLe marketing de sécurité conduit à l'utilisationAWSréseaux sociaux officiels pour partager des informations sur vos webinaires.

AWS Security HubFAQ sur les partenaires

Les questions suivantes sont courantes concernant la configuration et le maintien d'une intégration avecAWS Security Hub.

1. Quels sont les avantages de l'intégration avec Security Hub ?
   - Satisfaction client— La principale raison de s'intégrer à Security Hub est que vous avez demandé aux clients de le faire.

     Security Hub est le centre de sécurité et de conformité deAWSclients. Il est conçu comme le premier arrêt oùAWSles professionnels de la sécurité et de la conformité vont chaque jour comprendre leur état de sécurité et de conformité.

     Écoutez vos clients. Ils vous indiqueront s'ils veulent voir vos résultats dans Security Hub.
   - Possibilités de découverte— Nous promouvons des partenaires dotés d'intégrations certifiées dans la console Security Hub, y compris des liens vers leurAWS Marketplaceannonces. C'est un excellent moyen pour les clients de découvrir de nouveaux produits de sécurité.
   - Opportunités marketing— Les fournisseurs disposant d'intégrations approuvées peuvent participer à des webinaires, publier des communiqués de presse, créer des feuilles slick et démontrer leurs intégrations àAWSclients.
2. Quels sont les types de partenaires ?
   - Partenaires qui envoient les résultats à Security Hub
   - Partenaire recevant les résultats de Security Hub
   - Partenaires qui envoient et reçoivent des résultats
   - Partenaires-conseils qui aident les clients à configurer, personnaliser et utiliser Security Hub dans leur environnement
3. Comment fonctionne l'intégration d'un partenaire avec Security Hub à un niveau élevé ?

   Vous collectez les résultats à partir d'un compte client ou du vôtreAWScomptabilise et transforme le format des résultats enAWSFormat ASFF (Security Finding Format). Vous transférez ensuite ces résultats vers le point de terminaison régional Security Hub approprié.

   Vous pouvez également utiliserCloudWatchÉvénements pour recevoir les résultats de Security Hub.
4. Quelles sont les étapes de base pour terminer une intégration avec Security Hub ?

a. Envoyez les informations de manifeste de votre partenaire.

b. Recevez des ARN de produits à utiliser avec Security Hub, si vous souhaitez envoyer des résultats à Security Hub.

c. Mappez vos résultats à ASFF. Consultez the section called “Consignes pour la cartographie ASFF”.

d. Définissez votre architecture pour envoyer des résultats à Security Hub et recevoir des résultats depuis Security Hub. Suivez les principes énoncés dansthe section called “Principes de création et de mise à jour des résultats”.

e. Créez un cadre de déploiement pour les clients. Par exemple,AWS CloudFormationles scripts peuvent servir à cet effet.

f. Documentez votre configuration et fournissez des instructions de configuration aux clients.

g. Définissez toutes les informations personnalisées (règles de corrélation) que les clients peuvent utiliser avec votre produit.

h. Démontrez votre intégration à l'équipe Security Hub.

i. Soumettre des informations marketing pour approbation (langue du site Web, communiqué de presse, diapositive d'architecture, vidéo, feuille de présentation).

5. Quel est le processus de soumission du manifeste du partenaire ? Et pourAWSenvoyer les résultats à Security Hub ?

   Pour soumettre les informations du manifeste à l'équipe Security Hub, utilisez<securityhub-partners@amazon.com>.

   Vous recevez des ARN de produit dans un délai de sept jours civils.

6. Quels types de résultats dois-je envoyer à Security Hub ?

   La tarification du Security Hub est en partie basée sur le nombre de résultats ingérés. Pour cette raison, vous devez vous abstenir d'envoyer des résultats qui n'apportent pas de valeur ajoutée aux clients.

   Par exemple, certains fournisseurs de gestion des vulnérabilités envoient uniquement des résultats avec un score CVSS (Common Vulnerability Scoring System) égal ou supérieur à 3 sur 10 possibles.

7. Quelles sont les différentes approches pour envoyer les conclusions à Security Hub ?

   Voici les principales approches :

- Vous envoyez les résultats de leur propre pays désignéAWSutilisant le`BatchImportFindings`.
- Vous envoyez des résultats depuis le compte client à l'aide de la`BatchImportFindings`. Vous pouvez utiliser des approches assume-rôle, mais ces approches ne sont pas nécessaires.

Pour obtenir des directives générales sur l'utilisation`BatchImportFindings`, voirthe section called “Instructions relatives à l'utilisation du`BatchImportFindings`API”.

8. Comment puis-je rassembler mes résultats et les pousser vers un point de terminaison régional Security Hub ?

   Les partenaires ont utilisé différentes approches pour cela, car cela dépend fortement de l'architecture de votre solution.

   Par exemple, certains partenaires créent une application Python qui peut être déployée en tant queAWS CloudFormationscript. Le script rassemble les résultats du partenaire à partir de l'environnement client, les transforme en ASFF et les envoie au point de terminaison Security Hub Regional.

   D'autres partenaires créent un assistant complet qui offre au client une expérience en un seul clic pour transmettre les résultats vers Security Hub.

9. Comment savoir quand commencer à envoyer les résultats à Security Hub ?

   Security Hub prend en charge l'autorisation partielle par lots pour le`BatchImportFindings`Fonctionnement de l'API, afin que vous puissiez envoyer tous vos résultats à Security Hub pour tous vos clients.

   Si certains de vos clients ne sont pas encore abonnés à Security Hub, Security Hub n'ingère pas ces résultats. Il n'ingère que les résultats autorisés qui se trouvent dans le lot.

10. Quelles étapes dois-je effectuer pour envoyer les conclusions à l'instance Security Hub d'un client ?

    a. Assurez-vous que les bonnes stratégies IAM sont en place.

    b. Activez un abonnement produit (stratégies de ressources) pour les comptes. Utilisez soit le`EnableImportFindingsForProduct`Opération d'API ouIntégrations. Le client peut le faire ou vous pouvez utiliser des rôles entre comptes pour agir au nom du client.

    c. Assurer que le`ProductArn`du résultat est l'ARN public de votre produit.

    d. Assurer que le`AwsAccountId`de la recherche correspond à l'ID de compte du client.

e. Assurez-vous que vos résultats ne contiennent pas de données mal formées conformément à laAWSFormat ASFF (Security Finding Format). Par exemple, les champs obligatoires sont renseignés et aucune valeur non valide n'est disponible.

f. Envoyez les résultats par lots au point de terminaison régional approprié.

11. Quelles sont les autorisations IAM qui doivent être en place pour que je puisse envoyer des résultats ?

Les stratégies IAM doivent être configurées pour l'utilisateur ou le rôle IAM qui appelle`BatchImportFindings`ou d'autres appels d'API.

Le test le plus simple consiste à le faire à partir d'un compte administrateur. Vous pouvez les contraindre à`action: 'securityhub:BatchImportFindings'`et`resource: <productArn and/or productSubscriptionArn>`.

Les ressources d'un même compte peuvent être configurées avec des stratégies IAM sans avoir besoin de stratégies de ressources.

Pour exclure les problèmes de stratégie IAM de la part de l'appelant`BatchImportFindings`, définissez la stratégie IAM pour l'appelant comme suit :

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

Assurez-vous de vérifier qu'il n'y a pas de`Deny`les politiques de l'appelant. Une fois que vous l'avez fait fonctionner, vous pouvez limiter la stratégie aux éléments suivants :

```
{
    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. Qu'est-ce qu'un abonnement produit ?

    Pour recevoir les résultats d'un produit partenaire spécifique, le client (ou le partenaire ayant des rôles intercomptes travaillant pour le compte du client) doit établir un abonnement produit. Pour ce faire à partir de la console, ils utilisent leIntégrations. Pour ce faire à partir de l'API, ils utilisent le`EnableImportFindingsForProduct`Opération d'API.

    L'abonnement produit crée une stratégie de ressources qui autorise la réception ou l'envoi des résultats du partenaire par le client. Pour plus d'informations, consultez Cas d'utilisation et autorisations.

    Security Hub propose les types de stratégies de ressources suivants pour les partenaires :

    - `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
    - `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

    Au cours du processus d'intégration des partenaires, vous pouvez demander l'un ou les deux types de politiques.

    avec`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, vous pouvez envoyer des résultats à Security Hub uniquement à partir du compte répertorié dans l'ARN de votre produit.

    avec`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, vous ne pouvez envoyer des résultats que depuis le compte client qui vous a souscrit.

13. Supposons qu'un client ait créé un compte administrateur et ajouté quelques comptes membres. Le client doit-il m'abonner à chaque compte membre ? Ou est-ce que le client s'abonne uniquement à partir du compte administrateur, et je peux ensuite envoyer des résultats sur les ressources de tous les comptes membres ?

    Cette question demande si les autorisations sont créées pour tous les comptes membres en fonction de l'enregistrement du compte administrateur.

    Le client doit mettre en place un abonnement produit pour chaque compte. Ils peuvent le faire par programmation via l'API.

14. Qu'est-ce que l'ARN de mon produit ?

    L'ARN de votre produit est votre identifiant unique que Security Hub génère pour vous et que vous utilisez pour soumettre des résultats. Vous recevez un ARN produit pour chaque produit que vous

intégrez à Security Hub. Le bon ARN du produit doit faire partie de chaque recherche que vous envoyez à Security Hub. Les résultats sans ARN du produit sont supprimés. L'ARN du produit utilise le format suivant :

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

Voici un exemple :

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

Un ARN produit vous est attribué pour chaque région où Security Hub est déployé. L'ID de compte, la société et les noms de produits sont dictés par les soumissions du manifeste de votre partenaire. Vous ne modifiez jamais aucune des informations associées à l'ARN de votre produit, à l'exception du code de région. Le code de région doit correspondre à la région pour laquelle vous soumettez les résultats.

Une erreur courante consiste à modifier l'ID du compte pour qu'il corresponde au compte d'où vous travaillez actuellement. L'ID de compte ne change pas. Vous soumettez un ID de compte « domicile » dans le cadre de la soumission du manifeste. Cet ID de compte est verrouillé dans l'ARN de votre produit.

Lorsque Security Hub est lancé dans de nouvelles régions, il utilise automatiquement les codes de région standard pour générer les ARN de vos produits pour ces régions.

Chaque compte est également automatiquement provisionné avec un ARN de produit privé. Vous pouvez utiliser cet ARN pour tester les résultats d'importation dans votre propre compte de développement avant de recevoir votre ARN officiel de produit public.

15. Quel format doit-on utiliser pour envoyer les résultats à Security Hub ?

Les résultats doivent être fournis dans leAWSFormat ASFF (Security Finding Format). Pour plus d'informations, consultez .AWSFormat ASFF (Security Finding Format)dans leAWS Security HubGuide de l'utilisateur.

On s'attend à ce que toutes les informations contenues dans vos résultats natifs soient pleinement reflétées dans l'ASFF. Champs personnalisés tels que`ProductFields`et`Resource.Details.Other`vous permet de mapper des données qui ne s'intègrent pas parfaitement dans les champs prédéfinis.

16. Quel est le point de terminaison régional approprié à utiliser ?

Vous devez envoyer les résultats au point de terminaison régional Security Hub associé au compte client.

17. Où puis-je trouver la liste des points de terminaison régionaux ?

    Consultez Liste des points de terminaison Security Hub.

18. Puis-je soumettre des résultats interrégions ?

    Security Hub ne prend pas encore en charge la soumission de résultats entre régions pour le natif AWS services, tels qu'Amazon GuardDuty, Amazon Macie et Amazon Inspector. Si votre client l'autorise, Security Hub ne vous empêche pas de soumettre des résultats provenant de différentes régions.

    En ce sens, vous pouvez appeler un point de terminaison régional depuis n'importe où, et les informations sur les ressources de l'ASFF ne doivent pas nécessairement correspondre à la région du point de terminaison. Cependant, `ProductArn` doit correspondre à la région du point de terminaison.

19. Quelles sont les règles et directives applicables à l'envoi de lots de résultats ?

    Vous pouvez regrouper jusqu'à 100 résultats ou 240 Ko en un seul appel de `BatchImportFindings`. Mettez en file d'attente et regroupez autant de résultats que possible jusqu'à cette limite.

    Vous pouvez regrouper un ensemble de résultats provenant de différents comptes. Toutefois, si l'un des comptes du lot n'est pas abonné à Security Hub, l'ensemble du lot échoue. Il s'agit d'une limitation du modèle d'autorisation de ligne de base API Gateway.

    Consultez the section called “Instructions relatives à l'utilisation du `BatchImportFindings` API”.

20. Puis-je envoyer des mises à jour des résultats que j'ai créés ?

    Oui, si vous soumettez une recherche avec le même ARN de produit et le même ID de recherche, il écrase les données précédentes pour cette recherche. Notez que toutes les données sont écrasées, vous devez donc soumettre une recherche complète.

    Les clients sont comptés et facturés pour les nouveaux résultats et pour trouver des mises à jour.

21. Puis-je envoyer des mises à jour des résultats créés par quelqu'un d'autre ?

    Oui, si le client vous autorise à accéder au `BatchUpdateFindings` Opération API, vous pouvez mettre à jour certains champs à l'aide de cette opération. Cette opération est conçue pour être

utilisée par les clients, les SIEM, les systèmes de billetterie et les plates-formes SOAR (Security Orchestration, Automation and Response, Security Orchestration, Automation and Response).

22. Comment les résultats sont-ils vieillis ?

    Security Hub élimine les résultats 90 jours après la dernière mise à jour. Après cette période, les résultats de la période vieillissante sont purgés du Security HubOpenSearchcluster.

    Si vous mettez à jour une recherche avec le même ID de recherche et qu'elle a été annulée, une nouvelle recherche est créée dans Security Hub.

    Les clients peuvent utiliserCloudWatchÉvénements pour déplacer les résultats hors de Security Hub. Ce faisant, toutes les conclusions peuvent être envoyées aux cibles choisies par le client.

    En général, Security Hub vous recommande de créer de nouveaux résultats tous les 90 jours et de ne pas mettre à jour les résultats pour toujours.

23. Quels sont les gaz mis en place par Security Hub ?

    Accélérations avec Security Hub`GetFindings`Appels d'API, car l'approche recommandée pour les résultats d'accès utiliseCloudWatchÉvénements.

    Security Hub n'implémente aucune autre limitation sur les services internes, les partenaires ou les clients au-delà de celle appliquée par les appels API Gateway et Lambda.

24. Quels sont les SLA en temps opportun ou la latence ou les attentes concernant les résultats envoyés à Security Hub à partir des services source ?

    L'objectif est d'être le plus en temps quasi réel possible pour les résultats initiaux et les mises à jour des résultats. Vous devez envoyer les résultats à Security Hub dans les cinq minutes suivant leur création.

25. Comment puis-je recevoir les résultats de Security Hub ?

    Pour recevoir les résultats, utilisez l'une des méthodes suivantes.

    - Tous les résultats sont automatiquement envoyés àCloudWatchÉvénements. Un client peut créer des données spécifiquesCloudWatchRègles d'événements permettant d'envoyer des résultats à des cibles spécifiques, telles qu'un compartiment SIEM ou S3. Cette fonctionnalité a remplacé l'ancienne`GetFindings`Opération d'API.
    - UtiliserCloudWatchÉvénements pour les actions personnalisées. Security Hub permet aux clients de sélectionner des résultats ou des groupes de résultats spécifiques à partir de la console et de prendre des mesures à leur sujet. Par exemple, ils peuvent envoyer des résultats

à un SIEM, à un système de billetterie, à une plateforme de chat ou à un workflow de correction. Cela ferait partie d'un processus de triage des alertes effectué par un client dans Security Hub. Ces actions sont appelées actions personnalisées.

Lorsqu'un utilisateur sélectionne une action personnalisée, unCloudWatchest créé pour ces résultats spécifiques. Vous pouvez tirer parti de cette capacité et développerCloudWatchRègles et cibles d'événements que le client peut utiliser dans le cadre d'une action personnalisée. Notez que cette fonctionnalité n'est pas utilisée pour envoyer automatiquement tous les résultats d'un type ou d'une classe particulier àCloudWatchÉvénements. Il appartient à un utilisateur de prendre des mesures sur des résultats spécifiques.

Vous pouvez utiliser les opérations d'API d'actions personnalisées, telles que`CreateActionTarget`, pour créer automatiquement des actions disponibles pour votre produit (par exemple en utilisantAWS CloudFormationmodèles). Vous utiliseriez égalementCloudWatchOpérations d'API de règles d'événements pour créer des règlesCloudWatchRègles d'événements associées à l'action personnalisée. A l'aide deAWS CloudFormationmodèles, vous pouvez également créerCloudWatchRègles d'événements permettant d'ingérer automatiquement à partir de Security Hub tous les résultats ou tous les résultats présentant certaines caractéristiques.

26. Quelles sont les conditions requises pour qu'un fournisseur de services de sécurité géré (MSSP) devienne un partenaire Security Hub ?

    Vous devez démontrer comment Security Hub est utilisé dans le cadre de votre prestation de services aux clients.

    Vous devez disposer d'une documentation utilisateur expliquant votre utilisation de Security Hub.

    Si le MSSP est un fournisseur de recherche, il doit démontrer l'envoi de résultats à Security Hub.

    Si le MSSP ne reçoit que des résultats de Security Hub, il doit au minimum disposer d'unAWS CloudFormationpour configurer le modèle appropriéCloudWatchRègles relatives aux événements.

27. Quelles sont les conditions requises pour qu'un partenaire consultant APN non MSSP devienne un partenaire Security Hub ?

    Si vous êtes un partenaire consultant APN, vous pouvez devenir un partenaire Security Hub. Vous devez soumettre deux études de cas privées sur la façon dont vous avez aidé un client spécifique à effectuer les opérations suivantes.

    - Configurez Security Hub avec les autorisations IAM dont le client a besoin.

- Aidez à connecter des solutions ISV (éditeurs de logiciels indépendants) déjà intégrées à Security Hub à l'aide des instructions de configuration sur la page partenaire de la console.
- Aidez les clients avec des intégrations de produits personnalisées.
- Créez des informations personnalisées adaptées aux besoins des clients et aux jeux de données.
- Créez des actions personnalisées.
- Créez des classeurs de correction.
- Créez des démarrages rapides conformes aux normes de conformité Security Hub. Ils doivent être validés par l'équipe Security Hub.

Les études de cas n'ont pas besoin d'être publiquement partagées.

28. Quelles sont les exigences concernant la façon dont je déploie mon intégration avec Security Hub avec mes clients ?

    Les architectures d'intégration entre Security Hub et les produits partenaires varient d'un partenaire à l'autre en termes de fonctionnement de la solution de ce partenaire. Vous devez vous assurer que le processus de configuration de l'intégration ne dure pas plus de 15 minutes.

    Si vous déployez un logiciel d'intégration dans leAWSenvironnement, vous devez tirer partiAWS CloudFormationmodèles pour simplifier l'intégration. Certains partenaires ont créé une intégration en un clic, ce qui est fortement encouragé.

29. Quelles sont mes exigences en matière de documentation ?

    Vous devez fournir un lien vers la documentation qui décrit le processus d'intégration et de configuration entre votre produit et Security Hub, y compris votre utilisation deAWS CloudFormationmodèles.

    Cette documentation doit également inclure des informations sur votre utilisation d'ASFF. Plus précisément, vous devez énumérer les types de recherche ASFF que vous utilisez pour vos différents résultats. Si vous avez des définitions d'informations par défaut, nous vous recommandons de les inclure également ici.

    Pensez à inclure d'autres informations potentielles :

    - Votre cas d'utilisation pour l'intégration à Security Hub
    - Volume moyen de résultats envoyés
    - Votre architecture d'intégration

- Les régions que vous prenez en charge et que vous ne supportez pas
- Latence entre le moment où les résultats sont créés et quand ils sont envoyés à Security Hub
- Si vous mettez à jour les résultats

30. Que sont les informations personnalisées ?

    Nous vous encourageons à définir des informations personnalisées pour vos résultats. Les informations sont des règles de corrélation légères qui aident un client à hiérarchiser les résultats et les ressources qui nécessitent le plus d'attention et d'action.

    Security Hub dispose d'un`CreateInsight`Opération d'API. Vous pouvez créer des informations personnalisées dans un compte client dans le cadre de votreAWS CloudFormationmodèle. Ces informations apparaissent sur la console du client.

31. Puis-je soumettre des widgets de tableau de bord ?

    Non, pas à l'heure actuelle. Vous pouvez uniquement créer des informations gérées.

32. Quel est votre modèle de tarification ?

    ConsultezInformations de tarification avec Security Hub.

33. Comment puis-je soumettre les résultats au compte de démonstration de Security Hub dans le cadre du processus d'approbation final de mon intégration ?

    Envoyez les résultats au compte de démonstration de Security Hub à l'aide de votre ARN produit fourni, à l'aide de`us-west-2`en tant que région. Les résultats doivent inclure le numéro de compte de démonstration dans le`AwsAccountId`domaine de l'ASFF. Pour obtenir le numéro de compte de démonstration, contactez l'équipe Security Hub.

    Ne nous envoyez pas de données sensibles ou d'informations personnelles identifiables. Ces données sont utilisées pour les démonstrations publiques. Lorsque vous nous envoyez ces données, vous nous autorisez à les utiliser dans des démonstrations.

34. Quels sont les messages d'erreur ou de succès**`BatchImportFindings`**fournir ?

    Security Hub fournit une réponse pour autorisation et une réponse pour`BatchImportFindings`. Des messages de succès, d'échec et d'erreur plus nets sont en cours de développement.

35. De quelle gestion des erreurs le service source est-il responsable ?

    Les services sources sont responsables de la gestion de toutes les erreurs. Ils doivent gérer les messages d'erreur, les nouvelles tentatives, les limitations et les alarmants. Ils doivent également

gérer les commentaires ou les messages d'erreur envoyés via le mécanisme de rétroaction de Security Hub.

36. Quelles sont les solutions à des problèmes courants ?

    Un `AuthorizerConfigurationException` est causé soit par un mal formé `AwsAccountId` ou `ProductArn`.

    Lors du dépannage, notez les éléments suivants :

    - `AwsAccountId` doit comporter exactement 12 chiffres.
    - `ProductArn` doit être au format suivant : arn:aws:securityhub :*<us-west-2 or us-east-1>* :*<accountId>*:produit/*<company-id>*/*<product-id>*

      L'ID de compte ne change pas par rapport à celui que l'équipe Security Hub a inclus dans les ARN du produit qu'elle vous a fournis.

    `AccessDeniedException` est provoqué lorsqu'une recherche est envoyée vers ou depuis le mauvais compte, ou lorsque le compte ne possède pas de `ProductSubscription`. Le message d'erreur contiendra un ARN avec un type de ressource de `product` ou `product-subscription`. Cette erreur se produit uniquement pendant les appels entre comptes. Si vous appelez `BatchImportFindings` avec votre propre compte pour le même compte dans `AwsAccountId` et `ProductArn`, l'opération utilise les stratégies IAM et n'a rien à voir avec `ProductSubscriptions`.

    Assurez-vous que le compte client et le compte produit que vous utilisez sont les comptes enregistrés. Certains partenaires ont utilisé un numéro de compte pour le produit à partir de l'ARN du produit, mais ils essaient d'utiliser un compte entièrement différent pour appeler `BatchImportFindings`. Dans d'autres cas, ils ont créé `ProductSubscriptions` pour d'autres comptes clients, ou même pour leur propre compte produit. Ils n'ont pas créé `ProductSubscriptions` pour le compte client dans lequel ils ont tenté d'importer les conclusions.

37. Où puis-je envoyer des questions, des commentaires et des bugs ?

    `<securityhub-partners@amazon.com>`

38. Dans quelle région dois-je envoyer des résultats pour des éléments liés à l'échelle mondiale ? AWS services ? Par exemple, où dois-je envoyer les résultats liés à IAM ?

Envoyez les résultats à la même région où la découverte a été détectée. Pour un service tel que IAM, votre solution rencontrera probablement le même problème IAM dans plusieurs régions. Dans ce cas, la recherche est envoyée à chaque région où le problème a été détecté.

Si le client exécute Security Hub dans trois régions et que le même problème IAM est détecté dans les trois régions, envoyez la recherche aux trois régions.

Lorsqu'un problème est résolu, envoyez la mise à jour à la recherche à toutes les régions où vous avez envoyé la recherche initiale.

Historique du document pour le Partner Integration Guide

Le tableau suivant décrit les mises à jour de la documentation pour ce guide.

Modification	Description	Date
Exigences actualisées pour le logo de la console	Mise à jour des directives relatives au manifeste et au logo des partenaires afin d'indiquer que les partenaires doivent fournir à la fois une version en mode clair et une version en mode sombre du logo à afficher sur la console Security Hub. Les logos doivent être au format SVG.	10 mai 2021
Mise à jour des prérequis pour les nouveaux partenaires d'intégration	Security Hub permet désormais également aux partenaires qui ont rejoint leAWSparcours de partenaire ISV et qui utilise un produit d'intégration ayant terminé uneAWSExamen technique fondamental (FTR). Auparavant, tous les partenaires d'intégration devaient êtreAWSSélectionnez les partenaires de niveau.	29 avril 2021
`NewFindingProviderFields` objet dans ASFF	A mis à jour les informations sur la cartographie des résultats à l'ASFF. Pour`Confidence`,`Criticality`,`RelatedFindings`,`Severity`,	18 mars 2021

	et`Types`, les partenaires associent leurs valeurs aux domaines de`FindingProviderFields` .	
Nouveaux principes pour la création et la mise à jour des résultats	Ajout d'un nouvel ensemble de directives pour créer de nouvelles découvertes et mettre à jour les résultats existants dans Security Hub.	4 décembre 2020
Première version de ce guide	CeGuide d'intégration partenairesfournitAWSpartenaires fournissant des informations sur la manière d'établir une intégration avecAWS Security Hub.	23 Juin 2020

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.