Guide d'intégration des partenaires

# AWS Security Hub CSPM

# AWS Security Hub CSPM: Guide d'intégration des partenaires

# Table of Contents

# Vue d'ensemble de l'intégration de tiers avec AWS Security Hub CSPM

Ce guide est destiné aux AWS partenaires du réseau de partenaires (APN) qui souhaitent créer une intégration avec AWS Security Hub CSPM.

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

- Envoyer les résultats à Security Hub
- Consultez les résultats de Security Hub
- Les deux envoient des résultats à Security Hub et consomment les résultats de celui-ci
- Utilisez Security Hub comme centre d'une offre de fournisseurs de services de sécurité gérés (MSSP)
- Consultez les AWS clients pour savoir comment déployer et utiliser Security Hub

Ce guide d'intégration s'adresse principalement aux partenaires qui envoient des résultats à Security Hub.

Rubriques



## Pourquoi intégrer à AWS Security Hub CSPM ?

AWS Security Hub CSPM fournit une vue complète des alertes de sécurité prioritaires et de l'état de sécurité des comptes Security Hub. Security Hub permet à des partenaires tels que vous d'envoyer des résultats de sécurité à Security Hub afin de fournir à vos clients un aperçu des résultats de sécurité que vous générez.

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

- Répond à vos clients qui ont demandé une intégration avec Security Hub

- Fournit à vos clients une vue unique de leurs conclusions en matière de AWS sécurité
- Permet aux nouveaux clients de découvrir votre solution lorsqu'ils recherchent des partenaires fournissant des informations relatives à des types spécifiques d'événements de sécurité

Avant de créer une intégration avec Security Hub, examinez les raisons de cette intégration. Une intégration a plus de chances de réussir si vos clients souhaitent intégrer Security Hub à votre produit. Vous pouvez créer une intégration uniquement pour des raisons de marketing ou pour acquérir de nouveaux clients. Toutefois, si vous créez l'intégration sans aucune contribution du client actuel et que vous ne tenez pas compte des besoins de vos clients, l'intégration risque de ne pas donner les résultats escomptés.

# Préparation à l'envoi des résultats à AWS Security Hub CSPM

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

Au fur et à mesure que vous terminez les étapes d'intégration, assurez-vous de suivre les directives figurant dans the section called “Principes de création et de mise à jour des résultats”the section called “Directives pour le mappage ASFF”, etthe section called “Directives d'utilisation de l'`BatchImportFindings`API”.

1. Mappez vos résultats de AWS sécurité au format ASFF (Security Finding Format).
2. Créez votre architecture d'intégration pour transmettre les résultats au point de terminaison du Regional Security Hub approprié. Pour ce faire, vous définissez si vous allez envoyer les résultats depuis votre propre AWS compte ou 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 l'opération `EnableImportFindingsForProduct`API. Consultez la section Gestion des intégrations de produits dans le guide de AWS Security Hub CSPM l'utilisateur.

   Vous pouvez également vous abonner au produit pour eux. Pour ce faire, vous utilisez un rôle multi-comptes pour accéder à l'opération d'`EnableImportFindingsForProduct`API au nom du client.

   Cette étape définit les politiques de ressources nécessaires pour accepter les résultats de ce produit pour ce compte.

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

- Annonce de l'intégration de Cloud Custodian avec AWS Security Hub CSPM
- Utiliser AWS Fargate and Prowler pour envoyer les résultats de configuration de sécurité relatifs AWS aux services à Security Hub
- Comment importer des évaluations de AWS Config règles sous forme de résultats dans Security Hub

# Préparation à la réception des conclusions de AWS Security Hub CSPM

Pour recevoir les résultats de AWS Security Hub CSPM, utilisez l'une des options suivantes :

- Demandez à vos clients d'envoyer automatiquement tous les résultats à CloudWatch Events. Un client peut créer des règles d' CloudWatch événements spécifiques pour envoyer les résultats à des cibles spécifiques, telles qu'un SIEM ou un compartiment S3.
- Demandez à vos clients de sélectionner des résultats spécifiques ou des groupes de résultats dans la console Security Hub, puis de prendre des mesures en conséquence.

Par exemple, vos clients peuvent envoyer leurs résultats à un SIEM, à un système de billetterie, à une plateforme de chat ou à un flux de travail de correction. Cela ferait partie d'un flux de travail de triage des alertes effectué par un client au sein de Security Hub.

C'est ce que l'on appelle des actions personnalisées. Lorsqu'un utilisateur effectue une action personnalisée, un CloudWatch événement est créé pour ces résultats spécifiques. En tant que partenaire, vous pouvez tirer parti de cette fonctionnalité et créer des règles ou des cibles d' CloudWatch événements à utiliser par un client 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 en particulier à CloudWatch Events. Cette fonctionnalité permet à l'utilisateur de prendre des mesures en fonction de résultats spécifiques.

Les articles de blog suivants décrivent les solutions qui utilisent l'intégration avec Security Hub et CloudWatch Events pour des actions personnalisées.

- Comment intégrer des actions AWS Security Hub CSPM personnalisées avec PagerDuty

- Comment activer les actions personnalisées dans AWS Security Hub CSPM
- Comment importer des évaluations de AWS Config règles sous forme de résultats dans Security Hub

## Ressources pour en savoir plus sur AWS Security Hub CSPM

Les documents suivants peuvent vous aider à mieux comprendre la AWS Security Hub CSPM solution et à mieux comprendre comment AWS les clients peuvent utiliser le service.

- Présentation de la AWS Security Hub CSPM vidéo
- Guide de l'utilisateur de Security Hub
- Référence de l'API Security Hub
- Webinaire d'intégration

Nous vous encourageons également à activer Security Hub sur l'un de vos AWS comptes et à acquérir une expérience pratique du service.

# Conditions préalables requises pour les partenaires

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

- Vous êtes un partenaire de niveau AWS sélectionné ou supérieur.
- Vous avez rejoint le AWS ISV Partner Path et le produit que vous utilisez pour l'intégration de Security Hub a fait l'objet d'un examen technique de AWS base (FTR). Le produit reçoit ensuite un badge « Évalué par AWS ».

Vous devez également avoir conclu un accord mutuel de non-divulgation avec AWS.

# Cas d'utilisation de l'intégration et autorisations requises

AWS Security Hub CSPM permet aux AWS clients de recevoir les résultats des partenaires APN. Les produits du partenaire peuvent fonctionner à l'intérieur ou à l'extérieur du AWS compte du client. La configuration des autorisations dans le compte du client varie en fonction du modèle utilisé par le produit partenaire.

Dans Security Hub, le client contrôle toujours quels partenaires peuvent envoyer des résultats sur son compte. Les clients peuvent révoquer les autorisations accordées à 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 de détails sur la façon dont les clients gèrent les intégrations de produits, consultez la section Gestion des intégrations de produits dans le guide de l'AWS Security Hub CSPM utilisateur.

Une fois qu'un client s'est abonné à un produit partenaire, Security Hub crée automatiquement une politique de ressources gérées. La politique autorise le produit partenaire à utiliser l'opération `BatchImportFindings`API pour envoyer les résultats à Security Hub pour le compte du client.

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

## Hébergé par le partenaire : résultats envoyés depuis le compte du partenaire

Ce cas d'utilisation couvre les partenaires qui hébergent un produit sur leur propre AWS compte. Pour envoyer des résultats de sécurité à un AWS client, le partenaire appelle l'opération `BatchImportFindings`API depuis le compte du 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 l'opération d'`BatchImportFindings`API doit disposer d'une politique IAM autorisant le principal à appeler. `BatchImportFindings`

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

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

Pour envoyer les résultats de sécurité relatifs au compte du client, le produit partenaire utilise ses propres informations d'identification pour appeler l'opération `BatchImportFindings`API.

Voici un exemple de politique IAM qui accorde au principal du compte partenaire les autorisations Security Hub nécessaires.

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

## Hébergé par le partenaire : résultats envoyés depuis le compte client

Ce cas d'utilisation couvre les partenaires qui hébergent un produit sur leur propre AWS compte, mais qui utilisent un rôle multicompte pour accéder au compte du client. Ils appellent le fonctionnement de l'`BatchImportFindings`API depuis le compte du client.

Dans ce cas d'utilisation, pour appeler l'opération `BatchImportFindings`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 politique de ressources gérées doit autoriser l'utilisation de l'ARN du produit pour le compte du produit partenaire lors de l'appel. La politique de ressources gérées du Security Hub autorise le compte du produit partenaire et l'ARN du produit partenaire. L'ARN du produit est l'identifiant unique du partenaire en tant que fournisseur. Comme l'appel ne provient pas du compte du produit partenaire, le client doit explicitement autoriser le produit partenaire à envoyer les résultats à Security Hub.

La meilleure pratique pour les rôles entre comptes partenaires et comptes clients consiste à utiliser un identifiant externe fourni par le partenaire. Cet identifiant externe fait partie de la définition de la politique entre comptes dans le compte du client. Le partenaire doit fournir l'identifiant lorsqu'il assume le rôle. Un identifiant externe fournit un niveau de sécurité supplémentaire lorsque vous accordez l'accès au AWS compte à un partenaire. L'identifiant unique garantit que le partenaire utilise le bon compte client.

Pour permettre à un produit partenaire d'envoyer des résultats au client dans Security Hub avec un rôle multicompte, procédez en quatre étapes :

1. Le client, ou le partenaire utilisant des rôles multicomptes travaillant pour le compte du client, commence à s'abonner à un produit dans Security Hub.
2. Security Hub génère la bonne politique de ressources gérées avec la confirmation du client.
3. Le client configure le rôle multicompte manuellement ou à l'aide de. CloudFormation Pour plus d'informations sur les rôles entre comptes, consultez la section Fournir un accès aux AWS comptes détenus par des tiers dans le guide de l'utilisateur IAM.
4. Le produit enregistre en toute sécurité le rôle du client et l'identifiant externe.

Ensuite, le produit envoie les résultats à Security Hub :

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

Voici un exemple de politique IAM qui accorde les autorisations Security Hub nécessaires au rôle multicompte 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"
        }
    ]
```

```
}
```

La `Resource` section de la politique identifie l'abonnement au produit spécifique. 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 dont le produit est déployé sur le AWS compte du client. L'`BatchImportFindings`API est appelée depuis la solution qui s'exécute dans le compte du client.

Dans ce cas d'utilisation, le produit partenaire doit disposer d'autorisations supplémentaires pour appeler l'`BatchImportFindings`API. La manière dont cette autorisation est accordée varie en fonction de la solution partenaire et de la manière dont elle est configurée dans le compte du client.

Un exemple de cette approche est un produit partenaire qui s'exécute sur une EC2 instance du compte du client. Un rôle d' EC2 EC2 instance doit être associé à cette instance qui lui permet d'appeler l'opération `BatchImportFindings`d'API. Cela permet à l' EC2 instance d'envoyer les résultats de sécurité au compte du client.

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

Le client autorise le produit partenaire à envoyer les résultats de son compte au client dans Security Hub :

1. Le client déploie le produit partenaire sur son AWS compte manuellement à l'aide CloudFormation ou d'un autre outil de déploiement.
2. Le client définit la politique IAM nécessaire que le produit partenaire doit utiliser lorsqu'il envoie des résultats à Security Hub.
3. Le client associe la politique aux composants nécessaires du produit partenaire, tels qu'une EC2 instance, un conteneur ou une fonction Lambda.

Le produit peut désormais envoyer ses résultats à Security Hub :

1. Le produit partenaire utilise le AWS SDK ou AWS CLI appelle le fonctionnement de l'`BatchImportFindings`API dans Security Hub. Il effectue l'appel depuis le composant du compte du client auquel la police est attachée.

2. Pendant l'appel d'API, les informations d'identification temporaires nécessaires sont générées pour permettre à l'`BatchImportFindings`appel de réussir.

Voici un exemple de politique 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'intégration des 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 les résultats de sécurité à AWS Security Hub CSPM.

1. Vous engagez un engagement auprès de l'équipe des partenaires APN ou de l'équipe Security Hub et vous exprimez votre intérêt à devenir partenaire de Security Hub. Vous identifiez les adresses e-mail à ajouter aux canaux de communication du Security Hub.
2. AWS vous fournit le matériel d'accueil des partenaires du Security Hub.
3. Vous êtes invité à accéder à la chaîne Slack, partenaire de Security Hub, où vous pouvez poser des questions concernant votre intégration.
4. Vous fournissez aux contacts des partenaires APN un projet de manifeste d'intégration du produit à des fins de révision.

   Le manifeste d'intégration du produit contient des informations qui sont utilisées pour créer le produit partenaire Amazon Resource Name (ARN) avec lequel l'intégration doit être effectuée AWS Security Hub CSPM.

   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 du Security Hub.

   Il n'est pas nécessaire que cette version initiale du manifeste d'intégration du produit contienne tous les détails. Mais il doit au moins contenir les informations relatives au cas d'utilisation et à l'ensemble de données.

   Pour plus de détails sur le manifeste et les informations requises, consultezManifeste d'intégration du produit.
5. L'équipe Security Hub vous fournit un ARN de 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 pour en recevoir.

   Cartographie des résultats avec ASFF

   Pour envoyer des résultats à Security Hub, vous devez mapper vos résultats au format ASFF ( AWS Security Finding Format).

L'ASFF fournit une description cohérente des résultats qui peuvent être partagés entre les services de AWS sécurité, les partenaires et les systèmes de sécurité des clients. Cela réduit les efforts d'intégration, encourage l'adoption d'un langage commun et fournit un modèle aux responsables de la mise en œuvre.

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

Consultez the section called “Directives pour le mappage ASFF”.

Création et test de l'intégration

Vous pouvez effectuer tous les tests d'intégration à l'aide d'un AWS compte que vous possédez. Cela vous donne une visibilité complète sur la manière dont les résultats apparaissent dans Security Hub. Cela vous aide également à comprendre l'expérience du client face à vos résultats de sécurité.

Vous utilisez l'opération `BatchImportFindings`API pour envoyer des résultats nouveaux et actualisés à Security Hub.

Tout au long de la construction d'une intégration au Security Hub, vous AWS encourage à tenir vos contacts partenaires APN informés de la progression de votre intégration. Vous pouvez également demander à vos contacts partenaires APN de l'aide pour les questions relatives à l'intégration.

Consultez the section called “Directives d'utilisation de l'`BatchImportFindings`API”.

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

   Si elle est à l'aise avec l'intégration, l'équipe du Security Hub donne son accord pour procéder à votre inscription en tant que fournisseur.
8. Vous AWS fournissez 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 votre intégration au Security Hub. Consultez Go-to-market activités.

    Security Hub vous recommande au minimum 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 la AWS YouTube chaîne.
    - Un schéma d'architecture en une diapositive à ajouter au diaporama du premier appel de Security Hub.

# Go-to-market activités

Les partenaires peuvent également participer à des activités marketing facultatives pour expliquer et promouvoir leur AWS Security Hub CSPM intégration.

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

AWS Les 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 de détails sur ces programmes, contactez votre responsable des partenaires.

## Entrée sur la page des partenaires du Security Hub

Une fois que vous avez été approuvé en tant que partenaire du Security Hub, votre solution peut être affichée sur la page AWS Security Hub CSPM des partenaires.

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

- Brève description de votre solution, de son intégration à Security Hub et de la valeur que cette intégration apporte aux clients. Cette description est limitée à 700 caractères, espaces compris.
- URL d'une page qui décrit votre solution. Ce site doit être spécifique à votre AWS intégration et plus particulièrement à votre intégration au Security Hub. Il doit se concentrer sur l'expérience client et sur 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”.

## Communiqué de presse

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

Avant de publier le communiqué de presse, vous devez le soumettre AWS pour examen par le service marketing des partenaires APN, la direction du Security Hub et les services de sécurité AWS externes (ESS). Le communiqué de presse peut inclure une proposition de devis pour le vice-président de l'ESS.

Pour lancer ce processus, utilisez votre PDM. Nous avons un accord de niveau de service (SLA) de 10 jours ouvrables pour examiner les communiqués de presse.

# AWS Blog du réseau de partenaires (APN)

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

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

## Informations essentielles à savoir sur le blog APN

Lorsque vous créez un article de blog, gardez les points suivants à l'esprit.

Que contient un article de blog ?

- Les publications des partenaires doivent être éducatives et fournir une expertise approfondie sur un sujet pertinent pour les AWS clients.
- La longueur idéale ne doit pas dépasser 1 500 mots. Les lecteurs apprécient les contenus éducatifs approfondis qui leur enseignent ce qu'il est possible de faire sur AWS.
- Le contenu doit être original pour 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 relatives à la 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 Select dotés d'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, sa couverture AWS doit être équitable.

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 qu'il ne soit publié ?

Une fois que vous avez soumis le premier brouillon complet du billet de blog, il faut de quatre à six semaines pour le modifier.

## Pourquoi écrire pour le blog de l'APN ?

Un article de blog APN peut apporter les avantages suivants.

- Crédibilité — Pour les partenaires APN, la publication d'un article par AWS peut influencer les clients du monde entier.
- Visibilité — Le blog APN est l'un des blogs les plus lus AWS avec 1,79 million de pages vues en 2019, trafic influencé inclus.
- Business — Les publications des partenaires APN comportent des boutons de connexion qui peuvent générer des prospects par le biais du programme APN Customer Engagements (ACE).

## Quel type de contenu convient le mieux ?

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

- Le contenu technique est le type d'histoire le plus populaire. Cela inclut des informations sur les solutions et des instructions pratiques. Plus de 75 % des lecteurs consultent ce contenu technique.
- Les clients apprécient les histoires de niveau 200 ou plus qui montrent comment un produit fonctionne AWS ou comment un partenaire APN a résolu un problème commercial pour ses clients.
- Les publications rédigées par des experts techniques ou des experts en la matière sont de loin les plus performantes.

# Feuille Slick ou fiche marketing

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

Si vous créez une feuille de synthèse pour votre intégration, envoyez-en une copie à l'équipe du Security Hub. Ils l'ajouteront à la page partenaire.

# Livre blanc ou livre électronique

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

# Webinaire

Si vous organisez un webinaire sur votre intégration, envoyez un enregistrement du webinaire à l'équipe du Security Hub. L'équipe y redirigera depuis la page partenaire.

L'équipe peut également fournir un expert en la matière du 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 fonctionnelle. Publiez une telle vidéo sur le compte de votre plateforme vidéo, et l'équipe Security Hub créera un lien vers celle-ci depuis la page partenaire.

# Manifeste d'intégration du produit

Chaque partenaire AWS Security Hub CSPM d'intégration doit remplir un manifeste d'intégration du produit qui fournit les détails requis pour l'intégration proposée.

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

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

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

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

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

Table des matières

  - Logos pour la console Security Hub
  - Types de résultats
  - Hotline
  - Détection du rythme cardiaque
- AWS Security Hub CSPM informations sur la console
  - Informations sur l'entreprise
  - Informations sur le produit

# Cas d'utilisation et informations marketing

Les cas d'utilisation suivants peuvent vous aider à effectuer AWS Security Hub CSPM une configuration à différentes fins.

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

Nécessaire pour les fournisseurs de logiciels indépendants (ISV).

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

Les informations suivantes doivent figurer dans votre documentation.

- Allez-vous envoyer des résultats, en recevoir, 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 avez l'intention de recevoir des résultats, que ferez-vous avec ces résultats ? Quels types de conclusions recevrez-vous ? Par exemple, recevrez-vous tous les résultats, les résultats d'un certain type ou uniquement les résultats spécifiques sélectionnés par un client ?
- Prévoyez-vous de mettre à jour les résultats ? Dans l'affirmative, quels champs mettrez-vous 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 de recherche pour les clients.

  Pour mettre à jour un résultat, vous envoyez un résultat avec un numéro de recherche attribué à un résultat que vous avez déjà envoyé.

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 du partenaire consultant (CP)

Obligatoire si vous êtes un partenaire consultant du Security Hub.

Fournissez deux exemples d'utilisation par des clients pour votre travail avec Security Hub. Il peut s'agir de cas d'usage privé. L'équipe du Security Hub ne les annonce nulle part. Ils doivent décrire l'une ou l'autre 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 un modèle ? CloudFormation
- 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 configurer un tableau de bord exécutif ?

## Jeux de données

Obligatoire si vous envoyez des résultats à Security Hub.

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

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

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

## Architecture

Obligatoire si vous envoyez ou recevez des résultats depuis Security Hub.

Décrivez comment vous allez intégrer Security Hub. Ces informations doivent également être reflétées dans votre documentation.

Vous devez fournir des diagrammes d'architecture. Lorsque vous préparez vos diagrammes d'architecture, tenez compte des points suivants :

- Quels AWS services, agents du système d'exploitation, etc. utiliserez-vous ?
- Si vous envoyez des résultats à Security Hub, les enverrez-vous depuis le AWS compte client ou depuis votre propre AWS 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 ou recevez des résultats depuis Security Hub.

Décrivez comment un client configurera votre intégration à Security Hub.

Vous devez au minimum utiliser des CloudFormation modèles ou une infrastructure similaire telle que des modèles de code. Certains partenaires ont fourni une interface utilisateur permettant l'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 des résultats à Security Hub.

Combien de mises à jour par mois (en moyenne et au maximum) comptez-vous envoyer à Security Hub pour l'ensemble de votre clientèle ? Les estimations par ordre de grandeur sont acceptables.

## Latence

Obligatoire si vous envoyez des résultats à Security Hub.

En combien de temps comptez-vous regrouper les résultats et les envoyer à Security Hub ? En d'autres termes, quel est le temps de 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 courante des clients.

## Description de l'entreprise et du produit

Nécessaire 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 notre page dédiée aux partenaires du Security Hub.

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

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

## Ressources du site Web des partenaires

Nécessaire pour toutes les intégrations avec Security Hub.

Vous devez au minimum fournir une URL à utiliser pour le lien hypertexte Learn More sur la page des partenaires du 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 ne pouvez avoir qu'une seule page de destination pour eux. Security Hub recommande d'inclure sur cette page de destination un lien vers vos instructions de configuration.

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 un lien vers ces sites depuis sa page dédiée aux partenaires.

## Logo pour la page des partenaires

Nécessaire pour toutes les intégrations de Security Hub.

Fournissez l'URL d'un logo à afficher sur la page des partenaires du 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

Nécessaire pour toutes les intégrations.

Fournissez URLs les logos en mode clair et en 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, pas de rembourrage
- Fond : transparent

Pour des instructions détaillées concernant le petit logo, voirthe section called “Consignes relatives au logo de la console”.

## Types de résultats

Obligatoire si vous envoyez des résultats à Security Hub.

Fournissez un tableau qui décrit les types de recherche au format ASFF que vous utilisez et la manière 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 de l'AWS Security Hub CSPM utilisateur.

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

## Hotline

Nécessaire pour toutes les intégrations avec Security Hub.

Indiquez l'adresse e-mail et le numéro de téléphone ou le numéro de téléavertisseur d'un point de contact technique. Security Hub communiquera avec ce contact pour tout 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.

## Détection du rythme cardiaque

Recommandé si vous envoyez des résultats à Security Hub.

Pouvez-vous envoyer à Security Hub un message toutes les cinq minutes indiquant que votre intégration à Security Hub est fonctionnelle ?

Si vous le pouvez, faites-le en utilisant le type de rechercheHeartbeat.

# AWS Security Hub CSPM informations sur la console

Fournissez à l' AWS Security Hub CSPM équipe 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 du Security Hub.

## Informations sur l'entreprise

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 l'entreprise contiennent les champs suivants :

| Champ | Obligatoire | Description |
| --- | --- | --- |
| id | Oui | L'identifiant unique de l'entreprise. L'identifiant de l'entreprise doit être unique pour toutes les entreprises.<br><br>C'est probablement le même ou similaire ànname.<br><br>Type : String |

| Champ | Obligatoire | Description |
| --- | --- | --- |
| | | Longueur minimale : 5 caractères<br><br>Longueur maximale : 24 caractères<br><br>Caractères autorisés : lettres minuscules, chiffres et tirets<br><br>Doit commencer par une lettre minuscule. Doit se terminer par une minuscule ou un chiffre. |
| `name` | Oui | Le nom de la société du fournisseur à afficher sur la console Security Hub.<br><br>Type : String<br><br>Longueur maximale : 16 caractères |
| `description` | Oui | Description de la société du fournisseur à afficher sur la console Security Hub.<br><br>Type : String<br><br>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 les deux envoie et reçoit des résultats.<br><br>Si vous êtes un partenaire consultant, laissez ce champ vide.<br><br>Type : Tableau de chaînes<br><br>Valeurs valides : `SEND_FINDINGS_TO_SECURITY_HUB` \| `RECEIVE_FINDINGS_FROM_SECURITY_HUB` |
| `id` | Oui | L'identifiant unique du produit. Ils doivent être uniques au sein d'une entreprise. Il n'est pas nécessaire qu'ils soient uniques dans toutes les entreprises. C'est probablement le même ou similaire à`name`.<br><br>Type : String<br><br>Longueur minimale : 5 caractères<br><br>Longueur maximale : 24 caractères<br><br>Caractères autorisés : lettres minuscules, chiffres et tirets<br><br>Doit commencer par une lettre minuscule. Doit se terminer par une minuscule ou un chiffre. |

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

| Champ | Obligatoire | Description |
| --- | --- | --- |
| `commercialAccountNumber` | Oui | Numéro de AWS compte principal du produit pour les AWS régions.<br><br>Si vous envoyez des résultats à Security Hub, le compte que vous fournissez dépend de l'endroit d'où vous envoyez les résultats.<br><br>• Depuis votre AWS compte. Dans ce cas, indiquez le numéro de compte que vous utilisez pour soumettre les résultats.<br>• Depuis le AWS compte du client. Dans ce cas, Security Hub vous recommande de fournir le numéro de compte principal que vous utilisez pour tester l'intégration.<br><br>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.<br><br>Si vous recevez uniquement les résultats de Security Hub, ce numéro de compte n'est pas requis.<br><br>Type : String |

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

| Champ | Obligatoire | Description |
| --- | --- | --- |
| `chinaAccountNumber` | Non | Le numéro de AWS compte principal du produit pour les régions de Chine (si votre produit est disponible dans les régions de Chine).<br><br>Si vous envoyez des résultats à Security Hub, le compte que vous fournissez dépend de l'endroit d'où vous envoyez les résultats.<br><br>• Depuis votre AWS compte. Dans ce cas, indiquez le numéro de compte que vous utilisez pour soumettre les résultats.<br>• Depuis le AWS 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.<br><br>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.<br><br>Si vous recevez uniquement des résultats de Security Hub, il peut s'agir de n'importe quel compte que vous possédez dans une région de Chine.<br><br>Type : String |
| `name` | Oui | Le nom du produit du fournisseur à afficher sur la console Security Hub.<br><br>Type : String<br><br>Longueur maximale : 24 caractères |

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

| Champ | Obligatoire | Description |
| --- | --- | --- |
| `category` | Oui | Les catégories qui définissent votre produit. Vos sélections sont affichées sur la console Security Hub.<br><br>Choisissez jusqu'à trois catégories.<br><br>Les sélections personnalisées ne sont pas autorisées. Si vous pensez que votre catégorie est absente, contactez l'équipe Security Hub.<br><br>Type : Array<br><br>Catégories disponibles :<br><br>• `API Firewall`<br>• `Asset Management`<br>• `AV Scanning and Sandboxing`<br>• `Backup and Disaster Recovery`<br>• `Breach and Attack Simulation`<br>• `Bug Bounty Platform`<br>• `Certificate Management`<br>• `Cloud Access Security Broker`<br>• `Cloud Security Posture Managemen t`<br>• `Configuration and Patch Management`<br>• `Configuration Management Database (CMDB)`<br>• `Consulting Partner`<br>• `Container Security`<br>• `Cyber Range`<br>• `Data Access Management`<br>• `Data Classification` |

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

| Champ | Obligatoire | Description |
| --- | --- | --- |
| | | • `Managed Security Service Provider (MSSP)`<br>• `Micro-Segmentation`<br>• `Multi-Cloud Management`<br>• `Multi-Factor Authentication`<br>• `Network Access Control (NAC)`<br>• `Network Firewall`<br>• `Network Forensics`<br>• `Network Intrusion Detection Systems (IDS)`<br>• `Network Intrusion Prevention Systems (IPS)`<br>• `Phishing Simulation and Training`<br>• `Privacy Operations`<br>• `Privileged Access Management`<br>• `Rogue Device Detection`<br>• `Runtime Application Self-Protection (RASP)`<br>• `Secure Web Gateway` |
| `marketplaceUrl` | Non | URL de AWS Marketplace destination de votre produit. L'URL s'affiche dans la console Security Hub.<br><br>Type : String<br><br>Il doit s'agir d'une AWS Marketplace URL.<br><br>Si vous n'avez pas d' AWS Marketplace annonce, laissez ce champ vide. |

| Champ | Obligatoire | Description |
| --- | --- | --- |
| `configurationUrl` | Oui | URL de la documentation de votre produit concernant l'intégration à Security Hub. Ce contenu est hébergé sur votre site Web ou sur une page Web que vous gérez, telle qu'une GitHub page.<br><br>Type : String<br><br>Votre documentation doit inclure les informations suivantes.<br><br>• Instructions de configuration<br>• Liens vers CloudFormation des modèles (si nécessaire)<br>• Informations sur votre cas d'utilisation pour l'intégration<br>• Latence<br>• Cartographie ASFF<br>• Les types de résultats étaient les suivants :<br>• Architecture |

# Directives et listes de contrôle

Lorsque vous préparez le matériel requis pour votre AWS Security Hub CSPM intégration, suivez ces directives.

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

Rubriques



## Instructions relatives à l'affichage du logo sur la AWS Security Hub CSPM console

Pour que le logo s'affiche sur la AWS Security Hub CSPM console, suivez ces instructions.

Modes clair et foncé

Vous devez fournir une version du logo en mode clair et une version en mode sombre.

Format

Format de fichier SVG

Couleur d'arrière-plan

Transparent

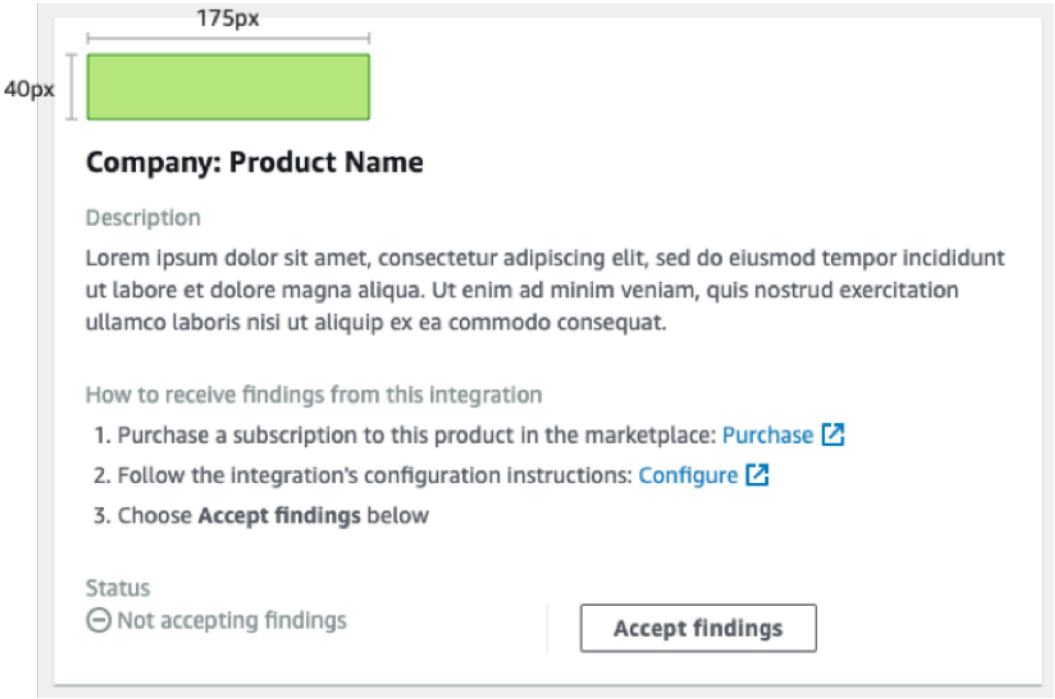
Size

Le ratio idéal est de 175 pixels de large sur 40 pixels de haut.

La hauteur minimale est de 40 pixels.

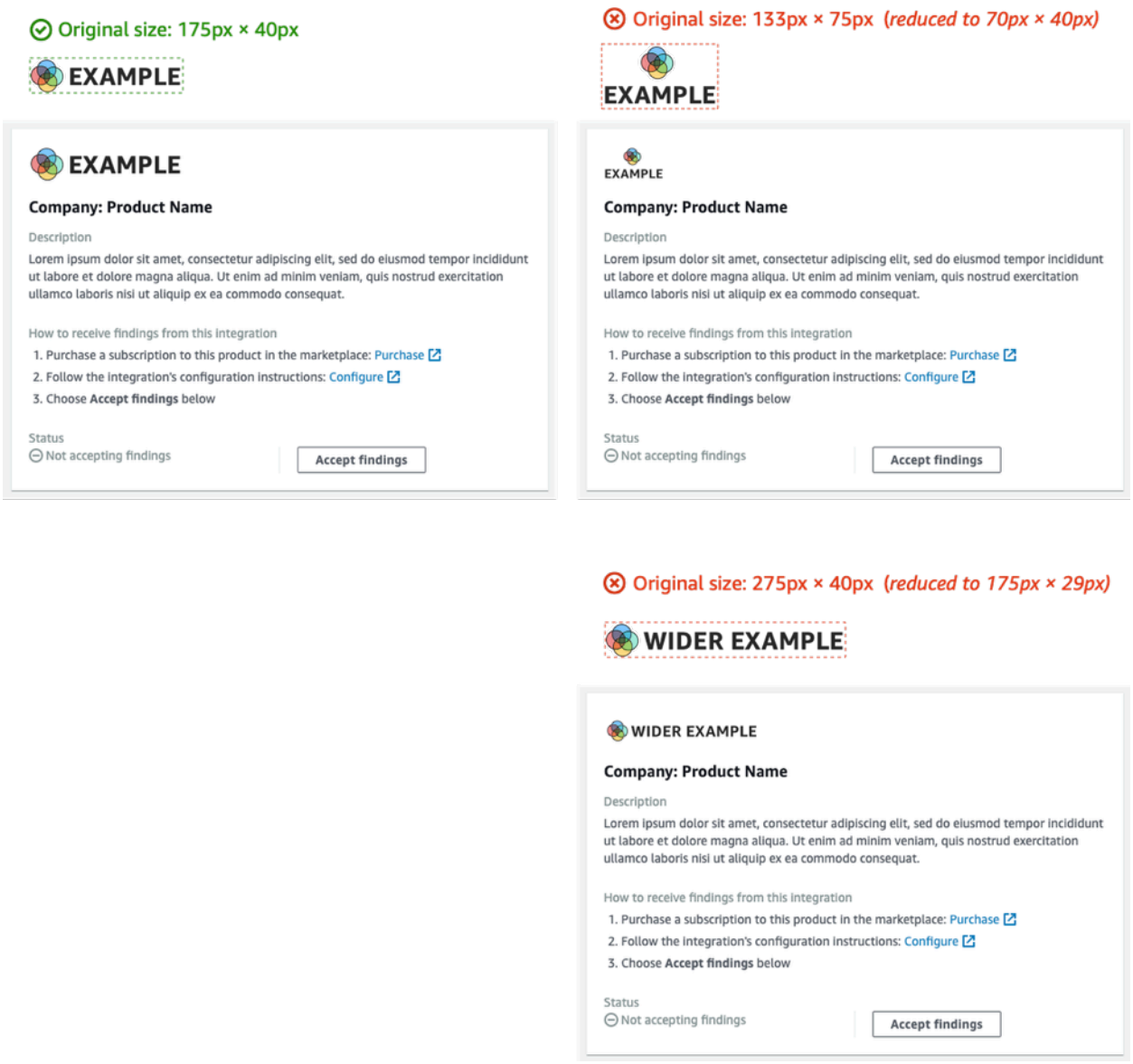
Les logos rectangulaires fonctionnent le mieux.

L'image suivante montre comment le 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 pixels et à une largeur maximale de 175 pixels. Cela affecte la manière dont le logo est affiché sur la console Security Hub.

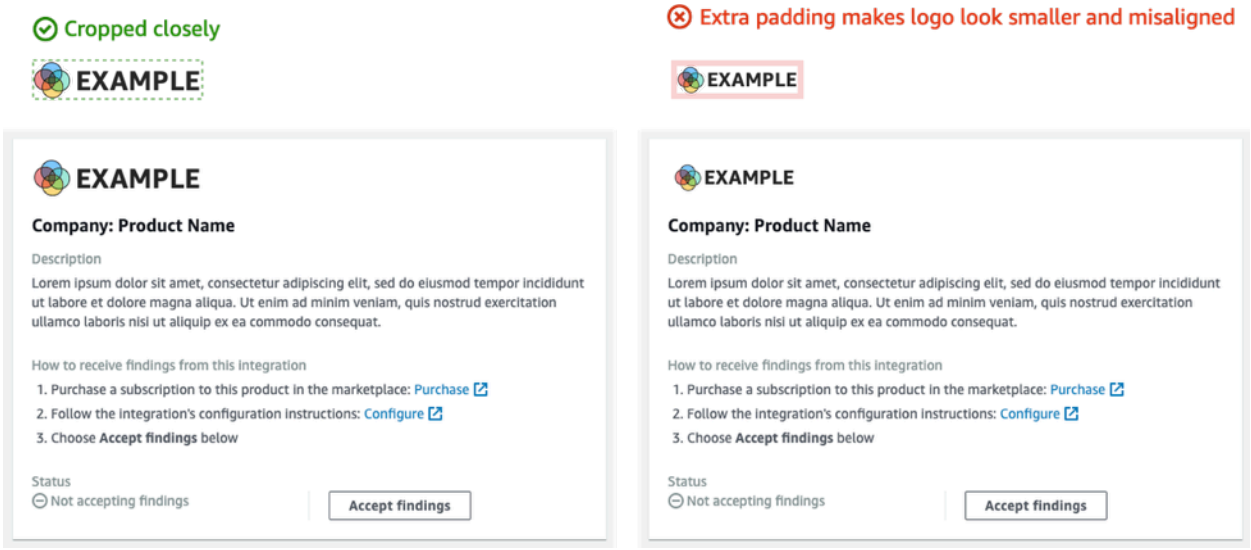
L'image suivante compare l'affichage d'un logo dont la taille était idéale à celui de logos plus larges ou plus hauts.




## Recadrage

Recadrez l'image du logo le plus près possible. Ne fournissez pas 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 la manière dont vous allez créer et mettre à jour les résultats dans AWS Security Hub CSPM, gardez les principes suivants à l'esprit.

Spécifiez les résultats afin que les clients puissent facilement prendre des mesures en conséquence.

Les clients souhaitent automatiser les actions de réponse et de correction et corréler les résultats avec les autres résultats. Pour étayer cette thèse, les résultats doivent présenter les caractéristiques suivantes :

- Ils doivent généralement traiter d'une ressource unique ou primaire.
- Ils doivent avoir un seul type de recherche.
- Ils doivent faire face à un seul événement de sécurité.

Lorsqu'un résultat contient des données relatives à plusieurs événements de sécurité, il est plus difficile pour les clients de prendre des mesures en conséquence.

Mappez tous vos champs de recherche au format ASFF ( AWS Security Finding Format). Permettez à vos clients de compter sur Security Hub comme source de vérité.

Les clients s'attendent à ce que chaque champ correspondant à 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 du résultat. L'absence de données les amène à perdre confiance dans Security Hub en tant que source centrale d'informations de sécurité.

Minimisez la redondance des résultats. Ne surchargez pas les clients à trouver des volumes.

Security Hub n'est pas un outil général de gestion des journaux. Vous devez envoyer à Security Hub des résultats hautement exploitables auxquels les clients peuvent directement répondre, corriger ou corréler avec d'autres résultats.

Lorsqu'une modification mineure est apportée à la constatation, mettez-la à jour au lieu d'en créer une nouvelle.

En cas de modification majeure du résultat, par exemple du score de gravité ou de l'identifiant de ressource, créez un nouveau résultat.

Par exemple, créer des résultats pour des scans de ports individuels en temps réel n'est pas très exploitable. Comme l'analyse des ports peut se faire en continu, elle produirait un grand nombre de résultats. Il est beaucoup plus convaincant et précis de simplement mettre à jour l'heure du dernier scan et le nombre de scans en fonction d'une seule recherche pour un scan de port sur un port MongoDB à partir d'un nœud TOR.

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

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

Par exemple, les clients souhaitent pouvoir ajouter des notes, des balises et ajuster les scores de sévérité en fonction du type de compte ou du type de ressource auquel le résultat est associé.

# Directives pour mapper les résultats dans le format ASFF ( AWS Security Finding Format)

Utilisez les directives suivantes pour associer vos résultats à l'ASFF. Pour une description détaillée de chaque champ et objet ASFF, voir AWS Security Finding Format (ASFF) dans le guide de l'AWS Security Hub CSPM utilisateur.

## Informations d'identification

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

`ProductArn`est l'ARN qui vous AWS Security Hub CSPM est attribué.

`Id`est la valeur que Security Hub utilise pour indexer les résultats. L'identifiant de recherche doit être unique, afin de garantir que les autres résultats ne soient pas remplacés. Pour mettre à jour un résultat, soumettez-le à nouveau avec le même identifiant.

`GeneratorId`peut être identique `Id` ou faire référence à une unité logique discrète, telle qu'un identifiant de GuardDuty détecteur Amazon, un identifiant d' AWS Config enregistreur ou un identifiant d'analyseur d'accès IAM.

## Title and Description

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

Ajoutez des informations plus détaillées à`Description`. `Description`est limité à 1024 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 les informations relatives au type de recherche dans`FindingProviderFields.Types`.

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

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

## Horodatages

Le format ASFF inclut plusieurs 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 ISO86 01 de Python 3.8.

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

**`FirstObservedAt` et `LastObservedAt`**

`FirstObservedAt`et `LastObservedAt` doit correspondre à la date à laquelle votre système a observé le résultat. Si vous n'enregistrez pas ces informations, vous n'avez pas besoin de soumettre ces horodatages.

Les valeurs correspondent au format ISO86 01 de Python 3.8.

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

## Severity

Vous fournissez des informations de gravité dans l'`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`**

L'indicateur Security Hub requis pour déterminer la gravité de la constatation. Les valeurs autorisées sont les suivantes.

- `INFORMATIONAL`— Aucun problème n'a été détecté.
- `LOW`— Le problème ne nécessite pas d'action en soi.
- `MEDIUM`— Le problème doit être traité, mais pas de toute urgence.
- `HIGH`— Le problème doit être traité en priorité.
- `CRITICAL`— Le problème doit être résolu immédiatement pour éviter de nouveaux dommages.

Les résultats conformes devraient toujours être `Label` définis sur`INFORMATIONAL`. Des exemples de `INFORMATIONAL` résultats sont les résultats des contrôles de sécurité réussis et AWS Firewall Manager les résultats corrigés.

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

Votre documentation d'intégration doit inclure la justification de votre mappage.

## Remediation

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

`Remediation.Recommendation.Text`apparaît dans la section Remédiation des détails des résultats. Il est lié par un hyperlien à la valeur de. `Remediation.Recommendation.Url`

À l'heure actuelle, seuls les résultats issus des normes Security Hub, d'IAM Access Analyzer et de Firewall Manager affichent des hyperliens vers la documentation expliquant comment remédier à ces résultats.

## SourceUrl

À utiliser uniquement `SourceUrl` si vous pouvez fournir une URL contenant un lien profond vers votre console pour cette recherche spécifique. Sinon, omettez-le du mappage.

Security Hub ne prend pas en charge les hyperliens provenant de ce champ, mais ils sont exposés sur la console Security Hub.

## Malware, Network, Process, ThreatIntelIndicators

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

Par exemple, si vous détectez un logiciel malveillant qui établit une connexion sortante avec un nœud de commande et de contrôle connu, fournissez les détails de l' EC2 instance dans`Resource.Details.AwsEc2Instance`. Fournissez les `ThreatIntelIndicator` objets et pertinents `Malware` pour cette EC2 instance. `Network`

### Malware

`Malware`est une liste qui accepte jusqu'à cinq ensembles d'informations sur les malwares. Faites en sorte que les entrées de malwares correspondent à la ressource et à la découverte.

Chaque entrée comporte les champs suivants.

**`Name`**

Le nom du logiciel malveillant. La valeur est une chaîne de 64 caractères maximum.

`Name`doit provenir d'une source approuvée de renseignements sur les menaces ou de chercheurs.

**`Path`**

Le chemin d'accès au logiciel malveillant. La valeur est une chaîne de 512 caractères maximum. `Path`doit être un chemin de fichier système Linux ou Windows, sauf dans les cas suivants.

- Si vous scannez des objets d'un compartiment S3 ou d'un partage EFS conformément aux règles YARA, le chemin de l'objet S3 ://ou HTTPS `Path` est alors indiqué.
- Si vous scannez des fichiers dans un dépôt Git, `Path` c'est l'URL Git ou le chemin du clone.

**`State`**

État du logiciel malveillant. Les valeurs autorisées sont `OBSERVED` | `REMOVAL_FAILED` |`REMOVED`.

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

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

Si `Malware.State` tel est le cas`OBSERVED`, le titre et la description de la recherche doivent indiquer que votre produit a détecté ce malware situé sur le chemin.

**`Type`**

Indique le type de logiciel malveillant. Les valeurs autorisées sont `ADWARE` `BLENDED_THREAT` `BOTNET_AGENT` `COIN_MINER` | `EXPLOIT_KIT` | `KEYLOGGER` | `MACRO` `POTENTIALLY_UNWANTED` | `SPYWARE` | `RANSOMWARE` `REMOTE_ACCESS` | `ROOTKIT` | `TROJAN` `VIRUS` | | `WORM`

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

## Network

`Network`est un objet unique. Vous ne pouvez pas ajouter plusieurs informations relatives au réseau. Lorsque vous mappez les champs, suivez les instructions suivantes.

Informations sur la destination et la source

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

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

- Pour une attaque DDo S sur une EC2 instance, la source est l'attaquant, bien qu'une véritable attaque DDo S puisse utiliser des millions d'hôtes. La destination est l' IPv4 adresse publique de l' EC2 instance. `Direction`est IN.
- Pour les programmes malveillants observés en train de communiquer entre une EC2 instance et un nœud de commande et de contrôle connu, la source est l' IPV4 adresse de l' EC2 instance. La destination est le nœud de commande et de contrôle. `Direction`est`0UT`. Vous fourniriez également `Malware` et`ThreatIntelIndicators`.

**`Protocol`**

`Protocol`correspond toujours à un nom enregistré par l'Internet Assigned Numbers Authority (IANA), sauf si vous pouvez fournir un protocole spécifique. Vous devez toujours l'utiliser et fournir les informations de port.

`Protocol`est indépendant des informations relatives à la source et à la destination. Ne le fournissez que lorsque cela a du sens.

**`Direction`**

`Direction`est toujours relatif aux limites du AWS réseau.

- `IN`signifie qu'il entre AWS (VPC, service).
- `0UT`signifie qu'il sort des limites du AWS réseau.

## Process

`Process`est un objet unique. Vous ne pouvez pas ajouter plusieurs détails relatifs au processus. Lorsque vous mappez les champs, suivez les instructions suivantes.

**`Name`**

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

**`Path`**

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

**`Pid`**, **`ParentPid`**

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

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

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

Si un client se fie à des horodatages pour une enquête médico-légale, il vaut mieux ne pas avoir d'horodatage qu'un mauvais horodatage.

## ThreatIntelIndicators

`ThreatIntelIndicators`accepte un ensemble de cinq objets de renseignement sur les menaces au maximum.

Pour chaque entrée, `Type` c'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` | `IPV6_ADDRESS` `MUTEX` | `PROCESS` | | `URL`

Voici quelques exemples de la façon de cartographier les indicateurs de renseignement sur les menaces :

- Vous avez trouvé un processus dont vous savez qu'il est associé à Cobalt Strike. Vous l'avez appris sur FireEye le blog de.

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

  Créez deux `ThreatIntelIndicator` objets. Un objet est pour le`DOMAIN`. L'autre est pour le`HASH_SHA1`.

- Vous avez trouvé un logiciel malveillant avec une règle de Yara (Loki, Fenrir, VirusScan Awss3,). BinaryAlert

  Créez deux `ThreatIntelIndicator` objets. L'un concerne le malware. L'autre est pour le`HASH_SHA1`.

## Resources

Pour cela`Resources`, utilisez les types de ressources et les champs de détail que nous avons fournis dans la mesure du 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 parvenez pas à ajuster les informations contenues dans les champs de détails pour un type de ressource modélisé, associez les autres détails à`Details.Other`.

Pour une ressource qui n'est pas modélisée dans ASFF, définissez sur`Type`. `Other` Pour obtenir des informations détaillées, utilisez`Details.Other`.

Vous pouvez également utiliser le type de `Other` ressource pour les AWS non-résultats.

## ProductFields

À utiliser uniquement `ProductFields` si vous ne pouvez pas utiliser un autre champ sélectionné `Resources` ou un objet descriptif tel que `ThreatIntelIndicatorsNetwork`, ou`Malware`.

Si vous en consommez`ProductFields`, vous devez fournir une justification stricte pour cette décision.

## Conformité d'

À utiliser uniquement `Compliance` si vos conclusions sont liées à la conformité.

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

Firewall Manager `Compliance` les utilise pour ses résultats, car ils sont liés à la conformité.

## Champs restreints

Ces champs sont destinés aux clients pour qu'ils puissent suivre leur enquête sur un résultat.

Ne mappez pas ces champs ou ces objets.

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

Pour ces champs, faites correspondre les champs présents dans l'`FindingProviderFields`objet. Ne mappez pas aux champs de niveau supérieur.

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

## Directives d'utilisation de l'**`BatchImportFindings`**API

Lorsque vous utilisez l'opération d'`BatchImportFindings`API pour envoyer des résultats AWS Security Hub CSPM, suivez les instructions suivantes.

- Vous devez appeler `BatchImportFindings`en utilisant le compte associé aux résultats. L'identifiant du compte associé est la valeur de l'`AwsAccountId`attribut pour la recherche.
- Envoyez le plus gros lot possible. Security Hub accepte jusqu'à 100 résultats par lot, jusqu'à 240 Ko par résultat et jusqu'à 6 Mo par lot.
- La limite de débit est de 10 TPS par compte et par région, avec une rafale de 30 TPS.
- Vous devez mettre en œuvre un mécanisme permettant de conserver l'état des résultats en cas de problème de régulation ou de réseau. Vous avez également besoin de l'état de constatation pour pouvoir soumettre des mises à jour au fur et à mesure qu'une constatation entre ou non en conformité.
- Pour plus d'informations sur la longueur maximale des chaînes et d'autres limitations, voir AWS Security Finding Format (ASFF) dans le guide de l'AWS Security Hub CSPM utilisateur.

# Liste de contrôle du niveau de préparation du produit

L'équipe AWS Security Hub CSPM et les équipes des partenaires APN utilisent cette liste de contrôle pour vérifier que l'intégration est prête à être lancée.

## Cartographie ASFF

Ces questions concernent le mappage de votre résultat au format ASFF ( AWS Security Finding Format).

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

- Mappez toutes vos découvertes à l'ASFF d'une manière ou d'une autre.
- Utilisez des champs sélectionnés tels que les types de ressources modélisés, `NetworkMalware`, ou. `ThreatIntelIndicators`
- Cartographiez tout autre élément dans `Resource.Details.Other` ou `ProductFields` comme il convient.

Le partenaire utilise-t-il **`Resource.Details`** des champs tels que **`AwsEc2instanceAwsS3Bucket`**, et **`Container`** ? Le partenaire définit-il les détails des ressources qui ne sont pas modélisés dans l'ASFF ? **`Resource.Details.Other`**

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

Le partenaire associe-t-il les valeurs à **`UserDefinedFields`** ?

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

Le partenaire mappe-t-il des informations **`ProductFields`** qui pourraient être mappées dans d'autres champs ASFF ?

- À utiliser uniquement `ProductFields` pour les informations spécifiques au produit, telles que les informations de version, les résultats de gravité spécifiques au produit ou d'autres informations qui ne peuvent pas être mappées dans un champ sélectionné ou. `Resources.Details.Other`

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

L'`FirstObservedAt`horodatage est destiné à enregistrer l'heure à laquelle une découverte a été observée dans le produit. Mappez ce champ dans la mesure du possible.

Le partenaire fournit-il des valeurs uniques générées pour chaque identifiant de recherche, à l'exception des résultats qu'il souhaite mettre à jour ?

Toutes les découvertes de Security Hub sont indexées sur l'identifiant de recherche (`Id`attribut). Cette valeur doit toujours être unique pour éviter que les résultats ne soient mis à jour accidentellement.

Vous devez également conserver l'état de l'identifiant de recherche afin 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`devrait être en mesure de lier logiquement les résultats à leur source.

Il peut s'agir d'un sous-composant d'un produit (produit A - Vulnerability 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 adaptée à son produit ? Le partenaire utilise-t-il les catégories de types de recherche ou les classificateurs recommandés dans ses types de recherche ?

La taxonomie des types de résultats doit correspondre étroitement aux résultats générés par le produit.

Les espaces de noms de premier niveau décrits dans le format de recherche AWS de sécurité sont obligatoires.

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

Le partenaire saisit-il des informations sur le flux réseau sur **`Network`** le terrain, s'il possède des données réseau ?

Si votre produit capture NetFlow des informations, associez-les au `Network` champ.

Le partenaire saisit-il les informations de processus (PID) dans les **`Process`** champs, s'il possède des données de processus ?

Si votre produit capture des informations sur le processus, associez-les au `Process` champ.

Le partenaire collecte-t-il des informations sur les malwares sur le **`Malware`** terrain, s'il possède des données sur les malwares ?

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

Le partenaire saisit-il des informations sur les menaces sur le terrain**`ThreatIntelIndicators`**, s'il possède des données de renseignement sur les menaces ?

Si votre produit capture des informations sur les menaces, associez-les au `ThreatIntelIndicators` terrain.

Le partenaire fournit-il une note de confiance pour les résultats ? Dans l'affirmative, 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 identifiant canonique ou un ARN comme identifiant de ressource dans la recherche ?

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

## Configuration et fonctionnement de l'intégration

Ces questions concernent la configuration et le day-to-day fonctionnement de l'intégration.

Le partenaire fournit-il un modèle infrastructure-as-code (iAc) pour déployer l'intégration avec Security Hub, tel que Terraform CloudFormation, ou ? AWS Cloud Development Kit (AWS CDK)

Pour les intégrations qui enverront des résultats depuis le compte client ou utiliseront CloudWatch des événements pour utiliser les résultats, une forme de modèle IaC est requise.

CloudFormation est préférable, mais AWS CDK Terraform peut également être utilisé.

Le produit partenaire est-il configuré 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 impliquer le provisionnement automatique des ressources et des autorisations. Si vous envoyez des résultats depuis un compte produit, la configuration en un clic est la méthode préférée.

Le partenaire envoie-t-il uniquement des résultats intéressants ?

Vous ne devez généralement envoyer que les résultats présentant une valeur de sécurité 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 par client et à quelle fréquence (moyenne et rafale) ?

Le nombre de résultats uniques est utilisé pour calculer la charge sur Security Hub. Un résultat unique est défini comme un résultat dont le mappage ASFF est différent de celui d'un autre résultat.

Par exemple, si un résultat est renseigné uniquement `ThreatIntelIndicators` et un autre uniquement renseigné`Resources.Details.AWSEc2Instance`, il s'agit de deux résultats uniques.

Le partenaire parvient-il à gérer les erreurs 4xx et 5xx de manière à ce qu'elles ne soient pas limitées et que tous les résultats puissent être envoyés ultérieurement ?

Il existe actuellement un taux de rafale de 30 à 50 TPS pour le fonctionnement de l'`BatchImportFindings`API. Si des erreurs 4xx ou 5xx sont renvoyées, vous devez conserver l'état de ces résultats infructueux afin de pouvoir les réessayer dans leur intégralité ultérieurement. Vous pouvez le faire par le biais d'une file d'attente de lettres mortes ou d'autres services de AWS messagerie tels qu'Amazon SNS ou Amazon SQS.

Le partenaire maintient-il l'état de ses résultats de manière à pouvoir archiver les résultats qui ne sont plus présents ?

Si vous prévoyez de mettre à jour les résultats en remplaçant l'identifiant 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 le résultat correct.

Si vous fournissez des résultats, n'utilisez pas l'`BatchUpdateFindings`opération pour mettre à jour les résultats. Cette opération ne doit être utilisée que par les clients. Vous ne l'utilisez que `BatchUpdateFindings`lorsque vous enquêtez et que vous prenez des mesures en fonction des résultats.

Le partenaire gère-t-il les nouvelles tentatives de manière à ne pas compromettre les résultats positifs déjà envoyés ?

Vous devez disposer d'un mécanisme permettant de conserver le résultat initial IDs en cas d'erreur afin de ne pas dupliquer ou remplacer par erreur les résultats positifs.

Le partenaire met-il à jour ses résultats en appelant l'**`BatchImportFindings`**opération avec le numéro de recherche des résultats existants ?

Pour mettre à jour un résultat, vous devez remplacer le résultat existant en soumettant le même numéro de résultat.

L'`BatchUpdateFindings`opération ne doit être utilisée que par les clients.

Le partenaire met-il à jour ses résultats à l'aide de l'**`BatchUpdateFindings`**API ?

Si vous agissez sur la base des résultats, vous pouvez utiliser cette `BatchUpdateFindings`opération pour mettre à jour des champs spécifiques.

Le partenaire fournit-il des informations sur le temps de latence entre le moment où un résultat est créé et le moment où il est envoyé de son produit à Security Hub ?

Vous devez minimiser le temps de latence pour que les clients puissent consulter les résultats le plus rapidement possible dans Security Hub.

Ces informations sont obligatoires dans le manifeste.

Si l'architecture du partenaire consiste à envoyer les résultats à Security Hub à partir d'un compte client, l'a-t-il démontré avec succès ? Si l'architecture du partenaire consiste à envoyer les 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 et qui est différent du compte fourni pour l'ARN du produit.

L'envoi d'une recherche depuis le compte du propriétaire de l'ARN du produit permet de contourner certaines exceptions d'erreur liées aux opérations de l'API.

Le partenaire communique-t-il une information sur le rythme cardiaque à Security Hub ?

Pour montrer que votre intégration fonctionne correctement, vous devez envoyer un résultat de pulsation. Le résultat du rythme cardiaque est envoyé toutes les cinq minutes et utilise le type `Heartbeat` de recherche.

C'est important si vous envoyez des résultats depuis un compte produit.

Le partenaire a-t-il intégré le compte de l'équipe produit de Security Hub lors des tests ?

Lors de la validation de préproduction, vous devez envoyer des exemples de recherche sur le AWS compte de l'équipe produit de Security Hub. Ces exemples montrent que les résultats sont envoyés et mappés correctement.

## Documentation

Ces questions sont liées à 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 Read the Docs ou d'un autre format dédié.

La documentation d'hébergement GitHub ne répond pas aux exigences d'un site Web dédié.

La documentation destinée aux partenaires fournit-elle des instructions sur la façon de configurer l'intégration de 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 fournit-elle une description de son cas d'utilisation ?

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

La documentation du partenaire justifie-t-elle les conclusions qu'il envoie ?

Vous devez justifier les types de résultats que vous envoyez.

Par exemple, votre produit peut détecter des vulnérabilités, des logiciels malveillants et des antivirus, mais vous envoyez uniquement les résultats de vulnérabilité et de programme malveillant à Security Hub. Dans ce cas, vous devez expliquer pourquoi vous n'envoyez pas les résultats de l'antivirus.

La documentation du partenaire fournit-elle une justification de la manière dont le partenaire associe ses résultats à l'ASFF ?

Vous devez justifier le mappage de la découverte native d'un produit avec ASFF. Les clients veulent savoir où trouver des informations spécifiques sur les produits.

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

Fournissez aux clients des informations sur la manière dont vous maintenez l'état, garantissez l'idempuissance et remplacez les résultats par des informations. up-to-date

La documentation destinée aux partenaires décrive-t-elle la recherche de la latence ?

Minimisez le temps de latence pour que les clients puissent consulter les résultats le plus rapidement possible dans Security Hub.

Ces informations sont obligatoires dans le manifeste.

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

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

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

La documentation destinée aux partenaires justifie-t-elle les cotes de confiance ?

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

Si vous utilisez des scores de confiance remplis de manière statique ou des mappages issus 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 soutient et ne soutient pas ?

Notez les régions prises en charge ou non afin que les clients sachent dans quelles régions ne pas tenter d'intégration.

## Informations sur la fiche produit

Ces questions concernent la fiche du produit affichée sur la page Intégrations de la console Security Hub.

L'identifiant de AWS compte fourni est-il valide et contient-il 12 chiffres ?

Les identifiants de compte sont composés de 12 chiffres. Si un identifiant 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 fichier JSON du manifeste ne doit pas comporter plus de 200 caractères, espaces compris.

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

Le lien de configuration doit mener à votre documentation en ligne. Cela ne doit pas mener à votre site Web principal ou à des pages marketing.

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

Si vous fournissez un lien d'achat, il doit s'agir d'une AWS Marketplace entrée. Security Hub n'accepte pas les liens d'achat qui ne sont pas hébergés par AWS.

Les catégories de produits décrivent-elles correctement le produit ?

Dans le manifeste, vous pouvez indiquer 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 du produit 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 indiqué dans le fichier JSON de la fiche produit doit correspondre au nom indiqué dans le manifeste.

## Informations commerciales

Ces questions sont liées au marketing pour l'intégration.

La description du produit pour la page des partenaires du Security Hub comporte-t-elle un maximum de 700 caractères, espaces compris ?

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

L'équipe modifiera les descriptions plus longues.

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

Fournissez une URL accessible au public avec le logo de l'entreprise au format PNG ou JPG dont la taille ne dépasse pas 600 x 300 pixels.

L'hyperlien « En savoir plus » sur la page des partenaires du Security Hub mène-t-il à la page Web dédiée du partenaire à propos de l'intégration ?

Le lien En savoir plus ne doit pas mener au site Web principal du partenaire ni aux informations de documentation.

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

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

Une vidéo de démonstration ou de présentation de l'intégration est facultative mais recommandée.

Un article de blog du AWS Partner Network est-il publié avec le partenaire et son responsable du développement des partenaires ou son représentant du développement des partenaires ?

AWS Les articles de blog du réseau de partenaires doivent être coordonnés à l'avance avec le responsable du développement des partenaires ou le représentant du développement des partenaires.

Ils sont distincts 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 les tests avec l'ARN du produit privé terminés.

Un communiqué de presse dirigé par un partenaire sera-t-il publié ?

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

Un article de blog publié par un partenaire est-il en cours de publication ?

Vous pouvez créer vos propres articles de blog pour présenter l'intégration en dehors du blog AWS Partner Network.

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

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

Si vous avez besoin de l'aide de l'équipe Security Hub, contactez l'équipe produit après avoir terminé les tests avec l'ARN privé du produit.

Le partenaire a-t-il demandé une assistance sur les réseaux sociaux AWS ?

Après votre libération, vous pourrez travailler avec le responsable marketing AWS de la sécurité pour utiliser les réseaux sociaux AWS officiels afin de partager des informations sur vos webinaires.

# AWS Security Hub CSPM FAQ pour les partenaires

Vous trouverez ci-dessous les questions les plus fréquemment posées sur la configuration et la maintenance d'une intégration avec AWS Security Hub CSPM.

1. Quels sont les avantages de l'intégration de Security Hub ?
   - Satisfaction du client — La principale raison d'intégrer Security Hub est que les clients vous demandent de le faire.

     Security Hub est le centre de sécurité et de conformité pour les AWS clients. Il est conçu comme la première étape où les professionnels AWS de la sécurité et de la conformité se rendent chaque jour pour comprendre leur état de sécurité et de conformité.

     Écoutez vos clients. Ils vous diront s'ils souhaitent voir vos résultats dans Security Hub.
   - Opportunités de découverte — Nous promouvons les partenaires dotés d'intégrations certifiées dans la console Security Hub, notamment des liens vers leurs AWS Marketplace listes. C'est un excellent moyen pour les clients de découvrir de nouveaux produits de sécurité.
   - Opportunités de marketing — Les fournisseurs dont les intégrations sont approuvées peuvent participer à des webinaires, publier des communiqués de presse, créer des fiches techniques et présenter leurs intégrations aux clients. AWS
2. Quels sont les types de partenaires ?
   - Partenaires qui envoient leurs résultats à Security Hub
   - Partenaire recevant les résultats de Security Hub
   - Des partenaires qui envoient et reçoivent des résultats
   - Des partenaires consultants qui aident les clients à configurer, personnaliser et utiliser Security Hub dans leur environnement
3. Comment fonctionne l'intégration d'un partenaire à Security Hub à un niveau élevé ?

   Vous collectez les résultats depuis un compte client ou depuis votre propre AWS compte et vous transformez le format des résultats en format ASFF ( AWS Security Finding Format). Vous transmettez ensuite ces résultats au point de terminaison régional Security Hub approprié.

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

a. Soumettez les informations du manifeste de votre partenaire.

b. Recevez le produit ARNs à utiliser avec Security Hub, si vous souhaitez envoyer des résultats à Security Hub.

c. Mappez vos résultats à l'ASFF. Consultez the section called “Directives pour le mappage ASFF”.

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

e. Créez un cadre de déploiement pour les clients. Par exemple, les CloudFormation scripts peuvent servir à cette fin.

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. Soumettez les informations marketing pour approbation (langue du site Web, communiqué de presse, diapositive d'architecture, vidéo, feuille de synthèse).

5. Quelle est la procédure à suivre pour soumettre le manifeste du partenaire ? Et pour que les AWS services envoient leurs résultats à Security Hub ?

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

   Vous recevez le produit ARNs dans un délai de sept jours calendaires.

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

   La tarification de 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 aucune valeur ajoutée aux clients.

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

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

   Voici les principales approches :

- Vous envoyez les résultats depuis leur propre AWS compte désigné en utilisant l'`BatchImportFindings`opération.
- Vous envoyez les résultats depuis le compte client à l'aide de l'`BatchImportFindings`opération. Vous pouvez utiliser des approches assumant des rôles, mais ces approches ne sont pas obligatoires.

Pour les directives générales d'utilisation `BatchImportFindings`, voirthe section called "Directives d'utilisation de l'`BatchImportFindings`API".

8. Comment puis-je recueillir mes résultats et les transmettre à un point de terminaison régional du 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 sous forme de CloudFormation script. Le script rassemble les conclusions du partenaire dans l'environnement du client, les transforme en ASFF et les envoie au point de terminaison régional du Security Hub.

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

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

   Security Hub prend en charge l'autorisation par lots partielle pour le fonctionnement de l'`BatchImportFindings`API, afin que vous puissiez envoyer toutes vos conclusions 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 ingère uniquement les résultats autorisés contenus dans le lot.

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

    a. Assurez-vous que les politiques IAM appropriées sont en place.

    b. Activez un abonnement au produit (politiques de ressources) pour les comptes. Utilisez l'opération `EnableImportFindingsForProduct`API ou la page Intégrations. Le client peut le faire, ou vous pouvez utiliser des rôles multicomptes pour agir en son nom.

    c. Assurez-vous que le résultat est `ProductArn` l'ARN public de votre produit.

    d. Assurez-vous que le `AwsAccountId` résultat est le numéro de compte du client.

e. Assurez-vous que vos résultats ne contiennent aucune donnée mal formée conformément au format ASFF ( AWS Security Finding Format). Par exemple, les champs obligatoires sont renseignés et aucune valeur n'est incorrecte.

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

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

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

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

Les ressources d'un même compte peuvent être configurées avec des politiques IAM sans nécessiter de politiques de ressources.

Pour exclure tout problème de politique IAM de la part de l'appelant `BatchImportFindings`, définissez la politique IAM pour l'appelant comme suit :

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

Assurez-vous de vérifier qu'il n'existe aucune `Deny` politique pour l'appelant. Une fois que vous l'avez fait fonctionner avec cela, vous pouvez limiter la politique 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 à un produit ?

    Pour recevoir les résultats d'un produit partenaire spécifique, le client (ou le partenaire ayant des rôles multicomptes travaillant pour le compte du client) doit souscrire un abonnement au produit. Pour ce faire depuis la console, ils utilisent la page Intégrations. Pour ce faire à partir de l'API, ils utilisent l'opération `EnableImportFindingsForProduct`API.

    L'abonnement au produit crée une politique de ressources qui autorise le client à recevoir ou à envoyer les résultats du partenaire. Pour plus de détails, consultez Cas d'utilisation et autorisations.

    Security Hub applique les types de politiques 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 un ou les deux types de politiques.

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

    Avec`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, vous ne pouvez envoyer les résultats qu'à partir du compte client auquel vous êtes abonné.

13. Supposons qu'un client ait créé un compte administrateur et ajouté quelques comptes de membre. 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 relatifs aux 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 souscrire un abonnement à un produit pour chaque compte. Ils peuvent le faire par programmation via l'API.

14. Quel est l'ARN de mon produit ?

    L'ARN de votre produit est l'identifiant unique que Security Hub génère pour vous et que vous utilisez pour soumettre des résultats. Vous recevez un ARN de produit pour chaque produit que vous intégrez à Security Hub. Le bon ARN du produit doit figurer dans chaque résultat que vous

envoyez à Security Hub. Les résultats sans l'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 de produit vous est attribué pour chaque région dans laquelle Security Hub est déployé. L'identifiant du compte, la société et les noms des produits sont dictés par les manifestes soumis par vos partenaires. Vous ne modifiez jamais les 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 des résultats.

Une erreur courante consiste à modifier l'identifiant du compte pour qu'il corresponde au compte sur lequel vous travaillez actuellement. L'identifiant du compte ne change pas. Vous soumettez un identifiant de compte « personnel » dans le cadre de la soumission du manifeste. Cet identifiant 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 votre produit ARNs pour ces régions.

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

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

Les résultats doivent être fournis au format ASFF ( AWS Security Finding Format). Pour plus de détails, voir AWS Security Finding Format (ASFF) dans le guide de l'AWS Security Hub CSPM utilisateur.

On s'attend à ce que toutes les informations contenues dans vos résultats natifs soient pleinement reflétées dans l'ASFF. Des champs personnalisés tels que `ProductFields` et vous `Resource.Details.Other` permettent de mapper des données qui ne rentrent 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 du Security Hub associé au compte client.

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

    Consultez la liste des points de terminaison du Security Hub.

18. Puis-je soumettre des résultats interrégionaux ?

    Security Hub ne prend pas encore en charge la soumission interrégionale des résultats pour les AWS services natifs, 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 de 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, elle `ProductArn` doit correspondre à la région du point de terminaison.

19. Quelles sont les règles et directives relatives 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 limite du modèle d'autorisation de base d'API Gateway.

    Consultez the section called “Directives d'utilisation de l'`BatchImportFindings`API”.

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

    Oui, si vous soumettez un résultat avec le même ARN de produit et le même ID de recherche, les données précédentes correspondant à ce résultat seront remplacées. Notez que toutes les données sont remplacées. Vous devez donc soumettre un résultat complet.

    Les clients sont mesurés et facturés à la fois pour les nouvelles découvertes et les mises à jour.

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

    Oui, si le client vous donne accès à l'opération `BatchUpdateFindings`API, vous pouvez mettre à jour certains champs à l'aide de cette opération. Cette opération est conçue pour être utilisée

par les clients SIEMs, les systèmes de billetterie et les plateformes SOAR (Security Orchestration, Automation, and Response).

22. Comment vieillissent les résultats ?

    Security Hub vieillit les résultats 90 jours après la date de dernière mise à jour. Passé ce délai, les résultats périmés sont supprimés du cluster Security Hub. OpenSearch

    Si vous mettez à jour un résultat avec le même ID de recherche et qu'il est périmé, un nouveau résultat est créé dans Security Hub.

    Les clients peuvent utiliser CloudWatch les événements pour transférer les résultats hors de Security Hub. Cela permet d'envoyer tous les résultats aux cibles choisies par le client.

    En général, Security Hub vous recommande de créer de nouvelles découvertes tous les 90 jours et de ne pas les mettre à jour indéfiniment.

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

    Security Hub limite les appels d'`GetFindings`API, car l'approche recommandée pour les résultats d'accès consiste à utiliser CloudWatch les événements.

    Security Hub n'implémente aucune autre restriction sur les services internes, les partenaires ou les clients que celle imposée par les invocations API Gateway et Lambda.

24. Quels sont les délais, le temps de latence SLAs ou les attentes en ce qui concerne les résultats envoyés à Security Hub par les services sources ?

    L'objectif est d'être aussi proche que possible du temps réel pour les premiers résultats 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, appliquez l'une des méthodes suivantes.

    - Tous les résultats sont automatiquement envoyés à CloudWatch Events. Un client peut créer des règles d' CloudWatch événements spécifiques pour envoyer les résultats à des cibles spécifiques, telles qu'un SIEM ou un compartiment S3. Cette fonctionnalité a remplacé l'ancienne opération `GetFindings` d'API.
    - Utilisez CloudWatch les événements pour des actions personnalisées. Security Hub permet aux clients de sélectionner des résultats spécifiques ou des groupes de résultats dans la console et de prendre des mesures en conséquence. Par exemple, ils peuvent envoyer leurs résultats

à un SIEM, à un système de billetterie, à une plateforme de chat ou à un flux de travail de correction. Cela ferait partie d'un flux de travail de triage des alertes effectué par un client au sein de Security Hub. C'est ce que l'on appelle des actions personnalisées.

Lorsqu'un utilisateur sélectionne une action personnalisée, un CloudWatch événement est créé pour ces résultats spécifiques. Vous pouvez tirer parti de cette fonctionnalité et créer CloudWatch des règles et des cibles relatives aux événements à utiliser par un client 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 en particulier à CloudWatch Events. Il appartient à l'utilisateur d'agir sur la base de résultats spécifiques.

Vous pouvez utiliser les opérations de l'API d'actions personnalisées, par exemple pour créer automatiquement des actions disponibles pour votre produit (par exemple en utilisant CloudFormation des modèles). `CreateActionTarget` Vous devez également utiliser CloudWatch les opérations de l'API des règles d' CloudWatch événements pour créer les règles d'événements correspondantes associées à l'action personnalisée. À l'aide de CloudFormation modèles, vous pouvez également créer CloudWatch des règles relatives aux événements afin d'ingérer automatiquement depuis 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 gérés (MSSP) devienne un partenaire du 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 des résultats à Security Hub.

    Si le MSSP reçoit uniquement les résultats de Security Hub, il doit au minimum disposer d'un CloudFormation modèle pour configurer les règles d' CloudWatch événements appropriées.

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 du Security Hub. Vous devez soumettre deux études de cas privées sur la façon dont vous avez aidé un client spécifique à effectuer les tâches suivantes.

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

- Aidez à connecter des solutions de fournisseurs de logiciels indépendants (ISV) déjà intégrées à Security Hub à l'aide des instructions de configuration figurant sur la page partenaire de la console.
- Aidez les clients à intégrer des produits personnalisés.
- Créez des informations personnalisées adaptées aux besoins et aux ensembles de données des clients.
- Créez des actions personnalisées.
- Élaborez des manuels de remédiation.
- Créez des Quickstarts conformes aux normes de conformité du Security Hub. Ils doivent être validés par l'équipe du Security Hub.

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

28. Quelles sont les exigences relatives à la manière dont je déploie mon intégration avec Security Hub auprès de mes clients ?

    Les architectures d'intégration entre Security Hub et les produits partenaires varient d'un partenaire à l'autre en termes de gestion 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 l' AWS environnement du client, vous devez utiliser CloudFormation des modèles pour simplifier l'intégration. Certains partenaires ont créé une intégration en un clic, ce qui est vivement recommandé.

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 des CloudFormation modèles.

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

    Envisagez d'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 soutenez et que vous ne soutenez pas
- Latence entre le moment où les résultats sont créés et leur envoi 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 le client à hiérarchiser les résultats et les ressources qui nécessitent le plus d'attention et d'action.

    Security Hub fonctionne `CreateInsight` via une API. Vous pouvez créer des informations personnalisées dans un compte client dans le cadre de votre CloudFormation modèle. 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 ne pouvez créer que des informations gérées.

32. Quel est votre modèle de tarification ?

    Consultez les informations tarifaires du Security Hub.

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

    Envoyez les résultats au compte de démonstration Security Hub à l'aide de l'ARN du produit que vous avez fourni, en utilisant `us-west-2` comme région. Les résultats devraient 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 le cadre de démos.

34. Quels sont les messages d'erreur ou de réussite **`BatchImportFindings`** fournis ?

    Security Hub fournit une réponse pour l'autorisation et une réponse pour `BatchImportFindings`. Des messages de réussite, d'échec et d'erreur plus précis 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 ralentissements et les alarmes. Ils doivent également gérer les commentaires ou les messages d'erreur envoyés via le mécanisme de feedback du Security Hub.

36. Quelles sont les solutions aux problèmes courants ?

Un `AuthorizerConfigurationException` est causé soit par une malformation, `AwsAccountId` soit `ProductArn` par.

Lors du dépannage, tenez compte des points suivants :

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

  L'identifiant du compte ne change pas par rapport à celui que l'équipe Security Hub a inclus dans le produit ARNs qu'elle vous a fourni.

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

Assurez-vous que le compte client et le compte produit que vous utilisez sont bien les comptes enregistrés. Certains partenaires ont utilisé un numéro de compte pour le produit issu de l'ARN du produit, mais ils essaient d'utiliser un compte totalement 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 résultats.

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

`<securityhub-partners@amazon.com>`

38. À quelle région dois-je envoyer les résultats pour les articles liés aux AWS services mondiaux ? Par exemple, où dois-je envoyer les résultats relatifs à l'IAM ?

Envoyez les résultats à la même région où ils ont été détectés. Pour un service tel que IAM, votre solution rencontrera probablement le même problème IAM dans plusieurs régions. Dans ce cas, le résultat est envoyé à chaque région où le problème a été détecté.

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

Lorsqu'un problème est résolu, envoyez la mise à jour du résultat à toutes les régions où vous avez envoyé le résultat initial.

# Historique du document pour le guide d'intégration des partenaires

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

| Modification | Description | Date |
| --- | --- | --- |
| Exigences mises à jour pour le logo de console | Les directives relatives au manifeste et au logo des partenaires ont été mises à jour pour 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 conditions préalables pour les nouveaux partenaires d'intégration | Security Hub autorise désormais également les partenaires qui ont rejoint le parcours des partenaires AWS ISV et qui utilisent un produit d'intégration ayant fait l'objet d'un examen technique de AWS base (FTR). Auparavant, tous les partenaires d'intégration devaient être des partenaires de niveau AWS sélectionné. | 29 avril 2021 |
| Nouvel `FindingProviderFields` objet dans ASFF | Mise à jour des informations sur la cartographie des résultats auprès de l'ASFF. Pour`Confidenc` | 18 mars 2021 |

| | | |
|---|---|---|
| | `e` ,`Criticali ty` , `RelatedFi ndings` `Severity`, etTypes, les partenaires associent leurs valeurs aux champs de`FindingProviderFie lds` . | |
| 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 découvertes existantes dans Security Hub. | 4 décembre 2020 |
| Publication initiale de ce guide | Ce guide d'intégration des AWS partenaires fournit aux partenaires des informations sur la manière d'établir une intégration avec AWS Security Hub CSPM. | 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.