Leitfaden zur Partnerintegration

AWS Security Hub

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

AWS Security Hub: Leitfaden zur Partnerintegration

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Überblick über die Integration von Drittanbietern mit AWS Security Hub ... 1
Warum integrieren? ... 1
Vorbereitung der Zusendung der Ergebnisse ... 2
Vorbereitung auf den Erhalt von Erkenntnissen ... 3
Informationsressourcen zum Security Hub ... 4
Voraussetzungen für Partner ... 5
Anwendungsfälle und Berechtigungen ... 6
Vom Partner gehostet: Die Ergebnisse wurden vom Partnerkonto gesendet ... 6
Vom Partner gehostet: Die Ergebnisse wurden über das Kundenkonto gesendet ... 7
Vom Kunden gehostet: Die Ergebnisse wurden über das Kundenkonto gesendet ... 9
Onboarding-Prozess für Partner ... 11
Go-to-market Aktivitäten ... 14
Eintrag auf der Security Hub-Partnerseite ... 14
Pressemitteilung ... 14
AWS Blog zum Partnernetzwerk (APN) ... 15
Die wichtigsten Dinge, die Sie über den APN-Blog wissen sollten ... 15
Warum sollten Sie für den APN-Blog schreiben? ... 16
Welche Art von Inhalt ist am besten geeignet? ... 16
Slick Sheet oder Marketing-Blatt ... 16
Whitepaper oder E-Book ... 17
Webinar ... 17
Demo-Video ... 17
Manifest zur Produktintegration ... 18
Anwendungsfall und Marketinginformationen ... 19
Anwendungsfall für die Suche nach Anbietern und Verbrauchern ... 19
Anwendungsfall Consulting Partner (CP) ... 20
Datensätze ... 20
Architektur ... 20
Konfiguration ... 21
Durchschnittliche Ergebnisse pro Tag und Kunde ... 21
Latency ... 21
Unternehmens- und Produktbeschreibung ... 22
Ressourcen der Partner-Website ... 22
Logo für die Partnerseite ... 22

Logos für die Security Hub Hub-Konsole ... 23
Erkenntnistypen ... 23
Hotline ... 23
Erkennung von Herzschlägen ... 24
Informationen Security Hub Hub-Konsole ... 24
Informationen zum Unternehmen ... 24
Produktinformationen ... 25
Richtlinien und Checklisten ... 36
Richtlinien für das Konsolenlogo ... 36
Grundsätze für die Erstellung und Aktualisierung von Ergebnissen ... 39
Richtlinien für die ASFF-Zuordnung ... 40
Identifizierende Informationen ... 40
Title and Description ... 41
Erkenntnistypen ... 41
Zeitstempel ... 41
Severity ... 42
Remediation ... 43
SourceUrl ... 43
Malware, Network, Process, ThreatIntelIndicators ... 43
Resources ... 47
ProductFields ... 47
Compliance ... 47
Eingeschränkte Felder ... 48
Richtlinien für die Verwendung der `BatchImportFindings` API ... 48
Checkliste zur Eignung des Produkts ... 49
ASFF-Zuordnung ... 49
Einrichtung und Funktion der Integration ... 51
Dokumentation ... 54
Informationen zur Produktkarte ... 56
Informationen zu Marketingzwecken ... 56
Häufig gestellte Fragen für Partner ... 59
Dokumentverlauf ... 72
... lxxiv

Überblick über die Integration von Drittanbietern mit AWS Security Hub

Dieser Leitfaden richtet sich an AWS Partner Network (APN) -Partner, die eine Integration mit einrichten möchten. AWS Security Hub

Als APN-Partner können Sie Security Hub auf eine oder mehrere der folgenden Arten integrieren.

- Ergebnisse an Security Hub senden
- Erkenntnisse aus Security Hub nutzen
- Beide senden Ergebnisse an Security Hub und verarbeiten Ergebnisse von Security Hub
- Verwenden Sie Security Hub als Mittelpunkt eines Managed Security Service Providers (MSSP) -Angebots
- Beraten Sie sich mit AWS Kunden über die Bereitstellung und Verwendung von Security Hub

Dieser Onboarding-Leitfaden konzentriert sich in erster Linie auf Partner, die Ergebnisse an Security Hub senden.

Themen

- Warum sollten Sie mit AWS Security Hub integrieren?
- Wir bereiten den Versand der Ergebnisse vor an AWS Security Hub
- Wir bereiten uns auf den Erhalt von Ergebnissen vor AWS Security Hub
- Ressourcen zum Erlernen von AWS Security Hub

Warum sollten Sie mit AWS Security Hub integrieren?

AWS Security Hub bietet einen umfassenden Überblick über Sicherheitswarnungen mit hoher Priorität und den Sicherheitsstatus aller Security Hub Hub-Konten. Security Hub ermöglicht es Partnern wie Ihnen, Sicherheitsergebnisse an Security Hub zu senden, um Ihren Kunden Einblick in die von Ihnen generierten Sicherheitserkenntnisse zu geben.

Eine Integration mit Security Hub kann auf folgende Weise einen Mehrwert bieten.

- Stellt Ihre Kunden zufrieden, die eine Security Hub Hub-Integration angefordert haben

- Bietet Ihren Kunden einen zentralen Überblick über ihre AWS sicherheitsrelevanten Ergebnisse
- Ermöglicht neuen Kunden, Ihre Lösung zu entdecken, wenn sie nach Partnern suchen, die Ergebnisse zu bestimmten Arten von Sicherheitsvorfällen bereitstellen

Bevor Sie eine Integration mit Security Hub erstellen, sollten Sie Ihre Gründe für die Integration untersuchen. Eine Integration ist mit größerer Wahrscheinlichkeit erfolgreich, wenn Ihre Kunden eine Security Hub Hub-Integration mit Ihrem Produkt wünschen. Sie können eine Integration ausschließlich aus Marketinggründen oder zur Gewinnung neuer Kunden erstellen. Wenn Sie die Integration jedoch ohne aktuelle Kundeneingaben erstellen und die Bedürfnisse Ihrer Kunden nicht berücksichtigen, führt die Integration möglicherweise nicht zu den erwarteten Ergebnissen.

Wir bereiten den Versand der Ergebnisse vor an AWS Security Hub

Als APN-Partner können Sie erst dann Informationen für Ihre Kunden an Security Hub senden, wenn das Security Hub Hub-Team Sie als Suchdienstleister aktiviert. Um als Suchdienstleister aktiviert zu werden, müssen Sie die folgenden Onboarding-Schritte ausführen. Auf diese Weise wird ein positives Security Hub Hub-Erlebnis für Sie und Ihre Kunden gewährleistet.

Beachten Sie beim Abschluss der Onboarding-Schritte unbedingt die Richtlinien unter the section called “Grundsätze für die Erstellung und Aktualisierung von Ergebnissen”the section called “Richtlinien für die ASFF-Zuordnung”, undthe section called “Richtlinien für die Verwendung der `BatchImportFindings` API”.

1. Ordnen Sie Ihre Sicherheitsergebnisse dem AWS Security Finding Format (ASFF) zu.
2. Erstellen Sie Ihre Integrationsarchitektur, um die Ergebnisse an den richtigen Regional Security Hub-Endpunkt weiterzuleiten. Zu diesem Zweck legen Sie fest, ob Sie Ergebnisse von Ihrem eigenen AWS Konto oder von den Konten Ihrer Kunden aus senden.
3. Bitten Sie Ihre Kunden, das Produkt über ihr Konto zu abonnieren. Dazu können sie die Konsole oder die `EnableImportFindingsForProduct`API-Operation verwenden. Weitere Informationen finden Sie im AWS Security Hub Benutzerhandbuch unter Verwaltung von Produktintegrationen.

   Sie können das Produkt auch für sie abonnieren. Zu diesem Zweck verwenden Sie eine kontoübergreifende Rolle, um im Namen des Kunden auf den `EnableImportFindingsForProduct`API-Vorgang zuzugreifen.

   In diesem Schritt werden die Ressourcenrichtlinien festgelegt, die erforderlich sind, um die Ergebnisse dieses Produkts für dieses Konto zu akzeptieren.

In den folgenden Blogbeiträgen werden einige der bestehenden Partnerintegrationen mit Security Hub erörtert.

- Ankündigung der Cloud Custodian-Integration mit AWS Security Hub
- Verwenden Sie AWS Fargate und Prowler, um Ergebnisse der Sicherheitskonfiguration zu AWS Diensten an Security Hub zu senden
- So importieren Sie AWS Config Regelauswertungen als Ergebnisse in Security Hub

Wir bereiten uns auf den Erhalt von Ergebnissen vor AWS Security Hub

Verwenden Sie eine der folgenden Optionen AWS Security Hub, um Ergebnisse von zu erhalten:

- Sorgen Sie dafür, dass Ihre Kunden alle Ergebnisse automatisch an CloudWatch Events senden. Ein Kunde kann spezifische CloudWatch Ereignisregeln erstellen, um Ergebnisse an bestimmte Ziele zu senden, z. B. an ein SIEM oder einen S3-Bucket.
- Lassen Sie Ihre Kunden bestimmte Ergebnisse oder Gruppen von Ergebnissen in der Security Hub Hub-Konsole auswählen und dann entsprechende Maßnahmen ergreifen.

Ihre Kunden können die Ergebnisse beispielsweise an ein SIEM, ein Ticketsystem, eine Chat-Plattform oder einen Korrektur-Workflow senden. Dies wäre Teil eines Alert-Triage-Workflows, den ein Kunde innerhalb von Security Hub durchführt.

Diese Aktionen werden als benutzerdefinierte Aktionen bezeichnet. Wenn ein Benutzer eine benutzerdefinierte Aktion ausführt, wird ein CloudWatch Ereignis für diese spezifischen Ergebnisse erstellt. Als Partner können Sie diese Funktion nutzen und CloudWatch Ereignisregeln oder -ziele erstellen, die ein Kunde als Teil einer benutzerdefinierten Aktion verwenden kann. Beachten Sie, dass diese Funktion nicht automatisch alle Ergebnisse eines bestimmten Typs oder einer bestimmten Klasse an CloudWatch Events sendet. Diese Funktion ermöglicht es einem Benutzer, aufgrund bestimmter Ergebnisse Maßnahmen zu ergreifen.

In den folgenden Blogbeiträgen werden Lösungen beschrieben, die die Integration mit Security Hub und CloudWatch Events für benutzerdefinierte Aktionen verwenden.

- So integrieren Sie AWS Security Hub benutzerdefinierte Aktionen mit PagerDuty
- So aktivieren Sie benutzerdefinierte Aktionen in AWS Security Hub

- So importieren Sie AWS Config Regelauswertungen als Ergebnisse in Security Hub

Ressourcen zum Erlernen von AWS Security Hub

Die folgenden Materialien können Ihnen helfen, die AWS Security Hub Lösung besser zu verstehen und zu erfahren, wie AWS Kunden den Service nutzen können.

- Einführung in das AWS Security Hub Video
- Security Hub Hub-Benutzerhandbuch
- Security Hub Hub-API-Referenz
- Onboarding-Webinar

Wir empfehlen Ihnen auch, Security Hub in einem Ihrer AWS Konten zu aktivieren und praktische Erfahrungen mit dem Service zu sammeln.

Voraussetzungen für Partner

Bevor Sie eine Integration mit beginnen können AWS Security Hub, müssen Sie eines der folgenden Kriterien erfüllen:

- Sie sind ein AWS Select-Tier-Partner oder höher.
- Sie sind dem AWS ISV-Partnerpfad beigetreten und das Produkt, das Sie für die Security Hub Hub-Integration verwenden, hat eine AWS grundlegende technische Überprüfung (FTR) abgeschlossen. Das Produkt erhält dann das Abzeichen „Geprüft von AWS“.

Sie müssen außerdem über eine gegenseitige Geheimhaltungsvereinbarung mit AWS verfügen.

Anwendungsfälle für die Integration und erforderliche Berechtigungen

AWS Security Hub ermöglicht es AWS Kunden, Erkenntnisse von APN-Partnern zu erhalten. Die Produkte des Partners können entweder innerhalb oder außerhalb des AWS Kundenkontos ausgeführt werden. Die Berechtigungskonfiguration im Kundenkonto unterscheidet sich je nach dem Modell, das das Partnerprodukt verwendet.

In Security Hub kontrolliert der Kunde immer, welche Partner Ergebnisse an das Konto des Kunden senden können. Kunden können die Berechtigungen eines Partners jederzeit widerrufen.

Damit ein Partner Sicherheitsergebnisse an sein Konto senden kann, abonniert der Kunde zunächst das Partnerprodukt in Security Hub. Der Abonnementschritt ist für alle unten beschriebenen Anwendungsfälle erforderlich. Einzelheiten dazu, wie Kunden Produktintegrationen verwalten, finden Sie im AWS Security Hub Benutzerhandbuch unter Verwaltung von Produktintegrationen.

Nachdem ein Kunde ein Partnerprodukt abonniert hat, erstellt Security Hub automatisch eine verwaltete Ressourcenrichtlinie. Die Richtlinie gewährt dem Partnerprodukt die Erlaubnis, den `BatchImportFindings`API-Vorgang zu verwenden, um Ergebnisse für das Konto des Kunden an Security Hub zu senden.

Hier sind die häufigsten Fälle für Partnerprodukte, die in Security Hub integriert sind. Die Informationen beinhalten die zusätzlichen Berechtigungen, die für jeden Anwendungsfall erforderlich sind.

Vom Partner gehostet: Die Ergebnisse wurden vom Partnerkonto gesendet

Dieser Anwendungsfall deckt Partner ab, die ein Produkt in ihrem eigenen AWS Konto hosten. Um Sicherheitsergebnisse für einen AWS Kunden zu senden, ruft der Partner den `BatchImportFindings`API-Vorgang vom Produktkonto des Partners aus auf.

Für diesen Anwendungsfall benötigt das Kundenkonto nur die Berechtigungen, die festgelegt werden, wenn der Kunde das Partnerprodukt abonniert.

Im Partnerkonto muss der IAM-Principal, der den `BatchImportFindings`API-Vorgang aufruft, über eine IAM-Richtlinie verfügen, die dem Principal den Aufruf ermöglicht. `BatchImportFindings`

Ein Partnerprodukt in die Lage zu versetzen, Ergebnisse in Security Hub an den Kunden zu senden, ist ein zweistufiger Prozess:

1. Der Kunde erstellt ein Abonnement für ein Partnerprodukt in Security Hub.
2. Security Hub generiert mit Bestätigung des Kunden die richtige Richtlinie für verwaltete Ressourcen.

Um Sicherheitsinformationen zu senden, die sich auf das Konto des Kunden beziehen, verwendet das Partnerprodukt seine eigenen Anmeldeinformationen, um den `BatchImportFindings`API-Vorgang aufzurufen.

Hier ist ein Beispiel für eine IAM-Richtlinie, die dem Principal im Partnerkonto die erforderlichen Security Hub Hub-Berechtigungen gewährt.

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

Vom Partner gehostet: Die Ergebnisse wurden über das Kundenkonto gesendet

Dieser Anwendungsfall gilt für Partner, die ein Produkt in ihrem eigenen AWS Konto hosten, aber eine kontoübergreifende Rolle verwenden, um auf das Konto des Kunden zuzugreifen. Sie rufen den `BatchImportFindings`API-Vorgang vom Konto des Kunden aus auf.

In diesem Anwendungsfall übernimmt das Partnerkonto zum Aufrufen des `BatchImportFindings`API-Vorgangs eine vom Kunden verwaltete IAM-Rolle im Konto des Kunden.

Dieser Anruf erfolgt vom Konto des Kunden aus. Daher muss die Richtlinie für verwaltete Ressourcen zulassen, dass der Produkt-ARN für das Konto des Partnerprodukts in dem Anruf verwendet wird. Die von Security Hub verwaltete Ressourcenrichtlinie gewährt Berechtigungen für das Partnerproduktkonto und den Partnerprodukt-ARN. Der Produkt-ARN ist die eindeutige Kennung des Partners als Anbieter. Da der Anruf nicht über das Partnerproduktkonto erfolgt, muss der Kunde dem Partnerprodukt ausdrücklich die Erlaubnis erteilen, Ergebnisse an Security Hub zu senden.

Die bewährte Methode für kontenübergreifende Rollen zwischen Partner- und Kundenkonten besteht darin, eine externe Kennung zu verwenden, die der Partner bereitstellt. Diese externe Kennung ist Teil der Definition der kontenübergreifenden Richtlinien im Kundenkonto. Der Partner muss die Kennung angeben, wenn er die Rolle übernimmt. Eine externe Kennung bietet eine zusätzliche Sicherheitsebene, wenn einem Partner AWS Kontozugriff gewährt wird. Die eindeutige Kennung stellt sicher, dass der Partner das richtige Kundenkonto verwendet.

Die Aktivierung eines Partnerprodukts zum Senden von Ergebnissen an den Kunden in Security Hub mit einer kontenübergreifenden Rolle erfolgt in vier Schritten:

1. Der Kunde oder Partner, der kontoübergreifende Rollen verwendet und im Namen des Kunden arbeitet, startet das Abonnement für ein Produkt in Security Hub.
2. Security Hub generiert mit Bestätigung des Kunden die richtige Richtlinie für verwaltete Ressourcen.
3. Der Kunde konfiguriert die kontenübergreifende Rolle entweder manuell oder mithilfe von. AWS CloudFormation Informationen zu kontenübergreifenden Rollen finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf AWS Konten Dritter.
4. Das Produkt speichert die Kundenrolle und die externe ID sicher.

Als Nächstes sendet das Produkt die Ergebnisse an Security Hub:

1. Das Produkt ruft AWS Security Token Service (AWS STS) auf, um die Kundenrolle zu übernehmen.
2. Das Produkt ruft den `BatchImportFindings`API-Vorgang auf Security Hub mit den temporären Anmeldeinformationen der angenommenen Rolle auf.

Hier ist ein Beispiel für eine IAM-Richtlinie, die der kontoübergreifenden Rolle des Partners die erforderlichen Security Hub Hub-Berechtigungen gewährt.

```
{
```

```
    "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"
        }
    ]
}
```

Der `Resource` Abschnitt der Richtlinie identifiziert das spezifische Produktabonnement. Dadurch wird sichergestellt, dass der Partner nur Ergebnisse für das Partnerprodukt senden kann, das der Kunde abonniert hat.

Vom Kunden gehostet: Die Ergebnisse wurden über das Kundenkonto gesendet

Dieser Anwendungsfall deckt Partner ab, deren Produkt im AWS Kundenkonto bereitgestellt wird. Die `BatchImportFindings`API wird von der Lösung aus aufgerufen, die im Konto des Kunden ausgeführt wird.

Für diesen Anwendungsfall müssen dem Partnerprodukt zusätzliche Berechtigungen zum Aufrufen der `BatchImportFindings`API gewährt werden. Wie diese Berechtigung erteilt wird, hängt von der Partnerlösung und der Konfiguration im Kundenkonto ab.

Ein Beispiel für diesen Ansatz ist ein Partnerprodukt, das auf einer EC2 Instanz im Kundenkonto ausgeführt wird. Dieser EC2 Instanz muss eine EC2 Instanzrolle zugewiesen sein, die dieser Instanz die Möglichkeit gibt, den `BatchImportFindings`API-Vorgang aufzurufen. Dadurch kann die EC2 Instance Sicherheitserkenntnisse an das Konto des Kunden senden.

Dieser Anwendungsfall entspricht funktionell einem Szenario, in dem ein Kunde Ergebnisse für ein Produkt, das er besitzt, in sein Konto lädt.

Der Kunde ermöglicht dem Partnerprodukt, Ergebnisse aus dem Kundenkonto an den Kunden in Security Hub zu senden:

1. Der Kunde stellt das Partnerprodukt manuell oder mithilfe eines AWS CloudFormation anderen Bereitstellungstools in seinem AWS Konto bereit.

2. Der Kunde definiert die erforderliche IAM-Richtlinie, die das Partnerprodukt verwenden soll, wenn es Ergebnisse an Security Hub sendet.
3. Der Kunde fügt die Richtlinie den erforderlichen Komponenten des Partnerprodukts hinzu, z. B. einer EC2 Instanz, einem Container oder einer Lambda-Funktion.

Jetzt kann das Produkt Ergebnisse an Security Hub senden:

1. Das Partnerprodukt verwendet das AWS SDK oder AWS CLI um den `BatchImportFindings`API-Vorgang in Security Hub aufzurufen. Der Anruf erfolgt über die Komponente im Kundenkonto, an die die Richtlinie angehängt ist.
2. Während des API-Aufrufs werden die erforderlichen temporären Anmeldeinformationen generiert, damit der `BatchImportFindings`Aufruf erfolgreich sein kann.

Hier ist ein Beispiel für eine IAM-Richtlinie, die dem Partnerprodukt im Kundenkonto die erforderlichen Security Hub Hub-Berechtigungen gewährt.

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

Onboarding-Prozess für Partner

Als Partner können Sie davon ausgehen, dass Sie im Rahmen Ihres Onboarding-Prozesses mehrere wichtige Schritte abschließen müssen. Sie müssen diese Schritte abschließen, bevor Sie Sicherheitsergebnisse an AWS Security Hub senden können.

1. Sie initiieren eine Zusammenarbeit mit dem APN-Partnerteam oder dem Security Hub-Team und bekunden Interesse daran, ein Partner von Security Hub zu werden. Sie identifizieren die E-Mail-Adressen, die zu den Security Hub Hub-Kommunikationskanälen hinzugefügt werden sollen.
2. AWS gibt Ihnen die Onboarding-Materialien für Security Hub-Partner.
3. Sie werden in den Slack-Channel des Security Hub-Partners eingeladen, wo Sie Fragen zu Ihrer Integration stellen können.
4. Sie stellen den Kontakten der APN-Partner den Entwurf eines Manifests zur Produktintegration zur Überprüfung zur Verfügung.

   Das Produktintegrationsmanifest enthält Informationen, die zur Erstellung des Partnerprodukts Amazon Resource Name (ARN) für die Integration mit verwendet AWS Security Hub werden.

   Es stellt dem Security Hub Hub-Team Informationen zur Verfügung, die auf der Partneranbieterseite in der Security Hub Hub-Konsole angezeigt werden. Es wird auch verwendet, um neue verwaltete Erkenntnisse im Zusammenhang mit der Integration vorzuschlagen, die der Security Hub Hub-Insight-Bibliothek hinzugefügt werden sollen.

   Diese erste Version des Produktintegrationsmanifests muss nicht die vollständigen Details enthalten. Sie sollte jedoch zumindest den Anwendungsfall und die Datensatzinformationen enthalten.

   Einzelheiten zum Manifest und zu den erforderlichen Informationen finden Sie unterManifest zur Produktintegration.
5. Das Security Hub Hub-Team gibt Ihnen einen Produkt-ARN für Ihr Produkt. Sie verwenden den ARN, um Ergebnisse an Security Hub zu senden.
6. Sie erstellen Ihre Integration, um Ergebnisse an Security Hub zu senden oder Ergebnisse von Security Hub zu empfangen.

   Zuordnung der Ergebnisse zu ASFF

   Um Ergebnisse an Security Hub zu senden, müssen Sie Ihre Ergebnisse dem AWS Security Finding Format (ASFF) zuordnen.

Das ASFF bietet eine konsistente Beschreibung der Ergebnisse, die von AWS Sicherheitsdiensten, Partnern und Sicherheitssystemen der Kunden gemeinsam genutzt werden kann. Dies reduziert den Integrationsaufwand, fördert eine gemeinsame Sprache und bietet Implementierern eine Blaupause.

ASFF ist das erforderliche Wire-Protokollformat, an das die Ergebnisse gesendet werden sollen. AWS Security Hub Die Ergebnisse werden als JSON-Dokumente dargestellt, die dem ASFF-JSON-Schema und dem I-JSON-Nachrichtenformat RFC-7493 entsprechen. Einzelheiten zum ASFF-Schema finden Sie unter AWS Security Finding Format (ASFF) im Benutzerhandbuch.AWS Security Hub

Siehe the section called “Richtlinien für die ASFF-Zuordnung”.

Die Integration erstellen und testen

Sie können alle Tests für Ihre Integration mit einem AWS Konto abschließen, das Ihnen gehört. Auf diese Weise erhalten Sie einen vollständigen Überblick darüber, wie die Ergebnisse in Security Hub angezeigt werden. Es hilft Ihnen auch dabei, die Erfahrungen des Kunden mit Ihren Sicherheitsergebnissen zu verstehen.

Sie verwenden den `BatchImportFindings`API-Vorgang, um neue und aktualisierte Ergebnisse an Security Hub zu senden.

AWS Ermutigt Sie, Ihre APN-Partnerkontakte während der gesamten Entwicklung einer Security Hub Hub-Integration über den Fortschritt Ihrer Integration auf dem Laufenden zu halten. Sie können auch Ihre APN-Partnerkontakte um Hilfe bei Fragen zur Integration bitten.

Siehe the section called “Richtlinien für die Verwendung der `BatchImportFindings` API”.

7. Sie demonstrieren dem Security Hub Hub-Produktteam die Integration. Diese Integration muss mit einem Konto nachgewiesen werden, das dem Security Hub Hub-Team gehört.

   Wenn sie mit der Integration zufrieden sind, erteilt das Security Hub Hub-Team die Genehmigung, Sie als Anbieter aufzulisten.

8. Sie stellen ein AWS endgültiges Manifest zur Überprüfung zur Verfügung.
9. Das Security Hub Hub-Team erstellt die Anbieterintegration in der Security Hub Hub-Konsole. Kunden können die Integration dann entdecken und aktivieren.
10. (Optional) Sie ergreifen zusätzliche Marketingmaßnahmen, um für Ihre Security Hub Hub-Integration zu werben. Siehe Go-to-market Aktivitäten.

Security Hub empfiehlt, dass Sie mindestens die folgenden Ressourcen bereitstellen.

- Ein Demonstrationsvideo (maximal 3 Minuten) der funktionierenden Integration. Das Video wird für Marketingzwecke verwendet und auf dem AWS YouTube Kanal veröffentlicht.
- Ein Architekturdiagramm mit einer Folie, das dem Security Hub Hub-Foliendeck für den ersten Anruf hinzugefügt werden kann.

Go-to-market Aktivitäten

Partner können auch optionale Marketingaktivitäten durchführen, um ihre AWS Security Hub Integration zu erläutern und zu fördern.

Wenn Sie Ihre eigenen Marketinginhalte zu Security Hub erstellen möchten, senden Sie vor der Veröffentlichung der Inhalte einen Entwurf zur Prüfung und Genehmigung an Ihren APN-Partnermanager. Auf diese Weise wird sichergestellt, dass alle auf dem gleichen Stand sind, was die Botschaft angeht.

AWS Partner Network (APN) können APN Partner Marketing Central und das Market Development Funds (MDF) -Programm verwenden, um Kampagnen zu erstellen und finanzielle Unterstützung zu erhalten. Nähere Informationen zu diesen Programmen erhalten Sie von Ihrem Partnermanager.

Eintrag auf der Security Hub-Partnerseite

Nachdem Sie als Security Hub-Partner zugelassen wurden, kann Ihre Lösung auf der AWS Security Hub Partnerseite angezeigt werden.

Um auf dieser Seite gelistet zu werden, geben Sie Ihren APN-Partnerkontakten die folgenden Informationen.

```
<Dies kann Ihr Partner Development Manager (PDM), Ihr Partner Solution Architect
```

- Eine kurze Beschreibung Ihrer Lösung, ihrer Integration mit Security Hub und des Werts, den die Integration mit Security Hub für Kunden bietet. Diese Beschreibung ist auf 700 Zeichen einschließlich Leerzeichen begrenzt.
- Die URL zu einer Seite, die Ihre Lösung beschreibt. Diese Website sollte spezifisch für Ihre AWS Integration und insbesondere für Ihre Security Hub Hub-Integration sein. Sie sollte sich auf das Kundenerlebnis und den Wert konzentrieren, den Kunden durch die Nutzung der Integration erhalten.
- Eine hochauflösende Kopie Ihres Logos mit einer Größe von 600 x 300 Pixeln. Einzelheiten zu den Anforderungen für dieses Logo finden Sie unterthe section called “Logo für die Partnerseite”.

Pressemitteilung

Als anerkannter Partner können Sie optional eine Pressemitteilung auf Ihrer Website und in Ihren PR-Kanälen veröffentlichen. Die Pressemitteilung muss von genehmigt werden AWS.

Bevor Sie die Pressemitteilung veröffentlichen, müssen Sie sie AWS zur Prüfung durch APN Partner Marketing, Security Hub Leadership und AWS External Security Services (ESS) einreichen. Die Pressemitteilung kann einen Angebotsvorschlag für den Vizepräsidenten von ESS enthalten.

Um diesen Prozess einzuleiten, arbeiten Sie mit Ihrem PDM zusammen. Wir haben ein Service Level Agreement (SLA) mit einer Laufzeit von 10 Arbeitstagen abgeschlossen, um Pressemitteilungen überprüfen zu können.

AWS Blog zum Partnernetzwerk (APN)

Wir können Ihnen auch dabei helfen, einen von Ihnen verfassten Blogeintrag im APN-Blog zu veröffentlichen. Der Blogeintrag muss sich auf eine Kundengeschichte und einen Anwendungsfall konzentrieren. Es kann nicht ausschließlich darauf ausgerichtet werden, ein Partner für die Einführung von Integrationen zu sein.

Wenn Sie interessiert sind, wenden Sie sich an Ihren PDM oder PSA, um den Prozess einzuleiten. Die endgültige Genehmigung und Veröffentlichung von APN-Blogs kann 8 Wochen oder länger dauern.

Die wichtigsten Dinge, die Sie über den APN-Blog wissen sollten

Beachten Sie beim Erstellen eines Blogbeitrags die folgenden Punkte.

Was gehört zu einem Blogbeitrag?

- Beiträge von Partnern sollten informativ sein und fundiertes Fachwissen zu einem für AWS Kunden relevanten Thema vermitteln.
- Die ideale Länge beträgt nicht mehr als 1.500 Wörter. Leser schätzen tiefgründige, lehrreiche Inhalte, die ihnen beibringen, was möglich ist AWS.
- Der Inhalt sollte originell für den APN-Blog sein. Verwenden Sie keine Inhalte aus Quellen wie bestehenden Blogbeiträgen oder Whitepapers für andere Zwecke.

Welche anderen Beschränkungen gelten für Beiträge im APN-Blog?

- Nur Partner der Stufen Advanced oder Premier können Beiträge im APN-Blog veröffentlichen. Es gibt Ausnahmen für Select-Partner, die über eine APN-Programmbezeichnung wie Service Delivery verfügen.

Jeder Partner ist auf drei Beiträge pro Jahr beschränkt. Bei Zehntausenden von APN-Partnern AWS muss die Abdeckung ausgewogen sein.

Jeder Beitrag muss einen technischen Sponsor haben, der die Lösung oder den Anwendungsfall validieren kann.

Wie lange dauert es, einen Blogbeitrag zu bearbeiten, bevor er veröffentlicht wird?

Nachdem Sie den ersten Entwurf des Blogbeitrags in voller Länge eingereicht haben, dauert die Bearbeitung vier bis sechs Wochen.

Warum sollten Sie für den APN-Blog schreiben?

Ein APN-Blogbeitrag kann die folgenden Vorteile bieten.

- Glaubwürdigkeit — Für APN-Partner AWS kann die Veröffentlichung einer Geschichte von Kunden auf der ganzen Welt beeinflussen.
- Sichtbarkeit — Der APN-Blog ist AWS mit 1,79 Millionen Seitenaufrufen im Jahr 2019, einschließlich beeinflusstem Traffic, einer der meistgelesenen Blogs.
- Unternehmen — Beiträge von APN-Partnern verfügen über Verbindungsschaltflächen, mit denen über das APN Customer Engagements (ACE) -Programm Leads generiert werden können.

Welche Art von Inhalt ist am besten geeignet?

Die folgenden Inhaltstypen eignen sich am besten für einen APN-Blogbeitrag.

- Technischer Inhalt ist die beliebteste Art von Geschichte. Dazu gehören auch Lösungsansätze und Anleitungen. Über 75% der Leser schauen sich diesen technischen Inhalt an.
- Kunden schätzen Geschichten mit mindestens 200 Stufen, die zeigen, wie etwas funktioniert AWS oder wie ein APN-Partner ein Geschäftsproblem für Kunden gelöst hat.
- Beiträge, die von technischen Experten oder Fachexperten verfasst wurden, schneiden mit Abstand am besten ab.

Slick Sheet oder Marketing-Blatt

Ein Slick Sheet ist ein einseitiges Dokument, in dem Ihr Produkt, seine Integrationsarchitektur und gemeinsame Anwendungsfälle von Kunden beschrieben werden.

Wenn Sie ein Slick Sheet für Ihre Integration erstellen, senden Sie eine Kopie an das Security Hub Hub-Team. Sie werden es der Partnerseite hinzufügen.

Whitepaper oder E-Book

Wenn Sie ein Whitepaper oder E-Book erstellen, in dem Ihr Produkt, seine Integrationsarchitektur und gemeinsame Anwendungsfälle von Kunden beschrieben werden, senden Sie eine Kopie an das Security Hub Hub-Team. Sie werden es der Security Hub-Partnerseite hinzufügen.

Webinar

Wenn Sie ein Webinar über Ihre Integration durchführen, senden Sie eine Aufzeichnung des Webinars an das Security Hub Hub-Team. Das Team wird von der Partnerseite aus darauf verlinken.

Das Team kann Ihnen auch einen Security Hub-Fachexperten für die Teilnahme an Ihrem Webinar zur Verfügung stellen.

Demo-Video

Zu Marketingzwecken können Sie ein Demo-Video der funktionierenden Integration erstellen. Veröffentlichen Sie ein solches Video auf Ihrem Videoplattformkonto, und das Security Hub Hub-Team wird von der Partnerseite aus darauf verlinken.

Manifest zur Produktintegration

Jeder AWS Security Hub Integrationspartner muss ein Produktintegrationsmanifest ausfüllen, das die erforderlichen Details für die vorgeschlagene Integration enthält.

Das Security Hub Hub-Team verwendet diese Informationen auf verschiedene Weise:

- Um Ihren Webseiteneintrag zu erstellen
- So erstellen Sie die Produktkarte für die Security Hub Hub-Konsole
- Um das Produktteam über Ihren Anwendungsfall zu informieren.

Um die Qualität der vorgeschlagenen Integration und der bereitgestellten Informationen zu bewerten, verwendet das Security Hub Hub-Team diethe section called “Checkliste zur Eignung des Produkts”. Diese Checkliste bestimmt, ob Ihre Integration startbereit ist.

Alle von Ihnen bereitgestellten technischen Informationen müssen auch in Ihrer Dokumentation enthalten sein.

Sie können eine PDF-Version des Produktintegrations-Manifests im Bereich Ressourcen auf der AWS Security Hub Partnerseite herunterladen. Beachten Sie, dass die Partnerseite in den Regionen China (Peking) und China (Ningxia) nicht verfügbar ist.

Inhalt

- Anwendungsfall und Marketinginformationen
  - Anwendungsfall für die Suche nach Anbietern und Verbrauchern
  - Anwendungsfall Consulting Partner (CP)
  - Datensätze
  - Architektur
  - Konfiguration
  - Durchschnittliche Ergebnisse pro Tag und Kunde
  - Latency
  - Unternehmens- und Produktbeschreibung
  - Ressourcen der Partner-Website
  - Logo für die Partnerseite

- Logos für die Security Hub Hub-Konsole
  - Erkenntnistypen
  - Hotline
  - Erkennung von Herzschlägen
- AWS Security Hub Informationen zur Konsole
  - Informationen zum Unternehmen
  - Produktinformationen

Anwendungsfall und Marketinginformationen

Die folgenden Anwendungsfälle können Ihnen bei der Konfiguration AWS Security Hub für verschiedene Zwecke helfen.

Anwendungsfall für die Suche nach Anbietern und Verbrauchern

Erforderlich für unabhängige Softwareanbieter (ISV).

Beantworten Sie die folgenden Fragen AWS Security Hub, um Ihren Anwendungsfall rund um Ihre Integration mit zu beschreiben. Wenn Sie weder beabsichtigen, Ergebnisse zu senden noch zu empfangen, notieren Sie dies in diesem Abschnitt und füllen Sie dann den nächsten Abschnitt aus.

Die folgenden Informationen müssen in Ihrer Dokumentation enthalten sein.

- Werden Sie Ergebnisse senden, Ergebnisse erhalten oder beides?
- Welche Arten von Ergebnissen werden Sie senden, wenn Sie beabsichtigen, Ergebnisse zu senden? Werden Sie alle Ergebnisse oder eine bestimmte Teilmenge von Ergebnissen senden?
- Was werden Sie mit diesen Ergebnissen tun, wenn Sie beabsichtigen, Ergebnisse zu erhalten? Welche Arten von Ergebnissen werden Sie erhalten? Erhalten Sie beispielsweise alle Ergebnisse, Ergebnisse einer bestimmten Art oder nur bestimmte Ergebnisse, die ein Kunde auswählt?
- Beabsichtigen Sie, die Ergebnisse zu aktualisieren? Falls ja, welche Felder werden Sie aktualisieren? Security Hub empfiehlt, die Ergebnisse zu aktualisieren, anstatt immer neue zu erstellen. Die Aktualisierung vorhandener Ergebnisse trägt dazu bei, dass Kunden weniger häufig zu Ergebnissen kommen.

  Um ein Ergebnis zu aktualisieren, senden Sie ein Ergebnis mit einer Ergebnis-ID, die einem Ergebnis zugewiesen ist, das Sie bereits gesendet haben.

Wenden Sie sich an den APN-Partner oder das Security Hub Hub-Team, um frühzeitig Feedback zu Ihrem Anwendungsfall und Ihren Datensätzen zu erhalten.

Anwendungsfall Consulting Partner (CP)

Erforderlich, wenn Sie ein Security Hub Hub-Beratungspartner sind.

Stellen Sie zwei Kundenanwendungsfälle für Ihre Arbeit mit Security Hub bereit. Dies können private Anwendungsfälle sein. Das Security Hub Hub-Team bewirbt sie nirgends. Sie sollten eine oder beide der folgenden Aktionen beschreiben.

- Wie helfen Sie Kunden beim Bootstrap Security Hub? Haben Sie beispielsweise Kunden bei der Nutzung von Professional Services, einem Terraform-Modul oder einer Vorlage unterstützt? AWS CloudFormation
- Wie unterstützen Sie Kunden bei der Operationalisierung und Erweiterung von Security Hub? Haben Sie beispielsweise Vorlagen für Reaktion oder Problembehebung bereitgestellt, benutzerdefinierte Integrationen entwickelt oder Business Intelligence-Tools zur Einrichtung eines Dashboards für Führungskräfte verwendet?

Datensätze

Erforderlich, wenn Sie Ergebnisse an Security Hub senden.

Geben Sie für die Ergebnisse, die Sie an Security Hub senden, die folgenden Informationen an.

- Die Ergebnisse in ihrem systemeigenen Format, wie JSON oder XML
- Ein Beispiel dafür, wie Sie die Ergebnisse in das AWS Security Finding Format (ASFF) konvertieren

Teilen Sie dem Security Hub Hub-Team mit, ob Sie Updates für die ASFF benötigen, um Ihre Integration zu unterstützen.

Architektur

Erforderlich, wenn Sie Ergebnisse an Security Hub senden oder Ergebnisse von Security Hub erhalten.

Beschreiben Sie, wie Sie Security Hub integrieren werden. Diese Informationen müssen auch in Ihrer Dokumentation enthalten sein.

Sie müssen Architekturdiagramme bereitstellen. Beachten Sie bei der Erstellung Ihrer Architekturdiagramme Folgendes:

- Welche AWS Dienste, Betriebssystemagenten usw. werden Sie verwenden?
- Wenn Sie Ergebnisse an Security Hub senden, senden Sie dann Ergebnisse über das AWS Kundenkonto oder über Ihr eigenes AWS Konto?
- Wenn Sie Ergebnisse erhalten, wie werden Sie die CloudWatch Events-Integration nutzen?
- Wie werden Sie die Ergebnisse in ASFF umwandeln?
- Wie können Sie Ergebnisse bündeln, den Status der Ergebnisse verfolgen und Drosselungsgrenzen vermeiden?

Konfiguration

Erforderlich, wenn Sie Ergebnisse an Security Hub senden oder Ergebnisse von Security Hub erhalten.

Beschreiben Sie, wie ein Kunde Ihre Integration mit Security Hub konfigurieren wird.

Sie müssen mindestens AWS CloudFormation Vorlagen oder eine ähnliche Infrastruktur wie Codevorlagen verwenden. Einige Partner haben eine Benutzeroberfläche zur Unterstützung der Integration mit einem Klick bereitgestellt.

Die Konfiguration sollte nicht länger als 15 Minuten dauern. Ihre Produktdokumentation muss auch Anleitungen zur Konfiguration Ihrer Integration enthalten.

Durchschnittliche Ergebnisse pro Tag und Kunde

Erforderlich, wenn Sie Ergebnisse an Security Hub senden.

Wie viele Suchupdates pro Monat (durchschnittlich und maximal) erwarten Sie, dass Ihr Kundenstamm an Security Hub sendet? Schätzungen in Größenordnungen sind akzeptabel.

Latency

Erforderlich, wenn Sie Ergebnisse an Security Hub senden.

Wie schnell werden Sie Ergebnisse stapeln und an Security Hub senden? Mit anderen Worten, wie groß ist die Latenz zwischen dem Zeitpunkt, an dem das Ergebnis in Ihrem Produkt erstellt wird, bis zu dem Zeitpunkt, an dem es an Security Hub gesendet wird?

Diese Informationen müssen für Ihre Integration in Ihrer Produktdokumentation enthalten sein. Dies ist eine häufig gestellte Frage von Kunden.

Unternehmens- und Produktbeschreibung

Für alle Integrationen mit Security Hub erforderlich.

Beschreiben Sie kurz Ihr Unternehmen und Ihr Produkt, wobei der Schwerpunkt auf der Art Ihrer Security Hub Hub-Integration liegt. Wir verwenden dies auf unserer Security Hub-Partnerseite.

Wenn Sie mehrere Produkte in Security Hub integrieren, können Sie für jedes Produkt eine separate Beschreibung angeben. Wir fassen sie jedoch zu einem einzigen Eintrag auf der Partnerseite zusammen.

Jede Beschreibung darf nicht mehr als 700 Zeichen mit Leerzeichen enthalten.

Ressourcen der Partner-Website

Für alle Integrationen mit Security Hub erforderlich.

Sie müssen mindestens eine URL angeben, die für den Hyperlink Weitere Informationen auf der Security Hub-Partnerseite verwendet werden soll. Es sollte sich um eine Marketing-Landingpage handeln, auf der die Integration zwischen Ihrem Produkt und Security Hub beschrieben wird.

Wenn Sie mehrere Produkte in Security Hub integrieren, können Sie eine einzige Landingpage für sie einrichten. Security Hub empfiehlt, dass diese Landing Page einen Link zu Ihren Konfigurationsanweisungen enthält.

Sie können auch Links zu anderen Ressourcen wie Blogs, Webinaren, Demo-Videos oder Whitepapers bereitstellen. Security Hub wird auch Links zu denen von seiner Partnerseite aus bereitstellen.

Logo für die Partnerseite

Für alle Security Hub Hub-Integrationen erforderlich.

Geben Sie eine URL zu einem Logo an, das auf der Security Hub-Partnerseite angezeigt werden soll. Das Logo muss die folgenden Kriterien erfüllen:

- Größe: 600 x 300 Pixel
- Zuschnitt: eng und ohne Polsterung

- Hintergrund: transparent
- Format: PNG

Logos für die Security Hub Hub-Konsole

Für alle Integrationen erforderlich.

Stellen Sie URLs die Logos für den hellen Modus und den dunklen Modus bereit, die auf der Security Hub Hub-Konsole angezeigt werden sollen.

Die Logos müssen die folgenden Kriterien erfüllen:

- Format: SVG
- Größe: 175 x 40 Pixel. Wenn es größer ist, sollte das Bild dieses Verhältnis verwenden.
- Zuschnitt: eng, keine Polsterung
- Hintergrund: transparent

Ausführliche Richtlinien für das kleine Logo finden Sie unterthe section called “Richtlinien für das Konsolenlogo”.

Erkenntnistypen

Erforderlich, wenn Sie Ergebnisse an Security Hub senden.

Stellen Sie eine Tabelle bereit, in der die von Ihnen verwendeten Befundtypen im ASFF-Format und deren Übereinstimmung mit Ihren systemeigenen Befundtypen dokumentiert sind. Einzelheiten zur Suche nach Typen in ASFF finden Sie unter Typentaxonomie für ASFF im Benutzerhandbuch.AWS Security Hub

Wir empfehlen Ihnen, diese Informationen auch in Ihre Produktdokumentation aufzunehmen.

Hotline

Für alle Integrationen mit Security Hub erforderlich.

Geben Sie eine E-Mail-Adresse und eine Telefonnummer oder Pager-Nummer für einen technischen Ansprechpartner an. Security Hub kommuniziert mit diesem Ansprechpartner bei technischen Problemen, z. B. wenn eine Integration nicht mehr funktioniert.

Stellen Sie außerdem rund um die Uhr einen Ansprechpartner für schwerwiegende technische Probleme zur Verfügung.

Erkennung von Herzschlägen

Wird empfohlen, wenn Sie Ergebnisse an Security Hub senden.

Können Sie Security Hub alle fünf Minuten einen „Heartbeat“ -Beat senden, der darauf hinweist, dass Ihre Integration mit Security Hub funktioniert?

Wenn Sie können, verwenden Sie dafür den Befundtyp`Heartbeat`.

AWS Security Hub Informationen zur Konsole

Stellen Sie dem AWS Security Hub Team JSON-Text zur Verfügung, der die folgenden Informationen enthält. Security Hub verwendet diese Informationen, um Ihren Produkt-ARN zu erstellen, die Anbieterliste in der Konsole anzuzeigen und Ihre vorgeschlagenen verwalteten Erkenntnisse in die Security Hub Hub-Insight-Bibliothek aufzunehmen.

Informationen zum Unternehmen

Die Unternehmensinformationen geben Auskunft über Ihr Unternehmen. Ein Beispiel:

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

Die Unternehmensinformationen enthalten die folgenden Felder:

Feld	Erforderlich	Beschreibung
`id`	Ja	Die eindeutige Kennung des Unternehmens. Die Unternehmenskennung muss unternehm ensübergreifend eindeutig sein. Dies ist wahrscheinlich dasselbe wie oder ähnlich wie`name`.

Feld	Erforderlich	Beschreibung
		Typ: Zeichenfolge Mindestlänge: 5 Zeichen Maximale Länge: 24 Zeichen Zulässige Zeichen: Kleinbuchstaben, Zahlen und Bindestriche Muss mit einem Kleinbuchstaben beginnen. Muss mit einem Kleinbuchstaben oder einer Zahl enden.
`name`	Ja	Der Name des Unternehmens des Anbieters , der auf der Security Hub Hub-Konsole angezeigt werden soll. Typ: Zeichenfolge Maximale Länge: 16 Zeichen
`description`	Ja	Die Beschreibung des Unternehmens des Anbieters, die auf der Security Hub Hub-Konso le angezeigt werden soll. Typ: Zeichenfolge Maximale Länge: 200 Zeichen

Produktinformationen

Dieser Abschnitt enthält Informationen zu Ihrem Produkt. Ein Beispiel:

```
{
    "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"
}
```

Die Produktinformationen enthalten die folgenden Felder.

Feld	Erforderlich	Beschreibung
`IntegrationType`	Ja	Gibt an, ob Ihr Produkt Ergebnisse an Security Hub sendet, Ergebnisse von Security Hub empfängt oder Ergebnisse sowohl sendet als auch empfängt. Wenn Sie ein Beratungspartner sind, lassen Sie dieses Feld leer. Typ: Zeichenketten-Array Zulässige Werte: `SEND_FINDINGS_TO_SECURITY_HUB` | `RECEIVE_FINDINGS_FROM_SECURITY_HUB`
`id`	Ja	Die eindeutige Kennung des Produkts. Diese müssen innerhalb eines Unternehmens einzigartig sein. Sie müssen nicht unternehmensübergreifend einzigartig sein. Dies ist wahrscheinlich dasselbe oder ähnlich wie `name`. Typ: Zeichenfolge Mindestlänge: 5 Zeichen Maximale Länge: 24 Zeichen Zulässige Zeichen: Kleinbuchstaben, Zahlen und Bindestriche

Feld	Erforderlich	Beschreibung
		Muss mit einem Kleinbuchstaben beginnen. Muss mit einem Kleinbuchstaben oder einer Zahl enden.
`regionsNotSupported`	Ja	Welche der folgenden AWS Regionen unterstützen Sie nicht? Mit anderen Worten, in welchen Regionen sollte Security Hub Sie nicht als Option auf unserer Partnerseite in der Security Hub Hub-Konsole anzeigen? Typ: Zeichenfolge Geben Sie nur den Regionalcode an. Beispiel, `us-west-1` . Eine Liste der Regionen finden Sie unter Regionale Endpunkte in der Allgemeine AWS-Referenz. Die Regionscodes für AWS GovCloud (US) sind `us-gov-west-1` (für AWS GovCloud (US-West)) und `us-gov-east-1` (für AWS GovCloud (US-Ost)). Die Regionalcodes für chinesische Regionen lauten `cn-north-1` (für China (Peking)) und `cn-northwest-1` (für China (Ningxia)).

Feld	Erforderlich	Beschreibung
`commercialAccountNumber`	Ja	Die primäre AWS Kontonummer für das Produkt für die AWS Regionen. Wenn Sie Ergebnisse an Security Hub senden, hängt das von Ihnen angegebene Konto davon ab, von wo aus Sie die Ergebnisse senden. • Von Ihrem AWS Konto aus. Geben Sie in diesem Fall die Kontonummer an, die Sie für die Einreichung der Ergebnisse verwenden. • Aus dem AWS Konto des Kunden. In diesem Fall empfiehlt Security Hub, dass Sie die primäre Kontonummer angeben, mit der Sie die Integration testen. Idealerweise verwenden Sie dasselbe Konto für alle Ihre Produkte in allen Regionen. Wenn dies nicht möglich ist, wenden Sie sich an das Security Hub Hub-Team. Wenn Sie nur Ergebnisse von Security Hub erhalten, ist diese Kontonummer nicht erforderlich. Typ: Zeichenfolge

Feld	Erforderlich	Beschreibung
`govcloudAccountNumber`	Nein	Die primäre AWS Kontonummer für das Produkt für AWS GovCloud (US) Regionen (falls Ihr Produkt in verfügbar ist AWS GovCloud (US)). Wenn Sie Ergebnisse an Security Hub senden, hängt das von Ihnen angegebene Konto davon ab, von wo aus Sie die Ergebnisse senden. • Von Ihrem AWS Konto aus. Geben Sie in diesem Fall die Kontonummer an, die Sie für die Einreichung der Ergebnisse verwenden. • Aus dem AWS Konto des Kunden. In diesem Fall empfiehlt Security Hub, dass Sie die primäre Kontonummer angeben, mit der Sie die Integration testen. Idealerweise verwenden Sie dasselbe Konto für alle Ihre Produkte in allen AWS GovCloud (US) Regionen. Wenn dies nicht möglich ist, wenden Sie sich an das Security Hub Hub-Team. Wenn Sie nur Ergebnisse von Security Hub erhalten, ist diese Kontonummer nicht erforderlich. Typ: Zeichenfolge

Feld	Erforderlich	Beschreibung
`chinaAccountNumber`	Nein	Die primäre AWS Kontonummer für das Produkt für China Regionen (wenn Ihr Produkt in den China Regionen verfügbar ist). Wenn Sie Ergebnisse an Security Hub senden, hängt das von Ihnen angegebene Konto davon ab, von wo aus Sie die Ergebnisse senden. • Von Ihrem AWS Konto aus. Geben Sie in diesem Fall die Kontonummer an, die Sie für die Einreichung der Ergebnisse verwenden. • Aus dem AWS Konto des Kunden. In diesem Fall empfiehlt Security Hub, dass Sie die primäre Kontonummer angeben, mit der Sie die Produktintegration testen. Idealerweise verwenden Sie dasselbe Konto für alle Ihre Produkte in allen Regionen China. Wenn dies nicht möglich ist, wenden Sie sich an das Security Hub Hub-Team. Wenn Sie nur Ergebnisse von Security Hub erhalten, kann dies jedes Konto sein, das Sie in einer Region China besitzen. Typ: Zeichenfolge
`name`	Ja	Der Name des Produkts des Anbieters, der auf der Security Hub Hub-Konsole angezeigt werden soll. Typ: Zeichenfolge Maximale Länge: 24 Zeichen

Feld	Erforderlich	Beschreibung
`description`	Ja	Die Beschreibung des Produkts des Anbieters , die auf der Security Hub Hub-Konsole angezeigt werden soll. Typ: Zeichenfolge Maximale Länge: 200 Zeichen
`importType`	Ja	Die Art der Ressourcenrichtlinie für den Partner. Während des Partner-Onboarding-Prozesse s können Sie eine der folgenden Ressource nrichtlinien angeben, oder Sie können Folgendes angeben`NEITHER`. • Mit `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` können Sie Ergebniss e nur von dem Konto an Security Hub senden, das in Ihrem Produkt-ARN aufgeführ t ist. • Mit `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` können Sie nur Ergebnisse von dem Kundenkonto senden, das Sie abonniert hat. Typ: Zeichenfolge Gültige Werte: `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` | | `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` `NEITHER`

Feld	Erforderlich	Beschreibung
`category`	Ja	Die Kategorien, die Ihr Produkt definieren. Ihre Auswahl wird auf der Security Hub Hub-Konsole angezeigt. Wählen Sie bis zu drei Kategorien aus. Benutzerdefinierte Auswahlen sind nicht zulässig. Wenn Sie der Meinung sind, dass Ihre Kategorie fehlt, wenden Sie sich an das Security Hub Hub-Team. Typ: Array Verfügbare Kategorien: • `API Firewall` • `Asset Management` • `AV Scanning and Sandboxing` • `Backup and Disaster Recovery` • `Breach and Attack Simulation` • `Bug Bounty Platform` • `Certificate Management` • `Cloud Access Security Broker` • `Cloud Security Posture Management` • `Configuration and Patch Management` • `Configuration Management Database (CMDB)` • `Consulting Partner` • `Container Security` • `Cyber Range` • `Data Access Management`

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

Feld	Erforderlich	Beschreibung
		• `Managed Security Service Provider (MSSP)` • `Micro-Segmentation` • `Multi-Cloud Management` • `Multi-Factor Authentication` • `Network Access Control (NAC)` • `Network Firewall` • `Network Forensics` • `Network Intrusion Detection Systems (IDS)` • `Network Intrusion Prevention Systems (IPS)` • `Phishing Simulation and Training` • `Privacy Operations` • `Privileged Access Management` • `Rogue Device Detection` • `Runtime Application Self-Protection (RASP)` • `Secure Web Gateway`
`marketplaceUrl`	Nein	Die URL zu Ihrem AWS Marketplace Produktziel. Die URL wird in der Security Hub Hub-Konsole angezeigt. Typ: Zeichenfolge Dies muss eine AWS Marketplace URL sein. Wenn Sie kein AWS Marketplace Angebot haben, lassen Sie dieses Feld leer.

Feld	Erforderlich	Beschreibung
`configurationUrl`	Ja	Die URL zu Ihrer Produktdokumentation über die Integration mit Security Hub. Dieser Inhalt wird auf Ihrer Website oder auf einer von Ihnen verwalteten Webseite, z. B. einer GitHub Seite, gehostet. Typ: Zeichenfolge Ihre Dokumentation sollte die folgenden Informationen enthalten. • Anweisungen zur Konfiguration • Links zu AWS CloudFormation Vorlagen (falls erforderlich) • Informationen zu Ihrem Anwendungsfall für die Integration • Latency • ASFF-Zuordnung • Zu den Arten der Ergebnisse gehörten • Architektur

Richtlinien und Checklisten

Verwenden Sie bei der Vorbereitung der erforderlichen Materialien für Ihre AWS Security Hub Integration diese Richtlinien.

Die Bereitschafts-Checkliste wird verwendet, um eine abschließende Überprüfung der Integration durchzuführen, bevor Security Hub sie Security Hub-Kunden zur Verfügung stellt.

Themen

- Richtlinien für die Anzeige des Logos auf der Konsole AWS Security Hub
- Grundsätze für die Erstellung und Aktualisierung von Ergebnissen
- Richtlinien für die Zuordnung von Ergebnissen zum AWS Security Finding Format (ASFF)
- Richtlinien für die Verwendung der BatchImportFindings API
- Checkliste zur Eignung des Produkts

Richtlinien für die Anzeige des Logos auf der Konsole AWS Security Hub

Damit das Logo auf der AWS Security Hub Konsole angezeigt wird, befolgen Sie diese Richtlinien.

Hell- und Dunkelmodus

Sie müssen sowohl eine Hellmodus- als auch eine Dunkelmodus-Version des Logos bereitstellen.

Format

SVG-Dateiformat

Hintergrundfarbe

Transparent

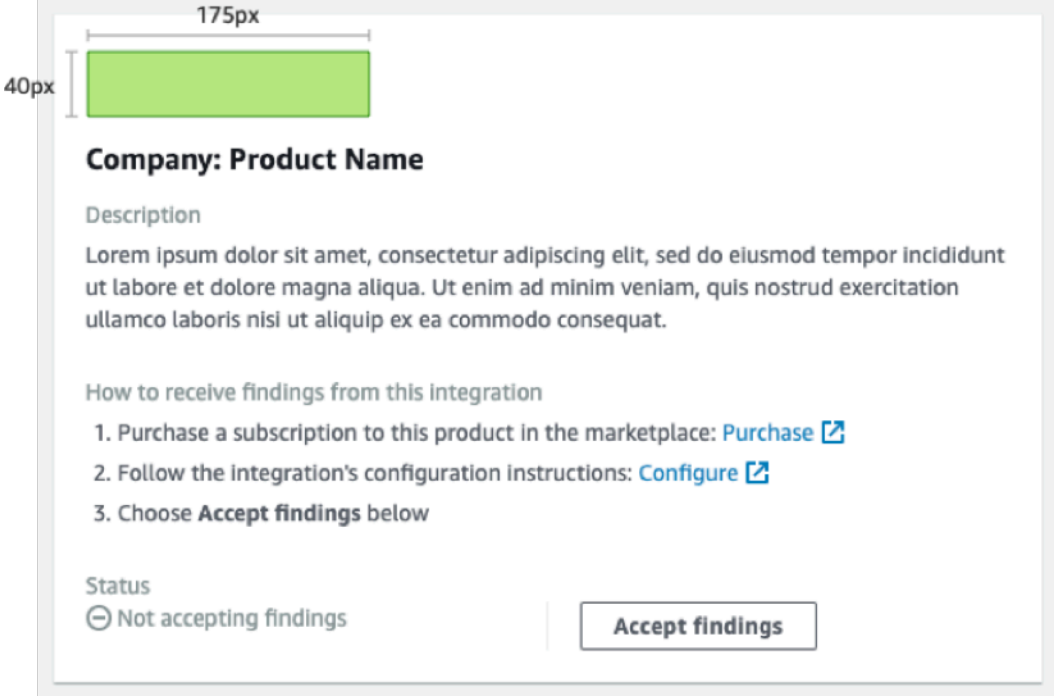
Größe

Das ideale Verhältnis ist 175 px breit und 40 px hoch.

Die Mindesthöhe beträgt 40 px.

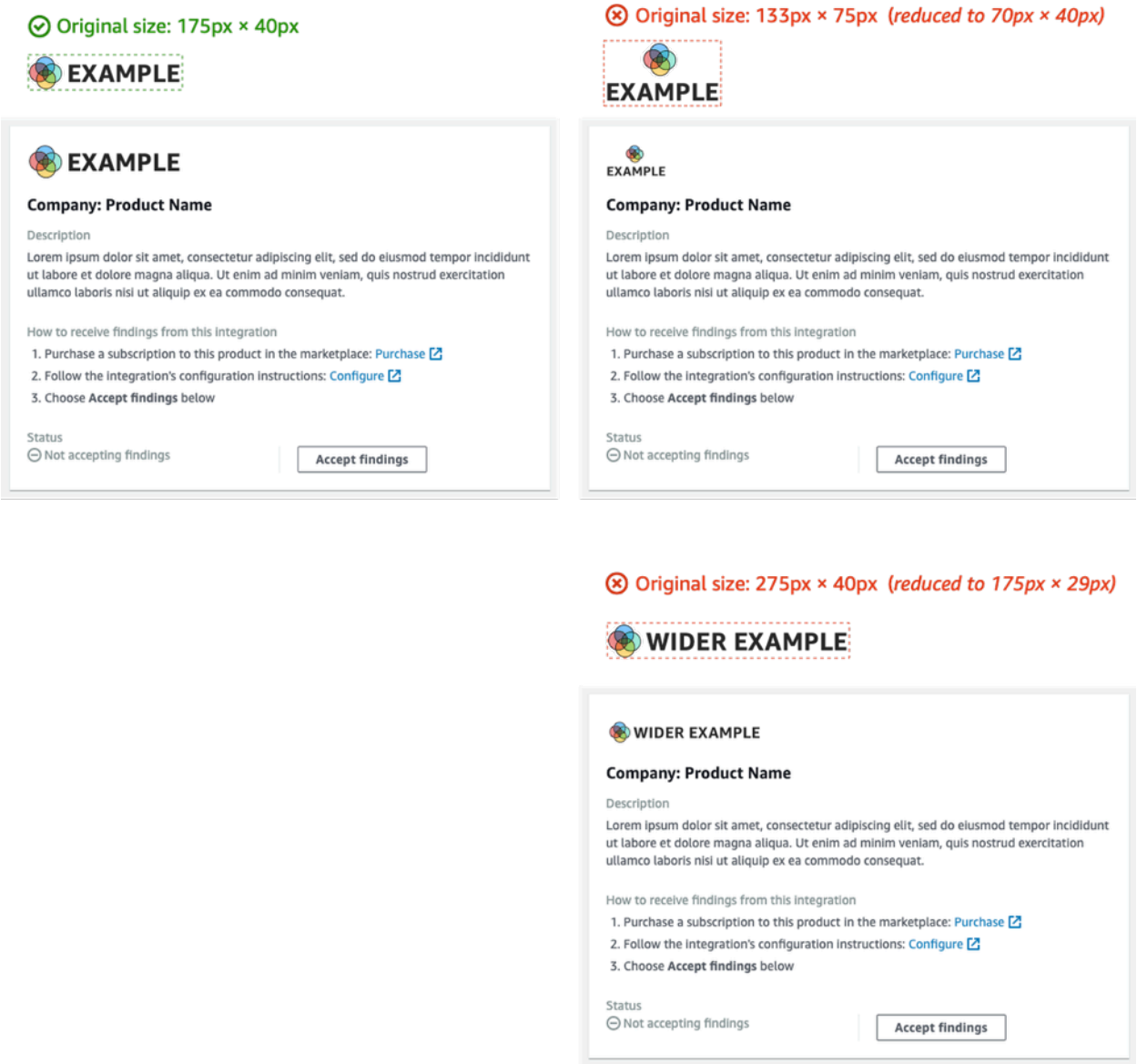
Rechteckige Logos funktionieren am besten.

Die folgende Abbildung zeigt, wie ein ideales Logo auf der Security Hub Hub-Konsole angezeigt wird.



Wenn Ihr Logo diesen Abmessungen nicht entspricht, reduziert Security Hub die Größe auf eine maximale Höhe von 40 px und eine maximale Breite von 175 px. Dies wirkt sich darauf aus, wie das Logo auf der Security Hub Hub-Konsole angezeigt wird.

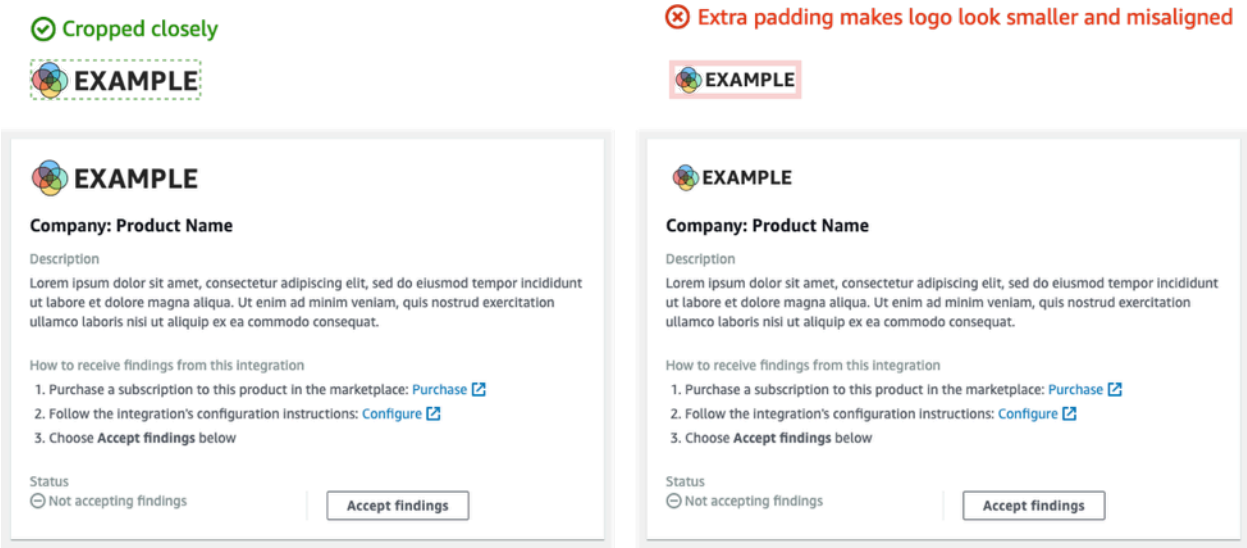
In der folgenden Abbildung wird die Anzeige eines Logos mit der idealen Größe mit Logos verglichen, die breiter oder höher waren.



Zuschneiden

Schneide das Logobild so nah wie möglich zu. Sorgen Sie nicht für zusätzliche Polsterung.

Die folgende Abbildung zeigt den Unterschied zwischen einem Logo, das eng beschnitten ist, und einem Logo mit zusätzlicher Polsterung.



Grundsätze für die Erstellung und Aktualisierung von Ergebnissen

Beachten Sie bei der Planung, wie Sie Ergebnisse in erstellen und aktualisieren werden AWS Security Hub, die folgenden Grundsätze.

Machen Sie die Ergebnisse spezifisch, damit Kunden problemlos Maßnahmen ergreifen können.

Kunden möchten Reaktions- und Abhilfemaßnahmen automatisieren und die Ergebnisse mit anderen Ergebnissen korrelieren. Um dies zu belegen, sollten die Ergebnisse die folgenden Merkmale aufweisen:

- Sie sollten sich in der Regel auf eine einzelne Ressource oder eine Primärressource beziehen.
- Sie sollten einen einzigen Befundtyp haben.
- Sie sollten sich mit einem einzigen Sicherheitsereignis befassen.

Wenn ein Ergebnis Daten für mehrere Sicherheitsereignisse enthält, ist es für Kunden schwieriger, Maßnahmen zu ergreifen.

Ordnen Sie all Ihre Ergebnisfelder dem AWS Security Finding Format (ASFF) zu. Ermöglichen Sie es Kunden, sich auf Security Hub als Informationsquelle zu verlassen.

Kunden erwarten, dass jedes Feld, das in Ihrem nativen Suchformat vorliegt, auch im Security Hub ASFF vertreten ist.

Kunden möchten, dass alle Daten in der Security Hub Hub-Version des Ergebnisses vorhanden sind. Fehlende Daten führen dazu, dass sie das Vertrauen in Security Hub als zentrale Quelle für Sicherheitsinformationen verlieren.

Reduzieren Sie die Redundanz der Ergebnisse. Überfordern Sie Ihre Kunden nicht mit der Suche nach Volumen.

- Security Hub ist kein allgemeines Protokollverwaltungstool. Sie sollten Ergebnisse an Security Hub senden, die sehr umsetzbar sind und auf die Kunden direkt reagieren, diese korrigieren oder mit anderen Ergebnissen korrelieren können.
- Wenn das Ergebnis nur geringfügig geändert wurde, aktualisieren Sie das Ergebnis, anstatt ein neues Ergebnis zu erstellen.
- Wenn sich das Ergebnis erheblich ändert, z. B. der Schweregrad oder die Ressourcen-ID, erstellen Sie ein neues Ergebnis.
- Es ist beispielsweise nicht sehr umsetzbar, Ergebnisse für einzelne Port-Scans in Echtzeit zu erstellen. Da Port-Scans kontinuierlich durchgeführt werden können, würde dies zu einer großen Menge an Ergebnissen führen. Es ist weitaus überzeugender und präziser, bei einem Portscan auf einem MongoDB-Port von einem TOR-Knoten aus einfach die Uhrzeit des letzten Scans und die Anzahl der Scans anhand eines einzigen Ergebnisses zu aktualisieren.

Ermöglichen Sie es Kunden, ihre Ergebnisse individuell anzupassen, um sie aussagekräftiger zu machen.

- Kunden möchten in der Lage sein, bestimmte Suchfelder so anzupassen, dass sie für ihre Umgebung oder ihre Anforderungen relevanter sind.
- Kunden möchten beispielsweise in der Lage sein, Notizen und Stichwörter hinzuzufügen und den Schweregrad je nach Kontotyp oder Ressourcentyp, mit dem das Ergebnis verknüpft ist, anzupassen.

Richtlinien für die Zuordnung von Ergebnissen zum AWS Security Finding Format (ASFF)

Verwenden Sie die folgenden Richtlinien, um Ihre Ergebnisse dem ASFF zuzuordnen. Eine ausführliche Beschreibung der einzelnen ASFF-Felder und -Objekte finden Sie im AWS Benutzerhandbuch unter Security Finding Format (ASFF).AWS Security Hub

Identifizierende Informationen

`SchemaVersion` ist immer `2018-10-08`.

`ProductArn`ist der ARN, der Ihnen AWS Security Hub zugewiesen wird.

`Id`ist der Wert, den Security Hub verwendet, um Ergebnisse zu indexieren. Die Ergebnis-ID muss eindeutig sein, um sicherzustellen, dass andere Ergebnisse nicht überschrieben werden. Um ein Ergebnis zu aktualisieren, reichen Sie das Ergebnis erneut mit derselben Kennung ein.

`GeneratorId`kann mit einer diskreten Logikeinheit identisch sein `Id` oder sich auf eine solche beziehen, z. B. eine GuardDuty Amazon-Detektor-ID, AWS Config Rekorder-ID oder IAM Access Analyzer-ID.

Title and Description

`Title`sollte einige Informationen über die betroffene Ressource enthalten. `Title`ist auf 256 Zeichen einschließlich Leerzeichen begrenzt.

Fügen Sie ausführlichere Informationen zu hinzu`Description`. `Description`ist auf 1024 Zeichen einschließlich Leerzeichen begrenzt. Sie können erwägen, Beschreibungen zu kürzen. Ein Beispiel:

```
"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.",
```

Erkenntnistypen

Sie geben Informationen zu Ihrem Suchtyp unter an`FindingProviderFields.Types`.

`Types`sollte der Typen-Taxonomie für ASFF entsprechen.

Bei Bedarf können Sie einen benutzerdefinierten Klassifikator (den dritten Namespace) angeben.

Zeitstempel

Das ASFF-Format enthält einige verschiedene Zeitstempel.

`CreatedAt` und **`UpdatedAt`**

> Sie müssen `UpdatedAt` jedes Mal, wenn Sie anrufen `BatchImportFindings`, jedes Ergebnis einreichen`CreatedAt`.

Die Werte müssen dem Format ISO86 01 in Python 3.8 entsprechen.

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

`FirstObservedAt` und **`LastObservedAt`**

`FirstObservedAt`und `LastObservedAt` müssen mit dem Zeitpunkt übereinstimmen, zu dem Ihr System den Befund beobachtet hat. Wenn Sie diese Informationen nicht aufzeichnen, müssen Sie diese Zeitstempel nicht einreichen.

Die Werte entsprechen dem Format ISO86 01 in Python 3.8.

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

Severity

Sie geben Informationen zum Schweregrad in dem `FindingProviderFields.Severity` Objekt ein, das die folgenden Felder enthält.

`Original`

Der Schweregradwert aus Ihrem System. `Original`kann eine beliebige Zeichenfolge sein, die dem von Ihnen verwendeten System entspricht.

`Label`

Der erforderliche Security Hub Hub-Indikator für den Schweregrad des Fundes. Die zulässigen Werte lauten wie folgt.

- `INFORMATIONAL`— Es wurde kein Problem gefunden.
- `LOW`— Das Problem erfordert keine eigenständigen Maßnahmen.
- `MEDIUM`— Das Problem muss angegangen werden, aber nicht dringend.
- `HIGH`— Das Problem muss vorrangig angegangen werden.
- `CRITICAL`— Das Problem muss sofort behoben werden, um weiteren Schaden zu vermeiden.

Feststellungen, die konform sind, hätten immer auf `INFORMATIONAL` Folgendes `Label` eingestellt werden müssen. Beispiele für `INFORMATIONAL` Ergebnisse sind Ergebnisse von Sicherheitsüberprüfungen, die bestanden wurden, und AWS Firewall Manager Ergebnisse, die behoben wurden.

Kunden sortieren die Ergebnisse häufig nach ihrem Schweregrad, um ihren Sicherheitsteams eine Aufgabenliste zu geben. Seien Sie vorsichtig, wenn Sie den Schweregrad der Ergebnisse auf `HIGH` oder `CRITICAL` setzen.

Ihre Integrationsdokumentation muss Ihre Begründung für die Zuordnung enthalten.

Remediation

`Remediation`besteht aus zwei Elementen. Diese Elemente werden auf der Security Hub Hub-Konsole kombiniert.

`Remediation.Recommendation.Text`wird im Abschnitt Problembehebung in den Details zu den Ergebnissen angezeigt. Es ist mit dem Wert von verlinkt. `Remediation.Recommendation.Url`

Derzeit enthalten nur Ergebnisse aus den Security Hub Hub-Standards, IAM Access Analyzer und Firewall Manager Hyperlinks zu Dokumentationen zur Behebung des Fehlers.

SourceUrl

Verwenden Sie diese Option nur`SourceUrl`, wenn Sie eine URL mit einem Deep-Link zu Ihrer Konsole für diesen spezifischen Befund angeben können. Andernfalls sollten Sie es in der Zuordnung weglassen.

Security Hub unterstützt keine Hyperlinks aus diesem Feld, aber es wird auf der Security Hub Hub-Konsole angezeigt.

Malware, Network, Process, ThreatIntelIndicators

Verwenden Sie gegebenenfalls`Malware`, `NetworkProcess`, oder`ThreatIntelIndicators`. Jedes dieser Objekte wird in der Security Hub Hub-Konsole angezeigt. Verwenden Sie diese Objekte im Zusammenhang mit dem Ergebnis, das Sie senden.

Wenn Sie beispielsweise Schadsoftware entdecken, die eine ausgehende Verbindung zu einem bekannten Command-and-Control-Knoten herstellt, geben Sie die Details für die EC2 Instanz in `Resource.Details.AwsEc2Instance` an. Geben Sie die relevanten `MalwareNetwork`, und `ThreatIntelIndicator` Objekte für diese EC2 Instanz an.

Malware

`Malware`ist eine Liste, die bis zu fünf Arrays mit Malware-Informationen akzeptiert. Machen Sie die Malware-Einträge relevant für die Ressource und das Ergebnis.

Jeder Eintrag hat die folgenden Felder.

`Name`

Der Name der Malware. Der Wert ist eine Zeichenfolge mit bis zu 64 Zeichen.

`Name`sollte aus einer geprüften Quelle für Bedrohungsinformationen oder Forscher stammen.

`Path`

Der Pfad zur Malware. Der Wert ist eine Zeichenfolge mit bis zu 512 Zeichen. `Path`sollte ein Linux- oder Windows-Systemdateipfad sein, außer in den folgenden Fällen.

- Wenn Sie Objekte in einem S3-Bucket oder einem EFS-Share anhand der YARA-Regeln scannen, `Path` ist dies der S3: //- oder HTTPS-Objektpfad.
- Wenn Sie Dateien in einem Git-Repository scannen, `Path` ist dies die Git-URL oder der Klonpfad.

`State`

Der Status der Malware. Die zulässigen Werte sind `OBSERVED` | `REMOVAL_FAILED` |`REMOVED`.

Stellen Sie sicher, dass Sie im Titel und in der Beschreibung des Befundes einen Kontext dafür angeben, was mit der Malware passiert ist.

Wenn dies beispielsweise der Fall `Malware.State` ist`REMOVED`, sollten der Titel und die Beschreibung des Befundes darauf hinweisen, dass Ihr Produkt die Malware entfernt hat, die sich auf dem Pfad befindet.

Falls ja `Malware.State`ist`OBSERVED`, sollten der Titel und die Beschreibung des Ergebnisses darauf hinweisen, dass Ihr Produkt auf diese Schadsoftware gestoßen ist, die sich im Pfad befindet.

`Type`

Gibt die Art der Malware an. Die zulässigen Werte sind `ADWARE` | | `BLENDED_THREAT` | `BOTNET_AGENT` | `COIN_MINER` | `EXPLOIT_KIT` | `KEYLOGGER` | | `MACRO` | `POTENTIALLY_UNWANTED` | `SPYWARE` | `RANSOMWARE` | `REMOTE_ACCESS` | `ROOTKIT` | | `TROJAN` | `VIRUS` |`WORM`.

Wenn Sie einen zusätzlichen Wert für benötigen`Type`, wenden Sie sich an das Security Hub Hub-Team.

Network

`Network`ist ein einzelnes Objekt. Sie können nicht mehrere netzwerkbezogene Details hinzufügen. Beachten Sie bei der Zuordnung der Felder die folgenden Richtlinien.

Ziel- und Quellinformationen

Ziel und Quelle können einfach TCP- oder VPC-Flow-Logs oder WAF-Logs zugeordnet werden. Sie sind schwieriger zu verwenden, wenn Sie Netzwerkinformationen beschreiben, um Erkenntnisse über einen Angriff zu erhalten.

In der Regel handelt es sich bei der Quelle um den Ursprung des Angriffs, es könnte sich aber auch um andere Quellen handeln, wie unten aufgeführt. Sie sollten die Quelle in Ihrer Dokumentation erläutern und sie auch im Titel und in der Beschreibung der Ergebnisse beschreiben.

- Bei einem DDo S-Angriff auf eine EC2 Instanz ist der Angreifer die Quelle, obwohl ein echter DDo S-Angriff Millionen von Hosts nutzen kann. Das Ziel ist die öffentliche IPv4 Adresse der EC2 Instanz. `Direction`ist IN.
- Bei Schadsoftware, bei der beobachtet wird, dass sie von einer EC2 Instanz zu einem bekannten Befehls- und Kontrollknoten kommuniziert, ist die Quelle die IPV4 Adresse der EC2 Instanz. Das Ziel ist der Befehls- und Kontrollknoten. `Direction`ist0UT. Sie würden auch bereitstellen `Malware` und`ThreatIntelIndicators`.

`Protocol`

`Protocol`wird immer einem bei der Internet Assigned Numbers Authority (IANA) registrierten Namen zugeordnet, es sei denn, Sie können ein bestimmtes Protokoll angeben. Sie sollten dies immer verwenden und die Portinformationen angeben.

`Protocol`ist unabhängig von den Quell- und Zielinformationen. Geben Sie sie nur an, wenn es sinnvoll ist.

`Direction`

`Direction`ist immer relativ zu den AWS Netzwerkgrenzen.

- `IN`bedeutet, dass es eintritt AWS (VPC, Service).
- 0UTbedeutet, dass es die AWS Netzwerkgrenzen verlässt.

Process

`Process`ist ein einzelnes Objekt. Sie können nicht mehrere prozessbezogene Details hinzufügen. Beachten Sie bei der Zuordnung der Felder die folgenden Richtlinien.

`Name`

`Name`sollte dem Namen der ausführbaren Datei entsprechen. Es akzeptiert bis zu 64 Zeichen.

`Path`

`Path`ist der Dateisystempfad zur ausführbaren Datei des Prozesses. Er akzeptiert bis zu 512 Zeichen.

`Pid`, **`ParentPid`**

`Pid`und `ParentPid` sollte mit der Linux-Prozess-ID (PID) oder der Windows-Ereignis-ID übereinstimmen. Verwenden Sie zur Differenzierung EC2 Amazon Machine Images (AMI), um die Informationen bereitzustellen. Kunden können wahrscheinlich zwischen Windows und Linux unterscheiden.

Zeitstempel (**`LaunchedAt`**und**`TerminatedAt`**)

Wenn Sie diese Informationen nicht zuverlässig abrufen können und sie nicht auf die Millisekunde genau sind, geben Sie sie nicht an.

Wenn sich ein Kunde bei forensischen Untersuchungen auf Zeitstempel verlässt, ist es besser, keinen Zeitstempel zu haben als einen falschen Zeitstempel zu haben.

ThreatIntelIndicators

`ThreatIntelIndicators`akzeptiert ein Array von bis zu fünf Threat-Intelligence-Objekten.

Steht für jeden `Type` Eintrag im Kontext der spezifischen Bedrohung. Die zulässigen Werte sind `DOMAIN` | | `EMAIL_ADDRESS` | `HASH_MD5` | `HASH_SHA1` | `HASH_SHA256` | `HASH_SHA512` | `IPV4_ADDRESS` | | `IPV6_ADDRESS` | `MUTEX` | `PROCESS` |`URL`.

Im Folgenden finden Sie einige Beispiele für die Zuordnung von Threat Intelligence-Indikatoren:

- Sie haben einen Prozess gefunden, von dem Sie wissen, dass er mit Cobalt Strike in Verbindung steht. Sie haben das aus FireEye unserem Blog gelernt.

  Setzen Sie `Type` auf `PROCESS`. Erstellen Sie auch ein `Process` Objekt für den Prozess.

- Ihr E-Mail-Filter hat festgestellt, dass jemand ein bekanntes Hash-Paket von einer bekannten bösartigen Domain gesendet hat.

  Erstellen Sie zwei `ThreatIntelIndicator` Objekte. Ein Objekt ist für die`DOMAIN`. Der andere ist für den`HASH_SHA1`.
- Sie haben Malware mit einer Yara-Regel gefunden (Loki, Fenrir, Awss3,). VirusScan BinaryAlert

  `ThreatIntelIndicator`Erstellen Sie zwei Objekte. Eines ist für die Malware. Der andere ist für die`HASH_SHA1`.

Resources

Verwenden Sie für`Resources`, wann immer möglich, unsere bereitgestellten Ressourcentypen und Detailfelder. Security Hub erweitert die ASFF ständig um neue Ressourcen. `<Um ein monatliches Protokoll der Änderungen an ASFF zu erhalten, wenden Sie sic`

Wenn Sie die Informationen nicht in die Detailfelder für einen modellierten Ressourcentyp einpassen können, ordnen Sie die restlichen Details zu. `Details.Other`

Stellen Sie für eine Ressource, die nicht in ASFF modelliert ist, auf ein. `Type` `Other` Nähere Informationen erhalten Sie mit. `Details.Other`

Sie können den `Other` Ressourcentyp auch für AWS Nichtergebnisse verwenden.

ProductFields

Verwenden Sie diese Option nur, `ProductFields` wenn Sie kein anderes kuratiertes Feld für `Resources` oder ein beschreibendes Objekt wie `ThreatIntelIndicatorsNetwork`, oder verwenden können. `Malware`

Wenn Sie es verwenden`ProductFields`, müssen Sie diese Entscheidung genau begründen.

Compliance

Verwenden Sie diese Option nur`Compliance`, wenn sich Ihre Ergebnisse auf die Einhaltung der Vorschriften beziehen.

Security Hub verwendet `Compliance` für die Ergebnisse, die es auf der Grundlage von Kontrollen generiert.

Firewall Manager verwendet `Compliance` für seine Ergebnisse, da sie sich auf die Einhaltung der Vorschriften beziehen.

Eingeschränkte Felder

Diese Felder sind für Kunden vorgesehen, damit sie den Überblick über ihre Untersuchung eines Befundes behalten können.

Ordnen Sie diese Felder oder Objekte nicht zu.

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

Ordnen Sie diese Felder den Feldern zu, die sich im `FindingProviderFields` Objekt befinden. Ordnen Sie sie nicht den Feldern der obersten Ebene zu.

- `Confidence`— Geben Sie nur dann einen Konfidenzwert (0-99) an, wenn Ihr Service über eine ähnliche Funktionalität verfügt oder wenn Sie zu 100% zu Ihrem Ergebnis stehen.
- `Criticality`— Der Kritikalitätswert (0-99) soll die Bedeutung der mit dem Ergebnis verbundenen Ressource zum Ausdruck bringen.
- `RelatedFindings`— Geben Sie nur dann verwandte Ergebnisse an, wenn Sie den Überblick über Ergebnisse behalten können, die sich auf dieselbe Ressource oder denselben Befundtyp beziehen. Um ein verwandtes Ergebnis zu identifizieren, müssen Sie auf die Ergebnis-ID eines Befundes verweisen, das sich bereits in Security Hub befindet.

Richtlinien für die Verwendung der **`BatchImportFindings`** API

Beachten Sie die folgenden Richtlinien, wenn Sie den `BatchImportFindings`API-Vorgang verwenden AWS Security Hub, um Ergebnisse an zu senden.

- Sie müssen `BatchImportFindings`über das Konto anrufen, das mit den Ergebnissen verknüpft ist. Die Kennung des zugehörigen Kontos ist der Wert des `AwsAccountId` Attributs für den Befund.
- Senden Sie den größten Stapel, den Sie können. Security Hub akzeptiert bis zu 100 Ergebnisse pro Stapel, bis zu 240 KB pro Ergebnis und bis zu 6 MB pro Stapel.

- Die Drosselungsrate ist auf 10 TPS pro Konto und Region begrenzt, bei einem Burst-Wert von 30 TPS.
- Sie müssen einen Mechanismus implementieren, um den Stand der Ergebnisse beizubehalten, falls Drosselungen oder Netzwerkprobleme auftreten. Außerdem benötigen Sie den Status der Ergebnisse, damit Sie Aktualisierungen der Ergebnisse einreichen können, wenn ein Ergebnis immer mehr konform ist oder nicht.
- Informationen zur maximalen Länge von Zeichenketten und zu anderen Einschränkungen finden Sie im AWS Security Hub Benutzerhandbuch unter AWS Security Finding Format (ASFF).

Checkliste zur Eignung des Produkts

Die Teams AWS Security Hub und die APN-Partnerteams überprüfen anhand dieser Checkliste, ob die Integration startbereit ist.

ASFF-Zuordnung

Diese Fragen beziehen sich auf die Zuordnung Ihres Ergebnisses zum AWS Security Finding Format (ASFF).

Sind alle Befunddaten des Partners ASFF zugeordnet?

> Ordnen Sie all Ihre Ergebnisse auf irgendeine Weise dem ASFF zu.
>
> Verwenden Sie kuratierte Felder wie modellierte Ressourcentypen,`Network`, `Malware` oder. `ThreatIntelIndicators`
>
> Ordnen Sie alles andere zu `Resource.Details.Other` oder nach `ProductFields` Bedarf zu.

Verwendet der Partner **`Resource.Details`** Felder wie **`AwsEc2instanceAwsS3Bucket`**, und**`Container`**? Definiert der Partner **`Resource.Details.Other`** damit Ressourcendetails, die nicht im ASFF modelliert sind?

> Verwenden Sie in Ihren Ergebnissen nach Möglichkeit die bereitgestellten Felder für kuratierte Ressourcen wie EC2 Instances, S3-Buckets und Sicherheitsgruppen.
>
> Ordnen Sie andere Informationen, die sich auf Ressourcen beziehen, `Resource.Details.Other` nur zu, wenn es keine direkte Übereinstimmung gibt.

Ordnet der Partner Werte zu**`UserDefinedFields`**?

> Verwenden Sie nicht `UserDefinedFields`.

Erwägen Sie, ein anderes kuratiertes Feld zu verwenden, z. B. `Resource.Details.Other` oder`ProductFields`.

Ordnet der Partner Informationen zu**`ProductFields`**, die anderen ASFF-Feldern zugeordnet werden könnten?

Nur `ProductFields` für produktspezifische Informationen wie Versionsinformationen, produktspezifische Schweregrade oder andere Informationen verwenden, die nicht einem kuratierten Feld oder zugeordnet werden können. `Resources.Details.Other`

Importiert der Partner seine eigenen Zeitstempel für? **`FirstObservedAt`**

Der `FirstObservedAt` Zeitstempel soll den Zeitpunkt aufzeichnen, zu dem ein Befund im Produkt beobachtet wurde. Ordnen Sie dieses Feld nach Möglichkeit zu.

Stellt der Partner eindeutige Werte bereit, die für jede Ergebnis-ID generiert werden, mit Ausnahme von Ergebnissen, die er aktualisieren möchte?

Alle Ergebnisse in Security Hub werden anhand der Ergebnis-ID (`Id`Attribut) indexiert. Dieser Wert muss immer eindeutig sein, um sicherzustellen, dass die Ergebnisse nicht versehentlich aktualisiert werden.

Sie sollten auch den Status der Ergebnis-ID beibehalten, um die Ergebnisse zu aktualisieren.

Stellt der Partner einen Wert bereit, der Ergebnisse einer Generator-ID zuordnet?

`GeneratorID`sollte nicht denselben Wert wie die Ergebnis-ID haben.

`GeneratorID`sollte in der Lage sein, Ergebnisse logisch danach zu verknüpfen, was sie generiert hat.

Dabei kann es sich um eine Unterkomponente innerhalb eines Produkts (Produkt A — Sicherheitslücke oder Produkt A — EDR) oder etwas Ähnliches handeln.

Verwendet der Partner die Namespaces der erforderlichen Findingtypen auf eine Weise, die für sein Produkt relevant ist? Verwendet der Partner die empfohlenen Kategorien oder Klassifikatoren für Suchtypen in seinen Suchtypen?

Die Taxonomie des Befundtyps sollte eng mit den Ergebnissen übereinstimmen, die das Produkt generiert.

Die Namespaces der ersten Ebene, die im Security Finding Format beschrieben sind, sind erforderlich AWS .

Sie können benutzerdefinierte Werte für die Namespaces der zweiten und dritten Ebene (Kategorien oder Klassifikatoren) verwenden.

Erfasst der Partner Netzwerkflussinformationen in den **`Network`** Feldern, wenn er über Netzwerkdaten verfügt?

Wenn Ihr Produkt NetFlow Informationen erfasst, ordnen Sie sie dem `Network` Feld zu.

Erfasst der Partner Prozessinformationen (PID) in den **`Process`** Feldern, wenn er über Prozessdaten verfügt?

Wenn Ihr Produkt Prozessinformationen erfasst, ordnen Sie sie dem `Process` Feld zu.

Erfasst der Partner Malware-Informationen in den **`Malware`** Feldern, wenn er über Malware-Daten verfügt?

Wenn Ihr Produkt Malware-Informationen erfasst, ordnen Sie diese dem `Malware` Feld zu.

Erfasst der Partner Bedrohungsinformationen vor Ort**`ThreatIntelIndicators`**, wenn er über Bedrohungsdaten verfügt?

Wenn Ihr Produkt Bedrohungsinformationen erfasst, ordnen Sie diese dem `ThreatIntelIndicators` Feld zu.

Gibt der Partner eine Vertrauensbewertung für die Ergebnisse ab? Falls ja, wird eine Begründung angegeben?

Wann immer Sie dieses Feld verwenden, geben Sie in Ihrer Dokumentation und Ihrem Manifest eine Begründung an.

Verwendet der Partner im Ergebnis eine kanonische ID oder einen ARN für die Ressourcen-ID?

Bei der Identifizierung von AWS Ressourcen empfiehlt es sich, den ARN zu verwenden. Wenn kein ARN verfügbar ist, verwenden Sie die kanonische Ressourcen-ID.

Einrichtung und Funktion der Integration

Diese Fragen beziehen sich auf den Aufbau und die day-to-day Funktion der Integration.

Stellt der Partner eine infrastructure-as-code (IaC-) Vorlage für die Implementierung der Integration mit Security Hub zur Verfügung, z. B. Terraform,, AWS CloudFormation oder? AWS Cloud Development Kit (AWS CDK)

Für Integrationen, die Ergebnisse aus dem Kundenkonto senden oder CloudWatch Ereignisse verwenden, um Ergebnisse zu nutzen, ist eine IaC-Vorlage erforderlich.

AWS CloudFormation wird bevorzugt, es kann aber auch AWS CDK Terraform verwendet werden.

Hat das Partnerprodukt auf seiner Konsole eine Einrichtung mit einem Klick für die Integration mit Security Hub?

Einige Partnerprodukte verwenden einen Schalter oder einen ähnlichen Mechanismus in ihrem Produkt, um die Integration zu aktivieren. Dies kann die automatische Bereitstellung von Ressourcen und Berechtigungen beinhalten. Wenn Sie Ergebnisse von einem Produktkonto aus senden, ist die Einrichtung mit einem Klick die bevorzugte Methode.

Sendet der Partner nur wertvolle Ergebnisse?

Generell sollten Sie nur Ergebnisse, die einen Sicherheitswert haben, an Security Hub-Kunden senden.

Security Hub ist kein allgemeines Protokollverwaltungstool. Sie sollten nicht jedes mögliche Protokoll an Security Hub senden.

Hat der Partner eine Schätzung abgegeben, wie viele Ergebnisse er pro Tag und Kunde senden wird und mit welcher Häufigkeit (Durchschnitt und Burst)?

Eine Reihe einzigartiger Ergebnisse wird verwendet, um die Auslastung von Security Hub zu berechnen. Ein eindeutiges Ergebnis ist definiert als ein Ergebnis, bei dem sich die ASFF-Zuordnung von einem anderen Befund unterscheidet.

Wenn beispielsweise nur ein Ergebnis `ThreatIntelIndicators` und ein anderes nur aufgefüllt wird`Resources.Details.AWSEc2Instance`, handelt es sich um zwei eindeutige Ergebnisse.

Verfügt der Partner über eine elegante Art, 4xx- und 5xx-Fehler zu behandeln, sodass sie nicht gedrosselt werden und alle Ergebnisse zu einem späteren Zeitpunkt gesendet werden können?

Der API-Vorgang weist derzeit eine Burst-Rate von 30—50 TPS auf. `BatchImportFindings` Wenn 4xx- oder 5xx-Fehler zurückgegeben werden, müssen Sie den Status dieser fehlgeschlagenen Ergebnisse beibehalten, damit Sie sie später vollständig wiederholen können. Sie können dies über eine Warteschlange für unzustellbare Nachrichten oder über andere AWS Messaging-Dienste wie Amazon SNS oder Amazon SQS tun.

Behält der Partner den Status seiner Ergebnisse bei, sodass er weiß, dass er Ergebnisse archivieren kann, die nicht mehr vorhanden sind?

Wenn Sie beabsichtigen, Ergebnisse zu aktualisieren, indem Sie die ursprüngliche Fund-ID überschreiben, müssen Sie über einen Mechanismus verfügen, um den Status beizubehalten, sodass die richtigen Informationen für den richtigen Befund aktualisiert werden.

Wenn Sie Ergebnisse angeben, verwenden Sie den `BatchUpdateFindings`Vorgang nicht, um Ergebnisse zu aktualisieren. Dieser Vorgang sollte nur von Kunden verwendet werden. Sie verwenden ihn nur `BatchUpdateFindings`, wenn Sie die Ergebnisse untersuchen und entsprechende Maßnahmen ergreifen.

Behandelt der Partner Wiederholungsversuche so, dass zuvor gesendete, erfolgreich gesendete Ergebnisse nicht beeinträchtigt werden?

Sie sollten über einen Mechanismus verfügen, mit dem das ursprüngliche Ergebnis IDs im Fehlerfall beibehalten wird, sodass Sie erfolgreiche Ergebnisse nicht duplizieren oder irrtümlich überschreiben.

Aktualisiert der Partner die Ergebnisse, indem er den **`BatchImportFindings`** Vorgang mit der Finde-ID der vorhandenen Ergebnisse aufruft?

Um ein Ergebnis zu aktualisieren, müssen Sie das vorhandene Ergebnis überschreiben, indem Sie dieselbe Ergebnis-ID einreichen.

Der `BatchUpdateFindings`Vorgang sollte nur von Kunden verwendet werden.

Aktualisiert der Partner die Ergebnisse mithilfe der **`BatchUpdateFindings`** API?

Wenn Sie aufgrund der Ergebnisse Maßnahmen ergreifen, können Sie den `BatchUpdateFindings`Vorgang verwenden, um bestimmte Felder zu aktualisieren.

Stellt der Partner Informationen zur Latenz zwischen der Erstellung eines Ergebnisses und dem Senden von seinem Produkt an Security Hub zur Verfügung?

Sie sollten die Latenz minimieren, um sicherzustellen, dass Kunden die Ergebnisse so schnell wie möglich im Security Hub sehen.

Diese Informationen sind im Manifest erforderlich.

Wenn die Architektur des Partners darin besteht, Ergebnisse von einem Kundenkonto an Security Hub zu senden, hat er dies erfolgreich nachgewiesen? Wenn die Architektur des Partners Ergebnisse von seinem eigenen Konto an Security Hub senden soll, hat er dies erfolgreich nachgewiesen?

Während des Tests müssen die Ergebnisse erfolgreich von einem Konto gesendet werden, das Ihnen gehört und das sich von dem für den Produkt-ARN bereitgestellten Konto unterscheidet.

Durch das Senden eines Ergebnisses über das Konto des Produkt-ARN-Besitzers können bestimmte Fehlerausnahmen aus den API-Vorgängen umgangen werden.

Stellt der Partner Security Hub einen Heartbeat-Beat zur Verfügung?

Um nachzuweisen, dass Ihre Integration korrekt funktioniert, sollten Sie einen Heartbeat-Befund senden. Der Heartbeat-Befund wird alle fünf Minuten gesendet und verwendet den Befundtyp. `Heartbeat`

Dies ist wichtig, wenn Sie Ergebnisse von einem Produktkonto aus senden.

Hat der Partner während des Tests das Konto des Security Hub Hub-Produktteams integriert?

Während der Validierung vor der Produktion sollten Sie Fundbeispiele an das AWS Konto des Security Hub Hub-Produktteams senden. Diese Beispiele zeigen, dass die Ergebnisse korrekt gesendet und zugeordnet wurden.

Dokumentation

Diese Fragen beziehen sich auf die von Ihnen bereitgestellte Dokumentation der Integration.

Hostet der Partner seine Dokumentation auf einer speziellen Website?

Die Dokumentation sollte auf Ihrer Website als statische Webseite, Wiki, Read the Docs oder in einem anderen speziellen Format gehostet werden.

Das Hosten der Dokumentation auf erfüllt GitHub nicht die Anforderungen an eine spezielle Website.

Enthält die Partnerdokumentation Anweisungen zur Einrichtung der Security Hub Hub-Integration?

Sie können die Integration entweder mithilfe einer IaC-Vorlage oder mithilfe einer konsolenbasierten Ein-Klick-Integration einrichten.

Enthält die Partnerdokumentation eine Beschreibung ihres Anwendungsfalls?

Der Anwendungsfall, den Sie im Manifest angeben, sollte auch in der Dokumentation beschrieben werden

Enthält die Partnerdokumentation eine Begründung für die von ihnen übermittelten Ergebnisse?

Sie sollten die Art der von Ihnen gesendeten Ergebnisse begründen.

Beispielsweise kann Ihr Produkt Ergebnisse für Sicherheitslücken, Malware und Antivirenprogramme liefern, aber Sie senden die Ergebnisse von Schwachstellen und Malware

nur an Security Hub. In diesem Fall müssen Sie begründen, warum Sie keine Antiviren-Ergebnisse senden.

Enthält die Partnerdokumentation eine Begründung dafür, wie der Partner seine Ergebnisse ASFF zuordnet?

Sie sollten die Gründe für die Zuordnung der systemeigenen Ergebnisse eines Produkts zu ASFF angeben. Kunden möchten wissen, wo sie nach bestimmten Produktinformationen suchen können.

Enthält die Partnerdokumentation Hinweise dazu, wie der Partner die Ergebnisse aktualisiert, falls er die Ergebnisse aktualisiert?

Informieren Sie Kunden darüber, wie Sie den Status beibehalten, die Idempotenz sicherstellen und die Ergebnisse mit Informationen überschreiben. up-to-date

Wird in der Partnerdokumentation beschrieben, wie Latenz festgestellt wird?

Minimiere die Latenz, um sicherzustellen, dass Kunden die Ergebnisse so schnell wie möglich im Security Hub sehen.

Diese Informationen sind im Manifest erforderlich.

Beschreibt die Partnerdokumentation, wie ihre Schweregradbewertung der ASFF-Schweregradbewertung entspricht?

Geben Sie Informationen darüber an, wie Sie `Severity.Original` sich `Severity.Label` zuordnen.

Wenn es sich bei Ihrem Schweregrad beispielsweise um einen Buchstabengrad (A, B, C) handelt, sollten Sie angeben, wie Sie den Schweregrad dem Schweregrad zuordnen.

Enthält die Partnerdokumentation eine Begründung für Konfidenzbewertungen?

Wenn Sie Konfidenzwerte angeben, sollten diese Werte nach einer Rangfolge geordnet werden.

Wenn Sie statisch aufgefüllte Konfidenzwerte oder Zuordnungen verwenden, die auf künstlicher Intelligenz oder maschinellem Lernen basieren, sollten Sie zusätzlichen Kontext angeben.

Ist in der Partnerdokumentation angegeben, welche Regionen der Partner unterstützt und welche nicht?

Notieren Sie sich Regionen, die unterstützt werden oder nicht, damit Kunden wissen, in welchen Regionen sie eine Integration nicht versuchen sollten.

Informationen zur Produktkarte

Diese Fragen beziehen sich auf die Karte für das Produkt, die auf der Seite Integrationen der Security Hub Hub-Konsole angezeigt wird.

Ist die angegebene AWS Konto-ID gültig und besteht sie aus 12 Ziffern?

Konto-Identifikatoren sind 12-stellig. Wenn eine Konto-ID weniger als 12 Ziffern enthält, ist der Produkt-ARN nicht gültig.

Enthält die Produktbeschreibung 200 oder weniger Zeichen?

Die im JSON-Format innerhalb des Manifests angegebene Produktbeschreibung sollte nicht länger als 200 Zeichen sein, einschließlich Leerzeichen.

Führt der Konfigurationslink zur Dokumentation für die Integration?

Der Konfigurationslink sollte zu Ihrer Online-Dokumentation führen. Er sollte nicht zu Ihrer Hauptwebsite oder zu Marketingseiten führen.

Führt der Kauflink (falls angegeben) zum AWS Marketplace Angebot für das Produkt?

Wenn Sie einen Kauflink angeben, muss es sich um einen AWS Marketplace Eintrag handeln. Security Hub akzeptiert keine Kauflinks, die nicht von gehostet werden AWS.

Beschreiben die Produktkategorien das Produkt korrekt?

Im Manifest können Sie bis zu drei Produktkategorien angeben. Diese sollten mit dem JSON übereinstimmen und dürfen nicht benutzerdefiniert sein. Sie können nicht mehr als drei Produktkategorien angeben.

Sind die Firmen- und Produktnamen gültig und korrekt?

Der Firmenname muss 16 oder weniger Zeichen lang sein.

Der Produktname muss 24 oder weniger Zeichen lang sein.

Der Produktname in der JSON-Produktkarte muss mit dem Namen im Manifest übereinstimmen.

Informationen zu Marketingzwecken

Diese Fragen beziehen sich auf das Marketing für die Integration.

Hat die Produktbeschreibung für die Security Hub-Partnerseite eine Länge von 700 Zeichen, einschließlich Leerzeichen?

Die Security Hub-Partnerseite akzeptiert nur bis zu 700 Zeichen, einschließlich Leerzeichen.

Das Team wird längere Beschreibungen bearbeiten.

Ist das Logo der Security Hub-Partnerseite nicht größer als 600 x 300 px?

Stellen Sie eine öffentlich zugängliche URL mit einem Firmenlogo in PNG oder JPG bereit, das nicht größer als 600 x 300 Pixel ist.

Führt der Hyperlink Weitere Informationen auf der Security Hub-Partnerseite zur speziellen Webseite des Partners über die Integration?

Der Link Weitere Informationen sollte nicht zur Haupt-Website des Partners oder zu den Dokumentationsinformationen führen.

Dieser Link sollte immer zu einer speziellen Webseite mit Marketinginformationen über die Integration führen.

Stellt der Partner eine Demo oder ein Anleitungsvideo zur Verwendung der Integration zur Verfügung?

Ein Demo- oder Integrationsvideo ist optional, wird aber empfohlen.

Wird zusammen mit dem AWS Partner und seinem Partner Development Manager oder einem Vertreter für Partnerentwicklung ein Blogbeitrag von Partner Network veröffentlicht?

AWS Blogbeiträge des Partnernetzwerks sollten im Voraus mit dem Partnerentwicklungsmanager oder dem Beauftragten für Partnerentwicklung abgestimmt werden.

Diese sind unabhängig von allen Blogbeiträgen, die Sie selbst erstellen.

Rechnen Sie mit einer Vorlaufzeit von 4—6 Wochen. Diese Bemühungen sollten gestartet werden, nachdem die Tests mit dem privaten Produkt ARN abgeschlossen sind.

Wird eine von Partnern geleitete Pressemitteilung veröffentlicht?

Sie können mit Ihrem Partner Development Manager oder einem Vertreter für Partnerentwicklung zusammenarbeiten, um ein Angebot vom VP of External Security Services zu erhalten. Sie können dieses Zitat in Ihrer Pressemitteilung verwenden.

Wird ein von Partnern geführter Blogbeitrag veröffentlicht?

Sie können Ihre eigenen Blogbeiträge erstellen, um die Integration außerhalb des AWS Partner Network-Blogs vorzustellen.

Wird ein von Partnern geführtes Webinar veröffentlicht?

Sie können Ihre eigenen Webinare erstellen, um die Integration zu präsentieren.

Wenn Sie Unterstützung vom Security Hub Hub-Team benötigen, arbeiten Sie nach Abschluss der Tests mit dem privaten Produkt-ARN mit dem Produktteam zusammen.

Hat der Partner Unterstützung in den sozialen Medien angefordert AWS?

Nach Ihrer Veröffentlichung können Sie gemeinsam mit dem AWS Marketingleiter für Sicherheit die AWS offiziellen Social-Media-Kanäle nutzen, um Einzelheiten zu Ihren Webinaren auszutauschen.

AWS Security Hub Häufig gestellte Fragen für Partner

Im Folgenden finden Sie häufig gestellte Fragen zum Einrichten und Verwalten einer Integration mit AWS Security Hub.

1. Was sind die Vorteile der Security Hub Hub-Integration?
   - Kundenzufriedenheit — Der Hauptgrund für die Integration mit Security Hub ist, dass Sie Kundenanfragen dazu haben.

     Security Hub ist das Sicherheits- und Compliance-Center für AWS Kunden. Es ist als erste Anlaufstelle konzipiert, an die sich AWS Sicherheits- und Compliance-Experten täglich wenden, um sich über ihren Sicherheits- und Compliance-Status zu informieren.

     Hören Sie Ihren Kunden zu. Sie werden Ihnen sagen, ob sie Ihre Ergebnisse im Security Hub sehen möchten.
   - Entdeckungsmöglichkeiten — Wir bewerben Partner mit zertifizierten Integrationen in der Security Hub Hub-Konsole, einschließlich Links zu ihren AWS Marketplace Angeboten. Dies ist eine hervorragende Möglichkeit für Kunden, neue Sicherheitsprodukte zu entdecken.
   - Marketingmöglichkeiten — Anbieter mit zugelassenen Integrationen können an Webinaren teilnehmen, Pressemitteilungen herausgeben, Übersichtsblätter erstellen und ihren Kunden ihre Integrationen vorführen. AWS
2. Welche Arten von Partnern gibt es?
   - Partner, die Ergebnisse an Security Hub senden
   - Partner, die Ergebnisse von Security Hub erhalten
   - Partner, die Ergebnisse sowohl senden als auch empfangen
   - Beratungspartner, die Kunden bei der Einrichtung, Anpassung und Verwendung von Security Hub in ihrer Umgebung unterstützen
3. Wie funktioniert eine Partnerintegration mit Security Hub auf hohem Niveau?

   Sie sammeln Ergebnisse in einem Kundenkonto oder in Ihrem eigenen AWS Konto und wandeln das Format der Ergebnisse in das AWS Security Finding Format (ASFF) um. Anschließend übertragen Sie diese Ergebnisse an den entsprechenden regionalen Security Hub Hub-Endpunkt.

   Sie können CloudWatch Ereignisse auch verwenden, um Ergebnisse von Security Hub zu erhalten.

4. Was sind die grundlegenden Schritte für den Abschluss einer Integration mit Security Hub?
   a. Reichen Sie Ihre Partner-Manifestinformationen ein.
   b. Erhalten Sie ein Produkt ARNs zur Verwendung mit Security Hub, wenn Sie Ergebnisse an Security Hub senden möchten.
   c. Ordnen Sie Ihre Ergebnisse ASFF zu. Siehe the section called “Richtlinien für die ASFF-Zuordnung”.
   d. Definieren Sie Ihre Architektur für das Senden von Ergebnissen an und das Empfangen von Ergebnissen von Security Hub. Folgen Sie den Grundsätzen, die unter beschrieben sind. the section called “Grundsätze für die Erstellung und Aktualisierung von Ergebnissen”
   e. Erstellen Sie ein Bereitstellungs-Framework für Kunden. AWS CloudFormation Skripte können diesem Zweck beispielsweise dienen.
   f. Dokumentieren Sie Ihr Setup und stellen Sie Ihren Kunden Konfigurationsanweisungen zur Verfügung.
   g. Definieren Sie alle benutzerdefinierten Erkenntnisse (Korrelationsregeln), die Kunden für Ihr Produkt verwenden können.
   h. Demonstrieren Sie dem Security Hub Hub-Team Ihre Integration.
   i. Reichen Sie Marketinginformationen zur Genehmigung ein (Sprache der Website, Pressemitteilung, Architekturfolie, Video, Übersichtsblatt).
5. Wie wird das Partnermanifest eingereicht? Und für AWS Dienste, die Ergebnisse an Security Hub senden?

   Um die Manifestinformationen an das Security Hub Hub-Team zu senden, verwenden Sie `<securityhub-partners@amazon.com>`.

   Das Produkt wird Ihnen ARNs innerhalb von sieben Kalendertagen ausgestellt.
6. Welche Arten von Ergebnissen sollte ich an Security Hub senden?

   Die Preisgestaltung von Security Hub basiert teilweise auf der Anzahl der aufgenommenen Ergebnisse. Aus diesem Grund sollten Sie davon absehen, Ergebnisse zu versenden, die für Kunden keinen Mehrwert bieten.

   Beispielsweise senden einige Anbieter von Vulnerability Management nur Ergebnisse mit einem Common Vulnerability Scoring System (CVSS) -Score von 3 oder mehr von möglichen 10 Punkten.
7. Was sind die verschiedenen Methoden für mich, um Ergebnisse an Security Hub zu senden?

Dies sind die wichtigsten Ansätze:

- Mithilfe der `BatchImportFindings`Operation senden Sie Ergebnisse von ihrem eigenen AWS Konto aus.
- Mithilfe des `BatchImportFindings`Vorgangs senden Sie Ergebnisse aus dem Kundenkonto heraus. Sie könnten Ansätze zur Rollenübernahme verwenden, diese Ansätze sind jedoch nicht erforderlich.

Allgemeine Richtlinien zur Verwendung finden Sie unter `BatchImportFindings`. the section called "Richtlinien für die Verwendung der `BatchImportFindings` API"

8. Wie sammle ich meine Ergebnisse und übertrage sie an einen regionalen Security Hub Hub-Endpunkt?

   Partner haben dafür unterschiedliche Ansätze verwendet, da dies stark von der Architektur Ihrer Lösung abhängt.

   Einige Partner erstellen beispielsweise eine Python-App, die als AWS CloudFormation Skript bereitgestellt werden kann. Das Skript sammelt die Ergebnisse des Partners aus der Kundenumgebung, wandelt sie in ASFF um und sendet sie an den regionalen Endpunkt von Security Hub.

   Andere Partner entwickeln einen umfassenden Assistenten, mit dem der Kunde seine Ergebnisse mit nur einem Klick an Security Hub weiterleiten kann.

9. Woher weiß ich, wann ich anfangen muss, Ergebnisse an Security Hub zu senden?

   Security Hub unterstützt die teilweise Batch-Autorisierung für den `BatchImportFindings`API-Vorgang, sodass Sie alle Ihre Ergebnisse für alle Ihre Kunden an Security Hub senden können.

   Wenn einige Ihrer Kunden Security Hub noch nicht abonniert haben, nimmt Security Hub diese Ergebnisse nicht auf. Es nimmt nur autorisierte Ergebnisse auf, die im Batch enthalten sind.

10. Welche Schritte muss ich ausführen, um Ergebnisse an die Security Hub Hub-Instanz eines Kunden zu senden?

    a. Stellen Sie sicher, dass die richtigen IAM-Richtlinien vorhanden sind.

    b. Aktivieren Sie ein Produktabonnement (Ressourcenrichtlinien) für die Konten. Verwenden Sie entweder den `EnableImportFindingsForProduct`API-Vorgang oder die Seite Integrationen. Der Kunde kann dies tun, oder Sie können kontoübergreifende Rollen verwenden, um im Namen des Kunden zu handeln.

c. Stellen Sie sicher, dass es sich bei dem Ergebnis um den öffentlichen ARN Ihres Produkts handelt. `ProductArn`

d. Stellen Sie sicher, dass es sich bei dem Ergebnis um die Konto-ID des Kunden handelt. `AwsAccountId`

e. Stellen Sie sicher, dass Ihre Ergebnisse keine fehlerhaften Daten gemäß dem AWS Security Finding Format (ASFF) enthalten. Beispielsweise sind Pflichtfelder ausgefüllt und es gibt keine ungültigen Werte.

f. Senden Sie die Ergebnisse stapelweise an den richtigen regionalen Endpunkt.

11. Welche IAM-Berechtigungen müssen vorhanden sein, damit ich Ergebnisse senden kann?

IAM-Richtlinien müssen für den IAM-Benutzer oder die IAM-Rolle konfiguriert werden, der oder die andere API-Aufrufe aufruft `BatchImportFindings`.

Der einfachste Test besteht darin, dies von einem Administratorkonto aus durchzuführen. Sie können diese auf `action: 'securityhub:BatchImportFindings'` und `resource: <productArn and/or productSubscriptionArn>` beschränken.

Ressourcen in demselben Konto können mit IAM-Richtlinien konfiguriert werden, ohne dass Ressourcenrichtlinien erforderlich sind.

Um auszuschließen, dass der Anrufer von Probleme mit der IAM-Richtlinie hat `BatchImportFindings`, legen Sie die IAM-Richtlinie für den Anrufer wie folgt fest:

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

Vergewissern Sie sich, dass es keine `Deny` Richtlinien für den Anrufer gibt. Nachdem Sie es damit zum Laufen gebracht haben, können Sie die Richtlinie auf Folgendes beschränken:

```
{
    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. Was ist ein Produktabonnement?

    Um Erkenntnisse aus einem bestimmten Partnerprodukt zu erhalten, muss der Kunde (oder der Partner mit kundenübergreifenden Rollen, der im Namen des Kunden arbeitet) ein Produktabonnement abschließen. Dazu verwenden sie von der Konsole aus die Seite Integrationen. Um dies von der API aus zu tun, verwenden sie die `EnableImportFindingsForProduct`API-Operation.

    Das Produktabonnement erstellt eine Ressourcenrichtlinie, die den Empfang oder Versand der Ergebnisse des Partners durch den Kunden autorisiert. Details hierzu finden Sie unter Anwendungsfälle und Berechtigungen.

    Security Hub bietet die folgenden Arten von Ressourcenrichtlinien für Partner:

    - `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
    - `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

    Während des Partner-Onboarding-Prozesses können Sie entweder eine oder beide Arten von Richtlinien anfordern.

    Mit `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` können Sie Ergebnisse nur von dem Konto an Security Hub senden, das in Ihrem Produkt-ARN aufgeführt ist.

    Mit `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` können Sie nur Ergebnisse von dem Kundenkonto senden, das Sie abonniert hat.

13. Angenommen, ein Kunde hat ein Administratorkonto erstellt und einige Mitgliedskonten hinzugefügt. Muss der Kunde jedes Mitgliedskonto bei mir abonnieren? Oder abonniert der Kunde nur über das Administratorkonto, und ich kann dann Ergebnisse zu Ressourcen in allen Mitgliedskonten senden?

    Bei dieser Frage wird gefragt, ob die Berechtigungen für alle Mitgliedskonten auf der Grundlage der Registrierung des Administratorkontos erstellt wurden.

    Der Kunde muss für jedes Konto ein Produktabonnement abschließen. Sie können dies programmgesteuert über die API tun.

14. Was ist mein Produkt-ARN?

Ihr Produkt-ARN ist Ihre eindeutige Kennung, die Security Hub für Sie generiert und die Sie verwenden, um Ergebnisse einzureichen. Sie erhalten für jedes Produkt, das Sie in Security Hub integrieren, einen Produkt-ARN. Der richtige Produkt-ARN muss in jedem Ergebnis enthalten sein, das Sie an Security Hub senden. Ergebnisse ohne das Produkt ARN werden gelöscht. Das Produkt ARN verwendet das folgende Format:

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

Ein Beispiel:

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

Sie erhalten einen Produkt-ARN für jede Region, in der Security Hub bereitgestellt wird. Die Konto-ID, das Unternehmen und die Produktnamen werden durch die von Ihnen eingereichten Partnermanifeste bestimmt. Sie ändern niemals die Informationen, die mit Ihrem Produkt-ARN verknüpft sind, mit Ausnahme des Regionalcodes. Der Regionalcode muss mit der Region übereinstimmen, für die Sie Ergebnisse einreichen.

Ein häufiger Fehler besteht darin, die Konto-ID so zu ändern, dass sie dem Konto entspricht, von dem aus Sie gerade arbeiten. Die Konto-ID ändert sich nicht. Im Rahmen der Einreichung des Manifests reichen Sie eine Konto-ID für Ihr Privatkonto ein. Diese Konto-ID ist mit Ihrem Produkt-ARN ARN.

Wenn Security Hub in neuen Regionen eingeführt wird, verwendet es automatisch die Standard-Regionscodes, um Ihr Produkt ARNs für diese Regionen zu generieren.

Jedes Konto wird außerdem automatisch mit einem privaten Produkt-ARN ARN. Sie können diesen ARN verwenden, um den Import von Ergebnissen in Ihrem eigenen Entwicklungskonto zu testen, bevor Sie Ihren offiziellen öffentlichen Produkt-ARN erhalten.

15. Welches Format sollte verwendet werden, um Ergebnisse an Security Hub zu senden?

Die Ergebnisse müssen im AWS Security Finding Format (ASFF) bereitgestellt werden. Einzelheiten finden Sie unter AWS Security Finding Format (ASFF) im AWS Security Hub Benutzerhandbuch.

Es wird erwartet, dass alle Informationen in Ihren systemeigenen Ergebnissen vollständig in der ASFF wiedergegeben werden. Benutzerdefinierte Felder wie `ProductFields` und

`Resource.Details.Other` ermöglichen es Ihnen, Daten zuzuordnen, die nicht genau in die vordefinierten Felder passen.

16. Welcher regionale Endpunkt ist der richtige zu verwendende?

    Sie müssen die Ergebnisse an den regionalen Security Hub Hub-Endpunkt senden, der mit dem Kundenkonto verknüpft ist.

17. Wo finde ich die Liste der regionalen Endpunkte?

    Sehen Sie sich die Liste der Security Hub Hub-Endpunkte an.

18. Kann ich regionsübergreifende Ergebnisse einreichen?

    Security Hub unterstützt noch nicht die regionsübergreifende Übermittlung von Ergebnissen für native AWS Dienste wie Amazon GuardDuty, Amazon Macie und Amazon Inspector. Wenn Ihr Kunde dies zulässt, hindert Sie Security Hub nicht daran, Ergebnisse aus verschiedenen Regionen einzureichen.

    In diesem Sinne können Sie einen regionalen Endpunkt von überall aus aufrufen, und die Ressourceninformationen des ASFF müssen nicht mit der Region des Endpunkts übereinstimmen. Sie `ProductArn` müssen jedoch mit der Region des Endpunkts übereinstimmen.

19. Welche Regeln und Richtlinien gelten für den Versand von Befundstapeln?

    Sie können bis zu 100 Ergebnisse oder 240 KB in einem einzigen Anruf von `BatchImportFindings`stapeln. Stellen Sie eine Warteschlange auf und stapeln Sie so viele Ergebnisse wie möglich bis zu diesem Limit.

    Sie können eine Reihe von Ergebnissen aus verschiedenen Konten stapeln. Wenn jedoch eines der Konten im Stapel nicht bei Security Hub abonniert ist, schlägt der gesamte Batch fehl. Dies ist eine Einschränkung des API Gateway Gateway-Baseline-Autorisierungsmodells.

    Siehe the section called “Richtlinien für die Verwendung der `BatchImportFindings` API”.

20. Kann ich Updates zu Ergebnissen senden, die ich erstellt habe?

    Ja, wenn Sie ein Ergebnis mit demselben Produkt-ARN und derselben Ergebnis-ID einreichen, werden die vorherigen Daten für dieses Ergebnis überschrieben. Beachten Sie, dass alle Daten überschrieben werden. Sie sollten daher ein vollständiges Ergebnis einreichen.

    Den Kunden werden sowohl neue Ergebnisse als auch Aktualisierungen der Ergebnisse in Rechnung gestellt.

21. Kann ich Updates zu Ergebnissen senden, die von einer anderen Person erstellt wurden?

    Ja, wenn der Kunde Ihnen Zugriff auf den `BatchUpdateFindings`API-Vorgang gewährt, können Sie mit diesem Vorgang bestimmte Felder aktualisieren. Dieser Vorgang ist für die Nutzung durch Kunden SIEMs, Ticketsysteme und SOAR-Plattformen (Security Orchestration, Automation and Response) konzipiert.

22. Wie veralten die Ergebnisse?

    Security Hub veraltert Ergebnisse 90 Tage nach dem letzten Aktualisierungsdatum. Nach Ablauf dieser Zeit werden die veralteten Ergebnisse aus dem Security Hub-Cluster gelöscht. OpenSearch

    Wenn Sie ein Ergebnis mit derselben Ergebnis-ID aktualisieren und es veraltet ist, wird ein neues Ergebnis in Security Hub erstellt.

    Kunden können CloudWatch Events verwenden, um Ergebnisse aus Security Hub zu übertragen. Auf diese Weise können alle Ergebnisse an Ziele nach Wahl des Kunden gesendet werden.

    Im Allgemeinen empfiehlt Security Hub, dass Sie alle 90 Tage neue Ergebnisse erstellen und die Ergebnisse nicht für immer aktualisieren.

23. Welche Drosselungen führt Security Hub ein?

    Security Hub drosselt `GetFindings` API-Aufrufe, da der empfohlene Ansatz für den Zugriff auf Ergebnisse die Verwendung von CloudWatch Ereignissen ist.

    Security Hub implementiert keine weitere Drosselung für interne Dienste, Partner oder Kunden, die über die durch API Gateway- und Lambda-Aufrufe erzwungenen Einschränkungen hinausgehen.

24. Wie hoch ist die Aktualität, Latenz SLAs oder Erwartungen bei Ergebnissen, die von Quelldiensten an Security Hub gesendet werden?

    Ziel ist es, sowohl für erste Ergebnisse als auch für Aktualisierungen der Ergebnisse so nahe wie möglich in Echtzeit zu sein. Sie sollten die Ergebnisse innerhalb von fünf Minuten nach ihrer Erstellung an Security Hub senden.

25. Wie kann ich Ergebnisse von Security Hub erhalten?

    Verwenden Sie eine der folgenden Methoden, um Ergebnisse zu erhalten.

    - Alle Ergebnisse werden automatisch an CloudWatch Events gesendet. Ein Kunde kann spezifische Regeln für CloudWatch Ereignisse erstellen, um Ergebnisse an bestimmte Ziele

zu senden, z. B. an ein SIEM oder einen S3-Bucket. Diese Funktion ersetzte den alten `GetFindings` API-Betrieb.

- Verwenden Sie CloudWatch Ereignisse für benutzerdefinierte Aktionen. Security Hub ermöglicht es Kunden, bestimmte Ergebnisse oder Gruppen von Ergebnissen aus der Konsole auszuwählen und entsprechende Maßnahmen zu ergreifen. Sie können die Ergebnisse beispielsweise an ein SIEM, ein Ticketsystem, eine Chat-Plattform oder einen Workflow zur Problembehebung senden. Dies wäre Teil eines Alert-Triage-Workflows, den ein Kunde innerhalb von Security Hub durchführt. Diese Aktionen werden als benutzerdefinierte Aktionen bezeichnet.

  Wenn ein Benutzer eine benutzerdefinierte Aktion auswählt, wird ein CloudWatch Ereignis für diese spezifischen Ergebnisse erstellt. Sie könnten diese Funktion nutzen und Regeln und Ziele für CloudWatch Ereignisse erstellen, die ein Kunde als Teil einer benutzerdefinierten Aktion verwenden kann. Beachten Sie, dass diese Funktion nicht verwendet wird, um automatisch alle Ergebnisse eines bestimmten Typs oder einer bestimmten Klasse an CloudWatch Events zu senden. Es ist Sache eines Benutzers, aufgrund bestimmter Ergebnisse Maßnahmen zu ergreifen.

  Sie können die API-Operationen für benutzerdefinierte Aktionen verwenden`CreateActionTarget`, um z. B. automatisch verfügbare Aktionen für Ihr Produkt zu erstellen (z. B. mithilfe von AWS CloudFormation Vorlagen). Sie würden auch API-Operationen für CloudWatch Ereignisregeln verwenden, um entsprechende CloudWatch Ereignisregeln zu erstellen, die der benutzerdefinierten Aktion zugeordnet sind. Mithilfe von AWS CloudFormation Vorlagen können Sie auch Regeln für CloudWatch Ereignisse erstellen, um automatisch alle Ergebnisse oder alle Ergebnisse mit bestimmten Merkmalen aus Security Hub aufzunehmen.

26. Was sind die Voraussetzungen für einen Managed Security Service Provider (MSSP), um ein Security Hub-Partner zu werden?

    Sie müssen nachweisen, wie Security Hub im Rahmen Ihrer Servicebereitstellung für Kunden verwendet wird.

    Sie sollten über eine Benutzerdokumentation verfügen, die Ihre Verwendung von Security Hub erklärt.

    Wenn es sich bei dem MSSP um einen Suchdienstleister handelt, muss er nachweisen, dass er die Ergebnisse an Security Hub gesendet hat.

Wenn der MSSP nur Ergebnisse von Security Hub erhält, muss er mindestens über eine AWS CloudFormation Vorlage verfügen, um die entsprechenden CloudWatch Event-Regeln einzurichten.

27. Was sind die Voraussetzungen, damit ein APN-Beratungspartner, der kein MSSP ist, ein Security Hub-Partner werden kann?

    Wenn Sie ein APN-Beratungspartner sind, können Sie ein Security Hub-Partner werden. Sie sollten zwei private Fallstudien darüber einreichen, wie Sie einem bestimmten Kunden dabei geholfen haben, Folgendes zu tun.

    - Richten Sie Security Hub mit IAM-Berechtigungen ein, die der Kunde benötigt.
    - Mithilfe der Konfigurationsanweisungen auf der Partnerseite in der Konsole können Sie bereits integrierte ISV-Lösungen (Independent Software Vendor) mit Security Hub verbinden.
    - Unterstützen Sie Kunden mit maßgeschneiderten Produktintegrationen.
    - Gewinnen Sie maßgeschneiderte Erkenntnisse, die für die Kundenbedürfnisse und Datensätze relevant sind.
    - Erstellen Sie benutzerdefinierte Aktionen.
    - Erstellen Sie Playbooks zur Problembehebung.
    - Erstellen Sie Schnellstarts, die den Compliance-Standards von Security Hub entsprechen. Diese müssen vom Security Hub Hub-Team validiert werden.

    Fallstudien müssen nicht öffentlich zugänglich sein.

28. Welche Anforderungen gelten für die Implementierung meiner Integration mit Security Hub bei meinen Kunden?

    Die Integrationsarchitekturen zwischen Security Hub und Partnerprodukten unterscheiden sich von Partner zu Partner in Bezug auf die Art und Weise, wie die Lösung dieses Partners betrieben wird. Sie sollten sicherstellen, dass der Einrichtungsprozess für die Integration nicht länger als 15 Minuten dauert.

    Wenn Sie Integrationssoftware in der AWS Kundenumgebung einsetzen, sollten Sie AWS CloudFormation Vorlagen nutzen, um die Integration zu vereinfachen. Einige Partner haben eine Ein-Klick-Integration eingeführt, die dringend empfohlen wird.

29. Was sind meine Dokumentationsanforderungen?

Sie müssen einen Link zur Dokumentation bereitstellen, in der der Integrations- und Einrichtungsprozess zwischen Ihrem Produkt und Security Hub beschrieben wird, einschließlich Ihrer Verwendung von AWS CloudFormation Vorlagen.

Diese Dokumentation sollte auch Informationen über Ihre Verwendung von ASFF enthalten. Insbesondere sollten darin die ASFF-Suchttypen aufgeführt sein, die Sie für Ihre verschiedenen Ergebnisse verwenden. Wenn Sie über Standarddefinitionen für Erkenntnisse verfügen, empfehlen wir, dass Sie diese auch hier angeben.

Erwägen Sie die Aufnahme weiterer potenzieller Informationen:

- Ihr Anwendungsfall für die Integration mit Security Hub
- Durchschnittliches Volumen der gesendeten Ergebnisse
- Ihre Integrationsarchitektur
- Die Regionen, die Sie unterstützen und die Sie nicht unterstützen
- Latenz zwischen dem Zeitpunkt, an dem Ergebnisse erstellt werden, und dem Zeitpunkt, zu dem sie an Security Hub gesendet werden
- Ob Sie die Ergebnisse aktualisieren

30. Was sind benutzerdefinierte Erkenntnisse?

    Sie werden ermutigt, benutzerdefinierte Erkenntnisse für Ihre Ergebnisse zu definieren. Bei Erkenntnissen handelt es sich um einfache Korrelationsregeln, anhand derer ein Kunde priorisieren kann, welche Ergebnisse und Ressourcen am dringendsten Aufmerksamkeit und Maßnahmen erfordern.

    Security Hub verfügt über einen `CreateInsight` API-Betrieb. Sie können benutzerdefinierte Einblicke in einem Kundenkonto als Teil Ihrer AWS CloudFormation Vorlage erstellen. Diese Erkenntnisse werden auf der Kundenkonsole angezeigt.

31. Kann ich Dashboard-Widgets einreichen?

    Nein, derzeit nicht. Sie können nur verwaltete Insights erstellen.

32. Was ist Ihr Preismodell?

    Sehen Sie sich die Preisinformationen für Security Hub an.

33. Wie reiche ich die Ergebnisse im Rahmen des endgültigen Genehmigungsprozesses für meine Integration an das Security Hub-Demo-Konto ein?

Senden Sie die Ergebnisse an das Security Hub-Demo-Konto mit dem von Ihnen bereitgestellten Produkt-ARN und geben Sie `us-west-2` als Region ein. Die Ergebnisse sollten die Demo-Kontonummer im `AwsAccountId` Bereich ASFF enthalten. Um die Demo-Kontonummer zu erhalten, wenden Sie sich an das Security Hub Hub-Team.

Senden Sie uns keine sensiblen Daten oder persönlich identifizierbaren Informationen. Diese Daten werden für öffentliche Demos verwendet. Wenn Sie uns diese Daten senden, autorisieren Sie uns, sie für Demos zu verwenden.

34. Welche Fehler- oder Erfolgsmeldungen werden angezeigt? **`BatchImportFindings`**

    Security Hub bietet eine Antwort zur Autorisierung und eine Antwort für `BatchImportFindings`. Weitere klare Erfolgs-, Misserfolgs- und Fehlermeldungen sind in Entwicklung.

35. Für welche Fehlerbehandlung ist der Quelldienst verantwortlich?

    Die Quelldienste sind für die gesamte Fehlerbehandlung verantwortlich. Sie müssen mit Fehlermeldungen, Wiederholungsversuchen, Drosselungen und Alarmen umgehen. Sie müssen auch Feedback oder Fehlermeldungen verarbeiten, die über den Security Hub-Feedback-Mechanismus gesendet werden.

36. Was sind einige Lösungen für häufig auftretende Probleme?

    An `AuthorizerConfigurationException` wird entweder durch eine Fehlbildung `AwsAccountId` oder `ProductArn` verursacht.

    Beachten Sie bei der Fehlerbehebung Folgendes:

    - `AwsAccountId`muss genau aus 12 Ziffern bestehen.
    - `ProductArn`muss das folgende Format haben: arn:aws:securityhub: ::product//*`<us-west-2 or us-east-1><accountId><company-id><product-id>`*

      Die Konto-ID ändert sich nicht von der, die das Security Hub Hub-Team in dem Produkt enthalten hat ARNs , das es Ihnen zur Verfügung gestellt hat.

    `AccessDeniedException`wird verursacht, wenn ein Ergebnis an oder von einem falschen Konto gesendet wird oder wenn das Konto kein Konto hat`ProductSubscription`. Die Fehlermeldung enthält einen ARN mit dem Ressourcentyp `product` oder`product-subscription`. Dieser Fehler tritt nur bei kontoübergreifenden Anrufen auf. Wenn Sie `BatchImportFindings`mit Ihrem eigenen Konto für dasselbe Konto in `AwsAccountId` und anrufen`ProductArn`, verwendet der Vorgang IAM-Richtlinien und hat nichts damit zu tun. `ProductSubscriptions`

Vergewissern Sie sich, dass es sich bei dem von Ihnen verwendeten Kundenkonto und Produktkonto um die tatsächlich registrierten Konten handelt. Einige Partner haben eine Kontonummer für das Produkt aus dem Produkt-ARN verwendet, versuchen aber, ein völlig anderes Konto für den Anruf zu verwenden `BatchImportFindings`. In anderen Fällen haben sie Konten `ProductSubscriptions` für andere Kunden oder sogar für ihr eigenes Produktkonto erstellt. Sie haben kein Kundenkonto erstelltProductSubscriptions, in das sie die Ergebnisse importieren wollten.

37 An wen sende ich Fragen, Kommentare und Bugs?

`<securityhub-partners@amazon.com>`

38 In welche Region sende ich Ergebnisse für Artikel im Zusammenhang mit globalen AWS Dienstleistungen? Wohin sende ich beispielsweise Ergebnisse im Zusammenhang mit IAM?

Senden Sie Ergebnisse an dieselbe Region, in der der Befund entdeckt wurde. Bei einem Dienst wie IAM wird Ihre Lösung wahrscheinlich in mehreren Regionen auf dasselbe IAM-Problem stoßen. In diesem Fall wird der Befund an alle Regionen gesendet, in denen das Problem festgestellt wurde.

Wenn der Kunde Security Hub in drei Regionen betreibt und in allen drei Regionen dasselbe IAM-Problem festgestellt wird, senden Sie das Ergebnis an alle drei Regionen.

Wenn ein Problem behoben ist, senden Sie die Aktualisierung des Ergebnisses an alle Regionen, in die Sie das ursprüngliche Ergebnis gesendet haben.

Dokumentenverlauf für den Partner Integration Guide

In der folgenden Tabelle werden die Dokumentationsaktualisierungen für dieses Handbuch beschrieben.

Änderung	Beschreibung	Datum
Die Anforderungen für das Konsolenlogo wurden aktualisiert	Das Partnermanifest und die Logo-Richtlinien wurden aktualisiert und weisen nun darauf hin, dass Partner sowohl eine helle als auch eine dunkle Version des Logos für die Anzeige auf der Security Hub Hub-Konsole bereitstellen müssen. Die Logos müssen im SVG-Format vorliegen.	10. Mai 2021
Die Voraussetzungen für neue Integrationspartner wurden aktualisiert	Security Hub unterstützt jetzt auch Partner, die dem AWS ISV-Partnerpfad beigetreten sind und ein Integrationsprodukt verwenden, das eine AWS grundlegende technische Überprüfung (FTR) abgeschlossen hat. Bisher mussten alle Integrationspartner AWS Select-Tier-Partner sein.	29. April 2021
Neues `FindingProviderFields` Objekt in ASFF	Die Informationen zur Zuordnung der Ergebnisse zu ASFF wurden aktualisiert. Für `Confidence`, `Criticality` `RelatedFindings`,	18. März 2021

	und `SeverityTypes`, Partner ordnen ihre Werte den Feldern in `FindingProviderFields` zu.	
Neue Grundsätze für die Erstellung und Aktualisierung von Ergebnissen	Es wurden neue Richtlinien für die Erstellung neuer Erkenntnisse und die Aktualisierung vorhandener Ergebnisse in Security Hub hinzugefügt.	4. Dezember 2020
Erste Version dieses Handbuchs	Dieser Leitfaden zur Partnerintegration bietet AWS Partnern Informationen darüber, wie sie eine Integration mit einrichten können AWS Security Hub.	23. Juni 2020

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.