Guida all'integrazione dei partner

AWS Security Hub

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

AWS Security Hub: Guida all'integrazione dei partner

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Panoramica dell'integrazione di terze parti con AWS Security Hub 1
Perché integrarsi? 1
Preparazione all'invio dei risultati 2
Prepararsi a ricevere i risultati 3
Risorse informative su Security Hub 4
Prerequisiti per i partner 5
Casi d'uso e autorizzazioni 6
Ospitato dal partner: risultati inviati dall'account del partner 6
Ospitato dal partner: risultati inviati dall'account del cliente 7
Customer hosted: risultati inviati dall'account del cliente 9
Processo di onboarding dei partner 11
Go-to-market attività 14
Accesso alla pagina dei partner del Security Hub 14
Comunicato stampa 14
AWS Blog del Partner Network (APN) 15
Cose chiave da sapere sul blog APN 15
Perché scrivere per il blog APN? 16
Qual è il tipo di contenuto più adatto? 16
Slick sheet o foglio di marketing 16
Whitepaper o ebook 17
Webinar 17
Video della demo 17
Manifesto di integrazione del prodotto 18
Caso d'uso e informazioni di marketing 19
Caso d'uso relativo alla ricerca di fornitori e consumatori 19
Caso d'uso di Consulting Partner (CP) 20
Set di dati 20
Architettura 20
Configurazione 21
Media dei risultati al giorno per cliente 21
Latenza 21
Descrizione dell'azienda e del prodotto 21
Risorse del sito web dei partner 22
Logo per la pagina dei partner 22

Loghi per la console Security Hub 22
Tipi di esiti 23
Hotline 23
Rilevamento del battito cardiaco 23
Informazioni sulla console Security Hub 24
Informazioni sull'azienda 24
Informazioni sul prodotto 25
Linee guida e liste di controllo 36
Linee guida per il logo della console 36
Principi per la creazione e l'aggiornamento dei risultati 39
Linee guida per la mappatura ASFF 40
Informazioni identificative 40
Title e Description 41
Tipi di esiti 41
Timestamp 41
Severity 42
Remediation 42
SourceUrl 43
Malware, Network, Process, ThreatIntelIndicators 43
Resources 46
ProductFields 46
Conformità 47
Campi con restrizioni 47
Linee guida per l'utilizzo dell'API `BatchImportFindings` 47
Lista di controllo per la preparazione del prodotto 48
Mappatura ASFF 48
Configurazione e funzione di integrazione 50
Documentazione 53
Informazioni sulla scheda del prodotto 54
Informazioni di marketing 55
Domande frequenti per i partner 58
Cronologia dei documenti 70
..... lxxii

Panoramica dell'integrazione di terze parti con AWS Security Hub

Questa guida è destinata ai AWS partner del Partner Network (APN) che desiderano creare un'integrazione con. AWS Security Hub

In qualità di partner APN, puoi integrarti con Security Hub in uno o più dei seguenti modi.

- Invia i risultati a Security Hub
- Consuma i risultati di Security Hub
- Entrambi inviano e utilizzano i risultati da Security Hub
- Usa Security Hub come centro dell'offerta di un provider di servizi di sicurezza gestiti (MSSP)
- Consulta AWS i clienti su come implementare e utilizzare Security Hub

Questa guida all'onboarding si concentra principalmente sui partner che inviano i risultati a Security Hub.

Argomenti

- Perché integrarsi con? AWS Security Hub
- Preparazione all'invio dei risultati a AWS Security Hub
- Prepararsi a ricevere i risultati da AWS Security Hub
- Risorse per saperne di più AWS Security Hub

Perché integrarsi con? AWS Security Hub

AWS Security Hub offre una visione completa degli avvisi di sicurezza ad alta priorità e dello stato di sicurezza tra gli account Security Hub. Security Hub consente a partner come te di inviare i risultati di sicurezza a Security Hub per fornire ai tuoi clienti informazioni dettagliate sui risultati di sicurezza che generi.

Un'integrazione con Security Hub può aggiungere valore nei seguenti modi.

- Soddisfa i clienti che hanno richiesto un'integrazione con Security Hub
- Fornisce ai clienti una visione unificata dei risultati relativi alla sicurezza AWS

- Consente ai nuovi clienti di scoprire la tua soluzione quando cercano partner che forniscano risultati relativi a tipi specifici di eventi di sicurezza

Prima di creare un'integrazione con Security Hub, esamina i motivi dell'integrazione. È più probabile che un'integrazione abbia successo se i tuoi clienti desiderano un'integrazione del Security Hub con il tuo prodotto. È possibile creare un'integrazione esclusivamente per motivi di marketing o per acquisire nuovi clienti. Tuttavia, se si crea l'integrazione senza l'input corrente del cliente e non si prendono in considerazione le esigenze dei clienti, l'integrazione potrebbe non produrre i risultati previsti.

Preparazione all'invio dei risultati a AWS Security Hub

In qualità di partner APN, non puoi inviare informazioni a Security Hub per i tuoi clienti finché il team di Security Hub non ti abilita come provider di ricerca. Per essere abilitato come fornitore di servizi di ricerca, devi completare i seguenti passaggi di onboarding. In questo modo garantisci un'esperienza positiva Security Hub per te e i tuoi clienti.

Mentre completi i passaggi di onboarding, assicurati di seguire le linee guida contenute in the section called “Principi per la creazione e l'aggiornamento dei risultati”the section called “Linee guida per la mappatura ASFF”, e. the section called “Linee guida per l'utilizzo dell'API `BatchImportFindings`”

1. Associa le tue scoperte sulla sicurezza al AWS Security Finding Format (ASFF).
2. Crea la tua architettura di integrazione per inviare i risultati all'endpoint Regional Security Hub corretto. A tale scopo, siete voi a definire se inviare i risultati dal vostro AWS account o dall'interno degli account dei vostri clienti.
3. Chiedi ai tuoi clienti di abbonare il prodotto al loro account. A tale scopo, possono utilizzare la console o il funzionamento dell'`EnableImportFindingsForProduct`API. Vedi Gestione delle integrazioni dei prodotti nella Guida per l'AWS Security Hub utente.

   Puoi anche abbonare il prodotto per loro. A tale scopo, utilizzi un ruolo interaccount per accedere al funzionamento dell'`EnableImportFindingsForProduct`API per conto del cliente.

   Questo passaggio stabilisce le politiche relative alle risorse necessarie per accettare i risultati di quel prodotto per quell'account.

I seguenti post del blog illustrano alcune delle integrazioni dei partner esistenti con Security Hub.

- Annuncio dell'integrazione di Cloud Custodian con AWS Security Hub
- Usa AWS Fargate and Prowler per inviare i risultati della configurazione di sicurezza relativi ai AWS servizi a Security Hub
- Come importare AWS Config le valutazioni delle regole come risultati in Security Hub

Prepararsi a ricevere i risultati da AWS Security Hub

Per ricevere risultati da AWS Security Hub, utilizza una delle seguenti opzioni:

- Chiedi ai tuoi clienti di inviare automaticamente tutti i risultati a CloudWatch Events. Un cliente può creare regole di CloudWatch evento specifiche per inviare i risultati a obiettivi specifici, come un SIEM o un bucket S3.
- Chiedi ai tuoi clienti di selezionare risultati o gruppi di risultati specifici dalla console Security Hub e quindi di agire di conseguenza.

Ad esempio, i clienti possono inviare i risultati a un SIEM, a un sistema di ticketing, a una piattaforma di chat o a un flusso di lavoro di correzione. Questo farebbe parte di un flusso di lavoro di valutazione degli avvisi eseguito da un cliente all'interno di Security Hub.

Queste sono chiamate azioni personalizzate. Quando un utente esegue un'azione personalizzata, viene creato un CloudWatch evento per quei risultati specifici. In qualità di partner, puoi sfruttare questa funzionalità e creare regole o obiettivi di CloudWatch evento che un cliente possa utilizzare come parte di un'azione personalizzata. Tieni presente che questa funzionalità non invia automaticamente tutti i risultati di un particolare tipo o classe a CloudWatch Events. Questa funzionalità consente all'utente di intervenire su risultati specifici.

I seguenti post del blog descrivono soluzioni che utilizzano l'integrazione con Security Hub ed CloudWatch Events per azioni personalizzate.

- Come integrare azioni AWS Security Hub personalizzate con PagerDuty
- Come abilitare le azioni personalizzate in AWS Security Hub
- Come importare AWS Config le valutazioni delle regole come risultati in Security Hub

Risorse per saperne di più AWS Security Hub

I seguenti materiali possono aiutarti a comprendere meglio la AWS Security Hub soluzione e come AWS i clienti possono utilizzare il servizio.

- Introduzione al AWS Security Hub video
- Guida per l'utente di Security Hub
- Riferimento all'API Security Hub
- Webinar di onboarding

Ti invitiamo inoltre ad abilitare Security Hub in uno dei tuoi AWS account e ad acquisire un'esperienza pratica con il servizio.

Prerequisiti per i partner

Prima di iniziare un'integrazione con AWS Security Hub, devi soddisfare uno dei seguenti criteri:

- Sei un partner AWS Select Tier o superiore.
- Hai aderito all'AWS ISV Partner Path e il prodotto che utilizzi per l'integrazione del Security Hub ha completato un AWS Foundational Technical Review (FTR). Al prodotto viene quindi assegnato il badge «Recensito da AWS».

È inoltre necessario disporre di un accordo di non divulgazione reciproca con. AWS

Casi d'uso di integrazione e autorizzazioni richieste

AWS Security Hub consente AWS ai clienti di ricevere i risultati dai partner APN. I prodotti del partner possono funzionare all'interno o all'esterno dell' AWS account del cliente. La configurazione delle autorizzazioni nell'account del cliente varia in base al modello utilizzato dal prodotto partner.

In Security Hub, il cliente controlla sempre quali partner possono inviare i risultati all'account del cliente. I clienti possono revocare le autorizzazioni di un partner in qualsiasi momento.

Per consentire a un partner di inviare i risultati di sicurezza al proprio account, il cliente sottoscrive innanzitutto il prodotto partner in Security Hub. La fase di sottoscrizione è necessaria per tutti i casi d'uso descritti di seguito. Per i dettagli su come i clienti gestiscono le integrazioni dei prodotti, consulta Gestire le integrazioni dei prodotti nella Guida per l'AWS Security Hub utente.

Dopo che un cliente si è abbonato a un prodotto partner, Security Hub crea automaticamente una politica delle risorse gestite. La politica concede al prodotto partner l'autorizzazione a utilizzare l'operazione `BatchImportFindings`API per inviare i risultati a Security Hub per l'account del cliente.

Ecco i casi più comuni di prodotti partner che si integrano con Security Hub. Le informazioni includono le autorizzazioni aggiuntive richieste per ogni caso d'uso.

Ospitato dal partner: risultati inviati dall'account del partner

Questo caso d'uso riguarda i partner che ospitano un prodotto AWS sul proprio account.
Per inviare i risultati di sicurezza relativi a un AWS cliente, il partner richiama l'operazione `BatchImportFindings`API dall'account del prodotto del partner.

In questo caso d'uso, l'account cliente necessita solo delle autorizzazioni stabilite quando il cliente si abbona al prodotto partner.

Nell'account partner, il principale IAM che chiama l'operazione `BatchImportFindings`API deve disporre di una policy IAM che consenta al principale di effettuare chiamate. `BatchImportFindings`

Consentire a un prodotto partner di inviare i risultati al cliente in Security Hub è un processo in due fasi:

1. Il cliente crea un abbonamento a un prodotto partner in Security Hub.

2. Security Hub genera la corretta politica delle risorse gestite con la conferma del cliente.

Per inviare i risultati di sicurezza relativi all'account del cliente, il prodotto partner utilizza le proprie credenziali per richiamare l'operazione `BatchImportFindings`API.

Ecco un esempio di policy IAM che concede al responsabile dell'account partner le autorizzazioni necessarie per il Security Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:*:product-subscription/company-
name/product-name"
        }
    ]
}
```

Ospitato dal partner: risultati inviati dall'account del cliente

Questo caso d'uso riguarda i partner che ospitano un prodotto nel proprio AWS account, ma utilizzano un ruolo interaccount per accedere all'account del cliente. Richiamano il funzionamento dell'`BatchImportFindings`API dall'account del cliente.

In questo caso d'uso, per richiamare l'operazione `BatchImportFindings`API, l'account partner assume un ruolo IAM gestito dal cliente nell'account del cliente.

Questa chiamata viene effettuata dall'account del cliente. Pertanto, la politica delle risorse gestite deve consentire l'utilizzo dell'ARN del prodotto per l'account del prodotto partner nella chiamata. La politica delle risorse gestite di Security Hub concede l'autorizzazione per l'account del prodotto partner e l'ARN del prodotto partner. L'ARN del prodotto è l'identificatore univoco del partner come fornitore. Poiché la chiamata non proviene dall'account del prodotto partner, il cliente deve concedere esplicitamente l'autorizzazione al prodotto partner per inviare i risultati a Security Hub.

La migliore pratica per i ruoli tra account partner e account cliente consiste nell'utilizzare un identificatore esterno fornito dal partner. Questo identificatore esterno fa parte della definizione

della politica tra account diversi nell'account del cliente. Il partner deve fornire l'identificatore quando assume il ruolo. Un identificatore esterno fornisce un ulteriore livello di sicurezza quando si concede l'accesso all' AWS account a un partner. L'identificatore univoco garantisce che il partner utilizzi l'account cliente corretto.

L'abilitazione di un prodotto partner a inviare i risultati al cliente in Security Hub con un ruolo interaccount avviene in quattro passaggi:

1. Il cliente, o il partner che utilizza ruoli interaccount che lavorano per conto del cliente, avvia l'abbonamento a un prodotto in Security Hub.
2. Security Hub genera la corretta politica delle risorse gestite con la conferma del cliente.
3. Il cliente configura il ruolo tra account diversi manualmente o utilizzando. AWS CloudFormation Per informazioni sui ruoli tra account diversi, consulta Fornire l'accesso agli AWS account di proprietà di terze parti nella IAM User Guide.
4. Il prodotto archivia in modo sicuro il ruolo del cliente e l'ID esterno.

Successivamente, il prodotto invia i risultati a Security Hub:

1. Il prodotto chiama il AWS Security Token Service (AWS STS) per assumere il ruolo di cliente.
2. Il prodotto richiama l'operazione `BatchImportFindings`API su Security Hub con le credenziali temporanee del ruolo assunto.

Ecco un esempio di policy IAM che concede le autorizzazioni di Security Hub necessarie al ruolo cross-account del partner.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

La `Resource` sezione della policy identifica l'abbonamento specifico del prodotto. Ciò garantisce che il partner possa inviare solo i risultati relativi al prodotto partner a cui il cliente è abbonato.

Customer hosted: risultati inviati dall'account del cliente

Questo caso d'uso riguarda i partner che dispongono di un prodotto distribuito nell' AWS account del cliente. L'`BatchImportFindings`API viene richiamata dalla soluzione che viene eseguita nell'account del cliente.

In questo caso d'uso, al prodotto partner devono essere concesse autorizzazioni aggiuntive per chiamare l'`BatchImportFindings`API. Il modo in cui viene concessa questa autorizzazione varia in base alla soluzione del partner e a come è configurata nell'account del cliente.

Un esempio di questo approccio è un prodotto partner che viene eseguito su un' EC2 istanza nell'account del cliente. A questa EC2 istanza deve essere associato un ruolo di EC2 istanza che garantisca a tale istanza la possibilità di richiamare l'operazione `BatchImportFindings`API. Ciò consente all' EC2 istanza di inviare i risultati di sicurezza all'account del cliente.

Questo caso d'uso è funzionalmente equivalente a uno scenario in cui un cliente carica nel proprio account i risultati di un prodotto di sua proprietà.

Il cliente consente al prodotto partner di inviare i risultati dall'account del cliente al cliente in Security Hub:

1. Il cliente implementa manualmente il prodotto partner nel proprio AWS account utilizzando AWS CloudFormation o un altro strumento di implementazione.
2. Il cliente definisce la politica IAM necessaria per il prodotto partner da utilizzare quando invia i risultati a Security Hub.
3. Il cliente allega la policy ai componenti necessari del prodotto partner, come un' EC2 istanza, un contenitore o una funzione Lambda.

Ora il prodotto può inviare i risultati a Security Hub:

1. Il prodotto partner utilizza l' AWS SDK o AWS CLI per chiamare l'operazione `BatchImportFindings`API in Security Hub. Effettua la chiamata dal componente dell'account del cliente a cui è allegata la politica.
2. Durante la chiamata API, vengono generate le credenziali temporanee necessarie per consentire l'esito positivo della `BatchImportFindings`chiamata.

Ecco un esempio di policy IAM che concede le necessarie autorizzazioni Security Hub al prodotto partner nell'account cliente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-2:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

Processo di onboarding dei partner

In qualità di partner, puoi aspettarti di completare diversi passaggi di alto livello come parte del processo di onboarding. È necessario completare questi passaggi prima di poter inviare i risultati di sicurezza a. AWS Security Hub

1. Inizi un rapporto con il team dei partner APN o il team di Security Hub ed esprimi interesse a diventare partner di Security Hub. Identifichi gli indirizzi e-mail da aggiungere ai canali di comunicazione del Security Hub.
2. AWS ti offre i materiali di onboarding del partner Security Hub.
3. Sei invitato al canale Slack dei partner di Security Hub, dove puoi porre domande relative alla tua integrazione.
4. Fornisci ai contatti dei partner APN una bozza del manifesto di integrazione del prodotto da esaminare.

   Il manifesto di integrazione del prodotto contiene informazioni utilizzate per creare il prodotto partner Amazon Resource Name (ARN) per l'integrazione con. AWS Security Hub

   Fornisce al team di Security Hub le informazioni che appaiono nella pagina del provider partner nella console di Security Hub. Viene anche utilizzato per proporre nuove informazioni gestite relative all'integrazione da aggiungere alla libreria di approfondimenti di Security Hub.

   Questa versione iniziale del manifesto di integrazione del prodotto non deve contenere i dettagli completi. Ma dovrebbe contenere almeno il caso d'uso e le informazioni sul set di dati.

   Per informazioni dettagliate sul manifesto e sulle informazioni richieste, vedereManifesto di integrazione del prodotto.
5. Il team di Security Hub ti fornisce un ARN per il tuo prodotto. Si utilizza l'ARN per inviare i risultati a Security Hub.
6. Crei la tua integrazione per inviare o ricevere risultati da Security Hub.

   Mappatura dei risultati su ASFF

   Per inviare i risultati a Security Hub, è necessario mappare i risultati al AWS Security Finding Format (ASFF).

L'ASFF fornisce una descrizione coerente dei risultati che possono essere condivisi tra servizi AWS di sicurezza, partner e sistemi di sicurezza dei clienti. Ciò riduce gli sforzi di integrazione, incoraggia un linguaggio comune e fornisce un modello per gli implementatori.

ASFF è il formato di protocollo di rete richiesto da utilizzare per inviare i risultati. AWS Security Hub I risultati sono rappresentati come documenti JSON che aderiscono allo schema ASFF JSON e all'RFC-7493 The I-JSON Message Format. Per i dettagli sullo schema ASFF, consulta AWS Security Finding Format (ASFF) nella Guida per l'utente.AWS Security Hub

Per informazioni, consulta the section called “Linee guida per la mappatura ASFF”.

Creazione e test dell'integrazione

Puoi completare tutti i test per la tua integrazione utilizzando un AWS account di tua proprietà. In questo modo avrai piena visibilità su come vengono visualizzati i risultati in Security Hub. Inoltre, ti aiuta a comprendere l'esperienza del cliente con i tuoi risultati di sicurezza.

L'operazione `BatchImportFindings`API viene utilizzata per inviare risultati nuovi e aggiornati a Security Hub.

Durante la creazione di un'integrazione con Security Hub, ti AWS incoraggia a tenere informati i contatti dei partner APN sullo stato di avanzamento dell'integrazione. Puoi anche chiedere aiuto ai tuoi contatti partner APN per domande sull'integrazione.

Per informazioni, consulta the section called “Linee guida per l'utilizzo dell'API `BatchImportFindings`”.

7. Dimostri l'integrazione al team di prodotto Security Hub. Questa integrazione deve essere dimostrata utilizzando un account di proprietà del team di Security Hub.

   Se sono a proprio agio con l'integrazione, il team di Security Hub dà l'approvazione per procedere all'inserimento nell'elenco di te come provider.

8. Fornisci AWS un manifesto finale da esaminare.
9. Il team di Security Hub crea l'integrazione del provider nella console Security Hub. I clienti possono quindi scoprire e abilitare l'integrazione.
10. (Facoltativo) Ti impegni in ulteriori iniziative di marketing per promuovere l'integrazione del Security Hub. Per informazioni, consulta Go-to-market attività.

    Come minimo, Security Hub consiglia di fornire le seguenti risorse.

- Un video dimostrativo (massimo 3 minuti) dell'integrazione funzionante. Il video viene utilizzato per scopi di marketing e pubblicato sul AWS YouTube canale.
- Un diagramma dell'architettura a una diapositiva da aggiungere alla slide deck di diapositive per la prima chiamata del Security Hub.

Go-to-market attività

I partner possono anche impegnarsi in attività di marketing opzionali per spiegare e promuovere la loro AWS Security Hub integrazione.

Se desideri creare i tuoi contenuti di marketing relativi a Security Hub, prima di pubblicarli, invia una bozza al tuo partner manager APN per la revisione e l'approvazione. Ciò garantisce che tutti siano allineati sulla messaggistica.

AWS I partner Partner Network (APN) possono utilizzare APN Partner Marketing Central e il programma Market Development Funds (MDF) per creare campagne e ottenere supporto finanziario. Per dettagli su questi programmi, contatta il tuo partner manager.

Accesso alla pagina dei partner del Security Hub

Dopo l'approvazione come partner di Security Hub, la soluzione può essere visualizzata nella pagina AWS Security Hub dei partner.

Per essere inserito in questa pagina, fornisci i seguenti dettagli ai tuoi contatti partner APN.
`<Potrebbe trattarsi del tuo Partner Development Manager (PDM), Partner Solution`

- Una breve descrizione della soluzione, della sua integrazione con Security Hub e del valore che l'integrazione con Security Hub offre ai clienti. Questa descrizione è limitata a 700 caratteri, spazi inclusi.
- L'URL di una pagina che descrive la soluzione. Questo sito dovrebbe essere specifico per la tua AWS integrazione e più specificamente per l'integrazione con Security Hub. Dovrebbe concentrarsi sull'esperienza del cliente e sul valore che i clienti ricevono quando utilizzano l'integrazione.
- Una copia ad alta risoluzione del tuo logo di 600 x 300 pixel. Per informazioni dettagliate sui requisiti di questo logo, consultathe section called “Logo per la pagina dei partner”.

Comunicato stampa

In qualità di partner approvato, puoi facoltativamente pubblicare un comunicato stampa sul tuo sito Web e sui canali di pubbliche relazioni. Il comunicato stampa deve essere approvato da AWS.

Prima di pubblicare il comunicato stampa, devi inviarlo AWS per la revisione ai Partner APN Marketing, alla leadership del Security Hub e ai Servizi di Sicurezza AWS Esterni (ESS). Il comunicato stampa può includere una proposta di preventivo per il vicepresidente di ESS.

Per avviare questo processo, utilizza il tuo PDM. Abbiamo sottoscritto un Service Level Agreement (SLA) di 10 giorni lavorativi per esaminare i comunicati stampa.

AWS Blog del Partner Network (APN)

Possiamo anche aiutarti a pubblicare un post di blog di cui sei autore sul blog APN. Il post di blog deve concentrarsi sulla storia di un cliente e su un caso d'uso. Non può essere concepito esclusivamente come partner per il lancio dell'integrazione.

Se sei interessato, contatta il tuo PDM o PSA per iniziare il processo. I blog APN possono richiedere 8 settimane o più per l'approvazione finale e la pubblicazione.

Cose chiave da sapere sul blog APN

Quando crei un post sul blog, tieni a mente i seguenti elementi.

Cosa c'è in un post sul blog?

- I post dei partner devono essere istruttivi e fornire competenze approfondite su un argomento rilevante per AWS i clienti.
- La lunghezza ideale non supera le 1.500 parole. I lettori apprezzano i contenuti approfonditi ed educativi che insegnano loro cosa è possibile fare. AWS
- I contenuti devono essere originali del blog APN. Non riutilizzare contenuti provenienti da fonti come post di blog o white paper esistenti.

Quali sono gli altri limiti alla pubblicazione sul blog APN?

- Solo i partner di livello Advanced o Premier possono pubblicare post sul blog APN. Esistono eccezioni per i partner selezionati che hanno una designazione di programma APN, ad esempio Service Delivery.
- Ogni partner è limitato a tre incarichi all'anno. Con decine di migliaia di partner APN, AWS deve garantire una copertura equa.

Ogni post deve avere uno sponsor tecnico in grado di convalidare la soluzione o il caso d'uso.

Quanto tempo occorre per modificare un post del blog prima che venga pubblicato?

Dopo aver inviato la prima bozza completa del post sul blog, la modifica richiede da quattro a sei settimane.

Perché scrivere per il blog APN?

Un post sul blog APN può offrire i seguenti vantaggi.

- Credibilità: per i partner APN, la pubblicazione di una storia da AWS può influenzare i clienti a livello globale.
- Visibilità: il blog APN è uno dei blog più letti, AWS con 1,79 milioni di visualizzazioni di pagina nel 2019, incluso il traffico influenzato.
- Business: i post per i partner APN dispongono di pulsanti di connessione che possono generare lead tramite il programma APN Customer Engagements (ACE).

Qual è il tipo di contenuto più adatto?

I seguenti tipi di contenuti sono i più adatti per un post sul blog APN.

- I contenuti tecnici sono il tipo di storia più popolare. Ciò include approfondimenti sulla soluzione e informazioni pratiche. Oltre il 75% dei lettori consulta questi contenuti tecnici.
- I clienti apprezzano le storie di almeno 200 livelli che dimostrano come funziona qualcosa AWS o come un partner APN ha risolto un problema aziendale per i clienti.
- I post scritti da esperti tecnici o esperti in materia danno di gran lunga i risultati migliori.

Slick sheet o foglio di marketing

Uno slick sheet è un documento di una pagina che descrive il prodotto, la sua architettura di integrazione e i casi d'uso congiunti con i clienti.

Se crei un semplice foglio per la tua integrazione, inviane una copia al team di Security Hub. Lo aggiungeranno alla pagina dei partner.

Whitepaper o ebook

Se crei un white paper o un ebook che descrive il tuo prodotto, la sua architettura di integrazione e i casi d'uso congiunti con i clienti, inviane una copia al team di Security Hub. Lo aggiungeranno alla pagina dei partner di Security Hub.

Webinar

Se conduci un webinar sulla tua integrazione, invia una registrazione del webinar al team di Security Hub. Il team vi collegherà dalla pagina del partner.

Il team può anche fornire un esperto in materia di Security Hub per partecipare al webinar.

Video della demo

Per scopi di marketing, puoi produrre un video dimostrativo dell'integrazione operativa. Pubblica un video di questo tipo sull'account della tua piattaforma video e il team di Security Hub lo collegherà dalla pagina del partner.

Manifesto di integrazione del prodotto

Ogni partner di AWS Security Hub integrazione deve compilare un manifesto di integrazione del prodotto che fornisca i dettagli richiesti per l'integrazione proposta.

Il team di Security Hub utilizza queste informazioni in diversi modi:

- Per creare la scheda del tuo sito web
- Per creare la scheda prodotto per la console Security Hub
- Per informare il team di prodotto del tuo caso d'uso.

Per valutare la qualità dell'integrazione proposta e delle informazioni fornite, il team di Security Hub utilizza ilthe section called “Lista di controllo per la preparazione del prodotto”. Questa lista di controllo determina se l'integrazione è pronta per essere lanciata.

Tutte le informazioni tecniche fornite devono essere riportate anche nella documentazione.

È possibile scaricare una versione PDF del manifesto di integrazione del prodotto dalla sezione Risorse della pagina dei AWS Security Hub partner. Tieni presente che la pagina dei partner non è disponibile nelle regioni Cina (Pechino) e Cina (Ningxia).

Indice

- Caso d'uso e informazioni di marketing
  - Caso d'uso relativo alla ricerca di fornitori e consumatori
  - Caso d'uso di Consulting Partner (CP)
  - Set di dati
  - Architettura
  - Configurazione
  - Media dei risultati al giorno per cliente
  - Latenza
  - Descrizione dell'azienda e del prodotto
  - Risorse del sito web dei partner
  - Logo per la pagina dei partner
  - Loghi per la console Security Hub

- Tipi di esiti
- Hotline
- Rilevamento del battito cardiaco
- AWS Security Hub informazioni sulla console
  - Informazioni sull'azienda
  - Informazioni sul prodotto

Caso d'uso e informazioni di marketing

I seguenti casi d'uso possono aiutarti a configurare AWS Security Hub per diversi scopi.

Caso d'uso relativo alla ricerca di fornitori e consumatori

Richiesto per i fornitori di software indipendenti (ISV).

Per descrivere il caso d'uso relativo all'integrazione con AWS Security Hub, rispondi alle seguenti domande. Se non avete intenzione di inviare o ricevere i risultati, tenetelo presente in questa sezione e poi completate la sezione successiva.

Le seguenti informazioni devono essere riportate nella documentazione.

- Invierai i risultati, li riceverai o entrambi?
- Se intendi inviare i risultati, che tipo di risultati invierai? Invierai tutti i risultati o un sottoinsieme specifico di risultati?
- Se avete intenzione di ricevere i risultati, cosa ne farete? Quali tipi di risultati riceverai? Ad esempio, riceverai tutti i risultati, i risultati di un certo tipo o solo i risultati specifici selezionati da un cliente?
- Hai intenzione di aggiornare i risultati? In caso affermativo, quali campi aggiornerai? Security Hub consiglia di aggiornare i risultati invece di crearne sempre di nuovi. L'aggiornamento dei risultati esistenti aiuta a ridurre il rumore dei risultati per i clienti.

  Per aggiornare un risultato, invii un risultato con un ID di ricerca assegnato a un risultato che hai già inviato.

Per ricevere un feedback tempestivo sul tuo caso d'uso e sui set di dati, contatta il team APN Partner o Security Hub.

Caso d'uso di Consulting Partner (CP)

Obbligatorio se sei un partner di consulenza Security Hub.

Fornisci due casi d'uso ai clienti per il tuo lavoro con Security Hub. Questi possono essere casi d'uso privati. Il team di Security Hub non li pubblicizza da nessuna parte. Dovrebbero descrivere una o entrambe le seguenti azioni.

- Come aiutate i clienti ad avviare Security Hub? Ad esempio, hai aiutato i clienti a utilizzare servizi professionali, un modulo Terraform o un AWS CloudFormation modello?
- In che modo aiutate i clienti a rendere operativo ed estendere Security Hub? Ad esempio, hai fornito modelli di risposta o correzione, creato integrazioni personalizzate o utilizzato strumenti di business intelligence per configurare una dashboard esecutiva?

Set di dati

Obbligatorio se si inviano i risultati a Security Hub.

Per i risultati che invierai a Security Hub, fornisci le seguenti informazioni.

- I risultati nel loro formato nativo, ad esempio JSON o XML
- Un esempio di come convertire i risultati nel formato ASFF (AWS Security Finding Format)

Fai sapere al team di Security Hub se hai bisogno di aggiornamenti all'ASFF per supportare la tua integrazione.

Architettura

Obbligatorio se si inviano o si ricevono risultati da Security Hub.

Descrivi come intendi integrarti con Security Hub. Queste informazioni devono inoltre essere riportate nella documentazione.

È necessario fornire diagrammi di architettura. Quando preparate i diagrammi di architettura, tenete presente quanto segue:

- Quali AWS servizi, agenti del sistema operativo e così via verranno utilizzati?
- Se invierai i risultati a Security Hub, li invierai dall' AWS account cliente o dal tuo AWS account?

- Se riceverai dei risultati, come utilizzerai l'integrazione CloudWatch Events?
- Come convertirai i risultati in ASFF?
- In che modo raggrupperete i risultati, monitorerete lo stato dei risultati ed eviterete i limiti di limitazione?

Configurazione

Obbligatorio se si inviano o si ricevono risultati da Security Hub.

Descrivi come un cliente configurerà la tua integrazione con Security Hub.

Come minimo, è necessario utilizzare AWS CloudFormation modelli o un'infrastruttura simile, ad esempio modelli di codice. Alcuni partner hanno fornito un'interfaccia utente per supportare l'integrazione con un solo clic.

La configurazione non dovrebbe richiedere più di 15 minuti. La documentazione del prodotto deve inoltre fornire indicazioni sulla configurazione per l'integrazione.

Media dei risultati al giorno per cliente

Obbligatorio se si inviano i risultati a Security Hub.

Quanti aggiornamenti di ricerca al mese (in media e al massimo) prevedi di inviare a Security Hub all'interno della tua base clienti? Le stime degli ordini di grandezza sono accettabili.

Latenza

Obbligatorio se si inviano i risultati a Security Hub.

Con quale rapidità verranno raggruppati e inviati i risultati a Security Hub? In altre parole, qual è la latenza tra il momento in cui il risultato viene creato nel prodotto e il momento in cui viene inviato a Security Hub?

Queste informazioni devono essere riportate nella documentazione del prodotto per l'integrazione. È una domanda comune posta dai clienti.

Descrizione dell'azienda e del prodotto

Richiesto per tutte le integrazioni con Security Hub.

Descrivi brevemente la tua azienda e il tuo prodotto, con un'enfasi specifica sulla natura dell'integrazione del Security Hub. Lo utilizziamo nella nostra pagina dedicata ai partner del Security Hub.

Se stai integrando più prodotti con Security Hub, puoi fornire una descrizione separata per ogni prodotto, ma li combineremo in un'unica voce nella pagina dei partner.

Ogni descrizione non può superare i 700 caratteri con spazi.

Risorse del sito web dei partner

Richiesto per tutte le integrazioni con Security Hub.

Come minimo, è necessario fornire un URL da utilizzare per il collegamento ipertestuale Ulteriori informazioni nella pagina dei partner di Security Hub. Dovrebbe essere una landing page di marketing che descriva l'integrazione tra il prodotto e Security Hub.

Se integri più prodotti con Security Hub, puoi avere un'unica pagina di destinazione per essi. Security Hub consiglia che questa pagina di destinazione includa un collegamento alle istruzioni di configurazione.

Puoi anche fornire link ad altre risorse come blog, webinar, video dimostrativi o white paper. Security Hub si collegherà anche a quelli presenti nella pagina dei partner.

Logo per la pagina dei partner

Richiesto per tutte le integrazioni di Security Hub.

Fornisci l'URL di un logo da visualizzare nella pagina dei partner del Security Hub. Il logo deve soddisfare i seguenti criteri:

- Dimensioni: 600 x 300 pixel
- Ritaglio: aderente senza imbottitura
- Sfondo: trasparente
- Formato: PNG

Loghi per la console Security Hub

Richiesto per tutte le integrazioni.

Fornisci URLs i loghi della modalità luce e della modalità scura da visualizzare sulla console Security Hub.

I loghi devono soddisfare i seguenti criteri:

- Formato: SVG
- Dimensioni: 175 x 40 pixel. Se è più grande, l'immagine dovrebbe usare quel rapporto.
- Ritaglio: stretto senza imbottitura
- Sfondo: trasparente

Per linee guida dettagliate per il logo piccolo, vedithe section called “Linee guida per il logo della console”.

Tipi di esiti

Obbligatorio se si inviano i risultati a Security Hub.

Fornisci una tabella che documenti i tipi di risultati in formato ASFF che utilizzi e il modo in cui si allineano ai tipi di risultati nativi. Per i dettagli sulla ricerca dei tipi in ASFF, consulta la tassonomia dei tipi per ASFF nella Guida per l'utente.AWS Security Hub

Ti consigliamo di includere queste informazioni anche nella documentazione del prodotto.

Hotline

Richiesto per tutte le integrazioni con Security Hub.

Fornisci un indirizzo e-mail e un numero di telefono o un numero di cercapersone per un punto di contatto tecnico. Security Hub comunicherà con questo contatto in merito a eventuali problemi tecnici, ad esempio quando un'integrazione non funziona più.

Fornisci inoltre un punto di contatto 24 ore su 24, 7 giorni su 7 per problemi tecnici di elevata gravità.

Rilevamento del battito cardiaco

Consigliato se si inviano i risultati a Security Hub.

È possibile inviare a Security Hub un «battito cardiaco» ogni cinque minuti che indica che l'integrazione con Security Hub è funzionante?

Se puoi, fallo usando il tipo di `Heartbeat` ricerca.

AWS Security Hub informazioni sulla console

Fornisci al AWS Security Hub team un testo JSON contenente le seguenti informazioni. Security Hub utilizza queste informazioni per creare l'ARN del prodotto, visualizzare l'elenco dei provider nella console e includere le informazioni gestite proposte nella libreria di approfondimenti di Security Hub.

Informazioni sull'azienda

Le informazioni sulla società forniscono informazioni sulla vostra azienda. Ecco un esempio:

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

Le informazioni sulla società contengono i seguenti campi:

Campo	Richiesto	Descrizione
`id`	Sì	L'identificatore univoco dell'azienda. L'identif icativo della società deve essere unico per tutte le aziende. Probabilmente è uguale o simile a `name`. Tipo: stringa Lunghezza minima: 5 caratteri Lunghezza massima: 24 caratteri Caratteri consentiti: lettere minuscole, numeri e trattini Deve iniziare con una lettera minuscola. Deve terminare con una lettera minuscola o un numero.

Campo	Richiesto	Descrizione
`name`	Sì	Il nome dell'azienda del provider da visualizzare sulla console Security Hub. Tipo: stringa Lunghezza massima: 16 caratteri
`description`	Sì	La descrizione dell'azienda del provider da visualizzare sulla console Security Hub. Tipo: stringa Lunghezza massima: 200 caratteri

Informazioni sul prodotto

Questa sezione fornisce informazioni sul prodotto. Ecco un esempio:

```
{
    "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"
}
```

Le informazioni sul prodotto contengono i seguenti campi.

Campo	Richiesto	Descrizione
`IntegrationType`	Sì	Indica se il prodotto invia i risultati a Security Hub, riceve i risultati da Security Hub o invia e riceve entrambi i risultati. Se sei un partner di consulenza, lascia vuoto questo campo. Tipo: matrice di stringhe Valori validi: `SEND_FINDINGS_TO_SECURITY_HUB` | `RECEIVE_FINDINGS_FROM_SECURITY_HUB`
`id`	Sì	L'identificatore univoco del prodotto. Questi devono essere unici all'interno di un'azienda. Non è necessario che siano unici in tutte le aziende. Probabilmente è uguale o simile a `name`. Tipo: stringa Lunghezza minima: 5 caratteri Lunghezza massima: 24 caratteri Caratteri consentiti: lettere minuscole, numeri e trattini Deve iniziare con una lettera minuscola. Deve terminare con una lettera minuscola o un numero.
`regionsNotSupported`	Sì	Quali delle seguenti AWS regioni non sono supportate? In altre parole, in quali regioni Security Hub non dovrebbe mostrarti come opzione nella pagina dei nostri partner nella console Security Hub?

Campo	Richiesto	Descrizione
		Tipo: stringa Fornisci solo il codice regionale. Ad esempio `us-west-1` . Per un elenco delle regioni, consulta Endpoint regionali in. Riferimenti generali di AWS I codici regionali per i AWS GovCloud (US) sono `us-gov-west-1` (per AWS GovCloud (Stati Uniti occidentali)) e `us-gov-east-1` (per AWS GovCloud (Stati Uniti orientali)). I codici regionali per la Cina Le regioni sono `cn-north-1` (per la Cina (Pechino)) e `cn-northwest-1` (per la Cina (Ningxia)).

Campo	Richiesto	Descrizione
`commercialAccountNumber`	Sì	Il numero di AWS account principale del prodotto per le AWS regioni. Se invii i risultati a Security Hub, l'account fornito dipende da dove li invii. • Dal tuo AWS account. In questo caso, fornisci il numero di conto che utilizzi per inviare i risultati. • Dall' AWS account del cliente. In questo caso, Security Hub consiglia di fornire il numero di account principale da utilizzare per testare l'integrazione. Idealmente, utilizzerai lo stesso account per tutti i tuoi prodotti in tutte le regioni. Se ciò non è possibile, contatta il team del Security Hub. Se ricevi i risultati solo da Security Hub, questo numero di account non è richiesto. Tipo: stringa

Campo	Richiesto	Descrizione
`govcloudAccountNumber`	No	Il numero di AWS account principale del prodotto per AWS GovCloud (US) le regioni (se il prodotto è disponibile in AWS GovCloud (US)). Se invii i risultati a Security Hub, l'account fornito dipende da dove li invii. • Dal tuo AWS account. In questo caso, fornisci il numero di conto che utilizzi per inviare i risultati. • Dall' AWS account del cliente. In questo caso, Security Hub consiglia di fornire il numero di account principale da utilizzare per testare l'integrazione. Idealmente, è possibile utilizzare lo stesso account per tutti i prodotti in tutte le AWS GovCloud (US) regioni. Se ciò non è possibile, contatta il team del Security Hub. Se ricevi i risultati solo da Security Hub, questo numero di account non è richiesto. Tipo: stringa

Campo	Richiesto	Descrizione
`chinaAccountNumber`	No	Il numero di AWS account principale del prodotto per le regioni della Cina (se il prodotto è disponibile nelle regioni della Cina). Se invii i risultati a Security Hub, l'account fornito dipende da dove li invii. • Dal tuo AWS account. In questo caso, fornisci il numero di conto che utilizzi per inviare i risultati. • Dall' AWS account del cliente. In questo caso, Security Hub consiglia di fornire il numero di account principale da utilizzare per testare l'integrazione del prodotto. Idealmente, utilizzi lo stesso account per tutti i tuoi prodotti in tutte le regioni della Cina. Se ciò non è possibile, contatta il team del Security Hub. Se ricevi i risultati solo da Security Hub, può trattarsi di qualsiasi account che possiedi in una regione della Cina. Tipo: stringa
`name`	Sì	Il nome del prodotto del provider da visualizz are sulla console Security Hub. Tipo: stringa Lunghezza massima: 24 caratteri

Campo	Richiesto	Descrizione
`description`	Sì	La descrizione del prodotto del provider da visualizzare sulla console Security Hub. Tipo: stringa Lunghezza massima: 200 caratteri
`importType`	Sì	Il tipo di politica delle risorse per il partner. Durante il processo di onboarding del partner, è possibile specificare o specificare una delle seguenti politiche in materia di risorse. `NEITHER` • Con`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, puoi inviare i risultati a Security Hub solo dall'account indicato nell'ARN del prodotto. • Con`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, puoi inviare i risultati solo dall'account cliente che ti ha sottoscritto. Tipo: stringa Valori validi: `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` || `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` `NEITHER`

Campo	Richiesto	Descrizione
`category`	Sì	Le categorie che definiscono il prodotto. Le selezioni vengono visualizzate sulla console Security Hub. Scegli fino a tre categorie. Le selezioni personalizzate non sono consentite. Se ritieni che manchi la tua categoria, contatta il team di Security Hub. Tipo: Array Categorie disponibili: • `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` • `Data Classification`

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

Campo	Richiesto	Descrizione
		• `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`	No	L'URL della Marketplace AWS destinazione del prodotto. L'URL viene visualizzato nella console Security Hub. Tipo: stringa Deve essere un Marketplace AWS URL. Se non hai un' Marketplace AWS inserzione, lascia questo campo vuoto.

Campo	Richiesto	Descrizione
`configurationUrl`	Sì	L'URL della documentazione del prodotto sull'integrazione con Security Hub. Questo contenuto è ospitato sul tuo sito Web o su una pagina Web gestita dall'utente, ad esempio una GitHub pagina. Tipo: stringa La documentazione deve includere le seguenti informazioni. • Istruzioni di configurazione • Collegamenti ai AWS CloudFormation modelli (se necessario) • Informazioni sul caso d'uso dell'integrazione • Latenza • Mappatura ASFF • Tipi di risultati inclusi • Architettura

Linee guida e liste di controllo

Mentre prepari i materiali necessari per l' AWS Security Hub integrazione, utilizza queste linee guida.

La checklist di preparazione viene utilizzata per condurre una revisione finale dell'integrazione prima che Security Hub la renda disponibile ai clienti di Security Hub.

Argomenti

- Linee guida per la visualizzazione del logo sulla console AWS Security Hub
- Principi per la creazione e l'aggiornamento dei risultati
- Linee guida per la mappatura dei risultati nel AWS Security Finding Format (ASFF)
- Linee guida per l'utilizzo dell'API BatchImportFindings
- Lista di controllo per la preparazione del prodotto

Linee guida per la visualizzazione del logo sulla console AWS Security Hub

Per visualizzare il logo sulla AWS Security Hub console, segui queste linee guida.

Modalità chiare e scure

È necessario fornire sia una versione del logo in modalità chiara che una in modalità scura.

Formato

Formato di file SVG

Background color (Colore di sfondo)

Transparent

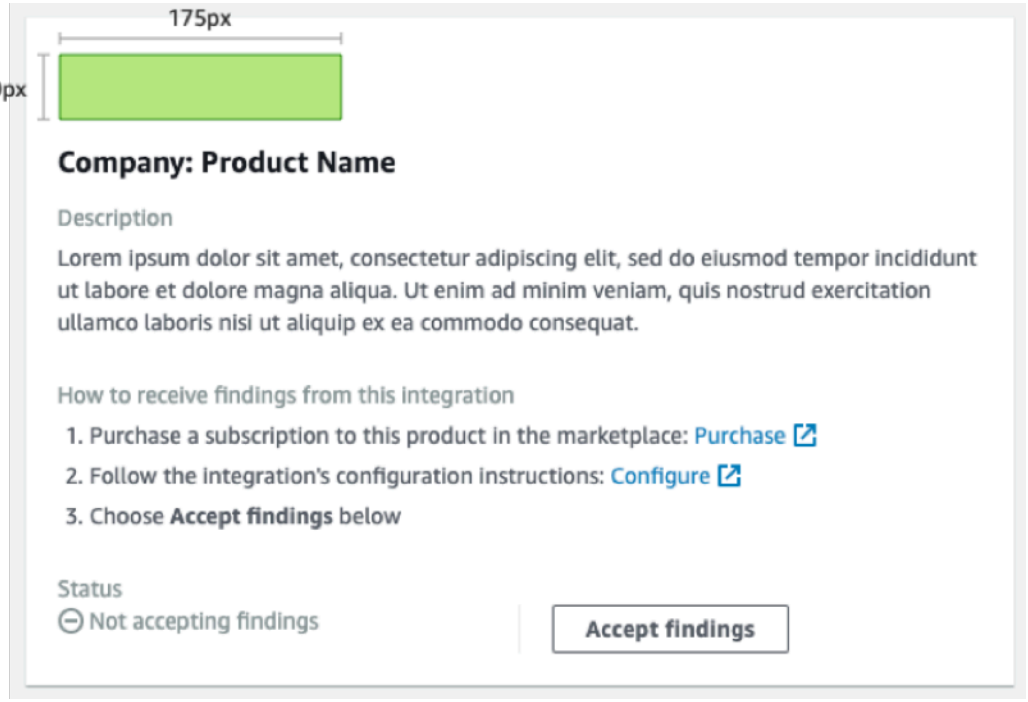
Size

Il rapporto ideale è 175 px di larghezza per 40 px di altezza.

L'altezza minima è di 40 px.

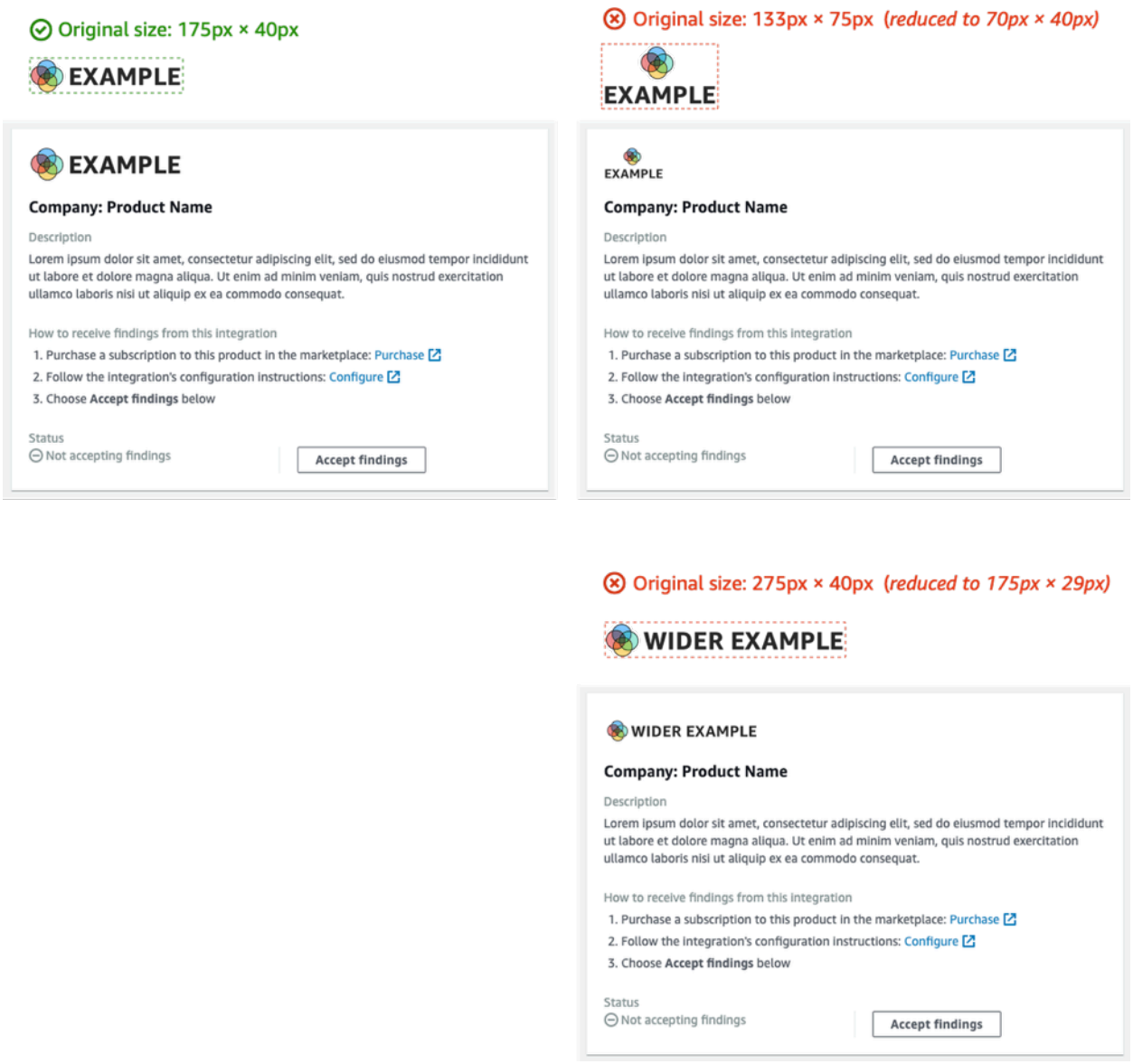
I loghi rettangolari funzionano meglio.

L'immagine seguente mostra come viene visualizzato un logo ideale sulla console Security Hub.



Se il logo non corrisponde a queste dimensioni, Security Hub riduce le dimensioni a un'altezza massima di 40 px e una larghezza massima di 175 px. Ciò influisce sulla modalità di visualizzazione del logo sulla console Security Hub.

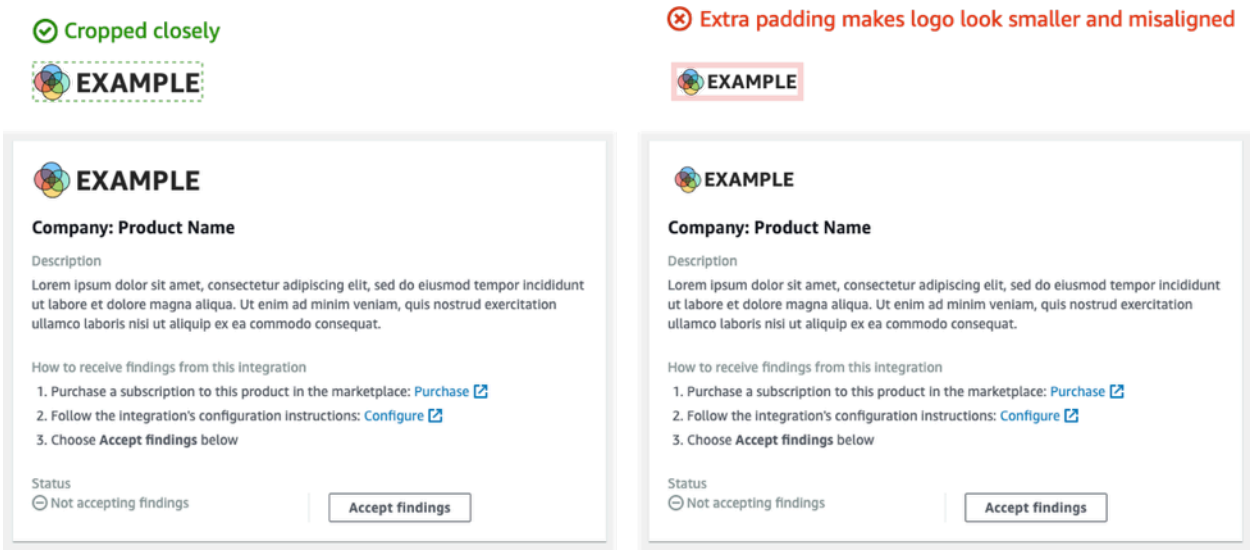
L'immagine seguente confronta la visualizzazione di un logo che utilizzava la dimensione ideale con loghi più larghi o più alti.



Ritaglio

Ritaglia l'immagine del logo il più vicino possibile. Non fornire imbottitura aggiuntiva.

L'immagine seguente mostra la differenza tra un logo ritagliato da vicino e un logo con un'imbottitura aggiuntiva.



Principi per la creazione e l'aggiornamento dei risultati

Mentre pianifichi come creare e aggiornare i risultati AWS Security Hub, tieni a mente i seguenti principi.

Rendi specifici i risultati in modo che i clienti possano agire facilmente sulla base di essi.

I clienti desiderano automatizzare le azioni di risposta e correzione e correlare i risultati con altri risultati. A supporto di ciò, i risultati devono avere le seguenti caratteristiche:

- In genere dovrebbero riguardare una risorsa singola o primaria.
- Dovrebbero avere un unico tipo di ricerca.
- Dovrebbero occuparsi di un unico evento di sicurezza.

Quando un risultato contiene dati relativi a più eventi di sicurezza, è più difficile per i clienti intervenire sulla base del risultato.

Associa tutti i campi di ricerca al AWS Security Finding Format (ASFF). Consenti ai clienti di fare affidamento sul Security Hub come fonte di verità.

I clienti si aspettano che ogni campo presente nel formato di ricerca nativo sia rappresentato anche nel Security Hub ASFF.

I clienti vogliono che tutti i dati siano presenti nella versione Security Hub del risultato. La mancanza di dati fa sì che perdano la fiducia in Security Hub come fonte centrale di informazioni sulla sicurezza.

Riduci al minimo la ridondanza nei risultati. Non sovraccaricate i clienti con la ricerca di volumi.

Security Hub non è uno strumento generale di gestione dei log. È necessario inviare a Security Hub risultati altamente utilizzabili e ai quali i clienti possano rispondere direttamente, correggere o correlare con altri risultati.

Se c'è solo una piccola modifica al risultato, aggiorna il risultato invece di crearne uno nuovo.

Quando viene apportata una modifica importante al risultato, ad esempio al punteggio di gravità o all'identificatore della risorsa, crea un nuovo risultato.

Ad esempio, creare risultati per le scansioni di singole porte in tempo reale non è molto fattibile. Poiché la scansione delle porte può avvenire continuamente, produrrebbe un grande volume di risultati. È molto più interessante e preciso aggiornare semplicemente l'ora dell'ultima scansione e il conteggio delle scansioni su un singolo risultato per una scansione delle porte su una porta MongoDB da un nodo TOR.

Consenti ai clienti di personalizzare le proprie scoperte per renderle più significative.

I clienti vogliono poter modificare determinati campi di ricerca per renderli più pertinenti al loro ambiente o ai loro requisiti.

Ad esempio, i clienti vogliono poter aggiungere note, tag e modificare i punteggi di gravità in base al tipo di account o al tipo di risorsa a cui è associata la ricerca.

Linee guida per la mappatura dei risultati nel AWS Security Finding Format (ASFF)

Utilizza le seguenti linee guida per associare i risultati all'ASFF. Per descrizioni dettagliate di ogni campo e oggetto ASFF, consulta AWS Security Finding Format (ASFF) nella Guida per l'AWS Security Hub utente.

Informazioni identificative

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

`ProductArn`è l'ARN che ti AWS Security Hub assegna.

`Id`è il valore utilizzato da Security Hub per indicizzare i risultati. L'identificatore del risultato deve essere univoco, per garantire che altri risultati non vengano sovrascritti. Per aggiornare un risultato, invia nuovamente il risultato con lo stesso identificatore.

`GeneratorId`può essere uguale `Id` o fare riferimento a un'unità logica discreta, come un Amazon GuardDuty detector ID, un AWS Config recorder ID o un ID IAM Access Analyzer.

Title e Description

`Title`dovrebbe contenere alcune informazioni sulla risorsa interessata. `Title`è limitato a 256 caratteri, spazi inclusi.

Aggiungi informazioni più dettagliate a`Description`. `Description`è limitato a 1024 caratteri, spazi inclusi. Puoi prendere in considerazione l'aggiunta del troncamento alle descrizioni. Ecco un esempio:

```
"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.",
```

Tipi di esiti

Fornisci le informazioni sul tipo di ricerca in. `FindingProviderFields.Types`

`Types`deve corrispondere alla tassonomia dei tipi per ASFF.

Se necessario, è possibile specificare un classificatore personalizzato (il terzo spazio dei nomi).

Timestamp

Il formato ASFF include alcuni timestamp diversi.

`CreatedAt` e `UpdatedAt`

Devi inviare `CreatedAt` `UpdatedAt` ogni volta che chiami `BatchImportFindings`per ogni risultato.

I valori devono corrispondere al formato ISO86 01 in Python 3.8.

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

`FirstObservedAt` e `LastObservedAt`

`FirstObservedAte` `LastObservedAt` devono corrispondere al momento in cui il sistema ha osservato il risultato. Se non si registrano queste informazioni, non è necessario inviare questi timestamp.

I valori corrispondono al formato ISO86 01 in Python 3.8.

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

Severity

Fornisci informazioni sulla gravità nell'`FindingProviderFields.Severity`oggetto, che contiene i seguenti campi.

`Original`

Il valore di gravità del sistema. `Original`può essere qualsiasi stringa, per adattarsi al sistema in uso.

`Label`

L'indicatore di gravità del rilevamento richiesto dal Security Hub. I valori consentiti sono i seguenti.

- `INFORMATIONAL`— Non è stato riscontrato alcun problema.
- `LOW`— Il problema non richiede di per sé un'azione.
- `MEDIUM`— La questione deve essere affrontata, ma non con urgenza.
- `HIGH`— La questione deve essere affrontata in via prioritaria.
- `CRITICAL`— Il problema deve essere risolto immediatamente per prevenire ulteriori danni.

I risultati conformi avrebbero dovuto essere sempre impostati `Label` su. `INFORMATIONAL` Esempi di `INFORMATIONAL` risultati sono i risultati dei controlli di sicurezza che sono stati superati e AWS Firewall Manager i risultati che sono stati corretti.

I clienti spesso ordinano i risultati in base alla loro gravità per fornire ai team addetti alle operazioni di sicurezza un elenco di cose da fare. Siate prudenti quando impostate la gravità del risultato su `HIGH` o`CRITICAL`.

La documentazione di integrazione deve includere le motivazioni della mappatura.

Remediation

`Remediation`ha due elementi. Questi elementi vengono combinati nella console Security Hub.

`Remediation.Recommendation.Text`appare nella sezione Riparazione dei dettagli del risultato. È collegato ipertestualmente al valore di. `Remediation.Recommendation.Url`

Attualmente, solo i risultati degli standard Security Hub, IAM Access Analyzer e Firewall Manager mostrano collegamenti ipertestuali alla documentazione su come correggere il risultato.

SourceUrl

Utilizzalo solo `SourceUrl` se puoi fornire un URL con collegamento diretto alla tua console per quel risultato specifico. Altrimenti, omettilo dalla mappatura.

Security Hub non supporta i collegamenti ipertestuali da questo campo, ma è esposto nella console Security Hub.

Malware, Network, Process, ThreatIntelIndicators

Se applicabile, usa `Malware` `NetworkProcess`, o`ThreatIntelIndicators`. Ciascuno di questi oggetti è esposto nella console Security Hub. Utilizzate questi oggetti nel contesto del risultato che state inviando.

Ad esempio, se rilevi un malware che stabilisce una connessione in uscita a un nodo di comando e controllo noto, fornisci i dettagli relativi all' EC2 istanza in`Resource.Details.AwsEc2Instance`. Fornisci gli `ThreatIntelIndicator` oggetti pertinenti `Malware` e per quell' EC2istanza. `Network`

Malware

`Malware`è un elenco che accetta fino a cinque matrici di informazioni sul malware. Rendi le voci relative al malware pertinenti alla risorsa e alla scoperta.

Ogni voce contiene i seguenti campi.

`Name`

Il nome del malware. Il valore è una stringa composta da un massimo di 64 caratteri.

`Name`deve provenire da una fonte controllata di intelligence o di ricercatori sulle minacce.

`Path`

Il percorso verso il malware. Il valore è una stringa composta da un massimo di 512 caratteri. `Path`deve essere un percorso di file di sistema Linux o Windows, tranne nei seguenti casi.

- Se esegui la scansione degli oggetti in un bucket S3 o in una condivisione EFS in base alle regole YARA, allora `Path` è il percorso dell'oggetto S3://o HTTPS.
- Se esegui la scansione di file in un repository Git, allora `Path` è l'URL Git o il percorso del clone.

`State`

Lo stato del malware. I valori consentiti sono `OBSERVED` | `REMOVAL_FAILED` |`REMOVED`.

Nel titolo e nella descrizione del risultato, assicurati di fornire un contesto per ciò che è accaduto con il malware.

Ad esempio, in caso `Malware.State` `REMOVED` affermativo, il titolo e la descrizione del risultato dovrebbero indicare che il prodotto ha rimosso il malware presente nel percorso.

In caso `Malware.State` `OBSERVED` affermativo, il titolo e la descrizione del risultato dovrebbero indicare che il prodotto ha rilevato il malware localizzato lungo il percorso.

`Type`

Indica il tipo di malware. I valori consentiti sono `ADWARE` `BLENDED_THREAT` | `BOTNET_AGENT` | `COIN_MINER` | `EXPLOIT_KIT` | `KEYLOGGER` | `MACRO` | `POTENTIALLY_UNWANTED` | `SPYWARE` | `RANSOMWARE` | `REMOTE_ACCESS` | `ROOTKIT` | `TROJAN` | `VIRUS` |`WORM`.

Se hai bisogno di un valore aggiuntivo per`Type`, contatta il team di Security Hub.

Network

`Network`è un oggetto singolo. Non è possibile aggiungere più dettagli relativi alla rete. Durante la mappatura dei campi, utilizza le seguenti linee guida.

Informazioni sulla destinazione e sulla fonte

La destinazione e l'origine sono facili da mappare i log di flusso TCP o VPC o i log WAF. Sono più difficili da usare quando si descrivono le informazioni di rete per individuare un attacco.

In genere, la fonte è l'origine dell'attacco, ma potrebbe avere altre fonti, come quelle elencate di seguito. È necessario spiegare la fonte nella documentazione e descriverla anche nel titolo e nella descrizione del reperto.

- Per un attacco DDo S su un' EC2 istanza, la fonte è l'aggressore, anche se un attacco DDo S reale può utilizzare milioni di host. La destinazione è l' IPv4 indirizzo pubblico dell' EC2 istanza. `Direction`è IN.
- Per il malware osservato mentre comunica da un' EC2 istanza a un nodo di comando e controllo noto, l'origine è l' IPV4 indirizzo dell' EC2 istanza. La destinazione

è il nodo di comando e controllo. `Direction`è`0UT`. Forniresti anche `Malware` e`ThreatIntelIndicators`.

`Protocol`

`Protocol`esegue sempre il mapping su un nome registrato della Internet Assigned Numbers Authority (IANA), a meno che non sia possibile fornire un protocollo specifico. Dovresti sempre usarlo e fornire le informazioni sulla porta.

`Protocol`è indipendente dalle informazioni di origine e destinazione. Forniscile solo quando ha senso farlo.

`Direction`

`Direction`è sempre relativo ai confini della AWS rete.

- `IN`significa che sta entrando AWS (VPC, servizio).
- `0UT`significa che sta uscendo dai confini della AWS rete.

Process

`Process`è un oggetto singolo. Non è possibile aggiungere più dettagli relativi al processo. Durante la mappatura dei campi, utilizza le seguenti linee guida.

`Name`

`Name`deve corrispondere al nome dell'eseguibile. Accetta fino a 64 caratteri.

`Path`

`Path`è il percorso del file system verso l'eseguibile del processo. Accetta fino a 512 caratteri.

`Pid`, **`ParentPid`**

`Pid`e `ParentPid` deve corrispondere all'identificatore di processo Linux (PID) o all'ID evento di Windows. Per differenziare, usa EC2 Amazon Machine Images (AMI) per fornire le informazioni. I clienti possono probabilmente distinguere tra Windows e Linux.

Timestamp (e) **`LaunchedAt`** **`TerminatedAt`**

Se non è possibile recuperare in modo affidabile queste informazioni e non sono accurate al millisecondo, non fornirle.

Se un cliente si affida ai timestamp per le indagini forensi, non avere un timestamp è meglio che avere un timestamp sbagliato.

ThreatIntelIndicators

`ThreatIntelIndicators`accetta una serie di fino a cinque oggetti di intelligence sulle minacce.

Per ogni voce, `Type` rientra nel contesto della minaccia specifica. I valori consentiti sono `DOMAIN` `EMAIL_ADDRESS` | `HASH_MD5` | `HASH_SHA1` | `HASH_SHA256` | `HASH_SHA512` | `IPV4_ADDRESS` | `IPV6_ADDRESS` | `MUTEX` | `PROCESS` |`URL`.

Ecco alcuni esempi di come mappare gli indicatori di intelligence sulle minacce:

- Hai scoperto un processo che sai essere associato a Cobalt Strike. L'hai imparato dal FireEye nostro blog.

  Imposta `Type` su `PROCESS`. Crea anche un `Process` oggetto per il processo.
- Il tuo filtro di posta ha rilevato che qualcuno ha inviato un noto pacchetto con hash da un dominio malevolo noto.

  Crea due `ThreatIntelIndicator` oggetti. Un oggetto è per`DOMAIN`. L'altro è per il`HASH_SHA1`.
- Hai trovato un malware con una regola Yara (Loki, Fenrir, Awss3,). VirusScan BinaryAlert

  Crea due oggetti. `ThreatIntelIndicator` Uno è per il malware. L'altro è per il`HASH_SHA1`.

Resources

Infatti`Resources`, utilizza i tipi di risorse e i campi di dettaglio forniti ogni volta che è possibile. Security Hub aggiunge costantemente nuove risorse all'ASFF. `<Per ricevere un registro mensile delle modifiche ad ASFF, contatta securityhub-`

Se non riesci a inserire le informazioni nei campi dei dettagli per un tipo di risorsa modellato, mappa i dettagli rimanenti a. `Details.Other`

Per una risorsa non modellata in ASFF, impostate su. `Type` `Other` Per informazioni dettagliate, utilizzare. `Details.Other`

È inoltre possibile utilizzare il tipo di `Other` risorsa per informazioni non AWS risultanti.

ProductFields

Utilizzalo solo `ProductFields` se non puoi utilizzare un altro campo curato per `Resources` o un oggetto descrittivo come `ThreatIntelIndicatorsNetwork`, o. `Malware`

Se lo utilizzi`ProductFields`, devi fornire una motivazione rigorosa per questa decisione.

Conformità

Utilizzalo solo `Compliance` se i risultati sono correlati alla conformità.

Security Hub utilizza `Compliance` i risultati che genera in base ai controlli.

Firewall Manager utilizza `Compliance` i risultati perché sono correlati alla conformità.

Campi con restrizioni

Questi campi sono destinati ai clienti per tenere traccia delle indagini condotte su un risultato.

Non eseguire la mappatura su questi campi o oggetti.

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

Per questi campi, esegui il mapping ai campi presenti nell'`FindingProviderFields`oggetto. Non eseguire il mapping ai campi di primo livello.

- `Confidence`— Includi un punteggio di affidabilità (0-99) solo se il tuo servizio ha una funzionalità simile o se condividi al 100% la tua opinione.
- `Criticality`— Il punteggio di criticità (0-99) ha lo scopo di esprimere l'importanza della risorsa associata alla scoperta.
- `RelatedFindings`— Fornisci risultati correlati solo se puoi tenere traccia dei risultati relativi alla stessa risorsa o tipo di scoperta. Per identificare un risultato correlato, è necessario fare riferimento all'identificatore del risultato di un risultato già presente in Security Hub.

Linee guida per l'utilizzo dell'API **`BatchImportFindings`**

Quando utilizzi l'operazione `BatchImportFindings`API per inviare i risultati a AWS Security Hub, utilizza le seguenti linee guida.

- È necessario chiamare `BatchImportFindings`utilizzando l'account associato ai risultati. L'identificatore dell'account associato è il valore dell'`AwsAccountId`attributo per il risultato.
- Invia il batch più grande possibile. Security Hub accetta fino a 100 risultati per batch, fino a 240 KB per risultato e fino a 6 MB per batch.
- Il limite di velocità di accelerazione è di 10 TPS per account per regione, con un picco di 30 TPS.
- È necessario implementare un meccanismo per mantenere lo stato dei risultati in caso di limitazione o problemi di rete. È inoltre necessario lo stato dei risultati in modo da poter inviare gli aggiornamenti dei risultati man mano che un risultato diventa o non è conforme.
- Per informazioni sulle lunghezze massime delle stringhe e altre limitazioni, consulta AWS Security Finding Format (ASFF) nella Guida per l'AWS Security Hub utente.

Lista di controllo per la preparazione del prodotto

I team APN AWS Security Hub e i partner APN utilizzano questa lista di controllo per verificare che l'integrazione sia pronta per essere lanciata.

Mappatura ASFF

Queste domande riguardano la mappatura dei risultati ottenuti con il AWS Security Finding Format (ASFF).

Tutti i dati di ricerca del partner sono mappati in ASFF?

> Associa in qualche modo tutte le tue scoperte all'ASFF.
>
> Usa campi curati come tipi di risorse modellati,`Network`, `Malware` o. `ThreatIntelIndicators`
>
> Mappa qualsiasi altra cosa in `Resource.Details.Other` o `ProductFields` come appropriato.

Il partner utilizza **`Resource.Details`** campi come **`AwsEc2instanceAwsS3Bucket`**, e**`Container`**? Il partner utilizza **`Resource.Details.Other`** per definire i dettagli delle risorse che non sono modellati nell'ASFF?

> Quando possibile, utilizza i campi forniti per inserire nei risultati risorse curate come EC2 istanze, bucket S3 e gruppi di sicurezza.

Mappa le altre informazioni relative alle risorse `Resource.Details.Other` solo quando non esiste una corrispondenza diretta.

Il partner mappa i valori su**`UserDefinedFields`**?

Non usare `UserDefinedFields`.

Prendi in considerazione l'utilizzo di un altro campo curato, ad esempio `Resource.Details.Other` o`ProductFields`.

Il partner mappa le informazioni **`ProductFields`** che potrebbero essere mappate in altri campi ASFF?

Utilizzale solo `ProductFields` per informazioni specifiche sul prodotto, come informazioni sulla versione, rilevamenti di gravità specifici del prodotto o altre informazioni che non possono essere mappate in un campo curato o. `Resources.Details.Other`

Il partner importa i propri timestamp per? **`FirstObservedAt`**

Il `FirstObservedAt` timestamp ha lo scopo di registrare l'ora in cui è stato osservato un risultato nel prodotto. Mappare questo campo, se possibile.

Il partner fornisce valori univoci generati per ogni identificatore di risultato, ad eccezione dei risultati che desidera aggiornare?

Tutti i risultati in Security Hub sono indicizzati in base all'identificatore del risultato (`Id`attributo). Questo valore deve essere sempre unico per garantire che i risultati non vengano aggiornati accidentalmente.

È inoltre necessario mantenere lo stato dell'identificatore dei risultati allo scopo di aggiornare i risultati.

Il partner fornisce un valore che associa i risultati a un ID del generatore?

`GeneratorID`non deve avere lo stesso valore dell'ID del risultato.

`GeneratorID`dovrebbe essere in grado di collegare logicamente i risultati in base a ciò che li ha generati.

Può essere un sottocomponente all'interno di un prodotto (Prodotto A - Vulnerabilità vs Prodotto A - EDR) o qualcosa di simile.

Il partner utilizza i namespace dei tipi di ricerca richiesti in modo pertinente al proprio prodotto? Il partner utilizza le categorie o i classificatori dei tipi di ricerca consigliati nei propri tipi di ricerca?

La tassonomia dei tipi di risultati dovrebbe corrispondere fedelmente ai risultati generati dal prodotto.

I namespace di primo livello descritti nel Security Finding Format sono obbligatori. AWS

È possibile utilizzare valori personalizzati per i namespace di secondo e terzo livello (Categorie o Classificatori).

Il partner acquisisce informazioni sul flusso di rete nei **`Network`** campi, se dispone di dati di rete?

Se il prodotto acquisisce NetFlow informazioni, associale al `Network` campo.

Il partner acquisisce informazioni sul processo (PID) nei **`Process`** campi, se dispone di dati di processo?

Se il prodotto acquisisce informazioni sul processo, associale al `Process` campo.

Il partner acquisisce informazioni sul malware nei **`Malware`** campi, se dispone di dati relativi al malware?

Se il prodotto acquisisce informazioni sul malware, associale al `Malware` campo.

Il partner acquisisce informazioni di intelligence sulle minacce sul **`ThreatIntelIndicators`** campo, se dispone di dati di intelligence sulle minacce?

Se il prodotto acquisisce informazioni di intelligence sulle minacce, associale al `ThreatIntelIndicators` campo.

Il partner fornisce una valutazione di affidabilità dei risultati? Se lo fanno, viene fornita una motivazione?

Ogni volta che utilizzi questo campo, fornisci una motivazione nella documentazione e nel manifesto.

Il partner utilizza un ID canonico o un ARN per l'ID della risorsa nella ricerca?

Quando si identificano AWS le risorse, la procedura migliore consiste nell'utilizzare l'ARN. Se un ARN non è disponibile, usa l'ID di risorsa canonico.

Configurazione e funzione di integrazione

Queste domande riguardano la configurazione e day-to-day la funzione dell'integrazione.

Il partner fornisce un modello infrastructure-as-code (IaC) per implementare l'integrazione con Security Hub, come Terraform, AWS CloudFormation oppure? AWS Cloud Development Kit (AWS CDK)

Per le integrazioni che invieranno i risultati dall'account del cliente o utilizzeranno CloudWatch Events per utilizzare i risultati, è necessaria una qualche forma di modello IaC.

AWS CloudFormation è preferibile, ma AWS CDK è possibile utilizzare anche Terraform.

Il prodotto partner dispone di una configurazione con un clic sulla console per l'integrazione con Security Hub?

Alcuni prodotti partner utilizzano un interruttore o un meccanismo simile per attivare l'integrazione. Ciò può comportare il rifornimento automatico di risorse e autorizzazioni. Se invii i risultati da un account di prodotto, il metodo preferito è la configurazione con un solo clic.

Il partner invia solo risultati utili?

In genere è necessario inviare solo i risultati che hanno un valore di sicurezza ai clienti di Security Hub.

Security Hub non è uno strumento generale di gestione dei log. Non dovresti inviare tutti i log possibili a Security Hub.

Il partner ha fornito una stima del numero di risultati che invierà al giorno per cliente e con quale frequenza (media e raffica)?

Per calcolare il carico su Security Hub vengono utilizzati numeri di risultati univoci. Un risultato unico è definito come un risultato con una mappatura ASFF diversa da un altro risultato.

Ad esempio, se un risultato è compilato solo `ThreatIntelIndicators` e un altro solo popolato`Resources.Details.AWSEc2Instance`, si tratta di due risultati unici.

Il partner è in grado di gestire gli errori 4xx e 5xx in modo da non limitarli e inviare tutti i risultati in un secondo momento?

Attualmente esiste una frequenza di burst di 30-50 TPS sul funzionamento dell'API. `BatchImportFindings` Se vengono restituiti errori 4xx o 5xx, è necessario mantenere lo stato di tali risultati non riusciti in modo da poterli riprovare completamente in un secondo momento. Puoi farlo tramite una coda di lettere morte o altri servizi di AWS messaggistica come Amazon SNS o Amazon SQS.

Il partner mantiene lo stato dei risultati in modo da sapere archiviare i risultati che non sono più presenti?

Se si prevede di aggiornare i risultati sovrascrivendo l'ID del risultato originale, è necessario disporre di un meccanismo per mantenere lo stato in modo che le informazioni corrette vengano aggiornate per il risultato corretto.

Se fornite i risultati, non utilizzate l'`BatchUpdateFindings`operazione per aggiornare i risultati. Questa operazione deve essere utilizzata solo dai clienti. Si utilizza solo `BatchUpdateFindings`quando si indagano e si interviene in base ai risultati.

Il partner gestisce i nuovi tentativi in modo da non compromettere i risultati positivi inviati in precedenza?

È necessario disporre di un meccanismo che consenta di conservare i risultati originali IDs in caso di errori, in modo da non duplicare o sovrascrivere erroneamente i risultati riusciti.

Il partner aggiorna i risultati richiamando l'**`BatchImportFindings`**operazione con l'ID di ricerca dei risultati esistenti?

Per aggiornare un risultato, è necessario sovrascrivere il risultato esistente inviando lo stesso ID del risultato.

L'`BatchUpdateFindings`operazione deve essere utilizzata solo dai clienti.

Il partner aggiorna i risultati utilizzando l'**`BatchUpdateFindings`**API?

Se si interviene sui risultati, è possibile utilizzare l'`BatchUpdateFindings`operazione per aggiornare campi specifici.

Il partner fornisce informazioni sulla latenza tra il momento in cui viene creato un risultato e il momento in cui viene inviato dal proprio prodotto a Security Hub?

È necessario ridurre al minimo la latenza per garantire che i clienti visualizzino i risultati il prima possibile in Security Hub.

Queste informazioni sono obbligatorie nel manifesto.

Se l'architettura del partner prevede l'invio dei risultati a Security Hub da un account cliente, lo hanno dimostrato con successo? Se l'architettura del partner prevede l'invio dei risultati a Security Hub dal proprio account, lo hanno dimostrato con successo?

Durante i test, i risultati devono essere inviati correttamente da un account di tua proprietà diverso dall'account fornito per l'ARN del prodotto.

L'invio di un risultato dall'account del proprietario dell'ARN del prodotto può aggirare alcune eccezioni di errore nelle operazioni API.

Il partner fornisce informazioni sul battito cardiaco a Security Hub?

Per dimostrare che l'integrazione funziona correttamente, è necessario inviare un risultato del battito cardiaco. Il risultato del battito cardiaco viene inviato ogni cinque minuti e utilizza il tipo di risultato. `Heartbeat`

Questo è importante se invii i risultati da un account di prodotto.

Il partner si è integrato con l'account del team di prodotto Security Hub durante i test?

Durante la convalida di preproduzione, è necessario inviare esempi di risultati all'account del team di prodotto Security Hub. AWS Questi esempi dimostrano che i risultati vengono inviati e mappati correttamente.

Documentazione

Queste domande si riferiscono alla documentazione dell'integrazione fornita.

Il partner ospita la propria documentazione su un sito Web dedicato?

La documentazione deve essere ospitata sul tuo sito web come pagina web statica, wiki, Read the Docs o altro formato dedicato.

La documentazione di hosting su GitHub non soddisfa i requisiti del sito Web dedicato.

La documentazione del partner fornisce istruzioni su come configurare l'integrazione del Security Hub?

È possibile configurare l'integrazione utilizzando un modello IaC o un'integrazione «one-click» basata su console.

La documentazione dei partner fornisce una descrizione del loro caso d'uso?

Il caso d'uso fornito nel manifesto deve essere descritto anche nella documentazione

La documentazione fornita dai partner fornisce una motivazione alla base dei risultati inviati?

È necessario fornire le motivazioni alla base dei tipi di risultati inviati.

Ad esempio, il tuo prodotto potrebbe fornire risultati per vulnerabilità, malware e antivirus, ma invii i risultati di vulnerabilità e malware solo a Security Hub. In tal caso, è necessario fornire una motivazione per cui non si inviano i risultati relativi all'antivirus.

La documentazione del partner fornisce una giustificazione del modo in cui il partner associa i propri risultati ad ASFF?

È necessario fornire la motivazione per la mappatura dei risultati nativi di un prodotto su ASFF. I clienti vogliono sapere dove cercare informazioni specifiche sul prodotto.

La documentazione del partner fornisce indicazioni su come il partner aggiorna i risultati, se aggiorna i risultati?

Fornisci ai clienti informazioni su come mantenere lo stato, garantire l'idempotenza e sovrascrivere i risultati con informazioni. up-to-date

La documentazione del partner descrive la ricerca della latenza?

Riduci al minimo la latenza per garantire che i clienti vedano i risultati il prima possibile in Security Hub.

Queste informazioni sono obbligatorie nel manifesto.

La documentazione del partner descrive in che modo il loro punteggio di gravità si collega al punteggio di gravità ASFF?

Fornisci informazioni su come mappare. `Severity.Original` `Severity.Label`

Ad esempio, se il valore di gravità è un grado in lettere (A, B, C), è necessario fornire informazioni su come associare il grado della lettera all'etichetta di gravità.

La documentazione relativa ai partner fornisce una giustificazione alla base dei punteggi di fiducia?

Se fornisci punteggi di fiducia, questi punteggi devono essere classificati.

Se utilizzi punteggi o mappature di confidenza compilati staticamente derivati dall'intelligenza artificiale o dall'apprendimento automatico, dovresti fornire un contesto aggiuntivo.

La documentazione del partner indica quali regioni il partner supporta e non supporta?

Nota le regioni che sono o non sono supportate in modo che i clienti sappiano in quali regioni non tentare un'integrazione.

Informazioni sulla scheda del prodotto

Queste domande riguardano la scheda del prodotto visualizzata nella pagina Integrazioni della console Security Hub.

L'ID dell' AWS account fornito è valido e contiene 12 cifre?

Gli identificatori dell'account sono composti da 12 cifre. Se un ID account contiene meno di 12 cifre, l'ARN del prodotto non sarà valido.

La descrizione del prodotto contiene 200 o meno caratteri?

La descrizione del prodotto fornita in formato JSON all'interno del manifesto non deve superare i 200 caratteri, spazi inclusi.

Il link di configurazione porta alla documentazione per l'integrazione?

Il link di configurazione dovrebbe portare alla documentazione online. Non dovrebbe portare al tuo sito web principale o a pagine di marketing.

Il link per l'acquisto (se fornito) porta all' Marketplace AWS elenco del prodotto?

Se fornisci un link per l'acquisto, deve essere un link per Marketplace AWS l'iscrizione. Security Hub non accetta link di acquisto non ospitati da AWS.

Le categorie di prodotti descrivono correttamente il prodotto?

Nel manifesto, puoi fornire fino a tre categorie di prodotti. Queste devono corrispondere al codice JSON e non possono essere personalizzate. Non puoi fornire più di tre categorie di prodotti.

I nomi delle aziende e dei prodotti sono validi e corretti?

Il nome dell'azienda deve contenere al massimo 16 caratteri.

Il nome del prodotto deve contenere al massimo 24 caratteri.

Il nome del prodotto nella scheda prodotto JSON deve corrispondere al nome nel manifesto.

Informazioni di marketing

Queste domande riguardano il marketing per l'integrazione.

La descrizione del prodotto per la pagina dei partner del Security Hub non supera i 700 caratteri, spazi inclusi?

La pagina dei partner di Security Hub accetta solo fino a 700 caratteri, spazi inclusi.

Il team modificherà le descrizioni più lunghe.

Il logo della pagina dei partner di Security Hub non supera le dimensioni di 600 x 300 px?

Fornisci un URL accessibile al pubblico con un logo aziendale in PNG o JPG di dimensioni non superiori a 600 x 300 pixel.

Il collegamento ipertestuale Ulteriori informazioni nella pagina dei partner di Security Hub conduce alla pagina Web dedicata del partner sull'integrazione?

Il link Ulteriori informazioni non deve portare al sito Web principale del partner o alle informazioni sulla documentazione.

Questo collegamento deve sempre indirizzare a una pagina Web dedicata con informazioni di marketing sull'integrazione.

Il partner fornisce una demo o un video didattico su come utilizzare la propria integrazione?

Una dimostrazione o un video illustrativo sull'integrazione sono facoltativi ma consigliati.

È stato pubblicato un post sul blog di AWS Partner Network con il partner e il suo responsabile dello sviluppo dei partner o rappresentante dello sviluppo dei partner?

AWS I post sul blog di Partner Network devono essere coordinati in anticipo con il responsabile dello sviluppo del partner o il rappresentante dello sviluppo del partner.

Questi sono separati da qualsiasi post sul blog che crei tu stesso.

Attendi 4-6 settimane di tempo di consegna. Questo sforzo dovrebbe essere avviato dopo il completamento del test con il prodotto privato ARN.

È in corso di pubblicazione un comunicato stampa guidato dai partner?

Puoi collaborare con il tuo partner development manager o con un rappresentante dello sviluppo partner per ottenere un preventivo dal vicepresidente dei servizi di sicurezza esterni. Puoi utilizzare questa citazione nel tuo comunicato stampa.

È in fase di pubblicazione un post sul blog gestito dai partner?

Puoi creare i tuoi post sul blog per mostrare l'integrazione anche al di fuori del blog di AWS Partner Network.

È in fase di pubblicazione un webinar guidato dai partner?

Puoi creare i tuoi webinar per mostrare l'integrazione.

Se hai bisogno di assistenza dal team di Security Hub, collabora con il team di prodotto dopo aver completato il test con il prodotto privato ARN.

Il partner ha richiesto l'assistenza sui social media a AWS?

Dopo il rilascio, puoi collaborare con il responsabile marketing AWS di Security per utilizzare i canali di social media AWS ufficiali per condividere i dettagli dei tuoi webinar.

AWS Security Hub domande frequenti per i partner

Di seguito sono riportate le domande più comuni sulla configurazione e la manutenzione di un'integrazione con AWS Security Hub.

1. Quali sono i vantaggi dell'integrazione con Security Hub?
   - Soddisfazione del cliente: il motivo principale per l'integrazione con Security Hub è perché i clienti lo richiedono.

     Security Hub è il centro di sicurezza e conformità per AWS i clienti. È progettato come la prima tappa in cui i professionisti della AWS sicurezza e della conformità si recano ogni giorno per comprendere il loro stato di sicurezza e conformità.

     Ascoltate i vostri clienti. Ti diranno se vogliono vedere le tue scoperte in Security Hub.
   - Opportunità di scoperta: promuoviamo i partner con integrazioni certificate all'interno della console Security Hub, inclusi i link alle loro Marketplace AWS offerte. Questo è un ottimo modo per i clienti di scoprire nuovi prodotti per la sicurezza.
   - Opportunità di marketing: i fornitori con integrazioni approvate possono partecipare a webinar, pubblicare comunicati stampa, creare fogli informativi e dimostrare le proprie integrazioni ai clienti. AWS
2. Quali tipi di partner esistono?
   - Partner che inviano i risultati a Security Hub
   - Partner che riceve i risultati dal Security Hub
   - Partner che inviano e ricevono i risultati
   - Partner di consulenza che aiutano i clienti a configurare, personalizzare e utilizzare Security Hub nel loro ambiente
3. In che modo l'integrazione di un partner con Security Hub funziona a un livello elevato?

   Raccogli i risultati all'interno di un account cliente o dal tuo AWS account e trasformi il formato dei risultati nel AWS Security Finding Format (ASFF). I risultati vengono quindi trasmessi all'endpoint regionale del Security Hub appropriato.

   Puoi anche utilizzare CloudWatch Events per ricevere risultati da Security Hub.
4. Quali sono i passaggi di base per completare l'integrazione con Security Hub?

   a. Invia le informazioni sul manifesto del tuo partner.

b. Ricevi ARNs il prodotto da utilizzare con Security Hub, se intendi inviare i risultati a Security Hub.

c. Mappa i risultati su ASFF. Per informazioni, consulta the section called “Linee guida per la mappatura ASFF”.

d. Definisci la tua architettura per l'invio e la ricezione dei risultati da Security Hub. Segui i principi descritti in. the section called “Principi per la creazione e l'aggiornamento dei risultati”

e. Crea un framework di implementazione per i clienti. Ad esempio, AWS CloudFormation gli script possono servire a questo scopo.

f. Documenta la tua configurazione e fornisci istruzioni di configurazione ai clienti.

g. Definisci eventuali approfondimenti personalizzati (regole di correlazione) che i clienti possono utilizzare con il tuo prodotto.

h. Dimostra la tua integrazione al team di Security Hub.

i. Invia le informazioni di marketing per l'approvazione (lingua del sito web, comunicato stampa, diapositiva sull'architettura, video, foglio illustrativo).

5. Qual è la procedura per l'invio del manifesto del partner? E AWS i servizi per inviare i risultati al Security Hub?

   Per inviare le informazioni del manifesto al team di Security Hub, usa `<securityhub-partners@amazon.com>`.

   Il prodotto ti verrà rilasciato ARNs entro sette giorni di calendario.

6. Quali tipi di risultati devo inviare a Security Hub?

   I prezzi di Security Hub si basano in parte sul numero di risultati acquisiti. Per questo motivo, dovresti evitare di inviare risultati che non forniscono valore ai clienti.

   Ad esempio, alcuni fornitori di servizi di gestione delle vulnerabilità inviano i risultati solo con un punteggio CVSS (Common Vulnerability Scoring System) pari o superiore a 3 su un massimo di 10.

7. Quali sono i diversi approcci per inviare i risultati a Security Hub?

   Questi sono gli approcci principali:

   - I risultati vengono inviati dal loro AWS account designato utilizzando l'`BatchImportFindings`operazione.

- I risultati vengono inviati dall'account del cliente utilizzando l'`BatchImportFindings`operazione. È possibile utilizzare approcci basati sull'assunzione di ruoli, ma questi approcci non sono obbligatori.

Per linee guida generali sull'utilizzo `BatchImportFindings`, vedere. the section called “Linee guida per l'utilizzo dell'API BatchImportFindings”

8. Come posso raccogliere le mie scoperte e inviarle a un endpoint regionale del Security Hub?

   I partner hanno utilizzato approcci diversi a tal fine, in quanto dipende in larga misura dall'architettura della soluzione.

   Ad esempio, alcuni partner creano un'app Python che può essere distribuita come script. AWS CloudFormation Lo script raccoglie i risultati del partner dall'ambiente del cliente, li trasforma in ASFF e li invia all'endpoint regionale del Security Hub.

   Altri partner creano una procedura guidata completa che offre al cliente un'esperienza con un solo clic per inviare i risultati a Security Hub.

9. Come faccio a sapere quando iniziare a inviare i risultati a Security Hub?

   Security Hub supporta l'autorizzazione parziale in batch per il funzionamento dell'`BatchImportFindings`API, in modo da poter inviare tutti i risultati a Security Hub per tutti i clienti.

   Se alcuni dei tuoi clienti non si sono ancora abbonati a Security Hub, Security Hub non acquisisce tali risultati. Ingerisce solo i risultati autorizzati presenti nel batch.

10. Quali passaggi devo completare per inviare i risultati all'istanza di Security Hub di un cliente?

    a. Assicurati che siano in atto le politiche IAM corrette.

    b. Abilita un abbonamento al prodotto (politiche delle risorse) per gli account. Utilizza il funzionamento dell'`EnableImportFindingsForProduct`API o la pagina delle integrazioni. Il cliente può farlo oppure puoi utilizzare ruoli tra account diversi per agire per conto del cliente.

    c. Assicurati che il `ProductArn` risultato sia l'ARN pubblico del tuo prodotto.

    d. Assicurati che il `AwsAccountId` risultato sia l'ID dell'account del cliente.

    e. Assicurati che i risultati non contengano dati errati secondo il AWS Security Finding Format (ASFF). Ad esempio, i campi obbligatori sono compilati e non ci sono valori non validi.

    f. Invia i risultati in batch all'endpoint regionale corretto.

11. Quali autorizzazioni IAM devono essere disponibili per poter inviare i risultati?

Le policy IAM devono essere configurate per l'utente o il ruolo IAM che chiama `BatchImportFindings`o altre chiamate API.

Il test più semplice consiste nell'eseguire questa operazione da un account amministratore. Puoi limitarli a `action: 'securityhub:BatchImportFindings' eresource: <productArn and/or productSubscriptionArn>`.

Le risorse nello stesso account possono essere configurate con le policy IAM senza richiedere policy relative alle risorse.

Per escludere problemi di policy IAM da parte del chiamante di `BatchImportFindings`, imposta la policy IAM per il chiamante come segue:

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

Assicurati di controllare che non vi siano `Deny` politiche per il chiamante. Dopo averlo fatto funzionare, puoi limitare la politica a quanto segue:

```
{
    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. Cos'è l'abbonamento a un prodotto?

Per ricevere informazioni su uno specifico prodotto del partner, il cliente (o il partner con ruoli trasversali che lavorano per conto del cliente) deve sottoscrivere un abbonamento al prodotto. Per eseguire questa operazione dalla console, utilizzano la pagina Integrazioni. Per eseguire questa operazione dall'API, utilizzano l'operazione `EnableImportFindingsForProduct`API.

L'abbonamento al prodotto crea una politica delle risorse che autorizza la ricezione o l'invio dei risultati del partner da parte del cliente. Per informazioni dettagliate, consultare Casi d'uso e autorizzazioni.

Security Hub offre i seguenti tipi di politiche sulle risorse per i partner:

- `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
- `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

Durante il processo di onboarding dei partner, puoi richiedere uno o entrambi i tipi di politiche.

Con`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, puoi inviare i risultati a Security Hub solo dall'account indicato nell'ARN del prodotto.

Con`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, puoi inviare i risultati solo dall'account cliente che ti ha sottoscritto.

13. Supponiamo che un cliente abbia creato un account amministratore e abbia aggiunto alcuni account membro. Il cliente deve sottoscrivere ogni account membro per me? Oppure il cliente si iscrive solo dall'account amministratore e posso quindi inviare i risultati relativi alle risorse di tutti gli account dei membri?

    Questa domanda chiede se le autorizzazioni vengono create per tutti gli account membro in base alla registrazione dell'account amministratore.

    Il cliente deve sottoscrivere un abbonamento al prodotto per ciascun account. Possono farlo a livello di codice tramite l'API.

14. Qual è l'ARN del mio prodotto?

    L'ARN del prodotto è l'identificatore univoco che Security Hub genera per te e che usi per inviare i risultati. Riceverai un ARN per ogni prodotto che integri con Security Hub. L'ARN corretto del prodotto deve far parte di ogni risultato inviato a Security Hub. I risultati senza l'ARN del prodotto vengono eliminati. L'ARN del prodotto utilizza il seguente formato:

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

    Ecco un esempio:

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

Ti viene assegnato un ARN del prodotto per ogni regione in cui viene distribuito Security Hub. L'ID dell'account, l'azienda e i nomi dei prodotti sono determinati dai manifesti inviati dal partner. Non modifichi mai nessuna delle informazioni associate all'ARN del prodotto, ad eccezione del codice regionale. Il codice regionale deve corrispondere alla regione per cui invii i risultati.

Un errore comune consiste nel modificare l'ID dell'account in modo che corrisponda all'account da cui lavori attualmente. L'ID dell'account non cambia. L'ID dell'account «home» viene inviato come parte dell'invio del manifesto. Questo ID account è bloccato nell'ARN del prodotto.

Quando Security Hub viene lanciato in nuove regioni, utilizza automaticamente i codici regionali standard per generare il prodotto ARNs per tali regioni.

A ogni account viene inoltre assegnato automaticamente l'ARN di un prodotto privato. Puoi utilizzare questo ARN per testare i risultati di importazione all'interno del tuo account di sviluppo prima di ricevere l'ARN ufficiale del prodotto pubblico.

15. Quale formato deve essere utilizzato per inviare i risultati a Security Hub?

I risultati devono essere forniti nel AWS Security Finding Format (ASFF). Per i dettagli, vedere AWS Security Finding Format (ASFF) nella Guida per l'AWS Security Hub utente.

L'aspettativa è che tutte le informazioni contenute nei risultati nativi si riflettano pienamente nell'ASFF. I campi personalizzati come `ProductFields` e `Resource.Details.Other` consentono di mappare i dati che non rientrano perfettamente nei campi predefiniti.

16. Qual è l'endpoint regionale corretto da utilizzare?

È necessario inviare i risultati all'endpoint regionale Security Hub associato all'account cliente.

17. Dove posso trovare l'elenco degli endpoint regionali?

Vedi l'elenco degli endpoint del Security Hub.

18. Posso inviare risultati interregionali?

Security Hub non supporta ancora l'invio interregionale dei risultati per i AWS servizi nativi, come Amazon GuardDuty, Amazon Macie e Amazon Inspector. Se il cliente lo consente, Security Hub non ti impedisce di inviare risultati da diverse regioni.

In questo senso, è possibile chiamare un endpoint regionale da qualsiasi luogo e le informazioni sulle risorse dell'ASFF non devono necessariamente corrispondere alla regione dell'endpoint. Tuttavia, `ProductArn` deve corrispondere alla regione dell'endpoint.

19. Quali sono le regole e le linee guida per l'invio di batch di risultati?

    È possibile raggruppare fino a 100 risultati o 240 KB in una singola chiamata di `BatchImportFindings`. Metti in coda e raggruppa il maggior numero possibile di risultati fino a questo limite.

    Puoi raggruppare una serie di risultati provenienti da diversi account. Tuttavia, se uno degli account del batch non è sottoscritto a Security Hub, l'intero batch fallisce. Si tratta di una limitazione del modello di autorizzazione di base di API Gateway.

    Per informazioni, consulta the section called “Linee guida per l'utilizzo dell'API `BatchImportFindings`”.

20. Posso inviare aggiornamenti ai risultati che ho creato?

    Sì, se invii un risultato con lo stesso ARN del prodotto e lo stesso ID del risultato, i dati precedenti relativi a tale risultato vengono sovrascritti. Tieni presente che tutti i dati vengono sovrascritti, quindi devi inviare un risultato completo.

    I clienti vengono misurati e fatturati sia per le nuove scoperte che per gli aggiornamenti dei risultati.

21. Posso inviare aggiornamenti ai risultati creati da qualcun altro?

    Sì, se il cliente ti concede l'accesso all'operazione `BatchUpdateFindings`API, puoi aggiornare determinati campi utilizzando tale operazione. Questa operazione è progettata per essere utilizzata dai clienti SIEMs, dai sistemi di ticketing e dalle piattaforme di Security Orchestration, Automation and Response (SOAR).

22. Come vengono invecchiate le scoperte?

    Security Hub archivia i risultati 90 giorni dopo la data dell'ultimo aggiornamento. Trascorso questo periodo, i risultati obsoleti vengono eliminati dal cluster Security Hub. OpenSearch

    Se aggiorni un risultato con lo stesso ID di ricerca ed è stato obsoleto, viene creato un nuovo risultato in Security Hub.

    I clienti possono utilizzare CloudWatch Events per spostare i risultati fuori dal Security Hub. In questo modo è possibile inviare tutti i risultati a obiettivi scelti dal cliente.

    In generale, Security Hub consiglia di creare nuovi risultati ogni 90 giorni e di non aggiornarli per sempre.

23. Quali limiti mette in atto Security Hub?

Security Hub limita le chiamate `GetFindings` API, poiché l'approccio consigliato per accedere ai risultati consiste nell'utilizzare CloudWatch gli eventi.

Security Hub non implementa nessun'altra limitazione sui servizi interni, sui partner o sui clienti oltre a quella imposta dalle chiamate API Gateway e Lambda.

24. Qual è la tempestività, la latenza SLAs o le aspettative per i risultati inviati a Security Hub dai servizi di origine?

    L'obiettivo è quello di essere il più possibile vicini al tempo reale sia per i risultati iniziali che per gli aggiornamenti dei risultati. È necessario inviare i risultati a Security Hub entro cinque minuti dalla loro creazione.

25. Come posso ricevere i risultati dal Security Hub?

    Per ricevere i risultati, usa uno dei seguenti metodi.

    - Tutti i risultati vengono inviati automaticamente agli CloudWatch Eventi. Un cliente può creare regole CloudWatch Events specifiche per inviare i risultati a obiettivi specifici, come un SIEM o un bucket S3. Questa funzionalità ha sostituito il funzionamento delle API precedenti`GetFindings`.
    - Usa CloudWatch Events per azioni personalizzate. Security Hub consente ai clienti di selezionare risultati o gruppi di risultati specifici dall'interno della console e agire di conseguenza. Ad esempio, possono inviare i risultati a un SIEM, a un sistema di ticketing, a una piattaforma di chat o a un flusso di lavoro di correzione. Questo farebbe parte di un flusso di lavoro di valutazione degli avvisi eseguito da un cliente all'interno di Security Hub. Queste sono chiamate azioni personalizzate.

      Quando un utente seleziona un'azione personalizzata, viene creato un CloudWatch evento per quei risultati specifici. È possibile sfruttare questa funzionalità e creare regole e obiettivi relativi agli CloudWatch eventi che un cliente possa utilizzare come parte di un'azione personalizzata. Tieni presente che questa funzionalità non viene utilizzata per inviare automaticamente tutti i risultati di un particolare tipo o classe a CloudWatch Events. Spetta all'utente intervenire su risultati specifici.

      Puoi utilizzare le operazioni dell'API Custom Action`CreateActionTarget`, ad esempio per creare automaticamente azioni disponibili per il tuo prodotto (come l'utilizzo AWS CloudFormation di modelli). Puoi anche utilizzare le operazioni dell'API CloudWatch Events rule per creare le regole CloudWatch Events corrispondenti associate all'azione personalizzata. Utilizzando AWS CloudFormation i modelli, puoi anche creare regole CloudWatch Events per

importare automaticamente da Security Hub tutti i risultati o tutti i risultati con determinate caratteristiche.

26. Quali sono i requisiti per un provider di servizi di sicurezza gestiti (MSSP) per diventare partner del Security Hub?

    È necessario dimostrare come viene utilizzato Security Hub nell'ambito della fornitura di servizi ai clienti.

    È necessario disporre di una documentazione per l'utente che spieghi l'utilizzo di Security Hub.

    Se l'MSSP è un provider di ricerca, deve dimostrare di aver inviato i risultati a Security Hub.

    Se l'MSSP riceve solo risultati da Security Hub, deve disporre almeno di un AWS CloudFormation modello per configurare le regole CloudWatch Events appropriate.

27. Quali sono i requisiti per un partner di consulenza APN non MSSP per diventare un partner Security Hub?

    Se sei un partner di consulenza APN, puoi diventare un partner Security Hub. Dovresti presentare due case study privati su come hai aiutato un cliente specifico a fare quanto segue.

    - Configura Security Hub con le autorizzazioni IAM di cui il cliente ha bisogno.
    - Aiuta a connettere soluzioni ISV (Independent Software Vendor) già integrate a Security Hub utilizzando le istruzioni di configurazione nella pagina partner nella console.
    - Aiuta i clienti con integrazioni di prodotti personalizzate.
    - Crea approfondimenti personalizzati pertinenti alle esigenze e ai set di dati dei clienti.
    - Crea azioni personalizzate.
    - Crea dei playbook di riparazione.
    - Crea Quickstart che si allineano agli standard di conformità del Security Hub. Questi devono essere convalidati dal team di Security Hub.

    I case study non devono necessariamente essere condivisi pubblicamente.

28. Quali sono i requisiti relativi alla modalità di implementazione della mia integrazione con Security Hub con i miei clienti?

    Le architetture di integrazione tra Security Hub e i prodotti dei partner variano da partner a partner in termini di modalità di gestione della soluzione del partner. È necessario assicurarsi che il processo di configurazione per l'integrazione non richieda più di 15 minuti.

Se state implementando un software di integrazione nell' AWS ambiente del cliente, dovreste sfruttare i AWS CloudFormation modelli per semplificare l'integrazione. Alcuni partner hanno creato un'integrazione con un solo clic, che è altamente consigliata.

29. Quali sono i miei requisiti di documentazione?

    È necessario fornire un collegamento alla documentazione che descrive il processo di integrazione e configurazione tra il prodotto e Security Hub, incluso l'uso dei AWS CloudFormation modelli.

    Tale documentazione deve includere anche informazioni sull'utilizzo di ASFF. In particolare, questo dovrebbe elencare i tipi di risultati ASFF che state utilizzando per i diversi risultati. Se disponi di definizioni di insight predefinite, ti consigliamo di includerle anche qui.

    Valuta la possibilità di includere altre potenziali informazioni:

    - Il tuo caso d'uso per l'integrazione con Security Hub
    - Volume medio dei risultati inviati
    - La tua architettura di integrazione
    - Le regioni supportate e non supportate
    - Latenza tra il momento in cui i risultati vengono creati e il momento in cui vengono inviati a Security Hub
    - Se aggiorni i risultati

30. Cosa sono gli approfondimenti personalizzati?

    Sei incoraggiato a definire approfondimenti personalizzati per i tuoi risultati. Gli approfondimenti sono regole di correlazione leggere che aiutano un cliente a stabilire le priorità dei risultati e delle risorse che richiedono più attenzione e azione.

    Security Hub ha un funzionamento `CreateInsight` API. Puoi creare approfondimenti personalizzati all'interno di un account cliente come parte del tuo AWS CloudFormation modello. Queste informazioni vengono visualizzate sulla console del cliente.

31. Posso inviare i widget del pannello di controllo?

    No, non in questo momento. Puoi solo creare approfondimenti gestiti.

32. Qual è il tuo modello di prezzo?

    Consulta le informazioni sui prezzi di Security Hub.

33. Come posso inviare i risultati all'account demo di Security Hub come parte del processo di approvazione finale della mia integrazione?

    Invia i risultati all'account demo di Security Hub utilizzando l'ARN del prodotto fornito, utilizzando `us-west-2` come regione. I risultati dovrebbero includere il numero di conto demo nel `AwsAccountId` campo dell'ASFF. Per ottenere il numero di conto demo, contatta il team di Security Hub.

    Non inviateci dati sensibili o informazioni di identificazione personale. Questi dati vengono utilizzati per dimostrazioni pubbliche. Quando ci invii questi dati, ci autorizzi a utilizzarli nelle demo.

34. Quali messaggi di errore o di successo fornisce **`BatchImportFindings`**?

    Security Hub fornisce una risposta per l'autorizzazione e una risposta per `BatchImportFindings`. Sono in fase di sviluppo messaggi di successo, fallimento ed errore più nitidi.

35. Di quale gestione degli errori è responsabile il servizio di origine?

    I servizi di origine sono responsabili di tutta la gestione degli errori. Devono gestire i messaggi di errore, i nuovi tentativi, le limitazioni e gli allarmi. Devono inoltre gestire i feedback o i messaggi di errore inviati tramite il meccanismo di feedback del Security Hub.

36. Quali sono le soluzioni ai problemi più comuni?

    An `AuthorizerConfigurationException` è causato da un or malformato`AwsAccountId`. `ProductArn`

    Durante la risoluzione dei problemi, tenete presente quanto segue:

    - `AwsAccountId`deve contenere esattamente 12 cifre.
    - `ProductArn`deve essere nel seguente formato: arn:aws:securityhub: ::product//*`<us-west-2 or us-east-1><accountId><company-id><product-id>`*

      L'ID dell'account non cambia rispetto a quello che il team di Security Hub ha incluso nel prodotto ARNs che ti ha fornito.

    `AccessDeniedException`è causato quando un risultato viene inviato o ricevuto dall'account sbagliato o quando l'account non dispone di un`ProductSubscription`. Il messaggio di errore conterrà un ARN con un tipo di `product` risorsa pari o. `product-subscription` Questo errore si verifica solo durante le chiamate tra account. Se chiami `BatchImportFindings`con

il tuo account per lo stesso account in `AwsAccountId` and`ProductArn`, l'operazione utilizza le politiche IAM e non ha nulla a che fare con`ProductSubscriptions`.

Assicurati che l'account cliente e l'account del prodotto che utilizzi siano gli account effettivamente registrati. Alcuni partner hanno utilizzato per il prodotto un numero di account del prodotto ARN, ma cercano di utilizzare un account completamente diverso per chiamare. `BatchImportFindings` In altri casi, hanno creato account `ProductSubscriptions` per altri clienti o addirittura per il proprio account di prodotto. Non l'hanno creato `ProductSubscriptions` per l'account cliente in cui hanno cercato di importare i risultati.

37 Dove posso inviare domande, commenti e bug?

`<securityhub-partners@amazon.com>`

38 A quale regione devo inviare i risultati per gli articoli relativi ai AWS servizi globali? Ad esempio, dove posso inviare i risultati relativi a IAM?

Invia i risultati alla stessa regione in cui è stato rilevato il risultato. Per un servizio come IAM, la tua soluzione probabilmente troverà lo stesso problema IAM in più regioni. In questo caso, il risultato viene inviato a tutte le regioni in cui è stato rilevato il problema.

Se il cliente esegue Security Hub in tre regioni e lo stesso problema IAM viene rilevato in tutte e tre le regioni, invia il risultato a tutte e tre le regioni.

Quando un problema viene risolto, invia l'aggiornamento del risultato a tutte le regioni a cui hai inviato il risultato originale.

Cronologia dei documenti per la Partner Integration Guide

La tabella seguente descrive gli aggiornamenti della documentazione per questa guida.

Modifica	Descrizione	Data
Requisiti aggiornati per il logo della console	Sono state aggiornate le linee guida del manifesto e del logo del partner per indicare che i partner devono fornire sia una versione del logo in modalità chiara che una in modalità scura da visualizzare sulla console Security Hub. I loghi devono essere in formato SVG.	10 maggio 2021
Aggiornati i prerequisiti per i nuovi partner di integrazione	Security Hub ora consente anche ai partner che hanno aderito al percorso AWS ISV Partner e che utilizzano un prodotto di integrazione che ha completato un AWS Foundatio nal Technical Review (FTR). In precedenza, tutti i partner di integrazione dovevano essere partner di livello AWS selezionato.	29 aprile 2021
Nuovo `FindingProviderFields` oggetto in ASFF	Sono state aggiornat e le informazioni sulla mappatura dei risultati su ASFF. Per `Confidence` ,, `Criticality` `RelatedFindings` , e `SeverityTypes`, i partner associano i propri	18 marzo 2021

	valori ai campi in. `FindingProviderFields`	
Nuovi principi per la creazione e l'aggiornamento dei risultati	È stata aggiunta una nuova serie di linee guida per la creazione di nuovi risultati e l'aggiornamento dei risultati esistenti in Security Hub.	4 dicembre 2020
Versione iniziale di questa guida	Questa guida all'integrazione AWS dei partner fornisce ai partner informazioni su come stabilire un'integrazione con AWS Security Hub.	23 giugno 2020

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.