Guida

AWS Security Hub

AWS Security Hub: Guida

Table of Contents

Panoramica dell'integrazione di terze parti conAWS Security Hub

Questa guida è destinata aAWSPartner Network (APN) Partner che desiderano creare un'integrazione conAWS Security Hub.

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

- Invia i risultati a Security Hub
- Utilizzo dei risultati di Security Hub
- Entrambi inviano risultati e consumano i risultati da Security Hub
- Utilizzare Security Hub come centro di un'offerta MSSP (Managed Security Service Provider)
- Consultazione conAWSclienti su come distribuire e utilizzare Security Hub

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

Argomenti

Perché integrarsi conAWS Security Hub?

AWS Security Hubfornisce una visione completa degli avvisi di sicurezza ad alta priorità e dello stato di sicurezza negli account Security Hub. Security Hub consente a partner come te di inviare risultati di sicurezza a Security Hub per fornire ai clienti informazioni dettagliate sui risultati di sicurezza generati.

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

- Soddisfa i clienti che hanno richiesto l'integrazione di Security Hub
- Fornisce ai tuoi clienti una visione unica della loroAWSrisultati relativi alla sicurezza

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

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

Preparazione per inviare i risultati aAWS Security Hub

In qualità di partner APN, non è possibile inviare informazioni a Security Hub per i clienti fino a quando il team di Security Hub non ti consente come provider di ricerca. Per essere abilitato come provider di ricerca, devi completare le fasi seguenti di onboarding. Ciò garantisce un'esperienza positiva Security Hub per te e i tuoi clienti.

Quando completi i passaggi di onboarding, assicurati di seguire le linee guida inthe section called “Principi per la creazione e l'aggiornamento dei risultati”,the section called “Linee guida per il mapping ASFF”, ethe section called “Linee guida per l'utilizzo del`BatchImportFindings`API”.

1. Mappare i risultati di sicurezza suAWSSecurity Finding Format (ASFF).
2. Crea la tua architettura di integrazione per inviare i risultati all'endpoint Regional Security Hub corretto. Per fare ciò, definisci se invierai i risultati dal tuoAWSaccount o dall'interno degli account del cliente.
3. Chiedi ai tuoi clienti di sottoscrivere il prodotto al loro account. A tale scopo, possono utilizzare la console o il`EnableImportFindingsForProduct`Operazione API. Consulta .Gestione delle integrazioni di prodottinellaAWS Security HubGuida per l’utente di.

   Puoi anche sottoscrivere il prodotto per loro. A tale scopo, utilizzi un ruolo tra account per accedere a`EnableImportFindingsForProduct`Operazione API per conto del cliente.

   Questo passaggio stabilisce i criteri delle risorse necessari per accettare i risultati di quel prodotto per tale account.

I seguenti post del blog parlano di alcune delle integrazioni di partner esistenti con Security Hub.

- Annuncio dell'integrazione con Cloud Custodian conAWS Security Hub

- UtilizzaAWS Fargatee Prowler per inviare i risultati della configurazione di sicurezza suAWSservizi a Security Hub
- Come importareAWS Configvalutazioni delle regole come risultati in Security Hub

Preparazione a ricevere i risultati daAWS Security Hub

Per ricevere i risultati daAWS Security Hub, utilizza una delle opzioni seguenti:

- Chiedi ai tuoi clienti di inviare automaticamente tutti i risultati aCloudWatchEventi. Un cliente può creare specificiCloudWatchregole eventi per inviare risultati a obiettivi specifici, come un SIEM o un bucket S3.
- Chiedi ai tuoi clienti di selezionare risultati specifici o gruppi di risultati dall'interno della console di Security Hub e quindi intervenire su di essi.

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

Queste operazioni sono chiamate operazioni personalizzate. Quando un utente intraprende un'azione personalizzata, aCloudWatchl'evento è creato per quei risultati specifici. Come partner, puoi sfruttare questa funzionalità e creareCloudWatchregole di evento o destinazioni da utilizzare per un cliente come parte di un'azione personalizzata. Notare che questa funzionalità non invia automaticamente tutti i risultati di un particolare tipo o classe aCloudWatchEventi. Questa funzione consente a un utente di intervenire su risultati specifici.

I seguenti post del blog descrivono le soluzioni che utilizzano l'integrazione con Security Hub eCloudWatchEventi per azioni personalizzate.

- Come integrareAWS Security HubOperazioni personalizzate conPagerDuty
- Come abilitare azioni personalizzate inAWS Security Hub
- Come importareAWS Configvalutazioni delle regole come risultati in Security Hub

Risorse per ulteriori informazioni suAWS Security Hub

I seguenti materiali possono aiutarti a capire meglio ilAWS Security Hubsoluzione e comeAWSi clienti possono utilizzare il servizio.

- Introduzione aAWS Security Hubvideo
- Guida dell'utente di Security Hub
- Riferimento API Security Hub
- Webinar di onboarding

Ti invitiamo inoltre a abilitare Security Hub in uno dei tuoiAWSaccount e ottieni esperienza pratica con il servizio.

Prerequisiti dei partner

Prima di iniziare un'integrazione conAWS Security Hub, è necessario soddisfare uno dei seguenti criteri:

- Sei unAWSSeleziona Tier Partner o superiore.
- Ti sei unito alAWSISV dei partnere il prodotto utilizzato per l'integrazione di Security Hub ha completato unAWSRevisione tecnica di base (FTR). Al prodotto viene quindi concesso un «Recensito daAWS«badge.

È inoltre necessario disporre di un accordo reciproco di non divulgazione conAWS.

Casi d'uso dell'integrazione e autorizzazioni richieste

AWS Security HubpermetteAWSclienti che ricevono risultati da APN Partners. I prodotti del partner potrebbero funzionare all'interno o all'esterno del clienteAWSconto. 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 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 si iscrive prima al prodotto partner in Security Hub. La fase di abbonamento è necessaria per tutti i casi d'uso descritti di seguito. Per informazioni dettagliate su come i clienti gestiscono le integrazioni dei prodotti, consultaGestione delle integrazioni di prodottinellaAWS Security HubGuida per l'utente di.

Dopo che un cliente si è abbonato a un prodotto partner, Security Hub crea automaticamente una policy sulle risorse gestite. La policy concede al prodotto partner l'autorizzazione all'usoBatchImportFindingsOperazione API per inviare i risultati a Security Hub per l'account del cliente.

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

Partner ospitato: risultati inviati dall'account partner

Questo caso d'uso copre i partner che ospitano un prodotto da soliAWSconto. Per inviare i risultati di sicurezza per unAWScliente, il partner chiama ilBatchImportFindingsOperazione API dall'account del prodotto partner.

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

Nell'account partner, il principale IAM che chiama ilBatchImportFindingsL'operazione API deve avere una policy IAM che consente all'operatore di chiamareBatchImportFindings.

Consentire a un prodotto partner di inviare 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 politica delle risorse gestite corrette con la conferma del cliente.

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

Di seguito è riportato un esempio di policy IAM che concede al principale nell'account partner le autorizzazioni necessarie per 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"
        }
    ]
}
```

Partner ospitato: risultati inviati dall'account cliente

Questo caso d'uso copre i partner che ospitano un prodotto da soliAWSaccount, ma utilizza un ruolo cross-account per accedere all'account del cliente. Chiamano`BatchImportFindings`Operazione API dall'account del cliente.

Per questo caso d'uso, per chiamare il`BatchImportFindings`Operazione API, l'account partner assume un ruolo IAM gestito dal cliente nell'account del cliente.

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

La best practice per i ruoli tra account tra partner e account cliente consiste nell'utilizzare un identificatore esterno fornito dal partner. Questo identificatore esterno fa parte della definizione del criterio tra account nel conto del cliente. Il partner deve fornire l'identificatore quando assume il ruolo. Un identificatore esterno fornisce un ulteriore livello di sicurezza durante la concessioneAWSaccesso

all'account a un partner. L'identificativo univoco garantisce che il partner utilizzi l'account cliente corretto.

Consentire a un prodotto partner di inviare risultati al cliente in Security Hub con un ruolo cross-account avviene in quattro passaggi:

1. Il cliente o il partner che utilizza ruoli cross-account che lavorano per conto del cliente, avvia l'abbonamento a un prodotto in Security Hub.
2. Security Hub genera la politica delle risorse gestite corrette con la conferma del cliente.
3. Il cliente configura il ruolo tra account manualmente o utilizzandoAWS CloudFormation. Per informazioni sui ruoli tra account, consultaFornire l'accesso aAWSaccount di proprietà di terze partinellaIAM User Guide.
4. Il prodotto memorizza in modo sicuro il ruolo del cliente e l'ID esterno.

Successivamente, il prodotto invia i risultati a Security Hub:

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

Di seguito viene fornito un esempio di policy IAM che concede le necessarie autorizzazioni Security Hub per il ruolo tra 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 politica identifica l'abbonamento specifico del prodotto. Ciò garantisce che il partner possa inviare solo risultati per il prodotto partner a cui è abbonato il cliente.

Cliente ospitato: risultati inviati dall'account cliente

Questo caso d'uso copre i partner che hanno un prodotto distribuito nel clienteAWSconto. La`BatchImportFindings`L'API viene richiamata dalla soluzione che viene eseguita nell'account del cliente.

Per questo caso d'uso, al prodotto partner devono essere concesse ulteriori autorizzazioni per chiamare il`BatchImportFindings`API. Il modo in cui questa autorizzazione viene concessa differisce in base alla soluzione partner e al modo in cui è configurata nell'account del cliente.

Un esempio di questo approccio è un prodotto partner che viene eseguito su un'istanza EC2 nell'account del cliente. Questa istanza EC2 deve avere un ruolo di istanza EC2 collegato che concede a tale istanza la possibilità di chiamare il`BatchImportFindings`Operazione API. Ciò consente all'istanza EC2 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 i risultati nel proprio conto per un prodotto di loro proprietà.

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

1. Il cliente distribuisce il prodotto partner nel proprioAWSaccount manualmente utilizzandoAWS CloudFormationo un altro strumento di distribuzione.
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 politica ai componenti necessari del prodotto partner, come un'istanza EC2, un contenitore o una funzione Lambda.

Ora il prodotto può inviare i risultati a Security Hub:

1. Il prodotto partner utilizza ilAWSSDK oAWS CLIper chiamare`BatchImportFindings`Operazione API in Security Hub. Effettua la chiamata dal componente nell'account del cliente in cui è allegata la policy.
2. Durante la chiamata API, vengono generate le credenziali temporanee necessarie per consentire il`BatchImportFindings`richiama per avere successo.

Di seguito è riportato un esempio di policy IAM che concede le autorizzazioni di Security Hub necessarie 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

Come 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 aAWS Security Hub.

1. Inizia un coinvolgimento con il team APN Partner o il team Security Hub ed esprimi interesse a diventare partner di Security Hub. Identifica gli indirizzi e-mail da aggiungere ai canali di comunicazione di Security Hub.
2. AWSfornisce il materiale di onboarding del partner Security Hub.
3. Sei invitato al canale Slack partner di Security Hub, dove puoi porre domande relative alla tua integrazione.
4. Fornisci ai contatti APN Partner una bozza di manifesto di integrazione dei prodotti per la revisione.

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

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

   Questa versione iniziale del manifesto di integrazione del prodotto non deve avere 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 necessarie, consultaManifest di integrazione dei prodotti.
5. Il team Security Hub ti fornisce un prodotto ARN per il tuo prodotto. Utilizzi l'ARN per inviare i risultati a Security Hub.
6. Create la vostra integrazione per inviare risultati o ricevere risultati da Security Hub.

   Mappatura dei risultati su ASFF

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

L'ASFF fornisce una descrizione coerente dei risultati che possono essere condivisi traAWSservizi 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 del protocollo wire richiesto da utilizzare per inviare i risultati aAWS Security Hub. I risultati sono rappresentati come documenti JSON conformi allo schema ASFF JSON e RFC-7493 The I-JSON Message Format. Per informazioni dettagliate sullo schema ASFF, vedereAWSSecurity Finding Format (ASFF)nellaAWS Security HubGuida per l'utente di.

Consulta the section called "Linee guida per il mapping ASFF".

Creazione e collaudo dell'integrazione

Puoi completare tutti i test per la tua integrazione utilizzando unAWSaccount che possiedi. In questo modo, ti dà piena visibilità su come appaiono i risultati in Security Hub. Inoltre, ti aiuta a comprendere l'esperienza del cliente con i tuoi risultati di sicurezza.

Utilizzi il file`BatchImportFindings`Operazione API per inviare i risultati nuovi e aggiornati a Security Hub.

Durante tutta la creazione di un'integrazione di Security Hub,AWSti incoraggia a tenere informati i tuoi contatti di APN Partner sui progressi della tua integrazione. Puoi anche chiedere aiuto ai tuoi contatti APN Partner per le domande sull'integrazione.

Consulta the section called "Linee guida per l'utilizzo del`BatchImportFindings`API".

7. Dimostra l'integrazione con il team di prodotti 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 andare avanti per elencarti come provider.

8. FornisciAWSCon un manifesto finale per la revisione.
9. Il team di Security Hub crea l'integrazione del provider nella console di Security Hub. I clienti possono quindi scoprire e abilitare l'integrazione.
10. (Facoltativo) Si impegna in ulteriori sforzi di marketing per promuovere l'integrazione di Security Hub. Consulta Go-to-marketattività.

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

- Un video dimostrativo (al massimo 3 minuti) dell'integrazione di lavoro. Il video viene utilizzato per scopi di marketing e viene pubblicato sulAWS YouTubecanale.
- Diagramma di architettura con una sola diapositiva da aggiungere Security Hub diapositive della prima chiamata

Go-to-marketattività

I partner possono inoltre impegnarsi in attività di marketing facoltative per aiutarli a spiegarne e promuoverneAWS Security Hubintegrazione.

Se desideri creare contenuti di marketing personalizzati relativi a Security Hub, prima di rilasciare il contenuto, invia una bozza al tuo APN Partner Manager per la revisione e l'approvazione. Ciò garantisce che tutti siano allineati alla messaggistica.

AWSI partner Partner Network (APN) possono utilizzare APN Partner Marketing Central e il programma Market Development Funds (MDF) per creare campagne e ottenere supporto ai finanziamenti. Per informazioni dettagliate su questi programmi, contatta il tuo partner manager.

Inserimento nella pagina dei partner di Security Hub

Dopo essere stato approvato come partner Security Hub, la soluzione può essere visualizzata sulAWS Security Hubpagina dei partner.

Per essere elencati in questa pagina, fornisci i seguenti dettagli ai tuoi contatti di APN Partner. Potrebbe trattarsi del vostro Partner Development Manager (PDM), partner Solution Architect (PSA) o un'e-mail a`<securityhub-pms@amazon.com>`.

- Una breve descrizione della soluzione, la sua integrazione con Security Hub e il valore che l'integrazione con Security Hub fornisce ai clienti. Questa descrizione è limitata a 700 caratteri inclusi gli spazi.
- L'URL di una pagina che descrive la soluzione. Questo sito dovrebbe essere specifico per il tuoAWSintegrazione e più specificamente l'integrazione di 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 i dettagli sui requisiti per 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 daAWS.

Prima di pubblicare il comunicato stampa, è necessario inviarlo aAWSper la revisione da parte di APN Partner marketing, leadership di Security Hub eAWSServizi di sicurezza esterni (ESS). Il comunicato stampa può includere un preventivo proposto per il VP di ESS.

Per avviare questo processo, collabora con il PDM. Abbiamo un Service Level Agreement (SLA) di 10 giorni lavorativi per rivedere i comunicati stampa.

AWSBlog di Partner Network (APN)

Possiamo anche aiutarti a pubblicare una voce di blog che hai creato sul blog APN. La voce del blog deve concentrarsi sulla storia del cliente e sul caso d'uso. Non può essere posizionato unicamente intorno all'essere un partner di 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 da sapere sul blog APN

Quando crei un post di blog, devi considerare i seguenti elementi.

Cosa succede in un post sul blog?

- I post dei partner dovrebbero essere educativi e fornire competenze approfondite su un argomento rilevanteAWSclienti.
- La lunghezza ideale non è superiore a 1.500 parole. I lettori apprezzano contenuti educativi profondi che insegnano loro cosa è possibileAWS.
- Il contenuto dovrebbe essere originale per il blog APN. Non riutilizzare i contenuti provenienti da fonti come post di blog o whitepaper esistenti.

Quali sono gli altri limiti per la pubblicazione sul blog APN?

- Solo i partner di livello Advanced o Premier possono pubblicare sul blog APN. Esistono eccezioni per i partner Select che dispongono di una designazione del programma APN come la fornitura di servizi.
- Ogni partner è limitato a tre posti all'anno. Con decine di migliaia di partner APN,AWSdeve essere equo nella sua copertura.

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

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

Dopo aver inviato la prima bozza completa del post del blog, ci vogliono da quattro a sei settimane per la modifica.

Perché scrivere per il blog APN?

Un post del blog di APN può fornire i seguenti vantaggi.

- Credibilità— Per APN Partners, avere una storia pubblicata daAWSpuò influenzare i clienti a livello globale.
- Visibilità— Il blog APN è uno dei blog più letti diAWScon 1,79 milioni di pagine visualizzate nel 2019, incluso il traffico influenzato.
- Business— I post di APN Partner 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 più adatti per un post sul blog di APN.

- Il contenuto tecnico è il tipo di storia più popolare. Ciò include i faretti della soluzione e le informazioni pratiche. Oltre il 75% dei lettori guarda a questo contenuto tecnico.
- I clienti apprezzano storie di livello 200 o superiore che dimostrano come funziona qualcosaAWSo come un partner APN ha risolto un problema aziendale per i clienti.
- I post scritti da esperti tecnici o esperti in materia prestano di gran lunga il meglio.

Foglio o foglio di marketing

Un foglio trasparente è un documento di una pagina che delinea il prodotto, la sua architettura di integrazione e i casi d'uso congiunti dei clienti.

Se crei un foglio trasparente per l'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 delinea il prodotto, la relativa architettura di integrazione e i casi d'uso congiunti dei clienti, inviane una copia al team di Security Hub. Lo aggiungeranno alla pagina dei partner di Security Hub.

Webinar su

Se esegui 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 tuo webinar.

Video dimostrativi

Per scopi di marketing, è possibile produrre un video demo dell'integrazione funzionante. Pubblica un video di questo tipo sul tuo account della tua piattaforma video e il team di Security Hub ti collegerà dalla pagina del partner.

Manifest di integrazione dei prodotti

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

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

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

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

Indice

  - Tipi di ricerca
  - Hotline
  - Rilevamento del battito cardiaco
- AWS Security Hubinformazioni sulla console
  - Informazioni sull'azienda
  - Informazioni sul prodotto

Caso d'uso e informazioni di marketing

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

Individuazione del caso d'uso di fornitori e consumatori

Necessario per i fornitori di software indipendenti (ISV).

Per descrivere il tuo caso d'uso relativo all'integrazione conAWS Security Hub, rispondi alle seguenti domande. Se non prevedi di inviare o ricevere i risultati, annotalo in questa sezione e poi completa la sezione successiva.

Le seguenti informazioni devono essere riportate nella documentazione.

- Invierai risultati, riceverai risultati o entrambi?
- Se intendi inviare i risultati, quali tipi di risultati invierai? Invierai tutti i risultati o un sottoinsieme specifico di risultati?
- Se prevedi di ricevere dei risultati, cosa ne farai? Quali tipi di risultati riceverai? Ad esempio, riceverai tutti i risultati, i risultati di un determinato tipo o solo i risultati specifici selezionati da un cliente?
- Avete 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 causato dalla ricerca per i clienti.

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

Per ricevere un feedback tempestivo sul caso d'uso e sui set di dati, contatta il partner APN o il team di 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. Devono 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 unAWS CloudFormation modello?
- Come 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 invii 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 (AWSSecurity Finding Format)

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

Architettura

Obbligatorio se invii i risultati a o ricevi i risultati da Security Hub.

Descrivi come ti integrerai con Security Hub. Queste informazioni devono essere riportate anche nella documentazione.

È necessario fornire diagrammi di architettura. Durante la preparazione dei diagrammi di architettura, considera quanto segue:

- QualiAWS servizi, agenti del sistema operativo e così via utilizzerai?
- Se invierai i risultati a Security Hub, li invierai dall'AWSaccount cliente o dal tuoAWS account?

- Se riceverai dei risultati, come utilizzerai l'integrazione con CloudWatch gli eventi?
- Come convertirai i risultati in ASFF?
- In che modo raggrupperai i risultati, monitorerai lo stato della ricerca ed eviterai i limiti di limitazione?

Configurazione

Obbligatorio se invii i risultati a o ricevi i risultati da Security Hub.

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

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

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

Risultati medi giornalieri per cliente

Obbligatorio se invii i risultati a Security Hub.

Quanti aggiornamenti di ricerca al mese (media e massima) prevedi di inviare a Security Hub nella tua base di clienti? Le stime degli ordini di grandezza sono accettabili.

Latenza

Obbligatorio se invii i risultati a Security Hub.

Quanto velocemente verranno raggruppati e inviati i risultati a Security Hub? In altre parole, qual è la latenza tra quando viene creata la ricerca nel prodotto a quando viene inviata a Security Hub?

Queste informazioni devono essere riportate nella documentazione del prodotto per l'integrazione. È una domanda comune da parte dei clienti.

Descrizione dell'azienda e del prodotto

Obbligatorio per tutte le integrazioni con Security Hub.

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

Risorse del sito web dei partner

Obbligatorio per tutte le integrazioni con Security Hub.

Come minimo, devi 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 descrive l'integrazione tra il tuo prodotto e Security Hub.

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

Puoi anche fornire link ad altre risorse come blog, webinar, video dimostrativi o white paper. Security Hub li collegherà anche alla pagina dedicata ai partner.

Logo per la pagina dei partner

Obbligatorio per tutte le integrazioni di Security Hub.

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

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

Loghi per la console Security Hub

Necessario per tutte le integrazioni.

Fornisci gli URL dei loghi della modalità chiara 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, consultathe section called “Linee guida per il logo della console”.

Tipi di ricerca

Obbligatorio se invii i risultati a Security Hub.

Fornisci una tabella che documenti i tipi di ricerca in formato ASFF che usi e come si allineano ai tipi di ricerca nativi. Per i dettagli sulla ricerca dei tipi in ASFF, consulta la tassonomia dei tipi per ASFF nella Guida per l'AWS Security Hubutente.

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

Hotline

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

Rilevamento del battito cardiaco

Consigliato se invii i risultati a Security Hub.

Puoi inviare a Security Hub una rilevazione «cardiaca» ogni cinque minuti che indichi che l'integrazione con Security Hub è funzionale?

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

AWS Security Hubinformazioni sulla console

Fornire alAWS Security Hub team un testo JSON che contiene 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 sull'azienda forniscono informazioni sulla tua 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 sull'azienda contengono i seguenti campi:

Campo	Campo obbligatorio	Descrizione
`id`	Sì	L'identificatore univoco dell'azienda. L'identif icatore dell'azienda deve essere univoco in tutte le società. Probabilmente è uguale o simile a`name`. Tipo: String Lunghezza minima: 5 caratteri Lunghezza massima: 24 caratteri Caratteri consentiti: lettere minuscole, numeri e trattini Devono iniziare con una lettera minuscola. Devono terminare con una lettera minuscola o un numero.

Campo	Campo obbligatorio	Descrizione
`name`	Sì	Il nome dell'azienda del provider da visualizzare sulla console di Security Hub. Tipo: String Lunghezza massima: 16 caratteri
`description`	Sì	La descrizione dell'azienda del provider da visualizzare sulla console di Security Hub. Tipo: String 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	Campo obbligatorio	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. Devono essere univoci nell'azienda. Non è necessario che siano univoci nelle varie aziende. Probabilmente è uguale o simile a `name`. Tipo: String Lunghezza minima: 5 caratteri Lunghezza massima: 24 caratteri Caratteri consentiti: lettere minuscole, numeri e trattini Devono iniziare con una lettera minuscola. Devono terminare con una lettera minuscola o un numero.
`regionsNotSupported`	Sì	Quale delle seguentiAWS regioni non supportate? In altre parole, in quali regioni Security Hub non dovrebbe mostrarti come opzione nella pagina dei nostri partner nella console di Security Hub?

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

Campo	Campo obbligatorio	Descrizione
`commercialAccountNumber`	Sì	Il numero diAWS conto principale del prodotto per leAWS regioni. Se invii i risultati a Security Hub, l'account fornito si basa sul luogo da cui li invii. • Dal tuoAWS account. In questo caso, fornisci il numero di conto che utilizzi per inviare i risultati. • Dall'AWSaccount del cliente. In questo caso, Security Hub consiglia di fornire il numero di account principale utilizzato 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 di Security Hub. Se ricevi i risultati solo da Security Hub, questo numero di account non è richiesto. Tipo: String

Campo	Campo obbligatorio	Descrizione
`govcloudAccountNumber`	No	Il numero diAWS conto principale del prodotto perAWS GovCloud (US) le regioni (se il prodotto è disponibile inAWS GovCloud (US)). Se invii i risultati a Security Hub, l'account fornito si basa sul luogo da cui li invii. • Dal tuoAWS account. In questo caso, fornisci il numero di conto che utilizzi per inviare i risultati. • Dall'AWSaccount del cliente. In questo caso, Security Hub consiglia di fornire il numero di account principale utilizzato per testare l'integrazione. L'ideale è utilizzare lo stesso account per tutti i prodotti in tutte leAWS GovCloud (US) regioni. Se ciò non è possibile, contatta il team di Security Hub. Se ricevi i risultati solo da Security Hub, questo numero di account non è richiesto. Tipo: String

Campo	Campo obbligatorio	Descrizione
`chinaAccountNumber`	No	Il numero diAWS conto 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 si basa sul luogo da cui li invii. • Dal tuoAWS account. In questo caso, fornisci il numero di conto che utilizzi per inviare i risultati. • Dall'AWSaccount del cliente. In questo caso, Security Hub consiglia di fornire il numero di account principale utilizzato per testare l'integrazione del prodotto. L'ideale è utilizzare lo stesso account per tutti i prodotti in tutte le regioni della Cina. Se ciò non è possibile, contatta il team di Security Hub. Se ricevi i risultati solo da Security Hub, può trattarsi di qualsiasi account che possiedi in una regione cinese. Tipo: String
`name`	Sì	Il nome del prodotto del provider da visualizz are nella console di Security Hub. Tipo: String Lunghezza massima: 24 caratteri

Campo	Campo obbligatorio	Descrizione
`description`	Sì	La descrizione del prodotto del provider da visualizzare sulla console di Security Hub. Tipo: String Lunghezza massima: 200 caratteri
`importType`	Sì	Il tipo di politica delle risorse per il partner. Durante il processo di onboarding dei partner, è possibile specificare una delle seguenti policy in materia di risorse oppure è possibile specificare`NEITHER`. • Con`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`, puoi inviare i risultati a Security Hub solo dall'account elencato nell'ARN del prodotto. • Con`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`, puoi inviare i risultati solo dall'account cliente a cui sei abbonato. Tipo: String Valori validi: `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` |`BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` | `NEITHER`

Campo	Campo obbligatorio	Descrizione
`category`	Sì	Le categorie che definiscono il tuo prodotto. Le selezioni vengono visualizzate nella console di 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`

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

Campo	Campo obbligatorio	Descrizione
		• IT Ticketing and Incident Management • 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 dellaMarketplace AWS destinazione del prodotto. L'URL viene visualizzato nella console di Security Hub. Tipo: String Deve essere unMarketplace AWS URL. Se non disponi di un'Marketplace AWSofferta, lascia vuoto questo campo.

Campo	Campo obbligatorio	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 che gestisci, ad esempio una GitHub pagina. Tipo: String La documentazione deve includere le seguenti informazioni. • Istruzioni di configurazione • Collegamenti aiAWS CloudFormation modelli (se necessario) • Informazioni sul tuo caso d'uso per l'integra zione • Latenza • Mappatura ASFF • Tipi di risultati inclusi • Architettura

Linee guida e elenco di controllo

Mentre prepari i materiali necessari per il tuoAWS Security Hubintegrazione, usa queste linee guida.

La checklist di prontezza 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 il logo da visualizzare sulAWS Security Hubplancia

Per visualizzare il logo sulAWS Security Hubconsole, segui queste linee guida.

Modalità luce e buio

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

Formato

Formato del file SVG

Background color (Colore di sfondo)

Transparent

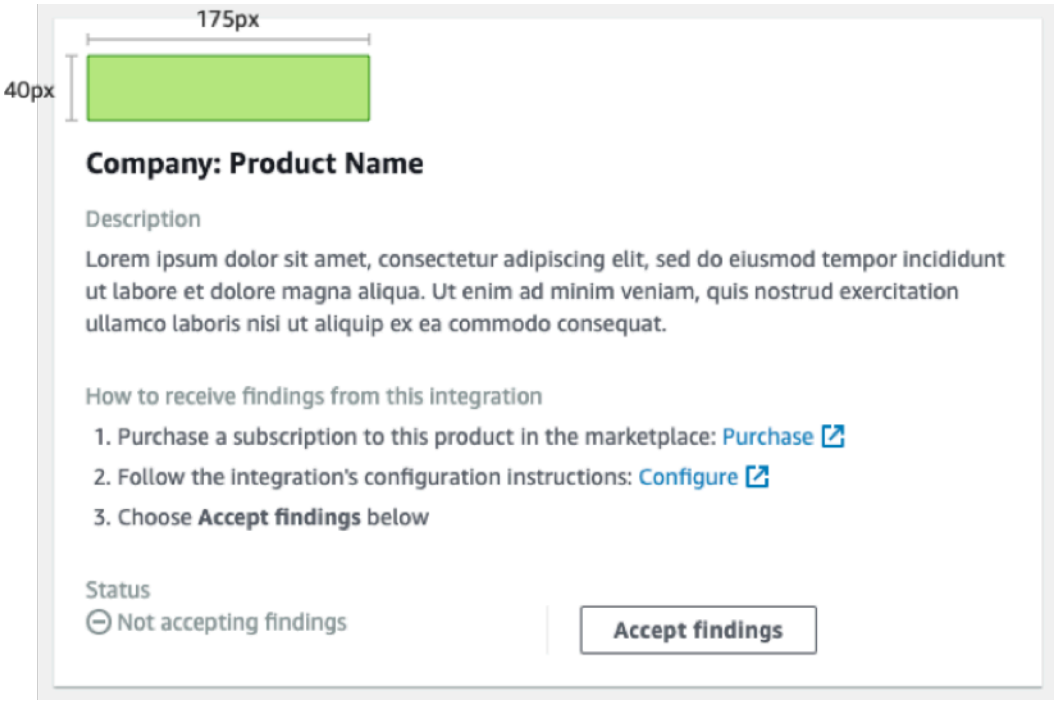
Size

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

L'altezza minima è di 40 px.

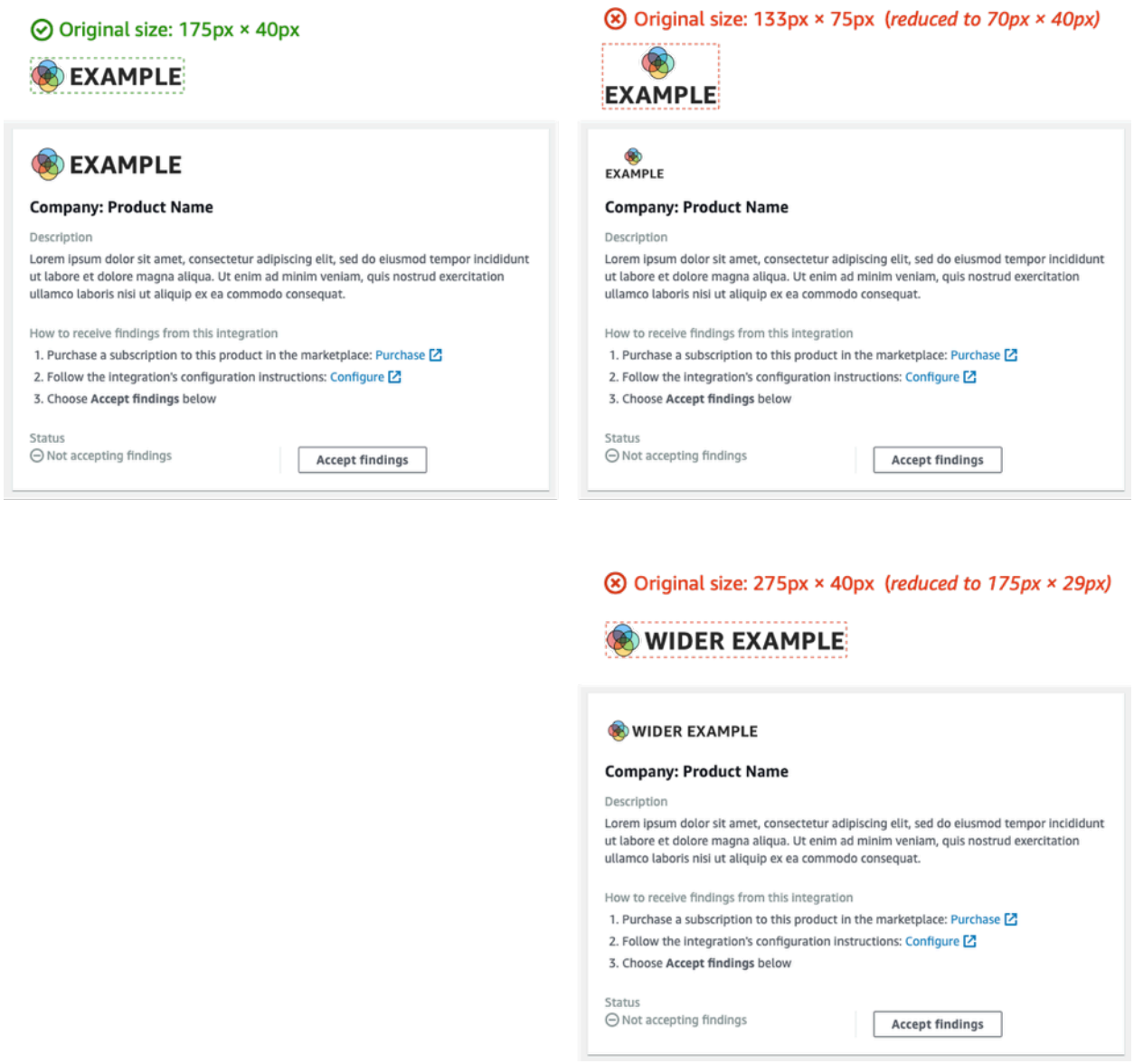
I loghi rettangolari funzionano meglio.

Nella seguente immagine viene mostrato in che modo viene visualizzato un logo ideale sulla console Security Hub.



Se il tuo 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 sul modo in cui il logo viene visualizzato sulla console di Security Hub.

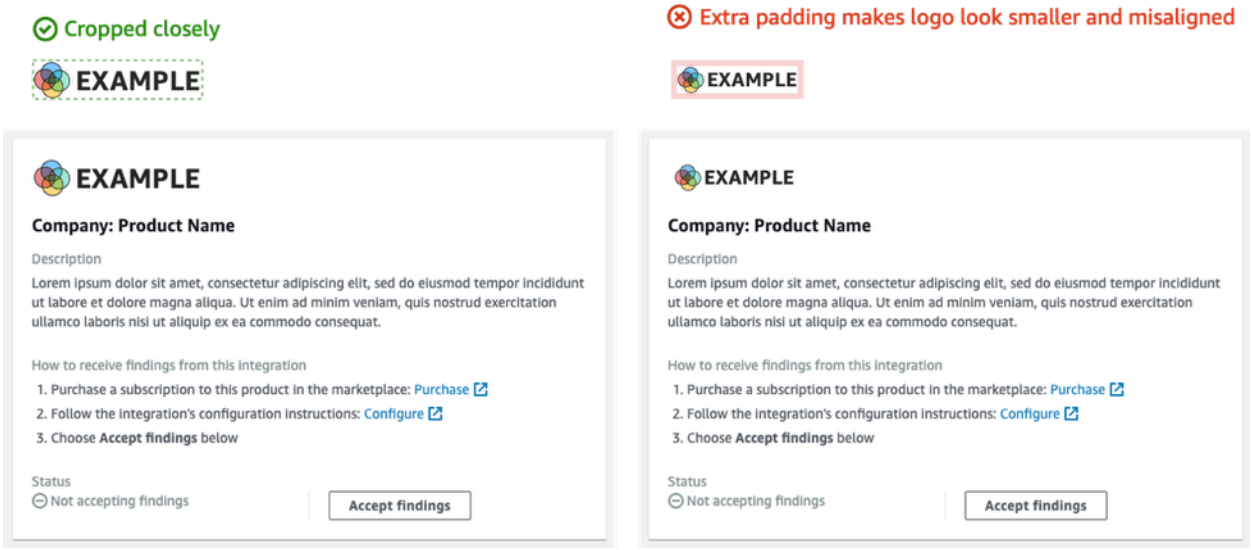
L'immagine seguente confronta la visualizzazione di un logo che utilizzava la dimensione ideale con loghi più larghi o più alti.



Ritaglio

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

L'immagine seguente mostra la differenza tra un logo ritagliato e un logo con imbottitura extra.



Principi per la creazione e l'aggiornamento dei risultati

Mentre pianifichi in che modo creerai e aggiornerai i risultati inAWS Security Hub, tieni presente i seguenti principi.

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

I clienti desiderano automatizzare le azioni di risposta e correzione e correlare i risultati con altri risultati. A tale scopo, i risultati dovrebbero avere le seguenti caratteristiche:

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

Quando una ricerca contiene dati per più eventi di sicurezza, è più difficile per i clienti intervenire in merito alla ricerca.

Mappare tutti i campi di ricerca sulAWSSecurity Finding Format (ASFF). Consenti ai clienti di fare affidamento su Security Hub come fonte di verità.

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

I clienti desiderano che tutti i dati siano presenti nella versione Security Hub del risultato. I dati mancanti causano la perdita di fiducia in Security Hub come fonte centrale di informazioni di sicurezza.

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

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

Quando c'è solo una piccola modifica al risultato, aggiorna il risultato invece di creare una nuova ricerca.

Quando c'è una modifica importante alla ricerca, ad esempio il punteggio di gravità o l'identificatore della risorsa, creare una nuova ricerca.

Ad esempio, creare risultati per le singole scansioni di porte in tempo reale non è molto fruibile. Poiché la scansione delle porte può avvenire continuamente, produrrebbe un grande volume di risultati. È molto più interessante e preciso aggiornare semplicemente l'ultimo tempo di scansione e contare su una singola ricerca per una scansione delle porte su una porta MongoDB da un nodo TOR.

Consenti ai clienti di personalizzare i risultati per renderli più significativi.

I clienti vogliono essere in grado di adeguare determinati campi di ricerca per renderli più pertinenti al loro ambiente o alle esigenze.

Ad esempio, i clienti desiderano essere in grado di aggiungere note, tag e regolare i punteggi di gravità in base al tipo di account o al tipo di risorsa a cui è associato il risultato.

Linee guida per la mappatura dei risultati nelAWSSecurity Finding Format (ASFF)

Utilizza le seguenti linee guida per mappare i risultati all'ASFF. Per descrizioni dettagliate di ogni campo e oggetto ASFF, vedereAWSSecurity Finding Format (ASFF)nellaAWS Security HubGuida per l'utente di.

Informazioni identificative

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

`ProductArn`è l'ARN cheAWS Security Hubti assegna.

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

`GeneratorId`può essere lo stesso`Id`oppure può fare riferimento a un'unità logica discreta, ad esempio AmazonGuardDutyID del rilevatore,AWS ConfigID registratore o ID IAM Access Analyzer.

Title e Description

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

Aggiungi informazioni più dettagliate a`Description`.`Description`è limitato a 1024 caratteri, inclusi gli spazi. È possibile prendere in considerazione l'aggiunta di 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 risultati

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

`Types`dovrebbe corrispondere a[tipi tassonomia 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`**

È necessario inviare`CreatedAt`e`UpdatedAt`ogni volta che chiami[`BatchImportFindings`](#)per ogni ritrovamento.

I valori devono corrispondere al formato ISO8601 in Python 3.8.

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

`FirstObservedAt` e `LastObservedAt`

`FirstObservedAt`e`LastObservedAt`deve corrispondere quando il sistema ha osservato il risultato. Se non registri queste informazioni, non è necessario inviare questi timestamp.

I valori corrispondono al formato ISO8601 in Python 3.8.

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

Severity

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

`Original`

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

`Label`

L'indicatore di Security Hub richiesto della gravità di ricerca. I valori consentiti sono i seguenti.

- `INFORMATIONAL`Nessun problema è stato rilevato.
- `LOW`— Il problema non richiede un'azione.
- `MEDIUM`— Il problema deve essere risolto, ma non con urgenza.
- `HIGH`— Il problema deve essere risolto in via prioritaria.
- `CRITICAL`— Il problema deve essere risolto immediatamente per evitare ulteriori danni.

I risultati conformi dovrebbero sempre avere`Label`impostata a`INFORMATIONAL`. Esempi di`INFORMATIONAL`i risultati sono risultati ottenuti dai controlli di sicurezza che sono passati eAWS Firewall Managerrisultati che vengono corretti.

I clienti spesso ordinano i risultati in base alla loro severità per fornire ai team delle operazioni di sicurezza un elenco di cose da fare. Sii prudente quando imposti la gravità della ricerca`HIGH`o`CRITICAL`.

La documentazione di integrazione deve includere la logica di mappatura.

Remediation

`Remediation`ha due elementi. Questi elementi sono combinati sulla console Security Hub.

`Remediation.Recommendation.Text`appare nelCorrezionesezione dei dettagli di ricerca. È collegato ipertestuale al valore di`Remediation.Recommendation.Url`.

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

SourceUrl

Usare solo`SourceUrl`se è possibile fornire un URL con collegamento approfondito alla console per la ricerca specifica. Altrimenti, omettilo dalla mappatura.

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

Malware, Network, Process, ThreatIntelIndicators

Se applicabile, utilizzare`Malware`,`Network`,`Process`, oppure`ThreatIntelIndicators`. Ognuno di questi oggetti è esposto nella console di Security Hub. Usa questi oggetti nel contesto del risultato che stai inviando.

Ad esempio, se si rileva malware che crea una connessione in uscita a un nodo di comando e controllo noto, fornire i dettagli per l'istanza EC2 in`Resource.Details.AwsEc2Instance`. Fornire il pertinente`Malware`,`Network`, e`ThreatIntelIndicator`oggetti per l'istanza EC2.

Malware

`Malware`è un elenco che accetta fino a cinque array di informazioni sul malware. Rendi le voci di malware pertinenti alla risorsa e alla ricerca.

Ogni voce dispone dei seguenti campi.

`Name`

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

`Name`dovrebbe provenire da un'intelligence o da una fonte di ricercatori verificata.

`Path`

Il percorso del malware. Il valore è una stringa di massimo 512 caratteri.`Path`dovrebbe essere un percorso di file di sistema Linux o Windows, tranne nei seguenti casi.

- Se si scansionano oggetti in un bucket S3 o in una condivisione EFS rispetto alle regole YARA,`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 clone.

`State`

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

Nel titolo e nella descrizione, assicurati di fornire il contesto per ciò che è successo con il malware.

Ad esempio, se`Malware.State`è`REMOVED`, quindi il titolo e la descrizione di ricerca dovrebbero riflettere che il prodotto ha rimosso il malware che si trova sul percorso.

Se`Malware.State`è`OBSERVED`, quindi il titolo e la descrizione di ricerca dovrebbero riflettere che il prodotto ha riscontrato questo malware situato sul percorso.

`Type`

Indica il tipo di malware. I valori consentiti sono`ADWARE|BLENDED_THREAT|BOTNET_AGENT|COIN_MINER|EXPLOIT_KIT|KEYLOGGER|MACRO|POTE`

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

Network

`Network`è un singolo oggetto. Non è possibile aggiungere più dettagli relativi alla rete. Quando mappi i campi, utilizzare le seguenti linee guida.

Informazioni sulla destinazione e sulla fonte

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

In genere, la fonte è da dove ha avuto origine l'attacco, ma potrebbe avere altre fonti come elencato di seguito. Dovresti spiegare la fonte nella tua documentazione e descriverla anche nel titolo e nella descrizione di ricerca.

- Per un attacco DDoS su un'istanza EC2, la fonte è l'attaccante, sebbene un attacco DDoS reale possa utilizzare milioni di host. La destinazione è l'indirizzo IPv4 pubblico dell'istanza EC2.`Direction`è IN.
- Per il malware osservato che comunica da un'istanza EC2 a un nodo di comando e controllo noto, l'origine è l'indirizzo IPV4 dell'istanza EC2. La destinazione è il nodo di comando e controllo.`Direction`è`OUT`. Dovresti anche fornire`MalwareeThreatIntelIndicators`.

`Protocol`

`Protocol`mappa sempre a un nome registrato IANA (Internet Assigned Numbers Authority), a meno che non sia possibile fornire un protocollo specifico. È sempre necessario utilizzarlo e fornire le informazioni sulla porta.

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

`Direction`

`Direction`è sempre relativo al*AWS*limiti della rete.

- `IN`significa che sta entrando*AWS*(VPC, servizio).
- `OUT`significa che sta uscendo dal*AWS*limiti della rete.

Process

`Process`è un singolo oggetto. Non è possibile aggiungere più dettagli relativi al processo. Quando mappi i campi, utilizzare le seguenti linee guida.

`Name`

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

`Path`

`Path`è il percorso del file system all'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 Windows. Per differenziare, utilizza EC2 Amazon Machine Images (AMI) per fornire le informazioni. I clienti possono probabilmente distinguere tra Windows e Linux.

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

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

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

ThreatIntelIndicators

`ThreatIntelIndicators`accetta una serie di massimo cinque oggetti di intelligence delle minacce.

Per ogni voce,`Type`è nel contesto della minaccia specifica. I valori consentiti sono`DOMAIN|EMAIL_ADDRESS|HASH_MD5|HASH_SHA1|HASH_SHA256|HASH_SHA512|IPV4_ADDRESS|IPV6`

Di seguito sono elencati alcuni esempi di come mappare gli indicatori di intelligence delle minacce:

- Hai trovato un processo che sai è associato a Cobalt Strike. L'hai imparato daFireEyedi blog.

  Imposta `Type` su `PROCESS`. Crea anche un`Process`oggetto per il processo.
- Il filtro di posta ha trovato qualcuno che inviava un noto pacchetto hash da un dominio dannoso noto.

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

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

Resources

Per`Resources`, utilizzare i nostri tipi di risorse e i campi di dettaglio forniti quando possibile. Security Hub aggiunge costantemente nuove risorse all'ASFF. Per ricevere un registro mensile delle modifiche apportate ad ASFF, contattare`<securityhub-partners@amazon.com>`.

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

Per una risorsa che non è modellata in ASFF, impostare`Type`a`Other`. Per informazioni dettagliate, utilizzare`Details.Other`.

È possibile utilizzare anche l'`0ther`tipo di risorsa per non-AWSrisultati.

ProductFields

Usare solo`ProductFields`se non è possibile utilizzare un altro campo curato per`Resource`o un oggetto descrittivo come`ThreatIntelIndicators`,`Network`, oppure`Malware`.

Se si utilizza`ProductFields`, è necessario fornire una logica rigorosa per questa decisione.

Conformità

Usare solo`Compliance`se le tue scoperte sono legate alla conformità.

Utilizzo di Security Hub`Compliance`per i risultati che genera in base ai controlli.

Utilizzo di Firewall Manager`Compliance`per le sue scoperte perché sono legate alla conformità.

Campi che sono soggetti a restrizioni

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

Non mappare su questi campi o oggetti.

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

Per questi campi, mappare i campi che si trovano nella`FindingProviderFields`soggetto. Non eseguire la mappatura ai campi di primo livello.

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

Linee guida per l'utilizzo del`BatchImportFindings`API

Quando utilizzi l'`BatchImportFindings`Operazione API per inviare risultati aAWS Security Hubutilizzare le linee guida seguenti.

- Devi chiamare`BatchImportFindings`utilizzando l'account associato ai risultati. L'identificatore del conto associato è il valore del`AwsAccountId`attributo per il ritrovamento.
- Invia il batch più grande possibile. Security Hub accetta fino a 100 risultati per batch, fino a 240 KB per individuazione e fino a 6 MB per batch.
- Il limite di velocità dell'acceleratore è di 10 TPS per conto per regione, con una raffica 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 di ricerca in modo da poter inviare aggiornamenti di ricerca man mano che una ricerca va avanti e fuori dalla conformità.
- Per informazioni sulla lunghezza massima di stringhe e altre limitazioni, consultareAWSSecurity Finding Format (ASFF)nellaAWS Security HubGuida per l'utente di.

Elenco di controllo della preparazione dei prodotti

LaAWS Security Hube i team di partner APN utilizzano questa lista di controllo per verificare che l'integrazione sia pronta per essere lanciata.

Mappatura ASFF

Queste domande riguardano la mappatura del tuo ritrovamento alAWSSecurity Finding Format (ASFF).

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

Mappare tutte le tue scoperte all'ASFF in qualche modo.

Utilizzare campi curati come tipi di risorse modellate,`Network`,`Malware`, oppure`ThreatIntelIndicators`.

Mappa qualsiasi altra cosa in`Resource.Details.Other`o`ProductFields`a seconda delle necessità.

Il partner usa**`Resource.Details`**campi, come**`AwsEc2instance`**,**`AwsS3Bucket`**, e**`Container`**? Il partner usa**`Resource.Details.Other`**per definire i dettagli delle risorse che non sono modellati nell'ASFF?

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

Mappare altre informazioni relative alle risorse`Resource.Details.Other`solo quando non c'è una corrispondenza diretta.

Il partner mappa i valori**`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 potrebbe essere mappato in altri campi ASFF?

Usare solo`ProductFields`per informazioni specifiche del prodotto come informazioni sul controllo delle versioni, risultati 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`**?

La`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 ricerca, ad eccezione dei risultati che vogliono aggiornare?

Tutti i risultati in Security Hub sono indicizzati sull'identificatore di ricerca (`Id`attributo). Questo valore deve sempre essere univoco per garantire che i risultati non vengano aggiornati accidentalmente.

È inoltre necessario mantenere lo stato identificativo di ricerca allo scopo di aggiornare i risultati.

Il partner fornisce un valore che mappa i risultati su un ID generatore?

`GeneratorID`non dovrebbe avere lo stesso valore dell'ID di ricerca.

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

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

Il partner utilizza gli spazi dei nomi dei tipi di ricerca richiesti in un modo pertinente al proprio prodotto? Il partner utilizza le categorie o i classificatori di tipo di ricerca consigliati nei loro tipi di ricerca?

La tassonomia del tipo di ricerca dovrebbe mappare attentamente i risultati generati dal prodotto.

Gli spazi dei nomi di primo livello delineati nellaAWSIl formato di ricerca di sicurezza è obbligatorio.

È possibile utilizzare valori personalizzati per gli spazi dei nomi di secondo e terzo livello (categorie o classificatori).

Il partner acquisisce le informazioni sul flusso di rete nel**`Network`**campi, se hanno dati di rete?

Se il prodotto viene catturatoNetFlowinformazioni, mappalo al`Network`.

Le informazioni del processo di acquisizione dei partner (PID) nel**`Process`**campi, se hanno dati di processo?

Se il tuo prodotto acquisisce le informazioni sul processo, mappale al`Process`.

Il partner acquisisce le informazioni sul malware nel**`Malware`**campi, se hanno dati malware?

Se il tuo prodotto acquisisce informazioni malware, mappale alla`Malware`.

Il partner acquisisce le informazioni di threat intelligence nel**`ThreatIntelIndicators`**campi, se hanno dati di intelligence sulle minacce?

Se il tuo prodotto acquisisce informazioni di threat intelligence, mappale alla`ThreatIntelIndicators`.

Il partner fornisce una valutazione di fiducia per i risultati? Se lo fanno, viene fornita una logica?

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

Il partner utilizza un ID canonico o un ARN per l'ID risorsa nel risultato?

Quando si identificaAWSrisorse, la migliore pratica è usare l'ARN. Se un ARN non è disponibile, utilizzare l'ID della risorsa canonica.

Configurazione e funzione dell'integrazione

Queste domande sono relative alla configurazione eday-to-dayfunzione dell'integrazione.

Il partner fornisce uninfrastructure-as-code(iAC) template per implementare l'integrazione con Security Hub, ad esempio Terraform,AWS CloudFormation, oppureAWS Cloud Development Kit (AWS CDK)?

Per integrazioni che invieranno risultati dall'account del cliente o utilizzerannoCloudWatchEventi per consumare i risultati, è necessaria una qualche forma di modello IAC.

AWS CloudFormationè preferibile, maAWS CDKÈ 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 nel loro prodotto per attivare l'integrazione. Ciò potrebbe comportare il provisioning automatico di risorse e autorizzazioni. Se invii risultati da un account prodotto, la configurazione con un clic è il metodo preferito.

Il partner invia solo risultati di valore?

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

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

Il partner ha fornito una stima su quanti risultati invieranno al giorno per cliente e a quale frequenza (media e raffica)?

Numeri di risultati univoci vengono utilizzati per calcolare il carico su Security Hub. Un risultato unico è definito come un risultato con una mappatura ASFF diversa da un'altra scoperta.

Ad esempio, se un individuo è popolato solo`ThreatIntelIndicators`e solo un altro popolato`Resources.Details.AWSEc2Instance`, sono due scoperte uniche.

Il partner ha un modo aggraziato di gestire gli errori 4xx e 5xx in modo tale da non essere limitati e tutti i risultati possono essere inviati in un secondo momento?

Attualmente c'è una velocità di burst di 30-50 TPS sul`BatchImportFindings`Operazione API. Se vengono restituiti errori 4xx o 5xx, è necessario mantenere lo stato dei risultati non riusciti in modo da poterli riprovare nella totalità in un secondo momento. Puoi farlo tramite una coda di lettere morte o un'altraAWSservizi di messaggistica come Amazon SNS o Amazon SQS.

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

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

Se fornisci risultati, non utilizzare il`BatchUpdateFindings`operazione per aggiornare i risultati. Questa operazione deve essere utilizzata solo dai clienti. Si usa solo`BatchUpdateFindings`quando indaghi e intraprendi provvedimenti sui risultati.

Il partner gestisce i tentativi in modo da non compromettere i risultati di successo inviati in precedenza?

Dovresti disporre di un meccanismo per conservare gli ID di ricerca originali in caso di errori in modo da non duplicare o sovrascrivere i risultati riusciti per errore.

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

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

La`BatchUpdateFindings`l'operazione deve essere utilizzata solo dai clienti.

Il partner aggiorna i risultati utilizzando il**`BatchUpdateFindings`**API?

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

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

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

Queste informazioni sono richieste nel manifesto.

Se l'architettura del partner deve inviare risultati a Security Hub da un account cliente, l'hanno dimostrato con successo? Se l'architettura del partner deve inviare risultati a Security Hub dal proprio account, l'hanno dimostrato con successo?

Durante il test, i risultati devono essere inviati con successo da un account di tua proprietà diverso da quello fornito per l'ARN del prodotto.

L'invio di un risultato dall'account del proprietario ARN del prodotto può ignorare alcune eccezioni di errore dalle operazioni API.

Il partner fornisce un risultato cardiaco a Security Hub?

Per dimostrare che la tua integrazione funziona correttamente, devi inviare una ricerca del battito cardiaco. Il rilevamento del battito cardiaco viene inviato ogni cinque minuti e utilizza il tipo di ricerca`Heartbeat`.

Questo è importante se invii risultati da un account prodotto.

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

Durante la convalida della pre-produzione, è necessario inviare esempi di ricerca al team di prodotti Security HubAWSconto. Questi esempi dimostrano che i risultati vengono inviati e mappati correttamente.

Documentazione

Queste domande riguardano la 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, Leggi i documenti o altro formato dedicato.

Documentazione di hosting suGitHubnon soddisfa i requisiti del sito web dedicato.

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

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

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

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

La documentazione del partner fornisce una logica per i risultati che inviano?

Dovresti fornire la logica per i tipi di risultati che invii.

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

La documentazione del partner fornisce una logica per il modo in cui il partner mappa i propri risultati ad ASFF?

Dovresti fornire la logica per la mappatura del reperimento nativo di un prodotto ad 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 conup-to-dateinformazioni.

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 richieste nel manifesto.

La documentazione del partner descrive in che modo il punteggio di gravità viene associato al punteggio di gravità ASFF?

Fornisci informazioni su come mappi`Severity.0riginalaSeverity.Label`.

Ad esempio, se il valore di gravità è un grado di lettera (A, B, C), è necessario fornire informazioni su come mappare il livello della lettera sull'etichetta di gravità.

La documentazione dei partner fornisce una logica per le valutazioni di fiducia?

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

Se si utilizzano punteggi di confidenza popolati staticamente o mappature derivati dall'intelligenza artificiale o dal machine learning, è necessario fornire un contesto aggiuntivo.

La documentazione del partner nota quali Regioni il partner supporta e non supporta?

Nota Regioni che sono o non sono supportate in modo che i clienti sappiano in quali Regioni non tentare l'integrazione.

Informazioni sulla scheda prodotto

Queste domande si riferiscono alla scheda del prodotto che viene visualizzata sulIntegrazionipagina della console Security Hub.

È fornitoAWSID account valido e contiene 12 cifre?

Gli identificatori dell'account hanno una lunghezza di 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 nel JSON all'interno del manifest non deve superare i 200 caratteri inclusi gli spazi.

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

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

Il link di acquisto (se fornito) porta alMarketplace AWSofferta per il prodotto?

Se fornisci un link per l'acquisto, deve essere per unMarketplace AWSingresso. Security Hub non accetta collegamenti di acquisto che non sono ospitati daAWS.

Le categorie di prodotti descrivono correttamente il prodotto?

Nel manifesto è possibile fornire fino a tre categorie di prodotti. Questi devono corrispondere al JSON e non possono essere personalizzati. Non è possibile fornire più di tre categorie di prodotti.

I nomi dell'azienda e dei prodotti sono validi e corretti?

Il nome della società deve essere pari o inferiore a 16 caratteri.

Il nome del prodotto deve essere pari o inferiore a 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 di Security Hub è compresa tra 700 caratteri, inclusi gli spazi?

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

Il team modificherà descrizioni più lunghe.

Il logo della pagina dei partner di Security Hub non è superiore a 600 x 300 px?

Fornisci un URL accessibile pubblicamente con un logo aziendale in PNG o JPG non superiore a 600 x 300 pixel.

Il collegamento ipertestuale Ulteriori informazioni sulla pagina dei partner di Security Hub porta alla pagina web dedicata del partner sull'integrazione?

LaUlteriori informazioniil link non dovrebbe portare al sito web principale del partner o alle informazioni sulla documentazione.

Questo link dovrebbe sempre andare 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?

Un video demo o di integrazione è facoltativo, ma consigliato.

È unAWSIl post del blog di Partner Network è stato rilasciato con il partner e il responsabile dello sviluppo partner o il rappresentante dello sviluppo dei partner?

AWSI post del blog di Partner Network dovrebbero essere coordinati in anticipo con il responsabile dello sviluppo partner o il rappresentante dello sviluppo dei partner.

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

Consenti un tempo di consegna di 4-6 settimane. Questo sforzo dovrebbe essere avviato dopo aver completato il test con il prodotto privato ARN.

Viene rilasciato un comunicato stampa guidato dai partner?

Puoi collaborare con il tuo responsabile dello sviluppo partner o il rappresentante dello sviluppo dei partner per ottenere un preventivo dal VP di Servizi di sicurezza esterna. Puoi utilizzare questa citazione nel tuo comunicato stampa.

Viene pubblicato un post sul blog guidato dai partner?

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

Viene rilasciato un webinar guidato dai partner?

Puoi creare webinar personalizzati 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 l'ARN del prodotto privato.

Il partner ha richiesto il supporto ai social mediaAWS?

Dopo il rilascio, puoi lavorare con ilAWSGuida all'uso del marketing per la sicurezzaAWScanali ufficiali di social media per condividere i dettagli sui tuoi webinar.

AWS Security HubDomande frequenti sui partner

Di seguito sono riportate le domande frequenti sull'impostazione e il mantenimento di un'integrazione conAWS Security Hub.

1. Quali sono i vantaggi principali di Security Hub?
   - La soddisfazione del cliente— Il motivo principale per l'integrazione con Security Hub è dovuto alle richieste dei clienti per farlo.

     Security Hub è il centro di sicurezza e conformità perAWSclienti. È progettato come la prima tappa doveAWSi professionisti della sicurezza e della conformità si rivolgono ogni giorno a comprendere il loro stato di sicurezza e conformità.

     Ascolta i tuoi clienti. Ti diranno se vogliono vedere i tuoi risultati in Security Hub.
   - Opportunità— Promuoviamo partner con integrazioni certificate all'interno della console Security Hub, inclusi i collegamenti ai loroMarketplace AWSinserzioni. Questo è un ottimo modo per i clienti di scoprire nuovi prodotti per la sicurezza.
   - Operazioni di marketing— I fornitori con integrazioni approvate possono partecipare a webinar, rilasciare comunicati stampa, creare fogli sottili e dimostrare le loro integrazioniAWSclienti.
2. Quali tipi di partner esistono?
   - Partner che inviano i risultati a Security Hub
   - Partner che riceve risultati dal Security Hub
   - Partner che inviano e ricevono risultati
   - Partner di consulenza che aiutano i clienti a configurare, personalizzare e utilizzare Security Hub nel proprio ambiente
3. Come funziona l'integrazione di un partner con Security Hub ad alto livello?

   Raccogli i risultati dall'interno di un account cliente o dal tuoAWStenere conto e trasformare il formato dei risultati inAWSSecurity Finding Format (ASFF). È quindi possibile inviare tali risultati all'endpoint regionale di Security Hub appropriato.

   È possibile utilizzare ancheCloudWatchEventi per ricevere i risultati dal Security Hub.
4. Quali sono i passaggi fondamentali per completare un'integrazione con Security Hub?
   a. Invia informazioni sul manifest dei tuoi partner.
   b. Ricevi gli ARN dei prodotti da utilizzare con Security Hub, se invii risultati a Security Hub.

c. Mappare i risultati su ASFF. Consulta the section called “Linee guida per il mapping ASFF”.

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

e. Crea un framework di distribuzione per i clienti. Ad esempio:AWS CloudFormationgli script possono servire a questo scopo.

f. Documenta la configurazione e fornisci istruzioni di configurazione per i clienti.

g. Definisci tutte le informazioni personalizzate (regole di correlazione) che i clienti possono utilizzare con il tuo prodotto.

h. Dimostra la tua integrazione con il team di Security Hub.

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

5. Qual è il processo per la presentazione del manifesto partner? E perAWSservizi per inviare i risultati a Security Hub?

   Per inviare le informazioni manifest al team di Security Hub, utilizzare<securityhub-partners@amazon.com>.

   Ti vengono emessi ARN di prodotti 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 astenerti dall'inviare risultati che non forniscono valore ai clienti.

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

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

   Questi sono gli approcci principali:

   - Inviate i risultati dal proprio designatoAWSaccount che utilizza ilBatchImportFindingsoperazione.
   - Inviate i risultati dall'interno del conto cliente utilizzando ilBatchImportFindingsoperazione. È possibile utilizzare approcci presumi-role, ma questi approcci non sono richiesti.

   Per linee guida generali sull'utilizzoBatchImportFindings, consultathe section called “Linee guida per l'utilizzo delBatchImportFindingsAPI”.

8. Come posso raccogliere i miei risultati e inviarli a un endpoint regionale di Security Hub?

I partner hanno utilizzato diversi approcci per questo, in quanto dipendono fortemente dall'architettura della soluzione.

Ad esempio, alcuni partner creano un'app Python che può essere distribuita comeAWS CloudFormationcopione. Lo script raccoglie i risultati del partner dall'ambiente cliente, li trasforma in ASFF e li invia all'endpoint regionale di 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 sapere quando iniziare a inviare i risultati a Security Hub?

   Security Hub supporta l'autorizzazione parziale in batch per il`BatchImportFindings`Operazione API, in modo da poter inviare tutte le tue scoperte a Security Hub per tutti i tuoi clienti.

   Se alcuni dei tuoi clienti non si sono ancora iscritti a Security Hub, Security Hub non acquisisce tali risultati. Esso ingerisce solo i risultati autorizzati presenti nel lotto.

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

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

    b. Abilita una sottoscrizione di prodotti (criteri delle risorse) per gli account. Usa o il`EnableImportFindingsForProduct`Operazione APIIntegrazioni(Certificato creato). Il cliente può farlo oppure è possibile utilizzare ruoli cross-account per agire per conto del cliente.

    c. Assicurarsi che il`ProductArn`del risultato è l'ARN pubblico del tuo prodotto.

    d. Assicurarsi che il`AwsAccountId`del risultato è l'ID dell'account del cliente.

    e. Assicurati che i tuoi risultati non dispongano di dati malformati in base alAWSSecurity Finding Format (ASFF). Ad esempio, i campi obbligatori vengono compilati e non ci sono valori non validi.

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

11. Quali autorizzazioni IAM devono essere in vigore per inviare i risultati?

    I criteri IAM devono essere configurati per l'utente o il ruolo IAM che chiama`BatchImportFindings`o altre chiamate API.

    Il test più semplice è farlo da un account amministratore. Puoi vincolarli `aaction: 'securityhub:BatchImportFindings'eresource: <productArn and/or productSubscriptionArn>`.

Le risorse nello stesso account possono essere configurate con i criteri IAM senza richiedere criteri per le risorse.

Per escludere problemi di politica IAM dal chiamante di`BatchImportFindings`, impostare il criterio IAM per il chiamante come segue:

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

Assicurati di verificare che non ci sianoDenypolitiche per il chiamante. Dopo averlo funzionato, è possibile limitare la policy 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 un abbonamento prodotto?

Per ricevere risultati da uno specifico prodotto partner, il cliente (o il partner con ruoli cross-account che lavorano per conto del cliente) deve stabilire un abbonamento al prodotto. Per farlo dalla console, utilizzano ilIntegrazioni(Certificato creato). Per fare ciò dall'API, usano il`EnableImportFindingsForProduct`Operazione API

La sottoscrizione del prodotto crea una politica sulle risorse che autorizza la ricezione o l'invio dei risultati del partner dal cliente. Per dettagli, consultare Casi d'uso e autorizzazioni.

Security Hub dispone dei seguenti tipi di criteri per le 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 policy.

conBATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT, puoi inviare i risultati a Security Hub solo dall'account elencato nel tuo prodotto ARN.

conBATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT, puoi inviare risultati solo dall'account cliente che ti ha sottoscritto.

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

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

    Il cliente deve mettere in atto un abbonamento prodotto per ciascun account. Possono farlo a livello di programmazione tramite l'API.

14. Qual è il mio prodotto ARN?

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

    `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`

    Viene fornito un ARN prodotto per ogni regione in cui è distribuito Security Hub. L'ID account, la società e i nomi dei prodotti sono dettati dalle comunicazioni manifest del partner. Non si modificano mai le informazioni associate all'ARN del prodotto, ad eccezione del codice regionale. Il codice regione deve corrispondere alla regione per la quale si inviano i risultati.

    Un errore comune è quello di modificare l'ID account in modo che corrisponda all'account da cui stai attualmente lavorando. L'ID account non cambia. Inviate un ID account «home» come parte dell'invio manifesto. Questo ID account è bloccato nell'ARN del prodotto.

Quando Security Hub viene avviato in nuove regioni, utilizza automaticamente i codici Regioni standard per generare gli ARN di prodotti per tali regioni.

A ogni account viene inoltre eseguito automaticamente il provisioning di un prodotto ARN privato. È possibile utilizzare questo ARN per testare i risultati di importazione all'interno del proprio account di sviluppo prima di ricevere il prodotto pubblico ufficiale ARN.

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

I risultati devono essere forniti nelAWSSecurity Finding Format (ASFF). Per informazioni dettagliate, consulta .AWSSecurity Finding Format (ASFF)nellaAWS Security HubGuida per l'utente di.

L'aspettativa è che tutte le informazioni contenute nei tuoi risultati nativi siano pienamente riflesse nell'ASFF. Campi personalizzati come`ProductFields`o`Resource.Details.Other`consente di mappare dati che non si adattano perfettamente ai campi predefiniti.

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

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

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

Consultare ilElenco endpoint Security Hub.

18. Posso inviare i risultati tra regioni?

Security Hub non supporta ancora l'invio di risultati tra regioni per il nativoAWSservizi, come AmazonGuardDuty, 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 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 lotti di risultati?

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

È possibile batch di una serie di risultati da conti diversi. Tuttavia, se uno qualsiasi dei conti nel batch non è sottoscritto a Security Hub, l'intero batch ha esito negativo. Questa è una limitazione del modello di autorizzazione di base API Gateway.

Consulta the section called “Linee guida per l'utilizzo del`BatchImportFindings`API”.

20. Posso inviare aggiornamenti ai risultati che ho creato?

    Sì, se invii una ricerca con lo stesso ARN del prodotto e lo stesso ID di ricerca, sovrascrive i dati precedenti per tale ricerca. Si noti che tutti i dati sono sovrascritti, quindi è necessario inviare un risultato completo.

    I clienti vengono contabilizzati e addebitati sia per i nuovi risultati che per la ricerca di aggiornamenti.

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

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

22. Come invecchiano i risultati?

    Security Hub elimina i risultati 90 giorni dopo l'ultimo aggiornamento. Trascorso questo tempo, i risultati obsoleti vengono eliminati dal Security HubOpenSearchgrappolo.

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

    I clienti possono utilizzareCloudWatchEventi per spostare i risultati da Security Hub. In questo modo, tutti i risultati possono essere inviati agli obiettivi di scelta del cliente.

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

23. Quali acceleratori mette in atto Security Hub?

    Acceleratori Security Hub`GetFindings`Chiamate API, poiché viene utilizzato l'approccio consigliato per accedere ai risultatiCloudWatchEventi.

Security Hub non implementa altre limitazioni su servizi interni, partner o clienti oltre a quella applicata dalle invocazioni API Gateway e Lambda.

24. Quali sono gli SLA di tempestività o latenza o le aspettative per i risultati inviati a Security Hub dai servizi di origine?

    L'obiettivo è quello di essere il più vicino possibile in 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, utilizza uno dei seguenti metodi.

    - Tutti i risultati vengono inviati automaticamente aCloudWatchEventi. Un cliente può creare specificiCloudWatchRegole degli eventi per inviare risultati a obiettivi specifici, come un SIEM o un bucket S3. Questa funzionalità ha sostituito il legacy`GetFindings`Operazione API
    - UtilizzaCloudWatchEventi per azioni personalizzate. Security Hub consente ai clienti di selezionare risultati specifici o gruppi di risultati all'interno della console e intervenire su di essi. Ad esempio, possono inviare i risultati a un SIEM, un sistema di ticketing, una piattaforma di chat o un flusso di lavoro di risanamento. Questo fa 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, aCloudWatchl'evento è creato per quei risultati specifici. Potresti sfruttare questa capacità e creareCloudWatchRegole degli eventi e obiettivi da utilizzare per un cliente come parte di un'azione personalizzata. Notare che questa funzionalità non viene utilizzata per inviare automaticamente tutti i risultati di un particolare tipo o classe aCloudWatchEventi. Spetta a un utente agire su risultati specifici.

      È possibile utilizzare le operazioni dell'API di azione personalizzate, ad esempio`CreateActionTarget`, per creare automaticamente le azioni disponibili per il tuo prodotto (ad esempio l'utilizzoAWS CloudFormationmodelli). Useresti ancheCloudWatchOperazioni API regole eventi per creare corrispondentiCloudWatchRegole eventi associate all'azione personalizzata. Utilizzo diAWS CloudFormationmodelli, puoi anche creareCloudWatchRegole degli eventi per l'acquisizione automatica 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 gestita (MSSP) per diventare un partner Security Hub?

È necessario dimostrare come Security Hub viene utilizzato come parte della fornitura di servizi ai clienti.

Dovresti avere una documentazione utente che spieghi l'utilizzo di Security Hub.

Se l'MSSP è un provider di ricerca, deve dimostrare l'invio dei risultati a Security Hub.

Se l'MSSP riceve solo risultati da Security Hub, deve avere almeno unAWS CloudFormationtemplate per impostare l'appropriatoCloudWatchRegole eventi

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.
    - Consente di collegare le soluzioni ISV (Independent Software Vendor) già integrate a Security Hub utilizzando le istruzioni di configurazione nella pagina partner della console.
    - Aiuta i clienti con integrazioni personalizzate di prodotti.
    - Crea insight personalizzati pertinenti alle esigenze e ai set di dati del cliente.
    - Crea azioni personalizzate.
    - Crea playbook di risanamento.
    - Crea Quickstart che si allineano agli standard di conformità di Security Hub. Questi devono essere convalidati dal team Security Hub.

    I casi di studio non hanno bisogno di essere condivisi pubblicamente.

28. Quali sono i requisiti relativi al modo in cui distribuisco la mia integrazione con Security Hub con i miei clienti?

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

    Se si sta distribuendo software di integrazione nel clienteAWSambiente, dovresti sfruttareAWS CloudFormationmodelli per semplificare l'integrazione. Alcuni partner hanno creato un'integrazione con un clic, che è altamente incoraggiata.

29. Quali sono i requisiti per la documentazione?

È necessario fornire un collegamento alla documentazione che descriva il processo di integrazione e configurazione tra il prodotto e Security Hub, incluso l'utilizzo diAWS CloudFormationmodelli di.

Tale documentazione dovrebbe includere anche informazioni sull'utilizzo di ASFF da parte dell'utente. Nello specifico, questo dovrebbe elencare i tipi di ricerca ASFF che stai utilizzando per i tuoi diversi risultati. Se si dispone di definizioni di insight predefinite, consigliamo di includerle anche qui.

Considera di includere altre informazioni potenziali:

- Il tuo caso d'uso per l'integrazione con Security Hub
- Volume medio di risultati inviati
- La tua architettura di integrazione
- Le regioni che fai e non supportate
- Latenza tra la creazione dei risultati e l'invio a Security Hub
- Se si aggiornano i risultati

30. Cosa sono gli insight personalizzati?

Sei incoraggiato a definire insight personalizzati per i tuoi risultati. Le informazioni approfondite sono regole di correlazione leggere che aiutano un cliente a dare priorità a quali risultati e risorse richiedono più attenzione e azione.

Security Hub ha un`CreateInsight`Operazione API Puoi creare insight personalizzati all'interno di un account cliente come parte del tuoAWS CloudFormationtemplate. Queste informazioni dettagliate vengono visualizzate sulla console del cliente.

31. Posso inviare widget del dashboard?

No, non al momento. È possibile creare solo informazioni dettagliate gestite.

32. Qual è il tuo modello di prezzo?

Consultare il[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 per la 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 di ASFF. Per ottenere il numero di conto demo, contatta il team di Security Hub.

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

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

Security Hub fornisce una risposta per l'autorizzazione e una risposta per`BatchImportFindings`. Sono in fase di sviluppo messaggi di errore, errori e successi 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 messaggi di errore, tentativi, limitazioni e allarmanti. Devono inoltre gestire feedback o messaggi di errore inviati tramite il meccanismo di feedback di Security Hub.

36. Quali sono alcune risoluzioni ai problemi più comuni?

Un record`AuthorizerConfigurationException`è causato da un malformato`AwsAccountId`o`ProductArn`.

Durante la risoluzione dei problemi, tieni presente quanto segue:

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

  L'ID account non cambia rispetto a quello incluso dal team di Security Hub negli ARN del prodotto che ti hanno fornito.

`AccessDeniedException`è causato quando un reperimento viene inviato da o dall'account sbagliato o quando l'account non ha`ProductSubscription`. Il messaggio di errore conterrà un ARN con un tipo di risorsa di`productoproduct-subscription`. Questo errore si verifica solo durante le chiamate cross-account. Se chiami`BatchImportFindings`con il tuo account per lo stesso account in`AwsAccountId`e`ProductArn`, l'operazione utilizza le policy IAM e non si deve considerare`ProductSubscriptions`.

Assicurati che l'account cliente e l'account del prodotto che utilizzi siano gli account registrati effettivi. Alcuni partner hanno utilizzato un numero di conto per il prodotto dal prodotto ARN, ma tentano di utilizzare un account completamente diverso per chiamare`BatchImportFindings`.

In altri casi, hanno creato`ProductSubscriptions`per altri account clienti o anche per il proprio account prodotto. Non hanno creato`ProductSubscriptions`per il conto del cliente in cui ha tentato di importare i risultati.

37 Dove posso inviare domande, commenti e bug?

`<securityhub-partners@amazon.com>`

38 A quale regione invio i risultati per gli articoli correlati a globaliAWSservizi? Ad esempio, dove posso inviare i risultati relativi all'IAM?

Invia i risultati alla stessa regione in cui è stato rilevato il risultato. Per un servizio come IAM, la 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 viene rilevato lo stesso problema IAM in tutte e tre le regioni, inviare il risultato a tutte e tre le regioni.

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

Cronologia dei documenti per i partner

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

Modifica	Descrizione	Data
requisiti aggiornati per il logo della console	Sono stati aggiornati il manifesto del partner e le linee guida per il logo per indicare che i partner devono fornire sia una versione in modalità chiara che una versione in modalità scura del logo da visualizzare sulla console di 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 alAWSPercorso ISV Partner e chi utilizza un prodotto di integrazione che ha completato unAWSRevisione tecnica fondamentale (FTR). In precedenza, tutti i partner di integrazione dovevano essereAWSPartner di livello selezionato.	29 aprile 2021
novità`FindingProviderFields` oggetto in ASFF	Sono state aggiornate le informazioni sulla mappatura dei risultati su ASFF. Per`Confidence`, `Criticality`, `RelatedFindings`, `SeverityeTypes`, 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	QuestoGuida all'integrazione dei partnerfornisceAWSpartner con informazioni su come stabilire un'integrazione conAWS 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.