パートナー統合ガイド

AWS Security Hub

AWS Security Hub: パートナー統合ガイド

Table of Contents

サードパーティとの統合の概要AWS Security Hub

このガイドは、AWSパートナーネットワーク (APN) との統合を作成したいパートナーAWS Security Hub。

APN パートナーは、次の 1 つ以上の方法でSecurity Hub と統合できます。

- 検出結果をSecurity Hub に送信する
- Security Hub から検出結果を使用する
- 両方とも、Security Hub に調査結果を送信し、結果を使用します。
- Security Hub をマネージドセキュリティサービスプロバイダー (MSSP) オファリングの中心として使用する
- と相談AWSSecurity Hub の展開と使用方法に関するお客様

このオンボーディングガイドでは、主に Security Hub に検出結果を送信するパートナーについて説明します。

トピック

と統合する理由AWS Security Hub?

AWS Security HubSecurity Hub アカウントにおける高優先度のセキュリティアラートとセキュリティステータスを包括的に確認できます。Security Hub を使用すると、パートナーのようなパートナーが Security Hub にセキュリティ結果を送信して、生成されたセキュリティ結果に関する洞察を顧客に提供できます。

Security Hub との統合は、次の方法で価値を高めることができます。

- Security Hub 統合を要求した顧客を満足させる
- 顧客に対する単一のビューを提供します。AWSSecurity Hub

- 新しいお客様が、特定のタイプのセキュリティイベントに関連する調査結果を提供するパートナーを探すときに、ソリューションを発見できるようにする

Security Hub との統合を構築する前に、統合の理由を確認してください。お客様が製品と Security Hub の統合を希望する場合は、統合が成功する可能性が高くなります。マーケティング上の理由から、または新規顧客を獲得するためだけに統合を構築できます。ただし、現在の顧客からの入力なしで統合を構築し、顧客のニーズを考慮しない場合、統合によって期待される結果が得られない可能性があります。

検出結果をに送信する準備AWS Security Hub

APN パートナーは、Security Hub チームがあなたを検索プロバイダーとして許可するまで、顧客の情報をSecurity Hub に送信することはできません。検出プロバイダーとして有効にするには、以下のオンボーディングステップを完了する必要があります。そうすることで、お客様とお客様にとってポジティブなエクスペリエンスが保証されます。

オンボーディングの手順を完了するときは、「」のガイドラインに従ってください。the section called “調査結果の作成と更新に関する教訓”,the section called “ASFF マッピングのガイドライン”, およびthe section called “を使用するガイドライン`BatchImportFindings`API”。

1. セキュリティ調査結果をAWSSecurity Finding 形式 (ASFF)。
2. 統合アーキテクチャを構築して、結果を正しいリージョナルSecurity Hub エンドポイントにプッシュします。これを行うには、自分の調査結果を送信するかどうかを定義します。AWSアカウント、または顧客のアカウント内から。
3. 顧客に商品を自分のアカウントに登録してもらいます。これを行うには、コンソールまたは`EnableImportFindingsForProduct`API オペレーション。「」を参照してください。製品統合の管理のAWS Security Hubユーザーガイド。

   また、それらの製品を購読することもできます。これを行うには、クロスアカウントロールを使用して`EnableImportFindingsForProduct`お客様に代わって API オペレーション。

   この手順では、そのアカウントのその製品からの結果を受け入れるために必要なリソースポリシーを設定します。

次のブログ記事では、Security Hub との既存のパートナー統合について説明します。

- クラウドカストディアンとの統合を発表AWS Security Hub

- を使用するAWS FargateとProwlerがセキュリティ構成に関する調査結果を送るAWSSecurity Hub へのサービス
- インポート方法AWS ConfigSecurity Hub での検出結果としてのルール評価

からの調査結果を受け取る準備AWS Security Hub

調査結果を受け取るにはAWS Security Hubでは、次のいずれかのオプションを使用します。

- 顧客にすべての調査結果を自動的に送信してもらうCloudWatch[Events (イベント)] 。顧客は特定のものを作成できるCloudWatchSIEM や S3 バケットなどの特定のターゲットに結果を送信するためのイベントルール。
- Security Hub コンソールから特定の結果または調査結果のグループを選択し、それらに対してアクションを実行してもらいます。

たとえば、顧客は調査結果をSIEM、チケットシステム、チャットプラットフォーム、または修復ワークフローに送信できます。これは、お客様が Security Hub 内で実行するアラートのトリアージワークフローの一部です。

これらはカスタムアクションと呼ばれます。ユーザーがカスタムアクションを実行すると、CloudWatchこれらの特定の調査結果に対してイベントが作成されます。パートナーとして、この機能を活用して構築できます。CloudWatch顧客がカスタムアクションの一部として使用するイベントルールまたはターゲット。この機能は、特定のタイプまたはクラスのすべての結果を自動的に送信するわけではないことに注意してください。CloudWatch[Events (イベント)] 。この機能は、ユーザーが特定の結果に対してアクションを実行するためのものです。

以下のブログ記事では、Security Hub と Security Hub との統合を使用するソリューションの概要について説明します。CloudWatchカスタムアクションのイベント。

- 統合方法AWS Security HubでのカスタムアクションPagerDuty
- でカスタムアクションを有効にする方法AWS Security Hub
- インポート方法AWS ConfigSecurity Hub での検出結果としてのルール評価

について学ぶリソースAWS Security Hub

次の資料は、よりよく理解するのに役立ちますAWS Security Hubソリューションとその方法AWS顧客はサービスを利用することができます。

- についてAWS Security Hubビデオ
- Security Hub ユーザーガイド
- Security Hub API 参照
- オンボーディングウェビナー

また、次のいずれかでSecurity Hub を有効にすることをお勧めします。AWSアカウントを使用して、サービスを実践的に体験できます。

パートナーの前提条件

との統合を開始する前にAWS Security Hubを満たすには、次の条件のうちの1つを満たす必要があります。

- 君はAWSティアパートナー以上を選択します。
- あなたは参加しましたAWSISV パートナーパスで、Security Hub の統合に使用する製品がAWS基礎技術レビュー (FTR)。その後、製品に「レビュー済み」が付与されます。AWS「バッジ。

また、との相互機密保持契約を締結する必要があります。AWS。

統合のユースケースと必要な権限

AWS Security Hub許可するAWSAPN パートナーからの調査結果を受け取るお客様。パートナーの製品は、お客様の内部または外部で動作する場合があります。AWSアカウント. 顧客のアカウントの権限設定は、パートナー製品が使用するモデルによって異なります。

Security Hub では、お客様のアカウントに調査結果を送信できるパートナーが常に制御されます。お客様は、パートナーからの権限をいつでも取り消すことができます。

パートナーが自分のアカウントにセキュリティ結果を送信できるようにするには、まず Security Hub でパートナー製品をサブスクライブします。サブスクリプションステップは、以下に示すすべてのユースケースに必要です。カスタマーが Product Integration を管理する方法の詳細については、「」を参照してください。製品統合の管理のAWS Security Hubユーザーガイド。

お客様がパートナー製品をサブスクライブすると、Security Hub は自動的に管理リソースポリシーを作成します。このポリシーでは、パートナー製品にBatchImportFindings顧客のアカウントの Security Hub に検出結果を送信する API オペレーション。

Security Hub と統合するパートナー製品の一般的なケースを次に示します。この情報には、各ユースケースに必要な追加の権限が含まれています。

パートナーホスト:パートナーアカウントから送信された調査結果

このユースケースは、自社で製品をホストしているパートナーを対象としています。AWSアカウント. のセキュリティ調査結果を送信するにはAWSお客様、パートナーはBatchImportFindingsパートナー製品アカウントからの API オペレーション。

このユースケースでは、カスタマーアカウントは、顧客がパートナー製品をサブスクライブするときに確立される権限のみを必要とします。

パートナーアカウントで、を呼び出す IAM プリンシパルBatchImportFindingsAPI オペレーションには、プリンシパルが呼び出すことを許可する IAM ポリシーが必要ですBatchImportFindings。

パートナー製品が Security Hub でお客様に調査結果を送信できるようにするには、次の 2 段階のプロセスです。

1. 顧客は Security Hub でパートナー製品のサブスクリプションを作成します。

2. Security Hub は、お客様の確認とともに正しい管理リソースポリシーを生成します。

お客様のアカウントに関連するセキュリティ結果を送信するために、パートナー製品は独自の認証情報を使用して、BatchImportFindingsAPI オペレーション。

次に、パートナーアカウントのプリンシパルに必要なSecurity Hub アクセス権限を付与する IAM ポリシーの例を示します。

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

パートナーホスト:カスタマーアカウントから送信された調査結果

このユースケースは、自社で製品をホストしているパートナーを対象としています。AWSアカウント。ただし、クロスアカウントロールを使用して顧客のアカウントにアクセスします。彼らはBatchImportFindingsカスタマーアカウントからの API オペレーション。

このユースケースでは、BatchImportFindingsAPI オペレーションの場合、パートナーアカウントは、お客様のアカウントでカスタマー管理の IAM ロールを引き受けます。

この電話は顧客のアカウントから行われます。したがって、マネージリソースポリシーでは、パートナー製品のアカウントの製品 ARN をコールで使用できるようにする必要があります。Security Hub 管理リソースポリシーは、パートナー製品アカウントとパートナー製品 ARN のアクセス許可を付与します。製品 ARN は、プロバイダーとしてのパートナーの一意の識別子です。コールはパートナー製品アカウントからのものではないため、お客様は、パートナー製品が Security Hub に結果を送信するための許可を明示的に付与する必要があります。

パートナーアカウントとカスタマーアカウント間のクロスアカウントロールのベストプラクティスは、パートナーが提供する外部識別子を使用することです。この外部識別子は、顧客のアカウント

のクロスアカウントポリシー定義の一部です。パートナーは、ロールを引き受けるときに識別子を提供する必要があります。外部識別子は、付与時に追加のセキュリティレイヤーを追加します。AWS パートナーへのアカウントアクセス。一意の識別子は、パートナーが正しいカスタマーアカウントを使用することを保証します。

パートナー製品が Security Hub でクロスアカウントロールを使用して顧客に調査結果を送信できるようにするには、次の 4 つの手順を実行します。

1. 顧客、または顧客に代わって業務を行うクロスアカウントロールを使用しているパートナーは、Security Hub で製品のサブスクリプションを開始します。
2. Security Hub は、お客様の確認とともに正しい管理リソースポリシーを生成します。
3. カスタマーは、手動で、またはを使用してクロスアカウントロールを設定します。AWS CloudFormation。クロスアカウントロールの詳細については、「」を参照してください。へのアクセス権を付与するAWS第三者が所有するアカウントのIAM ユーザーガイド。
4. 製品には、顧客の役割と外部 ID が安全に保存されます。

次に、検出結果を Security Hub に送信します。

1. この製品は、AWS Security Token Service(AWS STS) をクリックしてカスタマーロールを引き受けます。
2. この製品は、`BatchImportFindings`引き受けたロールの一時的な認証情報を使用した Security Hub での API 操作。

パートナーのクロスアカウントロールに必要なSecurity Hub アクセス許可を付与する IAM ポリシーの例を以下に示します。

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

-Resourceポリシーのセクションは、特定の製品サブスクリプションを識別します。これにより、パートナーは、顧客が購読しているパートナー製品の調査結果のみを送信できます。

カスタマーホスト:カスタマーアカウントから送信された調査結果

このユースケースは、お客様のに展開されている製品を持つパートナーを対象としています。AWS アカウント. -BatchImportFindingsAPI は、顧客のアカウントで実行されるソリューションから呼び出されます。

このユースケースでは、パートナー製品にBatchImportFindingsアピ。この権限の付与方法は、パートナーソリューションと、顧客のアカウントでの構成方法によって異なります。

このアプローチの例は、お客様のアカウントの EC2 インスタンスで実行されるパートナー製品です。この EC2 インスタンスには、そのインスタンスにBatchImportFindingsAPI オペレーション。これにより、EC2 インスタンスはお客様のアカウントにセキュリティ調査結果を送信できます。

このユースケースは、顧客が所有する製品の調査結果を自分のアカウントにロードするシナリオと機能的に等価です。

お客様は、パートナー製品が Security Hub でお客様のアカウントから顧客に結果を送信できるようにします。

1. 顧客は、パートナー製品を自分のパートナーにデプロイします。AWSアカウントを手動で使用するAWS CloudFormation、または別のデプロイメントツールです。
2. お客様は、パートナー製品が Security Hub に結果を送信する際に使用するのに必要なIAM ポリシーを定義します。
3. お客様は、EC2 インスタンス、コンテナ、Lambda 関数など、パートナー製品の必要なコンポーネントにポリシーをアタッチします。

これで、検出結果を Security Hub に送信できます。

1. パートナー製品では、AWSSDK またはAWS CLIはを呼び出します。BatchImportFindingsSecurity Hub での API オペレーション。ポリシーが添付されている顧客のアカウント内のコンポーネントから電話をかけます。
2. API 呼び出し中に、必要な一時的な認証情報が生成され、BatchImportFindings成功するために呼び出します。

以下は、カスタマーアカウントのパートナー製品に必要なSecurity Hub アクセス権限を付与する IAM ポリシーの例です。

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

パートナーオンボーディングプロセス

パートナーとして、オンボーディングプロセスの一環として、いくつかのハイレベルなステップを完了することが期待できます。セキュリティ調査結果をに送信するには、次の手順を完了する必要があります。AWS Security Hub。

1. APN パートナーチームまたはSecurity Hub チームとの契約を開始し、Security Hub のパートナーになることに興味を表明します。Security Hub 通信チャネルに追加する電子メールアドレスを特定します。
2. AWSSecurity Hub パートナーのオンボーディング資料を提供します。
3. Security Hub パートナーの Slack チャンネルに招待され、統合に関する質問をすることができます。
4. APN パートナー連絡先に、レビュー用のドラフト製品統合マニフェストを提供してください。

   製品統合マニフェストには、との統合のためのパートナー製品の Amazon リソースネーム (ARN) を作成するために使用される情報が含まれています。AWS Security Hub。

   Security Hub コンソールの [パートナープロバイダ] ページに表示される情報を Security Hub チームに提供します。また、Security Hub インサイトライブラリに追加する統合に関連する新しいマネージドインサイトの提案にも使用されます。

   この製品統合マニフェストの初期バージョンには、完全な詳細がある必要はありません。ただし、少なくともユースケースとデータセット情報が含まれている必要があります。

   マニフェストおよび必要な情報の詳細については、「」を参照してください。製品統合マニフェスト。
5. Security Hub チームは、製品の製品 ARN を提供します。ARN を使用して、検出結果を Security Hub に送信します。
6. Security Hub に検出結果を送信、または Security Hub から検出結果を受信する統合を作成します。

   調査結果を ASFF にマッピングする

   結果を Security Hub に送信するには、調査結果をAWSSecurity Finding 形式 (ASFF)。

   ASFF は、間で共有できる結果について一貫した説明を提供します。AWSセキュリティサービス、パートナー、およびカスタマーセキュリティシステム。これにより、統合作業が軽減され、共通言語が奨励され、実装者にブループリントが提供されます。

ASFF は、調査結果の送信に使用するために必要なワイヤプロトコル形式です。AWS Security Hub。調査結果は、ASFF JSON スキーマおよび RFC-7493 I-JSON メッセージ形式に準拠した JSON ドキュメントとして表されます。ASFF スキーマの詳細については、を参照してください。AWSSecurity Finding 形式のAWS Security Hubユーザーガイド。

「the section called “ASFF マッピングのガイドライン”」を参照してください。

統合の構築とテスト

統合のすべてのテストは、AWS所有するアカウント。そうすることで、Security Hub で結果がどのように表示されるかを完全に把握できます。また、セキュリティ調査結果に関するカスタマーエクスペリエンスの理解にも役立ちます。

You use the `BatchImportFindings`Security Hub に新しい結果および更新された結果を送信する API オペレーション。

Security Hub 統合の構築を通じて、AWSでは、APN パートナーの連絡先にインテグレーションの進捗状況を通知しておくことをお勧めします。APN パートナーの連絡先に、統合に関する質問について問い合わせることもできます。

「the section called “を使用するガイドライン`BatchImportFindings`API”」を参照してください。

7. Security Hub 製品チームへの統合を実証します。この統合は、Security Hub チームが所有するアカウントを使用してデモンストレーションする必要があります。

   統合に慣れていれば、Security Hub チームはあなたをプロバイダーとして挙げるよう前進することを承認します。
8. あなたが提供するAWSレビュー用の最終マニフェスト付き。
9. Security Hub チームは、Security Hub コンソールでプロバイダー統合を作成します。その後、お客様は統合を検出して有効にできます。
10. (オプション) Security Hub 統合を促進するために、追加のマーケティング活動に従事します。「G.o-to-marketアクティビティ」を参照してください。

    少なくとも Security Hub では、次のアセットを提供することをお勧めします。
    - ワーキングインテグレーションのデモビデオ (最大で3分)。動画はマーケティング目的で使用され、AWS YouTubeChannel
    - Security Hub の最初のコールスライドデッキに追加する 1 スライドアーキテクチャ図。

G.o-to-marketアクティビティ

パートナーは、オプションのマーケティング活動に参加して、パートナーの説明と宣伝に役立てることもできます。AWS Security Hubの統合。

Security Hub に関連する独自のマーケティングコンテンツを作成する場合は、コンテンツをリリースする前に、レビューおよび承認のために APN パートナーマネージャーにドラフトを送信してください。これにより、全員がメッセージングにアラインメントされます。

AWSパートナーネットワーク (APN) パートナーは、APN パートナーマーケティングセントラルおよび市場開発ファンド (MDF) プログラムを使用して、キャンペーンを作成し、資金調達支援を受けることができます。これらのプログラムの詳細については、パートナーマネージャーにお問い合わせください。

[Security Hub パートナー] ページへのエントリ

Security Hub パートナーとして承認されると、ソリューションをAWS Security Hubパートナーページ。

このページのリストを表示するには、APN パートナー連絡先に次の詳細を提供してください。これは、パートナー開発マネージャー (PDM)、パートナーソリューションアーキテクト (PSA)、または宛てにメールを送信できます。<securityhub-pms@amazon.com>。

- ソリューション、Security Hub との統合、および Security Hub との統合によってお客様に提供される価値についての簡単な説明。この説明は、スペースも含めて 700 文字に制限されています。
- ソリューションを説明するページへの URL。このサイトは、AWS統合、具体的には Security Hub の統合。これは、カスタマーエクスペリエンスと、統合を使用するときに顧客が受け取る価値に重点を置く必要があります。
- 600 x 300 ピクセルのロゴの高解像度コピー。このロゴの要件の詳細については、を参照してください。the section called “パートナーページのロゴ”。

プレスリリース

承認済みパートナーとして、必要に応じて Web サイトおよび広報チャネルでプレスリリースを公開できます。プレスリリースは以下によって承認されなければなりませんAWS。

プレスリリースを公開する前に、AWSAPN パートナーマーケティング、Security Hub リーダーシップ、およびAWS外部セキュリティサービス (ESS)。プレスリリースには、ESSの副社長の見積もり提案を含めることができます。

このプロセスを開始するには、PDM で作業します。プレスリリースを確認するために、10 営業日のサービスレベルアグリーメント (SLA) があります。

AWSパートナーネットワーク (APN) ブログ

また、作成したブログエントリを APN ブログに投稿するのにも役立ちます。ブログエントリは、顧客のストーリーとユースケースに焦点を当てる必要があります。統合ローンチパートナーであることだけに位置づけることはできません。

興味がある場合は、PDM または PSA に連絡してプロセスを開始してください。APN ブログは、最終承認と公開に 8 週間以上かかることがあります。

APN ブログについて知っておくべき重要なこと

ブログ投稿を作成する場合、次の点に注意してください。

ブログ記事には何が入っていますか？

パートナーの投稿は教育的であり、関連するトピックに関する深い専門知識を提供する必要があります。AWSお客様。

理想的な長さは1,500語以下です。読者は、何が可能なのかを教える、深く教育的なコンテンツを大切にしています。AWS。

コンテンツは APN ブログのオリジナルである必要があります。既存のブログ投稿やホワイトペーパーなどのソースからのコンテンツを転用しないでください。

APN ブログへの投稿には他にどのような制限がありますか？

APN ブログに投稿できるのは、アドバンストティアパートナーまたはプレミアティアパートナーのみです。サービスデリバリーなどの APN プログラム指定を持つセレクトパートナーには例外があります。

各パートナーは年間3回の投稿に制限されています。数万のAPNパートナーを抱え、AWSその報道において公平でなければならない。

各投稿には、ソリューションまたはユースケースを検証できるテクニカルスポンサーが必要です。

投稿される前にブログ投稿を編集するにはどれくらいの時間がかかりますか?

ブログ投稿の最初のフルレングスのドラフトを提出した後、編集には 4 週間から 6 週間かかります。

APN ブログを書くのはなぜですか？

APN ブログ投稿には、次の利点があります。

- 信頼性— APN パートナーの場合、ストーリーが公開されているAWS世界中の顧客に影響を与えることができます。
- 可視性— APN ブログは、最も読まれたブログの 1 つですAWS2019年のページビュー数は179万件で、影響を受けたトラフィックを含む。
- Business— APN パートナー投稿には、APN カスタマーエンゲージメント (ACE) プログラムを通じてリードを生成できる接続ボタンがあります。

どのタイプのコンテンツが最適ですか？

次のタイプのコンテンツは、APN ブログ投稿に最適です。

- テクニカルコンテンツは、最も人気のあるタイプのストーリーです。これには、ソリューションのスポットライトとハウツー情報が含まれます。75% 以上の読者がこの技術コンテンツを見ています。
- お客様は、何かがどのように機能するかを示す200レベル以上のストーリーを大切にしています。AWSまたは、APN パートナーがお客様のビジネス上の問題を解決した方法について説明します。
- 技術専門家または主題の専門家によって書かれた投稿は、これまでで最高のパフォーマンスを発揮します。

スリックシートまたはマーケティングシート

Slick Sheet は、製品、統合アーキテクチャ、共同顧客のユースケースを概説する 1 ページのドキュメントです。

統合用の滑らかなシートを作成する場合は、コピーを Security Hub チームに送信します。パートナーページに追加します。

ホワイトペーパーまたは電子ブック

製品、統合アーキテクチャ、共同のお客様のユースケースを説明するホワイトペーパーまたは電子ブックを作成する場合は、Security Hub チームにコピーを送信してください。Security Hub パートナーページに追加します。

ウェビナー

統合に関するウェビナーを実施する場合は、Webセミナーの記録を Security Hub チームに送信してください。チームはパートナーページからリンクします。

チームは、Webセミナーに参加するためのSecurity Hub 主題の専門家を提供することもできます。

デモビデオ

マーケティングの目的で、作業統合のデモビデオを作成できます。このようなビデオをビデオプラットフォームアカウントに投稿すると、Security Hub チームはパートナーページからリンクします。

製品統合マニフェスト

すべての AWS Security Hub 統合パートナーは、提案された統合に必要な詳細を提供する製品統合マニフェストを完了する必要があります。

Security Hub チームはこの情報をいくつかの方法で使用します。

- ウェブサイトリスティングを作成するには
- Security Hub コンソールの製品カードを作成するには
- 製品チームにユースケースを通知するには。

提案された統合の品質および提供された情報を評価するために、Security Hub チームは the section called “製品の準備チェックリスト” を使用します。このチェックリストは、統合を始める準備ができているかどうかを決定します。

提供するすべての技術情報は、ドキュメントにも反映されなければなりません。

製品統合マニフェストの PDF 版は、AWS Security Hub パートナーページのリソースセクションからダウンロードできます。中国 (北京) および中国 (寧夏) リージョンで、パートナーページは使用できません。

内容

- ホットライン
- ハートビート結果
- AWS Security Hub コンソール情報
  - 会社情報
  - 製品情報

ユースケースとマーケティング情報

次のユースケースは、さまざまな目的の AWS Security Hub の設定に役立ちます。

結果プロバイダーとコンシューマーユースケース

独立系ソフトウェアベンダー (ISV) に必要です。

AWS Security Hub との統合に関するユースケースを説明するには、以下の質問に回答します。結果を送受信する予定がない場合は、このセクションに注意し、次のセクションを完了します。

次の情報は、ドキュメントに反映される必要があります。

- 結果を送る、結果を受け取る、またはその両方ですか?
- 結果を送る予定がある場合、どのようなタイプの結果を送りますか? すべての結果または特定の結果のサブセットを送信しますか?
- 結果を受け取る予定がある場合、それらの結果をどうしますか? どのようなタイプの結果を受け取りますか? たとえば、すべての結果、特定のタイプの結果、またはお客様が選択した特定の結果のみを受け取りますか?
- 結果を更新する予定はありますか? その場合、どのフィールドを更新しますか? Security Hub では、常に新しい結果を作成するのではなく、結果を更新することをお勧めします。既存の結果を更新すると、お客様の結果ノイズを減らすことができます。

  結果を更新するには、すでに送信した結果に割り当てられている結果 ID の結果を送信します。

ユースケースとデータセットに関するフィードバックを早期に得るには、APN パートナーまたは Security Hub チームにお問い合わせください。

コンサルティングパートナー (CP) のユースケース

Security Hub コンサルティングパートナーの場合に必要です。

Security Hub での作業に 2 つのお客様ユースケースを提供します。これらはプライベートのユースケースでもかまいません。Security Hub チームはどこにも宣伝しません。以下のいずれかまたは両方のアクションを説明する必要があります。

- お客様が Security Hub をブートストラップするのをどのように支援していますか? たとえば、お客様がプロフェッショナルサービス、Terraform モジュール、または AWS CloudFormation テンプレートを使用するのを支援しましたか?
- お客様が Security Hub の運用し、拡張するのをどのように支援していますか? たとえば、応答または修復テンプレートを提供したり、カスタム統合を構築したり、ビジネスインテリジェンスツールを使用してエグゼクティブダッシュボードを設定したりしましたか?

データセット

Security Hub に結果を送信する場合に必要です。

Security Hub に送信する結果については、次の情報を提供します。

- JSON や XML などのネイティブ形式での結果
- 結果をどのように AWS Security Finding 形式 (ASFF) に変換するかの一例

統合をSupportするために ASFF の更新が必要かどうかを Security Hub チームに知らせてください。

アーキテクチャ

Security Hub との結果の送受信に必要です。

Security Hub との統合方法を説明します。この情報は、ドキュメントにも反映する必要があります。

アーキテクチャ図を提供する必要があります。アーキテクチャ図を準備する場合は、次を考慮します。

- どの AWS サービス、オペレーティングシステムエージェントなどを使用しますか?
- Security Hub に結果を送信する場合、お客様 AWS アカウントまたは自分の AWS アカウントから結果を送信しますか?
- 結果を受け取った場合、 CloudWatch Events統合をどのように使用しますか?
- 結果を ASFF にどのように変換しますか?
- どのように結果をバッチ処理し、結果状態を追跡し、スロットリング制限を回避しますか?

構成

Security Hub との結果の送受信に必要です。

Security Hub との統合をお客様がどのように設定するかを説明します。

少なくとも、AWS CloudFormation テンプレートまたはコードテンプレートなどの同様のインフラストラクチャを使用する必要があります。一部のパートナーは、ワンクリック統合をSupportするユーザーインターフェイスを提供しています。

設定にかかる時間は 15 分以内である必要があります。また、製品ドキュメントでは、統合の設定ガイダンスを提供する必要があります。

1 日あたり、お客様あたりの平均結果

Security Hub に結果を送信する場合に必要です。

お客様ベース全体で Security Hub に送信する予定の結果更新数 (平均と最大) は、1 か月あたりいくつありますか? 桁の推定値は許容されます。

レイテンシー

Security Hub に結果を送信する場合に必要です。

結果をバッチ処理して Security Hub に送信するのはどれくらいの速さですか? つまり、製品内で結果が作成されてから Security Hub に送信されるまでのレイテンシーはどれくらいですか?

この情報は、統合のために製品ドキュメントに反映される必要があります。お客様から多く寄せられる質問です。

会社と製品の説明

Security Hub とのすべての統合に必要です。

Security Hub 統合の性質に特に重点を置いて、会社と製品について簡単に説明します。これを Security Hub パートナーページで使用します。

複数の製品を Security Hub に統合する場合は、製品ごとに個別の説明を提供できますが、パートナーページの 1 つのエントリにまとめられます。

説明はスペースを含め、700 文字以下にしてください。

パートナーウェブサイトのアセット

Security Hub とのすべての統合に必要です。

少なくとも、Security Hub パートナーページの [詳細はこちら] ハイパーリンクで使用する URL を提供する必要があります。これは、製品と Security Hub の統合を説明するマーケティングランディングページである必要があります。

複数の製品を Security Hub に統合する場合は、1 つのランディングページを作成できます。Security Hub は、このランディングページに設定手順へのリンクを含めることをお勧めしています。

ブログ、ウェビナー、デモビデオ、ホワイトペーパーなどの他のリソースへのリンクを提供することもできます。Security Hub は、パートナーページからもリンクされます。

パートナーページのロゴ

すべての Security Hub 統合に必要です。

Security Hub パートナーページに表示するロゴの URL を指定します。ロゴは次の基準を満たしている必要があります。

- サイズ: 600 x 300 ピクセル
- 切り取り: パディングなしでタイト
- 背景: 透過
- フォーマット: PNG

Security Hub コンソールのロゴ

すべての統合に必要です。

Security Hub コンソールに表示するライトモードおよびダークモードのロゴの URL を提供します。

ロゴは次の基準を満たしている必要があります。

- 形式: SVG
- サイズ: 175 x 40 ピクセル。大きい場合、イメージはその比率を使用する必要があります。
- 切り取り: パディングなしでタイト

- 背景: 透過

小さいロゴの詳細なガイドラインについては、the section called “コンソールロゴのガイドライン” を参照してください。

結果タイプ

Security Hub に結果を送信する場合に必要です。

使用する ASFF 形式の結果タイプと、それらがネイティブの結果タイプにどのように整列するかを説明した表を提供します。ASFF でのタイプの結果の詳細については、AWS Security Hub ユーザーガイドの「ASFF のタイプ分類基準」を参照してください。

この情報は製品ドキュメントにも記載することもお勧めします。

ホットライン

Security Hub とのすべての統合に必要です。

技術的なお問い合わせのメールアドレス、電話番号、またはポケットベル番号を提供します。Security Hub は、統合が機能しなくなった場合など、技術的な問題についてこのお問い合わせに連絡します。

また、重要度の高い技術的な問題については、24 時間 365 日のお問い合わせを提供します。

ハートビート結果

Security Hub に結果を送信する場合に推奨されます。

Security Hub との統合が機能していることを示す「ハートビート」結果を 5 分ごとに送信できますか?

可能であれば、結果タイプ `Heartbeat` を使用してそれを行います。

AWS Security Hub コンソール情報

以下の情報を含む JSON テキストを AWS Security Hub チームに提供します。Security Hub はこの情報を使用して、製品 ARN を作成し、コンソールにプロバイダーリストを表示し、提案されたマネージドインサイトを Security Hub インサイトライブラリに含めます。

会社情報

会社情報は、会社に関する情報を提供します。例を示します。

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

会社情報には以下のフィールドが含まれます。

フィールド	必要	説明
id	はい	会社の一意の識別子。会社識別子は、会社全体で一意である必要があります。 これは、name と同じまたは類似している可能性があります。 型: 文字列 最小長: 5 文字 最大長: 24 文字 使用できる文字: 小文字の英文字、数字、ハイフン 小文字で始める必要があります。数字または小文字で終わる必要があります。
name	はい	Security Hub コンソールに表示されるプロバイダーの会社の名前。 型: 文字列 最大長: 16 文字

フィールド	必要	説明
`description`	はい	Security Hub コンソールに表示されるプロバイダーの会社の説明。 型: 文字列 最大長: 200 文字

製品情報

このセクションでは、製品についての情報を提供します。例を示します。

```
{
    "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"
}
```

製品情報には以下の情報が含まれます。

フィールド	必要	説明
`IntegrationType`	はい	製品が Security Hub に結果を送信するか、Security Hub から結果を受信するか、結果を送受信するかを示します。 コンサルティングパートナーの場合は、このフィールドを空白のままにします。 タイプ: 文字列の配列

フィールド	必要	説明
		有効な値: `SEND_FINDINGS_TO_SECURITY_HUB` | `RECEIVE_FINDINGS_FROM_SECURITY_HUB`
`id`	はい	製品の一意の識別子。これらは、会社内で一意である必要があります。会社全体で一意である必要はありません。これは、`name` と同じか類似している可能性があります。 型: 文字列 最小長: 5 文字 最大長: 24 文字 使用できる文字: 小文字の英文字、数字、ハイフン 小文字で始める必要があります。数字または小文字で終わる必要があります。

フィールド	必要	説明
`regionsNotSupported`	はい	次の AWS リージョンのうち、Supportしないのはどれですか? つまり、Security Hub コンソールの [パートナー] ページで Security Hub がオプションとして表示されないリージョンはどれですか? 型: 文字列 リージョンコードのみを提供します。たとえば、`us-west-1` です。 リージョンのリストについては、の「リージョンのエンドポイント」を参照してくださいAWS 全般のリファレンス。 AWS GovCloud (US)のリージョンコードは`us-gov-west-1` (AWS GovCloud (米国西部)) と`us-gov-east-1` (AWS GovCloud (米国東部)) です。 中国地域の地域コードは `cn-north-1` (中国 (北京) の場合) と `cn-northwest-1` (中国 (寧夏回族自治区) の場合) です。

フィールド	必要	説明
`commercialAccountNumber`	はい	AWS リージョンの製品のプライマリ AWS アカウント番号。 Security Hub に結果を送信する場合、提供するアカウントは、結果の送信元に基づきます。 • あなたの AWS アカウントから。この場合、結果の送信に使用するアカウント番号を入力します。 • お客様の AWS アカウントから。この場合、Security Hub では、統合のテストに使用するプライマリアカウント番号を指定することをお勧めします。 理想的には、すべてのリージョンのすべての商品に同じアカウントを使用します。これが不可能な場合は、Security Hub チームにお問い合わせください。 Security Hub からのみ結果を受け取る場合、このアカウント番号は不要です。 型: 文字列

フィールド	必要	説明
govcloudAccountNumber	いいえ	AWS GovCloud (US) リージョンの製品のプライマリ AWS アカウント番号 (製品が AWS GovCloud (US) で利用可能な場合)。 Security Hub に結果を送信する場合、提供するアカウントは、結果の送信元に基づきます。 • あなたの AWS アカウントから。この場合、結果の送信に使用するアカウント番号を入力します。 • お客様の AWS アカウントから。この場合、Security Hub では、統合のテストに使用するプライマリアカウント番号を指定することをお勧めします。 理想的には、すべての AWS GovCloud (US) リージョン全体のすべての製品で同じアカウントを使用します。これが不可能な場合は、Security Hub チームにお問い合わせください。 Security Hub からのみ結果を受け取る場合、このアカウント番号は不要です。 型: 文字列

フィールド	必要	説明
chinaAccountNumber	いいえ	中国の製品のプライマリ AWS アカウント番号 (製品が中国リージョンで利用可能な場合)。 Security Hub に結果を送信する場合、提供するアカウントは、結果の送信元に基づきます。 • あなたの AWS アカウントから。この場合、結果の送信に使用するアカウント番号を入力します。 • お客様の AWS アカウントから。この場合、Security Hub では、製品統合のテストに使用するプライマリアカウント番号を指定することをお勧めします。 理想的には、中国リージョン全体のすべての商品に同じアカウントを使用します。これが不可能な場合は、Security Hub チームにお問い合わせください。 Security Hub からのみ結果を受け取る場合、これは中国リージョンで所有しているアカウントであればどれでもかまいません。 型: 文字列
name	はい	Security Hub コンソールに表示するプロバイダーの製品の名前。 型: 文字列 最大長: 24 文字

フィールド	必要	説明
`description`	はい	Security Hub コンソールに表示するプロバイダーの製品の説明。 型: 文字列 最大長: 200 文字
`importType`	はい	パートナーのリソースポリシーのタイプ。 パートナーオンボーディングプロセス中に、次のリソースポリシーのいずれか 1 つを指定するか、`NEITHER` を指定することができます。 • `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` で、製品 ARN にリストされているアカウントからの結果のみを Security Hub に送信できます。 • `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` で、結果を送信できるのは、自分をサブスクライブしたお客様のアカウントからのみです。 型: 文字列 有効な値: `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT` | `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT` | `NEITHER`

フィールド	必要	説明
category	はい	商品を定義するカテゴリー。選択したものは Security Hub コンソールに表示されます。 最大 3 つのカテゴリーを選択します。 カスタム選択は許可されていません。カテゴリーが見つからないと思われる場合は、Security Hub チームにお問い合わせください。 型: 配列 使用可能なカテゴリー: • API Firewall • Asset Management • AV Scanning and Sandboxing • Backup and Disaster Recovery • Breach and Attack Simulation • Bug Bounty Platform • Certificate Management • Cloud Access Security Broker • Cloud Security Posture Management • Configuration and Patch Management • Configuration Management Database (CMDB) • Consulting Partner • Container Security • Cyber Range • Data Access Management • Data Classification • Data Loss Prevention

フィールド	必要	説明
		• Data Masking and Tokenization • Database Activity Monitoring • DDoS Protection • Deception • Device Control • Dynamic Application Security Testing • Data Encryption • Email Gateway • Encrypted Search • Endpoint Detection and Response (EDR) • Endpoint Forensics • Forensics Toolkit • Fraud Detection • Governance, Risk, and Compliance (GRC) • Host-based Intrusion Detection (HIDs) • Human Resources Information System • Interactive Application Security Testing (IAST) • Instant Messaging • IoT Security • IT Security Training • IT Ticketing and Incident Management • Managed Security Service Provider (MSSP)

フィールド	必要	説明
		• 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	いいえ	製品 AWS Marketplace 送信先への URL。URL は Security Hub コンソールに表示されます。 型: 文字列 これは、AWS Marketplace URL である必要があります。 AWS Marketplace リストがない場合、このフィールドは空白のままにします。

フィールド	必要	説明
`configurationUrl`	はい	Security Hub との統合に関する製品ドキュメントへの URL。このコンテンツは、お客様が管理するウェブページでホストされます。GitHub 型: 文字列 ドキュメントには次の情報が含まれている必要があります。 • 設定手順 • AWS CloudFormation テンプレートへのリンク (必要な場合) • 統合のユースケースに関する情報 • レイテンシー • ASFF マッピング • 含まれる結果のタイプ • アーキテクチャ

ガイドラインとチェックリスト

あなたに必要な資料を準備するときAWS Security Hub統合の場合は、次のガイドラインを使用してください。

準備チェックリストは、Security Hub のお客様が Security Hub を利用できるようにする前に、統合の最終レビューを実行するために使用されます。

トピック

にロゴを表示する際のガイドラインAWS Security Hubコンソール

にロゴを表示するにはAWS Security Hubコンソールでは、次のガイドラインに従います。

ライトモードとダークモード

ロゴには、ライトモードとダークモードの両方のバージョンを指定する必要があります。

形式

SVG ファイル形式

[Background color]

Transparent

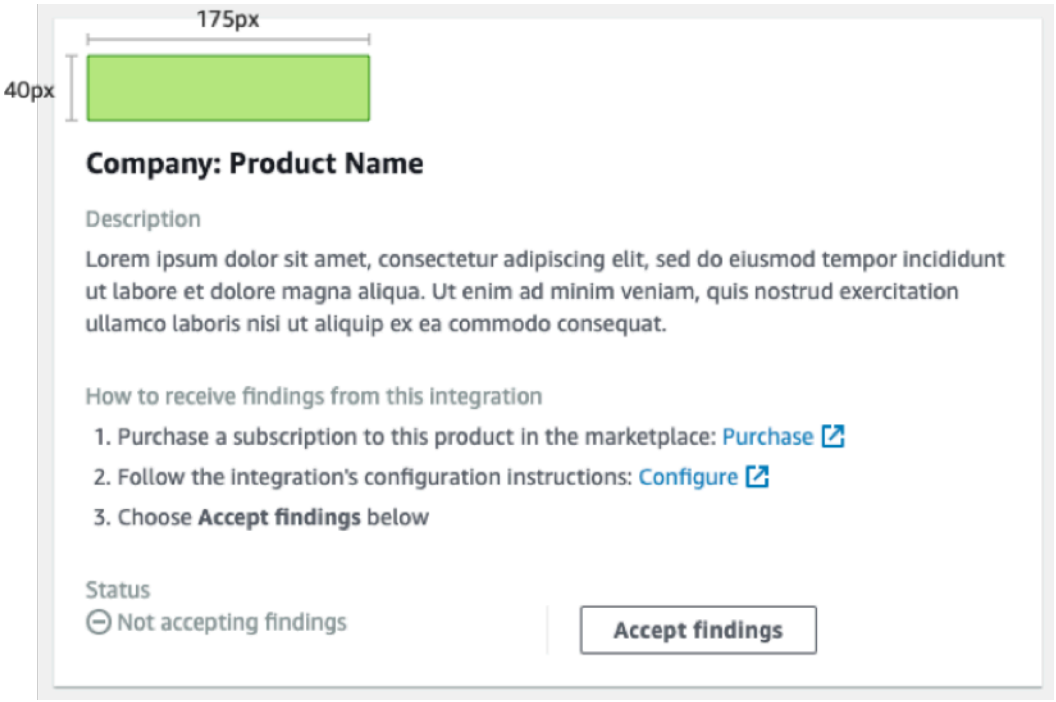
サイズ

理想的な比率は幅175ピクセル、高さ40ピクセルです。

最小の高さは40ピクセルです。

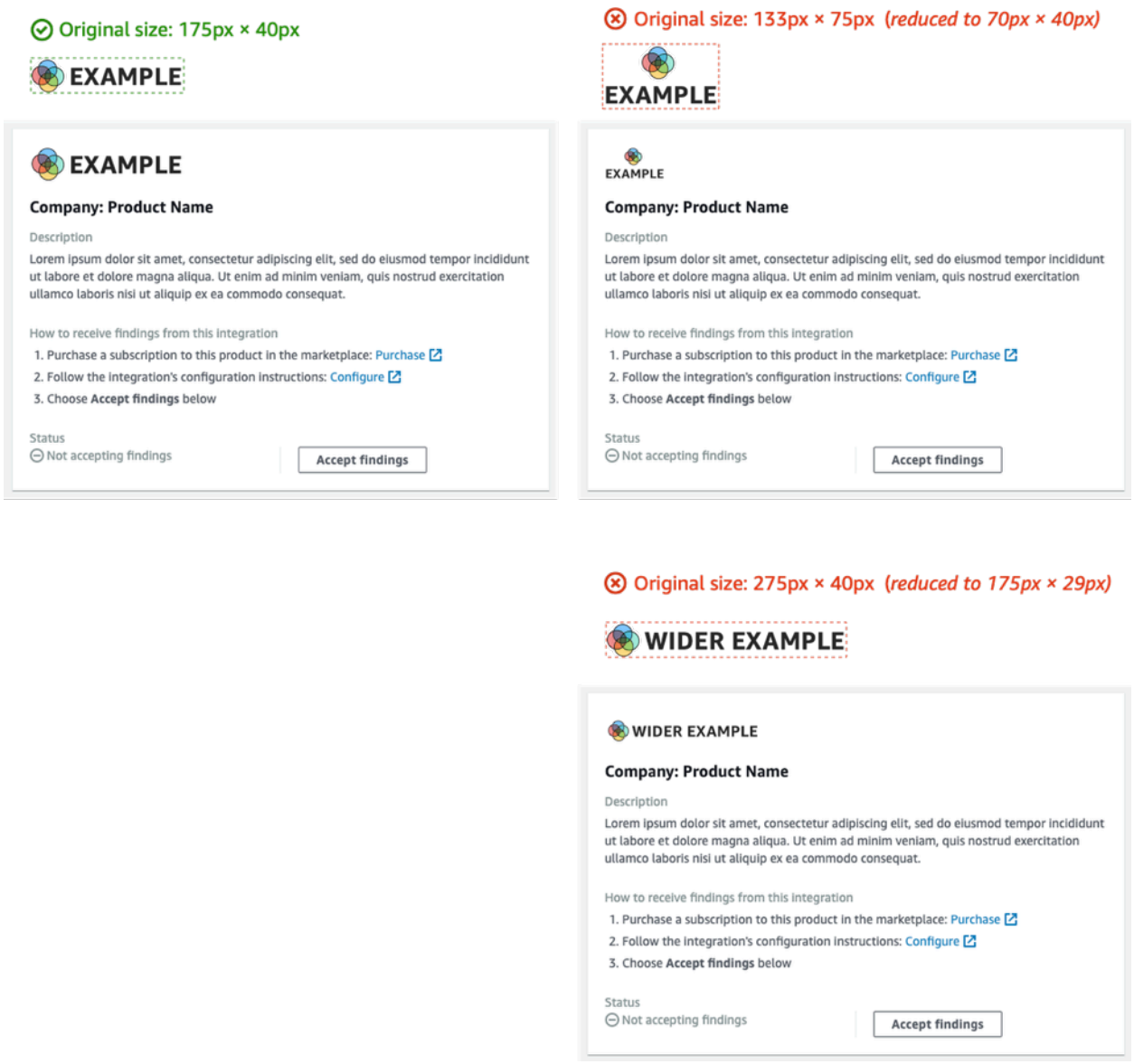
長方形の口ゴが最適です。

次の図は、Security Hub コンソールで理想的な口ゴがどのように表示されるかを示しています。



ロゴがこれらの寸法と一致しない場合、Security Hub はサイズを最大高さ 40 ピクセル、最大幅を 175 ピクセルに縮小します。これは、Security Hub コンソールでのロゴの表示方法に影響します。

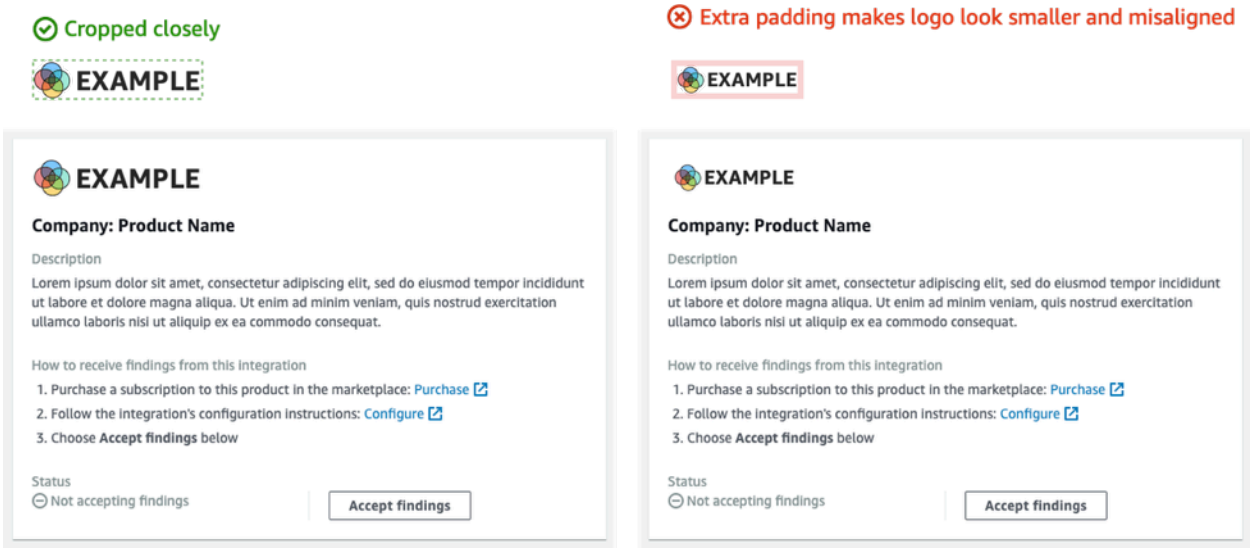
次の図は、理想的なサイズを使用したロゴの表示と、幅広または背の高いロゴを比較しています。



クロッピング

ロゴ画像をできるだけ近くに切り取ってください。余計なパディングは提供しないでください。

次の図は、密接に切り取られたロゴと、余分なパディングがあるロゴの違いを示しています。



調査結果の作成と更新に関する教訓

で結果を作成および更新する方法について説明します。AWS Security Hubでは、以下の教義を念頭に置いてください。

顧客が簡単にアクションを実行できるように、結果を特定します。

お客様は、対応と修復アクションを自動化して、調査結果を他の調査結果と相関させたいと考えています。これをサポートするには、結果には以下の特徴があります。

- 通常、単一のリソースまたはプライマリリソースを処理する必要があります。
- 彼らは単一の発見タイプを持つべきです。
- 彼らは単一のセキュリティイベントに対処する必要があります。

検索結果に複数のセキュリティイベントのデータが含まれている場合、顧客がその結果に対してアクションを実行することがより困難になります。

すべての検索フィールドをAWSSecurity Finding 形式 お客様が Security Hub を真実の源として信頼できるようにする。

お客様は、ネイティブ検索形式のすべてのフィールドが Security Hub ASFF にも表示されることを期待しています。

お客様は、すべてのデータが Security Hub バージョンの結果に存在することを望んでいます。データが欠落すると、セキュリティ情報の一元的なソースとして Security Hub への信頼が失われます。

調査結果の冗長性を最小限に抑えます。ボリュームを見つけることで顧客を圧倒しないでください。

Security Hub は、一般的なログ管理ツールではありません。アクション性の高い調査結果を Security Hub に送信し、お客様が他の結果に直接対応、修正、または関連づけることが可能。

結果にわずかな変更しかない場合は、新しい結果を作成するのではなく、結果を更新します。

重大度スコアやリソース識別子など、結果に大きな変更があった場合は、新しい結果を作成します。

たとえば、個々のポートスキャンの結果をリアルタイムで作成することは、あまり実用的ではありません。ポートスキャンは継続的に行われる可能性があるため、大量の調査結果を生成します。TORノードから MongoDB ポート上のポートスキャンの単一の検索で、最後のスキャン時間とスキャンカウントを更新するだけで、はるかに説得力があり、正確になります。

顧客が調査結果をカスタマイズして、より意味のあるものにできるようにしましょう。

お客様は、特定の検索フィールドを調整して、環境や要件により関連性の高いものにしたいと考えています。

たとえば、顧客は、取引先のタイプまたは検索結果が関連付けられているリソースのタイプに基づいて、メモ、タグを追加し、重大度スコアを調整できるようにしたいとします。

調査結果をにマッピングするためのガイドラインAWSSecurity Finding 形式

結果を ASFF にマッピングするには、次のガイドラインに従います。各 ASFF フィールドとオブジェクトの詳細については、を参照してください。AWSSecurity Finding 形式のAWS Security Hub ユーザーガイド。

識別情報

`SchemaVersion` は常に `2018-10-08` です。

`ProductArn`ARN はAWS Security Hub君に割り当てる。

`Id`は、Security Hub が結果のインデックスを作成するために使用する値です。他の調査結果が上書きされないように、結果識別子は一意である必要があります。結果を更新するには、同じ識別子を使用して結果を再送信します。

GeneratorIdと同じでもかまいませんIdまたは、Amazon などの論理の離散単位を指すこともできます。GuardDuty検出器 IDAWS Configレコーダー ID、または IAM アクセスアナライザー ID。

Title および Description

Title影響を受けるリソースに関する情報をいくつか含める必要があります。Titleは、スペースを含む 256 文字に制限されています。

より長い詳細情報をDescription。Descriptionは、スペースを含む 1024 文字に制限されています。説明に切り捨てを追加することを検討できます。例を示します。

```
"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.",
```

結果タイプ

検索タイプの情報をFindingProviderFields.Types。

Typesと一致するはずです。ASFF のタイプ分類。

必要に応じて、カスタム分類子 (3 番目の名前空間) を指定できます。

タイムスタンプ

ASFF 形式には、いくつかの異なるタイムスタンプが含まれています。

CreatedAt および UpdatedAt

提出する必要がありますCreatedAtそしてUpdatedAt電話するたびにBatchImportFindingsそれぞれの発見について。

値は Python 3.8 の ISO8601 形式と一致する必要があります。

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

FirstObservedAt および LastObservedAt

FirstObservedAtそしてLastObservedAtシステムが調査結果を観察したときと一致する必要があります。この情報を記録しない場合は、これらのタイムスタンプを送信する必要はありません。

値は Python 3.8 の ISO8601 形式と一致しています。

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

Severity

重大度情報は、FindingProviderFields.Severityオブジェクト。には以下のフィールドがあります。

Original

システムの重大度値。Originalは、使用するシステムに対応するために、任意の文字列にすることができます。

Label

検出の重大度を示す必須Security Hub インジケータ。指定できる値は次のとおりです。

- INFORMATIONAL— 問題は見つかりませんでした。
- LOW— この問題は単独で対処する必要はありません。
- MEDIUM— この問題は対処する必要がありますが、緊急ではありません。
- HIGH— この問題は優先事項として対処する必要があります。
- CRITICAL— さらなる被害を防ぐために、この問題は直ちに修正する必要があります。

準拠している所見は、常に持っている必要がありますLabelに設定します。INFORMATIONAL。の例INFORMATIONAL調査結果は、合格したセキュリティチェックの結果であり、AWS Firewall Manager修正された調査結果。

お客様は、セキュリティ運用チームに ToDo リストを提供するために、重要度で調査結果を並べ替えることがよくあります。検索の重大度をに設定するときは慎重に行ってくださいHIGHまたはCRITICAL。

統合ドキュメントには、マッピングの理論的根拠が含まれている必要があります。

Remediation

Remediationには 2 つの要素があります。これらの要素は、Security Hub コンソールで結合されます。

Remediation.Recommendation.Textに表示されます。修復検索の詳細のセクション。これは、の値にハイパーリンクされていますRemediation.Recommendation.Url。

現在、Security Hub 標準、IAM アクセスアナライザー、およびFirewall Manager からの結果のみに、結果の修正方法に関するドキュメントへのハイパーリンクが表示されます。

SourceUrl

使用のみSourceUrlその特定の結果のために、コンソールにディープリンク URL を提供できるかどうか。それ以外の場合は、マッピングから省略します。

Security Hub はこのフィールドからのハイパーリンクをサポートしていませんが、Security Hub コンソールで公開されます。

Malware, Network, Process, ThreatIntelIndicators

該当する場合は、Malware,Network,Process, またはThreatIntelIndicators。これらのオブジェクトはそれぞれ Security Hub コンソールで公開されます。これらのオブジェクトは、送信する結果のコンテキストで使用します。

たとえば、既知のコマンドおよびコントロールノードへのアウトバウンド接続を行うマルウェアを検出した場合は、EC2 インスタンスの詳細をで指定します。Resource.Details.AwsEc2Instance。関連するものを提供してくださいMalware,Network, およびThreatIntelIndicatorその EC2 インスタンスのオブジェクト。

Malware

Malwareは、最大 5 つのマルウェア情報の配列を受け入れるリストです。マルウェアエントリをリソースと発見に関連づけるようにします。

各エントリには以下のフィールドがあります。

Name

マルウェアの名前。値は 64 文字の文字列です。

Name検査済みの脅威インテリジェンスまたは研究者の情報源から入手する必要があります。

Path

マルウェアへのパス。値は、最大 512 文字の文字列です。Path次の場合を除き、Linux または Windows のシステムファイルパスにする必要があります。

- S3 バケットまたは EFS 共有内のオブジェクトを YARA ルールに対してスキャンすると、PathS3://または HTTPS オブジェクトパスです。
- Git リポジトリ内のファイルをスキャンすると、PathGit URL またはクローンのパスです。

State

マルウェアのステータス。指定できる値は次のとおりです。OBSERVED|REMOVAL_FAILED|REMOVED。

検索のタイトルと説明で、マルウェアで何が起こったかのコンテキストを提供していることを確認します。

たとえば、次のようになります。Malware.StateですREMOVEDの順にクリックすると、検索タイトルと説明に、パス上にあるマルウェアが製品によって削除されたことが反映されます。

もしMalware.StateですOBSERVEDの順にクリックすると、検索タイトルと説明に、パス上に存在するこのマルウェアが製品で検出されたことを反映する必要があります。

Type

マルウェアのタイプを示します。指定できる値は次のとおりです。ADWARE|BLENDED_THREAT|BOTNET_AGENT|COIN_MINER|EXPLOIT_KIT|KEYLOGGER|MACRO|POTE

に追加の値が必要な場合Type、Security Hub チームに連絡してください。

Network

Networkは 1 つのオブジェクトです。複数のネットワーク関連の詳細を追加することはできません。フィールドをマッピングする場合は、次のガイドラインに従います。

デスティネーションとソース情報

宛先と送信元は、TCP または VPC フローログ、または WAF ログを簡単にマッピングできます。あなたが攻撃に関する発見のためのネットワーク情報を記述しているとき、彼らは使用するのがより困難です.

通常、ソースは攻撃の発祥地ですが、以下に示すような他のソースがある可能性があります。ドキュメントでソースを説明し、検索のタイトルと説明にも説明する必要があります。

- EC2 インスタンスに対する DDoS 攻撃の場合、ソースは攻撃者ですが、実際の DDoS 攻撃では何百万ものホストが使用される可能性があります。宛先は EC2 インスタンスのパブリック IPv4 アドレスです。Directionは入っています。

- EC2 インスタンスから既知のコマンドおよびコントロールノードへの通信が観察されるマルウェアの場合、ソースは EC2 インスタンスの IPV4 アドレスです。デスティネーションは、コマンドおよびコントロールノードです。DirectionですOUT。また、MalwareそしてThreatIntelIndicators。

Protocol

Protocol特定のプロトコルを提供できる場合を除き、常にインターネット割り当て番号局 (IANA) の登録名にマッピングします。常にこれを使用し、ポート情報を提供してください。

Protocolは、送信元および宛先情報から独立しています。そうするのが理にかなっているときだけ提供してください。

Direction

Directionは、常に相対的であるAWSネットワーク境界。

- IN入ることを意味するAWS(VPC、サービス)。
- OUTそれは終了していることを意味し、AWSネットワーク境界。

Process

Processは 1 つのオブジェクトです。複数のプロセス関連の詳細を追加することはできません。フィールドをマッピングする場合は、次のガイドラインに従います。

Name

Nameは実行可能ファイルの名前と一致する必要があります。64 文字まで使用できます。

Path

Pathは、実行可能プロセスへのファイルシステムパスです。最大 512 文字まで使用できます。

Pid, **ParentPid**

PidそしてParentPidLinux プロセス識別子 (PID) または Windows イベント ID と一致する必要があります。区別するには、EC2 Amazon マシンイメージ (AMI) を使用して情報を提供します。お客様は、おそらく Windows と Linux を区別することができます。

タイムスタンプ**LaunchedAt**そして**TerminatedAt**)

この情報を確実に取得できず、ミリ秒単位で正確でない場合は、提供しないでください。

お客様がフォレンジック調査でタイムスタンプに依存している場合は、タイムスタンプがない方が間違ったタイムスタンプを持つよりも優れています。

ThreatIntelIndicators

ThreatIntelIndicators最大 5 個の脅威インテリジェンスオブジェクトの配列を受け入れます。

エントリごとに、Typeは、特定の脅威のコンテキストにあります。指定できる値は次のとおりです。DOMAIN|EMAIL_ADDRESS|HASH_MD5|HASH_SHA1|HASH_SHA256|HASH_SHA512|IPV4_ADDRESS|IPV6

ここでは、脅威インテリジェンスインジケータをマッピングする方法の例をいくつか紹介します。

- Cobalt Strikeに関連付けられていることがわかっているプロセスが見つかりました。これはから学んだFireEyeのブログ。

  Type を PROCESS に設定します。また、Processプロセスのオブジェクト。
- メールフィルタによって、既知の悪意のあるドメインから既知のハッシュ化されたパッケージを送信している人が見つかりました。

  2 つの作成ThreatIntelIndicatorオブジェクト。1つのオブジェクトは、DOMAIN。もう 1 つの場合はHASH_SHA1。
- ヤラルール (ロキ、フェンリル、Awss3VirusScan,BinaryAlert).

  2 つの作成ThreatIntelIndicatorオブジェクト。一つはマルウェア用です。もう 1 つの場合はHASH_SHA1。

Resources

を使用する場合Resourcesでは、可能な限り提供されているリソースタイプと詳細フィールドを使用します。Security Hub は常に ASFF に新しいリソースを追加しています。ASFF の変更の月次ログを受け取るには、<securityhub-partners@amazon.com>。

モデル化されたリソースタイプの詳細フィールドに情報を収められない場合は、残りの詳細をDetails.Other。

ASFF でモデル化されていないリソースについては、TypeにOther。詳細については、以下を使用します。Details.Other。

また、 を使用することもできますOther非リソースタイプAWS検出結果。

ProductFields

使用のみProductFieldsで別のキュレーションフィールドを使用できない場合Resourcesまたは次のような説明的なオブジェクトThreatIntelIndicators,Network, またはMalware。

あなたが使っている場合ProductFieldsでは、この決定には厳密な根拠を提供しなければならない。

コンプライアンス

使用のみCompliance調査結果が、コンプライアンスに関連している場合。

Security Hub の使用Complianceこれは、コントロールに基づいて生成する所見です。

Firewall Manager の使用Complianceその調査結果は、コンプライアンスに関連しているためです。

制限されているフィールド

これらのフィールドは、顧客が調査結果の調査を追跡できるようにするためのものです。

これらのフィールドまたはオブジェクトにはマップしないでください。

- Note
- UserDefinedFields
- VerificationState
- Workflow

これらのフィールドについては、内のフィールドにマップします。FindingProviderFieldsオブジェクト。最上位フィールドにはマップしないでください。

- Confidence— サービスに同様の機能がある場合、または結果が 100% 満たされている場合にのみ、信頼スコア (0 ~ 99) を含めてください。
- Criticality— 重要度スコア (0 ~ 99) は、結果に関連するリソースの重要性を表すことを目的としています。
- RelatedFindings：同じリソースまたは検索タイプに関連する調査結果を追跡できる場合にのみ、関連する結果を提供します。関連する結果を特定するには、Security Hub に既にある結果の検索 ID を参照する必要があります。

を使用するガイドライン**BatchImportFindings**API

を使用する場合BatchImportFindings検出結果をに送信する API オペレーションAWS Security Hubでは、次のガイドラインを使用します。

- 電話しなきゃBatchImportFindings調査結果に関連付けられているアカウントを使用する。関連付けられたアカウントの識別子は、AwsAccountId検索の属性。
- できる最大のバッチを送信してください。Security Hub は、バッチあたり最大 100 件の調査結果を受け入れ、1 回の検索あたり最大 240 KB、バッチあたり最大 6 MB まで受け付けます。
- スロットルレートの制限は、リージョンごとにアカウントあたり 10 TPS で、バーストは 30 TPS です。
- スロットリングまたはネットワークの問題が存在する場合、結果の状態を保持するメカニズムを実装する必要があります。また、検索結果がコンプライアンスの内外に移動するときに検索の更新を送信できるように、検索条件の状態も必要です。
- 文字列の最大長およびその他の制限事項の詳細については、を参照してください。AWSSecurity Finding 形式のAWS Security Hubユーザーガイド。

製品の準備チェックリスト

-AWS Security HubAPN パートナーチームはこのチェックリストを使用して、統合を開始する準備ができていることを確認します。

ASFF マッピング

これらの質問は、結果とAWSSecurity Finding 形式

パートナーの発見データはすべて ASFF にマッピングされていますか。

すべての調査結果を ASFF に何らかの方法でマッピングします。

モデル化されたリソースタイプなどのキュレーションされたフィールドを使用し、Network,Malware, またはThreatIntelIndicators。

他のものをにマップするResource.Details.OtherまたはProductFields必要に応じて。

パートナーは使っていますか**Resource.Details**フィールド (な
ど)**AwsEc2instance**,**AwsS3Bucket**, および**Container**? パートナーは使っています
か**Resource.Details.Other**ASFF でモデル化されていないリソースの詳細を定義するには

可能な場合は、結果の EC2 インスタンス、S3 バケット、セキュリティグループなどのキュレーションリソースに用意されているフィールドを使用します。

リソースに関連するその他の情報をResource.Details.Other直接試合がない場合のみ。

パートナーは値をにマップしますか**UserDefinedFields**?

使用しません。UserDefinedFields

次のような別のキュレーションフィールドの使用を検討してくださ
い。Resource.Details.OtherまたはProductFields。

パートナーは情報をにマップしますか**ProductFields**それは他の ASFF フィールドにマッピングできますか？

使用のみProductFieldsバージョン管理情報、製品固有の重要度の調査結果、または厳選されたフィールドにマッピングできないその他の情報など、製品固有の情報Resources.Details.Other。

パートナーは、独自のタイムスタンプをインポートしますか**FirstObservedAt**?

-FirstObservedAtタイムスタンプは、製品内で発見が観察された時刻を記録するためのものです。可能であれば、このフィールドをマップします。

パートナーは、更新する調査結果を除き、各検索識別子に対して生成された一意の値を提供していますか。

Security Hub のすべての結果が、検索識別子 (Id属性)。この値は、結果が不正に更新されないように、常に一意である必要があります。

また、結果を更新する目的で、検出識別子の状態を維持する必要があります。

パートナーは、結果をジェネレータ ID にマッピングする値を提供していますか。

GeneratorID検索 ID と同じ値であってはなりません。

GeneratorIDは、それらを生成したものによって調査結果を論理的にリンクできるはずです。

これは、製品内のサブコンポーネント（製品 A-脆弱性対製品 A-EDR）、または類似するものである可能性があります。

パートナーは、製品に関連する方法で、必要な検索タイプの名前空間を使用していますか？ パートナーは、検索タイプで推奨される検索タイプのカテゴリまたは分類子を使用していますか。

検出タイプのタクソノミは、製品が生成する調査結果に密接にマッピングする必要があります。

で概説されている第 1 レベルの名前空間AWSSecurity Finding 形式が必要です。

第 2 レベルおよび 3 番目のレベルの名前空間 (カテゴリまたは分類子) にはカスタム値を使用できます。

パートナーは、ネットワークフロー情報をキャプチャしますか**Network**フィールド、ネットワークデータがある場合

商品がキャプチャされた場合NetFlow情報、それをマップしてNetworkフィールド。

パートナーは、のPID (PID) 情報を処理しますか**Process**フィールド、プロセスデータがある場合

製品がプロセス情報を取得する場合は、その情報をProcessフィールド。

パートナーは、マルウェア情報をキャプチャしますか**Malware**フィールド、マルウェアデータがある場合

製品がマルウェア情報をキャプチャする場合は、その情報をMalwareフィールド。

パートナーは、脅威インテリジェンス情報を**ThreatIntelIndicators**フィールド、脅威インテリジェンスデータがあれば？

製品が脅威インテリジェンスの情報をキャプチャする場合は、その情報をThreatIntelIndicatorsフィールド。

パートナーは、調査結果の信頼評価を提供していますか。もしそうなら、理論的根拠は提供されますか？

このフィールドを使用するときはいつでも、ドキュメントとマニフェストに根拠を記載してください。

パートナーは、結果のリソース ID に正規 ID または ARN を使用していますか。

識別するときAWSリソースの場合、ベストプラクティスは ARN を使用することです。ARN が利用できない場合は、標準リソース ID を使用します。

統合セットアップと機能

これらの質問は、セットアップと関連しています。day-to-day統合の関数。

パートナーはinfrastructure-as-codeTerraform などの Security Hub との統合をデプロイするための (iaC) テンプレートAWS CloudFormation, またはAWS Cloud Development Kit (AWS CDK)?

カスタマーアカウントから調査結果を送信したり、CloudWatch調査結果を消費するイベント、何らかの形式の iaC テンプレートが必要です。

AWS CloudFormationが優先されますが、AWS CDKまたは Terraform を使用できます。

パートナー製品のコンソールに Security Hub との統合のためのワンクリック設定がありますか。

一部のパートナー製品は、製品内でトグルまたは同様のメカニズムを使用して統合をアクティブ化します。これには、自動的にリソースと権限のプロビジョニングが必要になる場合があります。製品アカウントから結果を送信する場合は、ワンクリックの設定が推奨されます。

パートナーは価値のある調査結果のみを送りますか？

通常、セキュリティ価値のある調査結果を Security Hub のお客様に送信する必要があります。

Security Hub は、一般的なログ管理ツールではありません。可能なすべてのログを Security Hub に送信しないでください。

パートナーは、顧客あたり1日に送信する調査結果の数と、どの頻度（平均とバースト）で送信されるかについての見積もりを提供しましたか？

Security Hub の負荷の計算には、固有の調査結果の数が使用されます。一意の結果は、別の結果と異なる ASFF マッピングを持つ結果として定義されます。

たとえば、ある検索が入力された場合のみThreatIntelIndicatorsもう一つは移入されただけResources.Details.AWSEc2Instance、これら2つのユニークな所見である。

パートナーは 4xx および 5xx エラーを処理し、スロットルされず、すべての調査結果を後で送信できるような優美な方法がありますか。

現在、には 30 ~ 50 TPS バーストレートがあります。BatchImportFindingsAPI オペレーション。4xx エラーまたは 5xx エラーが返された場合は、後ですべて再試行できるように、失敗した結果の状態を保持する必要があります。これは、デッドレターキューまたは別のキューを介して行うことができます。AWSAmazon SNS や Amazon SQS などのメッセージングサービス。

パートナーは、もはや存在しない調査結果をアーカイブすることがわかるように、調査結果の状態を維持していますか？

元の検索 ID を上書きして結果を更新する場合は、正しい結果に対して正しい情報が更新されるように、状態を保持するメカニズムが必要です。

調査結果を提供する場合は、BatchUpdateFindings結果を更新するオペレーション。この操作は、お客様のみが使用する必要があります。あなただけ使うBatchUpdateFindings結果を調査してアクションを実行するとき。

パートナーは、以前に送信された成功した結果に妥協しない方法で再試行を処理しますか。

エラー発生時に成功した結果を複製したり上書きしたりしないように、エラー発生時に元の検出 ID を保持するメカニズムが必要です。

パートナーは、**BatchImportFindings**既存の調査結果の発見IDでの操作？

結果を更新するには、同じ検索結果 ID を送信して、既存の結果を上書きする必要があります。

-BatchUpdateFindings操作は顧客のみが使用する必要があります。

パートナーは、**BatchUpdateFindings**API？

調査結果に対して行動を起こす場合は、BatchUpdateFindings特定のフィールドを更新する操作。

パートナーは、検索結果が作成されてから製品から Security Hub に送信されるまでのレイテンシの量に関する情報を提供していますか。

Security Hub でできるだけ早く結果を確認できるように、レイテンシーを最小限に抑える必要があります。

この情報はマニフェストで必要です。

パートナーのアーキテクチャが、お客様のアカウントから Security Hub に調査結果を送信する場合、このことを正常に実証しましたか。パートナーのアーキテクチャが自分のアカウントから Security Hub に調査結果を送信する場合、彼らはこれを正常に実証しましたか？

テスト中、製品 ARN に提供されたアカウントとは異なる所有のアカウントから結果が正常に送信される必要があります。

製品 ARN 所有者のアカウントから結果を送信すると、API オペレーションからの特定のエラー例外を回避できます。

パートナーは Security Hub にハートビートの発見を提供していますか。

インテグレーションが正しく動作していることを示すには、ハートビートの結果を送信する必要があります。ハートビートの検出は 5 分ごとに送信され、検出タイプが使用されます。`Heartbeat`。

これは、製品アカウントから調査結果を送信する場合に重要です。

テスト中に、パートナーは Security Hub 製品チームのアカウントと統合しましたか。

本番前の検証中に、検索例を Security Hub 製品チームに送信する必要があります。AWSアカウント. これらの例は、調査結果が正しく送信され、マッピングされていることを示しています。

ドキュメント

これらの質問は、提供する統合のドキュメントに関連しています。

パートナーは専用のウェブサイトでドキュメントをホストしていますか？

ドキュメントは、静的な Web ページ、Wiki、ドキュメントを読む、またはその他の専用形式としてウェブサイトでホストする必要があります。

ドキュメントをホストするGitHubは、専用ウェブサイトの要件を満たしていません。

Security Hub 統合のセットアップ方法については、パートナーのドキュメントに記載されていますか。

iaC テンプレートまたはコンソールベースの「ワンクリック」統合を使用して、統合をセットアップできます。

パートナーのドキュメントには、ユースケースの説明が記載されていますか。

マニフェストで提供するユースケースについては、ドキュメントにも説明する必要があります。

パートナーのドキュメントは、送信した調査結果の理論的根拠を提供していますか。

送信する調査結果の種類の理論的根拠を提供する必要があります。

たとえば、製品が脆弱性、マルウェア、およびウイルス対策に関する調査結果を生成する可能性がありますが、Security Hub には脆弱性とマルウェアの調査結果のみを送信します。その場合、ウイルス対策の結果を送信しない理由の根拠を提供する必要があります。

パートナーのドキュメントには、パートナーが調査結果を ASFF にどのようにマッピングするかについての論理的根拠がありますか。

ASFF への製品のネイティブな発見のマッピングの理論的根拠を提供する必要があります。お客様は、特定の製品情報をどこで検索すべきかを知りたいと考えています。

パートナーが調査結果を更新した場合に、パートナーが調査結果を更新する方法についてのガイダンスを提供していますか。

状態を保持し、冪等性を保証し、結果を上書きする方法について顧客に情報を提供するup-to-date情報。

パートナーのドキュメントには、レイテンシーの発見について記載されていますか。

レイテンシーを最小限に抑えて、Security Hub でできるだけ早く結果を確認できるようにします。

この情報はマニフェストで必要です。

パートナーのドキュメントには、重要度スコアがASFFの重大度スコアリングにどのようにマッピングされるかが記載されていますか。

マップ方法に関する情報を提供するSeverity.OriginalにSeverity.Label。

たとえば、重大度がレターグレード (A、B、C) の場合、レターグレードを重大度ラベルにマッピングする方法に関する情報を提供する必要があります。

パートナーのドキュメントは、信頼度評価の理論的根拠を提供していますか。

信頼度スコアを指定する場合は、これらのスコアをランク付けする必要があります。

人工知能や機械学習から派生した静的に入力された信頼スコアまたはマッピングを使用する場合は、追加のコンテキストを提供する必要があります。

パートナーのドキュメントには、パートナーがサポートしているリージョンとサポートしていないリージョンが記載されていますか。

注:どのリージョンで統合を試みないか把握できるように、サポートされている、またはサポートされていないリージョン。

製品カード情報

これらの質問は、に表示される製品のカードに関連しています。統合Security Hub コンソールのページ。

は提供されますかAWSアカウント ID が有効で、12 桁の数字が含まれていますか

アカウント ID の長さは 12 桁です。アカウント ID が 12 桁未満の場合、製品 ARN は無効になります。

商品説明に200文字以下が含まれていますか

マニフェスト内の JSON で提供される商品説明は、スペースを含む 200 文字以内でなければなりません。

構成リンクは、統合のドキュメントにつながりますか。

設定リンクは、オンラインドキュメントにつながるはずです。メインのウェブサイトやマーケティングページにつながるべきではありません。

購入リンク（提供されている場合）は、AWS Marketplace商品の出品？

購入リンクを提供する場合は、AWS Marketplaceエントリ。Security Hub は、によってホストされていない購入リンクを受け入れませんAWS。

商品カテゴリーは商品を正しく説明していますか？

マニフェストでは、最大 3 つの製品カテゴリを指定できます。これらは JSON と一致する必要があり、カスタムにすることはできません。3 つ以上の商品カテゴリーを提供することはできません。

会社名および製品名は有効で正しいですか

会社名は 16 文字以下である必要があります。

製品名は 24 文字以下である必要があります。

製品カード JSON 内の製品名は、マニフェストの名前と一致する必要があります。

マーケティング情報

これらの質問は、統合のマーケティングに関連しています。

Security Hub パートナーページの商品説明はスペースも含めて 700 文字以内ですか

Security Hub パートナーページには、スペースを含む最大 700 文字しか入力できません。

チームは長い説明を編集する。

Security Hub パートナーページのロゴは 600 x 300 ピクセル以下ですか。

PNG または JPG で 600 x 300 ピクセル以下の会社のロゴを含むパブリックアクセス可能な URL を指定します。

[Security Hub パートナー] ページの [詳細はこちら] ハイパーリンクは、統合に関するパートナー専用の Web ページにつながりますか。

-詳細はこちらリンクは、パートナーのメインWebサイトやドキュメント情報に接続してはいけません。

このリンクは、常に統合に関するマーケティング情報を含む専用のWebページに移動する必要があります。

パートナーは、インテグレーションの使用方法に関するデモまたは説明ビデオを提供していますか？

デモまたは統合ウォークスルービデオはオプションですが推奨されます。

ですかAWSパートナーネットワークブログ投稿は、パートナーとそのパートナー開発マネージャまたはパートナー開発担当者とリリースされていますか？

AWSパートナーネットワークのブログ投稿は、パートナー開発マネージャまたはパートナー開発担当者と事前に調整する必要があります。

これらは、自分で作成したブログ投稿とは別のものです。

4 ~ 6 週間のリードタイムを許容します。この作業は、プライベート製品 ARN でのテストが完了した後に開始する必要があります。

パートナー主導のプレスリリースはリリースされていますか？

パートナー開発マネージャまたはパートナー開発担当者と協力して、外部セキュリティサービス担当副社長から見積もりを受け取ることができます。この見積もりは、プレスリリースで使用できます。

パートナー主導のブログ投稿はリリースされていますか？

独自のブログ投稿を作成して、外部の統合を紹介することができます。AWSパートナーネットワークブログ。

パートナー主導のウェビナーがリリースされていますか。

独自のウェビナーを作成して、統合を披露できます。

Security Hub チームのサポートが必要な場合は、プライベート製品 ARN でテストを完了した後、製品チームと協力してください。

パートナーがソーシャルメディアのサポートをリクエストしましたかAWS?

リリース後は、AWSセキュリティマーケティングは利用につながるAWS公式ソーシャルメディアチャンネルでウェビナーの詳細を共有できます。

AWS Security Hubパートナーに関するよくある質問

との統合の設定と保守についてよく寄せられる質問を次に示します。AWS Security Hub。

1. Security Hub 統合の利点は何ですか。
   - 顧客満足度— Security Hub と統合する第一の理由は、お客様からの要求があるためです。

     Security Hub は、セキュリティとコンプライアンスのセンターです。AWS顧客。これは、最初の停留所として設計されています。AWSセキュリティとコンプライアンスのプロフェッショナルは、毎日セキュリティとコンプライアンスの状態を理解しています。

     顧客の声に耳を傾ける。Security Hub で調査結果を確認するかどうかがわかります。
   - 検出機会— Security Hub コンソール内の認定インテグレーションを持つパートナーを宣伝します。これには、パートナーへのリンクも含まれます。AWS Marketplaceリスティング。これは、お客様が新しいセキュリティ製品を発見するのに最適な方法です。
   - マーケティング機会— 承認済みのインテグレーションを持つベンダーは、ウェビナーへの参加、プレスリリースの発行、滑らかなシートの作成、および統合のデモンストレーションを行うことができますAWS顧客。
2. パートナーにはどのような種類がありますか？
   - 検出結果を Security Hub に送信するパートナー
   - Security Hub から検出結果を受け取るパートナー
   - 調査結果を送受信するパートナー
   - お客様が環境で Security Hub をセットアップ、カスタマイズ、および使用できるように支援するコンサルティングパートナー
3. Security Hub とのパートナー統合は、高いレベルでどのように機能しますか。

   顧客アカウント内または自分のアカウントから結果を収集します。AWS計算し、結果のフォーマットをAWSSecurity Finding 形式。次に、これらの結果を適切な Security Hub リージョンエンドポイントにプッシュします。

   また、CloudWatchSecurity Hub から検出結果を受け取るイベント。
4. Security Hub との統合を完了するための基本的な手順は何ですか。
   a. パートナーマニフェスト情報を送信します。
   b. Security Hub に調査結果を送信する場合は、Security Hub で使用する製品 ARN を受け取ります。

c. 調査結果を ASFF にマッピングします。「the section called “ASFF マッピングのガイドライン”」を参照してください。

d. Security Hub に結果を送信し、結果を受信するためのアーキテクチャを定義します。に概説されている教義に従うthe section called “調査結果の作成と更新に関する教訓”。

e. 顧客向けのデプロイフレームワークを作成します。たとえば、AWS CloudFormationスクリプトはこの目的を果たすことができます。

f. セットアップを文書化し、お客様に構成手順を提供してください。

g. 顧客が商品で使用できるカスタムインサイト (相関ルール) を定義します。

h. Security Hub チームとの統合をデモンストレーションします。

i. 承認のためにマーケティング情報を提出する (ウェブサイトの言語、プレスリリース、アーキテクチャスライド、ビデオ、滑らかなシート) 。

5. パートナーマニフェストを提出するプロセスは何ですか？ そしてのためにAWS検出結果を Security Hub に送信するためのサービス?

   Security Hub チームにマニフェスト情報を送信するには、<securityhub-partners@amazon.com>。

   7 暦日以内に製品 ARN が発行されます。

6. Security Hub に送信すべき調査結果の種類は何ですか。

   Security Hub の価格は、取り込まれた調査結果の数に部分的に基づいています。このため、顧客に価値を提供しない調査結果を送信することは控えるべきです。

   たとえば、一部の脆弱性管理ベンダーは、一般的な脆弱性スコアリングシステム (CVSS) のスコアが 10 のうち3以上の結果のみを送信します。

7. 検出結果を Security Hub に送信するには、どのような方法がありますか?

   主なアプローチは次のとおりです。

   - 自分の指定から調査結果を送るAWSアカウントを使用してBatchImportFindingsオペレーション.
   - 顧客アカウント内から結果を送信するには、BatchImportFindingsオペレーション. assume-role アプローチを使用することもできますが、これらのアプローチは必須ではありません。

   使用に関する全体的なガイドラインについてBatchImportFindings「」を参照してください。the section called “を使用するガイドラインBatchImportFindingsAPI”。

8. 調査結果を収集し、Security Hub リージョナルエンドポイントにプッシュするにはどうすればよいですか。

   パートナーは、ソリューションのアーキテクチャに大きく依存するため、さまざまなアプローチを使用してきました。

   たとえば、一部のパートナーは Python アプリケーションをビルドし、AWS CloudFormation スクリプト。このスクリプトは、顧客環境からパートナーの結果を収集し、ASFF に変換して、Security Hub リージョナルエンドポイントに送信します。

   他のパートナーは、シングルクリック操作で結果を Security Hub にプッシュできる完全なウィザードを構築しています。

9. 検出結果を Security Hub に送信するタイミングはどのようにしてわかりますか?

   Security Hub では、部分的なバッチ認証がサポートされています。`BatchImportFindings`API オペレーション。これにより、すべての顧客に対して Security Hub にすべての結果を送信できます。

   一部のお客様が Security Hub にまだサブスクライブしていない場合、Security Hub はそれらの結果を取り込みません。バッチに含まれる承認済みの調査結果のみを取り込みます。

10. 結果を Security Hub インスタンスに送信するには、どのような手順を完了する必要がありますか?

    a. 正しい IAM ポリシーが設定されていることを確認します。

    b. アカウントの製品サブスクリプション (リソースポリシー) を有効にします。次のいずれかを使用します。`EnableImportFindingsForProduct`API オペレーションまたは API オペレーション統合ページで. 顧客がこれを行うか、クロスアカウントロールを使用して顧客の代理として行動することができます。

    c. 以下の内容を確認します。`ProductArn`見つかったのは、製品のパブリック ARN です。

    d. 以下の内容を確認します。`AwsAccountId`検出結果のうち、顧客のアカウント ID です。

    e. 調査結果に不正な形式のデータがないことを確認します。AWSSecurity Finding 形式。たとえば、必須フィールドに入力され、無効な値はありません。

    f. 結果をバッチで正しいリージョナルエンドポイントに送信します。

11. 調査結果を送信するには、どの IAM 権限を設定する必要がありますか?

    IAM ポリシーは、を呼び出す IAM ユーザーまたはロールに対して設定する必要があります。`BatchImportFindings`またはその他の API 呼び出し。

最も簡単なテストは、管理者アカウントから行うことです。これらを制約してaction: 'securityhub:BatchImportFindings'そしてresource: *<productArn and/or productSubscriptionArn>*。

同じアカウント内のリソースは、リソースポリシーを必要とせずに IAM ポリシーで設定できます。

の呼び出し元からの IAM ポリシーの問題を除外するにはBatchImportFindingsで、呼び出し元の IAM ポリシーを次のように設定します。

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

何もないことを必ず確認してくださいDeny呼び出し元に対するポリシー。それを操作したら、ポリシーを次のように制限できます。

```
{
    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製品サブスクリプションとは何ですか？

特定のパートナー製品から結果を受け取るには、顧客（または顧客に代わってクロスアカウントの役割を持つパートナー）が製品サブスクリプションを確立する必要があります。コンソールからこれを行うには、統合ページで. これを API から行うには、EnableImportFindingsForProductAPI オペレーション。

製品サブスクリプションは、パートナーからの調査結果を顧客から受信または送信することを許可するリソースポリシーを作成します。詳細については、ユースケースとパーミッション を参照してください

Security Hub には、パートナー向けの次のタイプのリソースポリシーがあります。

- BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT
- BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT

パートナーオンボーディングプロセス中に、どちらか一方または両方のタイプのポリシーをリクエストできます。

とBATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNTでは、製品 ARN に記載されているアカウントからのみ結果を Security Hub に送信できます。

とBATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNTの場合、調査結果を送信できるのは、購読したカスタマーアカウントからのみです。

13顧客が管理者アカウントを作成し、いくつかのメンバーアカウントを追加したと仮定します。顧客は各メンバーアカウントを購読する必要がありますか？ または、顧客は管理者アカウントからのみサブスクライブし、すべてのメンバーアカウントのリソースに対して結果を送信できますか。

この質問では、管理者アカウントの登録に基づいて、すべてのメンバーアカウントに権限が作成されるかどうかを尋ねます。

お客様は、アカウントごとに製品サブスクリプションを設定する必要があります。これは API を通じてプログラムで実行できます。

14製品の ARN は何ですか。

製品 ARN は、Security Hub が生成し、結果を送信するために使用する一意の識別子です。Security Hub と統合する製品ごとに製品 ARN を受け取ります。正しい製品 ARN は、Security Hub に送信するすべての結果の一部である必要があります。製品 ARN がない所見は削除されます。製品 ARN は次の形式です。

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

以下がその例です。

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

Security Hub がデプロイされているリージョンごとに、製品 ARN が与えられます。アカウント ID、会社、および製品名は、パートナーマニフェストの提出によって決定されます。製品の ARN に関連付けられている情報は、リージョンコードを除き、決して変更しません。リージョンコードは、調査結果を送信するリージョンと一致する必要があります。

よくある間違いは、現在作業しているアカウントと一致するようにアカウント ID を変更することです。アカウント ID は変更されません。マニフェスト送信の一環として、「ホーム」アカウント ID を提出します。このアカウント ID は製品 ARN にロックされています。

Security Hub が新しいリージョンで起動すると、標準のリージョンコードが自動的に使用され、それらのリージョンの製品 ARN が生成されます。

すべてのアカウントは、プライベート製品 ARN を使用して自動的にプロビジョニングされます。この ARN を使用して、公式のパブリック製品 ARN を受け取る前に、独自の開発アカウント内で調査結果のインポートをテストできます。

15.検出結果を Security Hub に送信するには、どのような形式を使用する必要がありますか?

検出結果については、AWSSecurity Finding 形式。詳細については、「」を参照してください。AWSSecurity Finding 形式のAWS Security Hubユーザーガイド。

期待されるのは、ネイティブの結果に含まれるすべての情報が ASFF に完全に反映されるということです。カスタムフィールドProductFieldsそしてResource.Details.Other定義済みのフィールドにきちんと収まらないデータをマッピングできます。

16.使用する正しいリージョナルエンドポイントは何ですか。

顧客アカウントに関連付けられている Security Hub リージョナルエンドポイントに結果を送信する必要があります。

17.リージョンのエンドポイントの一覧はどこから入手できますか。

フレームワークの使用の詳細については、Security Hub エンドポイントリスト。

18.クロスリージョン調査結果を送信することはできますか？

Security Hub は、ネイティブの地域間での調査結果の送信をまだサポートしていません。AWSAmazonなどのサービスGuardDuty、Amazon Macie、Amazon Inspector。お客様が許可している場合、Security Hub は別のリージョンからの調査結果を送信することを妨げません。

この意味で、リージョンエンドポイントをどこからでも呼び出すことができ、ASFF のリソース情報はエンドポイントのリージョンと一致する必要はありません。ただし、`ProductArn`エンドポイントのリージョンと一致する必要があります。

19.調査結果のバッチを送信するためのルールとガイドラインは何ですか？

1 回の呼び出しで最大 100 件または 240 KB までバッチ処理できます。`BatchImportFindings`。この制限まで、できるだけ多くの調査結果をキューに入れてバッチ処理します。

異なるアカウントからの結果のセットをバッチ処理できます。ただし、バッチ内のいずれかのアカウントが Security Hub に登録されていない場合、バッチ全体が失敗します。これは、API Gateway ベースライン認証モデルの制限です。

「the section called “を使用するガイドラインBatchImportFindingsAPI”」を参照してください。

20.作成した調査結果に更新を送信することはできますか？

はい。同じ製品 ARN および同じ検索 ID を使用して結果を送信すると、その結果の以前のデータが上書きされます。すべてのデータが上書きされるため、完全な結果を送信する必要があります。

お客様は、新しい調査結果と更新情報の両方に対して従量課金され、請求されます。

21.他の誰かが作成した調査結果に更新を送信することはできますか？

はい、お客様からアクセス権を付与した場合`BatchUpdateFindings`API 操作の場合、その操作を使用して特定のフィールドを更新できます。この操作は、顧客、SIEM、チケットシステム、Security Orchestration, Automation, and Response (SOAR) プラットフォームで使用するように設計されています。

22.調査結果は何歳になりますか？

Security Hub は、最終更新日から 90 日後に検出結果を期限切れにします。この時間が経過すると、期限切れの結果はSecurity Hub から消去されます。OpenSearchクラスター。

同じ検索 ID で結果を更新し、それが期限切れになっている場合、新しい結果が Security Hub で作成されます。

お客様が使用できるCloudWatchSecurity Hub から調査結果を移動するイベント。これにより、すべての調査結果をお客様が選択したターゲットに送信できるようになります。

一般に、Security Hub は 90 日ごとに新しい結果を作成し、結果を永久に更新しないことを推奨します。

23.Security Hub はどのようなスロットルを設置していますか？

Security Hub のスロットル`GetFindings`API 呼び出し。調査結果にアクセスするための推奨されるアプローチはCloudWatch[Events (イベント)] 。

Security Hub は、API Gateway および Lambda 呼び出しによって強制される範囲を超えて、内部サービス、パートナー、または顧客に他のスロットリングを実装しません。

24.ソースサービスから Security Hub に送信される結果の適時性、レイテンシー SLA、または期待値はどれくらいですか。

目的は、初期調査結果と調査結果の更新の両方について、できるだけリアルタイムに近い時間になることです。結果の作成後 5 分以内に Security Hub に送信する必要があります。

25.Security Hub から検出結果を受け取るにはどうすればよいですか。

検出結果を受け取るには、次のいずれかの方法を使用します。

- すべての調査結果は自動的にに送信されますCloudWatch[Events (イベント)] 。顧客は特定のものを作成できるCloudWatchイベントルールは、SIEM や S3 バケットなどの特定のターゲットに結果を送信するためのルールです。この機能はレガシーに取って代わった`GetFindings`API オペレーション。
- を使用するCloudWatchカスタムアクションのイベント。Security Hub を使用すると、コンソール内から特定の結果または結果のグループを選択し、それらに対してアクションを実行できます。たとえば、調査結果を SIEM、チケットシステム、チャットプラットフォーム、または修復ワークフローに送信できます。これは、お客様が Security Hub 内で実行するアラートのトリアージワークフローの一部です。これらはカスタムアクションと呼ばれます。

  ユーザーがカスタムアクションを選択すると、CloudWatchこれらの特定の調査結果に対してイベントが作成されます。この機能を活用して構築できます。CloudWatch顧客がカスタムアクションの一部として使用するイベントのルールとターゲット。この機能は、特定のタイプまたはクラスのすべての結果を自動的に送信するために使用されないことに注意してください。CloudWatch[Events (イベント)] 。ユーザーが特定の調査結果に対してアクションを実行することです。

  次のようなカスタムアクション API オペレーションを使用できます。`CreateActionTarget`を使用して、製品に対して使用可能なアクションを自動的に作成する (など)。AWS CloudFormationテンプレート)。また、CloudWatchイベントルールの API オペ

レーションに対応するCloudWatchカスタムアクションに関連付けられているイベントルール。を使用するAWS CloudFormationテンプレートを作成することもできます。CloudWatch特定の特性を持つすべての結果またはすべての結果を Security Hub から自動的に取り込むためのイベントルール。

26.マネージドセキュリティサービスプロバイダー (MSSP) がSecurity Hub パートナーになるための要件は何ですか。

Security Hub が顧客へのサービス提供の一部としてどのように使用されているかを示す必要があります。

Security Hub の使用を説明するユーザドキュメントが必要です。

MSSP が検索プロバイダーである場合は、Security Hub に調査結果を送信することをデモンストレーションする必要があります。

MSSP がSecurity Hub からの結果のみを受信する場合は、少なくともAWS CloudFormation適切な設定を行うテンプレートCloudWatchEvents ルール。

27.MSSP 以外のAPN コンサルティングパートナーがSecurity Hub パートナーになるための要件は何ですか。

APN コンサルティングパートナーであれば、Security Hub パートナーになることができます。特定の顧客が次のことをどのように支援したかについて、2 つのプライベートケーススタディを提出する必要があります。

- お客様が必要とする IAM アクセス許可を使用して Security Hub をセットアップします。
- コンソールの [パートナー] ページの設定手順を使用して、すでに統合された独立系ソフトウェアベンダー (ISV) ソリューションを Security Hub に接続するのに役立ちます。
- カスタム製品統合で顧客を支援します。
- 顧客のニーズとデータセットに関連するカスタムインサイトを構築します。
- カスタムアクションを作成します。
- 修復 Playbook を構築します。
- Security Hub のコンプライアンス基準に適合するクイックスタートを構築します。これらは、Security Hub チームによって検証される必要があります。

ケーススタディは、パブリックに共有可能である必要はありません。

28.Security Hub との統合を顧客と展開する方法に関する要件は何ですか。

Security Hub とパートナー製品間の統合アーキテクチャは、パートナーのソリューションの運用方法に関してパートナーによって異なります。統合のセットアッププロセスに 15 分以上かからないようにする必要があります。

統合ソフトウェアをお客様の環境に展開する場合AWS環境、活用すべきAWS CloudFormation統合を簡素化するテンプレート。一部のパートナーはワンクリック統合を作成しており、これは強く推奨されています。

29.書類の要件は何ですか？

製品と Security Hub 間の統合とセットアッププロセスについて説明したドキュメントへのリンクを提供する必要があります。AWS CloudFormationテンプレート。

そのドキュメントには、ASFF の使用状況に関する情報も記載する必要があります。具体的には、さまざまな調査結果に使用している ASFF の検出タイプがリストされます。デフォルトのインサイト定義がある場合は、ここにインサイト定義を含めることをお勧めします。

その他の潜在的な情報を含めることを検討してください。

- Security Hub との統合ユースケース
- 送信された調査結果の平均量
- 統合アーキテクチャ
- あなたが行っている地域とサポートしていないリージョン
- 結果が作成されてから Security Hub に送信されるまでのレイテンシ
- 調査結果を更新するかどうか

30カスタムインサイトとは何ですか

調査結果のカスタムインサイトを定義することをお勧めします。インサイトは軽量な相関ルールで、顧客が注目とアクションを最も必要とする調査結果とリソースの優先順位付けに役立ちます。

Security Hub には、`CreateInsight`API オペレーション。カスタムインサイトは、お客様のアカウントの一部としてカスタマーアカウント内に作成できます。AWS CloudFormationテンプレート。これらのインサイトは、お客様のコンソールに表示されます。

31ダッシュボードウィジェットを送信できますか？

いいえ、現時点では利用できません。作成できるのはマネージド型インサイトのみです。

32.価格モデルは何ですか？

フレームワークの使用の詳細については、Security Hub の価格情報。

33統合の最終承認プロセスの一環として、調査結果を Security Hub デモアカウントに送信するにはどうすればよいですか。

提供された製品 ARN を使用して、Security Hub のデモアカウントに調査結果を送信します。us-west-2地域として。調査結果には、デモ口座番号をAwsAccountIdASFFのフィールド。デモ口座番号を入手するには、Security Hub チームにお問い合わせください。

機密データや個人を特定できる情報を当社に送信しないでください。このデータは公開デモに使用されます。このデータを送信すると、デモでデータを使用する権限が与えられます。

34エラーメッセージまたは成功メッセージは何ですかBatchImportFindings提供しますか。

Security Hub は、承認に対する応答と応答を提供します。BatchImportFindings。より鮮明な成功、失敗、エラーメッセージが開発中です。

35.ソースサービスはどのようなエラー処理を担当していますか。

ソースサービスは、すべてのエラー処理を担当します。エラーメッセージ、再試行、スロットリング、およびアラームを処理する必要があります。また、Security Hub フィードバックメカニズムを通じて送信されたフィードバックまたはエラーメッセージを処理する必要があります。

36.一般的な問題の解決策は何ですか？

AnAuthorizerConfigurationExceptionどちらかが不正なことが原因であるAwsAccountIdまたはProductArn。

トラブルシューティングを行う場合、以下の点に注意してください。

- AwsAccountId正確に 12 桁でなければなりません。
- ProductArnarn: aws securityHub の形式は次の形式である必要があります。*<us-west-2 or us-east-1>*:*<accountId>*:Product/*<company-id>*/*<product-id>*

  アカウント ID は、Security Hub チームが提供した製品 ARN に含まれていたアカウントIDとは変更されません。

AccessDeniedException間違ったアカウントとの間で検索情報が送信された場合、またはアカウントにProductSubscription。エラーメッセージには、リソースタイプが「」の ARN が含まれます。productまたはproduct-subscription。このエラーは、クロスアカウントコール中にのみ発生します。電話したらBatchImportFindings同じアカウントの自分のアカウント

でAwsAccountIdそしてProductArnオペレーションは IAM ポリシーを使用しており、とは無関係です。ProductSubscriptions。

使用する顧客アカウントと製品アカウントが実際の登録アカウントであることを確認してください。一部のパートナーは、製品 ARN の製品のアカウント番号を使用していますが、まったく別のアカウントを使用して電話をかけようとします。BatchImportFindings。他のケースでは、作成しました。ProductSubscriptions他の顧客アカウント、または自分の製品アカウントの場合。彼らは作成しなかったProductSubscriptions結果のインポートを試みたカスタマーアカウントについて。

37.質問、コメント、バグはどこで送られますか

<securityhub-partners@amazon.com>

38.グローバルに関連するアイテムについて調査結果を送信する地域はどれですかAWSサービス? たとえば、IAM 関連の調査結果をどこに送りますか。

結果が検出されたのと同じリージョンに調査結果を送信します。IAM などのサービスの場合、ソリューションが複数のリージョンで同じ IAM 問題を検出する可能性があります。この場合、調査結果は、問題が検出されたすべてのリージョンに送信されます。

お客様が 3 つのリージョンで Security Hub を実行し、3 つのリージョンすべてで同じ IAM の問題が検出された場合は、3 つのリージョンすべてに結果を送信します。

問題が解決したら、元の検索結果を送信したすべてのリージョンに、検索結果の更新情報を送信します。

パートナー統合ガイドのドキュメント履歴

以下の表は、このガイドのドキュメントの更新をまとめたものです。

変更	説明	日付
コンソールロゴの要件が更新されました	パートナーマニフェストとロゴのガイドラインを更新し、パートナーが Security Hub コンソールに表示されるロゴのライトモードとダークモードの両方のバージョンを提供する必要があることを示します。ロゴは SVG 形式である必要があります。	2021 年 5 月 10 日
新しい統合パートナーの前提条件を更新しました	Security Hub は、AWS ISV パートナーパスに参加し、AWS Foundational Technical Review (FTR) を完了した統合製品を使用するパートナーも許可するようになりました。以前は、すべての統合パートナーが AWS 選択ばれたティアパートナーである必要がありました。	2021 年 4 月 29 日
ASFF の新規 FindingProviderFields オブジェクト	結果を ASFF にマッピングする情報を更新しました。Confidence 、Criticality 、RelatedFindings 、Severity、および Types の場合、パートナーはその値を FindingProviderFields のフィールドにマッピングします。	2021 年 3 月 18 日

結果の作成と更新の新しい教義	Security Hub での新しい結果の作成と、既存の結果の更新のための新しいガイドラインを追加しました。	2020 年 12 月 4 日
このガイドの初回リリース	この パートナー統合ガイドは AWS パートナーが AWS Security Hub との統合を確立する方法に関する情報を提供します。	2020 年 6 月 23 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。