パートナー統合ガイド

AWS Security Hub CSPM

AWS Security Hub CSPM: パートナー統合ガイド

Table of Contents

とサードパーティーの統合の概要AWS Security Hub CSPM

このガイドは、 との統合を作成する AWSPartner Network (APN) パートナーを対象としています AWS Security Hub CSPM。

APN パートナーとして、次のいずれかの方法で Security Hub CSPM と統合できます。

- Security Hub CSPM に結果を送信する
- Security Hub CSPM から検出結果を使用する
- Security Hub CSPM に結果を送信し、Security Hub CSPM から結果を使用する
- Security Hub CSPM をマネージドセキュリティサービスプロバイダー (MSSP) サービスの中心として使用する
- Security Hub CSPM をデプロイして使用する方法については、AWSお客様と相談してください。

このオンボーディングガイドでは、主に Security Hub CSPM に結果を送信するパートナーに焦点を当てています。

トピック

と統合する理由AWS Security Hub CSPM

AWS Security Hub CSPMは、Security Hub CSPM アカウント全体で優先度の高いセキュリティアラートとセキュリティステータスの包括的なビューを提供します。Security Hub CSPM では、セキュリティ検出結果を Security Hub CSPM に送信して、生成したセキュリティ検出結果に関するインサイトを顧客に提供できます。

Security Hub CSPM との統合では、次の方法で値を追加できます。

- Security Hub CSPM 統合をリクエストした顧客を満たす
- セキュリティAWS関連の検出結果を 1 つのビューで顧客に提供

- 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します

Security Hub CSPM 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。顧客が Security Hub CSPM と製品との統合を希望する場合、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で、または新規お客様を獲得するためだけに統合を構築できます。ただし、現在のお客様からの入力なしで統合を構築し、お客様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 CSPM

APN パートナーとして、Security Hub CSPM チームが検出結果プロバイダーとしてお客様を有効にするまで、お客様のために Security Hub CSPM に情報を送信することはできません。結果プロバイダーとして有効にするには、オンボーディングに関する以下のステップを完了する必要があります。そうすることで、お客様とお客様のために Security Hub CSPM をポジティブに体験できます。

オンボーディングのステップを完了するときは、the section called “結果の作成と更新に関する教義”、the section called “ASFF マッピングのガイドライン”、および the section called “BatchImportFindings API 使用のガイドライン” のガイドラインに従ってください。

1. セキュリティ検出結果を AWSSecurity Finding 形式 (ASFF) にマッピングします。
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ンの Security Hub CSPM エンドポイントにプッシュします。これを行うには、結果を自分のAWSアカウントから送信するか、顧客のアカウント内から送信するかを定義します。
3. お客様にアカウントで製品をサブスクライブしてもらいます。これを行うには、コンソールまたは `EnableImportFindingsForProduct` API オペレーションを使用できます。AWS Security Hubユーザーガイドの「製品統合の管理」を参照してください。の。

   また、製品のサブスクライブを代行することもできます。これを行うには、お客様に代わり、アカウント間ロールを使用して、`EnableImportFindingsForProduct` API オペレーションにアクセスします。

   このステップでは、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 CSPM との既存のパートナー統合の一部について説明します。

- とのクラウドカストディアン統合の発表AWS Security Hub CSPM
- AWS Fargateと Prowler を使用して、AWSサービスに関するセキュリティ設定の検出結果を Security Hub CSPM に送信する
- Security Hub CSPM でAWS Configルール評価を結果としてインポートする方法

から結果を受信する準備AWS Security Hub CSPM

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

- お客様にすべての結果を CloudWatch Eventsに自動的に送信してもらいます。お客様は、特定の CloudWatch Eventsルールを作成して、SIEM や S3 バケットなどの特定のターゲットに結果を送信できます。
- Security Hub CSPM コンソール内から特定の検出結果または検出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するように顧客に指示します。

たとえば、お客様は、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結果を送信できます。これは、顧客が Security Hub CSPM 内で実行するアラートトリアージワークフローの一部になります。

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、それらの特定の結果に対して CloudWatch Eventsが作成されます。パートナーとして、この特徴を利用して、お客様がカスタムアクションのパートとして使用するための CloudWatch Eventsルールまたはターゲットを構築できます。この特徴は、特定のタイプまたはクラスのすべての結果を CloudWatch Eventsに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。この特徴は、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。

次のブログ投稿では、カスタムアクションに Security Hub CSPM および CloudWatch Events との統合を使用するソリューションの概要を説明します。

- PagerDuty で AWS Security Hub CSPM カスタムアクションを統合する方法
- でカスタムアクションを有効にする方法AWS Security Hub CSPM
- Security Hub CSPM でAWS Configルール評価を結果としてインポートする方法

について学ぶためのリソースAWS Security Hub CSPM

以下の資料は、AWS Security Hub CSPMソリューションとAWSお客様がサービスをどのように使用できるかを理解するのに役立ちます。

- AWS Security Hub CSPM 動画の説明
- Security Hub ユーザーガイド
- Security Hub API リファレンス
- オンボーディングウェビナー

また、AWSアカウントの 1 つで Security Hub CSPM を有効にし、サービスに関する実践的な経験を得ることをお勧めします。

パートナーの前提条件

との統合を開始する前にAWS Security Hub CSPM、次のいずれかの条件を満たす必要があります。

- AWSSelect Tier パートナー以上である。
- AWSISV パートナーパスに参加し、Security Hub CSPM 統合に使用する製品が AWSFoundational Technical Review (FTR) を完了しました。その後、製品には「Reviewed byAWS」バッジが付与されます。

また、相互秘密保持契約も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許可

AWS Security Hub CSPM では、 AWS APN パートナーから結果を受け取ることができます。パートナーの製品は、お客様のアカウントの内部または外部で実行される場合があります AWS 。お客様のアカウントの許可設定は、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 CSPM では、顧客はどのパートナーが顧客のアカウントに結果を送信できるかを常に制御します。お客様は、パートナーの許可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検出結果を送信できるようにするには、まず Security Hub CSPM 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。お客様が製品統合を管理する方法の詳細については、AWS Security Hub ユーザーガイドの「製品統合の管理」を参照してください。

顧客がパートナー製品をサブスクライブすると、Security Hub CSPM は自動的にマネージドリソースポリシーを作成します。このポリシーは、BatchImportFindingsAPI オペレーションを使用して顧客のアカウントの Security Hub CSPM に結果を送信するアクセス許可をパートナー製品に付与します。

Security Hub CSPM 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許可が含まれています。

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結果

このユースケースは、自分の AWS アカウントで製品をホストするパートナーを対象としています。AWS お客様のセキュリティ検出結果を送信するために、パートナーはパートナー製品アカウントから BatchImportFindings API オペレーションを呼び出します。

このユースケースで、お客様アカウントは、お客様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許可のみを必要とします。

パートナーアカウントで、BatchImportFindings API オペレーションをコールする IAM プリンシパルには、プリンシパルが BatchImportFindings をコールできる IAM ポリシーを持っている必要があります。

Security Hub CSPM でパートナー製品から顧客に結果を送信できるようにするには、次の 2 つのステップを実行します。

1. お客様は Security Hub CSPM 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 CSPM は、顧客の確認とともに正しいマネージド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 BatchImportFindings API オペレーションをコールします。

以下は、パートナーアカウントのプリンシパルに必要な Security Hub CSPM アクセス許可を付与する IAM ポリシーの例です。

JSON

```
{
    "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: お客様アカウントから送信された結果

このユースケースは、自分の AWS アカウントで製品をホストするが、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するパートナーを対象としています。お客様のアカウントから BatchImportFindings API オペレーションをコールします。

このユースケースでは、BatchImportFindings API オペレーションをコールするため、パートナーアカウントは、お客様のアカウントでお客様が管理する IAM ロールを引き受けます。

このコールはお客様のアカウントから行われます。したがって、マネージド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 CSPM マネージド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、顧客はパートナー製品に Security Hub CSPM に結果を送信するアクセス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お客様アカウント間のアカウント間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、お客様のアカウントのアカウント間ポリシー定義のパートです。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、アカウントにパートナー AWS へのアクセスを許可するときに、追加のセキュリティレイヤーを提供します。一意の識別子は、パートナーが適切なお客様アカウントを使用することを保証します。

パートナー製品がクロスアカウントロールを使用して Security Hub CSPM で顧客に結果を送信できるようにするには、次の 4 つのステップを実行します。

1. お客様、またはお客様に代わってクロスアカウントロールを使用するパートナーは、Security Hub CSPM で製品のサブスクリプションを開始します。
2. Security Hub CSPM は、顧客の確認とともに正しいマネージドリソースポリシーを生成します。
3. お客様は、クロスアカウントロールを手動で設定するか、 を使用します CloudFormation。クロスアカウントロールの詳細については、IAM ユーザーガイドの「第三者が所有する AWS アカウントへのアクセスを許可する」を参照してください。
4. 製品には、お客様のロールと外部 ID が安全に保存されます。

次に、製品は結果を Security Hub CSPM に送信します。

1. 製品は AWS Security Token Service (AWS STS) を呼び出して顧客ロールを引き受けます。
2. 製品は、引き受けたロールの一時的な認証情報を使用して、Security Hub CSPM で `BatchImportFindings` API オペレーションを呼び出します。

以下は、パートナーのクロスアカウントロールに必要な Security Hub CSPM アクセス許可を付与する IAM ポリシーの例です。

JSON

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

ポリシーの Resource 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、お客様がサブスクライブしているパートナー製品の結果のみを送信できます。

お客様ホスト: お客様アカウントから送信された結果

このユースケースは、お客様の AWS アカウントにデプロイされている製品を持つパートナーを対象としています。BatchImportFindings API は、お客様のアカウントで実行されるソリューションからコールされます。

このユースケースでは、パートナー製品に BatchImportFindings API をコールするための許可を追加で付与する必要があります。この許可の付与方法は、パートナーソリューションと、お客様のアカウントでの設定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、BatchImportFindings API オペレーションをコールする能力をインスタンスに付与する EC2 インスタンスロールが設定されている必要があります。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結果を送信できます。

このユースケースは、お客様が所有する製品の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同等です。

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

1. お客様は、 または別のデプロイツールを使用して CloudFormation、パートナー製品を自分の AWS アカウントに手動でデプロイします。
2. お客様は、Security Hub CSPM に結果を送信するときにパートナー製品で使用するために必要な 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、製品は Security Hub CSPM に結果を送信できるようになりました。

1. パートナー製品は AWS SDK または AWS CLI を使用して、Security Hub CSPM で BatchImportFindings API オペレーションを呼び出します。ポリシーがアタッチされているお客様のアカウント内のコンポーネントからコールします。
2. API コール中に、必要な一時的な認証情報が生成され、BatchImportFindings コールが成功します。

以下は、お客様のアカウントのパートナー製品に必要な Security Hub CSPM アクセス許可を付与する IAM ポリシーの例です。

JSON

```
{
    "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パートの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。セキュリティ検出結果を に送信する前に、これらのステップを完了する必要がありますAWS Security Hub CSPM。

1. APN パートナーチームまたは Security Hub CSPM チームとの契約を開始し、Security Hub CSPM のパートナーになることに関心を表明します。Security Hub CSPM 通信チャネルに追加する E メールアドレスを特定します。
2. AWSは、Security Hub CSPM パートナーオンボーディングマテリアルを提供します。
3. Security Hub CSPM パートナー Slack チャネルに招待され、統合に関する質問をすることができます。
4. APN パートナーの連絡先に、レビュー用に製品統合マニフェストの草案を提出します。

   製品統合マニフェストには、 との統合のためにパートナー製品の 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 CSPM。

   Security Hub CSPM コンソールのパートナープロバイダーページに表示される情報を Security Hub CSPM チームに提供します。また、Security Hub CSPM 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を提案するために使用されます。

   この製品統合マニフェストの初期バージョンに、完全な詳細は必要ありません。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、「製品統合マニフェスト」を参照してください。
5. Security Hub CSPM チームは、製品の製品 ARN を提供します。ARN を使用して、結果を Security Hub CSPM に送信します。
6. 統合を構築して、Security Hub CSPM に検出結果を送信または受信します。

   結果を ASFF にマッピングする

   Security Hub CSPM に結果を送信するには、結果を AWSSecurity Finding 形式 (ASFF) にマッピングする必要があります。

   ASFF は、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。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、結果の AWS Security Hub CSPM へ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。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、AWS Security Hub ユーザーガイドの「AWS Security Finding 形式 (ASFF)」を参照してください。

「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

所有AWSしているアカウントを使用して、統合のすべてのテストを完了できます。これにより、Security Hub CSPM での検出結果の表示を完全に可視化できます。また、セキュリティ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。

`BatchImportFindings` API オペレーションを使用して、新規および更新された検出結果を Security Hub CSPM に送信します。

Security Hub CSPM 統合の構築を通じて、 AWSでは、統合の進行状況について APN パートナーの連絡先に常に通知することをお勧めします。また、APN パートナーの連絡先に統合に関する疑問点を問い合わせることもできます。

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

7. Security Hub CSPM 製品チームとの統合をデモンストレーションします。この統合は、Security Hub CSPM 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。

   お客様が統合に慣れている場合は、Security Hub CSPM チームが承認し、プロバイダーとしてお客様を出品します。
8. レビュー用の最終マニフェストを AWSに提供します。
9. Security Hub CSPM チームは、Security Hub CSPM 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 CSPM 統合を促進するために、追加のマーケティング作業を行います。「ゴートゥマーケット活動」を参照してください。

    少なくとも、Security Hub CSPM では、次のアセットを指定することをお勧めします。
    - 機能する統合のデモビデオ (最大で 3 分間)。動画はマーケティング目的で使用され、AWSYouTube チャンネルに投稿されます。
    - Security Hub CSPM の初回コールスライドデッキに追加するワンスライドアーキテクチャ図。

ゴートゥマーケット活動

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、AWS Security Hub CSPM 統合の説明と宣伝に役立てることもできます。

Security Hub CSPM 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、レビューと承認のために APN パートナーマネージャーにドラフトを送信します。これにより、全員がメッセージングの方向性を一致させることができます。

AWSパートナーネットワーク (APN) パートナーは、APN Partner Marketing Central と Market Development Funds (MDF) プログラムを使用してキャンペーンを作成し、資金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 CSPM パートナーページのエントリ

Security Hub CSPM パートナーとして承認されると、ソリューションがAWS Security Hub CSPM パートナーページに表示されます。

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 `<securityhub-pms@amazon.com>` 宛てのメールの場合があります。

- ソリューションの簡単な説明、Security Hub CSPM との統合、Security Hub CSPM との統合がお客様に提供する値。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、統合AWS、より具体的には Security Hub CSPM 統合に固有である必要があります。顧客体験と、統合を使用するときに顧客が受け取る値に焦点を当てる必要があります。
- 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、the section called “パートナーページのロゴ” を参照してください。

プレスリリース

承認済みパートナーとして、必要に応じてウェブ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 によって承認される必要がありますAWS。

プレスリリースを公開する前に、APN パートナーマーケティング、Security Hub CSPM リーダーシップ、およびAWS外部セキュリティサービス (ESS) によるレビューAWSのために に送信する必要があります。プレスリリースには、ESS のVPの提案した引用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ーを APN ブログに投稿するのにも役立ちます。ブログエントリーは、お客様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。統合起動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キーこと

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含まれますか?

パートナーの投稿は教育的であり、AWS お客様に適切なトピックに深い専門知識を提供する必要があります。

理想的な長さは 1,500 語以下です。読者は、可能なことを教える深く教育的なコンテンツを重視します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、アドバンストまたはプレミアティアパートナーのみです。サービス提供などの APN プログラム指定を持つ選択パートナーには例外があります。

各パートナーの投稿は年間 3 回の制限があります。数万の APN パートナーを抱え、AWS はそのカバレッジにおいて公平でなければなりません。

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。

ブログ投稿が投稿されるまでにどれくらいの時間がかかりますか?

ブログ投稿の最初のドラフト全文を送信した後、編集には 4 週間から 6 週間かかります。

APN ブログを書き込みのはなぜですか?

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、 が公開したストーリーは世界中の顧客に影響を与えるAWS可能性があります。
- 可視性 — APN ブログは、 で最も読まれているブログの 1 つAWSで、影響を受けたトラフィックを含め、2019 年のページビュー数は 179 万件です。
- ビジネス – 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Connect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% 以上のリーダーがこのテクニカルコンテンツを見ています。
- お客様は、200 レベル以上のストーリーで、AWS でどのように動作するかや、APN パートナーがどのようにお客様のビジネス上の問題を解決したかを示しているものを価します。
- 技術エキスパートまたは内容領域エキスパート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ています。

スリックシートまたはマーケティングシート

スリックシートは、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概説する 1 ページのドキュメントです。

統合用のスリックシートを作成する場合は、Security Hub CSPM チームにコピーを送信します。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日本語ガイド

製品、統合アーキテクチャ、共同顧客のユースケースの概要を示すホワイトペーパーまたは電子書籍を作成する場合は、Security Hub CSPM チームにコピーを送信します。Security Hub CSPM パートナーページに追加されます。

ウェビナー

統合に関するウェビナーを実施する場合は、ウェビナーの記録を Security Hub CSPM チームに送信します。チームがパートナーページからリンクします。

チームは、Security Hub CSPM のサブジェクト分野のエキスパートにウェビナーに参加してもらうこともできます。

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。このような動画を動画プラットフォームアカウントに投稿すると、Security Hub CSPM チームが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 CSPM 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 CSPM 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 CSPM 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と提供された情報を評価するために、Security Hub CSPM チームは を使用しますthe section called “製品の準備チェックリスト”。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 バージョンは、 AWS Security Hub CSPM 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 CSPM 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

以下のユースケースは、 AWS Security Hub CSPM さまざまな目的で を設定するのに役立ちます。

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。

との統合に関するユースケースを記述するには AWS Security Hub CSPM、次の質問に答えてください。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 CSPM 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早期フィードバックを取得するには、APN パートナーまたは Security Hub CSPM 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 CSPM コンサルティングパートナーの場合は必須です。

Security Hub CSPM での作業に 2 つの顧客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 CSPM チームはそれらをどこにもアドバタイズしません。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。

- 顧客が Security Hub CSPM をブートストラップするのをどのように支援しますか? 例えば、顧客がプロフェッショナルサービス、Terraform モジュール、または CloudFormation テンプレートを使用するのを手伝ったことがありますか?
- Security Hub CSPM の運用と拡張をどのように支援しますか? 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 CSPM に結果を送信する場合に必要です。

Security Hub CSPM に送信する検出結果については、次の情報を入力します。

- JSON や XML などのネイティブ形式での結果
- 結果を AWS Security Finding Format (ASFF) に変換する方法の例

統合をサポートするために ASFF の更新が必要な場合は、Security Hub CSPM チームにお問い合わせください。

アーキテクチャ

検出結果を Security Hub CSPM との間で送受信する場合に必要です。

Security Hub CSPM との統合方法について説明します。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。

- どのような 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 CSPM に検出結果を送信する場合、顧客 AWS アカウントまたは自分の AWS アカウントから検出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?

設定

検出結果を Security Hub CSPM との間で送受信する場合に必要です。

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、 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 CSPM に結果を送信する場合に必要です。

顧客ベース全体で、1 か月あたり何件の検出結果の更新 (平均と最大) を Security Hub CSPM に送信すると予想されますか? 桁の推定値は許容されます。

レイテンシー

Security Hub CSPM に結果を送信する場合に必要です。

結果をどのくらい早くバッチ処理して Security Hub CSPM に送信しますか? つまり、製品で検出結果が作成されてから Security Hub CSPM 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 CSPM とのすべての統合に必要です。

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

複数の製品を Security Hub CSPM と統合する場合は、製品ごとに個別の説明を指定できますが、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 CSPM とのすべての統合に必要です。

少なくとも、Security Hub CSPM パートナーページの Learn More ハイパーリンクに使用する URL を指定する必要があります。これは、製品と Security Hub CSPM 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 CSPM と統合すると、1 つのランディングページを作成できます。Security Hub CSPM では、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 CSPM 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 CSPM 統合に必要です。

Security Hub CSPM パートナーページに表示するロゴへの 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 CSPM コンソールのロゴ

すべての統合に必要です。

Security Hub CSPM コンソールに表示するライトモードとダークモードのロゴへの URLs 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。

- 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 CSPM 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 CSPM 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 CSPM 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連絡先と通信します。

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 CSPM に結果を送信する場合に推奨されます。

Security Hub CSPM 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 CSPM コンソール情報

次の情報を含む JSON テキストを AWS Security Hub CSPM チームに提供します。Security Hub CSPM 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 CSPM 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。 タイプ: 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 CSPM コンソールに表示されるプロバイダーの会社名。

フィールド	必要	説明
		タイプ: 文字列 最大長: 16 文字
`description`	はい	Security Hub CSPM コンソールに表示されるプロバイダーの会社の説明。 タイプ: 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 CSPM に検出結果を送信するか、Security Hub CSPM から検出結果を受信するか、または検出結果を送受信するかを示します。

フィールド	必要	説明
		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 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。 タイプ: 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、サポートされていないのはどれですか? つまり、Security Hub CSPM コンソールのパートナーページで、Security Hub CSPM がオプションとして表示しないのはどのリージョンですか? タイプ: 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、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。 のリージョンコード AWS GovCloud (US) は `us-gov-west-1` (AWS GovCloud (米国西部) の場合) と `us-gov-east-1` (AWS GovCloud (米国東部) の場合) 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主要 AWS アカウント番号。 Security Hub CSPM に結果を送信する場合、指定するアカウントは、結果の送信元に基づきます。 • 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。 • 顧客の AWS アカウントから。この場合、Security Hub CSPM 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 CSPM チームにお問い合わせください。 Security Hub CSPM からのみ結果を受け取る場合、このアカウント番号は必要ありません。 タイプ: 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主要 AWS アカウント番号 (製品が利用可能な場合 AWS GovCloud (US))。 Security Hub CSPM に結果を送信する場合、指定するアカウントは、結果の送信元に基づきます。 • 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。 • 顧客の AWS アカウントから。この場合、Security Hub CSPM 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 CSPM チームにお問い合わせください。 Security Hub CSPM からのみ結果を受け取る場合、このアカウント番号は必要ありません。 タイプ: 文字列

フィールド	必要	説明
chinaAccountNumber	いいえ	中国リージョンの製品の主要 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 CSPM に結果を送信する場合、指定するアカウントは、結果の送信元に基づきます。 • 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。 • 顧客の AWS アカウントから。この場合、Security Hub CSPM 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 CSPM チームにお問い合わせください。 Security Hub CSPM 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任意のアカウントになります。 タイプ: 文字列
name	はい	Security Hub CSPM コンソールに表示するプロバイダーの製品の名前。 タイプ: 文字列 最大長: 24 文字

フィールド	必要	説明
`description`	はい	Security Hub CSPM コンソールに表示するプロバイダーの製品の説明。 タイプ: 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。 タイプ: 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。選択内容は Security Hub CSPM 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。カテゴリが見つからないと思われる場合は、Security Hub CSPM 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`

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

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

フィールド	必要	説明
`configurationUrl`	はい	Security Hub CSPM 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、GitHub ページなど、お客様が管理するウェブページでホストされます。 タイプ: 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 • 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

AWS Security Hub CSPM 統合に必要な資料を準備するときは、以下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 CSPM が Security Hub CSPM のお客様に利用可能になる前に、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

AWS Security Hub CSPM コンソールに表示されるロゴのガイドライン

ロゴを AWS Security Hub CSPM コンソールに表示するには、以下のガイドラインに従ってください。

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

背景色

透過

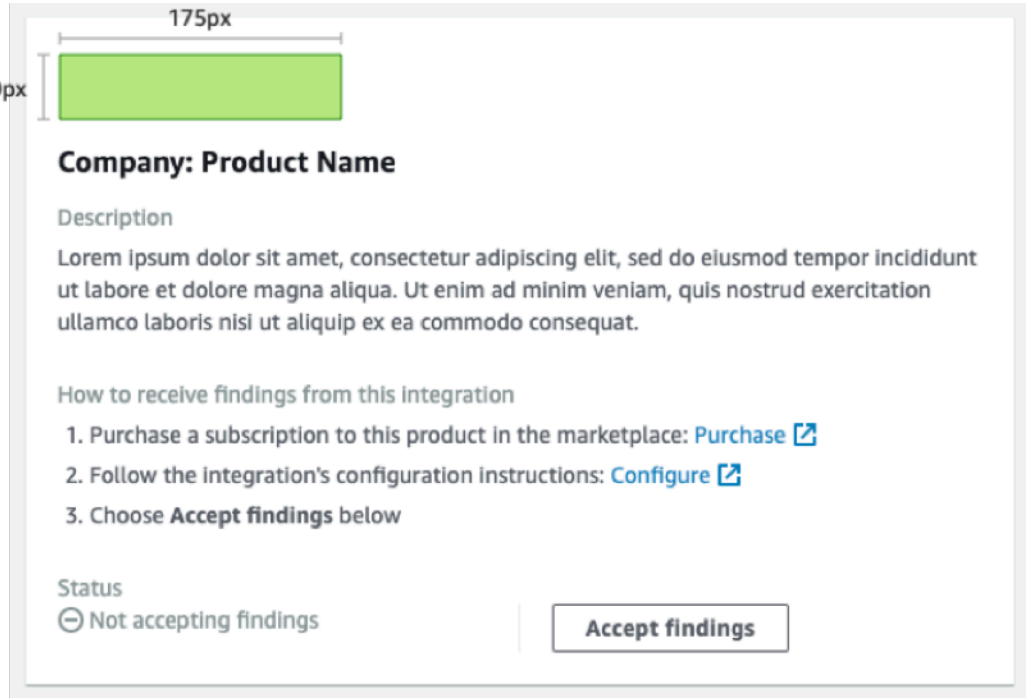
サイズ

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。

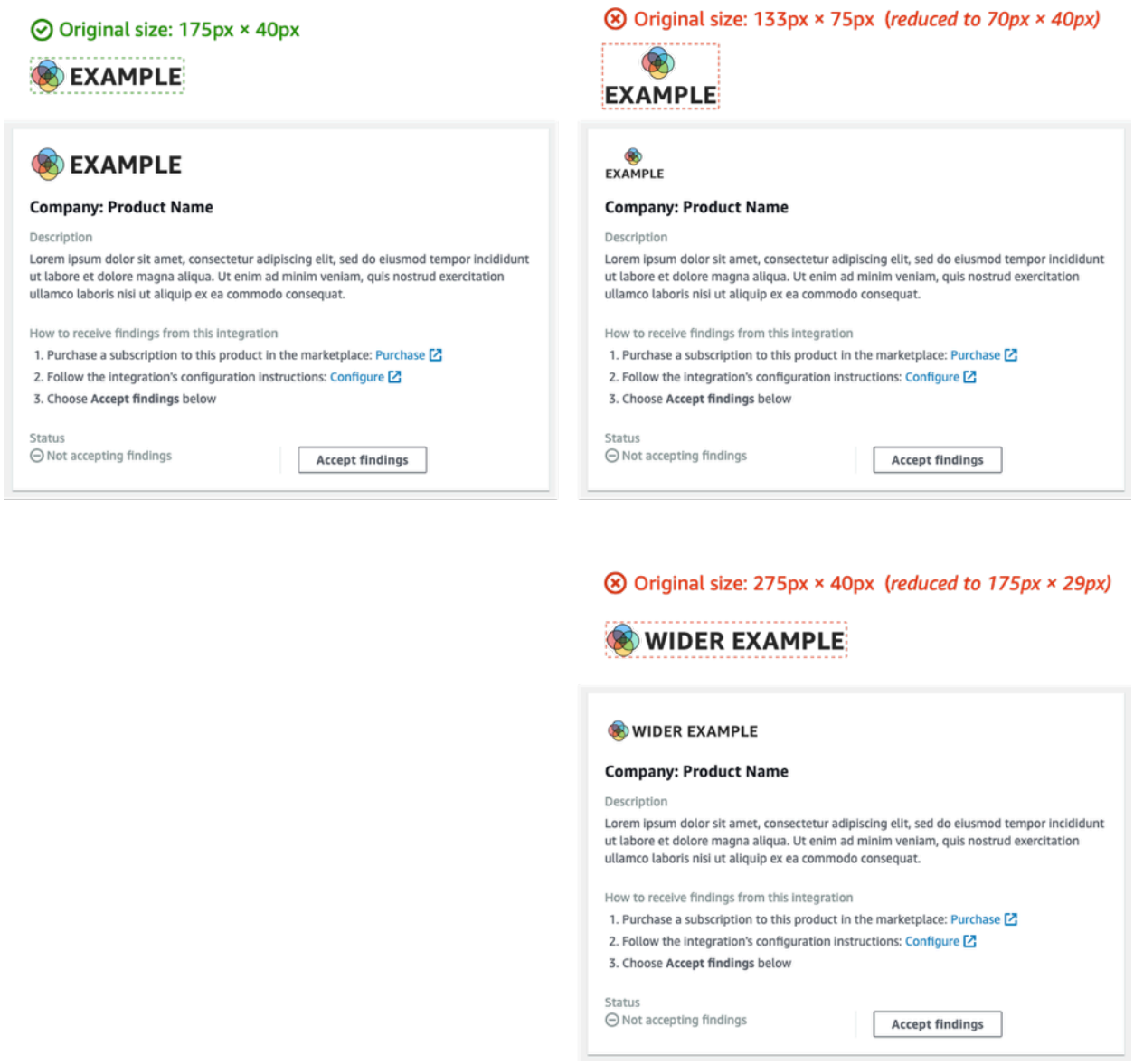
長方形の口ゴが最適です。

次の図は、Security Hub CSPM コンソールに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。



口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 CSPM コンソールでの口ゴの表示方法に影響します。

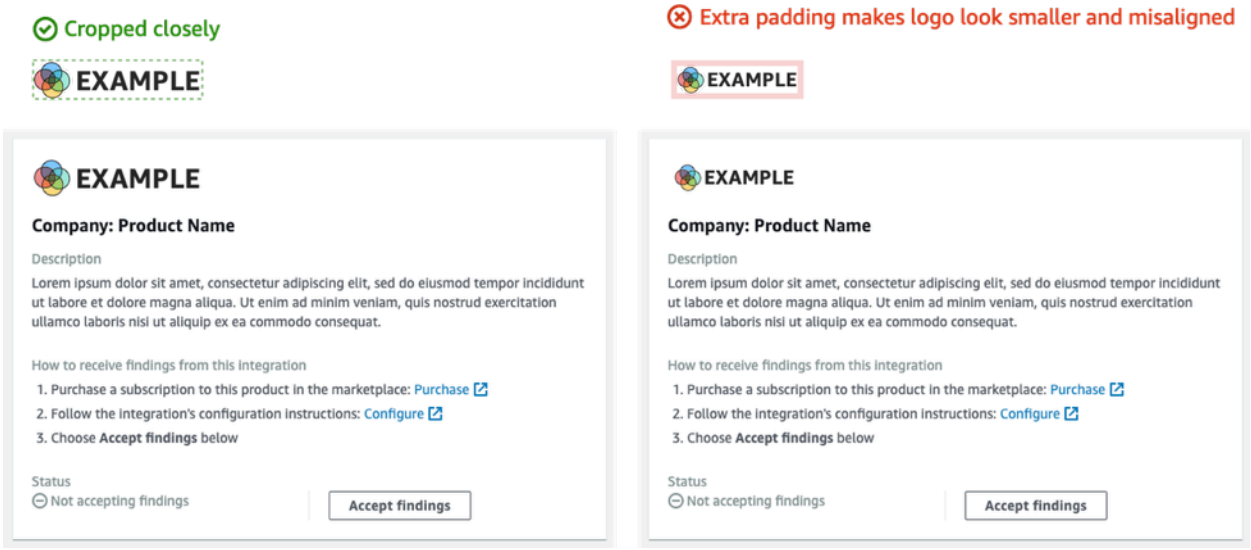
次のイメージは、理想的なサイズを使用した口ゴの表示と、幅広または背の高い口ゴを比較しています。



切り取り

ロゴイメージをできるだけ近くで切り取ってください。余分なパディングはいりません。

次のイメージは、近くで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。



結果の作成と更新に関する教義

の検出結果の作成と更新の計画を立てるときは AWS Security Hub CSPM、次の原則に留意してください。

結果を特定して、お客様が簡単にアクションを実行できるようにします。

お客様は、対応と修復アクションを自動化して、結果を他の結果と相関させたいと考えています。これをSupportするには、結果に次の特性が必要です。

- 通常、単一またはプライマリリ出典を処理する必要があります。
- 単一の結果タイプが必要です。
- 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。

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、お客様がその結果に対してアクションを実行することは困難です。

すべての検出結果を AWS Security Finding 形式 (ASFF) にマッピングします。お客様が Security Hub CSPM を信頼できるソースとして信頼できるようにします。

お客様は、ネイティブの検出結果形式のすべてのフィールドが Security Hub CSPM ASFF でも表されることを期待しています。

お客様は、すべてのデータを Security Hub CSPM バージョンの検出結果に含めたいと考えています。データがないと、セキュリティ情報の中心的なソースとして Security Hub CSPM への信頼が失われます。

結果の冗長性を最小限に抑えます。結果のボリュームでお客様を圧倒しないでください。

Security Hub CSPM は一般的なログ管理ツールではありません。実行可能性が高く、顧客が他の検出結果に直接対応、修復、または関連付けることができる検出結果を Security Hub CSPM に送信する必要があります。

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。

重要値スコアやリ出典識別子など、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結果で、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。

お客様が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す。

お客様は、特定の結果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、お客様は、アカウントのタイプまたは結果が関連付けられているリ出典のタイプに基づいて、メモ、タグを追加し、重要値スコアを調整できるようにしたいとします。

検出結果を AWS Security Finding Format (ASFF) にマッピングするためのガイドライン

結果を ASFF にマッピングするには、以下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、AWS Security Hub ユーザーガイドの「AWS Security Finding 形式 (ASFF)」を参照してください。

識別情報

`SchemaVersion` は常に `2018-10-08` です。

`ProductArn` は、 がユーザー AWS Security Hub CSPM に割り当てる ARN です。

`Id` は、Security Hub CSPM が検出結果のインデックス作成に使用する値です。他の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 は Id と同じ、または Amazon GuardDuty ディテクタ ID、 AWS Config レコーダー ID、または IAM アクセスアナライザー ID など、論理の離散単位を参照するものです。

Title および Description

Title は影響を受けるリ出典に関する情報をいくつか含める必要があります。Title は 256 文字に制限されています。

より長い詳細情報を Description に追加します。Description は 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

FindingProviderFields.Types の結果タイプの情報を提供します。

Types は ASFF のタイプ分類 と一致する必要があります。

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

BatchImportFindings をコールするたびにそれぞれの結果について CreatedAt および UpdatedAt を送信する必要があります。

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 および LastObservedAt はシステムが結果を観察したときと一致する必要があります。この情報をレコードしない場合は、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 形式と一致します。

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

Severity

FindingProviderFields.Severity オブジェクトの重要値情報には、次のフィールドが含まれます。

Original

システムの重要値値。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

検出結果の重要度を示す必須の Security Hub CSPM インジケータ。許容値は、次のとおりです。

- INFORMATIONAL – 問題は見つかりませんでした。
- LOW - この問題は独自のアクションを必要としません。
- 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 – さらなる危害を防ぐために、問題を直ちに修復する必要があります。

準拠している結果は、常に Label が INFORMATIONAL に設定されている必要があります。INFORMATIONAL 検出結果の例は、合格したセキュリティチェックの結果と修正された AWS Firewall Manager 検出結果です。

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、重要値で結果を並べ替えることがよくあります。結果の重要値を HIGH または CRITICAL に設定するときは慎重に行ってください。

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 CSPM コンソールで結合されます。

Remediation.Recommendation.Text は結果詳細の 修復 セクションに表示されます。これは、Remediation.Recommendation.Url の値にハイパーリンクされています。

現在、Security Hub CSPM 標準、IAM Access Analyzer、Firewall Manager の検出結果のみが、検出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を表示します。

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 を提供できる場合、SourceUrl のみを使用します。それ以外の場合は、マッピングから省略します。

Security Hub CSPM 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 CSPM コンソールで公開されています。

Malware, Network, Process, ThreatIntelIndicators

該当する場合、Malware、Network、Process、またはThreatIntelIndicators を使用します。これらの各オブジェクトは Security Hub CSPM 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、Resource.Details.AwsEc2Instance の EC2 インスタンスの詳細を提供します。その EC2 インスタンスの関連する Malware、Network、および ThreatIntelIndicator オブジェクトを提供します。

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出典と結果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。値は最大 64 文字の文字列です。

Name は検査済みの脅威インテリジェンスまたは研究者の情報である必要があります。

Path

マルウェアへのパス。値は 512 文字以内の文字列です。Path は次の場合を除き、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場合、Path は S3:// 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、Path は Git 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 OBSERVED | REMOVAL_FAILED | REMOVED です。

結果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、Malware.State が REMOVED の場合、結果タイトルと説明に、パス上にあるマルウェアを製品が除去したことを反映させる必要があります。

Malware.State が OBSERVED の場合、結果タイトルと説明に、パス上にあるこのマルウェアに製品が遭遇したことを反映させる必要があります。

Type

マルウェアのタイプを示します。指定できる値は、ADWARE | BLENDED_THREAT | BOTNET_AGENT | COIN_MINER | EXPLOIT_KIT | KEYLOGGER | MACRO | POTENTIALLY_UNWANTED | SPYWARE | RANSOMWARE | REMOTE_ACCESS | ROOTKIT | TROJAN | VIRUS | WORM です。

に追加の値が必要な場合はType、Security Hub CSPM チームにお問い合わせください。

Network

Network は単一オブジェクトです。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、以下のガイドラインに従います。

デスティネーションと出典情報

デスティネーションと出典は、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。攻撃に関する結果のネットワーク情報を記述しているとき、使用するのがより困難です。

通常、出典は攻撃が発生した場所ですが、以下に示すような他の出典がある可能性があります。ドキュメントで出典を説明し、結果タイトルと詳細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、出典は攻撃者ですが、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。デスティネーションは EC2 インスタンスの公開 IPv4 アドレスです。Direction は IN です。

- 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、出典は 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 は OUT です。また、Malware および ThreatIntelIndicators を提供します。

Protocol

Protocol は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) のメンバー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、デスティネーションと出典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のみ提供します。

Direction

Direction は常に AWS ネットワーク境界に対して相対的です。

- IN は AWS 、(VPC、サービス) を入力していることを意味します。
- OUT は、 AWS ネットワーク境界を出ることを意味します。

Process

Process は単一オブジェクトです。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、以下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。最大 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 および ParentPid は Linux 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 を区別できます。

タイムスタンプ (**LaunchedAt** および **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 は最大 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、DOMAIN | EMAIL_ADDRESS | HASH_MD5 | HASH_SHA1 | HASH_SHA256 | HASH_SHA512 | IPV4_ADDRESS | IPV6_ADDRESS | MUTEX | PROCESS | URL です。

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以下に示します。

- 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。これを FireEye のブログから知りました。

  Type を PROCESS に設定します。また、プロセスの Process オブジェクトを作成します。
- メールフィルターによって、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 ThreatIntelIndicator オブジェクトを作成します。1 つのオブジェクトは、DOMAIN のためです。もう 1 つは、HASH_SHA1 のためです。
- Yara ルール (Loki、Fenrir、awss3VirusScan、BinaryAlert) でマルウェアが見つかりました。

  2 つの ThreatIntelIndicator オブジェクトを作成します。1 つはマルウェアのためです。もう 1 つは、HASH_SHA1 のためです。

Resources

Resources の場合、可能な限り提供されているリ出典タイプと詳細フィールドを使用します。Security Hub CSPM は、ASFF に新しいリソースを常に追加しています。ASFF の変更の月次ログを受け取るには、<securityhub-partners@amazon.com> に問い合わせます。

モデル化されたリ出典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 にマッピングします。

ASFF でモデル化されていないリ出典については、Type を Other に設定します。詳細については、「Details.Other」を使用してください。

AWS 検出結果以外のOtherリソースタイプを使用することもできます。

ProductFields

Resources の別のキュレーションフィールドまたは ThreatIntelIndicators、Network、または Malware などの説明的なオブジェクトを使用できない場合、ProductFields のみを使用します。

ProductFields を使っている場合、この決定には厳密な根拠を提供する必要があります。

コンプライアンス

結果がコンプライアンスに関連している場合、Compliance のみを使用します。

Security Hub CSPM は、コントロールに基づいて生成する検出結果Complianceに を使用します。

Firewall Manager はコンプライアンスに関連しているため、Compliance を使用します。

制限されているフィールド

これらのフィールドは、お客様が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、FindingProviderFields オブジェクト内のフィールドにマップします。最上位フィールドにはマッピングしないでください。

- Confidence – サービスに同様の特徴がある場合、または結果が 100% 残っている場合にのみ、信頼スコア (0 ~ 99) を含めます。
- Criticality – 重要値スコア (0 ~ 99) は、結果に関連するリ出典の重要性を表すことを目的としています。
- RelatedFindings – 同じリ出典または結果タイプに関連する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。関連する検出結果を特定するには、Security Hub CSPM に既に存在する検出結果の検出結果識別子を参照する必要があります。

BatchImportFindings API 使用のガイドライン

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

- 結果に関連付けられているアカウントを使って BatchImportFindings をコールする必要があります。関連付けられたアカウントの識別子は、結果の AwsAccountId 属性の値です。
- 可能な最大のバッチを送信します。Security Hub CSPM は、バッチあたり最大 100 の検出結果、検出結果あたり最大 240 KB、バッチあたり最大 6 MB の検出結果を受け入れます。
- 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、結果がコンプライアンスの内外に移動するときに結果の更新を送信できるように、結果状態も必要です。
- 文字列の最大長およびその他の制限については、AWS Security Hub ユーザーガイドの「AWS Security Finding 形式 (ASFF)」を参照してください。

製品の準備チェックリスト

AWS Security Hub CSPM と APN パートナーチームは、このチェックリストを使用して、統合を起動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、検出結果を AWS Security Finding 形式 (ASFF) にマッピングすることに関連しています。

パートナーの結果データはすべて 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。

モデル化されたリ出典タイプ、Network、Malware、または ThreatIntelIndicators などのキュレートされたフィールドを使用します。

必要に応じて、他のものを Resource.Details.Other または ProductFields にマッピングします。

パートナーは **AwsEc2instance**、**AwsS3Bucket**、および **Container** などの **Resource.Details** フィールド使っていますか? パートナーは **Resource.Details.Other** を使って、ASFF でモデル化されていないリ出典の詳細を定義していますか?

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トされたリ出典に対して提供されたフィールドを使用します。

直接一致しない場合にのみ、リ出典に関連するその他の情報を Resource.Details.Other にマッピングします。

パートナーは値を **UserDefinedFields** にマッピングしますか?

UserDefinedFields を使用しません。

Resource.Details.Other または ProductFields などの別のキュレーションフィールドの使用を検討します。

パートナーは他の ASFF フィールドにマッピングできる **ProductFields** に情報をマッピングしますか?

バージョニング情報、製品固有の重要値の結果、またはキュレートされたフィールドまたは Resources.Details.Other にマッピングできないその他の情報など、製品固有の情報には ProductFields のみを使用します。

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

FirstObservedAt タイムスタンプは、製品内で結果が観察された時刻をレコード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ピングします。

パートナーは、更新する結果を除いて、各結果識別子に対して生成された一意の値を提供しますか?

Security Hub CSPM のすべての検出結果は、検出結果識別子 (Id 属性) でインデックス化されます。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、結果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ますか?

GeneratorID は結果 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り、結果を論理的にリンクできる必要があります。

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、必要な結果タイプの名前空間を使用していますか? パートナーは、結果タイプに推奨される結果タイプのカテゴリーまたは分類子を使用していますか?

結果タイプの分類基準は、製品が生成する結果の近くにマッピングする必要があります。

AWS Security Finding 形式で概説されている第 1 レベルの名前空間が必要です。

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

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

製品が NetFlow 情報をキャプチャする場合は、Network フィールドにマッピングします。

プロセスデータがある場合、パートナーは **Process** フィールドのパートナーキャプチャ処理 (PID) 情報を処理しますか?

製品がプロセス情報をキャプチャする場合は、Process フィールドにマッピングします。

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

製品がマルウェア情報をキャプチャする場合は、Malware フィールドにマッピングします。

脅威インテリジェンスデータがある場合、パートナーは **ThreatIntelIndicators** フィールドに脅威インテリジェンス情報をキャプチャしますか?

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、ThreatIntelIndicators フィールドにマッピングします。

パートナーは、結果の信頼値評価を提供していますか? その場合、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、結果のリ出典 ID に標準 ID または ARN を使用していますか?

AWS リソースを識別する場合の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、標準リ出典 ID を使用します。

統合の設定と特徴

これらの質問は、統合のセットアップと日常的な特徴に関連しています。

パートナーは、Terraform などの Security Hub CSPM との統合をデプロイするための infrastructure-as-code (IaC) テンプレートを提供しています AWS Cloud Development Kit (AWS CDK)か CloudFormation?

お客様のアカウントから結果を送信したり、CloudWatch Eventsを使用して結果を使用する統合の場合は、何らかの形式の IaC テンプレートが必要です。

CloudFormation が推奨されますが、 AWS CDK または Terraform を使用することもできます。

パートナー製品には、Security Hub CSPM との統合のためのワンクリック設定がコンソールにありますか?

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、自動的にリ出典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。

パートナーは値の結果のみを送信しますか?

通常、Security Hub CSPM のお客様にのみ、セキュリティ価値のある検出結果を送信してください。

Security Hub CSPM 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 CSPM に送信しないでください。

パートナーは、お客様あたり 1 日にいくつ、どのくらいの頻値 (平均とバースト) で結果が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 CSPM の負荷を計算するために、一意の検出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、ある結果が `ThreatIntelIndicators` のみ入力され、別は `Resources.Details.AWSEc2Instance` のみ入力された場合、これらは 2 つの一意の結果です。

パートナーは 4xx および 5xx エラーを適切に処理して、スロットルされず、すべての結果を後で送信できるようにしていますか?

現在、`BatchImportFindings` API オペレーションに 30 ~ 50 TPS バーストレートがあります。4xx または 5xx エラーが返された場合は、後で合計で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。これを行うには、デッドレターキューまたは Amazon SNS や Amazon SQS などの別の AWS メッセージングサービスを使用します。

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

元の結果 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。

結果を提供する場合は、BatchUpdateFindings オペレーションを使って、結果を更新しないでください。このオペレーションは、お客様のみが使用する必要があります。調査し、結果に基づいてアクションを実行する場合、BatchUpdateFindings のみを使用します。

パートナーは、以前に送信され、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結果 ID を保持するメカニズムが必要です。

パートナーは、既存の結果の結果 ID で **BatchImportFindings** オペレーションをコールすることにより、結果を更新しますか?

結果を更新するには、同じ結果 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 オペレーションはお客様のみが使用する必要があります。

パートナーは、**BatchUpdateFindings** API を使って結果を更新しますか?

結果に対してアクションを起こす場合は、BatchUpdateFindings オペレーションを使って、特定のフィールドを更新できます。

パートナーは、検出結果が作成されてから製品から Security Hub CSPM に送信されるまでのレイテンシーの量に関する情報を提供しますか?

Security Hub CSPM でできるだけ早く検出結果が表示されるように、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顧客アカウントから Security Hub CSPM に結果を送信する場合、これは正常に実証されていますか? 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 CSPM に結果を送信する場合、これは正常に実証されていますか?

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 CSPM にハートビートの検出結果を提供しますか?

統合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、結果タイプ `Heartbeat` を使用します。

これは、製品アカウントから結果を送信する場合に重要です。

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

本番稼働前の検証中に、Security Hub CSPM 製品チームの AWS アカウントに検出結果の例を送信する必要があります。これらの例は、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、静的なウェブページ、Wiki、ドキュメントの読み取り、またはその他の専用形式としてウェブサイトでホストされる必要があります。

GitHub でドキュメントをホストすることは、専用のウェブサイト要件を満たしていません。

パートナードキュメントには、Security Hub CSPM 統合を設定する手順が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、ユースケースの詳細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、送信した結果の理論的根拠を提供していますか?

送信する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、ウイルス対策の検出結果を生成する場合がありますが、脆弱性とマルウェアの検出結果を Security Hub CSPM にのみ送信します。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。

パートナードキュメントには、パートナーが結果を 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結果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。

パートナードキュメントには結果を更新した場合に、パートナーが結果を更新する方法についてのガイダンスが記載されていますか?

お客様に状態を保持し、冪等性を保証し、結果を最新の情報で上書きする方法についての情報を提供します。

パートナードキュメントには、結果のレイテンシー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、Security Hub CSPM でできるだけ早く検出結果が表示されるようにします。

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、重要値スコアが ASFF の重要値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?

`Severity.Original` を `Severity.Label` にマッピングする方法情報を提供します。

たとえば、重要値がレターグレード (A、B、C) の場合、レターグレードを重要値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。

パートナードキュメントには、信頼値評価の理論的根拠が記載されていますか?

信頼値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。

AIや機械学習から派生した静的に入力された信頼値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。

パートナードキュメントには、パートナーがSupportされているリージョンとSupportされていないリージョンが記載されていますか?

SupportされているリージョンとSupportされていないリージョンを明記し、お客様がどの地域で統合を試みてはいけないかを知ることができるようにします。

製品コード情報

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

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

アカウント識別子の長さは 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。

商品説明には 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、スペースを含め、200 文字以内でなければなりません。

設定リンクは、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必要があります。メインのウェブサイトまたは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) は製品の AWS Marketplace 出品につながりますか?

購入リンクを指定する場合は、 AWS Marketplace エントリ用である必要があります。Security Hub CSPM は、 によってホストされていない購入リンクを受け付けません 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 つの製品カテゴリーを提供できます。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。

会社および製品の名前は有効で正しいですか?

会社名は 16 文字未満である必要があります。

製品名は 24 文字未満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 CSPM パートナーページの製品説明は、スペースを含めて 700 文字以内ですか?

Security Hub CSPM パートナーページでは、スペースを含めて最大 700 文字しか使用できません。

チームは長い説明を編集して短くします。

Security Hub CSPM パートナーのページロゴは 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公開アクセス可能な URL を指定します。

Security Hub CSPM パートナーページの「Learn more hyperlink」は、統合に関するパートナーの専用ウェブ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のウェブサイトやドキュメント情報につなげてはいけません。

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ウェブページに移動する必要があります。

パートナーは、統合の使用方法に関するデモまたは手順ビデオを提供していますか?

デモまたは統合のチュートリアルビデオはオプションですが、推奨されています。

AWS Partner Network ブログ記事は、パートナーとそのパートナー開発マネージャーまたはパートナー開発担当者と共にリリースされていますか?

AWS Partner Network ブログ投稿は、パートナー開発マネージャー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の VP から引用を受け取ることができます。この引用は、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、 AWS パートナーネットワークブログの外で統合を紹介することができます。

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、統合を紹介できます。

Security Hub CSPM チームから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。

パートナーは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、 AWS セキュリティマーケティングリーダーと協力して、公式ソーシャルメディアチャネルを使用して AWS ウェビナーの詳細を共有できます。

AWS Security Hub CSPMパートナーに関するよくある質問

AWS Security Hub CSPM との統合の設定と保守についてよくある質問を次に示します。

1. Security Hub CSPM 統合の利点は何ですか?
   - 顧客満足度 – Security Hub CSPM と統合する一番の理由は、顧客からのリクエストがあるためです。

     Security Hub CSPM は、AWSお客様のためのセキュリティおよびコンプライアンスセンターです。これは、AWSセキュリティとコンプライアンスの専門家がセキュリティとコンプライアンスの状態を理解するための最初の停止として設計されています。

     お客様の声に耳を傾けます。Security Hub で結果を確認したいかどうかがわかります。
   - 検出の機会 – リストへのリンクなど、Security Hub CSPM コンソール内で認定された統合を持つパートナーを昇格させますAWS Marketplace。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。
   - マーケティングの機会 – 承認された統合を持つベンダーは、ウェビナーへの参加、プレスリリースの発行、スリックシートの作成、AWS顧客への統合のデモンストレーションを行うことができます。
2. パートナーにはどのような種類がありますか?
   - Security Hub CSPM に結果を送信するパートナー
   - Security Hub CSPM から検出結果を受け取るパートナー
   - 結果を送受信するパートナー
   - お客様が環境で Security Hub CSPM を設定、カスタマイズ、使用できるようにするコンサルティングパートナー
3. Security Hub CSPM とのパートナー統合は、どのように高レベルで機能しますか?

   顧客アカウント内または自分のAWSアカウントから検出結果を収集し、検出結果の形式をAWSSecurity Finding Format (ASFF) に変換します。次に、これらの検出結果を適切な Security Hub CSPM リージョンエンドポイントにプッシュします。

   CloudWatch Events を使用して、Security Hub CSPM から検出結果を受信することもできます。
4. Security Hub CSPM との統合を完了するための基本的なステップは何ですか?

   a. パートナーマニフェスト情報を送信します。

b. Security Hub に結果を送信する場合は、Security Hub CSPM で使用する製品 ARNs を受け取ります。

c. 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 CSPM との間で結果を送受信するためのアーキテクチャを定義します。the section called “結果の作成と更新に関する教義” に概説されている教義に従います。

e. お客様向けのデプロイフレームワークを構築します。たとえば、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、お客様に設定手順を提供します。

g. お客様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 CSPM チームへの統合をデモンストレーションします。

i. 認可のためにマーケティング情報を送信します (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、スリックシート)。

5. パートナーマニフェストを送信するプロセスはどのようなものですか? また、AWSサービスが Security Hub CSPM に結果を送信する場合

   マニフェスト情報を Security Hub CSPM チームに送信するには、`<securityhub-partners@amazon.com>` を使用します。

   7 暦日以内に製品 ARN が発行されます。

6. Security Hub CSPM にはどのような種類の検出結果を送信する必要がありますか?

   Security Hub CSPM の料金は、取り込まれた検出結果の数に一部基づいています。このため、お客様に値を提供しない結果を送信することは控えるべきです。

   たとえば、パート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. Security Hub CSPM に結果を送信するためのさまざまなアプローチは何ですか?

   主なアプローチは次のとおりです。

   - `BatchImportFindings` オペレーションを使用して、独自の指定されたAWSアカウントから結果を送信します。
   - お客様アカウント内から `BatchImportFindings` オペレーションで結果を送信します。assume-ロール 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。

`BatchImportFindings` の使用に関する全体的なガイドラインについては、「the section called "`BatchImportFindings` API 使用のガイドライン"」を参照してください。

8. 結果を収集して Security Hub CSPM リージョン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?

   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、パートナーは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、CloudFormationスクリプトとしてデプロイできる Python アプリケーションを構築します。このスクリプトは、パートナーの結果を顧客環境から収集し、ASFF に変換して、Security Hub CSPM リージョンエンドポイントに送信します。

   他のパートナーは、結果を Security Hub CSPM にプッシュするワンクリックエクスペリエンスを提供する完全なウィザードを構築します。

9. Security Hub CSPM に結果の送信を開始するタイミングを知るにはどうすればよいですか?

   Security Hub CSPM は `BatchImportFindings` API オペレーションの部分的なバッチ認可をサポートしているため、すべての顧客に対してすべての検出結果を Security Hub CSPM に送信できます。

   一部のお客様が Security Hub CSPM にまだサブスクライブしていない場合、Security Hub CSPM はこれらの検出結果を取り込みません。バッチに含まれる許可済みの調査結果のみを取り込みます。

10. 顧客の Security Hub CSPM インスタンスに結果を送信するには、どのようなステップを完了する必要がありますか?

    a. 正しい IAM ポリシーがあ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 (リ出典ポリシー) を有効にします。`EnableImportFindingsForProduct` API オペレーションまたは 統合 ページのいずれかを使用します。お客様がこれを行うか、アカウント間ロールを使用してお客様の代理として行うことができます。

    c. 結果の `ProductArn` が製品の公開 ARN であることを確認します。

    d. 結果の `AwsAccountId` がお客様のアカウント ID であることを確認します。

    e. Security AWSFinding Format (ASFF) に従って、結果に不正な形式のデータがないことを確認します。たとえば、必須フィールドは入力され、無効な値がないかです。

    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結果を送信するには、どの IAM 権限がある必要がありますか?

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

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 action: 'securityhub:BatchImportFindings' および resource: *<productArn and/or productSubscriptionArn>* に制約することができます。

同じアカウント内のリ出典は、リ出典ポリシーを必要とせずに IAM ポリシーで設定できます。

BatchImportFindings の発信者から IAM ポリシーの問題を除外するには、次のように IAM ポリシーを設定します。

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

発信者の Deny ポリシーに何もないことを必ずチェックします。それが動作するようになった後、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、お客様 (またはお客様に代わってアカウント間ロールを持つパートナー) が製品サブスクリプションを確立する必要があります。これをコンソールから行うには、統合ページを使用します。これを API から行うには、EnableImportFindingsForProduct API オペレーションを使用します。

製品サブスクリプションは、パートナーからの結果をお客様から受信または送信することを許可するリ出典ポリシーを構築します。詳細については、「ユースケースと許可」を参照してください。

Security Hub CSPM には、パートナー用に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。

ではBATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT、製品 ARN にリストされているアカウントからのみ、Security Hub CSPM に結果を送信できます。

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。

13. お客様が管理者アカウントを構築し、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。お客様は各メンバーアカウントをサブスクライブする必要がありますか? または、お客様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出典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メンバーに基づいて、すべてのメンバーアカウントに権限が構築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 CSPM が生成し、検出結果の送信に使用する一意の識別子です。Security Hub CSPM 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 CSPM に送信するすべての検出結果の一部である必要があります。製品 ARN がない結果は削除されます。製品 ARN は次の形式を使用します。

`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 CSPM 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送信によって決定されます。リージョンコードを除き、製品 ARN に関連付けられている情報を変更することはありません。リージョンコードは、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パートとして、「ホーム」アカウント ID を送信します。このアカウント ID は製品 ARN にロックされています。

Security Hub CSPM 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を使用して、それらのリージョンの製品 ARNs が自動的に生成されます。

また、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、公式の公開製品 ARN を受け取る前に、独自の開発アカウント内で結果のインポートをテストできます。

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

検出結果は AWSSecurity Finding 形式 (ASFF) で提供する必要があります。詳細は、AWS Security Hub ユーザーガイド の「AWS Security Finding 形式 (ASFF)」を参照してください 。

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ことです。`ProductFields` および `Resource.Details.Other` のようなカスタムフィールドにより、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 CSPM リージョン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リストはどこから入手できますか?

Security Hub CSPM エンドポイントリストを参照してください。

18.リージョン間結果を送信することはできますか?

Security Hub CSPM は、Amazon GuardDuty、Amazon Macie、Amazon Inspector などのネイティブAWSサービスの検出結果のクロスリージョン送信をまだサポートしていません。顧客が許可した場合、Security Hub CSPM は異なるリージョンから結果を送信できないようにします。

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 のリ出典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?

BatchImportFindings の 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。この制限まで、できるだけ多くの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 CSPM にサブスクライブされていない場合、バッチ全体が失敗します。これは、API Gateway ベースライン認可モデルの制限です。

「the section called “BatchImportFindings API 使用のガイドライン”」を参照してください。

20構築した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他の誰かが構築した結果に更新を送信することはできますか?

はい。お客様が BatchUpdateFindings API オペレーションへのアクセス権を付与した場合、そのオペレーションを使用して特定のフィールドを更新できます。このオペレーションは、お客様、SIEM、チケットシステム、Security オーケストレーション, オートメーション, 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結果はどのようにして期限切れになりますか?

Security Hub CSPM 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、期限切れの検出結果は Security Hub CSPM OpenSearch クラスターから消去されます。

同じ検出結果 ID で検出結果を更新し、期限切れになると、Security Hub CSPM に新しい検出結果が作成されます。

お客様は CloudWatch Events を使用して、Security Hub CSPM から検出結果を移動できます。そうすることで、すべての結果を、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。

一般的に、Security Hub CSPM では、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お勧めします。

23.Security Hub CSPM はどのようなスロットルを設定しますか?

Security Hub CSPM は `GetFindings` API コールをスロットリングします。検出結果にアクセスするための推奨アプローチは CloudWatch Events を使用することです。

Security Hub CSPM は、API Gateway および Lambda 呼び出しによって適用される以外の内部サービス、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 CSPM に送信される検出結果のタイムラインまたはレイテンシー SLAs または期待値は何ですか?

目的は、初期結果と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。検出結果は、作成後 5 分以内に Security Hub CSPM に送信する必要があります。

25.Security Hub CSPM から結果を受け取るにはどうすればよいですか?

結果を受け取るには、次のいずれかの方法を使用します。

- すべての結果が CloudWatch Eventsに自動的に送信されます。お客様は、特定の CloudWatch Eventsルールを構築して、SIEM や S3 バケットなどの特定のターゲットに結果を送信できます。この機能はレガシー `GetFindings` API オペレーションに取って代わりました。
- CloudWatch Events をカスタムアクションに使用します。Security Hub CSPM を使用すると、コンソール内から特定の検出結果または検出結果のグループを選択し、アクションを実行できます。たとえば、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、顧客が Security Hub CSPM 内で実行するアラートトリアージワークフローの一部になります。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、それらの特定の結果に対して CloudWatch イベントが構築されます。この機能を利用して、お客様がカスタムアクションの一パートとして使用するための CloudWatch Eventsルールとターゲットを構築できます。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 CloudWatch Eventsに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。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です。

  などのカスタムアクション API オペレーションを使用して`CreateActionTarget`、製品で使用できるアクションを自動的に作成できます (CloudFormationテンプレートの使用など) 。また、CloudWatch Eventsルール API オペレーションを使用して、カスタムアクションに関連付けられた対応する CloudWatch イベントルールを構築できます。CloudFormationテンプレート

を使用して CloudWatch Events ルールを作成して、Security Hub CSPM からすべての検出結果または特定の特性を持つすべての検出結果を自動的に取り込むこともできます。

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 CSPM パートナーになるための要件は何ですか?

    顧客へのサービス提供の一環として Security Hub CSPM がどのように使用されるかを示す必要があります。

    Security Hub CSPM の使用について説明するユーザードキュメントが必要です。

    MSSP が検出結果プロバイダーである場合は、Security Hub CSPM への検出結果の送信をデモンストレーションする必要があります。

    MSSP が Security Hub CSPM からのみ結果を受け取る場合、少なくとも適切な CloudWatch Events ルールを設定するためのテンプレートが必要ですCloudFormation。

27. MSSP 以外の APN コンサルティングパートナーが Security Hub CSPM 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の場合は、Security Hub CSPM パートナーになることができます。特定のお客様が次を行うのにどのように支援したかについて、2 つのプライベートな導入事例を送信する必要があります。

    - お客様が必要とする IAM アクセス許可を持つ Security Hub CSPM を設定します。
    - コンソールのパートナーページの設定手順を使用して、既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 CSPM に接続するのに役立ちます。
    - カスタム製品統合でお客様を支援します。
    - お客様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構築します。
    - 修復プレイブックを構築します。
    - Security Hub CSPM コンプライアンス標準に沿ったクイックスタートを構築します。これらは Security Hub CSPM チームによって検証される必要があります。

    導入事例は、パブリックに共有可能である必要はありません。

28. Security Hub CSPM との統合を顧客とデプロイする方法に関する要件は何ですか?

    Security Hub CSPM 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の観点から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AWS環境にデプロイする場合は、 CloudFormationテンプレートを活用して統合を簡素化する必要があります。パートのパートナーはワンクリック統合を構築しており、これは強く推奨されています。

29.ドキュメントの要件は何ですか?

CloudFormationテンプレートの使用を含め、製品と Security Hub CSPM の統合とセットアップのプロセスを説明するドキュメントへのリンクを提供する必要があります。

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 CSPM との統合のユースケース
- 送信された結果の平均ボリューム
- 統合アーキテクチャ
- Support対象とSupport対象外のリージョン
- 結果が構築されてから Security Hub に送信されるまでのレイテンシー
- 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

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、お客様が注目とアクションを最も必要とする結果とリ出典の優先順位付けに役立ちます。

Security Hub CSPM には `CreateInsight` API オペレーションがあります。CloudFormationテンプレートの一部として、顧客アカウント内でカスタムインサイトを作成できます。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。構築できるのはマネージドインサイトのみです。

32料金モデルは何ですか?

Security Hub CSPM の料金情報を参照してください。

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

リージョンus-west-2として を使用して、提供された製品 ARN を使用して Security Hub CSPM デモアカウントに結果を送信します。結果には、ASFF の AwsAccountId フィールドにデモアカウント番号を含める必要があります。デモアカウント番号を取得するには、Security Hub CSPM 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**BatchImportFindings** はどのようなエラーまたは成功メッセージを提供しますか?

Security Hub CSPM は、認可のレスポンスと のレスポンスを提供しますBatchImportFindings。より明確な成功、違反、エラーメッセージが開発されています。

35出典サービスはどのようなエラー処理を担当していますか?

出典サービスは、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、およびアラーミングを処理する必要があります。また、Security Hub CSPM フィードバックメカニズムを介して送信されるフィードバックやエラーメッセージを処理する必要もあります。

36.一般的な問題の解決策は何ですか?

AuthorizerConfigurationException は AwsAccountId または ProductArn のどちらかが不正なことが原因です。

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 は正確に 12 桁でなければなりません。
- ProductArn 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 CSPM チームによって提供された製品 ARNs に含まれていたものから変更されません。

AccessDeniedException は間違ったアカウントとの間で結果が送信された場合、またはアカウントに ProductSubscription がない場合に発生します。エラーメッセージには、product または product-subscription のリ出典タイプの ARN が含まれます。このエラーは、アカウントコール間中にのみ発生します。AwsAccountId および ProductArn の同じアカウントの自分のアカウントで BatchImportFindings をコールする場合、オペレーションは IAM ポリシーを使用し、ProductSubscriptions とは無関係です。

使用するお客様のアカウントと製品アカウントが実際のメンバーアカウントであることを確認してください。パートのパートナーは、製品 ARN から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 `BatchImportFindings` のコールを試します。それ以外の場合は、他のお客様のアカウント、または自分の製品アカウントの `ProductSubscriptions` を構築します。結果のインポートを試みたお客様のアカウントの `ProductSubscriptions` は構築されません。

37.質問、コメント、バグはどこに送信すれば良いですか?

`<securityhub-partners@amazon.com>`

38.グローバル AWS サービスに関する項目について結果を送信するリージョンはどれですか? たとえば、IAM 関連の結果はどこに送信すればよいですか?

結果が検出されたのと同じリージョンに結果を送信します。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、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 CSPM 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、元の結果を送信したすべてのリージョンに、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、Security Hub CSPM コンソールに表示するロゴのライトモードとダークモードバージョンの両方をパートナーが提供する必要があることを示しました。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 CSPM では、ISV AWSパートナーパスに参加し、AWS基盤技術レビュー (FTR) を完了した統合製品を使用するパートナーも許可されるようになりました。以前は、すべての統合パートナーが AWSSelect Tier パートナーである必要がありますでした。	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 CSPM で新しい検出結果を作成し、既存の検出結果を更新するための新しいガイドラインのセットを追加しました。	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では、 AWSとの統合を確立する方法について説明しますAWS Security Hub CSPM。	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。