Cisco Secure Cloud Analytics

初期導入ガイド

目次

展開の概要

Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud）は、可視化および高度脅威検出サービスです。Secure Cloud Analytics により、オンプレミスネットワークまたはパブリッククラウドからトラフィックを収集してホストを識別し、通常のホスト動作を把握し、デバイスの動作が組織のネットワークセキュリティに関連する方法で変化したときにアラートを生成することができます。Secure Cloud Analytics の販促資料では、このデータ分析はダイナミック エンティティ モデリングと呼ばれています。

> Secure Cloud Analytics PoV は、より一般的なセキュリティ アセスメント ツールであるセキュリティ オンライン可視性アセスメント（SOVA）と同じではありません。

シスコでは、Secure Cloud Analytics を「サービスとして」提供しており、Secure Cloud Analytics およびすべての関連サービスを運用および保守しています。お客様は、オンプレミスに展開された仮想アプライアンスを介したクラウド プラットフォームへのトラフィック情報のアップロード、またはアクセスを許可するクラウド セキュリティ ポリシーのアップロードを担当します。

Secure Cloud Analytics でダイナミック エンティティ モデリングを使用し、ホストおよび他のエンティティのトラフィックの完全なベースラインモデルを作成するには、36 日間の初期学習期間が必要です。この初期学習期間中には、約半数のアラート タイプを使用できます。学習期間が進み、システムがより多くのデータを収集すると、追加のアラートが使用可能になります。36 日目を過ぎると、システムは完全にベースライン化され、すべてのアラートが使用可能になります。

機能の概要

Secure Cloud Analytics は、オンプレミスおよびクラウドベースのネットワーク展開をモニターする Software as a Service（SaaS）ソリューションです。ネットワークトラフィックに関する情報を収集することによって、トラフィックに関する観測内容が作成され、トラフィック パターンに基づいてネットワーク エンティティのロールが自動的に識別されます。Secure Cloud Analytics は、この情報を他の脅威インテリジェンス（Talos など）のソースと組み合わせて使用してアラートを生成します。このアラートは、本質的に悪意のある可能性がある動作の存在を示す警告を構成します。Secure Cloud Analytics は、このアラートとともに、ネットワークおよびホストの可視性と、収集したコンテキスト情報を提供します。このコンテキスト情報により、アラートを調査して悪意のある動作の原因を特定するためのより優れた基盤が得られます。

展開

Secure Cloud Analytics は、ネットワークを支える次の 2 つの展開タイプをサポートしています。

- **パブリック クラウド モニターリング**（旧 Stealthwatch Cloud パブリック クラウド モニターリング）：ネイティブクラウドログの取り込みによるワークロードのエージェントレス モニターリング、および脅威の検出と設定のモニターリングを提供する API 統合
- **プライベート ネットワーク モニターリング**（旧 Stealthwatch Cloud プライベート ネットワーク モニタ—リング）：ネットワークフローデータ、SPAN/ミラーポートトラフィック、および NGFW ログ情報を取り込むための仮想 Cisco Secure Cloud Analytics センサー（旧 Stealthwatch Cloud センサー）の展開。

どちらか一方を展開するか、両方を同時に展開して、単一の Secure Cloud Analytics Web ポータル UI で両方の設定とアラートを確認できます。Web ポータルでは、同じページからすべての センサーとモニター対象のクラウド展開が表示されるため、モニターリングの状態をすばやく確認できます。

動的エンティティモデリング

Secure Cloud Analytics は、ダイナミック エンティティ モデリングを使用してネットワークの状態を追跡します。Secure Cloud Analytics のコンテキストにおけるエンティティとは、ネットワーク上のホストやエンドポイント、AWS 展開内の Lambda 関数といった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングでは、エンティティが送信するトラフィックとエンティティのネットワーク上でのアクティビティに基づいて、エンティティに関する情報が収集されます。Secure Cloud Analytics は、エンティティと、エンティティが通常送信するトラフィックのタイプを判別するために、ネイティブ クラウド ログ データと業界標準のテレメトリ、およびユーザーのクラウドプロバイダ API を取り込むことができます。エンティティはトラフィックを送信しつづけ、異なるトラフィックを送信する可能性があるため、Secure Cloud Analytics は、各エンティティの最新モデルを維持するために、これらのモデルを経時的に更新します。

この情報から、Secure Cloud Analytics は次のことを識別します。

- エンティティのロール：これは、エンティティが通常行うことの記述子です。たとえば、エンティティが、一般に電子メール サーバーに関連付けられるトラフィックを送信する場合、Secure Cloud Analytics は、そのエンティティに電子メール サーバー ロールを割り当てます。エンティティは複数のロールを実行する場合があるため、ロールとエンティティの関係は多対 1 である可能性があります。

- エンティティの観測内容：これは、ネットワーク上でのエンティティの動作に関する事実（外部 IP アドレスとのハートビート接続、ウォッチリスト上のエンティティとのやり取り、別のエンティティとの間で確立されたリモート アクセス セッションなど）です。観測内容それ自体は、それらが表すものの事実を超えた意味を持ちません。一般的なお客様は、何千もの観測内容と少数のアラートを持つ可能性があります。

アラートと分析

ロール、観測内容、およびその他の脅威インテリジェンスの組み合わせに基づいて Secure Cloud Analytics が生成するアラートは、潜在的な悪意のある動作をシステムによって識別されたものとして表す実用的な項目です。

上記の例で言えば、[新しい内部デバイス（New Internal Device）] 観測内容だけでは、潜在的な悪意のある動作は構成されません。ただし、時間の経過とともに、エンティティがドメイン コントローラと一致するトラフィックを送信する場合、システムではそのエンティティにドメイン コントローラ ロールが割り当てられます。その後、そのエンティティが、以前に接続を確立していない外部サーバーへの接続を確立し、異常なポートを使用して大量のデータを転送すると、システムは、[新しい大規模接続（外部）（New Large Connection（External））] 観測内容と [例外ドメインコントローラ（Exceptional Domain Controller）] 観測内容をログに記録します。その外部サーバーが Talos ウォッチリストに登録されているものと識別された場合、これらすべての情報の組み合わせにより Secure Cloud Analytics はこのエンティティの動作に関するアラートを生成し、悪意のある動作を調査して対処するように促します。

Secure Cloud Analytics Web ポータル UI でアラートを開くと、システムがアラートを生成した原因となっている観測内容を確認できます。これらの観測内容から、関連するエンティティに関する追加のコンテキスト（それらが送信したトラフィック、外部脅威インテリジェンス（利用可能な場合）など）も確認できます。また、エンティティが関係性を持っていたその他の観測内容やアラートを確認したり、この動作が他の潜在的に悪意のある動作に結び付いているかどうかを判断することもできます。

クイックスタート – Secure Cloud Analytics の展開

ここでは、Secure Cloud Analytics を展開する方法の概要と、それを使用してネットワーク上で発生する可能性のある悪意のある動作を検査する方法を示します。

初回サインアップ

1. https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html にアクセスして Secure Cloud Analytics にサインアップします。
2. AWS クラウドを導入している場合は、https://aws.amazon.com/marketplace/pp/B075MWZVBM にアクセスして Secure Cloud Analytics にサインアップします。
3. 招待電子メールが届くのを待ちます。サインアップしたタイミングにより、数時間から最大 12 時間で届きます。
4. 招待電子メールを受信したら、招待リンクをクリックしてカスタマー Web ポータルにアクセスし、初期管理者ログイン クレデンシャルを作成します。

> 招待リンクを使用できるのは 1 回だけで、初期管理者ログイン クレデンシャルを作成した後は無効になります。

モニターするネットワークのタイプを決定します。

- オンプレミス展開をモニターする場合、プライベートネットワークのモニタリングの設定の詳細については、「**プライベートネットワークのモニタリング展開と初期設定**」を参照してください。
- パブリック クラウド ネットワークをモニターする場合、パブリッククラウドのモニタリングの設定の詳細については、「**パブリッククラウドのモニタリング展開と初期設定**」を参照してください。
- オンプレミス展開とパブリック クラウド ネットワークの両方をモニターする場合、プライベートネットワークのモニタリングの設定の詳細については「**プライベートネットワークのモニタリング展開と初期設定**」を参照し、パブリッククラウドのモニタリングの設定の詳細については「**パブリッククラウドのモニタリング展開と初期設定**」を参照してください。

プライベートネットワークのモニタリング展開と初期設定

1. オンプレミス ネットワークをモニターするセンサーを展開します。詳細については、「**プライベートネットワークのモニタリング Sensor 導入の考慮事項**」および「**プライベートネットワークのモニタリング Sensor センサーメディアのインストールと設定**」を参照してください。センサーを Kubernetes クラスタに展開する方法の詳細については、「**プライベートネットワークのモニタリング Kubernetes 向け統合**」を参照してください。
2. 招待電子メールから作成された初期管理者ログイン クレデンシャルを使用して Secure Cloud Analytics Web ポータル UI にログインします。
3. センサー設定を確認して完了します。特定のサブネットをモニターして Syslog に出力するように設定を更新し、SNMP レポートを設定します。詳細については、「**プライベートネットワークのモニタリング Sensor設定**」を参照してください。

必要な追加のシステム設定の詳細については、「**推奨システム設定**」を参照してください。

パブリッククラウドのモニタリング展開と初期設定

1. Secure Cloud Analytics サービスがフロー ログを取得することを許可するようにクラウド展開を設定します。AWS 向けの PCM 設定の詳細については、「**パブリッククラウドのモニタリング Amazon Web Services 向けの設定**」を参照してください。GCP 向けの PCM 設定の詳細については、「**パブリッククラウドのモニタリング Google Cloud Platform 向けのパブリック クラウド モニターリング設定**」を参照してください。Azure 向けの PCM 設定の詳細については、「**パブリッククラウドのモニタリング Microsoft Azure の設定**」を参照してください。その他のクラウド展開に関する詳細については、support@obsrvbl.com にお問い合わせください。
2. 招待電子メールから作成された初期管理者ログイン クレデンシャルを使用して Secure Cloud Analytics Web ポータル UI にログインします。
3. パブリッククラウドのモニタリングの設定を確認して完了します。詳細については、「**パブリッククラウドのモニタリング Amazon Web Services 向けの設定**」、「**パブリッククラウドのモニタリング Google Cloud Platform 向けのパブリック クラウド モニターリング設定**」、および「**Secure Cloud Analytics Azure との統合**」を参照してください。

必要な追加のシステム設定の詳細については、「**推奨システム設定**」を参照してください。

推奨システム設定

1. アラート生成のためにシステムの機密性（サブネットの機密性とアラートの優先順位を含む）を設定します。
    - サブネットの機密性が高いほど、システムはアラートを生成するために低いしきい値を必要とします。詳細については、「**サブネット設定**」を参照してください。
    - 同様に、アラートの優先順位が高いほど、システムはアラートを生成するために低いしきい値を必要とします。詳細については、「**アラート優先順位設定**」を参照してください。
2. ユーザー アカウントを設定します。詳細については、「**ユーザーおよびサイト管理**」を参照してください。

オプションのシステム設定を続行するか、システムの使用を開始します。

- オプションのアラート生成設定（IP スキャナとサードパーティ ウォッチリスト、国のブラックリストなど）の詳細については、「**オプションのシステム設定**」を参照してください。
- Secure Cloud Analytics Web ポータル UI の使用の詳細については、「**Web ポータルの使用**」を参照してください。

オプションのシステム設定

1. 外部インテリジェンスを Secure Cloud Analytics を取得し、アラート生成を改善するように、サードパーティ ウォッチリストを設定します。詳細については、「**サードパーティ ウォッチリストの設定**」を参照してください。
2. 国のブラックリストを設定し、システムがどの国に関する観測内容を生成するかを定義します（システムがそれらの国へのトラフィックを検出する場合）。詳細については、「**ウォッチリスト設定**」を参照してください。
3. 既知のネットワークスキャナと承認済みのネットワークスキャナに関する IP スキャナ ホワイトリスト ルールを設定します。詳細については、「**IP スキャナルールの設定**」を参照してください。

Secure Cloud Analytics Web ポータル UI の使用の詳細については、「**Web ポータルの使用**」を参照してください。

Web ポータルの使用

1. Secure Cloud Analytics Web ポータル UI にログインします。

   > 招待電子メールから作成した初期管理者ログイン クレデンシャルを使用してログインするか、作成した別のユーザーとしてログインすることができます。

2. Secure Cloud Analytics のメイン ダッシュボードを確認します。このダッシュボードには、オープン アラート、エンティティ数、および最新のトラフィック統計情報が表示されます。詳細については、「**ダッシュボードの概要**」を参照してください。
3. [アラート（Alerts）] メニュー オプションからすべてのアラートを確認します。詳細については、「**アラートの概要**」を参照してください。
4. アラートに関連するエンティティに関するコンテキストと、関連する観察内容を確認することによって、アラートを調査し、アラートのステータスをクローズにして、そのアラートが役立つものかどうかをマークします。詳細については、「**アラートの詳細**」、「**観測内容の概要**」、および「**アラートのワークフロー**」を参照してください。
5. システムのモデルを表示して、傾向を特定し、ネットワークのトラフィックを確認します。詳細については、「**調査の概要**」を参照してください。
6. モニター対象のトラフィックと使用状況に関するレポートの詳細については、レポートメニューを参照してください。詳細については、「**[レポート（Report）] メニュー**」を参照してください。

プライベートネットワークのモニタリングの展開と設定

ここでは、次のようなプライベートネットワークのモニタリング センサー の展開と設定について説明します。

- システムの前提条件、ネットワーク環境の前提条件、および センサー 展開の推奨事項
- 物理アプライアンスまたは仮想マシンへの センサー のインストール、センサー の設定、およびセンサーの Web ポータルへの接続の手順
- 用の Kubernetes クラスタの設定手順 プライベートネットワークのモニタリング

プライベートネットワークのモニタリング Sensor 導入の考慮事項

センサー を展開する際は、NetFlow などのフローデータを収集するように、またはネットワーク上のルータやスイッチからミラー化されるネットワークトラフィックを取得するようにセンサーを設定できます。フローデータの収集とミラー化されたネットワークトラフィックの取得の両方を行うように センサー を設定することもできます。

フローデータを収集するように センサー を設定する場合、詳細については、「**フローデータを収集するSensorの設定**」を参照してください。

ミラーまたは SPAN ポートからのトラフィックを取得するように センサー を設定する場合、トラフィックをミラー化するためのネットワークデバイスの設定の詳細については、「**ネットワーク デバイス設定**」を参照してください。

> Sensor バージョン 4.0 以降では、拡張 NetFlow テレメトリを収集できます。これにより、Secure Cloud Analytics では新しいタイプの観測内容とアラートを生成できます。詳細については、『Secure Cloud AnalyticsConfiguration Guide for Enhanced NetFlow』[英語] を参照してください。

Sensor 前提条件

次の要件が満たされている場合に、センサー を物理アプライアンスまたは仮想マシンにインストールできます。

コンポーネント	最小要件
ネットワーク インターフェイス	Secure Cloud Analytics サービスに情報を渡すための、制御インターフェイスとして指定された、1 つ以上のネットワーク インターフェイス 任意で、ミラーポートを経由するネットワークトラフィックを複製するネットワークデバイスからのトラフィックを取得するように センサー を設定する場合は、ミラーインターフェイスとして指定された 1 つ以上のネットワークインターフェイスが必要です。

RAM	2 GB
CPU	2 つ以上のコア
記憶領域	32 GB
インストール ファイルのアップロード（物理アプライアンス）	インストール .iso ファイルをアップロードするには次のいずれかが必要です。 • 1 つの USB ポートと、USB フラッシュドライブ • 1 つの光学ディスクドライブと、書き込み可能な光学ディスク（CD-R ディスクなど） 仮想マシンは、追加の要件なしで .iso ファイルから直接起動できます。

パフォーマンスの評価指標と推奨事項については、このホワイトペーパーを参照してください。

指定されたミラー インターフェイスについては、次の点に注意してください。

- ミラー インターフェイスは、宛先へのすべてのインバウンドおよびアウトバウンド送信元トラフィックのコピーを受信します。ピークトラフィックが センサー のミラー インターフェイス リンクの容量より小さいことを確認してください。
- 多くのスイッチでは、ミラー ポートの宛先に過剰なトラフィックが設定されている場合、送信元インターフェイスからのパケットがドロップされます。

追加の仮想マシンの設定

センサー が仮想マシンとして展開されている場合、ミラーポートまたは SPAN ポートからのトラフィックを取得する予定のときは、2 つ目のネットワークインターフェイスで仮想ホストとネットワークが無差別モードに設定されていることを確認してください。

VMware ハイパーバイザ上で仮想マシンを実行している場合、無差別モードの詳細および設定手順については、VMware ナレッジベースを参照してください。VLAN ID を 4095 に設定する必要がある場合があります。

VirtualBox で仮想マシンを実行している場合は、[ネットワーク（Network）] 設定からミラー インターフェイス用のアダプタを選択し、[詳細オプション（Advanced Options）] で無差別モードを [許可（Allow）] に設定します。詳細については、仮想ネットワークに関する VirtualBox のドキュメントを参照してください。

プライベートネットワークのモニタリング Sensor アクセス要件

物理アプライアンスまたは仮想マシンは、インターネットを介して特定のサービスにアクセスできる必要があります。センサー と外部インターネットの間の次のトラフィックを許可するようにファイアウォールを設定します。

トラフィックのタイプ	必須	IP アドレスまたはドメインとポート
センサー の制御インターフェイスから Amazon Web Services でホストされている Secure Cloud Analytics サービスへのアウトバウンド HTTPS トラフィック	○	• 可変
Linux OS および関連する更新をダウンロードするための、センサー の制御インターフェイスから Ubuntu Linux サーバーへのアウトバウンドトラフィック	○	• us.archive.ubuntu.com:443/TCP • us.archive.ubuntu.com:80/TCP
ホスト名解決のための、センサー の制御インターフェイスから DNS サーバーへのアウトバウンドトラフィック	○	• [local DNS server]:53/UDP
リモートトラブルシューティング アプライアンスからのインバウンドトラフィック センサー	不可	• 54.83.42.41:22/TCP

ネットワーク デバイス設定

トラフィックのコピーをミラー化して センサー に渡すようにネットワークスイッチまたはルーターを設定できます。

> センサー は通常のトラフィックフローの外側にあるため、トラフィックに直接影響する可能性はありません。Web ポータルの UI で行った設定変更は、トラフィック フローのあり方ではなくアラートの生成に影響します。アラートに基づいてトラフィックを許可またはブロックするには、ファイアウォール設定を更新します。

ネットワーク スイッチの製造元と、ミラー化トラフィックを設定するためのリソースについては、次の資料を参照してください。

製造元	ミラー化トラフィック名	設定例
Cisco	スイッチ ポート アナライザ（SPAN）	『Configuration Examples and TechNotes』
Juniper	ポート ミラー	EX シリーズ スイッチで従業員のリソース使用をローカルでモニターリングするためのポートミラーリングの設定例については、Juniper の TechLibrary ドキュメントを参照してください。
NETGEAR	ポート ミラー	ポートミラーリングの例と、マネージドスイッチでの動作については、Netgear のナレッジベースのドキュメントを参照してください。

ZyXEL	ポート ミラー	ZyXEL スイッチでミラーリングを使用する方法については、ZyXEL のナレッジベースのドキュメントを参照してください。
その他	モニター ポート、アナライザ ポート、タップ ポート	複数のメーカーのスイッチリファレンスについては、Wireshark の wiki ドキュメントを参照してください。

ネットワーク テスト アクセス ポイント（タップ）デバイスを展開してトラフィックのコピーを センサー に渡すこともできます。ネットワーク タップの製造元と、ネットワーク タップを設定するためのリソースについては、次の資料を参照してください。

製造元	デバイス名	資料
NetOptics	ネットワーク タップ	ドキュメントおよびその他の情報については、ixia のリソースページを参照してください。
Gigamon	ネットワーク タップ	ドキュメントおよびその他の情報については、Gigamon のリソースページおよびナレッジページを参照してください。

フロー設定

NetFlow データを渡すようにネットワークデバイスを設定する必要があります。シスコネットワークデバイスでの NetFlow の設定の詳細については、https://configurenetflow.info/ または https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf を参照してください。

Cisco Defense Orchestrator およびSensorの展開

Cisco Defense Orchestrator（CDO）を使用して Firepower アプライアンスをネットワークに展開する場合は、シスコのセキュリティ分析とロギング（SaaS）ライセンス（**Firewall Analytics and Monitoring** または **Total Network Analytics and Monitoring**）を購入し、Firepower イベントデータに Secure Cloud Analytics の動的エンティティモデリングを適用できます。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging を参照してください。

Firewall Analytics and Monitoring または Total Network Analytics and Monitoring のライセンスを使用すると、既存の Secure Cloud Analytics ポータルを CDO の展開に関連付けるか、シスコに新しい Secure Cloud Analytics ポータルをプロビジョニングさせることができます。セキュリティ分析とロギング（SaaS）を設定すると、Firepower イベントデータ専用の `connection-events` という名前の センサー が自動的にプロビジョニングされます。詳細については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging/0201_Request_a_Stealthwatch_Cloud_Portal を参照してください。

Firewall Analytics and Monitoring ライセンスは動的エンティティモデリングを Firepower イベントデータにのみ適用するため、このライセンスのネットワークに追加の センサー を展開する必要はありません。これに対して、**Total Network Analytics and Monitoring** ライセンスは、Firepower イベントデータとオンプレミス ネットワークトラフィックの両方に動的エンティティモデリングを適用するため、ライセンス機能を最大限に活用するには、追加の センサー をネットワークに展開します。

> CDO の設定を完了しても、Secure Cloud Analytics ポータルに `connection-events` センサー が表示されない場合は、support@obsrvbl.com にお問い合わせください。

展開の推奨事項

ネットワークトポロジは大きく異なる可能性があるため、センサー を展開するときは、次の一般的なガイドラインに注意してください。

1. 次の目的のために センサー を展開するかどうかを決定します。
   - フロー データを収集する
   - ミラー化されたネットワークトラフィックを取得する
   - 一部のセンサーにフロー データを収集させ、その他のセンサーにミラー化されたネットワークトラフィックを取得させる
   - 両方のセンサーにフロー データを収集させるとともにミラー化されたネットワークトラフィックを取得させる
2. フローデータを収集する場合は、ネットワークデバイスがエクスポートできる形式（NetFlow v5、NetFlow v9、IPFIX、sFlow など）を決定します。

   > Cisco ASA ファイアウォールや Cisco Meraki MX アプライアンスなどの多数のファイアウォールが NetFlow をサポートしています。製造元のサポートドキュメントを参照して、ファイアウォールが NetFlow もサポートしているかどうかを確認してください。
3. センサー のネットワークポートがミラーポート容量をサポートできることを確認します。

ネットワークに複数の センサー 展開する際に支援が必要な場合は、support@obsrvbl.com にお問い合わせください。

Sensorのバージョンの確認

最新の センサー（バージョン 4.0）がネットワーク上に展開されていることを確認するには、コマンドラインから既存の センサー のバージョンを調べます。アップグレードする必要がある場合は、センサー を再インストールしてください。

センサー のバージョンの確認：

手順

1. 展開されている センサー に SSH でログインします。
2. プロンプトで、「`cat /opt/obsrvbl-ona/version`」と入力して Enter キーを押します。コンソールに 4.0.0 と表示されない場合は、旧規格の センサー です。Web ポータル UI から最新の センサー ISO をダウンロードしてください。

プライベートネットワークのモニタリング Sensor センサーメディアのインストールと設定

センサー を物理アプライアンスにインストールする場合は、.iso ファイルを使用してブート可能メディアを作成し、アプライアンスを再起動してそのメディアから起動する必要があります。

センサー を仮想マシンにインストールする場合は、.iso ファイルから直接起動できます。

> ⚠ インストールプロセスでは、センサー のインストール前に、センサー がインストールされるディスクのデータが消去されます。センサー をインストールする物理アプライアンスや仮想マシン上に、保存が必要なデータがないことを確認してください。

ブート メディアの作成

センサー を物理アプライアンスに展開する場合は、Ubuntu Linux をベースとする センサー をインストールする .iso ファイルを展開します。

CD や DVD などの光学ディスクに .iso ファイルを書き込む場合は、光学ディスクドライブ内の光学ディスクを使用して物理アプライアンスを再起動し、その光学ディスクから起動することを選択できます。

.iso ファイルと Rufus ユーティリティを使用して USB フラッシュドライブを作成した場合は、物理アプライアンスを再起動し、USB フラッシュドライブを USB ポートに挿入して、USB フラッシュドライブから起動することを選択できます。

> ℹ ISO を使用せずに センサー を展開する場合は、トラフィックを許可するようにローカルアプライアンスのファイアウォール設定を更新する必要がある場合があります。シスコでは、提供されている ISO を使用して センサー を展開することを強くお勧めします。

> ⚠ ブート可能な USB フラッシュドライブを作成すると、フラッシュドライブ上のすべての情報が削除されます。フラッシュドライブに他の情報がないことを確認してください。

センサー ISO ファイルのダウンロード:

最新バージョンの センサー ISO を Web ポータルからダウンロードしてください。これを使用してインストール（新しい センサー の場合）または再インストール（既存の センサー をアップグレードする場合）します。

手順

1. Web ポータル UI に管理者アカウントでログインします。
2. [ヘルプ(?)（Help (?)）] > **[インストール（Install）]Sensor** を選択します。
3. .iso のボタンをクリックして最新バージョンの ISO をダウンロードします。

ブート可能な光学ディスクの作成:

手順

- 製造元の指示に従って、.iso ファイルを光学ディスクにコピーしてください。

ブート可能な USB フラッシュドライブの作成:

はじめる前に

- ブート可能な USB フラッシュドライブを作成するために使用するアプライアンスの USB ポートに空の USB フラッシュドライブを挿入してください。
- ワークステーションにログインしてください。

手順

1. Web ブラウザで、Rufus ユーティリティの Web サイトに移動します。
2. 最新バージョンの Rufus ユーティリティをダウンロードします。
3. Rufus ユーティリティを開きます。
4. [デバイス(Device)]ドロップダウンで USB フラッシュドライブを選択します。
5. [ブートの選択(Boot selection)]ドロップダウンから[ディスクまたは ISO イメージ(Disk or ISO image)] を選択します。
6. [選択(SELECT)]をクリックし、センサー ISO ファイルを選択します。
7. [開始(START)]をクリックします。

> ⚠ ブート可能な USB フラッシュドライブを作成すると、フラッシュドライブ上のすべての情報が削除されます。フラッシュドライブに他の情報がないことを確認してください。

センサーのインストール

センサーのインストール

はじめる前に

- 物理アプライアンスにインストールする場合は、ブート可能メディアを挿入してアプライアンスを再起動し、ブート可能メディアから起動してください。
- 仮想マシンにインストールする場合は、.iso ファイルから起動してください。

手順

1. 最初のプロンプトで[観測可能なネットワーク アプライアンスのインストール(Install Observable Network Appliance)]を選択し、Enter キーを押します。
2. 矢印キーを使用して言語のリストから **言語を選択し**、Enter キーを押します。
3. 矢印キーを使用して国のリストから **使用場所を選択し**、Enter キーを押します。
4. 次の選択肢があります。
   - 矢印キーを使用して[はい(Yes)] を選択することによって **キーボードを設定し**、Enter キーを押して、**キーボード レイアウト**を選択してから Enter キーを押します。
   - 標準の米国英語キーボードを使用している場合は、[いいえ(No)] を選択してデフォルトを受け入れ、Enter キーを押します。
5. 矢印キーを使用して**キーボードの製造国**を選択し、Enter キーを押します。
6. 矢印キーを使用して**キーボード レイアウト**を選択し、Enter キーを押します。
7. **ネットワークを設定し**、矢印キーを使用して、制御インターフェイス(センサー を管理し、ネットワークデバイスからフローデータを収集する)として使用するプライマリ ネットワーク インターフェイスを選択し、Enter キーを押します。

他のすべてのネットワーク インターフェイスは、自動的にミラー インターフェイスとして設定されます。

8. インストールプロセスによってアプライアンスのコンポーネントが検出されるのを待ち、追加の設定を行います。インストール プロセスでは、DHCP を使用して、選択したプライマリ ネットワーク インターフェイスが制御インターフェイスとして設定されます。ネットワークで DHCP が使用されていない場合は、次の手順を実行します。

   システムに「Network auto configuration failed 」というメッセージが表示されたら、Enter キーを押します。

   [ネットワークの手動設定(Configure network manually)] を選択し、Enter キーを押します。

   アプライアンスの IP アドレスを入力し、矢印キーを使用して [続行(Continue)] を選択して、Enter キーを押します。

   ネットマスクを入力し、矢印キーを使用して [続行(Continue)] を選択して、Enter キーを押します。

   ゲートウェイ ルータ IP アドレスを入力し、矢印キーを使用して [続行(Continue)] を選択して、Enter キーを押します。

   最大 3 つのドメイン **ネーム サーバー アドレス**を入力し、矢印キーを使用して [続行(Continue)] を選択して、Enter キーを押します。

   > デフォルトでは、インストールでは自動的に DHCP が使用され、インストールを続行します。DHCP IP アドレスを上書きするには、インストールの完了後にインターフェイスを手動で編集する必要があります。

   > ローカル権威ネーム サーバーがネットワークに展開されている場合は、そのアドレスを入力することをお勧めします。

9. 管理者以外の権限用に root 以外のアカウントに関連付けられる**新しいユーザーのフルネーム**を入力し、矢印キーを使用して [続行(Continue)] を選択して、Enter キーを押します。
10. 管理者以外の権限を持つ root 以外のアカウントである**自分のアカウントのユーザー名**を入力し、矢印キーを使用して [続行(Continue)] を選択して、Enter キーを押します。
11. **新しいユーザーのパスワードを選択し**、矢印キーを使用して [続行(Continue)] を選択して、Enter キーを押します。
12. **確認のためにパスワードを再入力し**、矢印キーを使用して [続行(Continue)] を選択して、Enter キーをを押します。

    同じパスワードを 2 回入力しなかった場合は、やりなおしてください。
13. 矢印キーを使用して [はい(Yes)] を選択して**ホーム ディレクトリを暗号化し**、Enter キーを押します。
14. **矢印キーを使用してタイム ゾーンを選択し**、Enter キーを押します。

    セットアップ中に作成したアカウントは、仮想マシンへのアクセスに使用できる唯一のアカウントです。このインストールでは、個別の Secure Cloud Analytics ポータルアカウントは作成されません。

15. [ガイド付き – ディスク全体を使用してディスクドライブをパーティション分割(Guided – use entire disk to partition the disk drive)] を選択し、Enter キーを押します。ディスクの詳細設定を実行する場合は、他のオプションを選択してください。
16. **パーティション分割するディスクを選択し**、Enter キーを押します。
17. 矢印を使用して [パーティション分割を終了して変更をディスクに書き込む(Finish partitioning and write changes to disk)] を選択し、Enter キーを押します。
18. [はい(Yes)] を選択してアクションを確認し、Enter キーを押します。

    > ⚠ このアクションにより、ドライブ上のすべてのデータが削除されます。続行する前にドライブが空であることを確認してください。

    インストーラが必要なファイルをインストールするまで数分待ちます。
19. **HTTP プロキシ情報**を入力するか(HTTP プロキシを使用する場合)フィールドを空白のままにして(HTTP プロキシを使用しない場合)、矢印キーを使用して [続行(Continue)] を選択し、Enter キーを押します。

    インストーラが設定を実行するまで待ちます。
20. 矢印キーを使用してリストから更新ポリシーを選択し、Enter キーを押します。[セキュリティ更新の自動インストール(Install security updates automatically)] を選択することをお勧めします。

    インストーラが設定を実行し、追加のパッケージをインストールするまで待ちます。
21. **GRUB ブート ローダーをマスター ブート レコードにインストールする**ために矢印キーを使用して [はい(Yes)] を選択し、Enter キーを押します。

    インストーラが GRUB ブート ローダーをインストールするまで待ち、設定を完了します。
22. インストーラによって「**Installation Complete**」と表示されたら、矢印キーを使用して [続行(Continue)] を選択し、Enter キーを押してブートメディアを削除してから、設定を完了し、アプライアンスを再起動します。
23. アプライアンスが再起動したら、作成したアカウントでログインし、クレデンシャルが正しいことを確認します。

次の作業

- センサー を使用してネットワーク フロートラフィック(NetFlow など)を収集している場合、センサー の設定の詳細については、「**フローデータを収集するSensorの設定**」を参照してください。
- センサー を使用し、SPAN ポートまたはミラーポートに接続して、ミラートラフィックを収集している場合、Secure Cloud Analytics Web ポータルでの センサー 追加の詳細については、「**Secure Cloud Analytics ポータルへのSensorの接続**」を参照してください。
- 拡張 NetFlow テレメトリを送るように センサー を設定する場合は、『Cisco Secure Cloud Analytics Configuration Guide for Enhanced NetFlow』を参照してください。

Secure Cloud Analytics ポータルへのSensorの接続

VA のインストールが完了したら、ポータルにリンクさせる必要があります。そのためには、VA のパブリック IP アドレスを特定して Web ポータルに入力します。VA のパブリック IP アドレスを特定できない場合は、一意のサービス キーを使用して手動で VA をポータルにリンクさせることができます。

> 複数の センサー が MSSP などの中央ロケーションにステージングされ、複数のお客様が対象になっている場合は、新規のお客様を設定するたびにパブリック IP を削除する必要があります。ステージング環境のパブリック IP アドレスを複数の センサー に使用すると、センサー が誤ったポータルに不適切に接続される可能性があります。

Sensorのパブリック IP アドレスの検索とポータルへの追加

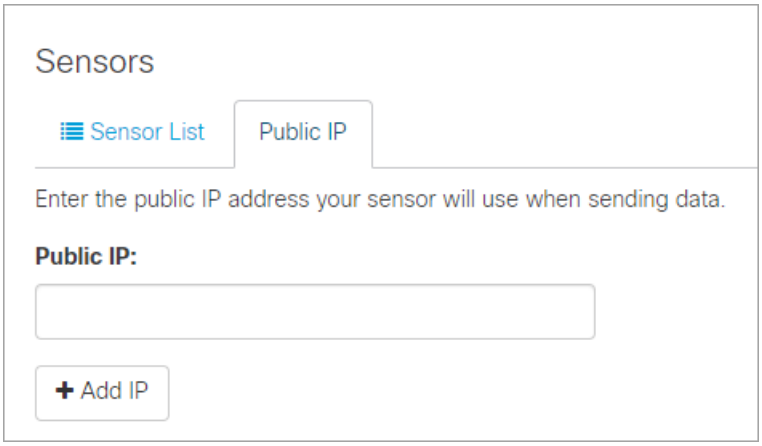
はじめる前に

- センサー に SSH で接続し、管理者としてログインします。

1. コマンドプロンプトで「`curl https://sensor.ext.obsrvbl.com`」と入力し、Enter を押します。`error` 値の `unknown identity` は、センサー がポータルに関連付けられていないことを意味します。次のスクリーンショットで例を参照してください。

```
observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$ curl https://sensor.ext.obsrvbl.com
{
  "error": "unknown identity",
  "identity": "72.163.2.237"
}observable@ona-e37255:/opt/obsrvbl-ona/logs/ipfix$
```

2. `identity` IP アドレスをコピーします。
3. センサー からログアウトします。
4. サイト管理者として Web ポータルにログインします。
5. **センサー（）アイコン > [パブリックIP（Public IP）]** を選択します。
6. [パブリックIP（Public IP）] フィールドに `identity` IP アドレスを入力します。次のスクリーンショットで例を参照してください。



7. [IPの追加（Add IP）] をクリックします。ポータルとセンサーがキーを交換した後は、パブリック IP アドレスではなくキーを使用して以降の接続が確立されます。

> 新しい センサー がポータルで反映されるまでに、最大 10 分かかる場合があります。

ポータルのサービス キーのセンサーへの手動による追加

> この手順は、センサー のパブリック IP アドレスが Web ポータルにすでに追加されている場合は必要**ありません**。この手順を試行する前に追加することを推奨します。ポータルのサービスキーの センサー への手動追加は、主に、2018 年 12 月時点で使用可能な ISO バージョン
> `ona-18.04.1-server-amd64.iso`
> より前に展開した古いセンサーを対象としています。また、Web ポータルで使用可能な現在のバージョンの センサー ISO を使用して、古い センサー を再展開することもできます。

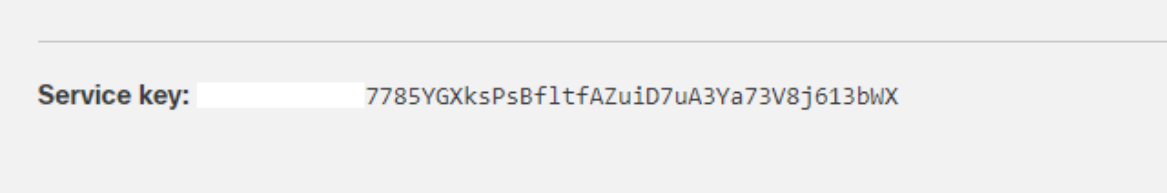
センサー のパブリック IP アドレスを Web ポータルに追加できない場合、または MSSP で複数の Web ポータルを管理している場合は、VA で センサー の `config.local` 設定ファイルを編集し、ポータルのサービスキーを手動で追加して センサー をポータルに関連付けます。

> 前の項のパブリック IP アドレスを使用すると、このキー交換が自動的に行われます。

はじめる前に

管理者としてポータル Web UI にログインします。

1. [設定（Settings）] > [センサー（Sensors）] を選択します。
2. センサー リストの末尾に移動して [サービスキー（Service key）] をコピーします。次のスクリーンショットで例を参照してください。

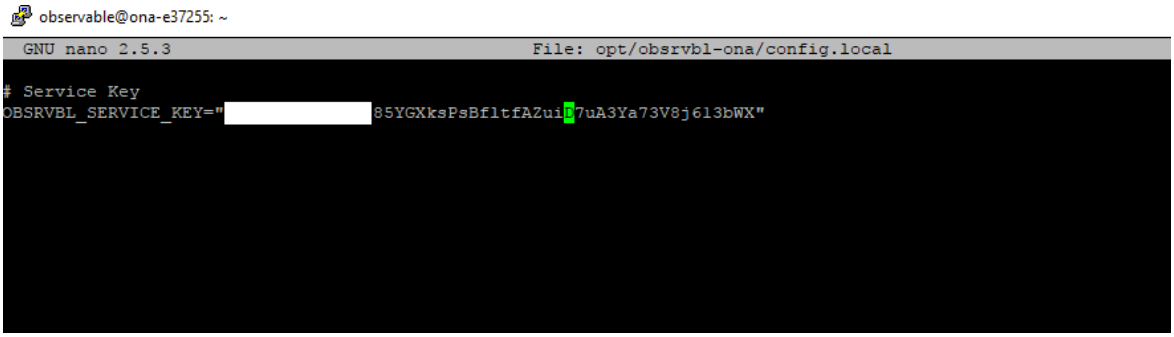


3. 管理者として センサー に SSH ログインします。
4. コマンドプロンプトで、このコマンドを入力し、`sudo nano opt/obsrvbl-ona/config.local` を入力し、Enter を押して設定ファイルを編集します。
5. `# Service Key` の下に次の行を追加します。

   <service-key> は次のポータルのサービスキーに置き換えてください。

   `OBSRVBL_SERVICE_KEY="<service-key>"`

   次に例を示します。



6. Ctrl+O を押して変更を保存します。
7. Ctrl+X を押して終了します。
8. コマンド プロンプトで「`sudo service obsrvbl-ona restart`」を入力し、Secure Cloud Analytics サービスを再起動します。

Sensorのポータル接続の確認

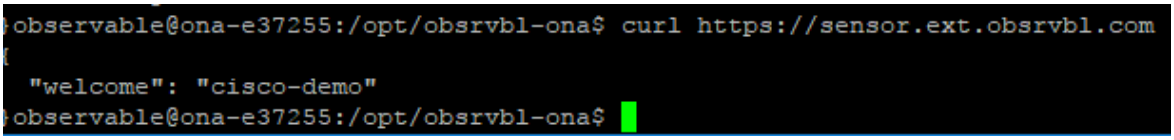
センサー をポータルに追加したら、接続を確認します。

> サービスキーを使用して `config.local` 設定ファイルを更新し、手動で センサー を Web ポータルにリンクさせた場合は、`curl` コマンドを使用して センサー からの接続を確認しても Web ポータルの名前が返されないことがあります。

はじめる前に

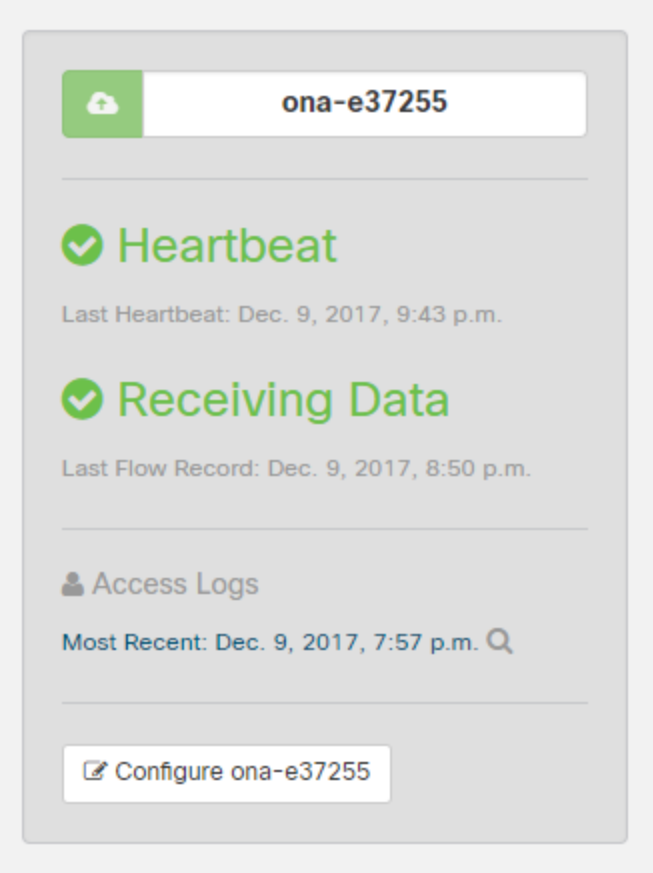
管理者として センサー に SSH ログインします。

1. コマンドプロンプトで「`curl https://sensor.ext.obsrvbl.com`」と入力し、Enter を押します。センサー は、ポータルの名前を返します。次のスクリーンショットで例を参照してください。



2. センサー からログアウトします。
3. ポータル Web UI にログインします。
4. [設定（Settings）] > [Sensor（Sensors）] を選択します。リストにセンサーが表示されます。次

のスクリーンショットで例を参照してください。



フローデータを収集するSensorの設定

センサー は、デフォルトでイーサネット インターフェイス上のトラフィックからフローレコードを作成します。このデフォルト設定は、センサー が SPAN またはミラーイーサネットポートに接続されていることを前提としています。ネットワーク上の他のデバイスでフローレコードを生成できる場合、これらのソースからフローレコードを収集してクラウドに送信するように、Web ポータル UI で センサー を設定できます。

ネットワークデバイスでさまざまなタイプのフローが生成される場合は、タイプごとに異なる UDP ポートで収集するように センサー を設定することをお勧めします。これにより、トラブルシューティングも容易になります。デフォルトでは、ローカル センサー ファイアウォール（`iptables`）のポート 2055/UDP、4739/UDP、および 9995/UDP が開いています。追加の UDP ポートを使用するには、Web ポータル UI でそれらのポートを開く必要があります。

次のポートを使用した、次のフロータイプの収集を設定できます。

- NetFlow v5：ポート 2055/UDP（デフォルトで開いている）
- NetFlow v9：ポート 9995/UDP（デフォルトで開いている）
- IPFIX：ポート 9996/UDP
- sFlow：ポート 6343/UDP

一部のネットワーク アプライアンスは、正しく機能させるために Web ポータル UI で選択する必要があります。

- Cisco Meraki：ポート 9998/UDP
- Cisco ASA：ポート 9997/UDP
- SonicWALL：9999/UDP

> Meraki ファームウェアバージョン 14.50 では、Meraki ログエクスポート形式が NetFlow 形式に準拠しています。Meraki デバイスがファームウェアバージョン 14.50 以降を実行している場合は、NetFlow v9 のプローブタイプと Meraki MX のソース（バージョン 14.50+）でセンサーを設定します。Meraki デバイスがファームウェアバージョン 14.50 より前のバージョンを実行している場合は、NetFlow v9 のプローブタイプと Meraki MX のソース（バージョン 14.50 より前）でセンサーを設定します。

フロー収集のためのSensorの設定

はじめる前に

- ポータルの Web UI に管理者アカウントでログインします。

手順

1. [設定（Settings）] > [Sensor（Sensors）] を選択します。
2. 追加した センサー について、[設定の変更（Change settings）] をクリックします。
3. [NetFlow/IPFIX] を選択します。

   > このオプションには最新バージョンの センサー が必要です。このオプションが表示されない場合は、[ヘルプ（？）（Help (?)）] > **[インストール（Install）]Sensor** を選択して、最新バージョンの センサー ISO をダウンロードしてください。

4. [新しいプローブの追加（Add New Probe）] をクリックします。
5. [プローブタイプ（Probe Type）] ドロップダウンからフロー タイプを選択します。
6. **ポート**番号を入力します。
7. [プロトコル（Protocol）] を選択します。
8. ドロップダウンから [送信元デバイス（Source device）] を選択します。
9. **[保存（Save）]**をクリックします。

次の作業

- Cisco Defense Orchestrator（CDO）の **Total Network Analytics and Monitoring** ライセンスを購入し、CDO を Secure Cloud Analytics と統合している場合については、https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging を参照してください。

プライベートネットワークのモニタリング Kubernetes 向け統合

Secure Cloud Analytics を Kubernetes クラスタと統合して、そのクラスタ内のノードに関する追加情報を Secure Cloud Analytics Web UI で確認できます。Kubernetes を Secure Cloud Analytics と統合するには、統合サービス キーを含むクラスタの Kubernetes 秘密キーを作成します。その後、新しいサービス アカウントを作成し、それを読み取り専用クラスタ ロールにバインドします。さらに、

DaemonSet 設定ファイルを設定して、センサー を、クラスタ内のノードに展開するためのポッドとしてスケジュールします。最後に、DaemonSet を作成します。数分後に、展開された センサー が Secure Cloud Analytics Web UI に表示されます。

Kubernetes 統合の設定

Kubernetes との統合の設定:

はじめる前に

- `kubectl` をクラスタにインストールしてください。詳細については、`kubectl` のインストールと設定に関する Kubernetes タスクのドキュメントを参照してください。
- Kubernetes クラスタに管理者アカウントでログインします。
- Secure Cloud Analytics Web ポータル UI に管理者アカウントでログインします。

手順

1. Secure Cloud Analytics Web ポータルで、[設定(Settings)] > [統合(Integrations)] > [Kubernetes] を選択します。
2. 指示に従って Kubernetes 統合を設定します。

Secure Cloud Analytics Web UI での展開されたSensorの表示

センサー がクラスタ内のノードに展開されていることを確認したら、数分待ってから、Secure Cloud Analytics Web UI にログインします。センサー のリストが更新され、Kubernetes クラスタ内に新しく展開された センサー が表示されます。

Secure Cloud Analytics Web UI での展開されたSensorの表示:

はじめる前に

- 管理者アカウントで Secure Cloud Analytics Web UI にログインします。

手順

- [設定(Settings)] > [Sensor(Sensors)] を選択して、展開された センサー を表示します。

パブリッククラウドのモニタリング設定

ここでは、パブリッククラウドのモニタリング用に Amazon Web Services（AWS）、Google Cloud Platform（GCP）、または Microsoft Azure クラウド展開を設定する手順と、Web ポータルを設定してパブリッククラウドのモニタリングの設定を完了する手順について説明します。

パブリッククラウドのモニタリング Amazon Web Services 向けの設定

Cisco Secure Cloud Analytics パブリッククラウドのモニタリング（旧 Stealthwatch Cloud パブリック クラウド モニターリング）は、Amazon Web Services（AWS）向けの可視化、脅威特定、およびコンプライアンスサービスです。Secure Cloud Analytics は、AWS パブリック クラウド ネットワークから仮想プライベートクラウド（VPC）フロー ログなどのネットワークトラフィック データを取得します。次に、そのデータに対して分析を実行して脅威と侵害の兆候を検出することによって、ダイナミック エンティティ モデリングを実行します。Secure Cloud Analytics は、適切な権限を持つクロスアカウント IAM ロールを使用して、AWS アカウントから直接 VPC フロー ログを消費します。さらに、Secure Cloud Analytics は、追加のコンテキストとモニターリングのために、その他のデータ ソース（CloudTrail や IAM など）を消費することができます。

フローログを保存する **S3 バケット**と、これらのフローログを取り込む Secure Cloud Analytics を設定するには、次の手順を実行します。

1. AWS で、VPC の VPC フローロギングを有効にし、フローログのエクスポート先の S3 バケットを設定します。詳細については、「**S3 バケット フロー ログ データ ストレージの設定**」を参照してください。
2. AWS で、IAM アクセスポリシーと IAM ロールを設定して、Secure Cloud Analytics のフロー ログへのアクセスと取得を可能にします。詳細については、「**フローログデータにアクセスするための AWS 権限の設定**」および「**フローログデータにアクセスするための IAM ロールの設定**」を参照してください。
3. Secure Cloud Analytics Web ポータル UIで、S3 バケットと IAM ロールを使用して 設定を更新して、AWS フローログデータの取得を可能にします。詳細については、「**S3 バケットからフローログデータにアクセスするための Secure Cloud Analytics の設定**」を参照してください。

S3 バケット フロー ログ データ ストレージの設定

既存の S3 バケットにフローログデータを保存できます。フローロギングを有効にするときに、新しい S3 バケットを作成することもできます。

S3 バケットの VPC への関連付け：

はじめる前に

- AWS 管理コンソールにログインして、VPD ダッシュボードにアクセスします。

手順

1. **使用している VPC** を選択します。
2. VPC を右クリックし、[フローログの作成（Create Flow Log）] を選択します。
3. [フィルタ（Filter）] ドロップダウンから、次のオプションのいずれかを選択します。

- 許可された IP トラフィックと拒否された IP トラフィックの両方を記録するには、[すべて（All）] を選択し、Secure Cloud Analytics で両方のタイプのトラフィックを表示できるようにします。
- [許可（Accept）] を選択すると、許可された IP トラフィックのみが記録され、Secure Cloud Analytics には許可されたトラフィックのみが表示されます。

4. [宛先（Destination）] に [S3バケットに送信（Send to an S3 bucket）] を選択します。
5. フローログデータを保存する S3 バケット ARN を入力します。

> S3 バケットが存在しない場合は、変更をコミットした後に AWS によって作成されます。

6. [ログレコード形式（Log record format）] ペインで、[カスタム形式（Custom format）] を選択します。
7. [ログ形式（Log format）] ドロップダウンリストからすべての属性を選択します。
8. [作成（Create）] をクリックします。

次の作業

- Secure Cloud Analytics によるフローログデータへのアクセスを許可する AWS 権限を設定します。詳細については、「**フローログデータにアクセスするための AWS 権限の設定**」を参照してください。

フローログデータにアクセスするための AWS 権限の設定

Secure Cloud Analytics Web UI に表示される JSON 設定を使用して、新しい IAM ポリシーを作成します。このポリシーには、Secure Cloud Analytics によるフローログデータへのアクセスを許可する権限が含まれています。

AWS クラウドポスチャを評価するには、AWS の IAM ポリシーに追加のアクセス許可を付与する必要があります。Secure Cloud Analytics の [AWSの概要（AWS About）] ページに、「`"Sid": "CloudCompliance"`」で始まる JSON オブジェクトの必要な権限が一覧表示されます。

Secure Cloud Analytics と AWS を初めて統合するお客様で、これらの追加の権限を付与したくない場合は、このオブジェクトを削除できますが、クラウドポスチャレポートは使用できなくなります。

フローログデータにアクセスする権限を持つポリシーの作成：

はじめる前に

- AWS 管理コンソールにログインして、IAM ダッシュボードにアクセスします。
- 管理者アカウントで Secure Cloud Analytics Web UI にログインします。

手順

1. Secure Cloud Analytics Web UI で、[設定（Settings）] > [統合（Integrations）] > [AWS] > [情報（About）] を選択します。
2. AWS リソースにアクセスする手順を確認します。
3. ポリシードキュメントの JSON 設定をコピーし、プレーンテキストエディタに貼り付けます。

4. Secure Cloud Analytics で AWS Cloud ポスチャを評価するために必要な追加の権限について、"Sid": "CloudCompliance" で始まる JSON オブジェクトを確認します。次の選択肢があります。
    - これらの追加の権限を付与しない場合は、"Sid": "CloudCompliance" で始まる JSON オブジェクトを削除します。Secure Cloud Analytics で AWS クラウドポスチャを評価することはできなくなります。次の手順に進みます。
    - これらの追加の権限を付与して AWS クラウドポスチャを評価する場合は、次の手順に進みます。
5. IAM ダッシュボードで、[ポリシー(Policies)] を選択します。
6. [ポリシーの作成(Create Policy)] をクリックします。
7. [JSON] タブを選択します。
8. プレーンテキストエディタからポリシーの JSON 設定をコピーし、JSON エディタに貼り付けます。
9. [ポリシーの確認(Review policy)] をクリックします。

    ポリシー検証ツールがエラーをスローした場合は、コピーして貼り付けたテキストを確認します。
10. [名前(Name)] フィールドに swc_policy と入力します。
11. Secure Cloud Analytics がイベントとログデータを読み取ることを許可するポリシーなどの [説明(Description)] を入力します。
12. [ポリシーの作成(Create Policy)] をクリックします。

次の作業

- Secure Cloud Analytics によるフローログデータへのアクセスを許可する新しいロールを作成します。詳細については、「**フローログデータにアクセスするための IAM ロールの設定**」を参照してください。

フローログデータにアクセスするための IAM ロールの設定

IAM ポリシーを作成したら、Secure Cloud Analytics によるフローログデータへのアクセスを許可する IAM ロールを作成します。

フローログデータにアクセスする権限を持つ IAM ロールの設定:

はじめる前に

- AWS 管理コンソールにログインして、IAM ダッシュボードにアクセスします。

手順

1. [ロール(Role)] を選択します。
2. [ロールを作成(Create role)] を選択します。
3. [別のAWSアカウント(Another AWS account)] ロールタイプを選択します。
4. [アカウントID(Account ID)] フィールドに 757972810156 と入力します。
5. [外部IDが必要(Require external ID)] オプションを選択します。

6. 外部 ID として Secure Cloud Analytics のWeb ポータル名を入力します。

   > Web ポータル名は、`https://`**`portal-name`**`.obsrvbl.com` の形式でポータル URL に埋め込まれます。たとえば、Web ポータルの URL が `https://`**`example-client`**`.obsrvbl.com` の場合、外部 ID として **`example-client`** を入力します。URL 全体を入力すると、統合設定は失敗します。

7. [次へ：権限（Next: Permissions）] をクリックします。
8. 作成した swc_policy ポリシーを選択します。
9. [次へ：タギング（Next: Tagging）] をクリックします。
10. [次へ：レビュー（Next: Review）] をクリックします。
11. [ロール名（Role name）] として `swc_role` を入力します。
12. クロスアカウントアクセスを許可するロールなどの [説明（Description）] を入力します。
13. [ロールを作成（Create Role）] をクリックします。
14. ロール ARN をコピーし、プレーンテキストエディタに貼り付けます。

次の作業

- IAM ロールと S3 バケット名を Secure Cloud Analytics Web UI に追加し、AWS に新しい S3 バケットポリシーをアップロードします。詳細については、「**S3 バケットからフローログデータにアクセスするための Secure Cloud Analytics の設定**」を参照してください。

S3 バケットからフローログデータにアクセスするための Secure Cloud Analytics の設定

フローログの設定を完了するには、Secure Cloud Analytics Web UI で IAM ロールと S3 バケット名を入力し、S3 バケット名を追加するときに Secure Cloud Analytics によって提供される設定を使用して、AWS で S3 バケットポリシーを変更します。

アカウントで VPC フローログを有効にしたばかりの場合は、10 分待ってから、フローログデータを取得するように Secure Cloud Analytics 設定してください。S3 バケットにログが含まれない、その **S3 パス**名を追加すると、エラーが返されることがあります。AWS は、約 10 分ごとに VPC フローログを生成します。

S3 バケットに保存されているフローログデータを取り込むための Secure Cloud Analytics の設定：

はじめる前に

- 管理者アカウントで Secure Cloud Analytics Web UI にログインします。

手順

1. [設定（Settings）] > [統合（Integrations）] > [AWS] > [クレデンシャル（Credentials）] を選択します。
2. [新しいクレデンシャルの追加（Add New Credentials）] をクリックします。
3. 分かりやすい**名前**を入力します。

4. 保存したロール ARN をプレーンテキストエディタからコピーし、[ロールARN（Role ARN）] フィールドに貼り付けます。
5. [作成（Create）] をクリックします。
6. [設定（Settings）] > [統合（Integrations）] > [AWS] > [VPCフローログ（VPC Flow Logs）] を選択します。
7. [VPCフローログを追加（Add VPC Flowlog）] をクリックします。
8. [S3パス（S3 Path）] フィールドに、フローログデータを含む S3 バケットの名前を入力します。

   > 複数の設定済み S3 バケットを追加できます。Secure Cloud Analytics と AWS の統合には、1 つの IAM アクセス ポリシーとロールを設定する必要だけがあります。

9. S3 バケットの [クレデンシャル（Credentials）] を選択し、[設定手順（Setup Instructions）] をクリックします。

   S3 バケットパスとクレデンシャルを使用して更新されたバケットポリシー JSON 設定が表示されます。
10. 表示されたバケットポリシー JSON 設定をコピーし、プレーンテキストエディタに貼り付けます。

    > このブラウザウィンドウを開いたままにします。S3 バケットポリシーを設定した後、Secure Cloud Analytics Web UI の設定を完了します。

Secure Cloud Analytics がフローログデータを取り込むための S3 バケットポリシーの設定：

はじめる前に

- AWS 管理コンソールにログインして、IAM ダッシュボードにアクセスしてください。
- 管理者アカウントで Secure Cloud Analytics Web UI にログインします。

手順

1. IAM ダッシュボードで、[ポリシー（Policies）] を選択します。
2. [ポリシーの作成（Create Policy）] をクリックします。
3. [JSON] タブを選択します。
4. プレーンテキストエディタからバケットポリシー JSON 設定をコピーし、ポリシーエディタに貼り付けて、既存のバケットポリシーを上書きします。
5. [ポリシーの確認（Review policy）] をクリックします。
6. ポリシーの [名前（Name）] を入力します。
7. 任意でポリシーの [説明（Description）] を入力します。
8. [ポリシーの作成（Create Policy）] をクリックします。
9. IAM ダッシュボードで、[ロール（Roles）] を選択します。
10. `swc_role` を選択します。
11. [権限（Permissions）] タブで、[ポリシーをアタッチ（Attach policies）] をクリックします。
12. ステップ 6 で入力したポリシー名を選択します。
13. [ポリシーをアタッチ（Attach policy）] をクリックします。

14. Secure Cloud Analytics Web UI で、入力した S3 バケットパスとクレデンシャルに対して [作成(Create)] をクリックします。

> S3 バケットからフローログデータを取り込むための適切な権限がない場合、システムはエラーを表示します。サポートが必要な場合は、support@obsrvbl.com にポータル名と S3 バケット名をご連絡ください。

次の作業

- AWS 統合を確認します。詳細については、「**AWS との統合の確認**」を参照してください。

AWS との統合の確認

AWS との統合を完了すると、[設定(Settings)] メニューの Cisco Secure Cloud Analytics センサー(旧 Stealthwatch Cloud センサー)ページに、次の名前の新しい センサー が表示されます。

`AWS: S3-bucket-name`

この センサー エントリには統合の健全性または S3 バケット名が表示されますが、センサー のページから直接設定することはできません。

> PCM の設定を完了してからトラフィックおよびエンティティ データの表示が開始されるまでに最大 24 時間かかります。

AWS 統合の確認:

はじめる前に

- 管理者アカウントで Secure Cloud Analytics Web UI にログインします。

手順

1. Secure Cloud Analytics Web UI で、[設定(Settings)] > [Sensor(Sensors)] を選択します。ページに S3 バケット名が表示されていることを確認します。
2. [統合(Integrations)] > [AWS] > [権限(Permissions)] の順に選択します。表示された AWS 権限が期待どおりであることを確認します。

パブリッククラウドのモニタリング Google Cloud Platform 向けのパブリック クラウド モニターリング設定

Cisco Secure Cloud Analytics パブリッククラウドのモニタリング(旧 Stealthwatch Cloud パブリック クラウド モニターリング)は、Google Cloud Platform(GCP)向けの可視化、脅威特定、およびコンプライアンスサービスです。Secure Cloud Analytics は、AWS パブリック クラウド ネットワークから仮想プライベートクラウド(VPC)フローログなどのネットワーク トラフィック データを取り込みます。次に、そのデータに対して分析を実行して脅威と侵害の兆候を検出することによって、ダイナミック エンティティ モデリングを実行します。Secure Cloud Analytics は、適切な権限を持つクロスアカウント IAM サービス アカウントを使用して、GCP アカウントから直接 VPC フロー ログを消費します。

単一 GCP プロジェクトの設定

単一プロジェクトのフローログデータを生成して保存し、Secure Cloud Analytics がそのデータを取り込むように GCP を設定するには、次の手順を実行します。

1. GCP で、フローログおよびその他のデータを表示し、JSON クレデンシャルを保存するための適切な権限を持つサービスアカウントを設定します。詳細については、「**VPC フロー ログを表示するためのサービス アカウントの設定**」を参照してください。
2. GCP で、メトリック収集のためのフローロギングと Stackdriver Monitoring API を有効にします。詳細については、「**VPC フローログを生成して権限を有効化するための GCP の設定**」を参照してください。
3. Secure Cloud Analytics Web ポータル UI で、サービスアカウントの JSON クレデンシャルをアップロードします。詳細については、「**JSON クレデンシャルのアップロード**」を参照してください。

高スループットの GCP 環境がある場合は、**必要に応じて**単一プロジェクトの Pub/Sub を設定して、フローログデータを Secure Cloud Analytics に配信できます。

1. 導入が高スループットであるかどうかを判断します。詳細については、「**高スループット環境の特定**」を参照してください。
2. フローログデータを取り込むための Pub/Subトピックと、フローログデータを配信するトピックの Pub/Sub サブスクリプションを設定します。詳細については、「**GCP Pub/Sub サブスクリプションの作成**」を参照してください。

複数の GCP プロジェクトの設定

複数プロジェクトのフローログデータを生成して保存し、Secure Cloud Analytics がそのデータを取り込むように GCP を設定するには、次の手順を実行します。

1. GCP で、フローログおよびその他のデータを表示し、JSON クレデンシャルを保存するための適切な権限を持つサービスアカウントを設定します。単一サービスアカウントを使用するように追加のプロジェクトを設定します。詳細については、「**VPC フロー ログを表示するためのサービス アカウントの設定**」を参照してください。
2. GCP で、サービスアカウントを使用する追加のプロジェクトを設定します。詳細については、「**複数のプロジェクトの VPC フローログを表示するための単一サービスアカウントの設定**」を参照してください。
3. GCP で、メトリック収集のためのフローロギングと Stackdriver Monitoring API を有効にします。詳細については、「**VPC フローログを生成して権限を有効化するための GCP の設定**」を参照してください。
4. Secure Cloud Analytics Web ポータル UI で、サービスアカウントの JSON クレデンシャルをアップロードします。詳細については、「**JSON クレデンシャルのアップロード**」を参照してください。

高スループットの GCP 環境がある場合は、**必要に応じて**複数プロジェクトの Pub/Sub を設定して、フローログデータを Secure Cloud Analytics に配信できます。

1. 導入が高スループットであるかどうかを判断します。詳細については、「**高スループット環境の特定**」を参照してください。
2. フローログデータを取り込むための Pub/Subトピックと、フローログデータを配信するトピックの Pub/Sub サブスクリプションを設定します。詳細については、「**GCP Pub/Sub サブスクリプションの作成**」を参照してください。
3. 追加のプロジェクト向けに、追加の Pub/Sub トピックとサブスクリプションを設定します。詳細については、「**Pub/Sub トピックおよびサブスクリプションの設定**」を参照してください。

VPC フロー ログを表示するためのサービス アカウントの設定

IAM サービスアカウントを設定するには、Secure Cloud Analytics用の情報を収集するために必要な権限を持つカスタムロールを作成します。次に、サービスアカウントを作成し、カスタムロールを含む複数のロールを関連付けます。GCP は、秘密キー情報を使用してアカウントを作成します。秘密キーを安全な場所に保存します。

VPC フロー ログを表示するためのサービスアカウントの設定:

手順

1. GCP コンソールから、[IAMと管理(IAM＆admin)] > [IAM] > [サービスアカウント(Service accounts)] を選択します。
2. [サービスアカウントの作成(Create Service Account)] をクリックします。
3. [サービスアカウント名(Service account name)] フィールドに「`logs-viewer`」と入力します。
4. [作成(Create)] をクリックします。
5. [ロールを選択(Select a role)] ドロップダウンをクリックします。Enter を押して、[ログビューア(Logs Viewer)] ロールを選択します。
6. [別のロールの追加(Add Another Role)] をクリックします。
7. 新しい [ロールを選択(Select a role)] ドロップダウンをクリックします。Enter を押して、[計算ビューア(Compute Viewer)] ロールを選択します。
8. [別のロールの追加(Add Another Role)] をクリックします。
9. 新しい [ロールを選択(Select a role)] ドロップダウンをクリックします。Enter を押して、[モニターリングビューア(Monitoring Viewer)] ロールを選択します。
10. [別のロールの追加(Add Another Role)] をクリックします。
11. 新しい [ロールを選択(Select a role)] ドロップダウンをクリックします。Enter を押して、[Pub/Subサブスクライバ(Pub/Sub Subscriber)] ロールを選択します。
12. **[続行(Continue)]** をクリックします。
13. [キーを作成(Create Key)] をクリックします。
14. [キーを作成(Create key)] フィールドで [JSON] を選択し、[作成(Create)] をクリックします。

    > ⚠ 生成される JSON 秘密キー ファイルにはアカウントが VPC フロー ログにアクセスするために必要な情報が含まれているので、ファイルを安全な場所に保存してください。

15. JSON 秘密キーを保存したら、[閉じる(Close)] をクリックします。
16. [完了(Done)] をクリックします。

次の作業

- **単一プロジェクト**をモニターする場合は、展開でフローロギングを有効にします。詳細については、「**VPC フローログを生成して権限を有効化するための GCP の設定**」を参照してください。
- **複数のプロジェクト**をモニターする場合は、展開でフローロギングを有効にする前に、サービスアカウントを追加の各プロジェクトに関連付けます。詳細については、「**複数のプロジェクトの VPC フローログを表示するための単一サービスアカウントの設定**」を参照してください。

複数のプロジェクトの VPC フローログを表示するための単一サービスアカウントの設定

GCP 展開で**複数のプロジェクトをモニターする**場合は、単一サービスアカウントを使用してプロジェクトをモニターできます。モニターする各プロジェクトのクラウドリソースマネージャ API を有効にし、作成したサービスアカウントの電子メールアドレスおよび適切なロール権限をそのプロジェクトに追加します。

サービスアカウントの電子メールアドレスの検索：

手順

1. GCP コンソールから、[IAMと管理（IAM＆admin）] > [IAM] を選択します。
2. 新しいサービスアカウントの編集アイコンをクリックします。
3. [メンバー（Member）] の次の形式の電子メールアドレスをコピーし、プレーンテキストエディタに貼り付けます。

   `[account-name]@[project-id].[gcp-info].com`

追加プロジェクトに対するクラウドリソースマネージャ API の有効化：

手順

1. GCP コンソールから、[APIとサービス（APIs＆Services）] > [ライブラリ（Library）] の順に選択します。
2. プロジェクトの [選択（Select）] をクリックします。
3. [クラウドリソースマネージャAPI（Cloud Resource Manager API）] を検索し、[クラウドリソースマネージャAPI（Cloud Resource Manager API）] を選択して、[有効（Enable）] をクリックします。

追加プロジェクトへのサービスアカウントの追加：

手順

1. GCP コンソールから、[IAMと管理（IAM＆admin）] > [IAM] を選択します。
2. [プロジェクト（Project）] ドロップダウンから追加のプロジェクトを選択します。
3. [追加（Add）] をクリックします。
4. プレーンテキストエディタからメンバーサービスアカウントの電子メールアドレスをコピーし、[新しいメンバー（New members）] フィールドに貼り付けます。
5. [ロールを選択（Select a role）] ドロップダウンをクリックします。Enter を押して、[ログビューア（Logs Viewer）] ロールを選択します。
6. [別のロールの追加（Add Another Role）] をクリックします。
7. 新しい [ロールを選択（Select a role）] ドロップダウンをクリックします。Enter を押して、[計算ビューア（Compute Viewer）] ロールを選択します。
8. [別のロールの追加（Add Another Role）] をクリックします。
9. 新しい [ロールを選択（Select a role）] ドロップダウンをクリックします。Enter を押して、[モニターリングビューア（Monitoring Viewer）] ロールを選択します。
10. [別のロールの追加（Add Another Role）] をクリックします。

11. 新しい [ロールを選択（Select a role）] ドロップダウンをクリックします。Enter を押して、[Pub/Subサブスクライバ（Pub/Sub Subscriber）] ロールを選択します。
12. **[保存（Save）]**をクリックします。
13. 追加のプロジェクトごとにステップ 2 ～ 13 を繰り返します。

次の作業

- 展開でフローロギングを有効にします。詳細については、「**VPC フローログを生成して権限を有効化するための GCP の設定**」を参照してください。

VPC フローログを生成して権限を有効化するための GCP の設定

サービスアカウントを設定したら、サブネットごとに GCP 展開でフローロギングを有効にした後で、Secure Cloud Analytics による取り込みを可能にします。その後、Stackdriver Monitoring API を有効にして、さまざまな GCP メトリックを収集します。

VPC フロー ログを生成するための GCP サブネットの設定：

手順

1. GCP Console から、[VPCネットワーク（VPC network）] を選択します。
2. サブネットを選択します。
3. [編集（Edit）] をクリックします。
4. [フローログ（Flow logs）] から [オン（On）] を選択します。
5. **[保存（Save）]**をクリックします。設定するサブネットごとにステップ 1 ～ 4 を繰り返します。

Stackdriver Monitoring API の有効化：

手順

1. [APIとサービス（APIs and Services）] ページから、プロジェクトを選択します。
2. [APIとサービスの有効化（Enable APIs and Service）] をクリックします。
3. 検索フィールドに、[Stackdriver Monitoring API] と入力して選択します。
4. API が有効になっていない場合は、[有効（Enable）] をクリックします。
5. **[保存（Save）]**をクリックします。

次の作業

- 保存した JSON クレデンシャルを Secure Cloud Analytics ポータルにアップロードします。詳細については、を参照してください。詳細については、「**JSON クレデンシャルのアップロード**」を参照してください。

JSON クレデンシャルのアップロード

設定を完了するには、JSON クレデンシャルを Secure Cloud Analytics Web ポータル UI にアップロードします。

サービス アカウントのクレデンシャルの Secure Cloud Analytics Web ポータルへのアップロード:

はじめる前に

- サイト管理者として Secure Cloud Analytics Web ポータルにログインします。

手順

1. [設定(Settings)] > [統合(Integrations)] > [GCP] > [クレデンシャル(Credentials)] を選択します。
2. [クレデンシャル ファイルのアップロード(Upload Credentials File)] をクリックし、JSON クレデンシャル ファイルを選択します。

次の作業

- 高スループット環境かどうかを確認し、そうである場合は、Pub/Sub がフローログデータを取り込むように設定します。

高スループット環境の特定

高スループット環境でのフローデータの送信を保証するため、Pub/Sub トピックとサブスクリプションを設定できます。VCP フローデータが GCP によって課されるロギング読み取り制限を超える場合は、GCP Pub/Sub コレクションが理想的であり、大規模な GCP 展開では強く推奨されます。

既存のログベースの GCP 統合で GCP のロギング制限を超えているかどうかを確認するには、次の手順を実行します。

- **GCP ロギングクォータの確認**します。

GCP ロギングクォータの確認

はじめる前に

- https://console.cloud.google.com/apis/api/logging.googleapis.com/quotas にログインします。

手順

1. プロジェクトを選択します。
2. *Quota exceeded errors count (1 min) – Read requests per minute* を検索します。クォータを超過した場合、Pub/Sub の設定の詳細については、「**Pub/Sub トピックおよびサブスクリプションの設定**」を参照してください。

GCP Pub/Sub サブスクリプションの作成

GCP 展開のトラフィックスループットが高い場合は、フローログデータ配信用に Pub/Sub を設定することを推奨します。フローログデータの取り込み用に Pub/Sub を設定するには、プライマリプロジェクト ID を取得し、ログエクスポートシンクを作成してから、トピックの Pub/Sub サブスクリプションを作成します。

GCP プロジェクト ID の検索：

はじめる前に

- GCP コンソールにログインします。

手順

1. [リソースの管理（Manage resources）] を選択します。
2. プライマリプロジェクトを選択し、プロジェクト ID をコピーします。
3. プロジェクト ID をテキストエディタに貼り付けます。

プロジェクト用の GCP ログエクスポートシンクの作成：

手順

1. GCP コンソールで、[Stackdriverロギング（Stackdriver Logging）] > [ログルータ（Logs Router）] を選択します。
2. [シンクを作成（Create Sink）] をクリックします。
3. ログエントリの上にある [ラベルまたはテキスト検索によるフィルタ（Filter by label or text search）] ドロップダウンフィールドから、[高度なフィルタに変換（Convert to advanced filter）] を選択します。
4. 次をコピーし、プレーンテキストエディタに貼り付けます。

```
                    resource.type="gce_subnetwork"
logName="projects/MY_PROJECT_
NAME/logs/compute.googleapis.com%2Fvpc_flows"
```

5. `MY_PROJECT_NAME` をプロジェクト ID に置き換えます。
6. 更新されたテキストをコピーし、[ラベルまたはテキスト検索によるフィルタ（Filter by label or text search）] フィールドに貼り付け、既存のテキストを上書きします。
7. [シンクを編集（Edit Sink）] ペインの [シンク名（Sink Name）] フィールドに `vpc_flows-sink` と入力します。
8. [シンクサービス（Sink Service）] ドロップダウンから [Pub/Sub] を選択します。
9. [シンクの宛先（Sink Destination）] ドロップダウンから [新しいクラウドPub/Subトピックの作成（Create new Cloud Pub/Sub topic）] を選択します。
10. [名前（Name）] フィールドに `vpc_flows-topic` と入力し、[作成（Create）] をクリックします。
11. [シンクを作成（Create Sink）] をクリックします。

プロジェクト用の GCP Pub/Sub サブスクリプションの作成：

手順

1. GCPコンソールから、[Pub/Sub] > [トピック（Topic）] の順に選択します。
2. `vpc_flows-topic` のコンテキストメニューから [サブスクリプションを作成（Create Subscription）] を選択します。

3. [サブスクリプション名(Subscription Name)]フィールドに `swc_subscription` と入力します。
4. [配信タイプ(Delivery Type)]で[プル(Pull)] を選択します。
5. [確認期限(Acknowledgment Deadline)]フィールドに `600` 秒と入力します。
6. [メッセージ保持期間(Message Retention Duration)]フィールドに `2` 時間と入力します。
7. [確認応答メッセージの保持(Retain Acknowledged Messages)]をオフにします。
8. [作成(Create)]をクリックします。

次の作業

- **複数のプロジェクト**をモニターしている場合は、追加プロジェクトごとに、Pub/Subトピックとサブスクリプションを設定します。詳細については、「**Pub/Subトピックおよびサブスクリプションの設定**」を参照してください。

Pub/Subトピックおよびサブスクリプションの設定

GCP展開で複数のプロジェクトをモニターする場合は、プライマリプロジェクトのPub/Subを設定した後、プライマリプロジェクトIDを参照する追加プロジェクトごとに、ログエクスポートシンクとPub/Subサブスクリプションを作成します。

追加プロジェクト用のGCPログエクスポートシンクの作成:

手順

1. GCPコンソールから、プライマリプロジェクト以外のプロジェクトを選択します。
2. [Stackdriverロギング(Stackdriver Logging)]>[ログルータ(Logs Router)]を選択します。
3. [シンクを作成(Create Sink)]をクリックします。
4. ログエントリの上にある[ラベルまたはテキスト検索によるフィルタ(Filter by label or text search)]ドロップダウンフィールドから、[高度なフィルタに変換(Convert to advanced filter)]を選択します。
5. 次をコピーし、プレーンテキストエディタに貼り付けます。

```
                    resource.type="gce_subnetwork"
logName="projects/MY_PROJECT_
NAME/logs/compute.googleapis.com%2Fvpc_flows"
```

6. `MY_PROJECT_NAME` を**プライマリ**プロジェクトIDに置き換えます。
7. 更新されたテキストをコピーし、[ラベルまたはテキスト検索によるフィルタ(Filter by label or text search)]フィールドに貼り付け、既存のテキストを上書きします。
8. [シンクを編集(Edit Sink)]ペインの[シンク名(Sink Name)]フィールドに `vpc_flows-sink` と入力します。
9. [シンク名(Sink Name)]フィールドに `vpc_flows-sink` と入力します。
10. [シンクサービス(Sink Service)] ドロップダウンから[Pub/Sub]を選択します。
11. [シンクの宛先(Sink Destination)] ドロップダウンから[新しいクラウドPub/Subトピックの作成(Create new Cloud Pub/Sub topic)]を選択します。

12. [名前(Name)]フィールドに vpc_flows-topic と入力し、[作成(Create)]をクリックします。
13. [シンクを作成(Create Sink)]をクリックします。
14. 追加のプロジェクトごとにステップ 1 ～ 13 を繰り返します。

追加プロジェクト用の GCP Pub/Sub サブスクリプションの作成:

手順

1. GCP コンソールから、プライマリプロジェクト以外のプロジェクトを選択します。
2. [Pub/Sub] > [トピック(Topics)]を選択します。
3. vpc_flows-topic のコンテキストメニューから[サブスクリプションを作成(Create Subscription)]を選択します。
4. [サブスクリプション名(Subscription Name)]フィールドに swc_subscription と入力します。
5. [配信タイプ(Delivery Type)]で[プル(Pull)] を選択します。
6. [確認期限(Acknowledgment Deadline)]フィールドに 600 秒と入力します。
7. [メッセージ保持期間(Message Retention Duration)]フィールドに 2 時間と入力します。
8. [確認応答メッセージの保持(Retain Acknowledged Messages)]をオフにします。
9. [作成(Create)]をクリックします。

   追加のプロジェクトごとにステップ 1 ～ 9 を繰り返します。

パブリッククラウドのモニタリング Microsoft Azure の設定

Cisco Secure Cloud Analytics パブリッククラウドのモニタリング(旧 Stealthwatch Cloud パブリック クラウド モニターリング)は、Microsoft Azure 向けの可視化、脅威特定、およびコンプライアンスサービスです。Secure Cloud Analytics は、Azure パブリック クラウド ネットワークからネットワーク セキュリティ グループ(NSG)フローログなどのネットワークトラフィック データを取得します。次に、そのデータに対して分析を実行して脅威と侵害の兆候を検出することによって、動的エンティティモデリングを実行します。Secure Cloud Analytics は、Azure ストレージアカウントから直接 NSG フローログを消費し、アプリケーションを使用して追加のコンテキストを取得します。

フローログデータを生成して保存し、Secure Cloud Analytics がそのフローログデータを取り込むように Azure を設定するには、次の手順を実行します。

- Azure で、少なくとも 1 つのリソースグループをモニターする必要があります。詳細については、「**Azure リソースグループの作成**」を参照してください。
- Azure で、Azure AD の URL とサブスクリプション ID を取得します。詳細については、「**Azure Active Directory の URL とサブスクリプション ID の取得**」を参照してください。
- Azure で、AD アプリケーションを作成し、アプリケーションにロールを関連付けます。詳細については、「**Azure AD アプリケーションの作成**」と「**アプリケーションへの Azure ロールの割り当て**」を参照してください。
- Azure で、フローログデータのストレージアカウントを作成し、SAS URL を生成します。詳細については、「**フローログデータを保存するための Azure ストレージアカウントの作成**」および「**Azure ストレージアカウントの共有アクセス署名 URL の生成**」を参照してください。

- Azure で、Network Watcher とフローログを有効にします。詳細については、「Azure Network Watcher の有効化」および「Azure NSG フローログの有効化」を参照してください。
- Azure で、実行されたアクティビティをさらに可視化する場合は、アクティビティログを保存するようにストレージアカウントを設定します。詳細については、「Azure アクティビティログストレージの有効化」を参照してください。
- Secure Cloud Analytics で、AD URL、サブスクリプション ID、アプリケーション ID とキー、および BLOB サービス SAS URL を含む Azure クレデンシャルとフローログのストレージ情報をアップロードします。詳細については、「Secure Cloud Analytics Azure との統合」を参照してください。

Secure Cloud Analytics 統合に必要な Azure 権限

次の表に、Secure Cloud Analytics との統合のために Azure を設定するのに必要なロールメンバーシップの詳細を示します。

アクション	メンバーユーザー（ネイティブテナントメンバー）に必要な権限	ゲストユーザー（コラボレーションゲスト）に必要な権限
Azure リソースグループの作成	ストレージアカウントのコントリビュータロールにメンバーユーザーを追加する	ストレージアカウントのコントリビュータロールにゲストユーザーを追加する
Azure Active Directory の URL とサブスクリプション ID の取得	メンバーユーザーのデフォルト権限	AD URL を取得するためのゲストユーザーのデフォルト権限、サブスクリプション ID を取得するための Cognitive Services ユーザーロールへのゲストユーザーの追加
Azure AD アプリケーションの作成	AD アプリケーション登録を作成するためのメンバーユーザーのデフォルト権限、ユーザーがアプリケーション登録を作成した場合にクライアントシークレットを生成するためのメンバーユーザーのデフォルト権限	アプリケーション開発者ロールにゲストユーザーを追加する
アプリケーションへの Azure ロールの割り当て	ユーザーがアプリケーション登録を作成した場合は、メンバーユーザーのデフォルト権限	アプリケーション開発者ロールにゲストユーザーを追加する
フローログデータを保存するための Azure ストレージアカウントの作成	ストレージアカウントのコントリビュータロールにメンバーユーザーを追加する	ストレージアカウントのコントリビュータロールにゲストユーザーを追加する
Azure ストレージアカウントの共有アクセス署名 URL の生成	ストレージアカウントのコントリビュータロールにメンバーユーザーを追加する	ストレージアカウントのコントリビュータロールにゲストユーザーを追加する
Azure Network	ネットワーク コントリビュータ ロールにメンバー	ネットワーク コントリビュータ ロールに

Watcher の有効化	ユーザーを追加する	ゲストユーザーを追加する
Azure NSG フローログの有効化	ネットワーク コントリビュータ ロールにメンバーユーザーを追加する	ネットワーク コントリビュータ ロールにゲストユーザーを追加する
Azure アクティビティログストレージの有効化	モニターリング コントリビュータ ロールにメンバーユーザーを追加する	モニターリング コントリビュータ ロールにゲストユーザーを追加する

ロールと権限の詳細については、Microsoft Azure のマニュアルで次の用語を検索してください。

- ゲストユーザーおよびメンバーユーザーの権限
- アプリケーション開発者ロール
- Cognitive Services ユーザーロール
- モニターリング コントリビュータ ロール
- ネットワーク コントリビュータ ロール
- ストレージ アカウント コントリビュータ ロール

Azure リソースグループの作成

最初に、モニターする 1 つ以上のリソースグループがあることを確認します。既存のリソースグループを使用することも、新しいリソースグループを作成して、仮想マシンなどのリソースを追加することもできます。

リソースグループの作成:

はじめる前に

- Azure ポータルにログインします。

手順

1. [リソースグループ(Resource Groups)] を選択します。
2. [追加(Add)] をクリックします。
3. [リソースグループ名(Resource group name)] を入力します。
4. [サブスクリプション(Subscription)] を選択します。
5. [リソースグループの場所(Resource group location)] を選択します。
6. [確認して作成(Review + create)] をクリックします。
7. [作成(Create)] をクリックします。

Azure Active Directory の URL とサブスクリプション ID の取得

Secure Cloud Analytics に Azure メタデータサービスへのアクセス権を提供するには、Azure Active Directory(AD)URL と Azure サブスクリプション ID を取得します。この情報を記録してください。このプロセスの最後に、この情報を Secure Cloud Analytics Web UI にアップロードして、Azure との統合を完了します。

AD URL とサブスクリプション ID の取得:

はじめる前に

- Azure ポータルにログインします。

手順

1. [Azure Active Directory] > [概要(Overview)] を選択します。
2. AD URL をコピーし、プレーンテキストエディタに貼り付けます。
3. [サブスクリプション(Subscriptions)] を選択し、自分のサブスクリプションを選択します。
4. サブスクリプション ID をコピーし、プレーンテキストエディタに貼り付けます。

Azure AD アプリケーションの作成

AD URL とサブスクリプション ID を取得したら、Secure Cloud Analytics がリソースグループからメタデータを読み取ることができるようにするアプリケーションを作成します。アプリケーションの作成が完了したら、アプリケーションキーをコピーします。

> Active Directory インスタンスごとに **1 つのアプリケーションのみ**を作成します。アプリケーションにロールを割り当てることで、Active Directory インスタンスの複数のサブスクリプションをモニターできます。詳細については、「**アプリケーションへの Azure ロールの割り当て**」を参照してください。

AD アプリケーションの作成:

はじめる前に

- Azure ポータルにログインします。

手順

1. [Azure Active Directory]、[アプリケーションの登録(App Registrations)]、[新規登録(New Registration)] の順に選択します。
2. [名前(Name)] に `swc-reader` と入力します。
3. [リダイレクトURI(Redirect URI)] ドロップダウンから [Web] を選択します。
4. デフォルトの [サポートされているアカウントタイプ(Supported Account Types)] の選択は変更しないでください。
5. リダイレクト URI として `https://obsrvbl.com/azure-api/swc-reader` と入力します。
6. [登録(Register)] をクリックします。
7. アプリケーション ID をコピーし、プレーンテキストエディタに貼り付けます。
8. [証明書と秘密(Certificates and Secrets)] > [新しいクライアント秘密(New Client Secret)] を選択します。
9. [説明(Description)] に `SWC Reader`と入力します。
10. [有効期日(Expires)] ドロップダウンから [期限なし(Never expires)] を選択します。
11. **[保存(Save)]**をクリックします。

12. アプリケーションキーの値をコピーし、プレーンテキストエディタに貼り付けます。

> このページから移動するとキーが表示されなくなるため、ここでアプリケーションキーをコピーします。

アプリケーションへの Azure ロールの割り当て

`swc-reader` アプリケーションを AD に登録した後、そのアプリケーションにネットワーク コントリビュータ ロールとモニターリング リーダー ロールを割り当てます。これにより、リソースグループからメタデータを読み取れるようになります。モニターするサブスクリプションごとに次の手順を実行します。

AD アプリケーションへのロールの割り当て:

はじめる前に

- Azure ポータルにログインします。

手順

1. [サブスクリプション(Subscriptions)] を選択し、自分のサブスクリプションを選択します。
2. [アクセス制御(IAM)(Access control (IAM))] を選択します。
3. [追加(Add)] > [ロール割り当ての追加(Add role Assignment)] を選択します。
4. [ネットワーク コントリビュータ ロール(Network Contributor Role)] を選択します。
5. [アクセス権の割り当て先(Assign access to)] ドロップダウンから Azure AD のユーザー、グループ、またはサービスプリンシパルを選択します。
6. [名前または電子メールアドレスで検索(Search by name or email address)] フィールドに `swc-reader` と入力して選択します。
7. **[保存(Save)]**をクリックします。
8. [追加(Add)] > [ロール割り当ての追加(Add role Assignment)] を選択します。
9. [モニターリングリーダーロール(Monitoring Reader Role)] を選択します。
10. [アクセス権の割り当て先(Assign access to)] ドロップダウンから Azure AD のユーザー、グループ、またはサービスプリンシパルを選択します。
11. ドロップダウンから `swc-reader` アプリケーションを選択します。
12. **[保存(Save)]**をクリックします。

フローログデータを保存するための Azure ストレージアカウントの作成

ネットワーク コントリビュータ ロールとモニターリングリーダーロールを `swc-reader` アプリケーションに割り当てたら、フローログデータを保存するストレージアカウントを作成します。リソースグループと同じ場所にバイナリラージオブジェクト(BLOB)ストレージアカウントを作成します。

> リソースグループと同じ場所にあり、そこに BLOB を保存できる場合は、既存のストレージアカウントを再利用できます。

BLOB ストレージアカウントを作成したら、ファイアウォールルールでインターネットからストレージアカウントへのアクセスが許可されていることを確認します。これにより、Secure Cloud Analytics と Azure の展開を適切に統合できます。

BLOB ストレージアカウントの作成：

はじめる前に

- Azure ポータルにログインします。

手順

1. [ストレージアカウント（Storage Accounts）] を選択します。
2. [追加（Add）] をクリックします。
3. [サブスクリプション（Subscription）] を選択します。
4. モニターする [リソースグループ（Resource group）] を選択します。
5. [ストレージアカウント名（Storage account name）] を入力します。
6. 指定したリソースグループと同じストレージアカウントの [場所（Location）] を選択します。
7. [アカウントの種類（Account kind）] として [ストレージv2（汎用）（Storage v2 (general purpose)）] を選択します。
8. 組織の要件に基づいて、ドロップダウンから [レプリケーション（Replication）] オプションを選択します。
9. ストレージアカウント内で BLOB にアクセスする頻度に応じて、[ホット（Hot）] または [クール（Cool）] アクセス階層を選択します。
10. [確認して作成（Review + create）] をクリックします。
11. [作成（Create）] をクリックします。

BLOB ストレージアカウントへのインターネットアクセスの有効化：

手順

1. BLOB ストレージアカウントから、[ファイアウォールと仮想ネットワーク（Firewalls and virtual network）] 設定を選択します。
2. [すべてのネットワークからのアクセスを許可（Allow access from All Networks）] を選択し、変更を保存します。

Azure ストレージアカウントの共有アクセス署名 URL の生成

ストレージアカウントを作成した後、ストレージアカウントからフローログデータを取得する権限を Secure Cloud Analytics に許可するために、ストレージアカウントの共有アクセス署名（SAS）を生成します。次に、BLOB サービス SAS URL をコピーします。Secure Cloud Analytics は、BLOB サービスSAS URL を使用して、ストレージアカウントからフローログデータを取得します。

> SAS 権限には、設定に基づく時間制限があります。SAS 権限が期限切れの場合、Secure Cloud Analytics はストレージアカウントからフローログデータを取得できません。

SAS URL の生成：

はじめる前に

- Azure ポータルにログインします。

手順

1. [その他のサービス（More Services）] > [ストレージ（Storage）] > [ストレージアカウント（Storage Accounts）] を選択します。
2. フローログデータを保存するように設定されたストレージアカウントを選択します。
3. [共有アクセス署名（Shared access signature）] を選択します。
4. [許可されるサービス（Allowed services）] で [BLOB] を選択します。
5. [許可されるリソースタイプ（Allowed resource types）] で [サービス（Service）]、[コンテナ（Container）]、および [オブジェクト（Object）] を選択します。
6. [許可される権限（Allowed permissions）] で [読み取り（Read）] および [リスト（List）] を選択します。
7. 現在の時刻に対応する [開始時刻（Start time）] を入力します。
8. 現在の時刻から少なくとも 1 年に対応する [終了時刻（End time）] を入力します。
9. [許可されるプロトコル（Allowed protocols）] で [HTTPS] を選択します。
10. [SASおよび接続文字列を生成（Generate SAS and connection string）] をクリックします。
11. BLOB サービス SAS URL をコピーし、プレーンテキストエディタに貼り付けます。

Azure Network Watcher の有効化

BLOB ストレージ SAS URL を生成した後、リソースグループを含むリージョンで Network Watcher を有効にします（まだ有効にしていない場合）。Azure では、ネットワーク セキュリティ グループのフローログを有効にするために、Network Watcher が必要です。

Network Watcher の有効化：

はじめる前に

- Azure ポータルにログインします。

手順

1. [Network Watcher] > [概要（Overview）] を選択します。
2. リージョンリストを選択して展開します。
3. リソースグループを含むリージョンのメニューを選択し、[Network Watcherの有効化（Enable Network Watcher）] を選択します。

Azure NSG フローログの有効化

Network Watcher を有効にした後、1 つ以上のネットワーク セキュリティ グループの NSG フローログを有効にします。これらのネットワーク セキュリティ グループは、モニターするリソースグループに対応している必要があります。

> BLOB ストレージアカウントは、NSG フローログの保持期間をサポートしていません。

フローロギングの有効化：

はじめる前に

- Azure ポータルにログインします。

手順

1. [Network Watcher] > [NSGフローログ（NSG Flow Logs）] を選択します。
2. ネットワーク セキュリティ グループを選択します。
3. [ステータス（Status）] で [オン（On）] を選択します。
4. [フローログバージョン2（Flow Logs Version 2）] を選択します。
5. 「**Azure ストレージアカウントの共有アクセス署名 URL の生成**」で SAS を設定した BLOB ストレージアカウントを選択します。
6. [トラフィック分析（Traffic Analytics）] ステータスとして [オフ（Off）] を選択します。

   > Secure Cloud Analytics では、トラフィック分析を有効にする必要はありませんが、この機能が必要な場合は有効にすることができます。

7. **[保存（Save）]**をクリックします。
8. フローロギングを有効にするネットワーク セキュリティ グループごとに、ステップ 2 ～ 7 を繰り返します。

Azure アクティビティログストレージの有効化

Secure Cloud Analytics には、サブスクリプションレベルのイベントに対する追加の可視性とセキュリティ検出機能があります。この機能を有効にするには、アクティビティログのストレージアカウントへのエクスポートを設定します。

アクティビティログをストレージアカウントにエクスポート:

手順

1. Azur eポータルから、[モニター（Monitor）] > [アクティビティログ（Activity Log）] > [診断設定（Diagnostic Settings）] の順に選択します。
2. バナーをクリックして、[アクティビティログのエクスポート（Export activity log）] ブレードを起動します。
3. 表示されるブレードで、次を指定します。
   - ドロップダウンから [サブスクリプション（Subscription）] を選択します。
   - ドロップダウンからエクスポートする [リージョン（Regions）] を選択します。
   - [レガシーエクスペリエンス（Legacy experience）] を選択します。
   - [ストレージアカウントへエクスポート（Export to storage account）] を選択します。
   - 設定したストレージアカウントを選択します。
   - [保持日数（Retention（days））] で 7 を選択します。
4. **[保存（Save）]**をクリックします。

Secure Cloud Analytics Azure との統合

フローロギングを設定したら、Secure Cloud Analytics Web UI に次の情報を入力して Azure との統合を完了します。

- Azure AD の URL
- サブスクリプション ID
- アプリケーション ID（Application ID）

- アプリケーションキー
- BLOB サービス SAS URL

Azure からフローログデータを取得するための Secure Cloud Analytics の設定：

はじめる前に

- 管理者アカウントで Secure Cloud Analytics Web UI にログインします。
- AD の URL とサブスクリプション ID の詳細については、「**Azure Active Directory の URL とサブスクリプション ID の取得**」を参照してください。
- アプリケーション ID とキーの詳細については、「**Azure AD アプリケーションの作成**」を参照してください。
- BLOB サービス SAS URL の詳細については、「**Azure ストレージアカウントの共有アクセス署名 URL の生成**」を参照してください。

手順

1. [設定（Settings）] > [統合（Integrations）] > [Azure] > [クレデンシャル（Credentials）] を選択します。
2. [新しいクレデンシャルの追加（Add New Credentials）] をクリックします。
3. Azure AD の URL を入力します。
4. Azure アプリケーション ID を入力します。
5. Azure アプリケーションキーを入力します。
6. [作成（Create）] をクリックします。
7. [ストレージアクセス（Storage Access）] をクリックします。
8. [新規統合（New Integration）] をクリックします。
9. [APIキー（API Key）] フィールドに **BLOB サービス SAS URL** を入力します。
10. [作成（Create）] をクリックします。
11. [サブスクリプション（Subscriptions）] を選択し、サブスクリプションがリストされていることを確認します。

Secure Cloud Analytics Web ポータルの設定

ここでは、初期設定をセットアップするために Secure Cloud Analytics Web ポータルで使用可能な推奨設定オプションについて説明しています。オプションには次のものがあります。

- プライベートネットワークのモニタリングセンサー 設定:
- アラート設定
- サブネット設定
- ユーザーおよびサイト管理

プライベートネットワークのモニタリング Sensor設定

ネットワーク上に センサー を展開したら、Secure Cloud Analytics Web UI を使用して次の項目を設定できます。

- センサー の表示名
- ネットワーク モニターリングの設定
- Syslog 出力の設定
- SNMP レポートの設定

パブリック IP アドレスに基づいて センサー を追加したり、センサー のログを表示することもできます。

パブリック IP アドレスによるSensorの追加

IP アドレスを使用して センサー を Secure Cloud Analytics Web UI に追加できます。センサー を展開したら、センサー に SSH 接続し、ログインしてその IP アドレスを取得します。

センサー のパブリック IP アドレスの取得:

はじめる前に

- 管理者として センサー のコンソールにログインします。

手順

1. コマンド プロンプトで「`curl https://sensor.ext.obsrvbl.com`」と入力し、Enter キーを押します。`error` 値の `unknown identity` は、センサー が Secure Cloud Analytics 展開に関連付けられていないことを意味します。
2. `identity` IP アドレスをコピーします。
3. センサー からログアウトします。

パブリック IP アドレスによる センサー の追加:

はじめる前に

- Secure Cloud Analytics Web UI にログインします。

手順

1. **(センサー)アイコン > [パブリックIP(Public IP)]** を選択します。
2. [パブリックIP(Public IP)] フィールドに `identity` IP アドレスを入力します。
3. [IPの追加(Add IP)] をクリックします。ポータルと センサー がキーを交換した後は、パブリック IP アドレスではなくキーを使用して以降の接続が確立されます。

> Secure Cloud Analytics Web UI に センサー が表示されるまでに最大 10 分かかる可能性があります。

Sensorの表示ラベルの設定

Secure Cloud Analytics Web UI では、センサー の表示ラベルを設定できます。

センサー の表示ラベルの設定:

手順

1. [設定(Settings)] > [Sensor(Sensors)] > [Sensorリスト(Sensor List)] を選択します。
2. Syslog 出力を設定する センサー に対して、[設定の変更(Change Settings)] をクリックします。
3. [ラベル(Label)] タブを選択します。
4. **ラベル**を入力します。
5. **[保存(Save)]**をクリックします。

Sensorのモニターリング設定

Secure Cloud Analytics Web UI では、センサー がモニターするサブネットを設定できます。また、パッシブ DNS を使用する場合は、キャプチャする 1 秒あたりのパケット数を設定できます。センサーの設定からサブネット範囲を削除すると、そのサブネットから送信されたパケットを無視するようにセンサー に指示されます。

センサー のモニター対象ネットワークにリストされていない IP アドレスに対してなぜエンティティが作成されるのか、混乱が生じます。これは、モニター対象範囲にリスト**されている**エンティティが、リストされていない範囲と通信しているためです。

たとえば、`192.168.0.0/24` の範囲だけをモニターするように設定された センサー があるとします。システムは、その範囲のトラフィックを送信する IP アドレスをエンティティと見なします。さらに、`192.168.0.0/24` の範囲内のエンティティが `10.0.0.0/8` の範囲内の IP アドレスと通信していることが確認された場合、`192.168.0.0/24` はモニター対象範囲と見なされるため、センサー はそのトラフィックをモニターします。次の理由により、システムはモニター対象でない `10.0.0.0/8` の範囲にある他の IP アドレスのエンティティも作成します。

- `10.0.0.0/8` の範囲は RFC 1918 スペースの一部である、および
- その範囲の IP アドレスがモニター対象の IP アドレスと通信していることが確認された。

センサー によるモニターリング用に 10.0.0.0/8 の範囲が定義されておらず、10.0.0.0/8 サブネット内の 2 つの IP アドレスが相互に通信するだけの場合、どちらも定義されたサブネットと直接通信していないため、どちらもエンティティとは見なされません。

センサー のモニターリングの設定

手順

1. [設定(Settings)] > [Sensor(Sensors)] > [Sensorリスト(Sensor List)] を選択します。
2. 設定する センサー について、[設定の変更(Change Settings)] をクリックします。
3. [モニターリング(Monitoring)] タブを選択します。
4. 1 つ以上の CIDR ブロックを [モニターするネットワーク(Networks to monitor)] フィールドに 1 行に 1 つずつ追加します。
5. **PDNS に関してキャプチャする 1 秒あたりのパケット数**を選択します。
6. **[保存(Save)]**をクリックします。

Sensorの Syslog 設定

Secure Cloud Analytics Web UI では、検出されたエンティティの観測内容とアラートをリモート Syslog サーバーに送信するように センサー を設定できます。

センサー の Syslog 設定:

手順

1. [設定(Settings)] > [Sensor(Sensors)] > [Sensorリスト(Sensor List)] を選択します。
2. Syslog 出力を設定する センサー に対して、[設定の変更(Change Settings)] をクリックします。
3. [Syslog] タブを選択します。
4. [Syslog公開の有効化(Enable syslog publishing)] を選択します。
5. [ユーザーSyslogファシリティ(user Syslog facility)] を選択します。
6. **Syslog サーバーの IP アドレス**を入力します。
7. **と Syslog サーバーの間の通信に使用する センサー サーバーポート**を入力します。
8. **[保存(Save)]**をクリックします。

Sensorの SNMP レポートの設定

Secure Cloud Analytics Web UI では、SNMP 情報(OID など)を SNMP サーバーにレポートするように センサー を設定できます。

センサー の SNMP レポートの設定:

手順

1. [設定(Settings)] > [Sensor(Sensors)] > [Sensorリスト(Sensor List)] を選択します。
2. Syslog 出力を設定する センサー に対して、[設定の変更(Change Settings)] をクリックします。

3. [SNMP] タブを選択します。
4. [SNMP レポートの有効化(Enable SNMP reporting)] を選択します。
5. **SNMP のバージョン**を選択します。
6. [コミュニティ/ユーザー(Community/User)] と関連する [パスフレーズ(Passphrase)] を入力します。
7. **Sensorの engineID** を入力します。
8. **OID(ASN.1)**を入力します。
9. センサー のレポート先となる **SNMP サーバー**を入力します。
10. センサー と SNMP サーバーの間の通信に使用される**サーバーポート(TRAP)**を入力します。
11. **[保存(Save)]**をクリックします。

Sensorのログの表示

Secure Cloud Analytics Web UI で センサー のログメッセージを表示できます。また、ログメッセージをカンマ区切り値ファイルでダウンロードできます。

センサー のログの表示:

手順

1. [設定(Settings)] > [Sensor(Sensors)] > [Sensorリスト(Sensor List)] を選択します。
2. [**Sensorリスト(Sensor List)**] を選択します。
3. ログを表示する センサー について、[ログへのアクセス(Access Logs)] ペインで [最新(Most Recent)] をクリックします。

情報を含むカンマ区切りファイルのダウンロード:

手順

- ダウンロードする表の [CSV] をクリックします。

アラート設定

[アラート(Alerts)] 設定により、次の項目を設定できます。

- アラートの有効期限
- アラートの優先順位
- IP スキャナ ルール
- ウォッチリスト エントリ

アラート優先順位設定

アラート タイプにはデフォルトの優先順位が設定されています。これは、このタイプのアラートを生成するシステムの機密性に影響します。アラートの優先順位は [低(low)] または [通常(normal)] にデフォルト設定されます。そのアラート タイプの優先順位も [低(low)]、[通常(normal)]、または [高(high)] に設定できます。

アラートの優先度は、アラートが自動的に閉じるかどうかを決定するためにサブネットの感度と組み合わせて使用されます。たとえば、[過剰アクセス試行回数(外部)(Excessive Access Attempts (External))] アラート タイプの優先順位はデフォルトで [低(low)] に設定されます。このアラートは、[高(High)] に設定されていないサブネットに対しては自動的にクローズされます。

アラート優先順位の更新

手順

1. 次の選択肢があります。
   - [設定(Settings)] > [アラート(Alerts)] > [優先順位(Priorities)] を選択します。
   - [モニター(Monitor)] > [アラート(Alerts)] を選択し、次に [関連する設定リンク(Related Config Links)] > [アラートの優先順位(Alert Priorities)] を選択します。
2. アラートタイプには、ドロップダウンからアラートの**優先順位**を選択します。

国のウォッチリストの設定

地理的位置情報に基づいてリストに含まれる国に関連するトラフィックに関するアラートを生成するように国のウォッチリストを設定できます。

国のウォッチリストのエントリの変更:

手順

1. [設定(Settings)] > [アラート(Alerts)] > [国のウォッチリスト(Country Watchlist)] を選択します。
2. [フィルタ(Filters)] ペインをクリックして展開します。
3. 国を選択して国のウォッチリストに追加するか、国の選択を解除して国のウォッチリストから削除します。

ウォッチリスト設定

ウォッチリストは、特定のエンティティからのトラフィックによってアラートが生成されるかどうかを制御します。エンティティに関連するトラフィックによって常にアラートが生成されるようにエントリを設定できます。また、設定した時間が経過すると期限切れになるようにウォッチリスト エントリを設定することもできます。期限切れになると、それらのエンティティに関連するトラフィックによってアラートが生成されなくなります。

Secure Cloud Analytics は、サードパーティの脅威インテリジェンスリストによってこれらのエンティティに関連するアラートを生成することをサポートしています。

内部接続ウォッチリストの設定

CIDR ブロックまたはエンティティグループのいずれかを追加することで、内部エンティティ間の接続を内部接続ブラックリストに追加できます。システムがこのリストにあるエントリに関連するトラフィックを検出すると、アラートが生成されます。トラフィックを許可してアラートを生成しないようにエントリを設定することもできます。

すべてのエントリを含むカンマ区切り値ファイルをダウンロードできます。

内部接続ウォッチリストへのエントリの追加:

手順

1. [設定(Settings)]>[アラート(Alerts)]>[内部接続ウォッチリスト(Internal Connections Watchlist)]を選択します。
2. [新しいウォッチリスト項目(New Watchlist Item)]をクリックします。
3. ウォッチリストエントリの[ルール名(Rule Name)]と[説明(Description)]を入力します。
4. このエントリに一致する接続で観測内容やアラートが生成されないようにするには、[許可(Allowed)]の[接続ルールタイプ(Connection Rule Type)] を選択します。このエントリに一致する接続で観測内容やアラートが生成されるようにするには、[不可(NOT Allowed)] を選択します。

   [許可(Allowed)] ルールを追加する前に、少なくとも 1 つの[不可(NOT Allowed)] ルールを内部接続ウォッチリストに追加する必要があります。
5. ドロップダウンリストから[プロトコル(Protocol)]を選択します。
6. [送信元(Source)]を選択してフィールドを展開します。
7. 次の選択肢があります。

   [CIDR]を選択し、[IPアドレス(IP Address)]と[バイト/長さ(Bytes/Length)]を入力して、送信元 CIDR ブロックを定義します。表示される IP アドレスだけをモニターする場合は、[バイト/長さ(Bytes/Length)]に「32」と入力し、より大きな CIDR ブロック値をモニターするには、異なる値を入力します。

   [エンティティグループ(Entity Groups)]を選択し、[エンティティグループを追加(Add Entity Group(s))]をクリックして 1 つ以上のエンティティグループを選択し、[送信元に追加(Add to Source)]をクリックします。
8. 送信元を特定のポートに制限する場合は、個別の送信元**ポート**またはポート範囲を入力します。
9. [宛先(Destination)]を選択してフィールドを展開します。
10. 次の選択肢があります。

    [CIDR]を選択し、[IPアドレス(IP Address)]と[バイト/長さ(Bytes/Length)]を入力して、宛先 CIDR ブロックを定義します。表示される IP アドレスだけをモニターする場合は、[バイト/長さ(Bytes/Length)]に「32」と入力し、より大きな CIDR ブロック値をモニターするには、異なる値を入力します。

    [エンティティグループ(Entity Groups)]を選択し、[エンティティグループを追加(Add Entity Group(s))]をクリックして 1 つ以上のエンティティグループを選択し、[宛先に追加(Add to Destination)]をクリックします。
11. 宛先を特定のポートに制限する場合は、個別の宛先**ポート**またはポート範囲を入力します。
12. **[保存(Save)]**をクリックします。

エントリの削除:

手順

1. [設定(Settings)]>[アラート(Alerts)]>[内部接続ウォッチリスト]を選択します。
2. 削除するエントリの横にある  **(削除)**アイコンをクリックします。

情報を含むカンマ区切りファイルのダウンロード:

手順

- ダウンロードする表の [CSV] をクリックします。

サードパーティ ウォッチリストの設定

サードパーティ ウォッチリストを Secure Cloud Analytics に追加し、信頼できるサードパーティ送信元のソースからの脅威インテリジェンスを使用してアラートを生成することができます。

これらのエントリが自動的に期限切れになるように設定するか、ルールを手動で期限切れにする（これ以降、アラートが生成されなくなる）ことができます。期限切れにならないように設定することもできます。この場合、これらのエンティティに関連するトラフィックが検出されると常にアラートが生成されます。ルールが期限切れになった場合は、手動で元に戻すことができます。

サードパーティ ウォッチリストへのエントリの追加:

手順

1. [設定（Settings）] > [アラート（Alerts）] > [サードパーティ ウォッチリスト（Third Party Watchlist）] を選択します。
2. [外部URLの追加（Add External URL）] をクリックします。
3. ウォッチリストのエントリ**名**を入力します。
4. サードパーティ ウォッチリストをポストする**リソース** URL を入力します。
5. このエントリを無期限に機能させるには、[無期限（Never Expire）] を選択します。それ以外の場合は、将来の**有効期限日**を選択してください。
6. システムがアラートを生成する前に検出するウォッチリスト上のエンティティの最小数の**しきい値**を入力します。この値は、1 より大きくする必要があります。
7. このエンティティに関連する双方向トラフィックが検出された場合にのみアラートが生成されるようにするには、[双方向トラフィックのみ（Bidirectional traffic only）] を選択します。
8. エントリの**理由**を入力します。
9. [作成（Create）] をクリックします。

エントリの手動による有効期限切れ:

手順

1. [設定（Settings）] > [アラート（Alerts）] > [サードパーティ ウォッチリスト（Third Party Watchlist）] を選択します。
2. 削除するアクティブテーブルの横にある  **（削除）**アイコンをクリックします。

期限切れのエントリの復元:

手順

1. [設定（Settings）] > [アラート（Alerts）] > [サードパーティ ウォッチリスト（Third Party Watchlist）] を選択します。
2. 復元する有効期限切れテーブルの横にある  **（削除）**アイコンをクリックします。

IP およびドメインのウォッチリストの設定

IP およびドメインウォッチリストに外部ドメイン名または IP アドレスを追加できます。システムがこのリストにあるエンティティに関連するトラフィックを検出すると、アラートが生成されます。

これらのエントリが自動的に期限切れになるように設定するか、ルールを手動で期限切れにする（これ以降、アラートが生成されなくなる）ことができます。期限切れにならないように設定することもできます。この場合、これらのエンティティに関連するトラフィックが検出されると常にアラートが生成されます。ルールが期限切れになった場合は、手動で削除することができます。

IP およびドメインウォッチリストへのエントリの追加：

手順

1. [設定（Settings）] > [アラート（Alerts）] > [IPおよびドメインウォッチリスト（IPs and Domain Watchlist）] を選択します。
2. [ドメインまたはIPの追加（Add Domain or IP）] をクリックします。
3. ウォッチリストのエントリ**名**を入力します。
4. トラフィックがアラートをトリガーする**リソース**ドメイン名または IP アドレスを入力します。
5. このエントリを無期限に機能させるには、[無期限（Never Expire）] を選択します。それ以外の場合は、将来の**有効期限日**を選択してください。
6. このエンティティに関連する双方向トラフィックが検出された場合にのみアラートが生成されるようにするには、[双方向トラフィックのみ（Bidirectional traffic only）] を選択します。
7. エントリの**理由**を入力します。
8. [作成（Create）] をクリックします。

エントリの手動による有効期限切れ：

手順

1. [設定（Settings）] > [アラート（Alerts）] > [IPおよびドメインウォッチリスト（IPs and Domains Watchlist）] を選択します。
2. 期限切れにするアクティブなエントリの横にある（編集）アイコン をクリックします。
3. [期限なし（Never Expire）] をオフにします。
4. [有効期限（Expiration Date）] を入力します。
5. **[保存（Save）]**をクリックします。

期限切れのエントリの削除：

手順

1. [設定（Settings）] > [アラート（Alerts）] > [IPおよびドメインウォッチリスト（IPs and Domain Watchlist）] を選択します。
2. 削除する有効期限切れテーブルの横にある **（削除）**アイコンをクリックします。

IP およびドメイン ウォッチリスト エントリ ファイルのアップロード

複数のウォッチリスト エントリ（1 行に 1 エントリずつ）を含むコンマ区切り値ファイルをアップロードできます。ファイルには、ドメイン名、IP アドレス、またはその両方を含めることができます。各行は次の形式である必要があります。

`<title>,<reason>,<identifier>,[is_bidirectional],[expires_on],[threshold]`

詳細については、次の各項を参照してください。

パラメータ	必須	使用可能な値
`<title>`	はい	任意の英数字。
`<reason>`	はい	任意の英数字。
`<identifier>`	はい	次のいずれかです。 • 有効なドメイン名 • 有効な IPv4 アドレス
`[is_bidirectional]`	いいえ	次のいずれかです。 • `true`:このエンティティに関連する双方向トラフィックが検出された場合にのみアラートが生成されます。 • `false`:このエンティティに関連する単方向または双方向トラフィックが検出された場合にアラートが生成されます。 未定義の場合、デフォルトは `false`。
`[expires_on]`	いいえ	タイムスタンプの形式: *`YYYY-MM-DDTHH:SS`* 未定義の場合、このウォッチリスト エントリは期限切れになりません。
`[threshold]`	いいえ	システムがアラートを生成する前にこのエンティティを検出する回数を表す正の整数。 未定義の場合、デフォルトは `1`。

ドメイン名または IP アドレス ウォッチリスト エントリ ファイルのアップロード:

手順

1. [設定(Settings)]>[アラート(Alerts)]>[IPおよびドメインウォッチリスト(IPs and Domains Watchlist)]を選択します。
2. [CSV のアップロード(Upload CSV)]をクリックします。
3. [ファイルのアップロード(Upload File)]をクリックして、アップロードするファイルを選択します。

AWS CloudTrail イベント ウォッチリストの設定

特定の AWS アカウントに対して生成された特定の AWSCloudtrail イベントに関してアラートを生成するようにウォッチリストを設定できます。

> AWS 統合を有効にする場合は、`obsrvbl_policy` ポリシーに `cloudtrail:LookupEvents` 権限が含まれていることを確認してください。シスコによって提供される AWSpolicy 設定にはこの権限が含まれています。

ウォッチリストのエントリを含むカンマ区切り値ファイルをダウンロードすることもできます。

AWS CloudTrail アラート ウォッチリストへのエントリの追加:

手順

1. [設定(Settings)] > [アラート(Alerts)] > [AWS CloudTrailウォッチリスト(AWS CloudTrail Watchlist)] を選択します。
2. [新しいウォッチリスト項目(New Watchlist Item)] をクリックします。
3. システムがモニター対象の AWS アカウントのいずれかで CloudTrail イベントを検出した場合にアラートを生成させるには、ドロップダウンから AWS **アカウント ID** を選択するか、[<Any Account ID>] を選択します。
4. CloudTrail **イベント**を入力します。サポートされているイベントの詳細については、CloudTrail イベントに関する AWS ドキュメントを参照してください。
5. [作成(Create)] をクリックします。

情報を含むカンマ区切りファイルのダウンロード:

手順

- ダウンロードする表の [CSV] をクリックします。

GCP ロギング ウォッチリストの設定

特定の GCP プロジェクトに対して生成された特定の GCP イベントに関してアラートを生成するようにウォッチリストを設定できます。

ウォッチリストのエントリを含むカンマ区切り値ファイルをダウンロードすることもできます。

GCP ロギング ウォッチリストへのエントリの追加:

手順

1. [設定(Settings)] > [アラート(Alerts)] > [GCPロギング ウォッチリスト(Country Watchlist)] を選択します。
2. [新しいウォッチリスト項目(New Watchlist Item)] をクリックします。
3. [GCPアクション(GCP Action)] を入力します。使用可能なアクションの詳細については、GCP のドキュメントを参照してください。
4. システムがモニター対象の GCP プロジェクトのいずれかでアクションを検出した場合にアラートを生成させるには、ドロップダウンから **GCP プロジェクト ID** を選択するか、[<Any

Account ID>] を選択します。

5. [作成(Create)] をクリックします。

情報を含むカンマ区切りファイルのダウンロード:

手順

- ダウンロードする表の [CSV] をクリックします。

IP スキャナルールの設定

ネットワーク上の信頼できる悪意のないスキャナに関するアラートを抑制するように IP スキャナルールを設定できます。たとえば、侵入テスト担当者が脆弱性を検索する場合は、それらのトラフィックに一致する IP スキャナ ルールを追加できます。

IP スキャナルールの設定:

手順

1. [設定(Settings)] > [アラート(Alerts)] > [IPスキャナ ルール ウォッチリスト(IP Scanner Rules Watchlist)] を選択します。
2. [Add Rule] をクリックします。
3. 特定の IP アドレスに関するアラートを抑制する場合は、**IP アドレス**を入力します。
4. CIDR ブロックに関するアラートを抑制する場合は、**CIDR 長**(/1 ～ /32)を入力します。
5. スキャンしてアラートから除外する**接続済みアドレス**を、IP アドレス、CIDR ブロック範囲、または IP アドレス範囲や、IP アドレス、CIDR ブロック範囲、または IP アドレス範囲のカンマ区切りリストとして入力します。
6. スキャンしてアラートから除外する**接続済みポート**を、ポートまたはポート範囲や、ポートまたはポート範囲のカンマ区切りリストとして入力します。
7. Secure Cloud Analytics Web UI にルールの説明を表示する場合は、**説明**を入力します。
8. [作成(Create)] をクリックします。

Azure アクティビティ ログ ウォッチリストの設定

特定の Azure イベントに関してアラートを生成するようにウォッチリストを設定できます。

ウォッチリストのエントリを含むカンマ区切り値ファイルをダウンロードすることもできます。

GCP ロギングウォッチリストへのエントリの追加:

手順

1. [設定(Settings)] > [アラート(Alerts)] > [Azureアクティビティ ログ ウォッチリスト(Azure Activity Log Watchlist)] を選択します。
2. [新しいウォッチリスト項目(New Watchlist Item)] をクリックします。
3. システムがモニター対象の Azure プロジェクトのいずれかでアクションを検出した場合にアラートを生成させるには、ドロップダウンから**サブスクリプション ID** を選択するか、[<Any Subscription ID>] を選択します。

4. 操作（またはアクション）を入力します。使用可能なアクションの詳細については、Azure のドキュメントを参照してください。
5. [作成（Create）] をクリックします。

情報を含むカンマ区切りファイルのダウンロード：

手順

- ダウンロードする表の [CSV] をクリックします。

Azure Advisor ウォッチリストの設定

Azure Advisor の推奨事項が Secure Cloud Analytics の観測内容として取り込まれるように設定できます。これらの観測内容を取り込んだ後、システムはそれらに基づいてアラートを生成できます。

ウォッチリストのエントリを含むカンマ区切り値ファイルをダウンロードすることもできます。

Azure Advisor の推奨事項を観測内容としての取り込むことを有効化：

手順

1. [設定（Settings）] > [アラート（Alerts）] > [Azure Advisorウォッチリスト（Azure Advisor Watchlist）] を選択します。
2. Secure Cloud Analytics が観測内容として Advisor の推奨事項を取り込むことができるようにするには、[観測中（Watching）] を選択します。

情報を含むカンマ区切りファイルのダウンロード：

手順

- ダウンロードする表の [CSV] をクリックします。

アラートの有効期限の更新

どのユーザーもアラートのステータスをクローズにしていない場合、有効期限を過ぎると、アラートのステータスが自動的にクローズになります。更新する必要がある場合は、クローズになった後に、再度オープンにすることができます。

無期限にオープン ステータスが維持されるようにアラートを設定できます。

アラートの有効期限の更新：

手順

1. [設定（Settings）] > [アラート（Settings）] > [アラートの有効期限（Alert Expiration）] を選択します。
2. **アラートが期限切れになるまでの日数**を入力します。「0」を入力すると、アラートのステータスが無期限にオープンになります。
3. **[保存（Save）]**をクリックします。

クラウド ポスチャ ウォッチリストの確認

システムがパブリック クラウド アカウントを評価する際に照会するクラウド ポスチャ フレームワークと推奨事項を確認できます。

クラウド ポスチャ ウォッチリストの確認：

手順

1. [設定（Settings）] > [アラート（Alerts）] > [クラウド ポスチャ ウオッチリスト（Cloud Posture Watchlist）] を選択します。
2. [フィルタ（Filters）] をクリックして [フィルタ（Filters）] ペインを展開します。
3. **説明のキーワード**、**プロバイダーとフレームワークのバージョン**、**推奨事項 ID**、**レベル**、または**重大度**に基づいて、フレームワークの推奨事項をフィルタリングします。
4. **並べ替えの基準**とするフィールドを選択し、結果を**昇順**または**降順**のどちらで表示するかを選択します。
5. [適用（Apply）] をクリックしてフィルタを適用します。

エンティティグループの設定

ユーザー定義のサブネットと CIDR ブロックをグループ化する、Secure Cloud Analytics 展開のエンティティグループを設定できます。その後、内部接続ウォッチリストエントリにこれらのグループを使用して、エンティティごとに個別のエントリを作成するのではなく、複数のエンティティまたは特定のブロックの IP アドレスの可能なエンティティをモニターできます。

サブネットを追加するには、まず [サブネット（Subnets）] 設定でサブネットを設定します。詳細については、「サブネットの設定」を参照してください。

CIDR ブロックを追加するには、それらを個別に定義するか、複数の CIDR ブロックを含むカンマ区切り値（CSV）ファイルをアップロードします。ファイル内の各エントリは、`prefix,length` 形式に従う必要があり、1 行につき最初のエントリのみがアップロードされます。システムが重複 CIDR ブロックを検出した場合、重複ブロックはエンティティグループに追加されません。

エンティティグループの設定

エンティティグループの作成：

手順

1. [設定（Settings）] > [エンティティグループ（Entity Groups）] を選択します。
2. [新しいエンティティグループ（New Entity Group）] をクリックします。
3. エンティティグループの [名前（Name）] と [説明（Description）] を入力します。
4. [次へ（Next）] をクリックします。

   [サブネット（Subnets）] タブが表示されます。
5. サブネットを追加する場合は、次のオプションがあります。
   - [サブネットを追加（Add Subnets）] ペインから 1 つ以上のサブネットを選択し、[選択したものをグループに追加（Add Selected to Group）] をクリックしてエンティティグループに追加します。

- [現在グループ内にある(Currently In Group)] ペインから 1 つ以上のサブネットを選択し、[選択したものを削除(Delete Selected)] をクリックしてエンティティグループから削除します。

サブネットの作成についての詳細は、「サブネットの設定」を参照してください。

6. [CIDRs] タブを選択します。
7. CIDR ブロックを追加する場合は、次のオプションがあります。
   - [CIDRプレフィックス(CIDR Prefix)] と [長さ(Length)] を入力し、[追加(Add)] をクリックして 1 つの CIDR ブロックをエンティティグループに追加します。表示される IP アドレスだけをモニターする場合は、[長さ(Length)] に「32」と入力し、より大きな CIDR ブロック値をモニターするには、異なる値を入力します。
   - [参照(Browse)] をクリックし、`prefix,length` の形式で CIDR ブロックを含む CSV ファイルを 1 行に 1 エントリずつ選択し、[アップロード(Upload)] をクリックして各行の最初の CIDR ブロックをエンティティグループに追加します。
8. [作成(Create)] をクリックします。

エンティティグループの変更:

手順

1. [設定(Settings)] > [エンティティグループ(Entity Groups)] を選択します。
2. 既存のエンティティグループの [編集(Edit)] をクリックします。
3. エンティティグループに異なる [名前(Name)] と [説明(Description)] を入力します。
4. [サブネット(Subnets)] タブを選択します。
5. 次の選択肢があります。
   - [CIDRプレフィックス(CIDR Prefix)] と [長さ(Length)] を入力し、[追加(Add)] をクリックして 1 つの CIDR ブロックをエンティティグループに追加します。表示される IP アドレスだけをモニターする場合は、[長さ(Length)] に「32」と入力し、より大きな CIDR ブロック値をモニターするには、異なる値を入力します。
   - [参照(Browse)] をクリックし、`prefix,length` の形式で CIDR ブロックを含む CSV ファイルを 1 行に 1 エントリずつ選択し、[アップロード(Upload)] をクリックして各行の最初の CIDR ブロックをエンティティグループに追加します。
6. [CIDRs] タブを選択します。
7. 次の選択肢があります。
   - [サブネットを追加(Add Subnets)] ペインから 1 つ以上のサブネットを選択し、[選択したものをグループに追加(Add Selected to Group)] をクリックしてエンティティグループに追加します。
   - [現在グループ内にある(Currently In Group)] ペインから 1 つ以上のサブネットを選択し、[選択したものを削除(Delete Selected)] をクリックしてエンティティグループから削除します。

   サブネットの作成についての詳細は、「サブネットの設定」を参照してください。
8. [完了(Done)] をクリックして変更を保存します。

エンティティグループの削除

手順

1. [設定(Settings)] > [エンティティグループ(Entity Groups)] を選択します。
2. 既存のエンティティグループの削除アイコンをクリックし、選択を確認します。

サブネット設定

ローカル、仮想クラウド、および VPN サブネット内のエンティティに対するアラートの生成方法を設定できます。また、エンティティグループに設定済みのサブネットを追加して、エンティティグループにエンティティの範囲を一度に追加することもできます。設定とサブネットタイプに基づいて、サブネットの感度を設定できます。これにより、サブネットの設定に基づいてシステムが生成するアラートが調整されます。サブネット範囲内の新しいエンティティを検出した場合にシステムがアラートを生成するかどうかも設定できます。詳細については、次の各項を参照してください。

サブネットタイプ	設定オプション	推奨されるサブネット範囲
ローカル(Local)	• サブネット範囲 • アラート生成の相対しきい値 • サブネット内で IP アドレスが静的または動的に割り当てられるかどうか • サブネット範囲内で検出された新しいエンティティに対してアラートを生成するかどうか	• オンプレミスネットワーク展開のローカルエンティティ • 制御対象のオンプレミスネットワーク展開の外部にあるエンティティ
仮想クラウド(AWS および GCP)	• サブネット範囲 • アラート生成の相対しきい値 • サブネット範囲内で検出された新しいエンティティに対してアラートを生成するかどうか	• クラウドベースのネットワーク展開のクラウドエンティティ
VPN	• サブネット範囲	• 追跡対象ではない、重複が原因でネットワーク変換が必要な VPN 内のエンティティ • サードパーティによって制御される、ネットワーク展開の外部にあるエンティティ

ローカル サブネット アラート設定の指定

ローカルサブネットは、主にオンプレミス展開用に設定します。具体的には、オンプレミスネットワークに対してローカルなエンティティ、または制御対象のオンプレミスネットワークの外部にあるエンティティのローカルサブネットを設定できます。一度に 1 つのエントリを追加することも、複数のエントリをカンマ区切り値（CSV）ファイルでアップロードすることもできます。

ローカルサブネットを追加する際に、次のローカルサブネットのアラート設定を行うことができます。

パラメータ	説明
プレフィックス	IPv4 形式のサブネットプレフィックス。
長さ	CIDR 表記のサブネット長（1 ～ 32）。詳細については、https://tools.ietf.org/html/rfc4632 を参照してください。
デフォルトのエンドポイント感度	生成可能なアラートに影響するデフォルトのサブネット感度： • [高（high）]：システムは、[低（low）]、[通常（normal）]、および [高（high）] 優先度のアラートを生成できます。 • [通常（normal）]：システムは、[通常（normal）] および [高（high）] 優先度のアラートを生成できます。 • [低（low）]：システムは、[高（high）] 優先度のアラートを生成できます。 • [なし（none）]：システムはアラートを生成しませんが、このサブネットのトラフィックをモニターします。
説明	インターフェイスに表示されるローカルサブネットの説明。

Cisco Secure Cloud Analytics センサー（旧 Stealthwatch Cloud センサー）のモニターリング設定からデフォルトの内部サブネットを削除しても、システムは引き続きこれらのサブネット内のエンティティに対して動的エンティティモデリングを実行します。これらのエンティティでアラートの受信を停止するには、サブネットをローカルサブネットとして明示的に追加し、感度を [なし（none）] に設定する必要があります。

ローカルサブネットを追加した後、次のアラート生成設定を行うことができます。

パラメータ	説明
Sensitivity	サブネットの感度は、生成可能なアラートに影響します。 • [高(high)]:システムは、[低(low)]、[通常(normal)]、および [高(high)] 優先度のアラートを生成できます。 • [通常(normal)]:システムは、[通常(normal)] および [高(high)] 優先度のアラートを生成できます。 • [低(low)]:システムは、[高(high)] 優先度のアラートを生成できます。 • [なし(none)]:システムはアラートを生成しませんが、このサブネットのトラフィックをモニターします。
Static	エンティティに、このサブネット内の IP アドレスが静的に割り当てられているのか、DHCP などによって動的に割り当てられているのか。このサブネット内のエンティティが、静的に割り当てられた IP アドレスを受信すると、システムは、IP アドレスが常に同じエンティティと相関すると見なします。
New Device Alerts	このサブネットに新しいデバイスが出現した場合に、システムがこのサブネットに関してアラートを生成するかどうか。 このサブネットの静的 IP 割り当ても有効にする場合にのみ、このパラメータを有効にすることをお勧めします。動的に割り当てられた IP アドレスは、既存のデバイスに異なる IP アドレスが動的に割り当てられるたびに、システムに過剰な量の新しいデバイス アラートを生成させる可能性があります。

ローカル サブネット アラート設定へのエントリの追加:

手順

1. [設定(Settings)] > [サブネット(Subnets)] > [オンプレミス(On-Premises)] を選択します。
2. [オンプレミスサブネットの作成(Create On-Premises Subnet)] をクリックします。
3. CIDR ブロックの**プレフィックス**を IPv4 アドレスとして入力します。
4. CIDR ブロック**長**(1 ～ 32)を入力します。
5. エントリの**説明**を入力します。
6. 次の選択肢があります。
   - IP アドレスを静的に割り当てるサブネットを識別するには、[静的(Static)] をオンにします。
   - IP アドレスを動的に割り当てるサブネットを識別するには、[静的(Static)] をオフにします。
7. 次の選択肢があります。
   - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)] を選択します。

- システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)]を選択します。

8. [作成(Create)]をクリックします。
9. ドロップダウンリストから[感度(Sensitivity)]を選択します。
    - [なし(none)]:システムでアラートが生成されません。
    - [低(low)]:システムはアラートを生成するために高い相対しきい値を必要とします。
    - [通常(normal)]:システムはアラートを生成するために中程度のしきい値を必要とします。
    - [高(high)]:システムはアラートを生成するために低いしきい値を必要とします。

ローカルサブネットアラート設定エントリの検索:

手順

1. [設定(Settings)]>[サブネット(Subnets)]>[オンプレミス(On-Premises)]を選択します。
2. **サブネットプレフィックス**を入力し、[適用(Apply)]をクリックして、ローカルサブネットアラート設定エントリを見つけます。

ローカル サブネット アラート設定エントリの変更:

手順

1. [設定(Settings)]>[サブネット(Subnets)]>[オンプレミス(On-Premises)]を選択します。
2. 既存のエントリについて、ドロップダウン リストから[機密性(Sensitivity)]を選択します。
3. 次の選択肢があります。
    - IP アドレスを静的に割り当てるサブネットを識別するには、[静的(Static)]をオンにします。
    - IP アドレスを動的に割り当てるサブネットを識別するには、[静的(Static)]をオフにします。
4. 次の選択肢があります。
    - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)]を選択します。
    - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)]を選択します。

ローカル サブネット設定ファイルのアップロード

複数のローカル サブネット エントリ(1 行に 1 エントリずつ)を含むコンマ区切り値ファイルをアップロードできます。各行は次の形式である必要があります。

```
<cidr-prefix>,<cidr-length>,<description>,[sensitivity],[static-ip-assign],[new-device-alerts]
```

詳細については、次の各項を参照してください。

パラメータ	必須	使用可能な値
<cidr-prefix>	はい	IPv4 アドレス。
<cidr-length>	はい	1 ～ 32 の整数。
<description>	はい	任意の英数字。
[sensitivity]	いいえ	次のいずれかです。 • [なし(none)]:システムでアラートが生成されません。 • [低(low)]:システムはアラートを生成するために高い相対しきい値を必要とします。 • [通常(normal)]:システムはアラートを生成するために中程度のしきい値を必要とします。 • [高(high)]:システムはアラートを生成するために低いしきい値を必要とします。
[static-ip-assign]	いいえ	次のいずれかです。 • [真(true)]:サブネット内のエンティティは静的に割り当てられた IP　アドレスを受け取ります。 • [偽(false)]:サブネット内のエンティティは動的に割り当てられた IP　アドレスを受け取ります。
[new-device-alerts]	いいえ	次のいずれかです。 • [真(true)]:システムはサブネット内で検出された新しいデバイスに関してアラートを生成します。 • [偽(false)]:システムはサブネット内で検出された新しいデバイスに関してアラートを抑制します。 [static-ip-assign] も [真(true)] に設定する場合にのみ、このパラメータを [真(true)] に設定することをお勧めします。動的に割り当てられた IP アドレスは、既存のデバイスに異なる IP アドレスが動的に割り当てられるたびに、システムに過剰な量の新しいデバイス アラートを生成させる可能性があります。

サブネット アラート設定ファイルのアップロード:

手順

1. [設定(Settings)] > [サブネット(Subnets)] > [オンプレミス(On-Premises)] を選択します。
2. [CSV のアップロード(Upload CSV)] をクリックします。
3. [ファイルのアップロード(Upload File)] をクリックして、アップロードするファイルを選択します。

仮想クラウド サブネット設定の変更

提供されているデフォルトのポリシー設定を使用してクラウドベース環境向けに Cisco Secure Cloud Analytics パブリッククラウドのモニタリング（旧 Stealthwatch Cloud パブリック クラウド モニータリング）を設定すると、Secure Cloud Analytics では、設定済みの権限を介してクラウドサブネット情報が取得されます。

エントリを検出した後、仮想クラウドサブネットに関して次のアラート生成設定を指定できます。

パラメータ	説明
Sensitivity	サブネットの感度は、生成可能なアラートに影響します。 • [高（high）]：システムは、[低（low）]、[通常（normal）]、および [高（high）] 優先度のアラートを生成できます。 • [通常（normal）]：システムは、[通常（normal）] および [高（high）] 優先度のアラートを生成できます。 • [低（low）]：システムは、[高（high）] 優先度のアラートを生成できます。 • [なし（none）]：システムはアラートを生成しませんが、このサブネットのトラフィックをモニターします。
Static	エンティティに、このサブネット内の IP アドレスが静的に割り当てられているのか、DHCP などによって動的に割り当てられているのか。このサブネット内のエンティティが、静的に割り当てられた IP アドレスを受信すると、システムは、IP アドレスが常に同じエンティティと相関すると見なします。
New Device Alerts	このサブネットに新しいデバイスが出現した場合に、システムがこのサブネットに関してアラートを生成するかどうか。 このサブネットの静的 IP 割り当ても有効にする場合にのみ、このパラメータを有効にすることをお勧めします。動的に割り当てられた IP アドレスは、既存のデバイスに異なる IP アドレスが動的に割り当てられるたびに、システムに過剰な量の新しいデバイス アラートを生成させる可能性があります。

システムが仮想クラウドサブネットを追加した後、エントリを検索できます。

仮想クラウドサブネットアラート設定エントリの検索：

手順

1. [設定（Settings）] > [サブネット（Subnets）] を選択します。
2. [Amazon Web Services]、[Google Cloud Platform]、または [Microsoft Azure] を選択します。
3. **サブネットプレフィックス**を入力し、[適用（Apply）] をクリックして、仮想クラウドサブネットアラート設定エントリを見つけます。

仮想クラウド サブネット アラート設定エントリの変更：

手順

1. [設定（Settings）] > [サブネット（Subnets）] を選択します。
2. [Amazon Web Services]、[Google Cloud Platform]、または [Microsoft Azure] を選択します。

3. 既存のエントリについて、ドロップダウン リストから [機密性(Sensitivity)] を選択します。
4. 次の選択肢があります。
    - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)] を選択します。
    - システムがこのサブネット上の新しいデバイスを検出したときに新しいデバイスのアラートを受信するには、[新しいデバイスのアラート(New Device Alerts)] を選択します。

VPN サブネット アラート設定の指定

VPN サブネットは、信頼できるサードパーティの関係会社など、管理対象ネットワークの拡張と見なされる外部 IP アドレススペースを識別します。これらのサブネットは、追跡対象でないサードパーティによって制御される外部エンティティに設定できます。

VPN サブネットを追加する際に、次の VPN サブネットアラート設定を構成できます。

パラメータ	説明
プレフィックス	IPv4 形式のサブネットプレフィックス。
長さ	CIDR 表記のサブネット長(1 ～ 32)。詳細については、https://tools.ietf.org/html/rfc4632 を参照してください。
説明	インターフェイスに表示されるローカルサブネットの説明。

VPN サブネットを追加したら、エントリを検索できます。

ローカルサブネットアラート設定とは対照的に、機密性や IP アドレス割り当て、または VPN サブネットに関して新しいエンティティが検出されたときにアラートが生成されるかどうかを変更することはできません。インターフェイスに表示される説明のみを変更できます。

VPN サブネット アラート設定へのエントリの追加:

手順

1. [設定(Settings)] > [サブネット(Subnets)] > [仮想プライベートネットワーク(Virtual Private Networks)] を選択します。
2. [VPNサブネットの作成(Create VPN Subnet)] をクリックします。
3. CIDR ブロックの**プレフィックス**を IPv4 アドレスとして入力します。
4. CIDR ブロック**長**(1 ～ 32)を入力します。
5. エントリの**説明**を入力します。
6. [作成(Create)] をクリックします。

VPN サブネットアラート設定エントリの検索:

手順

1. [設定(Settings)] > [サブネット(Subnets)] > [仮想プライベートネットワーク(Virtual Private Networks)] を選択します。
2. **サブネットプレフィックス**を入力し、[検索(Search)] をクリックして、VPN サブネットアラート設定エントリを見つけます。

VPN サブネット アラート設定エントリの変更:

手順

1. [設定(Settings)] > [サブネット(Subnets)] > [仮想プライベートネットワーク(Virtual Private Networks)] を選択します。
2. [編集(Edit)] アイコンをクリックします。
3. [説明(Description)] を更新します。
4. **[更新(Update)]** をクリックします。

ユーザーおよびサイト管理

[サイトの管理(Site Management)] 設定により、サイト管理者は次を実行できます。

- ユーザーに招待電子メールを送信する
- ユーザー アカウントの権限を更新する
- セッション タイムアウトを設定する

セキュア Sign-On への移行の詳細については、『Cisco Secure Sign-On への移行ガイド』[英語] を参照してください。

ユーザーの管理

ユーザーは、[サイトの管理(Site Management)] ページから招待された後に Secure Cloud Analytics Web UI でアカウントを作成します。

ユーザーがアカウントを作成した後に、サイト管理者ロール権限を持つユーザーは、ユーザー アカウントの次の点を更新できます。

- アクティブか無効か
- 電子メール アドレス
- ロール メンバーシップ

ユーザー アカウントは、次の 3 つのロールのいずれかを持つことができます。

- [読み取り専用ユーザー(Read-only User)]:このユーザーには、[サイトの管理(Site Management)] ページを除くすべての情報の表示権限があります。
- [標準ユーザー(Normal User)]:このユーザーには、[サイトの管理(Site Management)] ページを除くすべての情報の読み取り/書き込み権限があります。ユーザー アカウントは、デフォルトでは、このロール メンバーシップを持ちます。

- [サイト管理者(Site Manager)]:このユーザーには、すべての機能に対する読み取り/書き込み権限があります。

Cisco Secure Sign-On との統合については、『セキュア Sign-On ガイド』[英語] を参照してください。

招待電子メールの送信:

はじめる前に

- サイト管理者権限を持つユーザーとしてログインします。

手順

1. [設定(Settings)] > [アカウント管理(Account Management)] > [ユーザー管理(User Management)] を選択します。
2. [ユーザーの管理(Manage Users)] をクリックします。
3. [招待(Invite)] をクリックします。
4. **電子メール**アドレスを入力します。
5. [招待(Invite)] をクリックします。

ユーザー アカウントの修正:

はじめる前に

- サイト管理者権限を持つユーザーとしてログインします。

手順

1. [設定(Settings)] > [アカウント管理(Account Management)] > [ユーザー管理(User Management)] を選択します。
2. [ユーザー管理(User Management)] をクリックします。
3. [**Cisco Secure Sign-Onユーザー(Cisco Secure Sign-On Users)**] と [招待および[ポータル] ユーザー(Invited and [portal] Users)] を切り替えて、そのタイプのユーザーアカウントを表示します。
4. 次の選択肢があります。
   - ユーザーをサイト管理者ロールに追加するには、[サイト管理者(Site Manager)] を選択します。
   - ユーザーを読み取り専用ユーザー ロールに追加するには、[読み取り専用ユーザー(Read-only User)] を選択します。
   - ユーザーを標準ユーザー ロールに追加するには、[サイト管理者(Site Manager)] と [読み取り専用ユーザー(Read-only User)] をオフにします。
5. **[保存(Save)]**をクリックします。

セッション タイムアウトの設定

セッション タイムアウトにより、ユーザー セッションがログアウトされる前に非アクティブのままでログイン状態を維持できる時間を制御できます。最小 5 分のセッションタイムアウト、または最大 20160 分（14 日間に相当）のセッションタイムアウトを設定できます。

セッション タイムアウトの設定：

はじめる前に

- サイト管理者権限を持つユーザーとしてログインします。

手順

1. [設定（Settings）] > [アカウント管理（Account Management）] > [セッションタイムアウト（Session Timeout）] を選択します。
2. **セッション タイムアウト**を分単位で入力します。
3. **[保存（Save）]**をクリックします。

Web ポータルの使用

ここでは、Secure Cloud Analytics Web ポータルを使用して次のことを行う方法について説明します。

- ダッシュボードからネットワークの全体的な健全性を確認する
- オープン アラートとそれの裏付けとなる観測内容やその他の状況を確認して、ネットワーク動作が悪意のあるものかどうかを判断する
- モデルを確認して、エンティティ、ネットワーク、およびその他の関連動作の履歴パターンを経時的に検出する
- [ヘルプ(Help)] メニューでレポートを確認して、システムによってモニターされているトラフィックの幅と深さを把握する

ダッシュボードの概要

[ダッシュボード(Dashboard)] メニュー オプションは、ネットワークの概要を表示するためのさまざまな方法を提供します。

- ダッシュボードには、アラート、ネットワーク上のエンティティ、およびトラフィック統計情報のサマリーが表示されます。
- AWS 可視化機能により、AWS 関連のスパイダー グラフが、AWS リソース、セキュリティ グループ、および IAM 権限を節点として表示されます。

アラートの概要

[アラート(Alerts)] メニュー オプションにより、システムによって生成されたオープン アラート、クローズ アラート、およびスヌーズ アラートが提供されます。システムは、次のようなネットワークに関するさまざまな情報の分析に基づいて、潜在的な悪意のあるアクティビティを示すそれらのアラートを生成します。

- 用に設定されているさまざまなタイプのクラウド展開 Cisco Secure Cloud Analytics パブリック クラウドのモニタリング
- オンプレミスネットワークのCisco Secure Cloud Analytics プライベートネットワークのモニタリング(設定されている場合)
- モニター対象のエンティティのロールと、それらのエンティティについてログに記録された観測内容
- モニター対象のサブネットの機密性
- アラート タイプの優先順位
- IP スキャナのルール
- 設定されているウォッチリスト、地理位置情報、およびその他の脅威インテリジェンス

生成されたすべてのアラートのサマリーを表示できます。サマリーから、アラートの詳細を表示して、そのアラートに関する詳細なコンテキストを収集し、ワークフローを使用してその進捗状況を追跡することができます。

アラートの現在のステータスに基づいてステータスを変更することで、ワークフロー内でアラートを移動させることができます。

アラートのステータスが次の場合：	次のように変更できます。
オープン（Open）	終了（Closed） スヌーズ（Snoozed）
スヌーズ（Snoozed）	（再）オープン（(Re-)Open）
終了（Closed）	（再）オープン（(Re-)Open）

アラートのワークフロー

アラートのワークフローは、そのステータスに基づいて異なります。システムによってアラートが生成される場合、そのデフォルト ステータスは [オープン（Open）] であり、ユーザーは割り当てられません。アラートのサマリーを表示すると、デフォルトでは、当面注意が必要なすべてのオープン アラートが表示されます。

アラートのサマリーを確認する際は、初期トリアージとして、アラートにステータスを割り当て、タグ付けし、更新することができます。フィルタ機能と検索機能を使用して、特定のアラートを検索したり、さまざまなステータスのアラートを表示したり、さまざまなタグや割り当て対象を関連付けたりすることができます。

> アラートを閉じるとき、アラートのステータスは [スヌーズ（Snoozed）] に設定できます。この場合、そのアラートはスヌーズ期間が経過するまでオープンアラートのリストに表示されません。アラートから [スヌーズ（Snoozed）] ステータスを削除して、再びオープン アラートとして表示されるようにすることもできます。

アラートを確認する際は、それらのアラートをそのユーザー自身またはシステム内の別のユーザーに割り当てることができます。ユーザーは、自分のユーザー名に割り当てられているすべてのアラートを検索できます。

アラートのサマリーから、アラートの詳細ページを表示できます。このページでは、このアラートを生成させた、裏付けとなる観測内容に関する追加のコンテキストと、このアラートに関連するエンティティに関する追加のコンテキストを確認できます。

この情報は、ネットワーク上の問題をさらに調査して悪意のある動作を潜在的に解決するために実際の問題を特定する上で役立ちます。Secure Cloud Analytics Web ポータル UI 内やネットワーク上で調査しているときに、発見した内容を説明するコメントをアラートに残すことができます。これは、将来参照できる調査の記録を作成するために役立ちます。

分析が完了したら、ステータスを [クローズ（Closed）] に更新できます。これにより、デフォルトではオープンアラートとして表示されなくなります。将来、状況が変わった場合は、クローズ アラートのステータスを再度オープンにすることもできます。

アラートの次の手順

ここでは、特定のアラートを調査する方法に関する一般的なガイドラインと推奨事項を示します。Secure Cloud Analytics はアラートをログに記録するときに追加のコンテキストを提供するため、このコンテキストを参照しながら調査を進めることができます。

これらの手順は、総合的または包括的であることを意図したものではありません。これらは単にアラートの調査を開始するための一般的な枠組みを提供するためのものです。

一般に、次の手順でアラートを確認できます。

オープン アラートのトリアージ:

特に複数の調査が必要な場合は、オープン アラートのトリアージを行います。

手順

- [アラート(Alerts)]をクリックして、オープンアラートを表示します。

次の作業

- 次の質問に答えてください。
  - このアラート タイプを優先度の高いものとして設定しましたか。
  - 影響を受けるサブネットに高い機密性を設定しましたか。
  - この異常な動作はネットワーク上の新しいエンティティによるものですか。
  - エンティティの通常のロールは何ですか。また、このアラートの動作はそのロールにどのように適合しますか。
  - これは、このエンティティの通常の動作からの例外的な逸脱ですか。
  - ユーザーが関与している場合、これはユーザーの予想される動作ですか、それとも例外的な動作ですか。
  - 保護されたデータや機密データが侵害を受けるリスクがありますか。
  - この動作の継続を許可すると、ネットワークへの影響はどの程度深刻になりますか。
  - 外部エンティティとの通信がある場合、それらのエンティティは過去にネットワーク上の他のエンティティとの接続を確立しましたか。
- これが優先度の高いアラートである場合は、調査を進める前に、インターネットからエンティティを隔離するか、隔離しないときは接続を閉じることを検討してください。

後で分析するためにアラートをスヌーズ:

他のアラートと比較して優先度が低いときに、アラートをスヌーズします。たとえば、組織が電子メールサーバーを FTP サーバーとして再利用する場合、緊急プロファイルアラートが生成されます。これは想定される動作であるため、このアラートをスヌーズして、後日再検討できます。スヌーズされたアラートは、オープンアラートと一緒に表示されません。これらのスヌーズされたアラートを確認するには、特別にフィルタリングする必要があります。

手順

1. [アラートを閉じる(Close Alert)]をクリックします。
2. [このアラートをスヌーズ(Snooze this alert)]ペインで、ドロップダウンからスヌーズ期間を選択します。
3. **[保存(Save)]**をクリックします。

詳細な調査のためのアラートの更新:

アラートの詳細情報を確認します。

手順

1. [アラート（Alerts）] を選択します。
2. アラートタイプ名をクリックします。

次の作業

- 初期トリアージに基づいて、次の作業を行います。
    - アラートを割り当てて、ユーザーが調査を開始できるようにします。
    - アラートにタグを追加して、将来の識別のためにアラートをより適切に分類したり、アラートの長期的なパターンの国定を試みることができます。
    - アラートの詳細で、**このアラートに関するコメント**を入力し、[コメント（Comment）] をクリックします。

アラートの確認と調査の開始：

割り当てられたアラートを確認する際は、アラートの詳細情報を確認して、Secure Cloud Analytics がアラートを生成した理由を把握してください。

裏付けとなる観測内容を確認し、これらの観測内容がソースエンティティに対して持つ意味を理解します。ソースエンティティの一般的な動作やパターンを理解するための観測内容をすべて表示し、このアクティビティがより長いトレンドの一部になっている可能性があるかどうかを確認します。

手順

- 次の選択肢があります。
    - 観測タイプの横にある矢印アイコンをクリックすると、そのタイプの記録されたすべての観測内容が表示されます。
    - [すべての観測内容（All Observations）] の横にある矢印アイコンをクリックして、このアラートのソースエンティティのすべての記録された観測内容を表示します。

次の作業

- アラートのサマリー（特に説明）を確認して、基本的な状況を把握します。
- 裏付けとなる観測内容を確認します。これらの観測内容がソース エンティティに対して持つ意味を理解します。
- このソース エンティティの一般的な動作やパターンを理解するための観測内容をすべて表示し、このアクティビティがより長いトレンドの一部になっている可能性があるかどうかを確認します。
- 観測内容から、ソース エンティティに関連する追加コンテキスト（それが関与している可能性がある他のアラートや観測内容、デバイス自体に関する情報、それが送信しているセッショントラフィックのタイプなど）を表示します。この動作が悪意のある動作を示しているかどうかを判断してください。ソース エンティティが複数の外部エンティティとの接続を確立している場合は、それらのエンティティが何らかの関連性を持つかどうか（それらのすべてが類似の地理位置情報を持っているか、それらの IP アドレスが同じサブネットからのものであるかなど）を確認します。
- 観測内容から、ソース エンティティが接続を確立したエンティティのコンテキストを確認します。地理位置情報を調査し、いずれかの地理位置情報データまたは Umbrella データによって悪意のあるエンティティが特定されるかどうかを確認します。これらのエンティティによって生成されたトラフィックを表示します。Talos、AbuseIPDB、または Google にこれらのエンティ

ティに関する情報があるかどうかを確認します。複数の日にわたる IP アドレスを見つけて、外部エンティティがネットワーク上のエンティティと確立した他のタイプの接続を確認します。必要に応じて、それらの内部エンティティを見つけ、侵害または意図しない動作の証拠があるかどうかを判断します。

- アラートの詳細で、**このアラートに関するコメント**を入力し、[コメント(Comment)] をクリックします。

裏付けとなる観測結果とコンテキスト詳細の確認:

裏付けとなる観測内容を確認し、これらの観測内容がソースエンティティに対して持つ意味を理解します。ソースエンティティの動作が悪意のある動作を示しているかどうかを判断してください。ソースエンティティが複数の外部エンティティとの接続を確立している場合は、それらのエンティティが何らかの関連性を持つかどうか(それらのすべてが類似の地理位置情報を持っているか、それらの IP アドレスが同じサブネットからのものであるかなど)を確認します。ソースエンティティに関連する追加コンテキスト(それが関与している可能性がある他のアラートや観測内容、デバイス自体に関する情報、それが送信しているセッショントラフィックのタイプなど)を表示します。

手順

- 観測内容では、次のオプションがあります。
    - エンティティに関連するすべてのアラートを表示するには、IP アドレスまたはホスト名のドロップダウンから、[アラート(Alerts)] を選択します。
    - エンティティに関連するすべてのアラートを表示するには、IP アドレスまたはホスト名のドロップダウンから、[観測内容(Observations)] を選択します。
    - デバイスに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[デバイス(Device)] を選択します。
    - このエンティティに関連するセッショントラフィックを表示するには、IP アドレスまたはホスト名のドロップダウンから、[セッショントラフィック(Session Traffic)] を選択します。
    - IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから、[コピー(Copy)] を選択します。

観測内容から、他の外部エンティティに関する情報を調べます。地理位置情報を調査し、いずれかの地理位置情報データまたは Umbrella データによって悪意のあるエンティティが特定されるかどうかを確認します。これらのエンティティによって生成されたトラフィックを表示します。Talos、AbuseIPDB、または Google にこれらのエンティティに関する情報があるかどうかを確認します。複数の日にわたる IP アドレスを見つけて、外部エンティティがネットワーク上のエンティティと確立した他のタイプの接続を確認します。必要に応じて、それらの内部エンティティを見つけ、侵害または意図しない動作の証拠があるかどうかを判断します。ソースエンティティが接続を確立したエンティティのコンテキストを確認します。

手順

- 観測内容では、次のオプションがあります。
    - このエンティティの最近のトラフィック情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[IPトラフィック(IP Traffic)] を選択します。
    - このエンティティの最近のセッショントラフィック情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[セッショントラフィック(Session Traffic)] を選択します。
    - AbuseIPDB のウェブサイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[AbuseIPDB] を選択します。

- Cisco Umbrella のウェブサイト上でこのエンティティに関する情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[Cisco Umbrella] を選択します。
- Google でこの IP アドレスを検索するには、IP アドレスまたはホスト名のドロップダウンから、[Google検索（Google Search）] を選択します。
- Talos のウェブサイト上で情報を表示するには、IP アドレスまたはホスト名のドロップダウンから、[Talos Intelligence] を選択します。
- このエンティティをウォッチリストに追加するには、IP アドレスまたはホスト名のドロップダウンから、[IPをウォッチリストに追加（Add IP to watchlist）] を選択します。
- 前月のこのエンティティのトラフィックを検索するには、IP アドレスまたはホスト名のドロップダウンから、[複数日のIPを検索（Find IP on multiple days）] を選択します。
- IP アドレスまたはホスト名をコピーするには、IP アドレスまたはホスト名のドロップダウンから、[コピー（Copy）] を選択します。

エンティティとユーザーの調査:

ソース エンティティと、このアラートに関与した可能性のあるすべてのユーザーに関する追加のコンテキストを収集します。

- このエンティティのログ ファイルを見つけます。それがネットワーク上の物理エンティティである場合は、デバイスにアクセスしてログ情報を確認し、この動作の原因となっているものに関する情報があるかどうかを確認します。それが仮想エンティティである場合またはクラウドに保存されている場合は、ログにアクセスして、このエンティティに関連するエントリを検索します。不正なログイン、承認されていない設定変更などに関する詳細について、ログを調査します。
- エンティティを調査します。マルウェアまたはエンティティ自体にある脆弱性を特定できるかどうかを判断してください。デバイスの物理的な変更（組織によって承認されていない USB スティックなど）を含め、何らかの悪意のある変更があったかどうかを確認します。
- ネットワーク上のユーザーまたはネットワーク外のユーザーによる関与があったかどうかを確認します。可能であれば、何をしていたのかをユーザーに尋ねてください。ユーザーに尋ねることができない場合は、そのユーザーがアクセス権を持っていたと考えられるかどうかと、この動作を促す状況（解雇された従業員が退社する前に外部サーバーにファイルをアップロードするなど）が発生したかどうかを確認します。
- 調査結果に関するコメントを残します。

調査結果に関するコメントを残します。

手順

- アラートの詳細で、**このアラートに関するコメント**を入力し、[コメント（Comment）] をクリックします。

問題の修正:

悪意のある動作によってアラートが発生した場合は、悪意のある動作を修正します。

- 悪意のあるエンティティまたはユーザーがネットワーク外からのログインを試みた場合は、ファイアウォール ルールを更新して、それらのエンティティまたはユーザーがネットワークにアクセスできないようにします。
- 脆弱性またはエクスプロイトを特定した場合は、影響を受けるエンティティを更新したり、それらにパッチを適用して脆弱性を削除するか、ファイアウォール設定を更新して不正アクセスを

防止します。ネットワーク上の他のエンティティが同様に影響を受ける可能性があるかどうかを判断し、それらのエンティティに同じ更新またはパッチを適用します。現時点で脆弱性またはエクスプロイトを修正する手段がない場合は、該当するベンダーに連絡し、それらを通知してください。

- マルウェアを特定した場合は、エンティティを隔離してマルウェアを削除します。ネットワーク上の他のエンティティが危険にさらされているかどうかを判断し、エンティティまたはセキュリティ ソリューションを更新して、このマルウェアが広がることを防止します。このマルウェアまたはこのマルウェアの原因となったエンティティに関する情報によってセキュリティ情報を更新してください。必要に応じてベンダーに通知してください。
- 悪意のある動作によってデータが漏洩した場合は、許可されていないソースに送信されたデータの性質を確認します。不正なデータ漏洩に関する組織の規定に従ってください。

修正に関するコメントを残します。

手順

- アラートの詳細で、**このアラートに関するコメント**を入力し、[コメント(Comment)] をクリックします。

Secure Cloud Analytics 設定の微調整:

アラートと修正に基づいて、今後のこの動作の識別に役立つように Secure Cloud Analytics の設定を更新します。

- 外部エンティティが悪意のある動作を引き起こした場合は、それらをウォッチリストに追加します。詳細については、「**ウォッチリスト設定**」を参照してください。
- ある国の複数のエンティティによって悪意のある動作が引き起こされた場合は、その国を国のウォッチリストに追加します。詳細については、「**国のウォッチリストの設定**」を参照してください。
- 必要に応じて、追加のサブネットをモニターするように センサー 設定を更新します。詳細については、「**Sensorのモニターリング設定**」を参照してください。
- 特定のサブネットがターゲットになっている場合は、サブネットの機密性を更新します。詳細については、「**サブネット設定**」を参照してください。
- 特定のアラートが懸念される場合は、アラート タイプの優先順位設定を更新します。詳細については、「**アラート優先順位の更新**」を参照してください。

アラートの更新とアラート ステータスのクローズへの変更:

追加タグと最後のコメントでアラートを更新し、そのステータスをクローズまたはスヌーズにします。

手順

1. アラートの詳細で、ドロップダウンから 1 つ以上の [タグ(Tags)] を選択します。
2. **このアラートに関するコメント**を入力し、[コメント(Comment)] をクリックします。
3. [アラートを閉じる(Close Alert)] をクリックします。
4. アラートが有用だった場合は [はい(Yes)] を、アラートが有用でなかった場合は [いいえ(No)] を選択します。これはアラートが悪意のある動作に起因するかどうかではなく、単にアラートが組織にとって有用であったかどうかを意味します。
5. アラートの優先順位を調整する場合は、次のオプションがあります。

- 優先度を現在のレベルに維持する場合は、[アラートの動作を調整しない（Do not adjust alert Behavior）] を選択します。
- アラート優先度を [低（Low）] に変更するには、[このアラートタイプの優先度を低に設定（Set this alert type's priority to low）] を選択します。アラートの優先度がすでに [低（Low）] の場合、これは効果がありません。
- このアラートタイプを [有効（Enabled）] から [無効（Disabled）] に変更するには、[このアラートタイプを無効にする（Disable this alert type）] を選択します。

6. アラートをスヌーズする場合は、[選択した時間枠でこのアラートをスヌーズするために、上記の基準に一致する期間のアラートを表示しない（Don't show the alert matching the above criteria for a period of to snooze this alert for the selected timeframe）] から値を選択します。

   アラートを閉じる場合は、このドロップダウンから [スヌーズしない（Don't snooze）] を選択します。
7. [作成（Create）] をクリックします。

閉じたアラートを再度開く:

クローズしたアラートに関連する追加情報を検出した場合、またはそのアラートに関連するコメントを追加する場合は、そのアラートを再度開いてステータスを [オープン（Open）] に変更できます。その後、必要に応じてアラートを変更し、追加調査が完了したら再度閉じます。

手順

- クローズされたアラートから、[アラートを再オープン（Reopen Alert）] をクリックします。

スヌーズしたアラートのスヌーズ解除:

スヌーズしたアラートを確認する準備ができたら、スヌーズを解除できます。これにより、ステータスが [オープン（Open）] に設定され、他のオープンアラートとともにアラートが表示されます。

手順

- スヌーズしたアラートから、[アラートのスヌーズ解除（Unsnooze Alert）] をクリックします。

アラートサマリー

アラートサマリーには、システムが報告するアラートの概要が表示されます。特定のテキストを検索したり、ステータス、タグ、または担当者でフィルタリングしたりできます。また、アラート生成に関連する設定を行うこともできます。

アラートサマリーから、1 つ以上のアラートのステータス、タグ、および担当者を更新できます。

アラートサマリーを含むカンマ区切り値ファイルをダウンロードできます。

アラートサマリーフィールド

フィールド	説明
アラートタイプ（Alert type）	生成されたアラートのタイプ。
ソースエンティティ（Source entity）	このアラートを生成したソースエンティティ。

アラートID（Alert ID）	アラート ID 番号。
最終更新時刻（Last update time）	このアラートが最後に更新された時刻。
コメント数（Number of comments）	このアラートに関連付けられているコメントの数。
担当者（Assignee）	このアラートに割り当てられたユーザー。

アラート関連の設定

手順

1. [モニター（Monitor）] > [アラート（Alerts）] を選択します。
2. [関連する設定リンク（Related Config Links）] をクリックします。次の選択肢があります。
   - [アラートの優先順位（Alert Priorities）] を選択すると、アラートの優先順位を設定できます。詳細については、「**アラート優先順位設定**」を参照してください。
   - [国のウォッチリスト（Country Watchlist）] を選択すると、地理位置情報に基づいて、トラフィックが発生した場合にアラートを生成する必要がある国を設定できます。詳細については、「**国のウォッチリストの設定**」を参照してください。
   - [内部C（Internal C）] を選択します。
   - [IPスキャナルール（IP Scanner Rules）] を選択すると、ネットワーク上で許可する IP スキャナを設定できます。詳細については、「**IP スキャナルールの設定**」を参照してください。
   - [IPおよびドメインウォッチリスト（IPs and Domain Watchlist）] を選択すると、ウォッチリストを設定できます。詳細については、「**ウォッチリスト設定**」を参照してください。
   - [サブネット感度（Subnet Sensitivity）] を選択すると、アラート生成対象のサブネットの感度を設定できます。詳細については、「**サブネット設定**」を参照してください。

アラートサマリーの使用

ステータスに基づくアラートの表示

手順

1. [モニター（Monitor）] > [アラート（Alerts）] を選択します。
2. 使用可能なタブから、[オープン（Open）] を選択してすべてのオープンアラートを表示するか、[クローズド（Closed）] を選択してすべてのクローズドアラートを表示するか、[未公開（Unpublished ）] を選択してすべての未公開アラートを表示するか、[スヌーズ（Snoozed）] を選択してすべてのスヌーズアラートを表示します。

アラートの詳細を表示：

手順

- アラートサマリーで、アラートタイプ名をクリックします。

表示されたアラートのソート：

手順

- アラートサマリーで、列ヘッダーをクリックして値を昇順または降順でソートします。

表示されたアラートのフィルタリング:

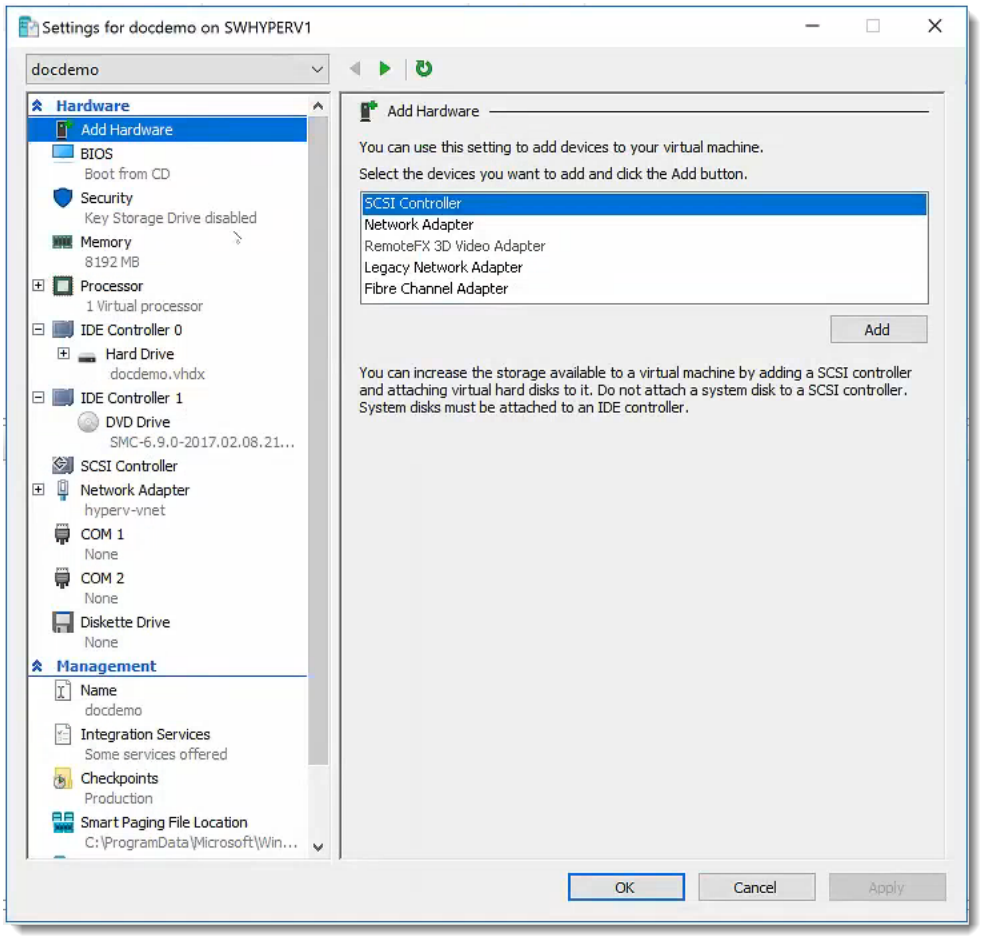
手順

1. アラートサマリーで、[フィルタ(Filters)]🔍 をクリックしてペインを展開します。
2. **検索**条件を入力します。
3. ドロップダウンから [アラートタイプ(Alert Type)] を選択して、アラートタイプを検索します。
4. [担当者(Assignee)] を選択して、担当者に基づいてアラートを検索します。
5. [タグ(Tag)] を選択して、タグに基づいてアラートを検索します。
6. [開始日(Start Date)]、[開始時刻(Start Time)]、[終了日(End Date)]、[終了時刻(End Time)] を選択して、指定した時間枠内に生成されたアラートを検索します。
7. [適用(Apply)] をクリックしてアラートをフィルタリングします。

アラートタグの管理:

手順

1. アラートの概要で、[タグの割り当て(Assign Tag)] ドロップダウンの横にある



(**設定**)アイコンをクリックします。

2. [新しいタグの追加（Add new Tag）] フィールドにタグを入力し、[+] をクリックしてタグを追加します。
3. 既存のタグの横にある  （**削除**）アイコンをクリックして削除します。

情報を含むカンマ区切りファイルのダウンロード:

手順

- ダウンロードする表の [CSV] をクリックします。

アラートサマリーでのアクションの実行

[アラートサマリー（Alerts summary）] から、アラートのステータス、タグ、または担当者を更新できます。[アラートサマリー（Alert summary）] から複数のアラートを同時に一括更新することもできます。

ステータスに基づくアラートの表示

手順

1. [モニター（Monitor）] > [アラート（Alerts）] を選択します。
2. [オープン（Open）] を選択してすべてのオープンアラートを表示するか、[クローズド（Closed）] を選択してすべてのクローズドアラートを表示するか、[スヌーズ（Snoozed）] を選択して**すべての**スヌーズアラートを表示します。

アラートサマリーからのアラートを更新

手順

1. [モニター（Monitor）] > [アラート（Alerts）] を選択します。
2. 1 つ以上のアラートのチェックボックスをオンにするか、ヘッダーのチェックボックスをオンにして、ページに表示されるすべてのアラートを選択します。
3. 次の選択肢があります。
    - [ステータスの変更（Change Status）] ロップダウンからステータスを選択し、選択したアラートに割り当てます。
    - [タグの割り当て（Assign Tags）] ロップダウンからタグを選択して、選択したアラートにタグを割り当てます。
    - [ユーザーの割り当て（Assign User）] ロップダウンからユーザーを選択して、選択したアラートにユーザーを割り当てます。

アラートの詳細

アラートの詳細ページには、サマリー情報や関連する観測内容を含め、アラートに関する詳細な情報が表示されます。

アラート詳細ページでは、アラートを調査するときにワークフローを使用してステータスを更新することもできます。コメントをアラートの記録として残すこともできます。

関連するアラートの観察

アラートの詳細ページには、このアラートが生成される原因となった観測内容のリストが表示されます。このアラートの原因となったネットワークの動作の詳細については、これらの情報を参照してください。

アラートの詳細ページから、影響を受けるエンティティに対して生成されたすべての観測内容を確認することもできます。

アラートの詳細ページの操作

アラートの詳細表示:

手順

1. [モニター(Monitor)] > [アラート(Alerts)] を選択します。
2. アラートタイプ名をクリックします。

   [ステータス(Status)]、[ID]、[更新済み(Updated)]、[作成済み(Created)]、[担当者(Assignee)]、[タグ(Tags)]、[インシデントの投稿(Post an Incident)]、および [クローズドアラート(Closed Alerts)] フィールドがこの特定のアラートに適用されることに注意してください。[説明(Description)]、[次の手順(Next Steps)]、[MITRE戦術(MITRE Tactics)]、[MITRE手法(MITRE Techniques)]、および [アラートタイプの優先度(Alert Type Priority)] が、この特定のアラートに加えて、アラートタイプにも適用されます。

アラートの詳細ページからのユーザーの割り当て:

手順

- [担当者(Assignee)] ドロップダウンからユーザーを選択します。

このアラートタイプの優先度設定:

手順

- [アラートタイプの優先度(Alert Type Priority)] ドロップダウンから、優先度レベルを選択します。この選択は、この特定のアラートだけでなく、アラートタイプにも適用されます。

アラートの詳細ページからのタグの追加:

手順

- ドロップダウンから 1 つ以上の**タグ**を選択します。

新しい Cisco SecureX インシデントの作成

アラートの詳細から SecureX インシデントを作成し、SecureX でそのインシデントで表示できます。

> この機能を有効にするには、SecureX リボンにログインする必要があります。

手順

- [Threat Responseへの投稿(Post to Threat Response)] をクリックします。

MITER ATT&CK の戦術と手法のコンテキストを表示

手順

- 詳細を確認するには、カーソルを [MITRE戦術(MITRE Tactic)] または [MITRE手法(MITRE Technique)] に合わせます。これらは、この特定のアラートだけでなく、アラートタイプにも適用されることに注意してください。

アラートの詳細ページから追加の観測内容を表示:

手順

1. このアラートのソースエンティティのすべてのログに記録された観測内容を表示するには、[(エンティティ)のすべての観測内容(All Observations for (entity))] をクリックします。

情報を含むカンマ区切りファイルのダウンロード:

手順

- ダウンロードする表の [CSV] をクリックします。

ソースエンティティの追加情報を表示:

手順
(missing or bad snippet)

外部エンティティの追加情報を表示:

手順
(missing or bad snippet)

アラートをスヌーズ:

手順

1. [アラートを閉じる(Close Alert)] をクリックします。
2. アラートが有用だった場合は [はい(Yes)] を、アラートが有用でなかった場合は [いいえ(No)] を選択します。これはアラートが悪意のある動作に起因するかどうかではなく、単にアラートが組織にとって有用であったかどうかを意味します。
3. アラートの優先順位を調整する場合は、次のオプションがあります。
    - 優先度を現在のレベルに維持する場合は、[アラートの動作を調整しない(Do not adjust alert Behavior)] を選択します。
    - アラート優先度を [低(Low)] に変更するには、[このアラートタイプの優先度を低に設定(Set this alert type's priority to low)] を選択します。アラートの優先度がすでに [低(Low)] の場合、これは効果がありません。
    - このアラートタイプを [有効(Enabled)] から [無効(Disabled)] に変更するには、[このアラートタイプを無効にする(Disable this alert type)] を選択します。
4. [選択した時間枠でこのアラートをスヌーズするために、上記の基準に一致する期間のアラートを表示しない(Don't show the alert matching the above criteria for a period of to snooze this alert for the selected timeframe)] から時間値を選択します。
5. [作成(Create)] をクリックします。

スヌーズしたアラートのスヌーズ解除:

手順

- スヌーズしたアラートから、[アラートのスヌーズ解除(Unsnooze Alert)] をクリックします。

アラートを閉じる:

手順

1. [アラートを閉じる(Close Alert)]をクリックします。
2. アラートが有用だった場合は[はい(Yes)]を、アラートが有用でなかった場合は[いいえ(No)]を選択します。これはアラートが悪意のある動作に起因するかどうかではなく、単にアラートが組織にとって有用であったかどうかを意味します。
3. アラートの優先順位を調整する場合は、次のオプションがあります。
    - 優先度を現在のレベルに維持する場合は、[アラートの動作を調整しない(Do not adjust alert Behavior)] を選択します。
    - アラート優先度を[低(Low)]に変更するには、[このアラートタイプの優先度を低に設定(Set this alert type's priority to low)] を選択します。アラートの優先度がすでに[低(Low)]の場合、これは効果がありません。
    - このアラートタイプを[有効(Enabled)]から[無効(Disabled)]に変更するには、[このアラートタイプを無効にする(Disable this alert type)] を選択します。
4. [選択した時間枠でこのアラートをスヌーズするために、上記の基準に一致する期間のアラートを表示しない(Don't show the alert matching the above criteria for a period of to snooze this alert for the selected timeframe)] から[スヌーズしない(Don't snooze)]を選択します。
5. [作成(Create)]をクリックします。

閉じたアラートを再度開く:

手順

- クローズされたアラートから、[アラートを再オープン(Reopen Alert)]をクリックします。

このアラートに関するコメントを入力:

手順

- このアラートに関するコメントを入力し、[コメント(Comment)]をクリックします。

エンティティの詳細

エンティティの詳細ページには、次のようなエンティティに関する情報が表示されます。

- [履歴(History)]:[履歴(History)]折れ線グラフには、エンティティとの間で送受信されるトラフィックの量、およびエンティティが関与した接続の数が 1 日間隔で表示されます。
- [概要(Summary)]:[概要(Summary)]タブには、システムに保存されているエンティティのモデルの概要が表示されます。
- [トラフィック(Traffic)]:[トラフィック(Line)]折れ線グラフには、エンティティとの間で送受信されたトラフィックの量、およびエンティティが関与した接続の数が 10 分間隔で表示されます。[トラフィック(Traffic)]タブには、エンティティが関与していた接続に関する情報も含まれます。
- [プロファイリング(Profiling)]:[プロファイリング(Profiling)]タブには、このエンティティに関連付けられているロールと、各ロールに関連付けられているトラフィックに関する情報が表示されます。
- [DNS]:[DNS]タブには、エンティティが送信した DNS 要求に関する情報と、DNS 要求に基づく IP 解決が表示されます。

[概要（Summary）]、[トラフィック（Traffic）]、[プロファイリング（Profiling）]、および [DNS] タブには、当日の情報が表示されます。別の日に変更して、その日にシステムによって収集された情報を表示できます。

エンティティ詳細フィールド

エンティティ概要フィールド

フィールド	説明
通常アクティブ（Normally Active）	このエンティティが通常アクティブである期間。
IP アドレス（IP Addresses）	エンティティの IP アドレス。
接続（Connections）	このエンティティが関与していた接続の数。
内部接続（Internal Connections）	このエンティティが関与していた内部エンティティとの接続数。
外部接続（External Connections）	このエンティティが関与していた外部エンティティとの接続数。
上位内部接続 （Top Internal Connections）	送信されたトラフィックの合計数に基づく、エンティティが接続を確立した上位 5 つの内部エンティティ。
上位外部接続 （Top External Connections）	送信されたトラフィックの合計数に基づく、エンティティが接続を確立した上位 5 つの外部エンティティ。
トラフィック：受信バイト （Traffic: Bytes In）	エンティティが受信したトラフィックの量。
トラフィック：送信バイト （Traffic: Bytes Out）	エンティティが送信したトラフィックの量。
トラフィック：合計バイト （Traffic: Bytes Total）	エンティティが送信したトラフィックの合計。
内部トラフィック：受信バイト （Traffic Internal: Bytes In）	エンティティが内部エンティティから受信したトラフィックの量。
内部トラフィック：送信バイト （Traffic Internal: Bytes Out）	エンティティが内部エンティティに送信したトラフィックの量。
外部トラフィック：受信バイト （Traffic External: Bytes In）	エンティティが外部エンティティから受信したトラフィックの量。
外部トラフィック：送信バイト （Traffic External: Bytes Out）	エンティティが外部エンティティに送信したトラフィックの量。

DNS 名（DNS name）	エンティティに関連付けられた DNS ドメイン名。
オープンアラート（Open Alerts）	このエンティティに関連付けられているオープンアラート。
クローズドアラート（Closed Alerts）	このエンティティに関連付けられているクローズ済みアラート。
オブザベーション（Observations）	このエンティティに関連付けられている観測内容。
ロール（Roles）	このエンティティに関連付けられているロール。
プロファイル（Profiles）	リストされたプロファイルに対応してエンティティが動作した時間の割合。

エンティティトラフィック フィールド

フィールド	説明
接続済み IP（Connected IP）	このエンティティが接続を確立した IP アドレス。
ホスト名 / PDNS レコード（Hostname/PDNS Record）	この IP アドレスのホスト名（使用可能な場合）。
受信バイト数（Bytes In）	接続されたエンティティからエンティティが受信したバイト数。
送信バイト数（Bytes Out）	エンティティによって接続されたエンティティに送信されたバイト数。
合計バイト数（Bytes Total）	この接続のエンティティによって送信された合計バイト数。
最初の接続時間（Time of First Connection）	接続された IP との、この日の最初の接続時刻。
最終接続時刻（Time of Last Connection）	接続された IP との、この日の最後の接続時刻。

エンティティ プロファイル フィールド

フィールド	説明
名前	エンティティに関連付けられているプロファイルの名前。
参加者（Attendance）	このプロファイルと一致する、このエンティティがアクティブであった 1 日の時間の割合。

受信バイト数（Bytes In）	このプロファイルと一致する、エンティティが受信したバイト数。
送信バイト数（Bytes Out）	このプロファイルと一致する、エンティティによって送信されたバイト数。
合計バイト数（Bytes Total）	このプロファイルと一致する、エンティティによって送信された合計バイト数。
接続（Connections）	このプロファイルと一致する、このエンティティが関与していた接続の数。

エンティティ DNS フィールド

フィールド	説明
時刻（Time）	DNS 要求の時刻。
要求されたドメイン（Requested Domain）	DNS 要求内のドメイン。
結果の IP（Resulting IP）	DNS 要求に基づいて解決された IP アドレス。

エンティティの詳細の表示

エンティティの詳細の表示：

手順

1. 送信元または内部エンティティの IP アドレスの横にある下矢印アイコン（⌄）をクリックし、[デバイス（Device）] を選択します。
2. [履歴（History）] 線グラフにマウスポインタを合わせると、その日のエンティティのトラフィックの詳細が表示されます。
3. [前日（Previous Day）] をクリックして前日の統計情報を表示するか、[翌日（Next Day）] をクリックして翌日の統計情報を表示します。注：統計情報のデフォルトは現在の日付です。現在の日の統計情報が表示されている場合は、[翌日（Next Day）] を選択できません。

[概要（Summary）] タブの使用：

手順

1. **[サマリー]** をクリックします。
2. [参加者IPアドレス（Attendance IP Address）] をクリックして、エンティティのトラフィックに関する詳細情報を表示します。詳細については、「**エンティティのトラフィックの詳細**」を参照してください。
3. [オープンアラート（Open Alerts）] の横にある矢印アイコン（➔）をクリックして、このエンティティが関与するオープンアラートごとにフィルタリングされた [アラート（Alerts）] ページに移動します。詳細については、「**アラートサマリー**」を参照してください。

4. [クローズドアラート(Open Alerts)] の横にある矢印アイコン( )をクリックして、このエンティティが関与するクローズドアラートごとにフィルタリングされた [アラート(Alerts)] ページに移動します。詳細については、「**アラートサマリー**」を参照してください。
5. [観測内容(Observations)] の横にある矢印アイコン( )をクリックして、このエンティティが関与する観測内容ごとにフィルタリングされた [観測内容(Observations)] ページに移動します。詳細については、「**観測内容の概要**」を参照してください。
6. このエンティティのロールを提案する場合は、[デバイスのロールの提案(Suggest Role for Device)] をクリックし、[ロールの提案とオプションの詳細を指定(Suggest a role and input optional details)] フィールドに推奨事項を入力して、[提案(Suggest)] をクリックします。

[トラフィック(Traffic)] タブの使用:

手順

1. [トラフィック(Traffic)] をクリックします。
2. [履歴(History)] 線グラフにマウスポインタを合わせると、エンティティのトラフィックの詳細が 10 分間隔で表示されます。
3. 接続の詳細をフィルタリングするには、次のオプションがあります。
   - このエンティティが接続を確立したすべてのエンティティに関する情報を表示するには、[すべて(All)] をクリックします。
   - このエンティティが接続を確立した内部エンティティに関する情報を表示するには、[内部(Internal)] をクリックします。
   - このエンティティが接続を確立した外部エンティティに関する情報を表示するには、[外部(External)] をクリックします。
   - エンティティがこれまで接続を確立していない新しいエンティティに関する情報を表示するには、[新規(New)] をクリックします。

[プロファイリング(Profiling)] タブの使用:

手順

1. [プロファイリング(Profiling)] をクリックします。
2. 円グラフにマウスポインタを合わせると、そのプロファイルと一致する、エンティティの確立された合計接続の割合が表示されます。

[DNS] タブの使用:

手順

- [DNS] をクリックします。

情報を含むカンマ区切りファイルのダウンロード:

手順

- ダウンロードする表の [CSV] をクリックします。

観測内容の概要

システムがトラフィックを検査すると、ネットワーク上のエンティティについての観察内容（事実）がログに記録されます。これらの観測内容は、[観測内容（Observations）] メニュー オプションから確認できます。選択したハイライト観測内容や、タイプ別またはソース別の観測内容を表示してフィルタリングできます。

ドリルダウンして、そのタイプのすべての観測内容を表示できます。ドリルダウンすると、このページに新しいタブが開き、それらの観測内容が表示されます。別の観察内容タイプを選択してドリルダウンすると、その新しいタブがそれらの観察内容で更新されます。

最近のハイライト観測

観測データはエンティティごとに記録されるため、合理的なレビュー量を超える観測データがネットワークで生成される可能性があります。システムは、ネットワークについて記録された最も注目すべき観測データのサブセットを提示します。これらを確認してフィルタリングすることで、アラートが生成される可能性のある動作のタイプをより深く理解することができます。

> アラートは、観測データを組み合わせて生成されます。単独の観測データが必ずしも悪意のある動作を示すものではありません。最近のハイライト観察結果は、それ自体が、ネットワーク上に悪意のある動作があることを必ずしも意味するものではありません。アラートを確認して、悪意のある可能性のある動作の全体像を把握します。

最近の観測ハイライトの表示

最近の観測ハイライトの表示：

手順

1. [モニター（Monitor）] > [観測内容（Observations）] > [ハイライト（Highlights）] を選択します。

最近の観察ハイライトのフィルタリング：

手順

1. [モニター（Monitor）] > [観測内容（Observations）] > [ハイライト（Highlights）] を選択します。
2. 特定の観測タイプについて、検索フィールドにフィルタ値を入力し、Enter キーを押します。

観測タイプに関する詳細の表示：

手順

1. [モニター（Monitor）] > [観測内容（Observations）] > [ハイライト（Highlights）] を選択します。
2. ポインタを情報アイコン（ ）の上に置きます。

任意タイプのすべての観測データの表示：

手順

1. [モニター（Monitor）] > [観測内容（Observations）] を選択します。
2. [最近のハイライト（Recent Highlights）] タブを選択します。
3. 表示する観測タイプの横にある矢印アイコン（ ）をクリックします。
   新しいタブが開き、このエンティティの観測データが表示されます。

ソースエンティティに関する詳細情報の表示

手順
(missing or bad snippet)

外部エンティティに関する詳細情報の表示:

手順
(missing or bad snippet)

観測タイプ

観測タイプのリストには、ログに記録できるすべての観測タイプが、説明、およびログに記録された観測数とともに表示されます。

ドリルダウンして、そのタイプのすべての観測内容を表示できます。ドリルダウンすると、このページに新しいタブが開き、それらの観測内容が表示されます。別の観察内容タイプを選択してドリルダウンすると、その新しいタブがそれらの観察内容で更新されます。

タイプ別の観測データの表示

タイプ別の観測データの表示:

手順

1. [モニター(Monitor)] > [観測内容(Observations)] > [タイプ(Types)] を選択します。

任意タイプのすべての観測データの表示:

手順

1. [モニター(Monitor)] > [観測内容(Observations)] > [タイプ(Types)] **を選択します。**。
2. 表示する観測タイプの横にある矢印アイコン( )をクリックします。
   新しいタブが開き、このエンティティの観測データが表示されます。

デバイス別の観測

デバイス別の観測のリストには、エンティティ、そのエンティティに関連付けられた観測の数、およびそのエンティティの観測が最後に記録された時刻が表示されます。これを使用して、観測データが最も多いエンティティを確認できます。

オープンアラートに関連付けられているエンティティの横にはオープンアラートアイコン( )が表示され、オープンアラートに現在関連付けられていないエンティティの横には情報アイコン( )が表示されます。

> 観測データが多いほどアラート数が多いとは限りません。たとえば、観測データの多いエンティティでは、さまざまなトラフィックが大量に通過している可能性がありますが、ダイナミック エンティティ モデリングは、この動作が正常であり、このエンティティの予測範囲内と判断した可能性があります。同様に、観測データが少なければ、アラートが生成されないとは限りません。たとえば、エンティティで検出された唯一のアクティビティが、不適切なクレデンシャルを使用したサーバーへの継続的なログインである場合、観測データが比較的少なくても、複数回のログイン試行の失敗を通知するアラートが生成される可能性があります。

ソースごとの観測データの表示

ソースごとの観測データの表示::

手順

1. [モニター(Monitor)] > [観測内容(Observations)] > [デバイス別(By Device)] を選択します。

任意タイプのすべての観測データの表示:

手順

1. [モニター(Monitor)] > [観測内容(Observations)] > [デバイス別(By Device)] を選択します。
2. エンティティの横にあるコンテキストメニューをクリックし、[観測内容(Observations)] を選択して、そのエンティティに関連付けられた観測データを表示します。

   新しいタブが開き、このエンティティの観測データが表示されます。

選択された観測内容

[選択された観測内容(Selected Observation)] ウィンドウから、特定のタイプの観測内容がすべて表示されます。これにより、ネットワークトラフィックに基づいて Secure Cloud Analytics がログに記録している観測データを確認できます。

選択された観測内容の表示

手順

1. [モニター(Monito)] > [観測内容(Observations)] > [選択された観測内容(Selected Observation)] を選択します。
2. [フィルタ(Filters)] をクリックして [フィルタ(Filters)] ペインを展開します。
3. [検索(Search)] フィールドにフィルタ値を入力します。
4. ドロップダウンから [観測タイプ(Observation Type)] を選択します。
5. フィルタを適用して結果を表示します。

調査の概要

[調査(Investigate)] メニューオプションにより、モニター対象エンティティ、トラフィック、およびユーザーに関連するさまざまなグラフと表が表示されます。

セッション トラフィック モデル

[セッショントラフィックモデル(Session Traffic Model)] には、システムがモニターした特定のセッショントラフィックに関する詳細情報が含まれます。デフォルトでは、過去 24 時間の情報が表示されます。表示される情報の期間や表示されるセッションの基準を変更できます。

トラフィック

トラフィックの表には、フィルタ条件に一致するセッションに関する情報が表示されます。

集約トラフィック

[集約トラフィック(Aggregate Traffic)] 表には、フィルタ条件に一致するセッションに関する情報が、関連セッションを 1 行の項目に集約して表示されます。

トラフィックチャート

[トラフィックチャート(Traffic Chart)] には、過去 48 時間の一致するセッションで送信されたデータを表す棒グラフが表示されます。

拒否

[拒否(Rejects)] 表には、基準に一致したものの適合性を理由に拒否されたセッションに関する情報が表示されます。

接続グラフ

[接続グラフ(Connection Graph)] には、スパイダー グラフが、エンティティを節点とし、エンティティ間に確立された接続を辺として表示されます。

外部サービス モデル

[トラフィックモデル(Traffic Model)] には、選択された外部サービス(ファイル ストレージ アプリケーション、リモート アクセス アプリケーション、ソーシャル メディア サイトなど)に関するセッション情報が含まれます。

デバイス モデル

[デバイスモデル(Device model)] には、Secure Cloud Analytics によってモニターされるエンティティに関する履歴情報が含まれます。[エンドポイントモデル(Endpoints model)] には次のものが表示されます。

デバイスグラフ

[デバイスグラフ(Device Graph)] には、過去 30 日間のモニター対象のエンティティの数が表示されます。特定の日に関する詳細情報を表示できます。

デバイスの概要

[デバイス概要(Device Overview)] には、特定の日に Secure Cloud Analytics によってモニターされた各エンティティに関する詳細情報(そのエンティティの可能なロールなど)が表示されます。

デバイスの役割

[デバイスロール(Device Roles)] には、その日の特定のロールに適合するエンティティについて、その数のモザイクプロットが表示されます。

IP またはドメイン検索

エンティティ検索では、エンティティが送信するトラフィックに関する詳細情報を表示できます。

暗号化されたトラフィックレポート

暗号化トラフィックレポートには、暗号化トラフィック分析に基づき、送信元および宛先エンティティ、暗号化方式の詳細など、システムがモニターした暗号化トラフィックに関する詳細情報が表示されます。デフォルトでは、過去 24 時間の情報が表示されます。表示される情報の期間を変更したり、表示される暗号化接続をフィルタリングしたりできます。暗号化された接続に関する詳細を含むカンマ区切り値(CSV)ファイルをダウンロードすることもできます。

このモデルを実装するには、拡張 NetFlow データがクラウドに送られるように センサー を設定する必要があります。詳細については、『Secure Cloud Analytics Configuration Guide for Enhanced NetFlow』を参照してください。

ユーザー アクティビティ モデル

[ユーザーアクティビティモデル(User Activity model)]には、システムを使用したユーザーに関する情報(ユーザーに関連付けられている観測内容など)が含まれます。

ロール モデル

[ロールモデル(Roles model)]には、ロールに一致するエンティティに関する情報が含まれます。[ロールモデル(Roles model)]には次のものが表示されます。

アクティブ ロール

[アクティブロール(Active Roles)]リストには、選択した期間に 1 つ以上の一致するエンティティを持つ各ロールが表示されます。

選択されたロール

[選択されたロール(Selected Roles)]リストには、一致するエンティティを表示するために選択したロールが表示されます。

一致するソース

[一致するソース(Matching Sources)]リストには、選択されたロールのリストと一致するすべてのエンティティが表示されます。

イベントビューア

イベントビューアでは、プライベートネットワークのモニタリング と パブリッククラウドのモニタリングの両方のトラフィックを含む、Secure Cloud Analytics 向け Cisco Cloud に送信されたセッショントラフィックを表示できます。

パブリッククラウドのモニタリング を AWS 用に設定した場合は、AWS で拒否されたトラフィックを別の [イベントビューア(Event Viewer)] タブで表示することもできます。

パブリッククラウドのモニタリング を AWS または Azure 用に設定する場合は、イベントビューアのクラウドポスチャレポートを使用して、セキュリティの推奨事項に対して設定を評価できます。Secure Cloud Analytics は、1 日 1 回展開を評価するため、セキュリティ設定を改善し、環境の保護を強化できます。

> AWS のクラウドポスチャには追加の設定が必要です。詳細については、「**AWS クラウドポスチャ権限の設定**」を参照してください。

セッショントラフィックおよび拒否されたトラフィックのフィールド

[セッショントラフィック(Session Traffic)] または [拒否されたトラフィック(Rejected Traffic)] を表示すると、イベントビューアで次のフィールドを使用できます。

フィールド	説明
時刻(Time)	イベントに関連付けられたタイムスタンプ。
IP	このトラフィックに関連付けられた IP アドレス。
Connected_IP	このトラフィックに関連付けられている他の IP アドレス。

フィールド	説明
Port	このトラフィックに関連付けられたポート。
Connected_port	このトラフィックに関連付けられている他のポート。
Protocol	このトラフィックに関連付けられたインターネットプロトコル。
Bytes_to	IP から接続先 IP に送信されたバイト数。
Bytes_from	接続先 IP から IP に送信されたバイト数。拒否されたトラフィックでは使用できません。
Packets_to	IP から接続先 IP に送信されたパケット数。
Packets_from	接続先 IP から IP に送信されたパケット数。拒否されたトラフィックでは使用できません。

クラウドポスチャ

AWS または Azure 用に パブリッククラウドのモニタリング を設定する場合は、イベントビューアのクラウドポスチャレポートを使用して、セキュリティの推奨事項に対して設定を評価し、推奨事項の判定を行うことができます。AWS または Azure 内でネイティブ コンプライアンス チェックを有効にした場合、クラウドポスチャには、クラウドプロバイダからの追加の推奨事項と推奨事項の判定が表示されることがあります。Secure Cloud Analytics は、1 日 1 回展開を評価するため、セキュリティ設定を改善し、環境の保護を強化できます。

AWS クラウドポスチャを評価するには、IAM 権限を更新する必要があります。詳細については、「**AWS クラウドポスチャ権限の設定**」を参照してください。

Azure クラウドポスチャの評価では、権限を更新する必要はありません。

クラウドポスチャフィールド

クラウドポスチャレポートでは、次のフィールドを使用できます。

フィールド	データタイプ	説明
Account_ID	文字列	この推奨事項がチェックされた AWS アカウント ID または Azure サブスクリプション ID。
Compliant	文字列	推奨の判定。リソースがこの推奨に準拠しているか（合格）、準拠していないか、または Secure Cloud Analytics がアクセス拒否応答を受信しているか（失敗）を示します。
Description	文字列	推奨事項の概要説明。

フィールド	データタイプ	説明
Details	ネストされたフィールド（Nested fields）	推奨の判定に関する情報の要約。
Framework	文字列	関連するコンプライアンスのフレームワーク名。
Last_Scanned	文字列（日付）	次のいずれかです。 • Secure Cloud Analytics が推奨の判定を実施した時刻。 • AWS または Azure のネイティブコンプライアンスの場合、Secure Cloud Analytics が推奨の判定を取得した時刻。 タイムスタンプの形式は「%Y-%m-%d %H:%M:%S」です。
レベル	文字列	CIS フレームワークの推奨事項向けに Center for Internet Security から提供されるコンテキスト。レベル 1 は、マシンを使用可能な状態に保ち、ビジネス機能を妨げないようにしながら、組織の攻撃対象領域を減少されることを目的としています。レベル 2 は「多層防御」が求められ、セキュリティを最優先する環境を対象としています。
プライオリティ	文字列	推奨事項に割り当てられた優先度レベル。優先度レベルの詳細については、セキュリティ推奨フレームワークのマニュアルを参照してください。
プロバイダ	文字列	クラウドプロバイダ名（AWS や Azure など）。
Recommendation_ID	文字列	推奨の ID。詳細については、推奨 ID をクリックしてください。
地域	文字列	この推奨の判定が適用される AWS または Azure リソースのリージョン。
リソース	ネストされたフィールド（Nested fields）	この推奨の判定で適用されるリソース。**リソース名**と**タイプ**が常に表示されます。追加情報が表示される場合もあります。
Resource.name	文字列	推奨の判定で評価されるリソース名。

フィールド	データタイプ	説明
Resource.type	文字列	推奨の判定で評価されるリソースタイプ。
重大度	文字列	AWS または Azure ネイティブ コンプライアンス チェックによって定義された推奨の重大度。

AWS クラウドポスチャ権限の設定

AWS クラウドポスチャを評価するには、AWS の IAM ポリシーに追加のアクセス許可を付与する必要があります。Secure Cloud Analytics の [AWSの概要(AWS About)] ページに、「`"Sid": "CloudCompliance"`」で始まる JSON オブジェクトの必要な権限が一覧表示されます。

Secure Cloud Analytics と AWS を初めて統合するお客様で、これらの追加の権限を付与したくない場合は、このオブジェクトを削除できますが、クラウドポスチャレポートは使用できなくなります。

すでに AWS と統合された Secure Cloud Analytics があり、これらの追加の権限を付与しない場合は、AWS の IAM ポリシーを変更しないでください。クラウドポスチャレポートを使用できなくなります。既存の IAM ポリシーを更新するには、次の手順を実行します。

AWS のクラウドポスチャ権限の確認:

はじめる前に

- Secure Cloud Analytics Web ポータルに管理者アカウントでログインします。

手順

1. [設定(Settings)] > [統合(Integrations)] > [AWS] > [情報(About)] を選択します。
2. [ポリシードキュメント(Policy Document)] ペインで、`"Sid": "CloudCompliance"` で始まる JSON オブジェクトを参照すると、Secure Cloud Analytics で AWS Cloud ポスチャを評価するために必要な追加の権限を確認できます。次の選択肢があります。
    - これらの追加の権限を付与しない場合は、ここで終了します。Secure Cloud Analytics で AWS クラウドポスチャを評価することはできなくなります。
    - これらの追加の権限を付与して AWS クラウドポスチャを評価する場合は、ポリシードキュメントの JSON 設定をコピーし、プレーンテキストエディタに貼り付けます。次の手順に進みます。

Secure Cloud Analytics AWS での IAM ポリシーの更新:

はじめる前に

- 管理者として AWS コンソールにログインします。

手順

1. IAM コンソールから [ポリシー(Policies)] を選択し、Secure Cloud Analytics IAM ポリシーを選択します。
2. [権限(Permissions)] をクリックし、[ポリシーの編集(Edit policy)] を選択します。

3. [JSON] を選択し、更新されたポリシーをプレーンテキストエディタからコピーして貼り付け、既存のポリシーを上書きします。
4. [ポリシーの確認（Review policy）] をクリックします。
5. [変更を保存（Save changes）] をクリックします。

イベントビューアへのアクセス

イベントビューアへのアクセス

はじめる前に

- Secure Cloud Analytics ポータルにログインします。

手順

1. [調査（Investigate）] > [イベントビューア（Event Viewer）]を選択します。
2. 次の選択肢があります。
    - ネットワーク展開で送信されるセッショントラフィックを表示するには、[イベントビューア（Event Viewer）] を選択します。
    - パブリッククラウドのモニタリング を AWS で設定した場合、AWS で拒否されたトラフィックを表示するには、[拒否されたトラフィック（Rejected Traffic）] を選択します。

列の表示と非表示

イベントビューアに表示される列を変更できます。

列の表示および非表示

手順

1. イベントビューアには、次のオプションがあります。
    - 左下の [設定（Settings）] アイコンをクリックし、[列の管理（Manage Columns）] を選択します。
    - 右上の設定アイコンをクリックします。
2. 表示する列のチェックボックスをオンにし、非表示にする列のチェックボックスをオフにします。
3. イベントビューアの更新が完了したら、[x] をクリックします。

追加のフィールド情報の表示

特定のイベントには、追加のフィールドが含まれる場合があります。これらのフィールドには、複数のサブフィールドと関連する値を含めることもできます。これらを表示するには、品目を展開します。

追加のフィールド情報を表示する

手順

- 追加フィールドを含むイベントの場合は、▼（下に移動）アイコン をクリックしてイベントを展開し、追加のフィールド情報を表示します。

イベントビューアのフィルタリング

イベントビューアのデフォルトでは、過去 1 時間のすべてのイベントが表示されます。イベントビューアは、一度に複数の結果をロードします。一度に表示できるよりも多くの結果が使用可能な場合は、イベントビューアを下にスクロールすると、追加の結果がロードされます。

イベントビューアのデフォルトはインラインフィルタリング方式です。これにより、値を追加したり、列フィルタから複数の演算子のいずれかを選択したりすることができます（等号、大なり、小なり、範囲など）。インラインフィルタリングを使用して複数の値をフィルタリングできます。一致するイベントは、追加するすべての評価と一致する必要があります。

インラインフィルタリングからクエリフィルタリングに切り替えることができます。これにより、Lucene クエリ構文に基づいてより高度なクエリを作成できます。時間選択オプションは、クエリフィルタリングでも引き続き使用できます。複数のブール演算子（AND、OR、NOT）を使用できるため、インラインフィルタリングよりも詳細な検索を作成できます。

イベントビューアのクエリ構文

詳細については、Lucene クエリ構文のマニュアルを参照してください。

クエリ構文オプション

次のクエリ構文オプションを使用できます。

構文オプション	構文	説明
基本的なフィールド/値の評価	`field1: "value1"`	field1 が value1 に等しい結果を返します
単一文字のワイルドカード	`?`	この？は任意の文字と一致します ワイルドカード検索は、列のインラインフィルタが英数字の文字列値を受け入れる場合にのみサポートされます。
複数文字のワイルドカード	`*`	この＊は任意の数の任意の文字と一致します ワイルドカード検索は、列のインラインフィルタが英数字の文字列値を受け入れる場合にのみサポートされます。
包含的範囲検索	`["value1" TO "value2"]`	value1、value2、またはその間の任意の値を返します
排他的範囲検索	`{"value1" TO "value2"}`	value1 と value2 の間の値を返しますが、value1 または value2 の値は返しません
ブール演算子 AND	`AND`	AND 前後の両方の評価が true である結果を返します

構文オプション	構文	説明
ブール演算子 OR	または	OR 前後の評価のいずれかが true である結果を返します
ブール演算子 NOT	`NOT`	NOT の前の評価が true で、NOT 後の評価が false である結果を返します
グループ化	`()`	括弧内を単独で評価します
フィールドのグループ化	`field1: ()`	単一フィールドの括弧内の複数の値と演算子を評価します

評価の順序

クエリはシステムにより次の優先順位で評価されます。

1. グループ化。()(括弧)、[](包含的範囲検索)、{}(排他的範囲検索)を含む
2. :(等しい)
3. NOT ブール演算子
4. AND ブール演算子
5. OR ブール演算子

クエリ構文例

次の表に、一般的なクエリ構文の例を示します。

説明	構文例	返される結果
1 つのフィールド、1 つの値	`field1: "value1"`	field1 が value1 に等しいすべてのイベント
1 つのフィールド、1 つの値、1 文字のワイルドカード	`field1: "value?"`	field1 が "value?" に等しいすべてのイベント (? は任意の文字)
1 つのフィールド、1 つの値、複数文字のワイルドカード	`field1: "value*"`	field1 が "value*" に等しいすべてのイベント (* は任意の数の文字)

説明	構文例	返される結果
1 つのフィールド、複数の値（フィールドのグループ化）	`field1:("value*1" AND "value*2")`	field1 に value*1 と value*2 が含まれるすべてのイベント 1 つのフィールドで複数の値を検索する場合は、一致する結果が得られる可能性を高めるために、各値にワイルドカードを使用することを推奨します。
1 つのフィールド、どちらかの値	`field1:("value1" OR "value2")`	field1 が value1 または value2 と等しいすべてのイベント
2 つのフィールド、AND 演算子	`field1: "value1" AND field2: "value2"`	field1 が value1 に等しく、かつ field2 が value2 に等しいすべてのイベント 複数のフィールド値の評価の間に演算子を明示的に定義しない場合、システムは評価間に AND 演算子を暗黙的に解釈します。
2 つのフィールド、OR 演算子	`field1: "value1" OR field2: "value2"`	field1 が value1 に等しい、または field2 が value2 に等しいすべてのイベント
2 つのフィールド、NOT 演算子	`field1: "value1" AND NOT field2: "value2"`	field1 が value1 に等しく、field2 が value2 に等しくないすべてのイベント
2 つのフィールド、OR NOT 演算子	`field1: "value1" OR NOT field2: "value2"`	field1 が value1 に等しい、または field2 が value2 に等しくないすべてのイベント
1 つのフィールド包含的範囲検索	`field1:["value1" TO "value2"]`	field1 が value1、value2、またはその範囲内の任意の値に等しいすべてのイベント
1 つのフィールド、排他的範囲検索	`field1:{"value1" TO "value2"}`	field1 が value1 と value2 の間の任意の値に等しいが、value1 または value2 ではないすべてのイベント

説明	構文例	返される結果
1 つのフィールド、包含的範囲検索と排他的範囲検索	`field1:["value1" TO "value2"}`	field1 が value1、または value1 と value2 の間の任意の値に等しいが、value2 ではないすべてのイベント
複数のフィールド、混合演算子	`field1: "value1" OR field2: "value2" AND field: "value3"`	AND ブール演算子は OR ブール演算子よりも優先されるため、以下に一致するすべてのイベント: • field2 が value2 に等しく、かつ field3 が value 3 に等しい、または • field1 が value1 に等しい
複数のフィールド、混合演算子および括弧	`(field1: "value1" OR field2: "value2") AND field3: "value3"`	グループ化は他の演算子よりも優先され、最初に評価されるため、以下に一致するすべてのイベント: • field1 が value1 に等しいか、または field2 が value2 に等しい、かつ • field3 が value3 に等しい

次の表に、ユーザーが展開のために実行できるクエリの例を示します。

説明	構文例	返される結果
内部 Web サーバーとの正常な非 HTTPS 接続を確立した内部デバイス	`Connected_ip: "192.168.105.28" AND IP: "192.168.0.0/16" AND NOT Port: "443" AND NOT Connected_port: "443" AND Packets_from: { "10" TO * } AND Packets_to: { "10" TO * }`	以下のすべてのイベント: • `IP` が `192.168.0.0/16`（内部エンティティ）の内部 CIDR 範囲に等しい • `Connected_ip` が `192.168.105.28`（内部 Web サーバー）に等しい • `Port` が `443` に等しくない（非 HTTPS トラフィック）、 • `Connected_port` が `443` に等しくない（非 HTTPS トラフィック）、

説明	構文例	返される結果
		• Packets_from が 11 以上（接続成功、トラフィック通過）、かつ • Packets_to が 11 以上（接続成功、トラフィック通過）
リモート デスクトップ アプリケーションに関連する接続	Port: ("23" OR "3389" OR ["5800" TO "5803"] OR ["5900" TO "5903"] OR ["6000" TO "6063"]) AND NOT Connected_port: ["0" TO "1023"] AND Packets_from: ["10" TO *] AND Packets_to: ["10" TO *]	以下のすべてのイベント: • Port が 23、3389、5800 ～ 5803、5900 ～ 5903、または 6000 ～ 6063 に等しい（共通のリモート デスクトップ アプリケーション ポート）、 • Connected_port が 0 ～ 1023 に等しくない（エフェメラル ポートを使用する接続）、 • Packets_from が 10以上（接続成功、トラフィック通過）、かつ • Packets_to が 10 以上（接続成功、トラフィック通過）

イベントビューアのネストされたフィールドの検索

イベントにサブフィールドを持つフィールドが含まれている場合は、ドット表記を使用してサブフィールドを指定することで、クエリフィルタでこれらのフィールド値を検索できます。

たとえば、品目エントリには、[クレデンシャル（Credentials）] と [問題（Issues）] の 2 つのサブフィールドを備えた [詳細（Details）] フィールドが含まれる場合があります。[クレデンシャル（Credentials）] フィールドで username1 を検索する場合は、次のドット表記構文を使用します。

```
Details.credentials: "username1"
```

異なる推奨の特定のフィールドには、推奨タイプごとに異なるサブフィールドが含まれることがあります。

イベントビューアのインラインフィルタリング

時間選択の変更:

手順

1. イベントビューアの時間フィールドで、カレンダーアイコンをクリックします。

   タイムスタンプのデフォルトはローカルタイムゾーン(表示中)、またはローカルタイムゾーンが UTC の場合は UTC に設定されています。
2. 事前設定されたタイムフレームのいずれかを選択して、そのタイムフレームを自動的に設定します。
3. カスタムタイムフレームを選択するには、[カスタム(Custom)]を選択します。
4. [開始日時(From Date/Time)]と[終了日時(To Date/Time)]を選択します。
5. タイムフレームを選択したら、時間フィールドをクリックして結果を更新します。

列のフィルタリング:

手順

1. イベントビューアで、インラインフィルタリング方式が選択されていることを確認します。
2. 次の選択肢があります。
   - 値をクリックし、コピーアイコンをクリックして、その値を列フィルタフィールドに貼り付けます。
   - 列フィルタフィールドに値を入力します。
3. 列フィルタアイコンをクリックし、演算子を選択します。
4. 値を入力して演算子を選択したら、列フィルタフィールドをクリックして結果をフィルタリングします。
5. 結果からフィルタを削除するには、フィルタの横にある[x]をクリックします。

クエリフィルタリングへの切り替え:

手順

1. インラインフィルタリングを選択した状態で、イベントビューアからクエリフィルタリングを選択します。
2. 現在適用されているインラインフィルタを保持する場合は、[すべての適用済みフィルタをクエリ構文に変換する(Convert all applied filters to query syntax)]をオンにします。
3. **[確認(Confirm)]**をクリックします。

イベントビューアのクエリフィルタリング

時間選択の変更:

手順

1. イベントビューアの時間フィールドで、カレンダーアイコンをクリックします。
2. [時刻を表示(Show time)]を[ローカル(Local)]または[UTC]のいずれかに選択します。
3. 事前設定されたタイムフレームのいずれかを選択して、そのタイムフレームを自動的に設定します。

4. カスタムタイムフレームを選択するには、[カスタム（Custom）] を選択します。
5. [開始日時（From Date/Time）] と [終了日時（To Date/Time）] を選択します。
6. タイムフレームを選択したら、時間フィールドをクリックして結果を更新します。

イベントのクエリ：

手順

1. イベントビューアで、クエリフィルタリングが選択されていることを確認します。
2. [クエリ（Query）] フィールドにクエリを入力します。詳細については、「**イベントビューアのクエリ構文**」および Lucene 構文のマニュアルを参照してください。
3. [適用（Apply）] をクリックして結果をフィルタリングします。

インラインフィルタリングへの切り替え：

手順

1. インラインフィルタリングを選択した状態で、イベントビューアからインラインフィルタリングを選択します。
2. 現在の時間範囲をコピーする場合は、[時間範囲（Time Range）] のコピーアイコンをクリックします。
3. 現在適用されているクエリをコピーする場合は、[クエリ（Query）] のコピーアイコンをクリックします。
4. **[確認（Confirm）]** をクリックします。

IP アドレスの追加コンテキストの表示

イベントビューアから、IP アドレスに関する追加情報を表示できます。

ソースエンティティの追加情報を表示：

手順
(missing or bad snippet)

外部エンティティの追加情報を表示：

手順
(missing or bad snippet)

イベント情報のダウンロード

イベントをカンマ区切り値（CSV）ファイルとしてダウンロードすることができます。次の点に注意してください。

- Secure Cloud Analytics イベントを .csv ファイルに追加し、.gz 形式で圧縮します。
- 1 つの .csv ファイルに、最大約 50 GB の圧縮情報を収容できます。
- ダウンロード可能なファイルの生成は並行して実行できます。
- 作成された .csv.gz ファイルは Secure Cloud Analytics に保存され、そこから直接ダウンロードされます。これらのファイルは Secure Cloud Analytics の課金サブスクリプションには影響しません。

- 作成されたダウンロード可能な .csv.gz ファイルは 7 日間保存され、その後削除されます。
- 進行中のジョブは手動でキャンセルできます。

CSV.GZ ファイルの生成およびダウンロード:

手順

1. イベントビューアで、[ダウンロード(Download)] アイコンをクリックし、[エクスポートするファイルを生成(Generate a file for export)] をクリックします。
2. [ファイル名(File Name)] を入力します。
3. [送信(Submit)] をクリックします。ファイルの生成には数分かかる場合があります。

   処理中のファイル生成をキャンセルするには、[ダウンロード(Download)] アイコンをクリックし、[ファイルのエクスポートをキャンセル(Cancel file export)] をクリックします。

4. ファイルをダウンロードする準備ができたら、[ダウンロード(Download)] アイコンをクリックし、生成されたファイル名をクリックします。

[レポート(Report)] メニュー

[レポート(Report)] メニューを使用すると、ネットワークに関する一目でわかる情報を提供するレポートを生成できます。これにはモニター対象のエンティティやスループットに関連するレポートが含まれ、展開でモニターされるトラフィック量を把握するために役立ちます。

AWS の可視化

AWS の可視化には、AWS の導入に関する次の情報が表示されます。

- [CloudTrail]:[CloudTrail] タブには、AWS CloudTrail ログが表示されます。
- [ネットワークグラフ(Network Graph)]:[ネットワークグラフ(Network Graph)] タブには、AWS 導入を表すスパイダグラフが表示されます。
- [セキュリティグループ(Security Groups)]:[セキュリティグループ(Security Groups)] タブには、AWS 導入のセキュリティグループを表すスパイダグラフが表示されます。
- [IAM]:[IAM] タブには、IAM のロールと権限を表すスパイダグラフが表示されます。
- [インスペクタ(Inspector)]:[インスペクタ(Inspector)] タブには、EC2 インスタンスのインスペクタ評価が表示されます。

計測レポート

プライベートネットワークのモニタリングを使用してオンプレミス展開をモニターしている場合は、[計測レポート(Metering Report)] ページに、Secure Cloud Analytics によってモニターされる 1 秒あたりの平均フローが含まれます。グラフには過去の暦月の FPS モニターリングが表示されます。プライベートネットワークのモニタリング請求は 1 ヵ月あたりの平均 FPS に基づいているため、これにより、使用状況を確認できます。

月次フロー レポート

パブリッククラウドのモニタリングを使用してクラウドベース展開をモニターしている場合は、[月次フローレポート(Monthly Flows Report)] ページに、Secure Cloud Analytics によってモニターされる 1 日あたりの有効フローの数が含まれます。デフォルトでは、過去 30 日間の EF モニターリングが表示されます。フィルタを変更して、異なる時間範囲を表示することができます。パブリッククラウドの

モニタリング請求は 1 ヵ月あたりの有効メガフロー（EMF）（つまり、約 100 万の有効フロー）に基づいているため、これにより、使用状況を確認できます。

サブネット レポート

[サブネットレポート（Subnet Report）] ページには、トラフィックを送信したものとしてシステムが検出したサブネットが含まれます。レポートには、次の概要が含まれます。

- すべてのアクティブなサブネット
- これらのサブネットが生成するトラフィック
- サブネット内のアクティブな IP アドレスの数
- サブネット間で送信されるトラフィックを表示するテーブル

デフォルトでは、レポートには過去 24 時間分のトラフィックが表示されます。システムに表示されるサブネットのタイムスタンプと、それらのサブネットに関連する情報を変更できます。レポートからの情報を含むカンマ区切りファイルをダウンロードすることもできます。

トラフィック モデル

[トラフィックモデル（Traffic Model）] には、システムがモニターしたトラフィックに関する詳細情報が含まれます。デフォルトでは、過去 24 時間の情報が表示されます。表示される情報の期間を変更できます。

トラフィックの概要

[トラフィックの概要（Traffic Overview）] には、送信されたトラフィックの全般概要と、そのトラフィックの送信元に関する情報が表示されます。

最上位 IP

[最上位IP（Top IPs）] 表には、最も多くのトラフィックを送信した内部および外部 IP アドレスに関する情報が表示されます。

最上位ポート

[最上位ポート（Top Ports）] 表には、エンティティがトラフィックを送信するにあたって最も多くのトラフィックが経由した内部および外部ポートに関する情報が表示されます。

可視性アセスメント

[可視性アセスメント（Visibility Assessment）] ページには、過去 30 日間のネットワークアクティビティに関する情報を示すレポートが表示されます。このレポートには、次の情報が含まれています。

- 内部ネットワークのトラフィックの概要
- 外部ホストとの過剰な SMB 接続を確立した最新のエンティティのリスト
- 不正な DNS サーバーとして機能しているエンティティのリスト
- DNS サーバーとの接続数が過剰なエンティティのリスト
- リモート ネットワーク アクセスを提供するエンティティのリスト（VNC や RDP など）
- 過剰な Telnet 接続があるエンティティのリスト
- シスコによって定義された、リスクの高い国への複数の接続を持つエンティティのリスト

デフォルトでは、レポートには、ネットワーク上の過去 30 日間のトラフィックに基づく情報が表示されます。Web ポータル UI でレポートを表示するか、情報を含む PDF をダウンロードできます。

その他のリソースおよびサポート

さらにサポートが必要な場合は、support@obsrvbl.com まで電子メールでお問い合わせください。

Secure Cloud Analytics の詳細については、次を参照してください。

- 概要については、https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html を参照してください。
- 60 日間の無料トライアルに登録するには、https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html にアクセスしてください。
- ドキュメントリソースについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html を参照してください。
- Secure Cloud Analytics 無料トライアルのガイドなど、インストールおよび設定ガイドについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html を参照してください。

変更履歴

リビジョン	改訂日	説明
1.0	2018 年 8 月 7 日	最初のバージョン。
1.1	2018 年 11 月 26 日	センサー フローコレクションを更新。
1.2	2019 年 1 月 22 日	センサー フローコレクションの設定を更新。
1.3	2019 年 4 月 18 日	廃止された用語を更新。
1.4	2019 年 6 月 6 日	AWS および Azure の PCM を更新。
1.5	2019 年 7 月 9 日	更新された UI の用語を更新。
1.6	2019 年 10 月 8 日	拡張 NetFlow の統合用に更新。
1.7	2019 年 10 月 22 日	PCM for AWS の設定手順を更新。
1.8	2020 年 1 月 6 日	Cisco Defense Orchestrator の統合に関する追加情報を更新。
1.9	2020 年 6 月 23 日	外部接続のウォッチリスト情報を修正。
1.10	2020 年 10 月 16 日	UI の更新に基づく更新。
1.11	2020 年 10 月 22 日	Meraki 設定の更新。
1.12	2020 年 12 月 11 日	イベントビューア、アラート、および観測内容の更新。
1.13	2021 年 1 月 26 日	クラウドポスチャ管理の更新。
1.14	2021 年 2 月 3 日	PCM 用の Azure ストレージアカウントの作成方法を更新。
1.15	2021 年 2 月 18 日	AWS の PCM 統合について更新。
2.0	2021 年 11 月 3 日	製品のブランド名を更新。

著作権情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリックドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

このドキュメントのすべての印刷版と複製ソフトは管理対象外と見なされます。最新版については、現在のオンライン バージョンを参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。住所と電話番号は、シスコの Web サイト（https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html）に記載されています。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL：https://www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。（1721R）