Cisco Secure Cloud Analytics ポータルを使用する

この章では、Cisco Secure Cloud Analytics ポータルについて説明します。

Cisco Secure Cloud Analytics ポータルのプロビジョニング

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

Logging Analytics and Detection ライセンスまたは **Total Network Analytics and Monitoring** ライセンスを購入した場合、Secure Event Connector（SEC）を展開して設定した後、Secure Cloud Analytics ポータルを Security Cloud Control ポータルに関連付けて、Secure Cloud Analytics アラートを表示する必要があります。ライセンスを購入すると、既存の Secure Cloud Analytics ポータルがある場合は、Secure Cloud Analytics ポータル名を指定して、すぐに Security Cloud Control ポータルに関連付けることができます。

それ以外の場合は、Security Cloud Control UI から新しい Secure Cloud Analytics ポータルをリクエストできます。Secure Cloud Analytics アラートに初めてアクセスすると、システムに Secure Cloud Analytics ポータルを要求するページが表示されます。このポータルを要求するユーザーには、ポータルの管理者権限が付与されます。

手順

ステップ 1 左側のペインで、**[分析（Analytics）] > [Cisco Secure Cloud Analytics]** をクリックし、新しいウィンドウで Cisco Secure Cloud Analytics の UI を開きます。

ステップ 2 [無料トライアルを開始（Start Free Trial）] をクリックして、Secure Cloud Analytics ポータルをプロビジョニングし、Security Cloud Control ポータルに関連付けます。

（注）
ポータルを要求した後、プロビジョニングに数時間かかる場合があります。

次の手順に進む前に、ポータルがプロビジョニングされていることを確認してください。

1. 左側のペインで、**[分析（Analytics）] > [Cisco Secure Cloud Analytics]** をクリックし、新しいウィンドウで Cisco Secure Cloud Analytics の UI を開きます。
2. 次の選択肢があります。
   - Secure Cloud Analytics ポータルを要求したものの、まだポータルのプロビジョニング中であることがシステムに表示されている場合は、しばらく待ってから、後でアラートへのアクセスを試行してください。
   - Secure Cloud Analytics ポータルがプロビジョニング済みの場合は、[ユーザー名（Username）] と [パスワード（Password）] を入力し、[サインイン（Sign in）] をクリックします。

（注） 管理者ユーザーは、Secure Cloud Analytis ポータル内でアカウントを作成するように他のユーザーを招待できます。詳細については、Security Cloud Control で Cisco Secure Cloud Analytics アラートを表示する （5 ページ）を参照してください。

次のタスク

- **Logging Analytics and Detection** ライセンスを購入した場合、設定は完了しています。Secure Cloud Analytics ポータル UI から Security Cloud Control 統合のステータスやセンサーの正常性のステータスを表示する場合は、「Cisco Secure Cloud Analytics でのセンサーの正常性と Security Cloud Control 統合ステータスの確認 （3 ページ）」で詳細を参照してください。Secure Cloud Analytics ポータルでアラートを操作する場合は、「Security Cloud Control で Cisco Secure Cloud Analytics アラートを表示する （5 ページ）」および「Firepower Threat Defense イベントに基づくアラートの使用」を参照してください。
- **Total Network Analytics and Monitoring** ライセンスを購入した場合は、1 つ以上の Secure Cloud Analytics センサーを内部ネットワークに展開して、ネットワークフローデータをクラウドに渡します。クラウドベースのネットワークフローデータを監視する場合は、フ

ローデータを Secure Cloud Analytics に渡すようにクラウドベースの展開を設定します。詳細については、総合的なネットワーク分析およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開 （4 ページ）を参照してください。

Cisco Secure Cloud Analytics でのセンサーの正常性と Security Cloud Control 統合ステータスの確認

Sensor Status

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

Cisco Secure Cloud Analytics Web UI では、[センサーリスト（Sensor List）] ページで Security Cloud Control 統合ステータスと設定済みセンサーを確認できます。Security Cloud Control 統合は、読み取り専用の接続イベントセンサーです。Stelathwatch Cloud のメインメニューには、センサーの全体的な正常性が示されます。

- 緑色の雲のアイコン（）：すべてのセンサーと Security Cloud Control（設定されている場合）との接続が確立されています
- 黄色の雲のアイコン（）：一部のセンサー、または Security Cloud Control（設定されている場合）との接続が確立されており、1 つ以上のセンサーが正しく設定されていません
- 赤色の雲のアイコン（）：設定されているすべてのセンサーと Security Cloud Control（設定されている場合）との接続が失われています

センサーまたは Security Cloud Control 統合ごとに、緑色のアイコンは接続が確立されていることを示し、赤色のアイコンは接続が失われていることを示します。

手順

ステップ 1 1. Cisco Secure Cloud Analytics ポータル UI で、[設定（Settings）]（）> [センサー（Sensors）] を選択します。

ステップ 2 [センサーリスト（Sensor List）] を選択します。

総合的なネットワーク分析およびレポーティングのための Cisco Secure Cloud Analytics センサーの展開

Secure Cloud Analytics センサーの概要と展開

必要なライセンス：Total Network Analytics and Monitoring

Total Network Analytics and Monitoring ライセンスを取得している場合は、Secure Cloud Analytics ポータルをプロビジョニングした後に、次のことができます。

- オンプレミスネットワーク内に Secure Cloud Analytics センサーを展開し、ネットワークフローデータを分析のためにクラウドに渡すように設定します。
- フローデータを分析のために Secure Cloud Analytics に渡すようにクラウドベースの展開を設定します。

ネットワーク境界のファイアウォールが内部ネットワークと外部ネットワークの間のトラフィックに関する情報を収集する一方で、Secure Cloud Analytics センサーは内部ネットワーク内のトラフィックに関する情報を収集します。

（注） FDM による管理Cisco Secure Firewall Threat Defense デバイスは、NetFlow データを渡すように設定できます。センサーを展開するときは、イベント情報を Security Cloud Control に渡すように設定されている FDM による管理Cisco Secure Firewall Threat Defense デバイスからの NetFlow データを渡すようにセンサーを設定しないでください。

センサーの展開手順と推奨事項については、Secure Cloud Analytics センサーのインストールガイドを参照してください。

クラウドベース展開の設定手順と推奨事項については、Secure Cloud Analytics パブリック クラウド モニタリング ガイドを参照してください。

（注） Secure Cloud Analytics ポータルの UI で手順を確認して、センサーとクラウドベース展開を設定することもできます。

Secure Cloud Analytics の詳細については、Secure Cloud Analytics 無料試用ガイドを参照してください。

次の手順

- Security Cloud Control で Cisco Secure Cloud Analytics アラートを表示する （5 ページ）に進みます。

Security Cloud Control で Cisco Secure Cloud Analytics アラートを表示する

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

[イベントロギング（Event Logging）] ページでファイアウォールイベントを確認できますが、Security Cloud Control ポータル UI から Cisco Secure Cloud Analytics アラートを確認することはできません。[セキュリティ分析（Security Analytics）] メニューオプションを使用して Security Cloud Control から Secure Cloud Analytics ポータルを相互起動し、ファイアウォール イベントデータ（および [Total Network Analytics and Monitoring] を有効にしている場合はネットワークフローデータ）から生成されたアラートを表示できます。[セキュリティ分析（Security Analytics）] メニューオプションには、1 つ以上のワークフローステータスが開いている場合、開いているワークフローステータスの Secure Cloud Analytics アラートの数を示すバッジが表示されます。

Security Analytics and Logging ライセンスを使用して Secure Cloud Analytics アラートを生成し、新しい Secure Cloud Analytics ポータルをプロビジョニングした場合は、Security Cloud Control にログインしてから、Cisco Security Cloud Sign On を使用して Secure Cloud Analytics を相互起動します。URL を使用して Secure Cloud Analytics ポータルに直接アクセスすることもできます。

詳細については、「Cisco Security Cloud Sign On」を参照してください。

Cisco Secure Cloud Analytics ポータルへに参加するようユーザーを招待する

Cisco Secure Cloud Analytics ポータルのプロビジョニングをリクエストする最初のユーザーには、Cisco Secure Cloud Analytics ポータルの管理者権限があります。そのユーザーは、他のユーザーを電子メールで招待してポータルに参加させることができます。招待されたユーザーは、Cisco Security Cloud Sign On のログイン情報を持っていない場合、招待メールのリンクを使用して作成できます。ユーザーは、Security Cloud Control から Cisco Secure Cloud Analytics へのクロス起動中に、Cisco Security Cloud Sign On のログイン情報を使用してログインできます。

電子メールで他のユーザーを Cisco Secure Cloud Analytics ポータルに招待するには、次の手順を実行します。

手順

ステップ 1 Cisco Secure Cloud Analytics ポータルに管理者としてログインします。

ステップ 2 **[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。

ステップ 3 [電子メール（Email）] アドレスを入力します。
ステップ 4 [招待（Invite）] をクリックします。

Security Cloud Control から Cisco Secure Cloud Analytics を相互起動する

Security Cloud Control からのセキュリティアラートを表示するには以下を実行します。

手順

ステップ 1 Security Cloud Control ポータルにログインします。
ステップ 2 左側のペインで、**[分析（Analytics）]** > **[Cisco Secure Cloud Analytics]** を選択します。
ステップ 3 Secure Cloud Analytics インターフェイスで [監視（Monitor）] > [Alerts（アラート）] を選択します。 >

Cisco Secure Cloud Analytics とダイナミック エンティティ モデリング

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

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。ファイアウォールイベントとネットワークフローデータを含め、ネットワークトラフィックに関する情報を送信元から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。Cisco 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。Cisco 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。

ダイナミック エンティティ モデリング

ダイナミック エンティティ モデリングは、ファイアウォールイベントとネットワークフローデータの動作分析を実行することにより、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いて、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 モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。**Logging Analytics and Detection** ライセンスと統合された Secure Cloud Analytics は、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、ファイアウォールイベントやその他のトラフィック情報から引き出すことができます。**Total Network Analytics and Monitoring** ライセンスを購入すると、Secure Cloud Analytics は、エンティティトラフィックのモデル化にNetFlowおよびその他のトラフィック情報を含めることもできます。各エンティティの最新のモデルを維持するため、Secure Cloud Analytics では、エンティティがトラフィックを送信し続け、場合によっては異なるトラフィックを送信する可能性があるため、これらのモデルを徐々に更新します。この情報から、Secure Cloud Analytics は以下を識別します。

- 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、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。Security Cloud Control と統合すると、ファイアウォールイベントからこれらの事実を取得できます。**Total Network Analytics and Monitoring** ライセンスも購入すると、システムはNetFlowから事実を取得し、ファイアウォールイベントとNetFlowの両方から観測内容を生成することもできます。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。1 つのアラートが複数の観測内容を表す場合があることに注意してください。ファイアウォールが同じ接続とエンティティに関連する複数の接続イベントをログに記録する場合、アラートが 1 つだけになる可能性があります。

上記の例で言えば、新しい内部デバイスの観測内容だけでは、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 の 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。

Secure Cloud Analytics でアラートを表示して閉じる場合、Secure Cloud Analytics UI からのトラフィックを許可またはブロックできないことに注意してください。デバイスをアクティブモードで展開した場合、ファイアウォール アクセス コントロール ルールを、トラフィックを許可またはブロックするように更新する必要があり、ファイアウォールがパッシブモードで展開されている場合は、ファイアウォールアクセスコントロールルールを更新する必要があります。

ファイアウォールイベントに基づくアラートの使用

必要なライセンス：**Logging Analytics and Detection** または **Total Network Analytics and Monitoring**

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。

注: **Total Network Analytics and Monitoring** ライセンスを持っている場合、アラートは、NetFlow から生成された観測結果、ファイアウォールイベントから生成された観測結果、または両方のデータ ソースからの観測結果に基づいて生成できます。

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。

Security Cloud Control の 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。

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。

1. オープンアラートのトリアージ （9 ページ）
2. 後で分析するためにアラートをスヌーズする （10 ページ）
3. 詳細な調査のためのアラートの更新 （10 ページ）
4. アラートの確認と調査の開始 （11 ページ）
5. エンティティとユーザーの調査 （13 ページ）
6. Secure Cloud Analytics を使用して問題を解決する （14 ページ）
7. アラートの更新とクローズ （15 ページ）

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。

- Security Cloud Control から Secure Cloud Analytics への相互起動とアラート表示の詳細については、「Monitoring Secure Cloud Analytics Alerts Generated from FTD Events」を参照してください。

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。

これが優先順位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切断す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する

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（エンティティの現在のトラフィックが、以前には一致しなかった動作プロファイルと一致することを示します）。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。

アラートをスヌーズする：

手順

ステップ1 [アラートを閉じる（Close Alert）] をクリックします。
ステップ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。
ステップ3 [保存（Save）] をクリックします。

次のタスク

スヌーズしたアラートを確認する準備ができたら、アラートの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。

スヌーズしたアラートのスヌーズを解除する：

- 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。

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

ステップ1 **[モニター（Monitor）]** > **[アラート（Alerts）]** を選択します。

ステップ 2 アラートタイプ名をクリックします。

次のタスク

初期トリアージと優先順位付けに基づいて、アラートを割り当て、タグを付けます。

1. [担当者（Assignee）] ドロップダウンからユーザーを選択してアラートを割り当てます。これにより、ユーザーが調査を開始できるようになります。
2. [タグ（Tags）] ドロップダウンから 1 つ以上のタグを選択して、アラートにタグを追加することにより、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確立を試みることができます。
3. 必要に応じて、**このアラートに関するコメント**を入力し、[コメント（Comment）]をクリックすることにより、最初の調査結果を追跡するためのコメントを残し、アラートに割り当てられた担当者を支援することができます。アラートは、システムコメントとユーザーコメントの両方を追跡します。

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場合は、アラートの詳細を確認して、Stealthwatch Cloud 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。

アラートがファイアウォールイベントに基づいて生成された場合、ファイアウォールの展開がこのアラートのソースであることはシステムに認識されません。

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に、サポートされている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である可能性があるかどうかを確認します。

手順の概要

1. アラートの詳細で、観測タイプの横にある矢印アイコン（➔）をクリックして、そのタイプの記録されたすべての観測内容を表示します。
2. [ネットワークのすべての観測内容（All Observations for Network）] 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記録された観測内容をすべて表示します。

手順の詳細

手順

ステップ 1 アラートの詳細で、観測タイプの横にある矢印アイコン（➔）をクリックして、そのタイプの記録されたすべての観測内容を表示します。

ステップ 2 [ネットワークのすべての観測内容（All Observations for Network）] 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記録された観測内容をすべて表示します。

観測内容に対して追加の分析を実行する場合は、サポートされている観測内容をコンマ区切り値ファイルでダウンロードします。

- アラートの詳細の [サポートされている観測内容（Supporting Observations）] ペインで、[CSV] をクリックします。

観測内容から、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判断します。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の IP アドレスまたはホスト名から、ソースエンティティに関連する追加コンテキスト（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、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。

- 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観測内容を表示するには、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。

Stealthwatch Cloud のソースエンティティは常にネットワークの内部にあることに注意してください。この点を、接続を開始したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのイニシエータ IP と比較してください。

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外部エンティティの IP アドレスまたはホスト名のコンテキストを確認します。

- 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 Web 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 Web 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 Web サイト上でこの情報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 [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。

Stealthwatch Cloudの接続エンティティは、常にネットワークの外部にあることに注意してください。この点を、接続要求に応答したエンティティを示し、ネットワークの内部または外部にある可能性がある、ファイアウォールイベントのレスポンダ IP と比較してください。

調査結果に関するコメントを残します。

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

エンティティとユーザーの調査

Stealthwatch Cloud ポータル UI でアラートを確認した後、ソースエンティティ、このアラートに関係している可能性のあるユーザー、およびその他の関連エンティティに対して、追加の調査を直接実行できます。

- ソースエンティティがネットワーク上のどこ（物理的またはクラウド上）にあるかを特定し、直接アクセスします。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。

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

Secure Cloud Analytics を使用して問題を解決する

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。次に例を示します。

- 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とファイアウォール構成を更新して、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。
- エンティティが不正または悪意のあるドメインにアクセスを試みた場合は、影響を受けるエンティティを調べて、マルウェアが原因かどうかを判断します。悪意のある DNS リダイレクトがある場合は、ネットワーク上の他のエンティティが影響を受けているかどうか、またはボットネットの一部であるかどうかを判断します。これがユーザーによる意図である場合は、ファイアウォール設定のテストなど、正当な理由があるかどうかを判断します。ファイアウォールルールとファイアウォール構成を更新して、ドメインへのそれ以上のアクセスを防止します。
- エンティティが過去のエンティティモデルの動作と異なる動作を示している場合は、動作の変更が意図されたものかどうかを判断します。意図されたものでない場合は、変更の責任がネットワーク上の承認されたユーザーにあるかどうかを調べます。ネットワークの外部にあるエンティティが関係している場合は、ファイアウォールルールとファイアウォール構成を更新して意図せぬ動作に対処します。
- 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、ファイアウォール構成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。ファイアウォールファイルおよびマルウェアイベントを確認して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、エンティティを検疫および更新して、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。ファイアウォールのアクセス制御およびファイルとマルウェアルールを更新して、今後このマルウェアがネットワークに感染するのを防ぎます。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。ファイアウォール構成を更新して、このソースによる今後のデータ漏洩の試みを防ぎます。

アラートの更新とクローズ

調査結果に基づいてタグを追加する。

手順

ステップ 1 Secure Cloud Analytics ポータルの UI で、[監視（Monitor）] > [アラート（Alerts）] を選択します。 >
ステップ 2 ドロップダウンから 1 つ以上の**タグ**を選択します。

調査結果と実行された修正手順を説明する最終コメントを追加する。

- 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。

アラートをクローズして、有用だったかどうかをマークする。

1. アラートの詳細から、[アラートをクローズ（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. [保存（Save）] をクリックします。

次のタスク

クローズしたアラートをオープンする

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。

クローズしたアラートをオープンする

- クローズしたアラートの詳細から、[アラートを再オープン（Reopen Alert）] をクリックします。

アラートの優先順位を変更する

必要なライセンス：Logging Analytics and Detection または **Total Network Analytics and Monitoring**

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、シスコのインテリジェンスおよびその他の要因に基づいて、[低（low）] または [通常（normal）] にデフォルト設定されます。ネットワーク環境に基づいて、関心のある特定のアラートを強調するために、アラートタイプの優先順位を変更することができます。アラートタイプの優先順位は、[低（low）]、[通常（normal）]、または [高（high）] に設定できます。

- **[モニター（Monitor）]** > **[アラート（Alerts）]** を選択します。
- 設定のドロップダウンアイコン（）をクリックし、[アラートのタイプと優先順位（Alert Types and Priorities）] を選択します。
- アラートタイプの横にある編集のアイコン（）をクリックし、[低（low）]、[中（medium）]、または [高（high）] を選択して優先順位を変更します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。