Cisco Secure Cloud Analytics

SecureX 統合ガイド

目次

Cisco SecureX との Cisco Secure Cloud Analytics の統合

Cisco SecureX プラットフォームは広範なシスコの統合型セキュリティポートフォリオとお客様のインフラストラクチャをつなぐことで、一貫した操作性を提供します。これにより可視性が統一され、自動化が実現し、ネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティが強化されます。統合プラットフォームでの接続技術により、SecureX は測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。

Cisco Secure Cloud Analytics（以前の Stealthwatch Cloud）と SecureX を統合して SecureX ダッシュボードからの Secure Cloud Analytics の展開に関する追加のコンテキストを表示したり、Secure Cloud Analytics Web ポータル内から SecureX リボンを使用したりできます。

SecureX リボンにログインしている場合は、アラートに基づいて Cisco SecureX 脅威対応（以前の [Cisco Threat Response]）のインシデントを作成し、IP アドレスから他の SecureX 製品統合にピボットすることもできます。これらの機能の使用についての詳細は、『Secure Cloud Analytics Initial Deployment Guide』を参照してください。

無料トライアルの詳細については、https://info.observable.net/SecureX-Trial-Request.html を参照してください。

SecureX アカウントを作成した後に、https://securex.us.security.cisco.com/help/ribbon でリボンの詳細を参照してください。

SecureX での Cisco Secure Cloud Analytics のタイル

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（ネットワーク上の動作に関する事実）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。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。観測内容、ロール、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。

Secure Cloud Analytics また、Web ポータルの UI から確認できるように、関心のある動作の観測内容も識別されます（観測内容を強調表示）。これらの観測内容は、それ自体は悪意のある動作を意味するものではありませんが、ネットワーク上の注目すべきトラフィックを表している可能性があります。

次に、SecureX ダッシュボードに表示できる、Secure Cloud Analytics の結果を表す Secure Cloud Analytics のタイルについて説明します。

アラート概要チャート（Alert Overview Chart）

[アラート概要チャート（Alert Overview Chart）] タイルには、選択した期間に基づいたマルチレベルの円グラフが外側のリングに表示されます。

- 期間内に作成された新しい Secure Cloud Analytics アラート
- 期間より前に作成され、期間内にまだ閉じられていない未解決の Secure Cloud Analytics アラート
- 期間中に閉じられた解決済みの Secure Cloud Analytics アラート

内側のリング内のアラート：

- 割り当てられている Secure Cloud Analytics アラート
- 未割り当ての Secure Cloud Analytics アラート

アラートクイックビュー（Alert Quick View）

[アラートクイックビュー（Alert Quick View）] タイルには、未解決の Secure Cloud Analytics アラートと未割り当ての Secure Cloud Analytics アラートの現在の数が表示されます。

デバイス数チャート（Device Count Chart）

[デバイス数チャート（Device Count Chart）] タイルには、指定した期間中にネットワーク上でトラフィックの送信を Secure Cloud Analytics が検出した一意のエントリの数を縦棒チャートとして表示されます。

監視数（Observation Count）

[監視数（Observation Count）] タイルには、指定した期間内に Secure Cloud Analytics が生成した監視内容の数と、その期間内のハイライトされた監視内容の合計数が表示されます。[監視内容（Observations）] リンクと [ハイライトされた監視内容（Highlighted Observations）] リンクをクリックすると、ポータルの UI に移動して、これらの監視内容に関する詳細情報を表示できます。

Cisco Secure Cloud Analytics センサーステータス（Sensor Status）

[センサーステータス（Sensor Status）]**Cisco Secure Cloud Analytics** タイルには、構成済みの Cisco Secure Cloud Analytics センサー（以前の Stealthwatch Cloud Sensor）のリストと、それらがアクティブか非アクティブかが表示されます。

トラフィック時系列チャート（Traffic Over Time Chart）

[トラフィック時系列チャート（Traffic Over Time Chart）] タイルには、選択した期間に Secure Cloud Analytics がモニターしたインバウンドトラフィック、インバウンド暗号化トラフィック、アウトバウンドトラフィック、およびアウトバウンド暗号化トラフィックの数が積み上げ棒チャートとして表示されます。

Cisco Secure Cloud Analytics との SecureX の統合の構成

SecureX の統合を構成するには、次の手順を実行します。

- Secure Cloud Analytics からの SecureX へのアクセスを許可する
- Secure Cloud Analytics または SecureX で統合を有効にする

SecureX アカウントを持っている必要があります。詳細については、https://www.cisco.com/c/en/us/td/docs/security/secure-sign-on/sso-quick-start-guide.html を参照してください。

Cisco Secure Cloud Analytics から SecureX へのアクセスを許可する

SecureX へのアクセスを承認すると、Secure Cloud Analytics のリボンが有効になります。

手順

1. Secure Cloud Analytics Web ポータルにログインします。
2. ページの一番下にあるリボンの [+] をクリックして展開します。
3. [SecureX の取得（Get SecureX）] をクリックし、指示に従ってアクセスを承認します。

Secure Cloud Analytics または SecureX での統合を有効にする

Secure Cloud Analytics Web ポータルまたは SecureX から SecureX の統合を有効にすることができます。

前提条件

- Secure Cloud Analytics のサイトマネージャーであること。
- SecureX の組織管理者であること。

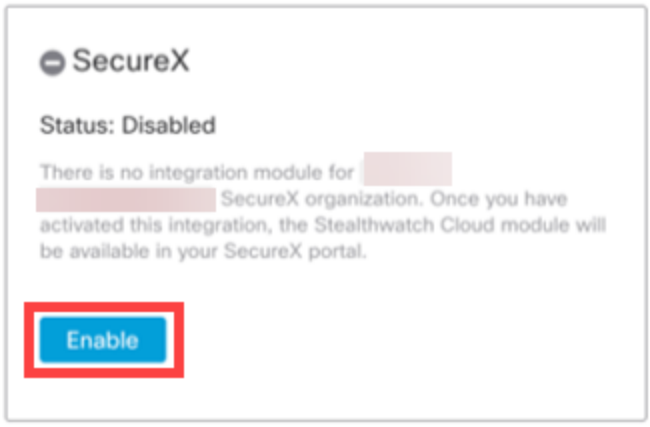
これらのロールのいずれでもない場合は、読み取りアクセス権のみが付与されます。

Cisco Secure Cloud Analytics の使用

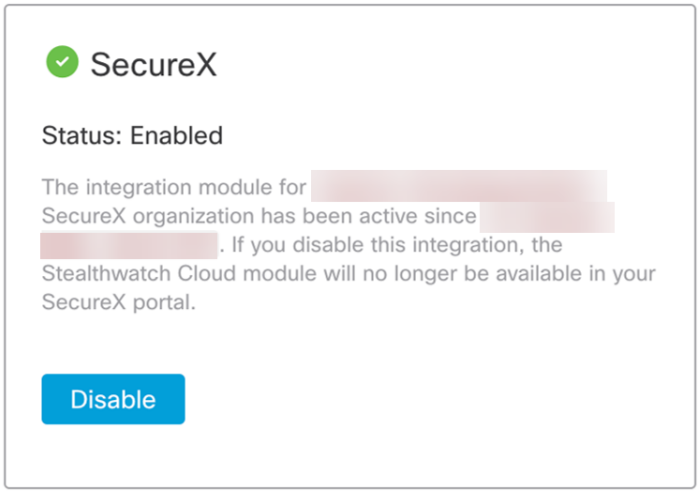
手順

1. サイトマネージャーとして Web ポータルにログインします。Secure Cloud Analytics
2. [設定（Settings）] > [統合（Integrations）] > SecureX を選択します。

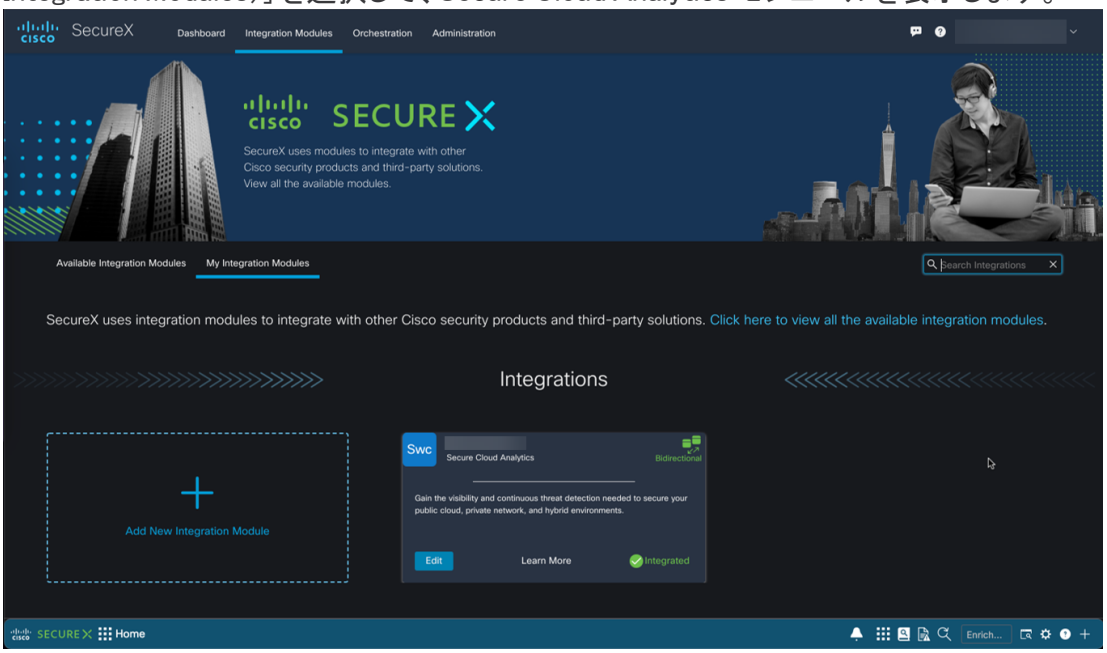
3. [有効(Enable)] をクリックします。



4. SecureX モジュールのステータスが [有効(Enabled)] に更新されます。



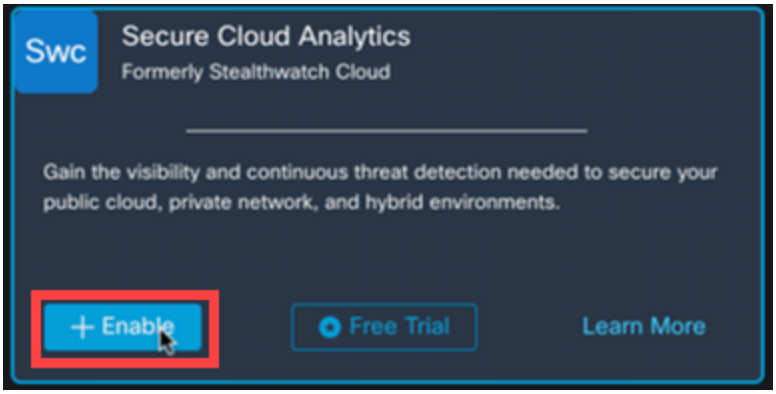
5. SecureXに進みます。[統合モジュール(Integration Modules)] > [マイ統合モジュール(My Integration Modules)] を選択して、Secure Cloud Analytics モジュールを表示します。



SecureX の使用

手順

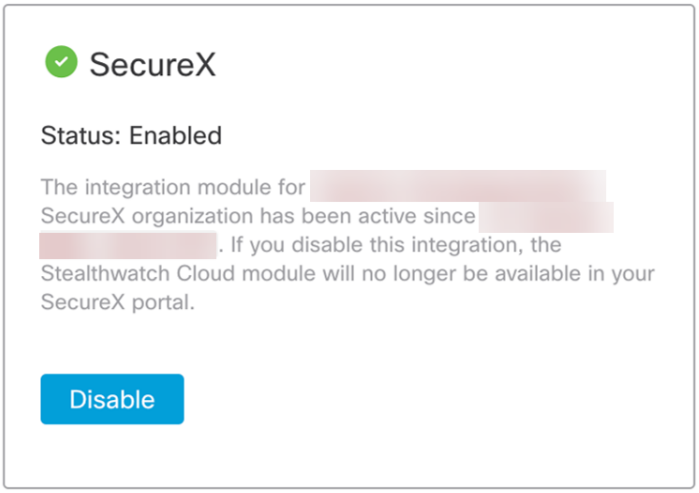
1. SecureX にログインします。
2. [統合モジュール(Integration Modules)] に移動します。
3. [利用可能な統合モジュール(Available Integration Modules)] タブで Secure Cloud Analytics モジュールを見つけ、[有効にする(Enable)] をクリックします。



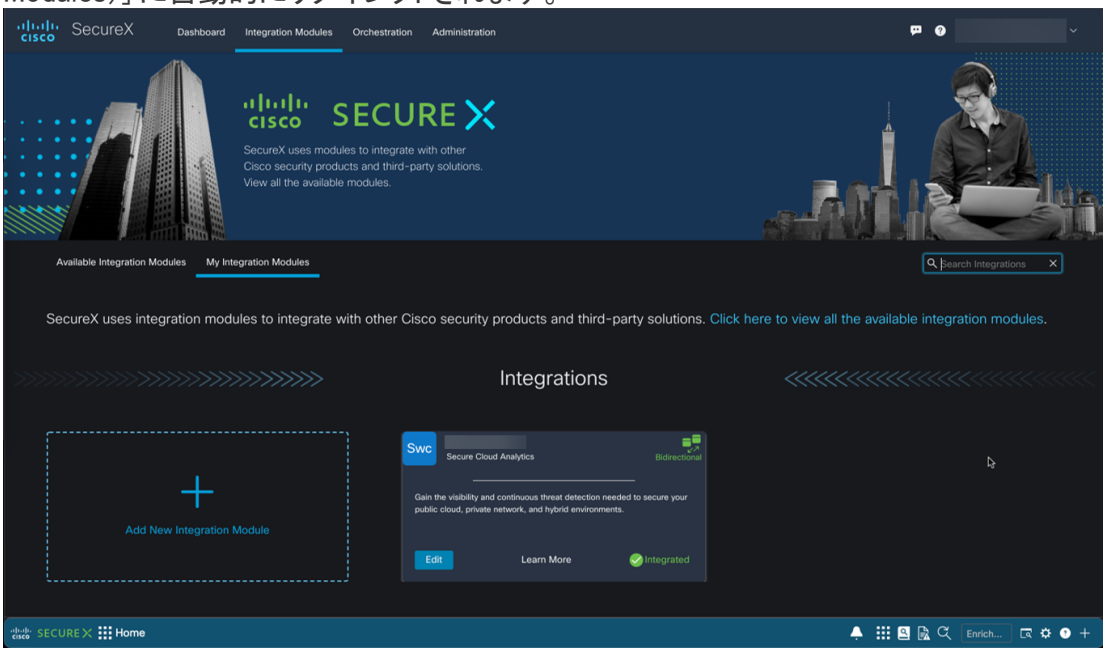
Secure Cloud Analytics の SecureX の統合ページに自動的にリダイレクトされます。

> 複数の Secure Cloud Analytics ポータルがある場合は、SecureX セキュリティのリボンに接続しているポータルを選択する必要があります。

4. SecureX モジュールのステータスが [有効(Enabled)] になります。



5. **SecureX** > [統合モジュール(Integration Modules)] > [マイ統合モジュール(My Integration Modules)] に自動的にリダイレクトされます。



SecureX へのアラートの発行

Secure Cloud Analytics Web ポータルから、**SecureX** への公開機能を使用してアラートコンテンツを送信できます。これにより、次を含む SecureX の Secure Cloud Analytics アラートデータを完全に表示できるようになります。

- アラートタイプ
- Secure Cloud Analytics アラート ID
- Secure Cloud Analytics アラートへの参照
- アラートが発生した Secure Cloud Analytics テナント（複数の Secure Cloud Analytics ポータルを SecureX と統合した場合）
- 詳細説明
- 次のステップ
- アラートの更新タイムスタンプ
- アラートの時点でわかっている IP アドレスとホスト名
- MITRE ATT&CK の戦術とテクニック（該当する場合）
- アラート担当者
- アラートの優先順位
- アラートに関連付けられたユーザータグ

アラート発行の有効化

- Talos Intelligence ウォッチリスト ヒット アラートは、SecureX に発行されるように自動的に有効になっています。
- アラートが無効になっている場合は、そのアラートを SecureX に発行することはできません。

1. Secure Cloud Analytics Web ポータルにログインします。
2. [設定（Settings）] > [アラート（Alerts）] を選択します。
3. SecureX に送信するアラートを見つけ、[SecureX に発行（Publish to SecureX）] 列の （[トグル（Toggle）]）アイコン をクリックします。

関連リソース

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 初期導入ガイドなど、インストールおよびコンフィギュレーション 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。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
- Secure Cloud Analytics 無料トライアルの試用時に電子メールでケースを開く場合：
  swatchc-support@cisco.com

変更履歴

リビジョン	改訂日	説明
1.0	2020 年 6 月 24 日	最初のバージョン。
1.1	2020 年 12 月 10 日	SecureX の統合に関する追加情報を更新。
2.0	2021 年 11 月 3 日	製品のブランド名を更新。
3.0	2022 年 2 月 15 日	構成手順を更新。
4.0	2022 年 7 月 20 日	アラートの SecureX への発行とサポートへの連絡のセクションを追加。

著作権情報