Cisco Stealthwatch

Cisco SecureX v7.3 統合ガイド

目次

はじめに

Cisco SecureX は、複数の製品やソースから集約されたデータを使用して、脅威を検出、調査、分析、対応するために役立つ Cisco Cloud のプラットフォームです。

この統合により、Stealthwatch で以下を行うことができます。

- SecureX ダッシュボードの Stealthwatch タイルを使用して、主要な業務メトリクスをモニターする。
- SecureX のコンテキストメニューを使用して、他のシスコ セキュリティおよびサードパーティの統合にピボットする。
- SecureX のリボンへのアクセスを提供する。
- Cisco Threat Response プライベート インテリジェンス ストアへ Stealthwatch アラームを送信する。
- Threat Response ワークフローの調査コンテキストを強化するために、SecureX で Stealthwatch からのセキュリティイベントを要求できるようにする。

SecureX の詳細については、次のリンクを参照してください。

- SecureX の Web サイト
- SecureX のマニュアル

新機能

バージョン v7.3 には、統合に対するいくつかの拡張機能が含まれています。

- Stealthwatch を Cisco Threat Response プライベート インテリジェンス ストアに送信するための設定オプションを [SecureX の設定（SecureX Configuration）] ページから [対応管理（Response Management）] に移動しました。アラームをインシデントとして Cisco Threat Response に昇格するために、脅威対応インシデントアクションを含むルールを設定できます。詳細については、「Cisco Threat Response への Stealthwatch アラームの送信について」の項を参照してください。
- Cisco Security Service Exchange（SSE）での Stealthwatch 管理コンソール（SMC）を自動登録できるオプションを追加しました。詳細については、「Cisco Cloud での SMC の登録」の項を参照してください。

7.2 から 7.3 へのアップグレード

7.2 の SecureX 設定で Cisco Threat Response に Stealthwatch アラームを送信するオプションが有効になっている場合は、Cisco Threat Response にアラームを送信し続けるように Threat Response のインシデントアクションが自動的に設定されます。

SecureX の地域クラウド

地域	リンク	サポートされている Stealthwatch 統合
北米	• Threat Response Web コンソール：https://visibility.amp.cisco.com • SecureX ポータル：https://securex.us.security.cisco.com	• SecureX ピボットメニュー • SecureX のリボン • Cisco Threat Response への Stealthwatch アラームの送信 • Stealthwatch セキュリティイベントで強化
欧州	• Threat Response Web コンソール：https://visibility.eu.amp.cisco.com • SecureX ポータル：https://securex.eu.security.cisco.com	• SecureX ピボットメニュー • SecureX のリボン • Cisco Threat Response への Stealthwatch アラームの送信 • Stealthwatch セキュリティイベントで強化
アジア（APJC）	• Threat Response Web コンソール：https://visibility.apjc.amp.cisco.com • SecureX ポータル：https://securex.apjc.security.cisco.com	• SecureX ピボットメニュー • SecureX のリボン • Cisco Threat Response への Stealthwatch アラームの送信

地域クラウドの選択に関する注意事項と制約事項

- 可能な場合は、Stealthwatch の導入環境に最も近い地域クラウドを使用してください。
- 異なるクラウド内のデータを集約またはマージすることはできません。
- 複数の地域からデータを集約する必要がある場合は、すべての地域のデバイスが同じ地域のクラウドにデータを送信する必要があります。
- 各地域のクラウド上にアカウントを作成できます。各クラウドのデータは区分されます。

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。
- Cisco Stealthwatch サポートのお問い合わせ先:
  - 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:
    www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

Stealthwatch データと SecureX

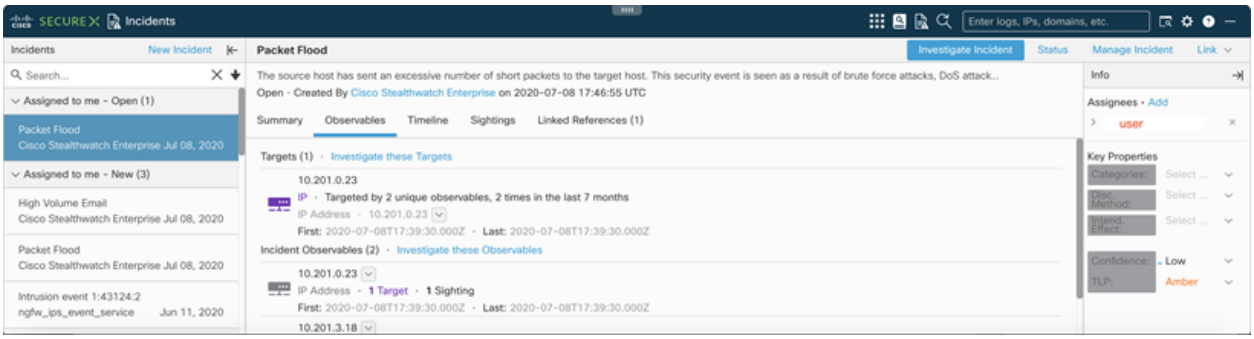
SecureX のリボンとピボットメニュー

SecureX のリボン

SecureX のリボンは、ページの下部にある SMC UI に表示されるウィジェットです。このリボンは、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散型機能を提供します。これらの機能は、リボン内にアプリケーション（アプリ）とツールの形式で表示されます。

リボンを設定すると、SMC の任意のページから、インシデント、ケースブックの管理、オブザーバブルの検索、調査と脅威ハンティングの開始、SecureX と統合された他の製品へのアクセスなどを行うことができます。

リボンを設定するには、「SecureX のリボンとピボットメニューの許可」の項を参照してください。



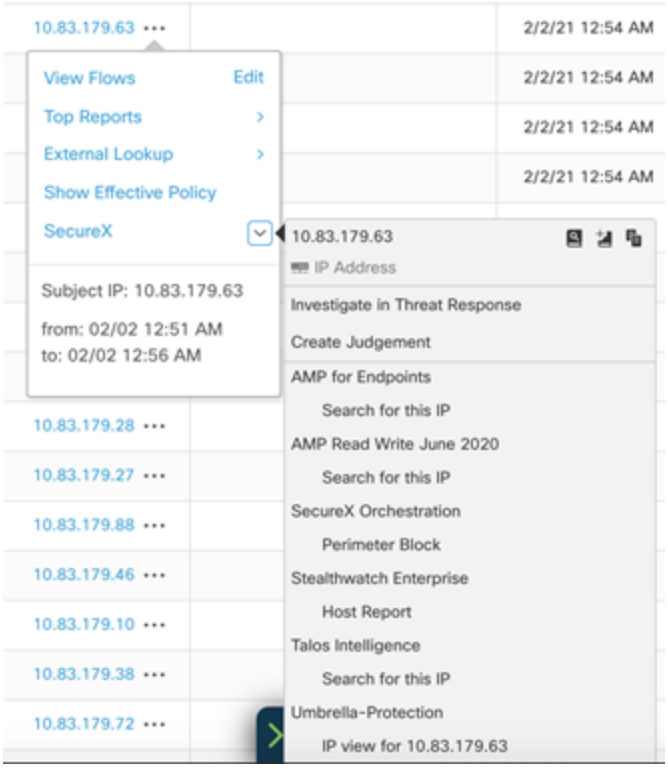
リボンの詳細については、『Cisco SecureX Getting Started Guide』の「Cisco SecureX Ribbon」の項を参照してください。

SecureX ピボットメニュー

ピボットメニューでは、SecureX によって、他のシスコ製品のデータとともにシスコの脅威インテリジェンスリソースを活用できる中心的なアクセスポイントが提供されます。

ピボットメニューは、SecureX に統合されている他の製品とグループにリンクしています。ピボットメニューで一部のアクションを直接実行することも、統合製品にピボットして追加のアクションを実行することもできます。

Stealthwatch では、SecureX 統合の設定後に、SMC の該当する IP アドレスの横にある ••• ([省略記号（Ellipsis）])アイコン をクリックすることでピボットメニューを使用できます。



ピボットメニューから使用できる機能の詳細については、「SecureX Pivot menu」のヘルプトピック（英語）を参照してください。

ピボットメニューのヘルプを表示するには、SecureX にログインする必要があります。

SecureX ダッシュボードの Stealthwatch タイルについて

次の Stealthwatch タイルは、SecureX ダッシュボードで使用できます。

タイル名	説明	使用可能時間帯	ピボット先
上位のアラームホスト	最後のリセット時以降ネットワーク上でアクティブになっていて、アラーム重大度別にソートされた上位 7 位までの内部ホストを提供する。	直近の 24 時間	Host Report
カテゴリ別のホストのアラーム	最後のリセット時以降ネットワーク上でアクティブになっていて、アラーム重大度別にソートされた上位 7 位までの内部ホスト。	直近の 24 時間	ネットワーク セキュリティ ダッシュボード

タイル名	説明	使用可能時間帯	ピボット先
カウント別の上位のアラーム	カウント別の上位 10 位のアラームを表す。	直近の 24 時間 過去 7 日	ネットワーク セキュリティ ダッシュボード
可視性アセスメント	内部ネットワークスキャナ、Remote Access 侵害、感染の可能性があるマルウェア、脆弱なプロトコルサーバー、DNS リスクなど、可視性アセスメントカテゴリ内のホスト数。	直近の 24 時間 過去 7 日	可視性アセスメントダッシュボード
ネットワークの可視性	ホスト数とトラフィック量の統計情報を提供する。	直近の 24 時間 過去 7 日	可視性アセスメントダッシュボード
トラフィック別の上位の内部ホストグループ	相互に通信されたトラフィック別の上位 10 位の内部ホストグループ。	直近の 12 時間	内部ホストグループのホストグループレポート
トラフィック別の上位のホストグループ	内部ホストグループと通信したトラフィック別の上位 10 位の外部ホストグループ。	直近の 12 時間	内部ホストグループのホストグループレポート

Stealthwatch タイルを使用して SecureX ダッシュボードを設定する方法については、「Stealthwatch タイルを使用した SecureX ダッシュボードの設定」のセクションを参照してください。

Cisco Threat Response への Stealthwatch アラームの送信について

SecureX 統合を設定すると、アラームメタデータから作成された、対応する検出情報、オブザーバブル、およびインジケータのオブジェクトを持つインシデントを使用して、Stealthwatch のアラームから Cisco Threat Response プライベート インテリジェンス ストアにシステムを昇格できるようになります。

この情報は、インシデントから派生した対応する検出情報として調査プロセス時に Incident Manager 内で、また、Cisco Threat Response の Web コンソール内で使用できます。

対応管理の Threat Response インシデントアクションでは、一般的なアクションパラメータの他に次のオプションを設定できます。

- [インシデント信頼度レベル(Incident Confidence Level)]:Cisco Threat Response に送信されるインシデントに設定する信頼度レベルを選択できます。

- [新しいターゲットエンティティの作成（Create a new Target entity）]：Stealthwatch が Cisco Threat Response のターゲットとしてアラームからホストを指定できるようにします。詳細については、「CTIM オブジェクトへの Stealthwatch アラームの変換について」の項を参照してください。
    - Cisco Threat Response に送信する必要があるホスト情報を決定するときに内部 IP アドレスのみを含める場合は、[Threat Response にターゲットを作成する（内部ホストのみ）（Create Targets in Threat Response for Internal hosts only）] オプションを選択します。
    - Cisco Threat Response に送信する必要があるホスト情報を決定するときに内部と外部の両方の IP アドレスを含める場合は、[Threat Response にターゲットを作成する（内部ホストと外部ホスト）（Create Targets in Threat Response for internal and external hosts）] オプションを選択します。
- [アラームデータからのホストの詳細を使用（Use host details from the alarm data）]：ターゲットオブジェクトを送信元ホストとターゲットホスト用に構築するか、送信元ホストのみまたはターゲットホストのみ用に構築するかを指定できます。

詳細については、『*対応管理の設定*』のヘルプトピックを参照してください。

- 以前のバージョンの Stealthwatch で Cisco Threat Response に Stealthwatch のアラームを送信するように設定した場合は、Threat Response のインシデントアクションが自動的に作成されます。
- 関係ポリシーから派生したアラーム用に作成されたインシデントには、この情報はアラームで利用できないため、Observable としての IP アドレスは含まれません。
- インシデントには、「CTIM オブジェクトへの Stealthwatch アラームの変換について」セクションで指定された特定の条件のターゲットオブジェクトが含まれます。
- Stealthwatch アラームから作成されたインシデントは、地域クラウドとともに配置された CTR コンソールから表示できます。詳細については、「SecureX の地域クラウド」のセクションを参照してください。

SecureX の Stealthwatch エンリッチメントデータについて

SMC が Cisco Security Services Exchange に登録され、Stealthwatch モジュールが SecureX で設定されると、Threat Response ワークフローで Stealthwatch からのエンリッチメントデータを確認できるようになります。

調査で要求されたすべての有効な IP アドレスについて、Stealthwatch は、この IP に関連付けられているセキュリティイベントを、該当する Sighting および Indicator オブジェクトの形式で返します。

[SecureX 設定（SecureX Configuration）] フォームで返されるセキュリティイベントに、次のパラメータを設定できます。

- SecureX からの調査リクエストを許可するかどうか。
- セキュリティイベントを返す Stealthwatch ドメイン。
- 送信される上位イベントの数。
- セキュリティイベントを返す期間。

Cisco Threat Intel モデルについて

SecureX に送信する前に、Stealthwatch アラームとセキュリティイベントが Cisco Threat Intel Model（CTIM）オブジェクトに変換されます。

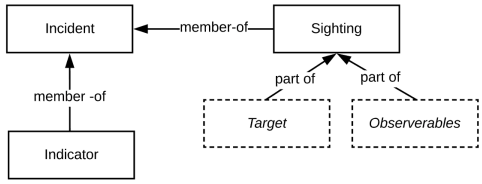
CTIM の詳細については、『Threat Intel Model documentation』を参照してください。

この変換で使用される主要なエンティティを次に示します。

- Incident：組織に影響する指標の個別のインスタンスと、インシデント対応に関連する情報。
- Sighting：特定の日時にサイバー上で観測されたデータにおける記録
- Observable：一貫性のある ID を持ち、意図または特性（ドメイン名、IP アドレス、ファイルハッシュ、特定のデバイスまたはユーザー）ごとに分類されるのに十分な安定性がある、単純で原始的な値。Stealthwatch では、IP アドレスタイプにおける Observable のみを共有します。
- Target：脅威の標的となったデバイス、ID、またはリソース。ターゲットは 1 つ以上の Observable によって識別されます。
- Indicator：悪意のある動作を示す動作パターンまたは一連の条件についての記述。

CTIM オブジェクトへの Stealthwatch アラームの変換について

Threat Response のインシデントアクションによって送信されたすべてのアラームは、インシデント、検出情報、インジケータとそれらの間の関係に変換されます。次の図は、CTIM モデルでの Stealthwatch アラームの表示を示しています（簡易版）。



インシデントの Sighting オブジェクトを作成する場合、Stealthwatch には、以下の制約を持つ Observable が含まれます。

- リレーションシップ ポリシー イベントから派生したアラームには、Sighting オブジェクトに Observable オブジェクトがありません。
- 送信元が「複数の送信元」またはターゲットが「複数の送信先」であるアラームには、該当する Observable は、Sighting のオブジェクトに含まれません。

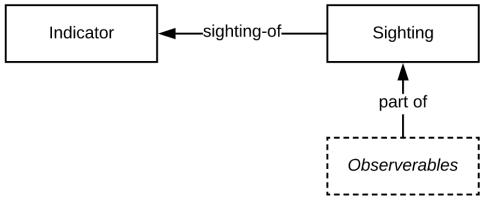
検出情報のターゲットオブジェクトを構築するためのルールは、次の追加の成約を使用してアラームを処理する Threat Response のインシデントアクションから取得されます。

- アラームの送信元または宛先が「複数の宛先」の場合、ターゲットオブジェクトは含まれません。

Stealthwatch セキュリティイベントの CTIM オブジェクトへの変換について

SecureX からの調査リクエストに応じて、Stealthwatch は IP アドレスに関連付けられたセキュリティイベントを返します。

すべてのセキュリティイベントは、次の図に示すように、リレーションシップを使用して CTIM モデルの Sighting および Indicator オブジェクトに変換されます。



Stealthwatch セキュリティイベントを CTIM オブジェクトに変換する場合、次の制約事項とルールが適用されます。

- ターゲットオブジェクトは、セキュリティイベントの Sighting オブジェクトに含まれていません。

Cisco Cloud アカウント

SecureX アクセスに必要なアカウント

SecureX および関連ツールを使用するには、使用予定の地域クラウドで次のいずれかのアカウントを持っている必要があります。

- シスコ セキュリティアカウント
- AMP for Endpoints アカウント
- Cisco Threat Grid アカウント

> お客様またはお客様の組織ですでに、使用予定の地域クラウドで上記のいずれかのアカウントをお持ちの場合は、既存のアカウントを使用してください。新しいアカウントを作成しないでください。

SecureX にアクセスするためのアカウントの作成

アカウントの作成の詳細については、『SecureX Sign-On Guide』を参照してください。

組織のシスコ セキュリティアカウントへのアクセスの管理

お客様がシスコ セキュリティアカウントの所有者または管理者の場合は、別のユーザーに組織のシスコ セキュリティアカウントへのアクセス権を付与でき、既存のユーザーを管理できます（アカウントのアクティベーションの電子メールを再送信するなど）。

ユーザーを管理するには、次の手順を実行します。

1. ブラウザウィンドウで、自身の地域のシスコセキュリティアカウントに移動します。
   - 北米：https://castle.amp.cisco.com
   - ヨーロッパ：https://castle.eu.amp.cisco.com
   - アジア（APJC）：https://castle.apjc.cisco.com
2. [ユーザー（Users）] をクリックします。
3. ユーザーアクセス権を追加または編集します。
   [アカウント管理者（Account Administrator）] を選択した場合は、ユーザーにはユーザーアクセス権を付与して管理する権限が与えられます。

Stealthwatch と SecureX の設定

SecureX 統合の設定

Stealthwatch で SecureX 統合を設定すると、次のことが可能になります。

- Stealthwatch UI の SecureX ピボットメニュー。
- Stealthwatch の UI 内の SecureX のリボン
- Cisco Threat Response プライベート インテリジェンス ストアへ Stealthwatch アラームを送信する。

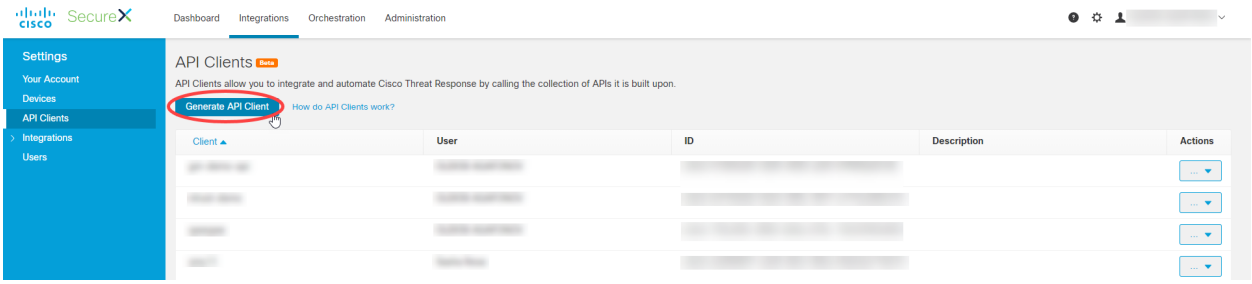
前提条件

- SMC v7.2.1 以降
- SecureX にアクセスするためのアカウントがある（「SecureX アクセスに必要なアカウント」を参照）。
- SMC は、アウトバウンドで Cisco Cloud に接続できる必要があります。
    - 北米クラウド：
        - api-sse.cisco.com、ポート 443
        - visibility.amp.cisco.com、ポート 443
    - EU クラウド：
        - api.eu.sse.itd.cisco.com、ポート 443
        - visibility.eu.amp.cisco.com、ポート 443
    - アジア（APJC）クラウド：
        - api.eu.sse.itd.cisco.com、ポート 443
        - visibility.apjc.amp.cisco.com、ポート 443
- Stealthwatch の導入により、セキュリティイベントとアラームが予期したとおりに生成されています。

手順

SecureX 統合を設定するには、次の手順を実行します。

1. 地域の SecureX クラウドに移動します。
    - 北米のクラウド：https://visibility.amp.cisco.com
    - ヨーロッパのクラウド：https://visibility.eu.amp.cisco.com
    - アジア（APJC）クラウド：https://visibility.apjc.amp.cisco.com
2. エンドポイント向け AMP、Cisco Threat Grid、またはシスコのセキュリティ アカウントのクレデンシャルを使用してサインインします。
3. [統合（Integrations）] タブに移動し、[設定（Settings）] メニューの [API クライアント（API Clients）] をクリックします。
4. [API クライアントの生成（Generate API Client）] をクリックします。

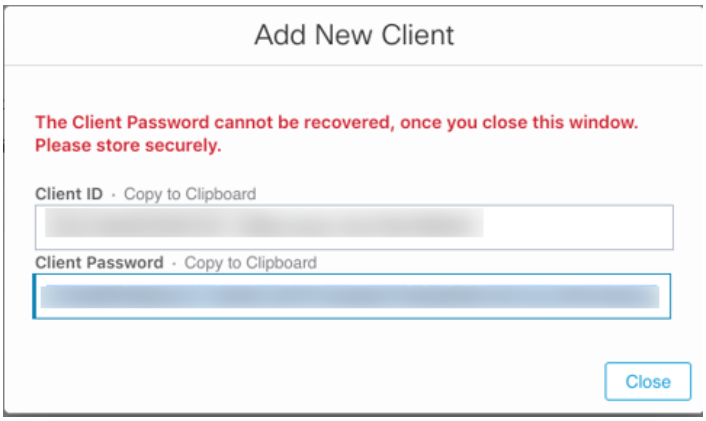


5. 開いているダイアログで、API クライアントの名前と説明を入力し、次の範囲を選択します。

- Casebook
- Global Intel:read
- Notification
- Private Intel
- Response
- Webhook
- Enrich:read
- Inspect:read
- Oauth
- Profile
- Telemetry:write
- Feedback
- Integration
- Orbital
- Registry
- Users

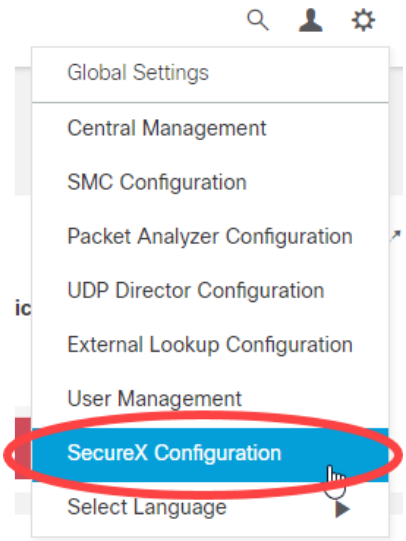
> API クライアントが生成された後は範囲を変更できません。

6. [新しいクライアントの追加(Add New Client)] をクリックします。
7. システムは、クライアント ID とクライアントパスワードを作成します。

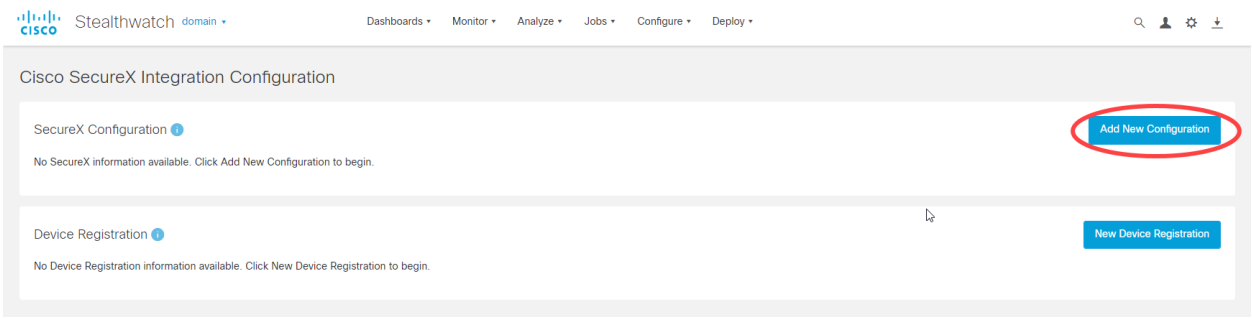


> このウィンドウを閉じると、クライアントパスワードを回復できません。

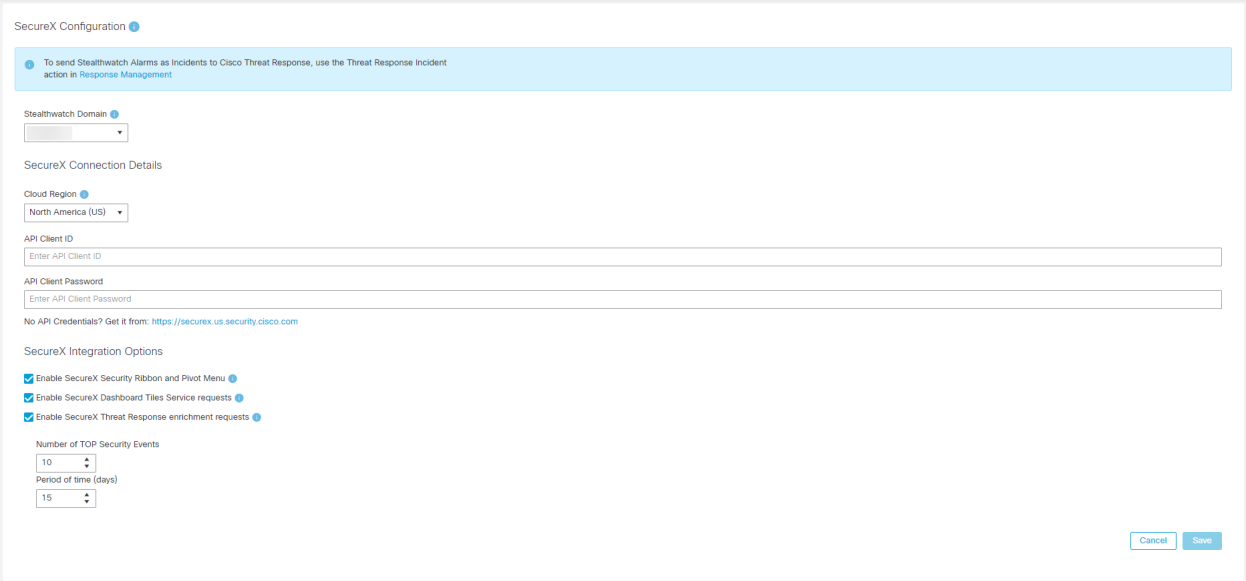
8. プライマリ管理者または設定管理者として SMC にログインします。
9. [ナビゲーション(Navigation)] メニューから ⚙ ([グローバル設定(Global Settings)]) アイコンをクリックし、[SecureX に設定(SecureX Configuration)] を選択します。



10. [SecureX 設定（SecureX Configuration）] セクションで、[新しい設定を追加（Add New Configuration）] をクリックします。



11. 開いているフォームで、API クライアントの作成に使用した地域クラウドを選択し、ステップ 6 のクライアント ID とクライアントパスワードを貼り付けます。
12. 有効にする統合オプションを選択し、[保存（Save）] をクリックします。



13. システムは API クレデンシャルを検証して保存します。

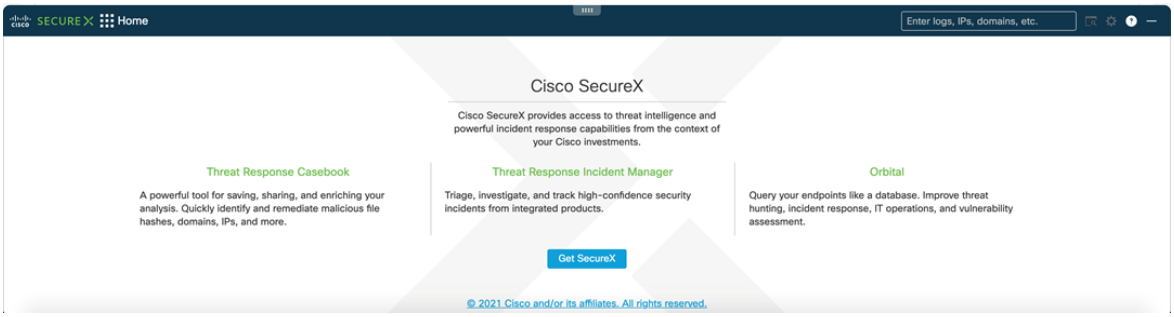
SecureX のリボンとピボットメニューの認定

SecureX の設定が完了したら、SMC の任意のページのリボン、または [SecureX の設定（SecureX Configuration）] ページから、SecureX のリボンと [ピボット（Pivot）] メニューを承認できます。

[SecureX の設定（SecureX Configuration）] ページの SecureX リボンの認証ウィジェットには、リボンの現在の承認ステータスが表示され、リボンを承認したり、承認を解除したりできます。

SecureX のリボンからの承認

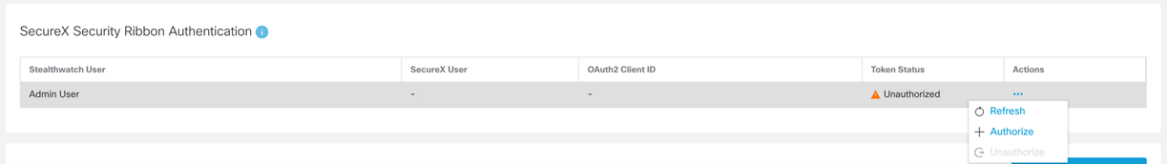
1. SMC のページの下部にある SecureX リボンを展開します。



2. [SecureX の取得（Get SecureX）] をクリックします。SecureX のログインページにリダイレクトされます。
3. クレデンシャルを使用して SecureX にログインします。
4. 指定した範囲で SecureX にアクセスするには、SMC SecureX のリボンクライアントを承認するように求められます。
5. アクセス権を付与します。リボンが開いた状態で SMC ページにリダイレクトされ、SMC でリボンが使用できるようになります。

[SecureX の設定（SecureX Configuration）] ページからの許可

1. SMC にログインします。
2. ⚙（[グローバル設定（Global Settings）]）アイコン をクリックし、[SecureX の設定（SecureX Configuration）] をクリックします。
3. [SecureX セキュリティリボンの認証（SecureX Security Ribbon Authentication）] ウィジェットの [アクション（Actions）] メニューを開き、[許可（Authorize）] をクリックします。SecureX のログインページにリダイレクトされます。



4. クレデンシャルを使用して SecureX にログインします。
5. 指定した範囲で SecureX にアクセスするには、SMC SecureX のリボンクライアントを承認するように求められます。
6. アクセス権を付与します。リボンが開いた状態で SMC ページにリダイレクトされ、SMC でリボンが使用できるようになります。

別の SecureX アカウントで SecureX のリボンを使用する必要がある場合は、現在のユーザーの承認を解除してから新しいユーザーで再度承認する必要があります。

現在の SecureX リボンの承認解除

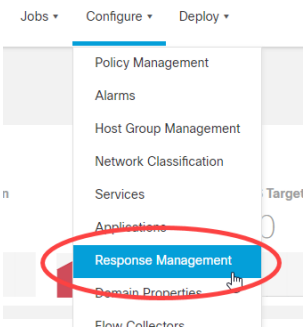
1. [SecureX の設定（SecureX Configuration）] ページで、[SecureX セキュリティリボンの認証（SecureX Security Ribbon Authentication）] ウィジェットにある [アクション（Actions）] メニューを開き、[承認解除（Unauthorize）] をクリックします。
2. 上記の手順に従って、別のユーザーで認証します。

Threat Response インシデントアクションの設定

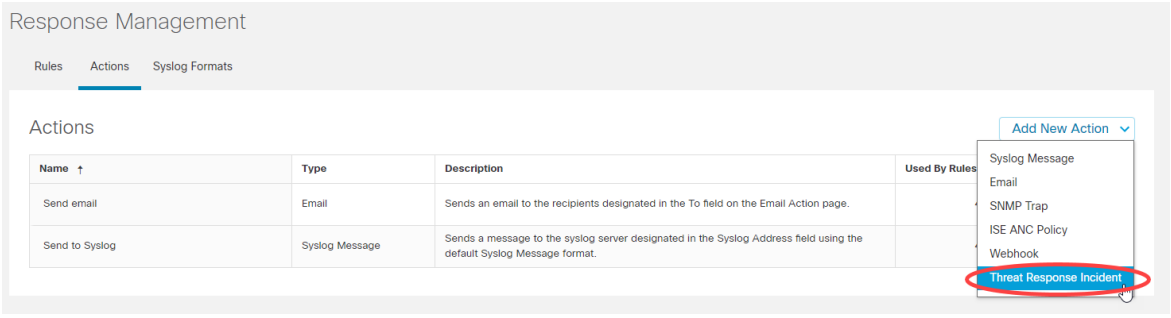
> 以前のバージョンの Stealthwatch で Cisco Threat Response に Stealthwatch のアラームを送信するように設定した場合は、Threat Response のインシデントアクションが自動的に作成されます。

対応管理で Threat Response のインシデントアクションを設定するには、次の手順を実行します。

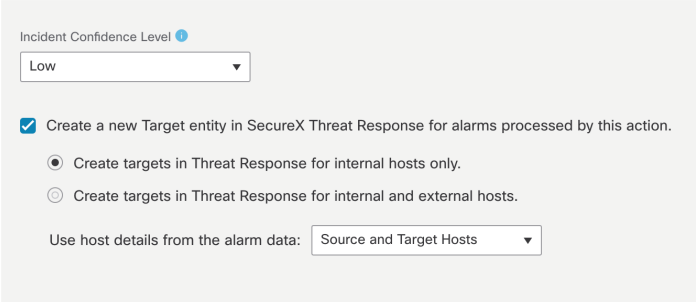
1. StealthWatch Management Console にログインします。
2. [設定（Configure）] > [応答の管理（Response Management）] をクリックします。



3. [アクション（Actions）] タブをクリックし、[新しいアクションの追加（Add New Action）] > [Threat Response インシデント（Threat Response Incident）] をクリックします。



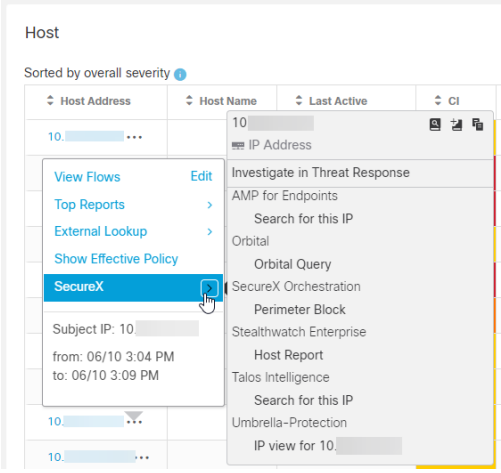
4. フォームに入力し、[保存（Save）] をクリックします。



アクションのオプションの詳細については、「Cisco Threat Response への Stealthwatch アラームの送信について」と「*対応管理の設定*」ヘルプトピックを参照してください。

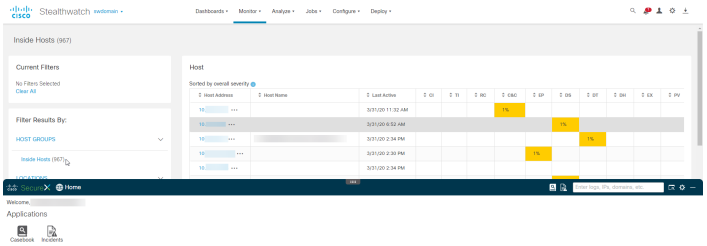
検証

1. SMC で SecureX ピボットメニューとセキュリティリボンが使用可能であることを確認します。
   - SecureX ピボットメニューの場合は次の手順を実行します。
     - 該当する IP アドレスを含んでいる SMC の任意のページを開きます。
     - 該当する IP アドレスの横にある ••• ([省略記号(Ellipsis)])アイコン をクリックします。
     - 表示されるポップアップメニューで、[SecureX] の横にある矢印をクリックします。第 2 のポップアップメニューがメニューコンテンツと共に表示されます。



   - SecureX のリボンの場合は次の手順を実行します。
     - SMC の任意のページに移動します。ページの下部にある 

([SecureX のリボン(SecureX ribbon)])アイコンをクリックしてウィジェットを展開します。



2. SecureX で Stealthwatch アラームを確認します。
   a. Stealthwatch がクリティカルまたは重大なセキュリティアラームを検出するか、テストセキュリティアラームが生成されるまで待ちます。
   b. 地域の SecureX クラウドにログインします。
   c. SecureX のリボンのインシデント アプリケーション、または Cisco Threat Response の Incident Manager まで移動します。
   d. アラームはリストに記載されている必要があります。

Cisco Cloud での SMC の登録

Cisco Security Services Exchange（SSE）クラウドは、一元管理の SMC で使用できます。SSE クラウドで SMC を登録すると、SecureX により、SMC からのセキュリティイベントなどのエンリッチメントデータを調査ワークフローに含めたり、SecureX ダッシュボードの Stealthwatch タイルを取得したりできます。

詳細については、「SecureX の Stealthwatch エンリッチメントデータについて」および「SecureX ダッシュボードの Stealthwatch タイルについて」のセクションを参照してください。

- SSE はデフォルトで有効になっています。
- 自動登録を使用する場合は、SSE アカウントとスマート ライセンス アカウントをリンクする必要があります。

デフォルトの SMC アイデンティティ証明書で提供されるものとは異なるカスタム SMC アイデンティティ証明書を使用している場合は、SMC で追加の設定手順が必要になることがあるため、テクニカルサポートにお問い合わせください。

自動登録手順

次の条件が満たされると、SMC は SSE クラウドに自動的に登録されます。

- SSE オプションは、外部サービスで SMC に対して有効になります。
- SMC が SSE にまだ登録されていません。
- お使いの製品はスマート ソフトウェア ライセンスに登録されています。手順については、『Smart Software Licensing』ガイドを参照してください。

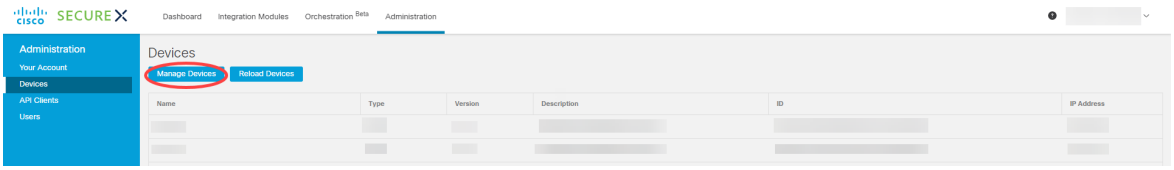
SSE を有効または無効にするには、次の手順を実行します。

1. StealthWatch Management Console にログインします。
2. ⚙（[グローバル設定（Global Settings）]）アイコン をクリックし、[一元管理（Central Management）] をクリックします。
3. SMC の [アクション（Actions）] 列の下にある ••• （[省略記号（Ellipsis）]）アイコン をクリックし、[アプライアンス設定の編集（Edit Appliance Configuration）] をクリックします。
4. [General（全般）] をクリックします。
5. [外部サービス（External Services）] で、[Cisco Security Services Exchange] チェックボックスをオンまたはオフにして、自動登録を有効または無効にします。
6. [設定の適用（Apply Settings）] をクリックします。

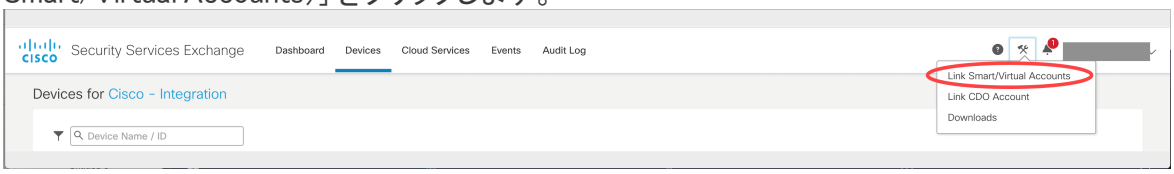
アカウントのリンク

スマート ライセンス アカウントを Cisco Security Services Exchange アカウントにリンクするには、次の手順を実行します。

1. SecureX 地域クラウドに移動し、エンドポイント向け AMP、Cisco Threat Grid、またはシスコ セキュリティアカウントのログイン情報を使用してログインします。
2. [Administration] タブをクリックします。[デバイス（Devices）] > [デバイスの管理（Manage Devices）] を選択して Security Services Exchange に移動できるようにします。



3. ([ツール(Tools)] アイコンをクリックし、[スマート/仮想アカウントのリンク(Link Smart/Virtual Accounts)] をクリックします。

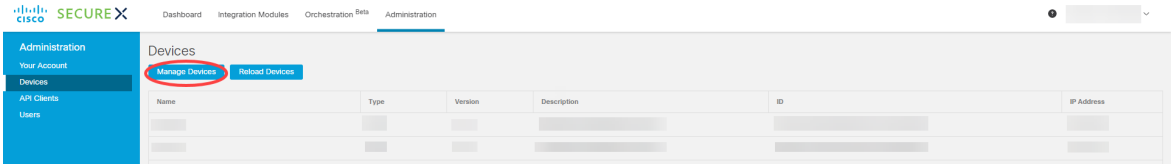


4. アカウントのリストを含むポップアップからスマートアカウントを選択します。

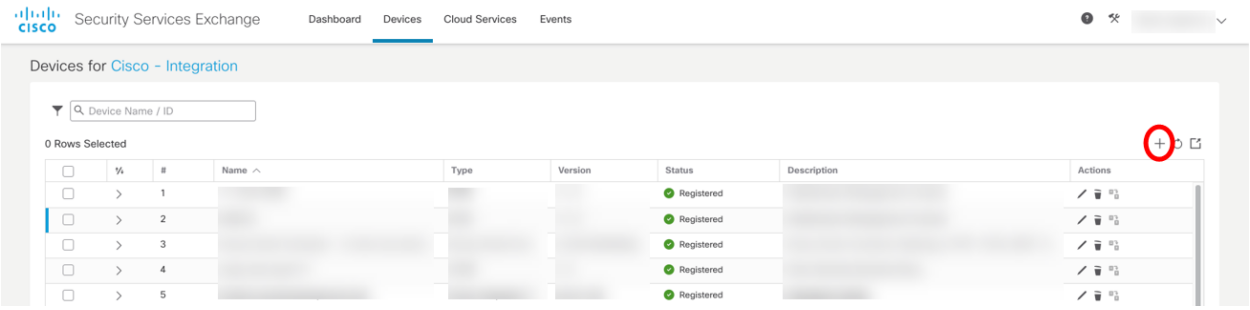
手動登録手順

Cisco セキュリティで保護された Exchange クラウドに SMC を手動で登録するには、次の手順を実行します。

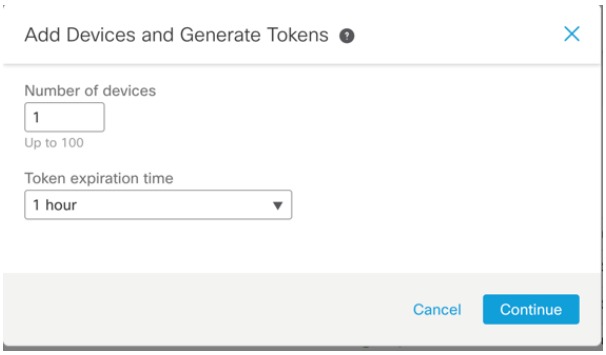
1. SecureX 地域クラウドに移動し、エンドポイント向け AMP、Cisco Threat Grid、またはシスコ セキュリティアカウントのログイン情報を使用してログインします。
2. [Administration] タブをクリックします。[デバイス(Devices)] > [デバイスの管理(Manage Devices)] を選択して Security Services Exchange に移動できるようにします。



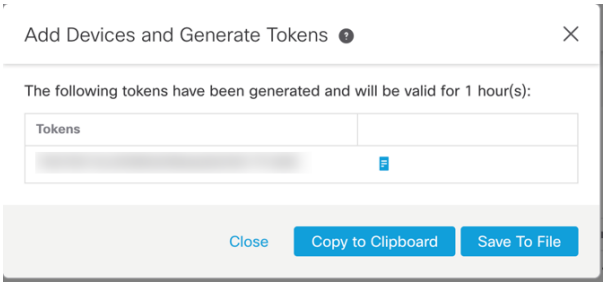
3. [デバイス(Devices)] タブをクリックし、ページの右側にある ＋ ([デバイスの追加とトークンの生成(Add Devices and Generate Tokens)]) をクリックします。



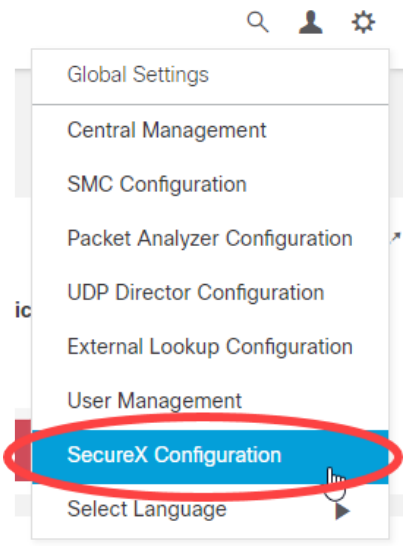
4. 開いているダイアログで、[続行(Continue)] をクリックし、デバイスのトークンをシステムに生成させます。



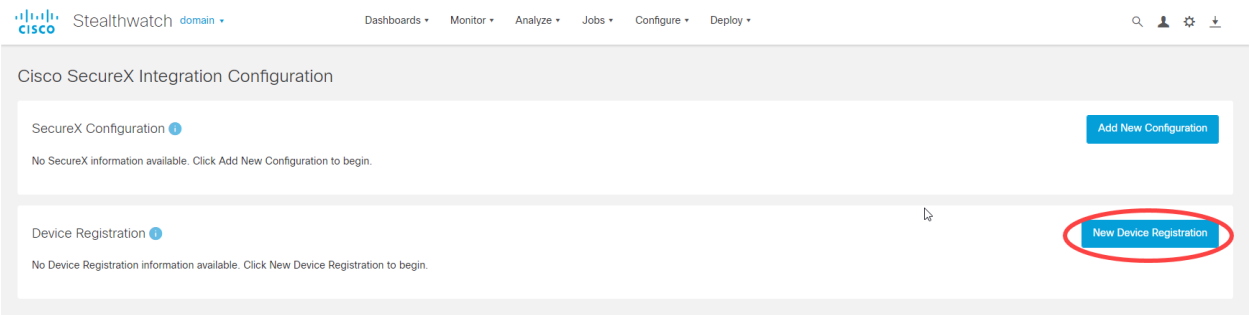
5. 生成されたトークンをメモリバッファにコピーするか、生成されたトークンをファイルに保存します。



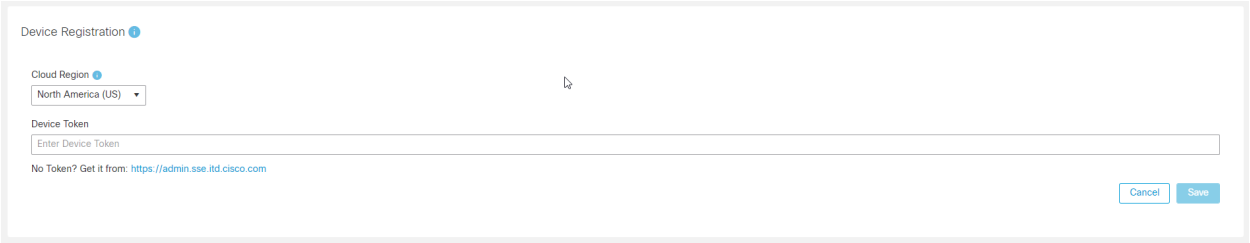
6. プライマリ管理者または設定管理者として SMC にログインします。
7. [ナビゲーション(Navigation)] メニューから ⚙ ([グローバル設定(Global Settings)]) アイコンをクリックし、[SecureX に設定(SecureX Configuration)] を選択します。



8. [デバイス登録(Device Registration)] セクションで、[新しいデバイスの登録(New Device Registration)] をクリックします。



9. 開いているダイアログで、SecureX 地域クラウドと一致するクラウド地域を選択し、ステップ 5 で生成して保存したセキュリティサービス Exchange トークンを挿入します。[保存(Save)] をクリックします。



10. デバイスは Cisco Security Services Exchange に登録され、ステータスは [登録済み(Enrolled)] として表示されます。
11. Cisco Security Services Exchange ポータルでデバイスのステータスを確認します。デバイスのステータスは、[登録済み(Enrolled)] として表示される必要があります。

SecureX での Stealthwatch 統合モジュールの設定

SecureX が Stealthwatch からエンリッチメントデータとダッシュボードタイルを取得するには、統合モジュールを設定する必要があります。

前提条件

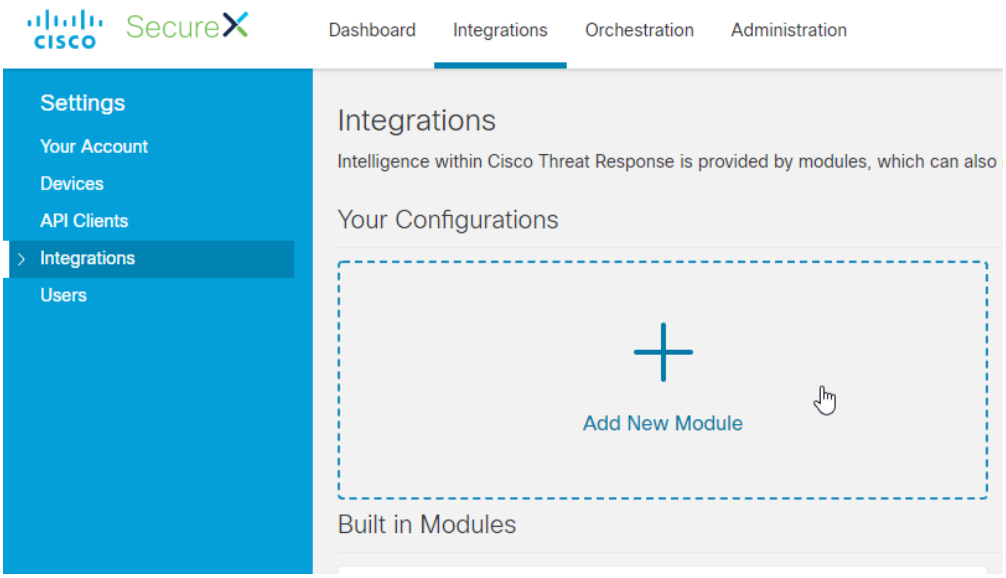
- SMC が Cisco Security Services Exchange クラウドに登録されています。
- Cisco Threat Response は、Cisco Security Services Exchange portal クラウドサービスで有効になっています。

  詳細については、「Cisco Cloud の SMC の登録」のセクションを参照してください。

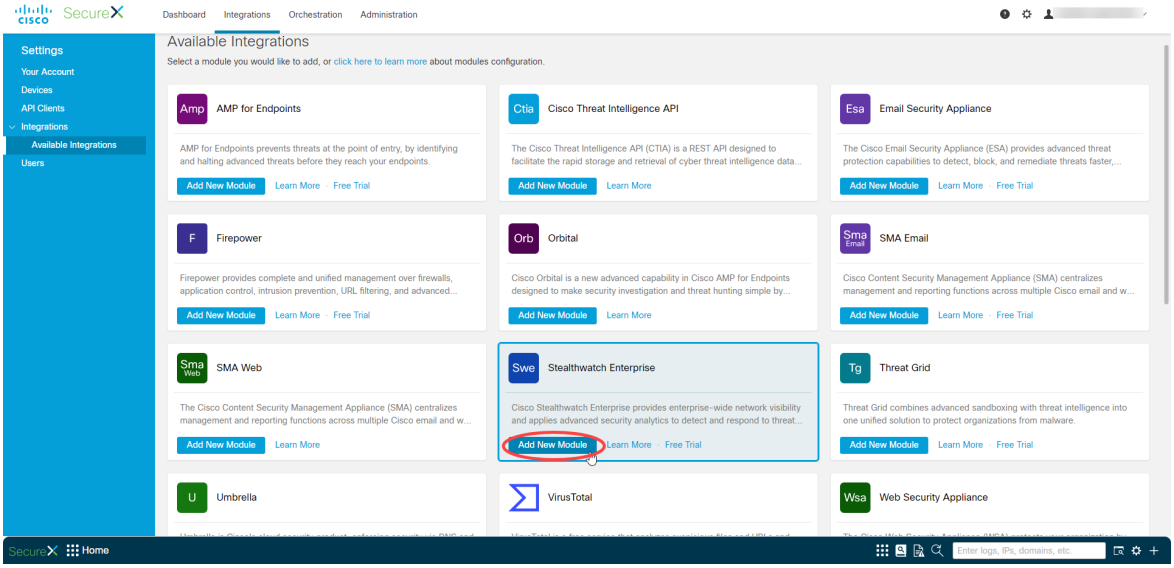
手順

SecureX で Stealthwatch モジュールを設定するには、次の手順を実行します。

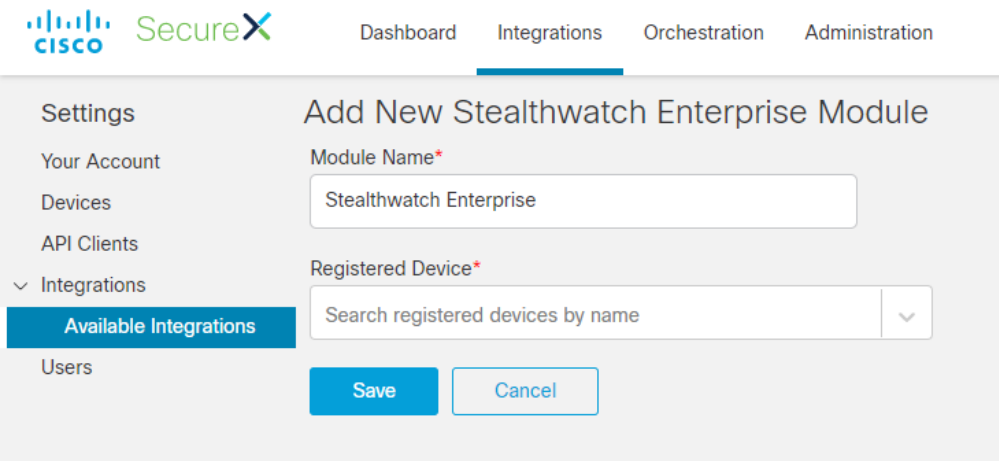
1. SecureX 地域クラウドに移動し、エンドポイント向け AMP、Cisco Threat Grid、またはシスコ セキュリティアカウントのログイン情報を使用してログインします。
2. [統合(Integrations)] タブに移動し、[設定(Settings)] メニューの [統合(Integrations)] をクリックします。
3. [新しいモジュールを追加(Add New Module)] をクリックします。[使用可能な統合(Available Integrations)] ページが開きます。



4. Stealthwatch Enterprise モジュールを見つけて、[新しいモジュールを追加（Add New Module）] をクリックします。



5. 開いているダイアログで、次のようにします。
   a. モジュールに名前を付けます。
   b. [登録済みデバイス（Registered Device）] ドロップダウンから、SMC を見つけます。
   c. [保存（Save）] をクリックします。



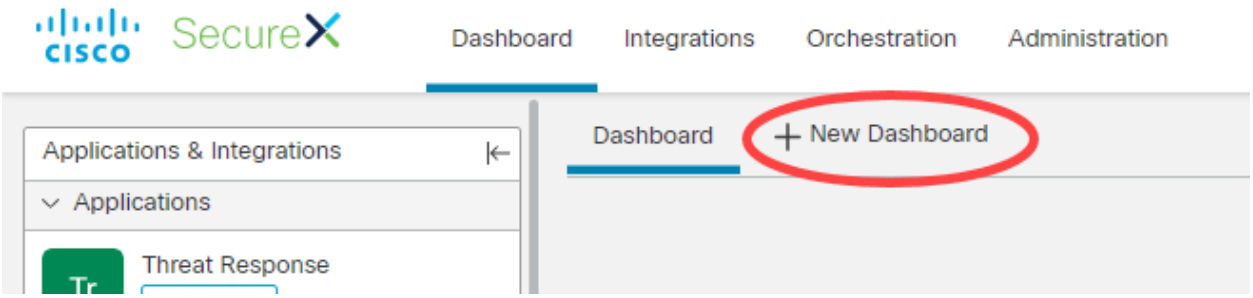
6. Threat Response が SMC からエンリッチメントデータを取得できることを確認します。手順は次のとおりです。
    a. SMC セキュリティダッシュボードを確認し、セキュリティイベントを生成する IP に注目してください。
    b. Threat Response の調査検索パネルにこの IP を入力します。
    c. グラフには、要求されたホストとのセキュリティイベントに関連する他のホストが表示されます。
    d. Sightings は要求されたホストに関連付けられているセキュリティイベントを表します。

Stealthwatch タイルを使用した SecureX ダッシュボードの設定

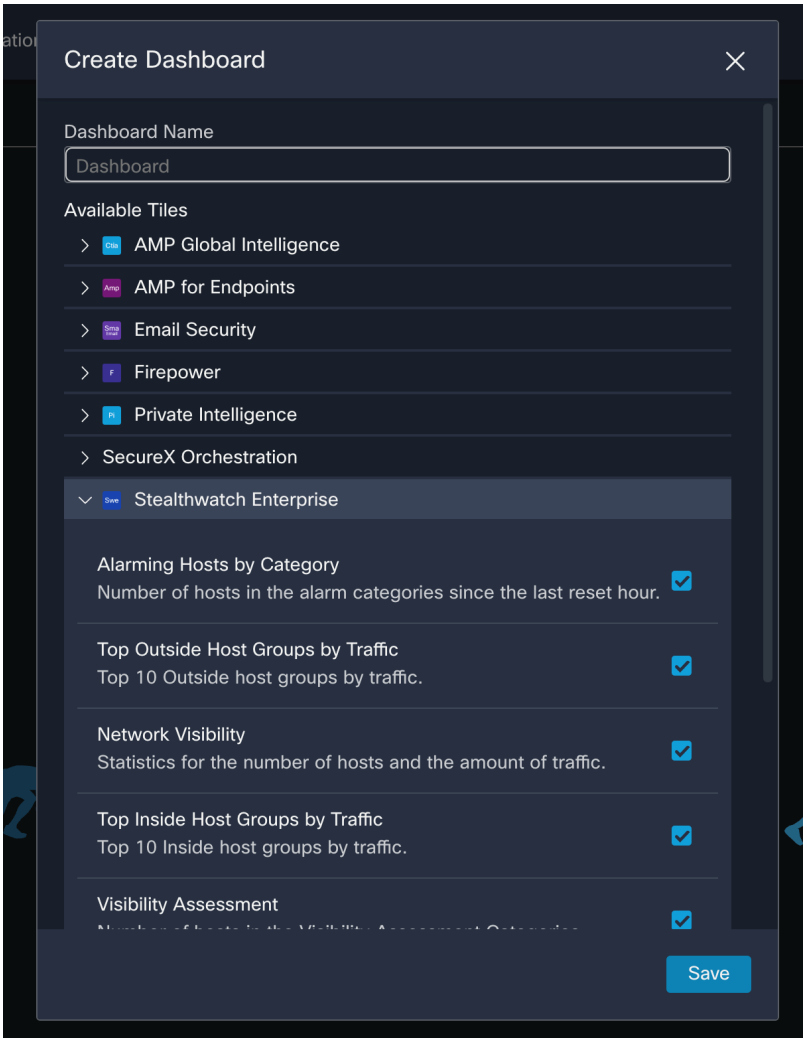
> Stealthwatch タイルを SecureX ダッシュボードに追加する前に、Stealthwatch Enterprise 統合モジュールを設定する必要があります。

Stealthwatch タイルをダッシュボードに追加するには、次の手順を実行します。

1. ブラウザウィンドウで、自身の地域の SecureX ポータルに移動します。
    - 北米：https://securex.us.security.cisco.com
    - ヨーロッパ：https://securex.eu.security.cisco.com
    - アジア（APJC）：https://securex.apjc.security.cisco.com
2. シスコ セキュリティまたは Cisco Threat Grid アカウントを使用してログインします。
3. ダッシュボードのメニューバーで、[新規ダッシュボード（New Dashboard）] をクリックして、[ダッシュボードの作成（Create Dashboard）] フォームを開きます。



4. 開いたダイアログで、[ダッシュボード名（Dashboard Name）] に入力し、使用可能なタイルの下にある Stealthwatch Enterprise モジュールを見つけます。
5. Stealthwatch Enterprise を展開し、ダッシュボードに追加するタイルを選択します。



6. [保存（Save）] をクリックします。
7. 選択したタイルが、関連するデータとともにダッシュボードレイアウトに表示されます。

既知の問題と制限事項

- フェールオーバーは、v7.3 の SecureX 統合ではサポートされていません。統合を機能させるには、セカンダリ SMC で設定を繰り返す必要があります。
- Backup and Restore は、Cisco Security Services Exchange Cloud ポータルのデバイス登録ではサポートされていません。SMC の SecureX 設定の [デバイス登録(Device Registration)] パネルには、クラウドでのデバイス登録の実際のステータスが表示されます。したがって、デバイス登録のバックアップから設定を復元することはできません。バックアップ後に削除した場合は、復元後に登録を再実行する必要があります。

著作権情報