

Cisco SecureXとCisco Umbrellaの統合

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[モジュールの作成](#)

[APIの調査](#)

[適用API](#)

[レポートAPI](#)

[モジュールの保存](#)

[SecureXダッシュボードの作成](#)

[確認](#)

[調査](#)

[適用](#)

[レポート](#)

[ビデオ](#)

[関連情報](#)

はじめに

このドキュメントでは、3つの使用可能なAPIを使用したSecureXとのUmbrella統合を設定および確認するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Umbrella
- シスコセキュアX
- シスコの脅威対策

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- DNSアドバンテージライセンスを持つ包括アカウント
- セキュアX

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

この統合をすべての機能で完全に設定するには、次の3つのAPIにアクセスする必要があります

- レポートAPI (すべてのライセンスに含まれる)
- 適用API
- APIの調査

Umbrella統合を設定するには、まずUmbrellaインスタンスから情報を収集し、次に「Add New Umbrella Module」フォームに入力する必要があります。

設定

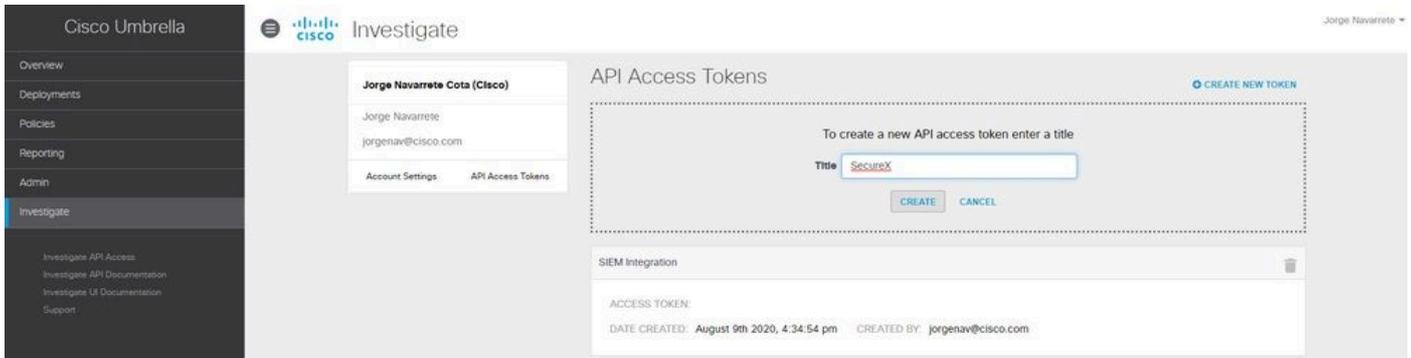
モジュールの作成

1. Secure Xアカウントにログインします。まだアカウントをお持ちでない場合は、[Cisco Secure Sign-On](#)を使用してアカウントを作成できます。
2. Integrations > Add New Moduleの順に移動します。Available IntegrationsページでUmbrellaオプションまでスクロールダウンし、Add New Moduleをクリックします。

次の手順を使用して、Umbrellaアカウントから必要な情報を収集し、「Add New Umbrella Module」フォームで送信します。

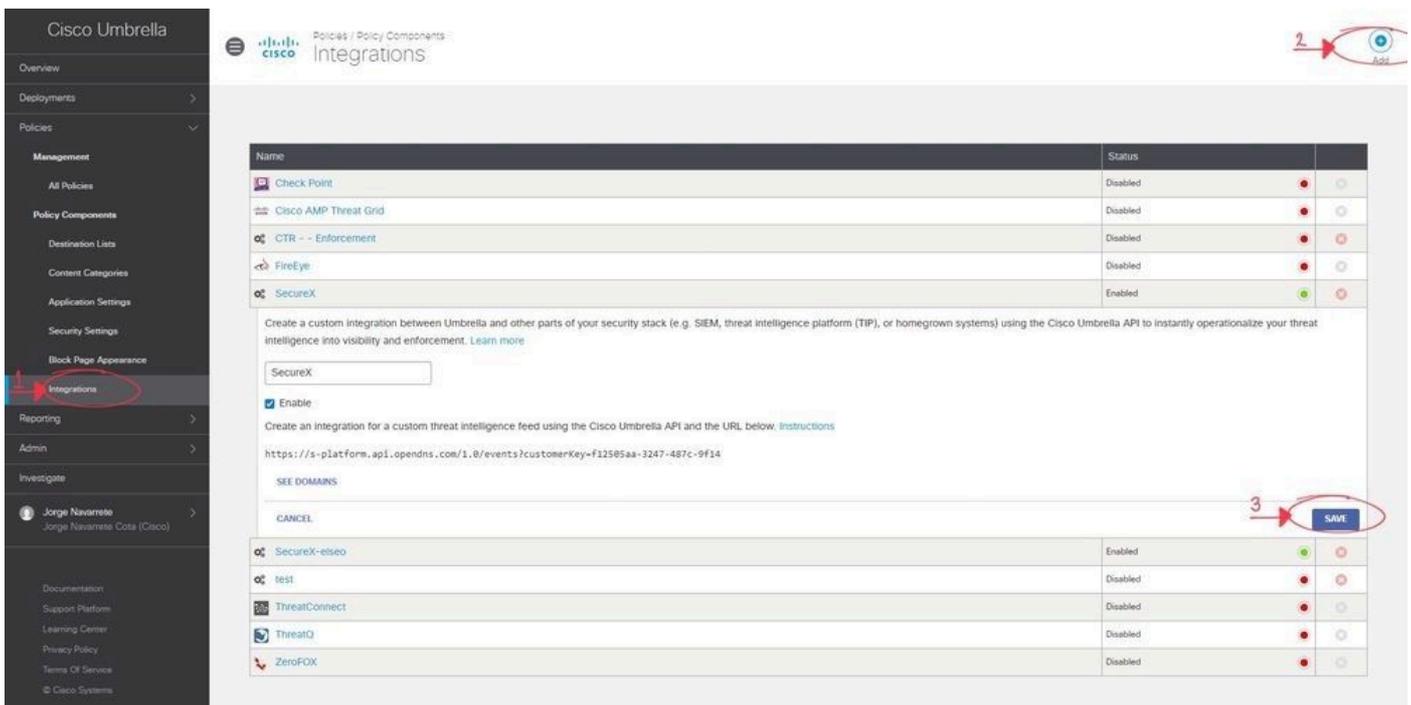
APIの調査

1. Umbrellaで、Investigate > Investigate API Accessに移動し、Create New Tokenをクリックしてトークンのタイトルを入力し、再度Create New Tokenをクリックします。
2. Access Tokenの値をAdd New Umbrella ModuleフォームのAPI Tokenフィールドにコピーします。



適用API

1. Umbrellaで、Policies > Policy Components > Integrationsの順に移動し、Addをクリックして名前を入力し、Createをクリックします。
2. 新しく作成した統合名のリンクをクリックし、Enablecheckボックスにチェックマークを入れて保存します。
3. 統合名をクリックして、統合URLを表示します。統合URLを、Add New Umbrella ModuleフォームのCustom Umbrella Integration URLフィールドにコピーします。



 注:Umbrella Enforcement APIを統合するには、Umbrellaコンソールの管理者ではなく、Umbrellaスタンドアロン組織または子組織の管理者である必要があります。

レポートAPI

1. Umbrellaで、Admin > API Keysの順に移動し、Createをクリックします。
2. What should this API do?の下で、Umbrella Reporting オプションボタンをクリックし、次にCreateをクリックします。

3. 次の値をAdd New Umbrella ModuleフォームのReportingフィールドにコピーします。

- APIキー (自分のキー)
- APIシークレット (自分のシークレット)
- 組織ID : ブラウザURLから、 /o/と /#/の間の数字のセット
- Request Timeframe (日数) : 最新のDNS要求の洞察を強化するための期間 (日数) を入力します

Cisco Umbrella Admin API Keys

Cisco Umbrella generates authentication keys for several types of integrations. These include software, Umbrella-enabled devices, and Cisco network hardware. Click Create, then specify the type of integration key you need.

What should this API do?
Choose the API that you would like to use.

- Umbrella Network Devices
Integrate Umbrella-enabled hardware with your organization's networks. This also enables you to create, update, list, and delete identities in Umbrella.
- Legacy Network Devices
A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.
- Umbrella Reporting
Enables API access to query for Security Events and traffic to specific Destinations.
- Umbrella Management
Manage organizations, networks, roaming clients and more using the Umbrella Management API.

CANCEL CREATE

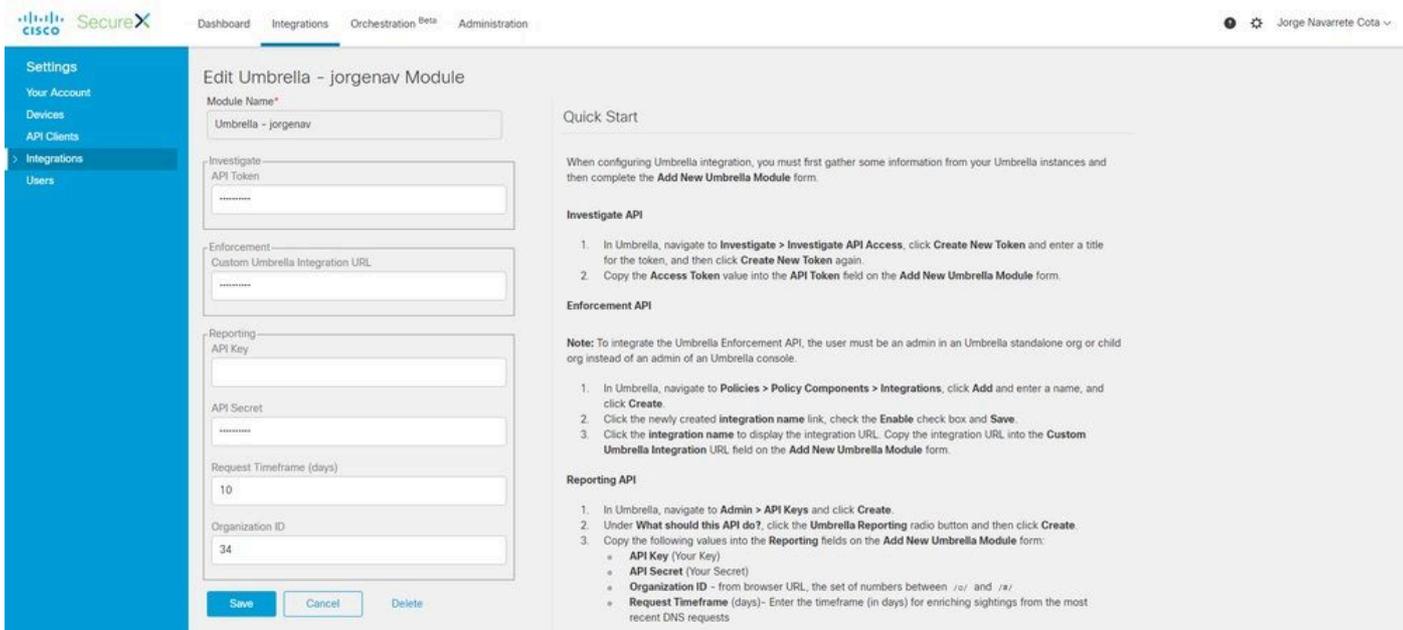
Documentation
Read here to get authentication set up for your first endpoint queries, explore what you can do and search for any answers you need.

Our Legacy APIs
Some of our older legacy APIs use a different authentication mechanism than what you are setting up here and have unique functions.

Investigate
Looking for information about the Investigate API? That API is managed separately.

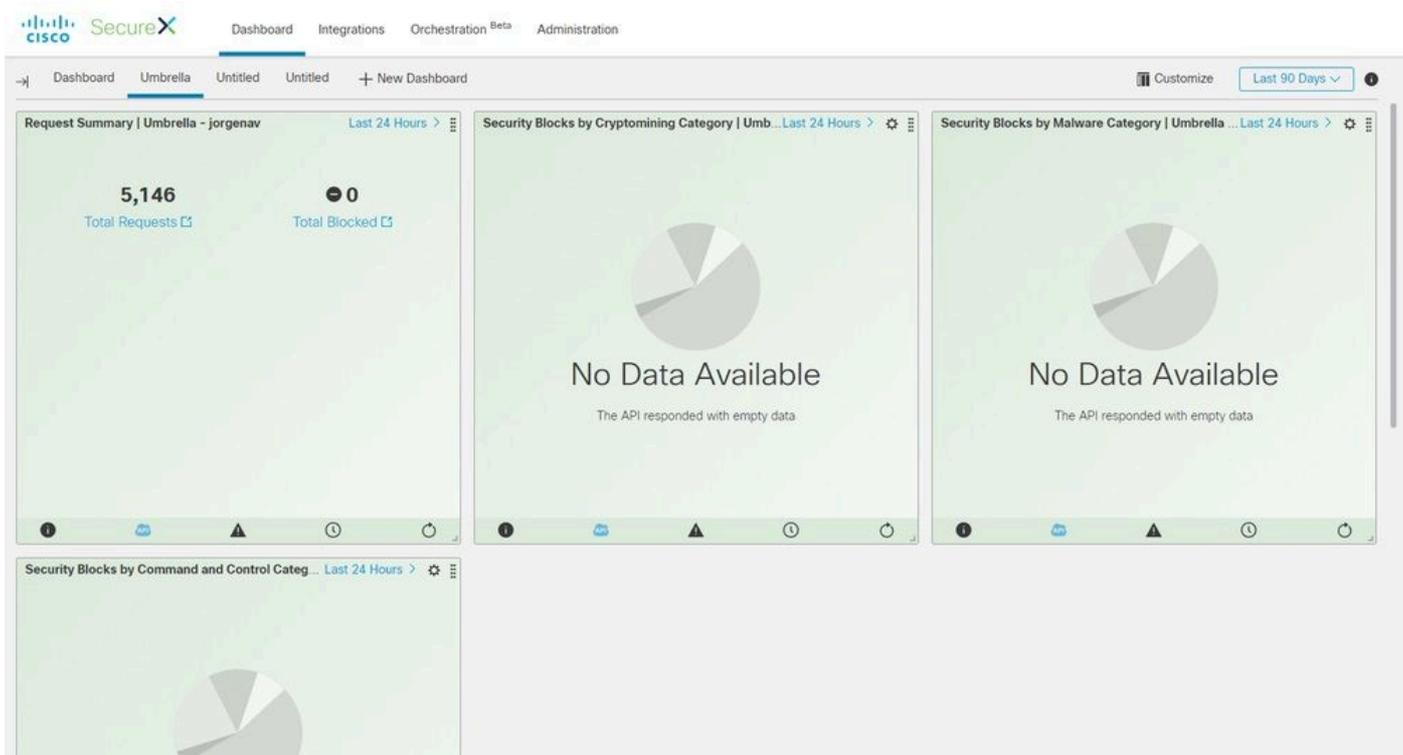
モジュールの保存

1. UmbrellaモジュールのAPI情報を入力し、Saveをクリックします。



SecureXダッシュボードの作成

1. モジュールを追加したら、Secure Xに移動して新しいダッシュボードを作成できます。
2. 使用可能なダッシュボードで、Umbrellaモジュールを選択し、表示するカテゴリを追加します。
3. Saveをクリックし、APIを介して情報が入力されていることを確認します。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

調査

Investigate APIを使用すると、CTR調査にフィードを追加して、ドメインの性質を確認し、他のモジュールで調査を強化できます。

1. この統合を確認するために、[Cisco Threat Response](#)で新しい調査を行います。Umbrellaが提供する評価は、cisco.comなどの既知のドメインを検索することで確認できます。
2. リレーショングラフのドメインの下をクリックすると、そこからUmbrellaの調査ダッシュボードにピボットすることもできます。

The screenshot shows the Cisco Umbrella Investigate interface. At the top, there are navigation tabs for Threat Response, Investigate, Snapshots, Incidents, and Intelligence. Below the navigation, there are several status indicators: 0 Targets, 1 Observable, 0 Indicators, 1 Domain, 0 File Hashes, 0 IP Addresses, 0 URLs, and 3 Modules. The main area is divided into several sections:

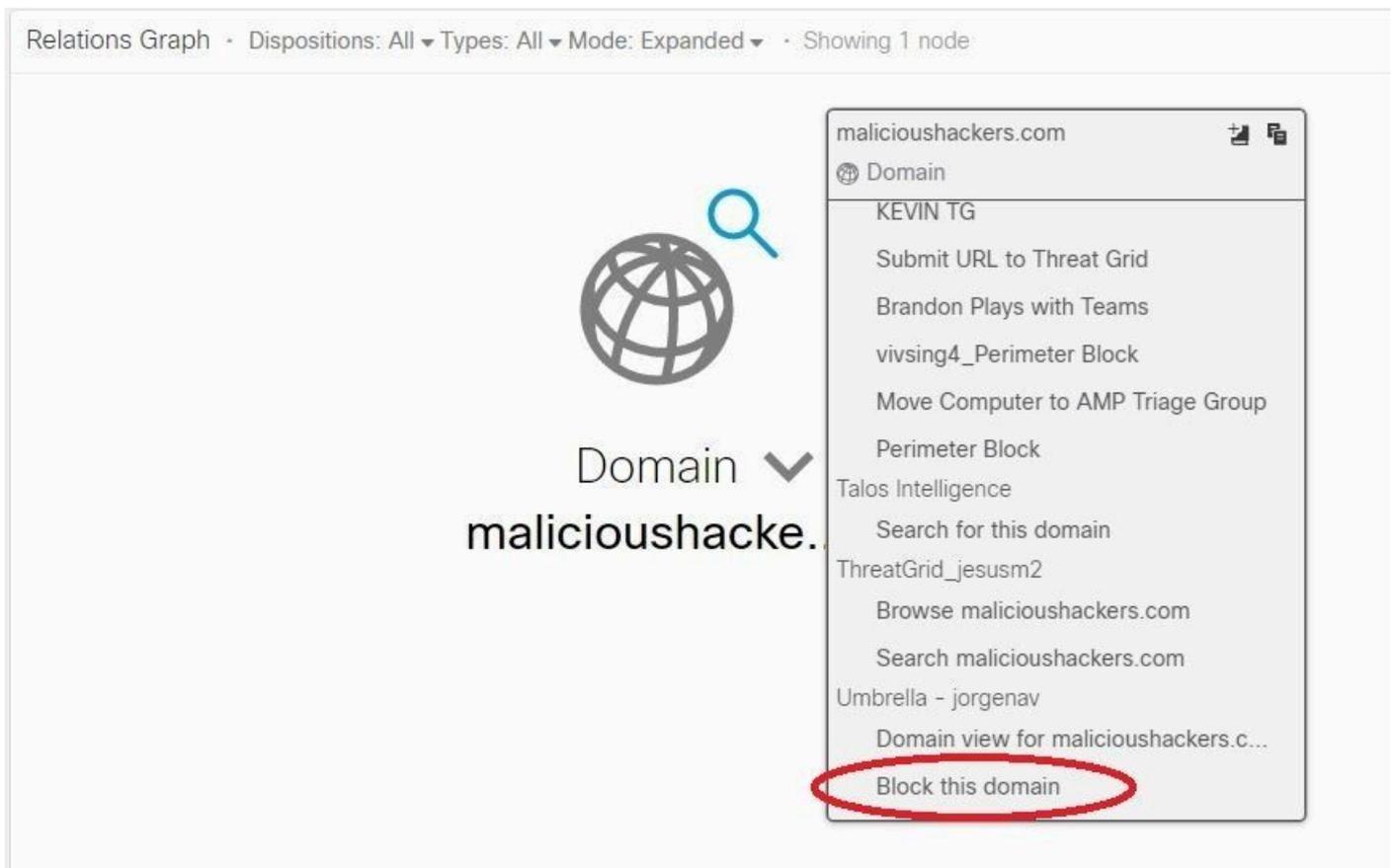
- Investigation:** Shows '1 of 1 enrichments complete' and the domain 'cisco.com'. There are buttons for 'Investigate', 'Clear', and 'Reset', and a search prompt 'What can I search for?'.
- Relations Graph:** A graph showing 'Clean Domain cisco.com' at the center, connected to '3 IPs', '2 SHA-256s', and a 'Clean Domain' icon.
- Observables:** A section for 'cisco.com' showing 'Clean Domain' and 'My Environment: Global'. It includes a chart with 0 sightings and a table of judgements.
- Judgements Table:** A table with columns: Module, Observable, Disposition, Reason, Source. It shows two entries for 'cisco.com' with a 'Clean' disposition.

Module	Observable	Disposition	Reason	Source
Umbrella - jorgenav	DOMAIN: cisco.com	Clean	Good Cisco Umbrella reputation status	Umbrella Investigate API
Talos Intelligence	DOMAIN: cisco.com	Clean	Good Talos Intelligence reputation score	Talos Intelligence

適用

Enforcement APIを使用すると、調査から直接ドメインをブロックまたはブロック解除できます。

1. APIが機能していることを確認するために、調査で確認されたドメインをブロックし、そのドメインをUmbrellaのポリシーブロックリストに追加できます。
2. ブロックリストにURLが追加されたことを確認するために、Policies > Policy Components > Integrationsの順に移動します。SecureX統合を選択し、[ドメインを表示]をクリックします。CTRから追加されたドメインがウィンドウに表示されます。



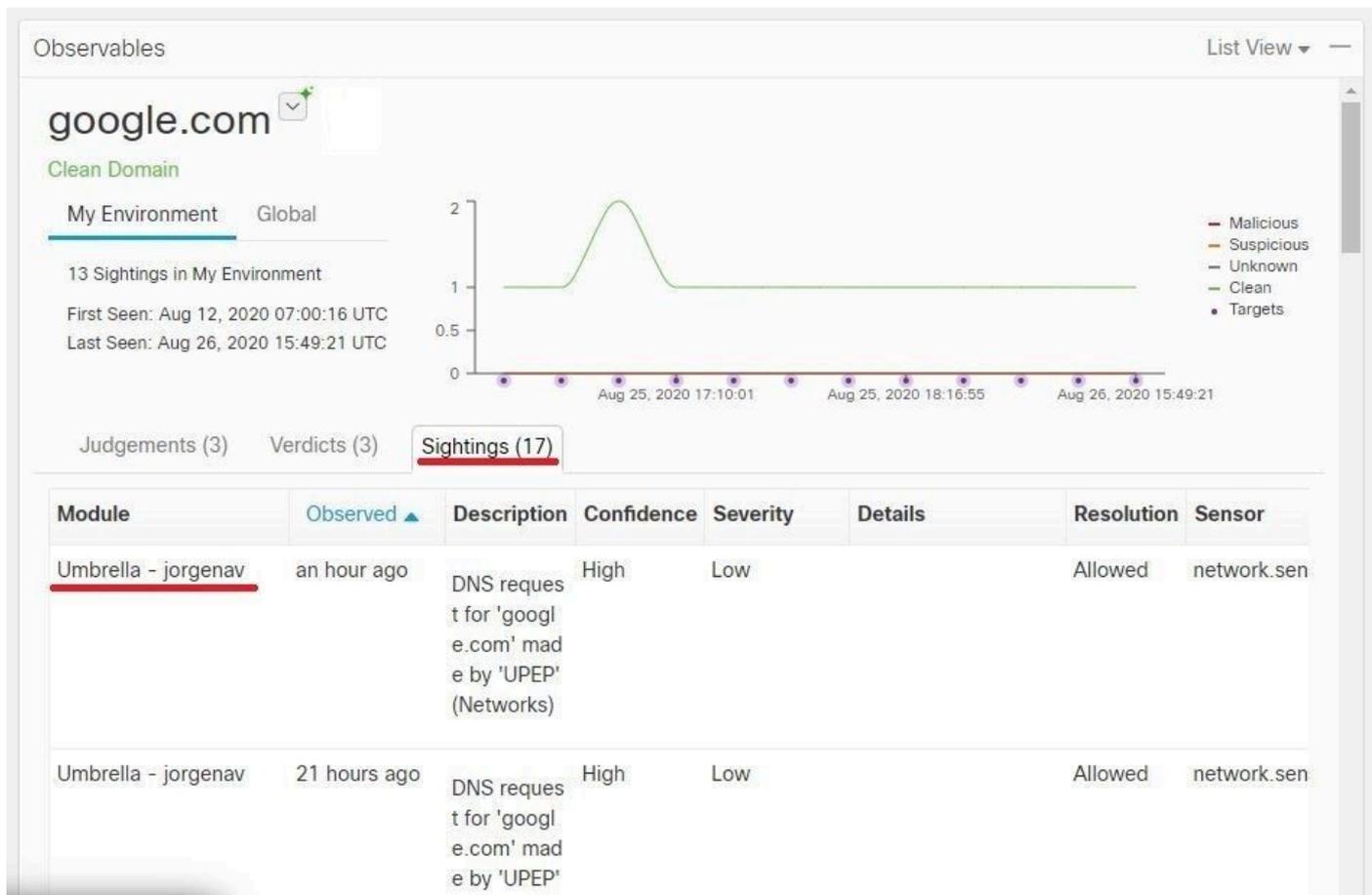
3. ドメインがブロックされていない場合は、Umbrellaダッシュボードでポリシー>ポリシーコンポーネント>セキュリティ設定に移動します。統合の下で、目的のリストを適用したことを確認します。

レポート

Reporting APIを使用すると、SecureX内のUmbrella展開の情報を表示できます。

CTRの環境で確認されているドメインを調査することで、統合を確認できます。

CTR Investigationでは、特定のドメインにアクセスしたコンピュータのリストがSightingsの下に表示されます。



ビデオ

このビデオでは、この記事に含まれる設定情報について説明します。

関連情報

- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。