

# Intégrer Cisco SecureX à Cisco Umbrella

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Créer un module](#)

[Étudier l'API](#)

[API d'application](#)

[API de rapport](#)

[Enregistrer le module](#)

[Créer un tableau de bord SecureX](#)

[Vérifier](#)

[Enquêter](#)

[Application](#)

[Rapports](#)

[Vidéo](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit le processus de configuration et de vérification de l'intégration d'Umbrella avec SecureX avec les 3 API disponibles.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Umbrella
- Cisco Secure X
- Réponse aux menaces Cisco

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Compte parapluie avec licence DNS Advantage
- Sécuriser X

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informations générales

Afin de configurer entièrement cette intégration avec toutes ses fonctionnalités, vous devez accéder à ces 3 API

- API de rapport (incluse dans toutes les licences)
- API d'application
- Étudier l'API

Afin de configurer l'intégration Umbrella, vous devez d'abord recueillir des informations à partir de vos instances Umbrella, puis remplir le formulaire Add New Umbrella Module.

## Configurer

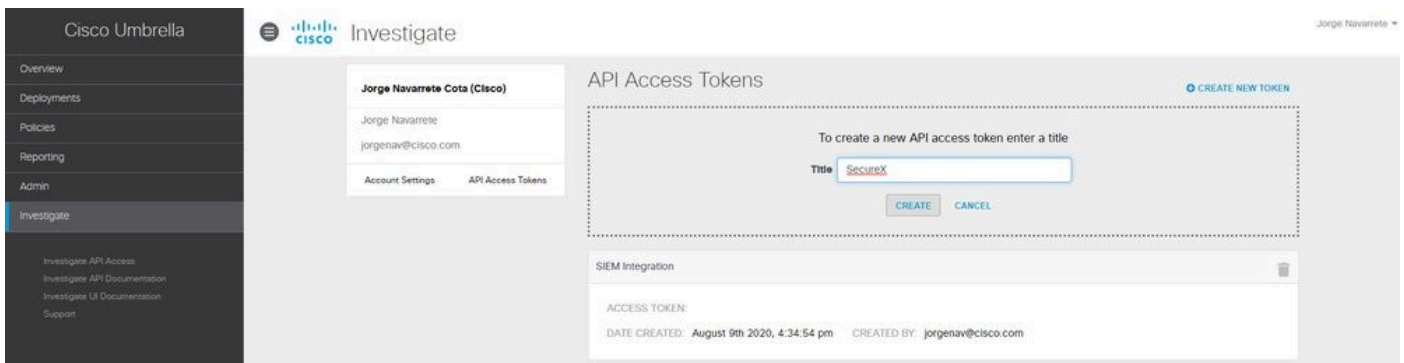
### Créer un module

1. Connectez-vous à votre compte Secure X. Si vous n'avez pas encore de compte, vous pouvez en créer un avec [Cisco Secure Sign-On](#).
2. Accédez à Integrations > Add New Module. Dans la page Available Integrations, faites défiler jusqu'à l'option Umbrella et cliquez sur Add New Module.

Suivez ces étapes pour recueillir les renseignements nécessaires à partir de votre compte parapluie et les soumettre dans le formulaire Ajouter un nouveau module parapluie.

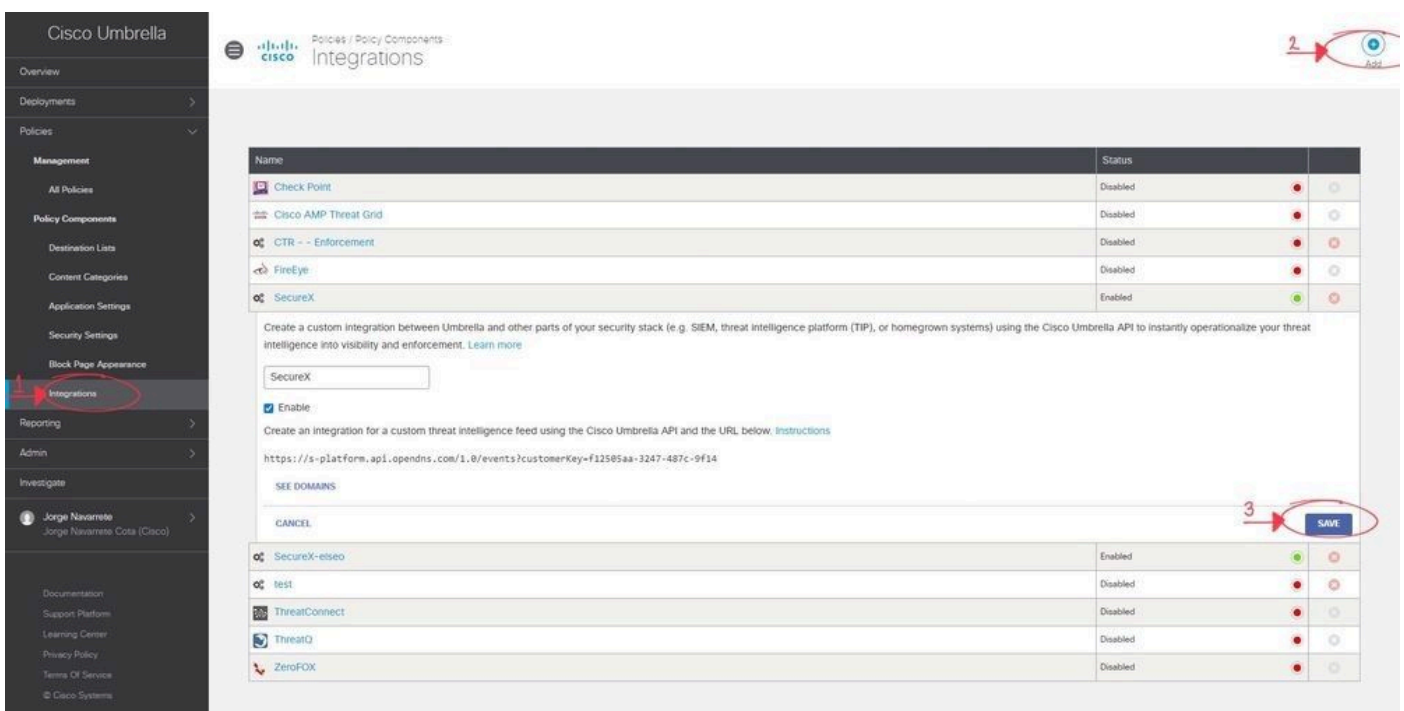
### Étudier l'API


1. Dans Umbrella, accédez à Investigate > Investigate API Access, cliquez sur Create New Token et entrez un titre pour le jeton, puis cliquez à nouveau sur Create New Token.
2. Copiez la valeur du jeton d'accès dans le champ du jeton d'API du formulaire Ajouter un nouveau module de parapluie.



## API d'application

1. Dans Umbrella, accédez à Politiques > Policy Components > Integrations, cliquez sur Add et entrez un nom, puis cliquez sur Create.
2. Cliquez sur le lien du nom de l'intégration nouvellement créé, cochez la case Activer et Enregistrer.
3. Cliquez sur le nom d'intégration pour afficher l'URL d'intégration. Copiez l'URL d'intégration dans le champ Custom Umbrella Integration URL du formulaire Add New Umbrella Module.



 Remarque : pour intégrer l'API Umbrella Enforcement, vous devez être un administrateur dans une organisation autonome Umbrella ou une organisation enfant au lieu d'un administrateur d'une console Umbrella.

## API de rapport

1. Dans Umbrella, accédez à Admin > API Keys et cliquez sur Create.
2. Sous What should this API do ?, cliquez sur la case d'option Umbrella Reporting, puis cliquez sur Create.

### 3. Copiez les valeurs suivantes dans les champs Reporting du formulaire Add New Umbrella Module :

- Clé API (votre clé)
- Secret API (votre secret)
- ID d'organisation - à partir de l'URL du navigateur, l'ensemble des nombres compris entre /o/et/#/
- Request Timeframe (days) : saisissez le délai (en jours) d'enrichissement des observations provenant des requêtes DNS les plus récentes

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.

## Enregistrer le module

1. Complétez les informations API dans votre module Umbrella, cliquez sur Save.

**Edit Umbrella - jorgenav Module**

Module Name\*  
Umbrella - jorgenav

Investigate  
API Token  
.....

Enforcement  
Custom Umbrella Integration URL  
.....

Reporting  
API Key  
.....

API Secret  
.....

Request Timeframe (days)  
10

Organization ID  
34

Save Cancel Delete

**Quick Start**

When configuring Umbrella integration, you must first gather some information from your Umbrella instances and then complete the **Add New Umbrella Module** form.

**Investigate API**

- In Umbrella, navigate to **Investigate > Investigate API Access**, click **Create New Token** and enter a title for the token, and then click **Create New Token** again.
- Copy the **Access Token** value into the **API Token** field on the **Add New Umbrella Module** form.

**Enforcement API**

**Note:** To integrate the Umbrella Enforcement API, the user must be an admin in an Umbrella standalone org or child org instead of an admin of an Umbrella console.

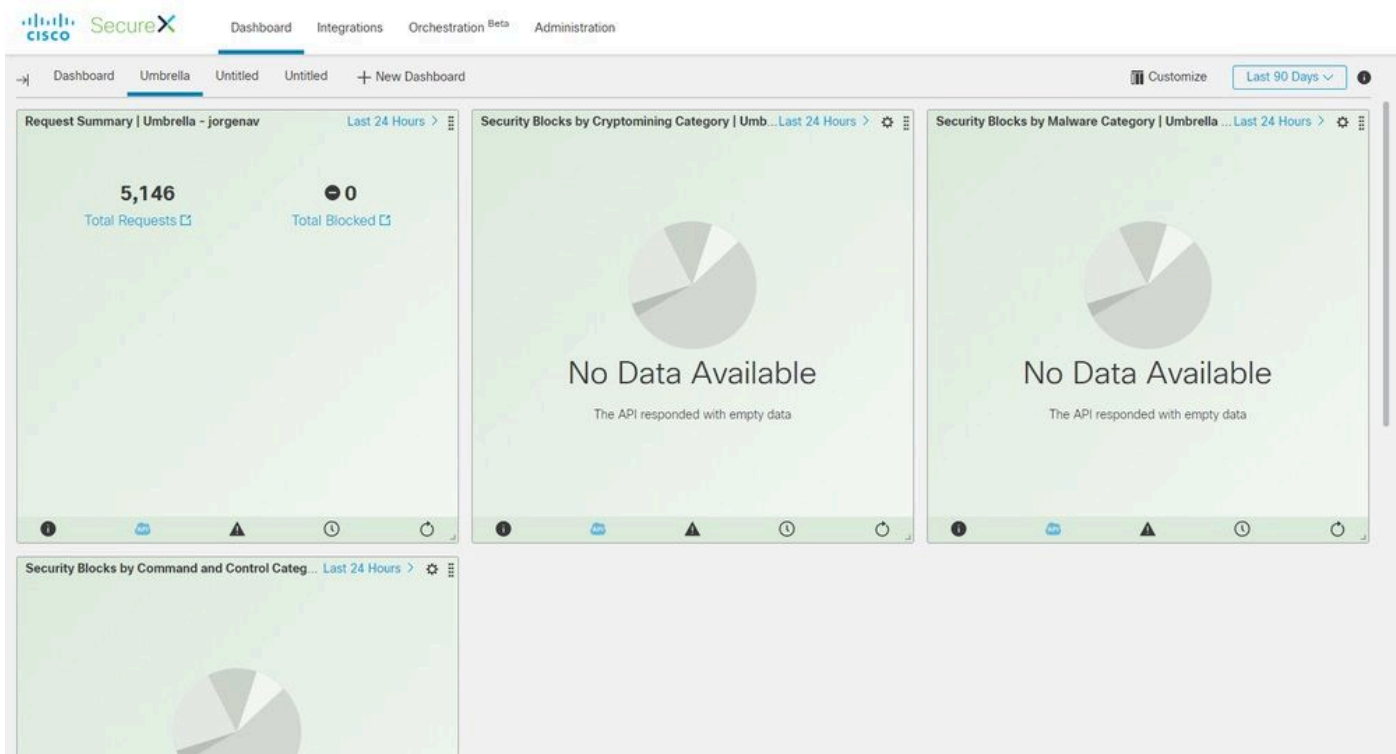
- In Umbrella, navigate to **Policies > Policy Components > Integrations**, click **Add** and enter a name, and click **Create**.
- Click the newly created **integration name** link, check the **Enable** check box and **Save**.
- Click the **integration name** to display the integration URL. Copy the integration URL into the **Custom Umbrella Integration URL** field on the **Add New Umbrella Module** form.

**Reporting API**

- In Umbrella, navigate to **Admin > API Keys** and click **Create**.
- Under **What should this API do?**, click the **Umbrella Reporting** radio button and then click **Create**.
- Copy the following values into the **Reporting** fields on the **Add New Umbrella Module** form:
  - API Key** (Your Key)
  - API Secret** (Your Secret)
  - Organization ID** - from browser URL, the set of numbers between `/o/` and `/a/`
  - Request Timeframe** (days) - Enter the timeframe (in days) for enriching sightings from the most recent DNS requests

## Créer un tableau de bord SecureX

1. Une fois que vous avez ajouté votre module, vous pouvez naviguer vers Secure X et créer un nouveau tableau de bord.
2. Sous les tableaux de bord disponibles, sélectionnez votre module Umbrella et ajoutez les catégories qui vous intéressent.
3. Cliquez sur Save, et voir vos informations renseignées via l'API.



## Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

## Enquêter

L'API Investigate vous permet d'ajouter un flux à une investigation CTR, pour voir la disposition d'un domaine et enrichir l'investigation avec d'autres modules.

1. Afin de vérifier cette intégration, effectuez une nouvelle enquête dans [Cisco Threat Response](#). Une Disposition fournie par Umbrella peut être trouvée avec une recherche d'un domaine connu, tel que cisco.com.

2. Si vous cliquez sous le domaine dans le graphique Relations, vous pouvez également pivoter de là vers le tableau de bord Enquêter dans Umbrella.

The screenshot displays the Cisco Threat Response Investigate interface. At the top, there are navigation tabs for Threat Response, Investigate, Snapshots, Incidents, and Intelligence. The main area is divided into several sections:

- Investigation:** Shows '1 of 1 enrichments complete' for the domain 'cisco.com'. There are buttons for 'Investigate', 'Clear', and 'Reset', along with 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 red document icon.
- Observables:** A section for 'cisco.com' showing 'Clean Domain' and 'My Environment' with a graph of '0 Sightings in My Environment'.
- Judgements (2):** A table showing results from Umbrella and Talos Intelligence.

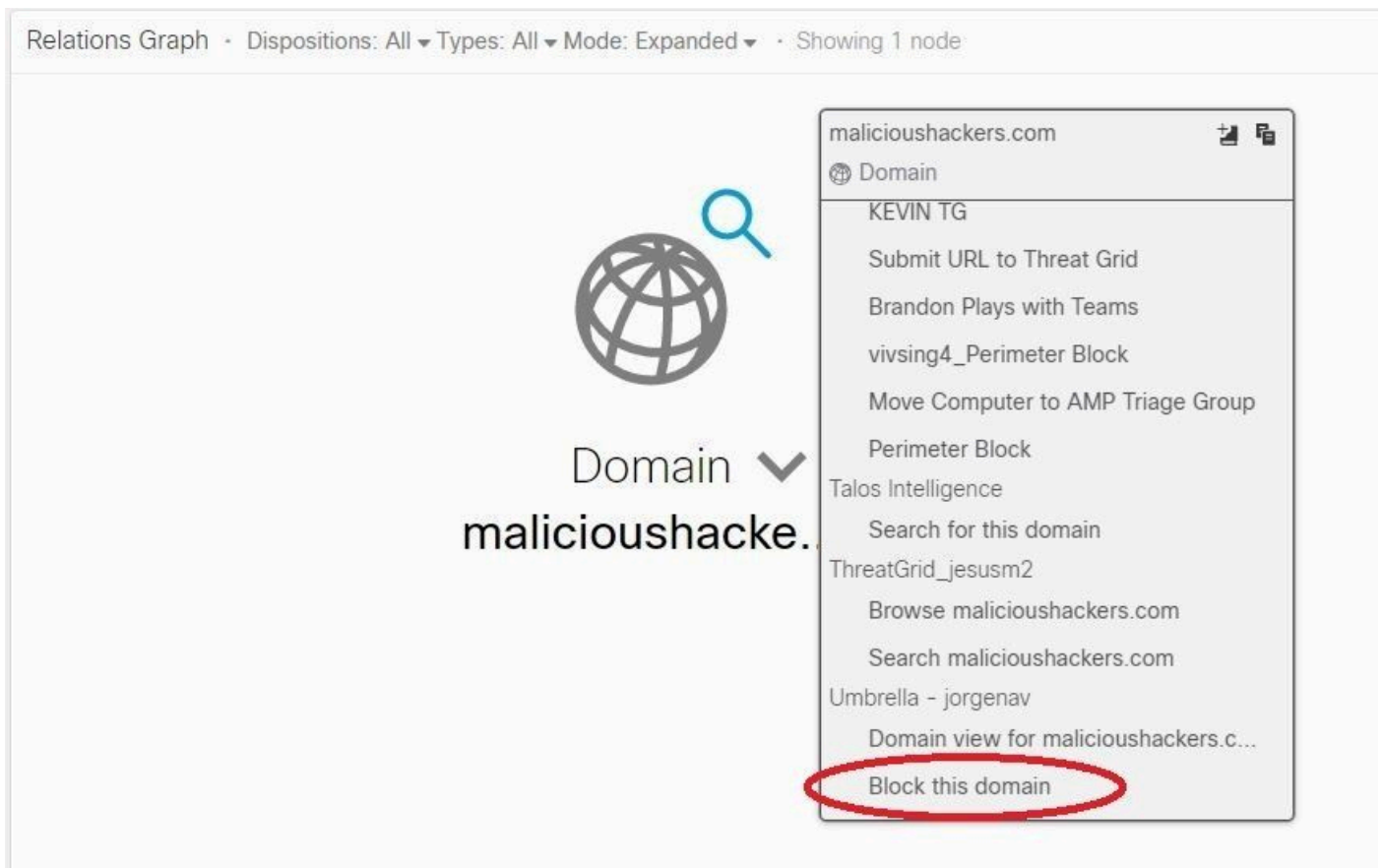
Module	Observable	Disposition	Reason	Source
Umbrella - jorgenav	DOMAIN: cisco.com	Clean	Good Cisco Umbrella reputation status	Umbrella Investigate API
Talos Intelligence	DOMAIN: cisco.com	Clean	Good Talos Intelligence reputation score	Talos Intelligence

## Application

Avec l'API d'application, vous pouvez bloquer ou débloquer un domaine directement à partir d'une investigation.

1. Afin de vérifier que l'API fonctionne, vous pouvez bloquer un domaine vu dans une investigation et qui ajoute le domaine à la liste de blocage de stratégie dans Umbrella.

2. Afin de vérifier que l'URL a été ajoutée à la liste de blocage, naviguez vers Politiques > Composants de la politique > Intégrations. Sélectionnez votre intégration SecureX, puis cliquez sur Voir Domaines. Une fenêtre affiche les domaines ajoutés à partir de CTR.



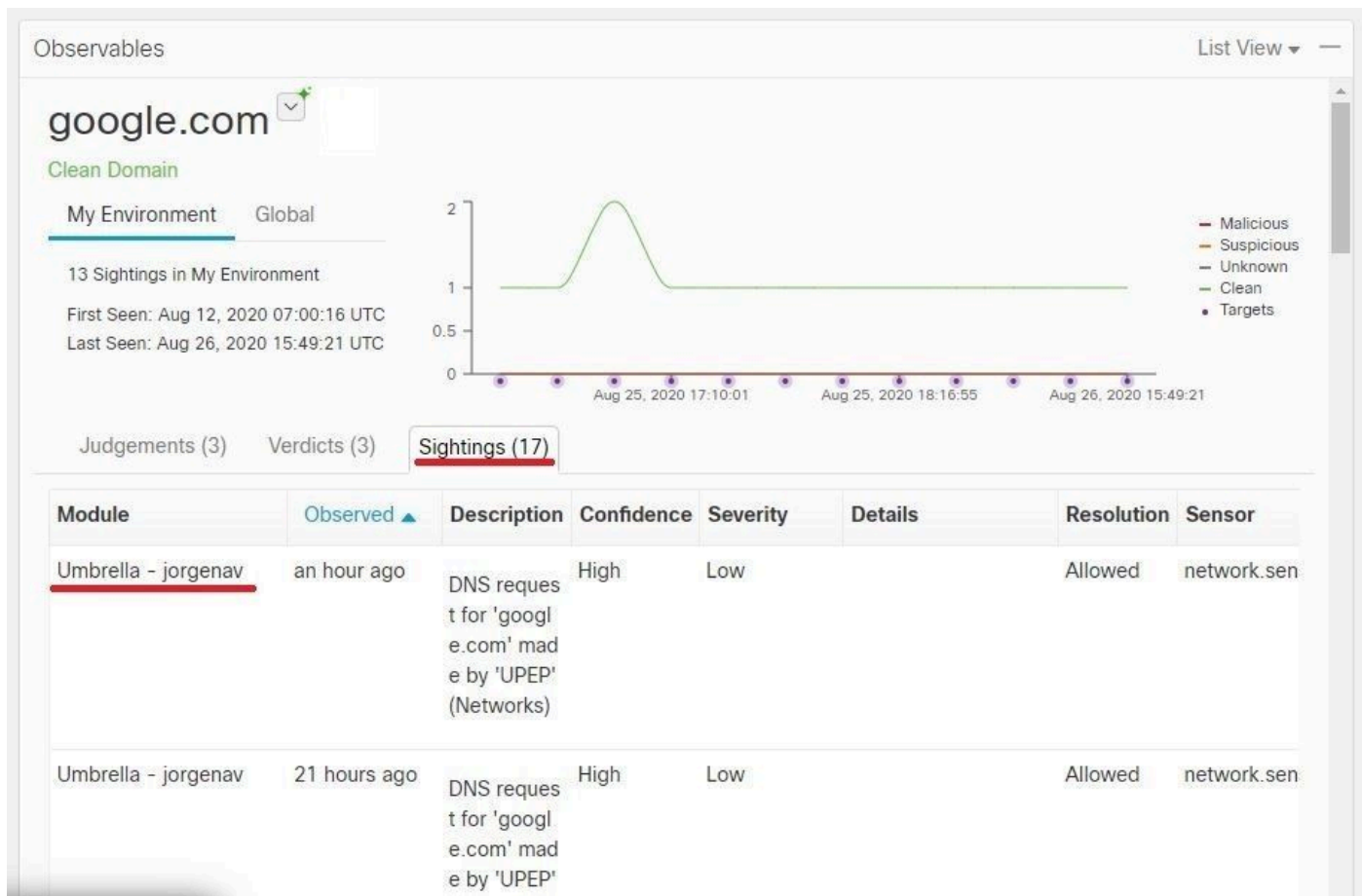
3. Si les domaines ne sont pas bloqués, sur votre tableau de bord Umbrella, accédez à Stratégies > Composants de stratégie > Paramètres de sécurité. Sous Integrations, vérifiez que vous avez appliqué la liste souhaitée.

## Rapports

L'API de création de rapports vous permet de consulter les informations relatives à vos déploiements Umbrella dans SecureX.

Vous pouvez vérifier l'intégration avec une investigation d'un domaine que vous savez avoir été vu dans votre environnement dans CTR.

Dans l'enquête CTR, la liste des ordinateurs ayant accédé à un domaine particulier s'affiche sous Observations.



## Vidéo

Cette vidéo présente les informations de configuration contenues dans cet article.

## Informations connexes

- [Assistance et documentation techniques - Cisco Systems](#)



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.