Intégrer Cisco SecureX à Cisco Umbrella

Table des matières

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

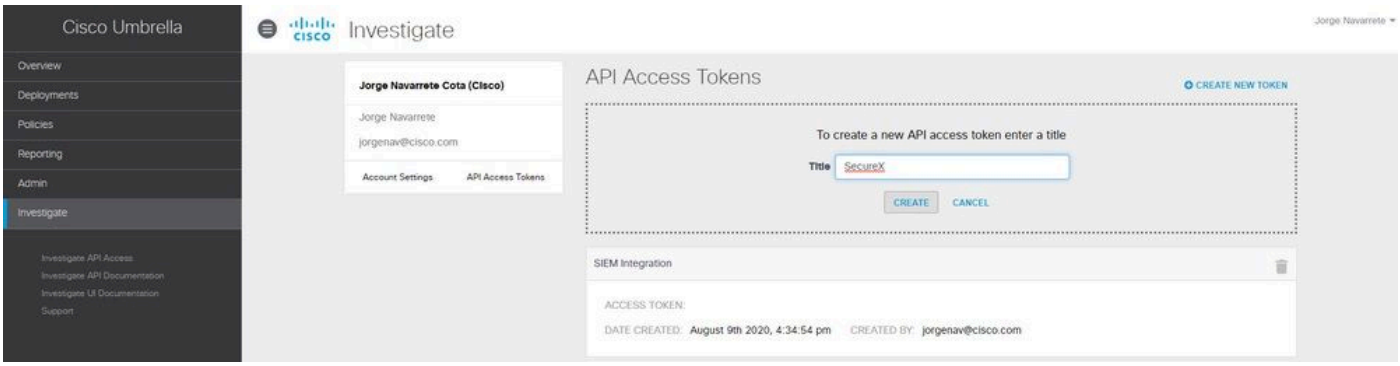
Créer un module

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.

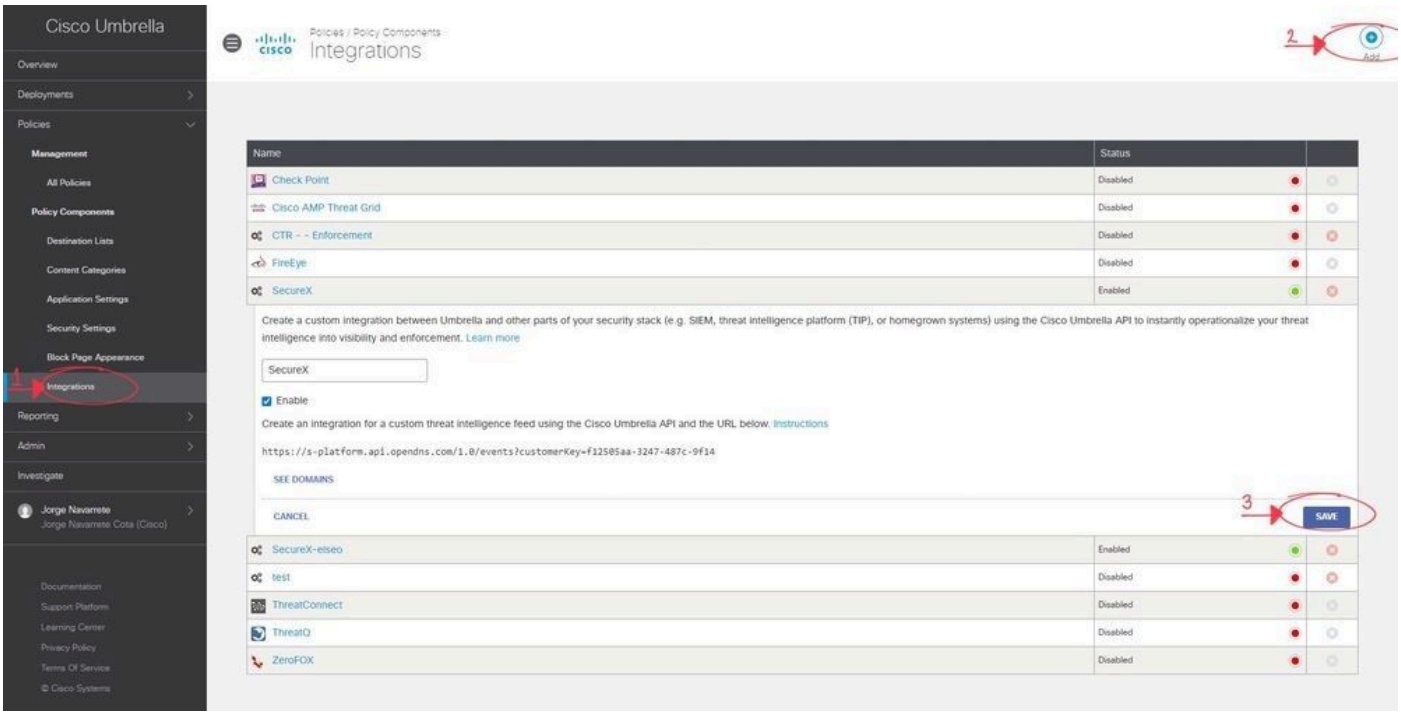
Étudier l'API

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 Policies > 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 etEnregistrer.
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.



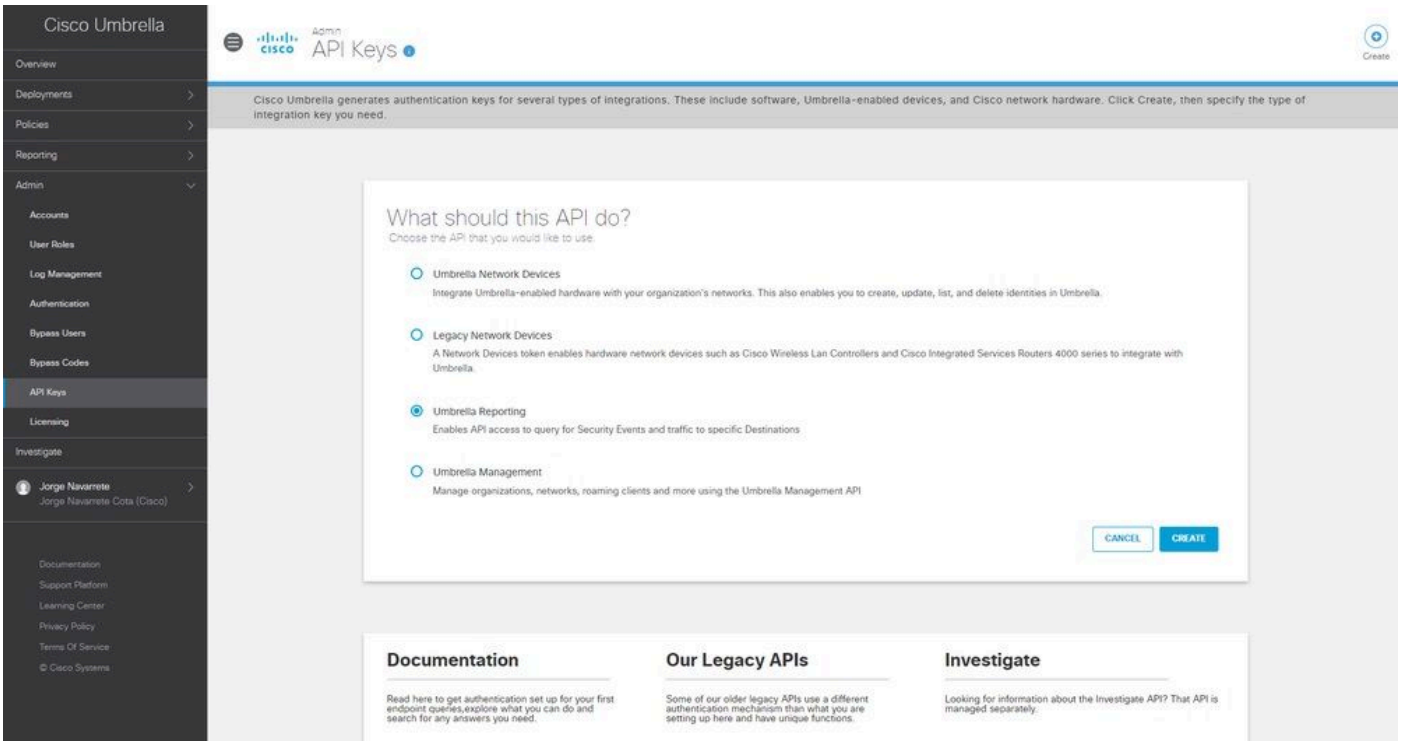
Remarque : pour intégrer l'API Umbrella Enforcement, vous devez être un administrateur dans une organisation autonome Umbrella ou une organisation enfant au lieu d'un administrateur d'une console Umbrella.

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.

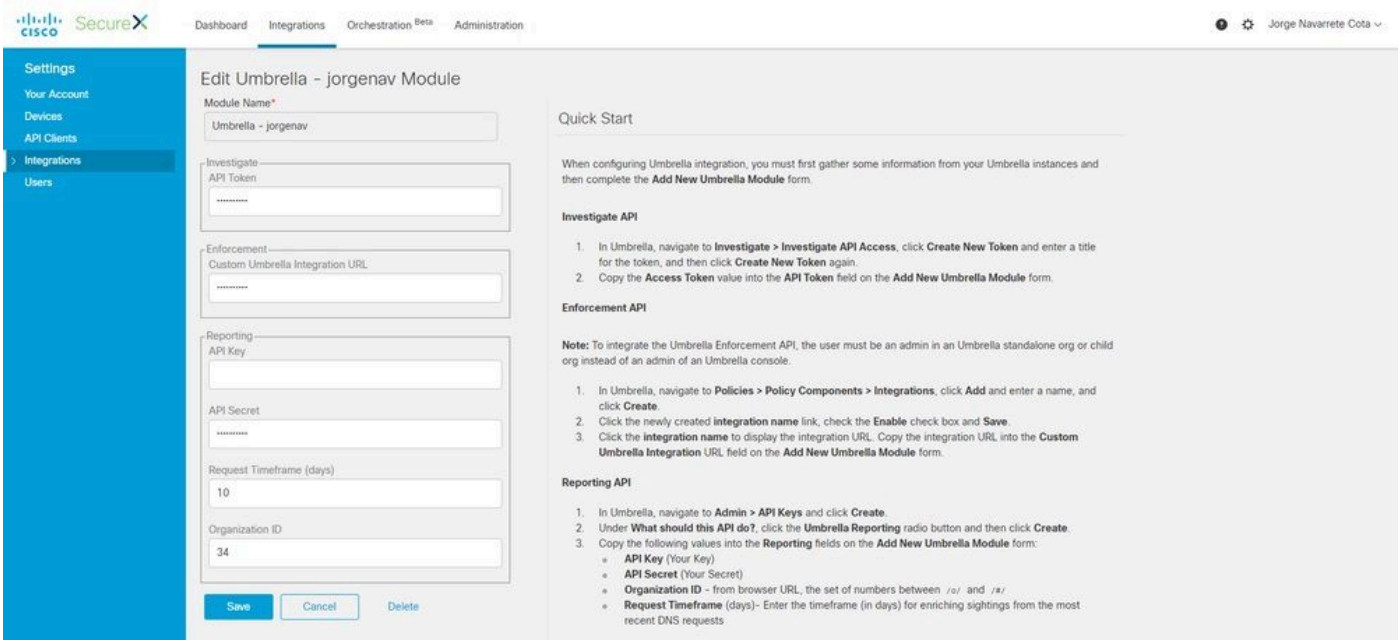
3. Copiez les valeurs suivantes dans les champs Reporting du formulaire Add New Umbrella Module :

    - 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



Enregistrer le module

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

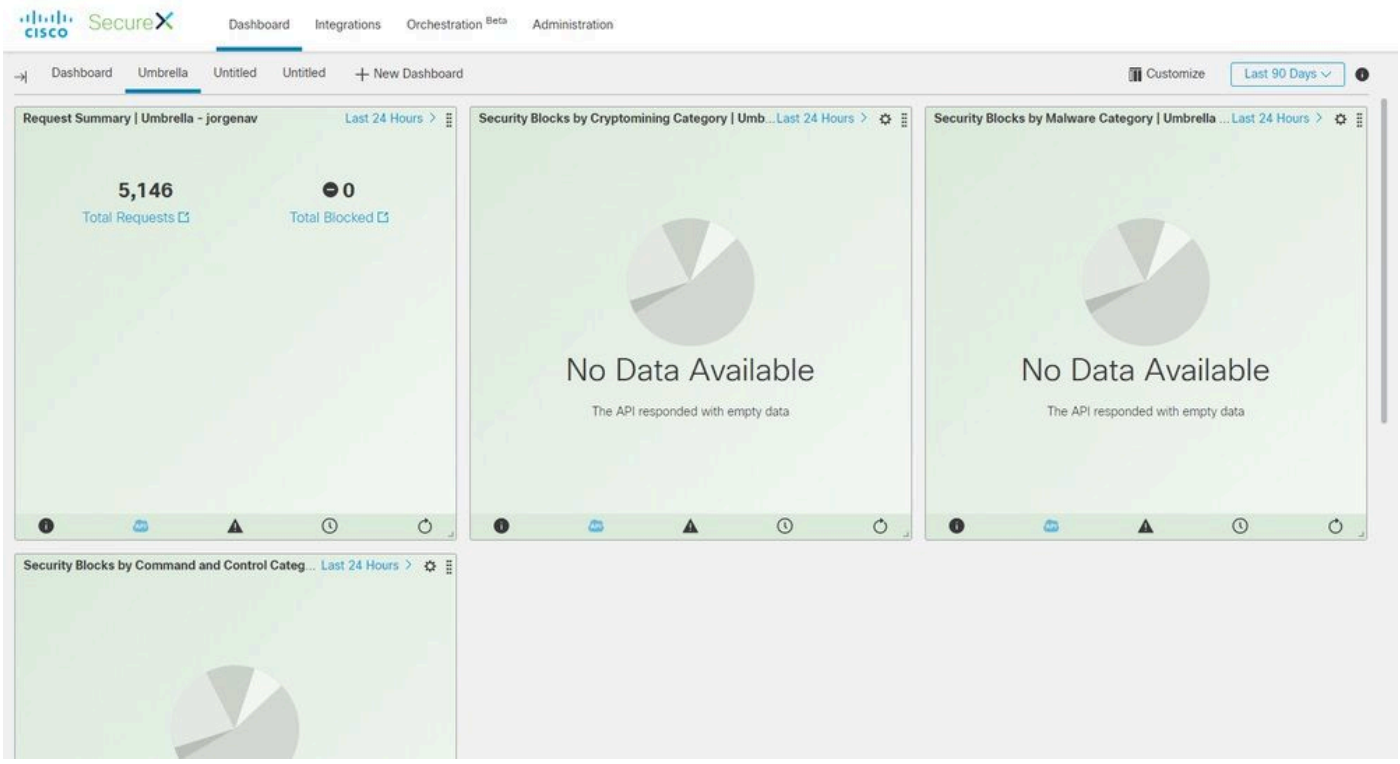


Créer un tableau de bord SecureX

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

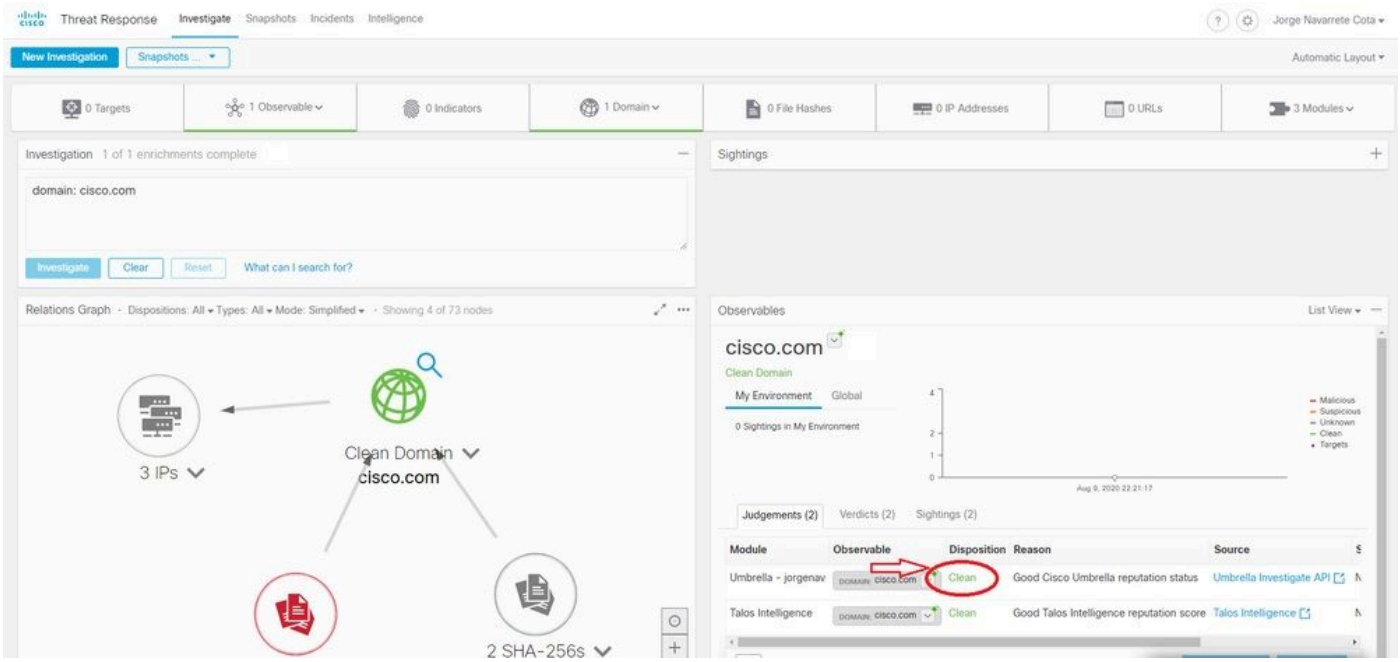
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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.

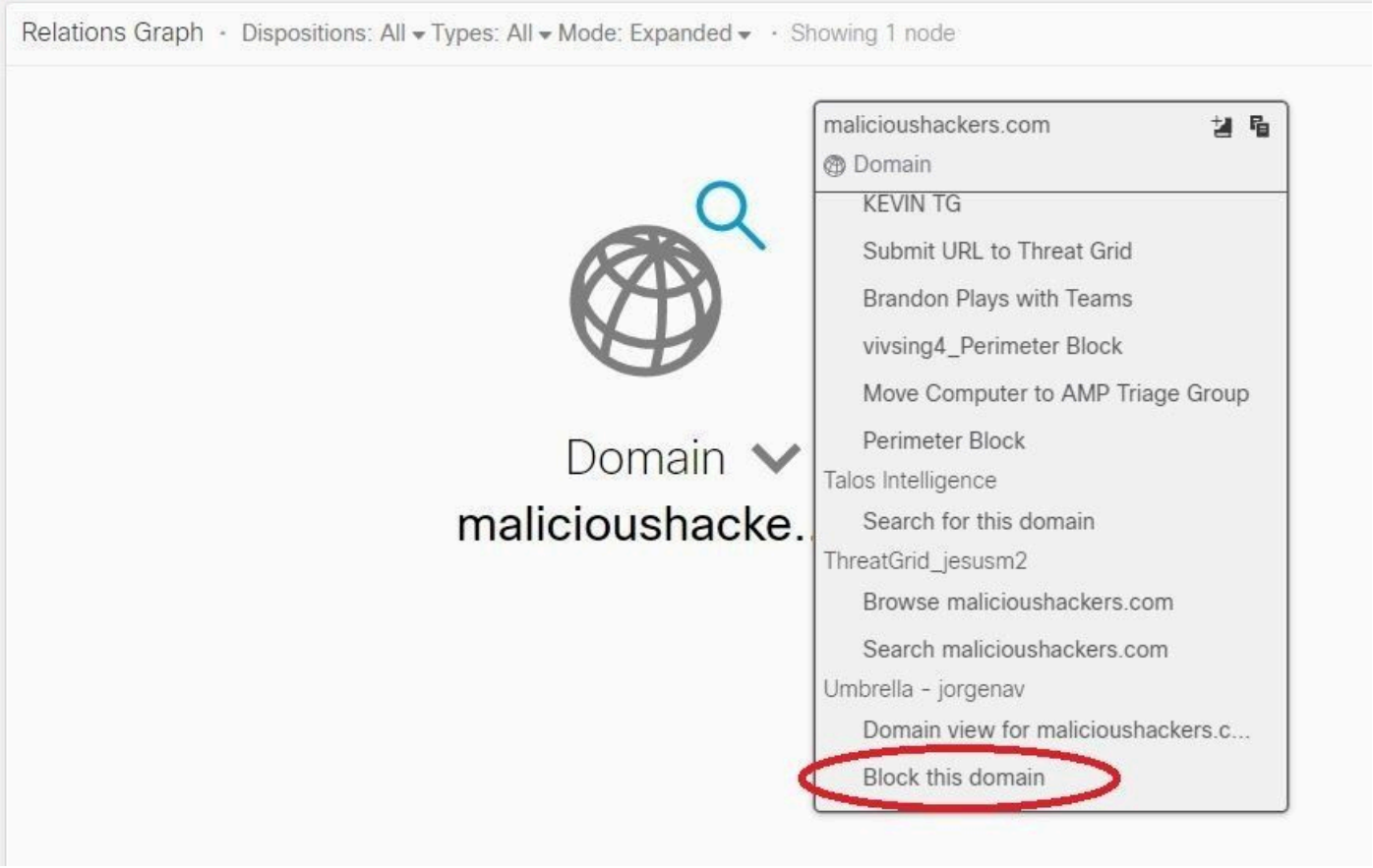


Application

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.



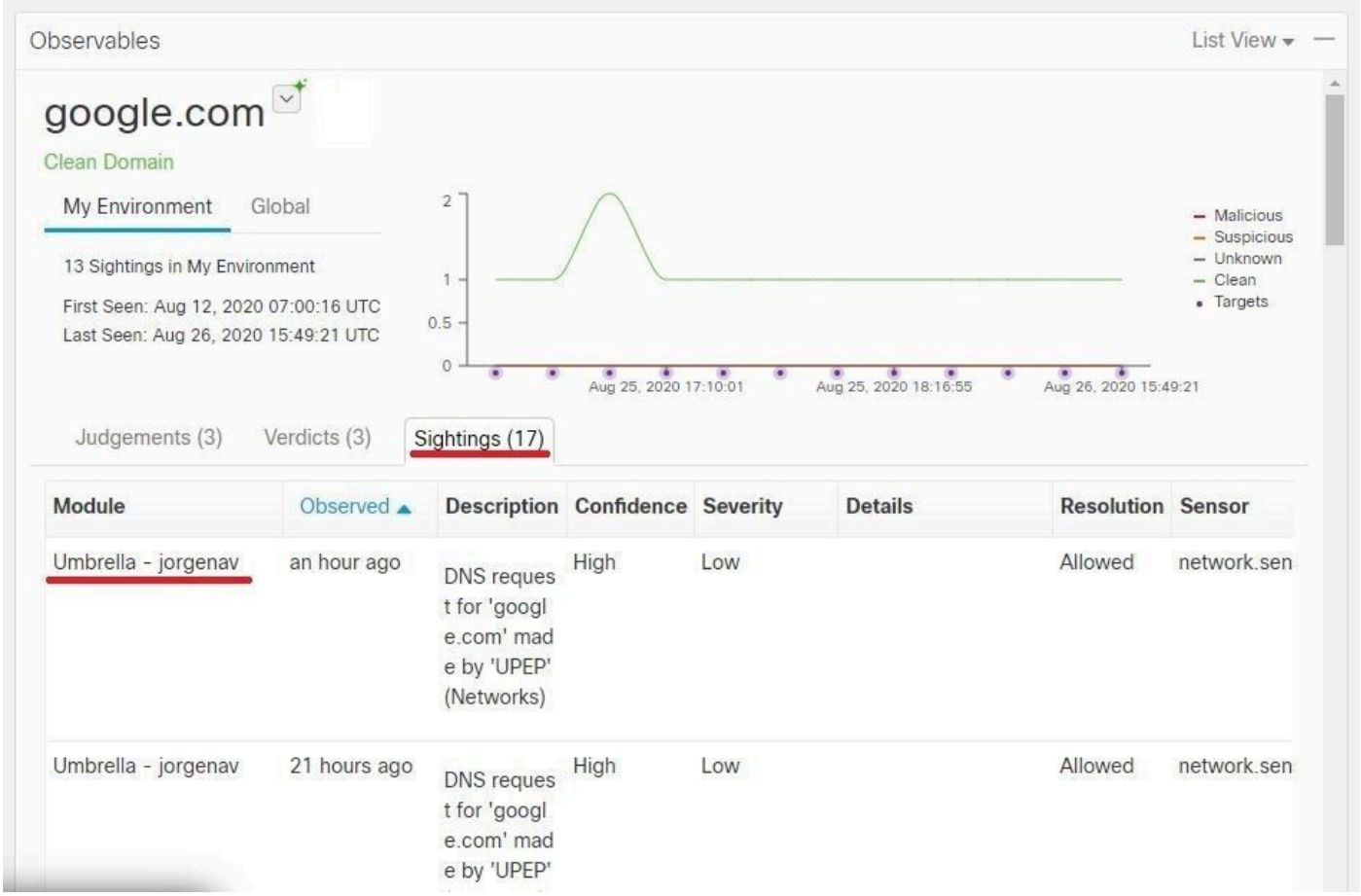
3. Si les domaines ne sont pas bloqués, sur votre tableau de bord Umbrella, accédez à Stratégies > Composants de stratégie > Paramètres de sécurité. Sous Integrations, vérifiez que vous avez appliqué la liste souhaitée.

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.