

将Cisco SecureX与Cisco Umbrella集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[创建模块](#)

[调查API](#)

[实施API](#)

[报告API](#)

[保存模块](#)

[创建SecureX控制面板](#)

[验证](#)

[调查](#)

[实施](#)

[报告](#)

[视频](#)

[相关信息](#)

简介

本文档介绍配置和验证Umbrella与SecureX的集成以及3个可用API的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Umbrella
- 思科安全X
- 思科威胁响应

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 具有DNS Advantage许可证的Umbrella帐户
- 安全X

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

为了完整配置此集成及其所有功能，您需要访问以下3个API

- 报告API（包括在所有许可证中）
- 实施API
- 调查API

为了配置Umbrella集成，您必须首先从Umbrella实例收集一些信息，然后完成添加新的Umbrella模块表单。

配置

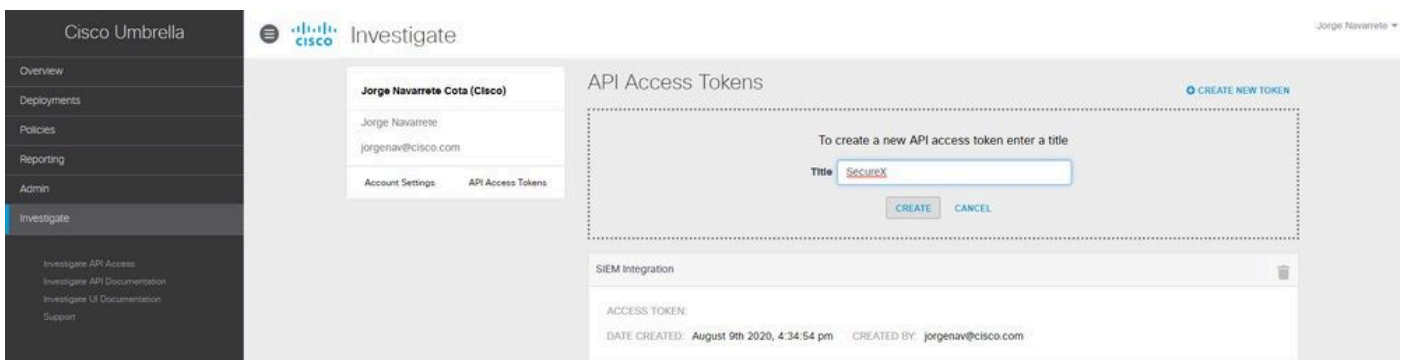
创建模块

1. 登录您的Secure X帐户。如果您还没有帐户，可以用[Cisco安全登录](#)创建一个帐户。
2. 导航到集成>添加新模块。在“可用集成”页中，向下滚动到Umbrella选项并单击添加新模块。

使用以下步骤从Umbrella帐户收集必要信息，以在添加新的Umbrella模块表单中提交。

调查API

1. 在Umbrella中，导航到调查>调查API访问，点击创建新令牌并输入令牌标题，然后再次点击创建新令牌。
2. 将访问令牌值复制到Add New Umbrella Module表单上的API Token字段中。



实施API

1. 在Umbrella中，导航到策略>策略组件>集成，单击添加并输入名称，然后单击创建。
2. 单击新建的integration name链接、选中Enablecheck框和Save。
3. 单击integration name以显示集成URL。将集成URL复制到添加新Umbrella模块表单上的自定义

义Umbrella集成 URL字段。

Name	Status		
Check Point	Disabled	●	○
Cisco AMP Threat Grid	Disabled	●	○
CTR - - Enforcement	Disabled	●	○
FireEye	Disabled	●	○
SecureX	Enabled	●	○

Create a custom integration between Umbrella and other parts of your security stack (e.g. SIEM, threat intelligence platform (TIP), or homegrown systems) using the Cisco Umbrella API to instantly operationalize your threat intelligence into visibility and enforcement. [Learn more](#)

SecureX

Enable


Create an integration for a custom threat intelligence feed using the Cisco Umbrella API and the URL below. [Instructions](#)

`https://s-platform.api.opendns.com/1.0/events?customerKey=f32585aa-3247-487c-9f34`

SEE DOMAINS

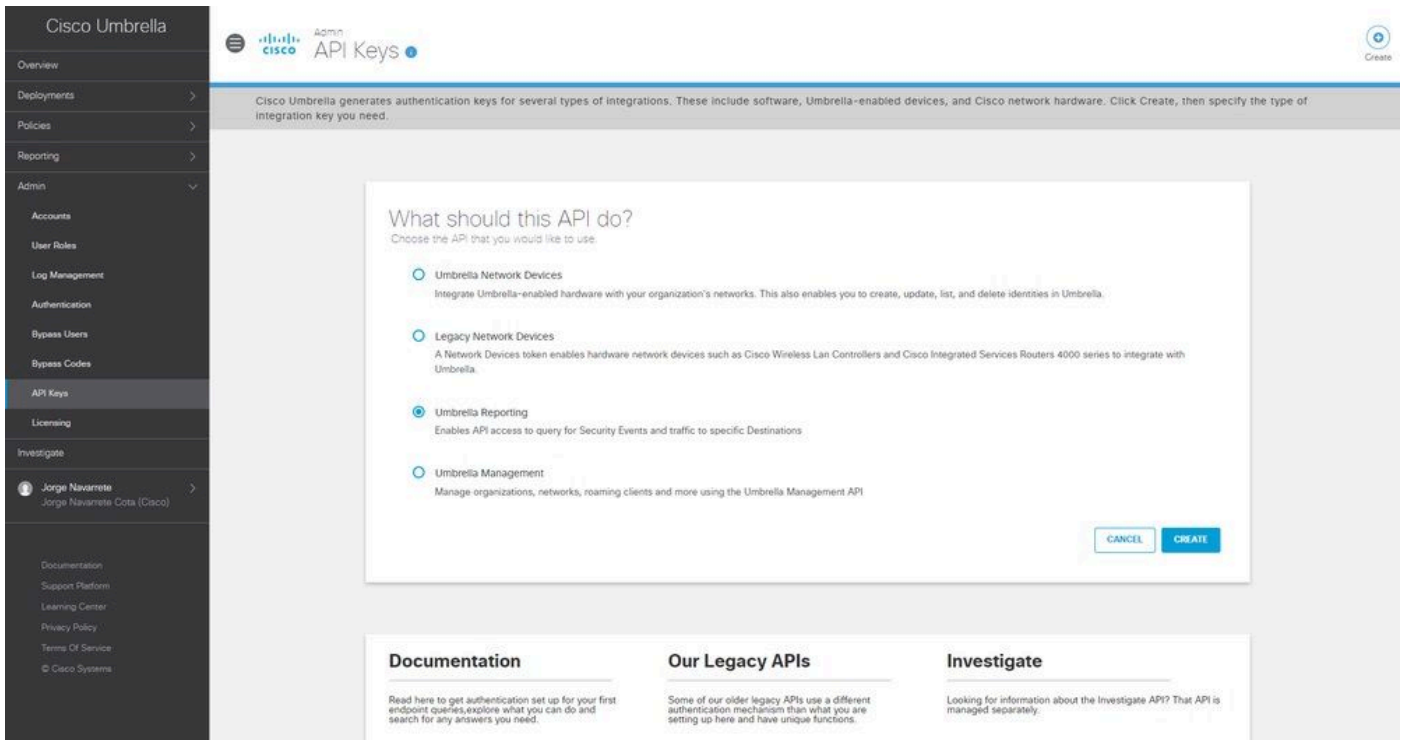
CANCEL

SAVE

 注意：要集成Umbrella实施API，您必须是Umbrella独立组织或子组织中的管理员，而不是Umbrella控制台的管理员。

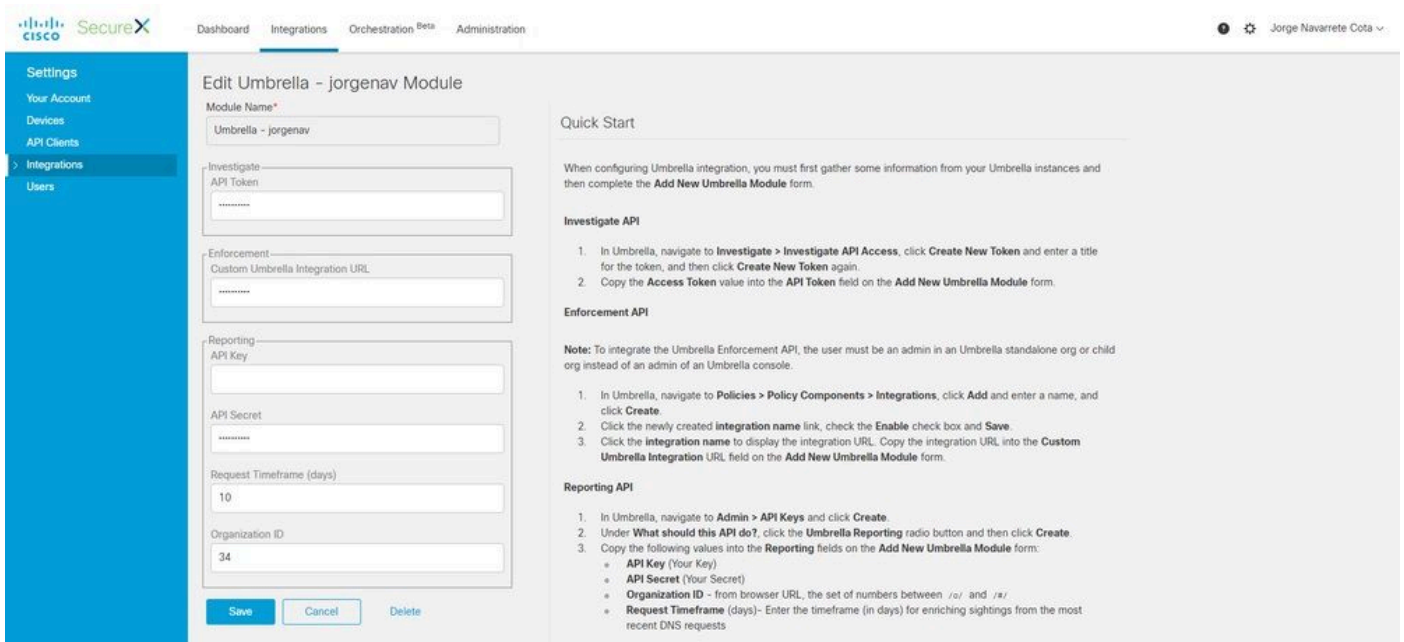
报告API

1. 在Umbrella中，导航到管理> API密钥，然后单击创建。
2. 在此API应做什么？下，单击Umbrella Reporting 单选按钮，然后单击创建。
3. 将以下值复制到添加新的Umbrella模块窗体上的报告字段中：
 - API密钥（您的密钥）
 - API密钥（您的密钥）
 - 组织ID - 来自浏览器URL的/o/和/#/之间的数字集
 - 请求时间范围（天）-输入根据最新DNS请求丰富发现的时间范围（以天为单位）



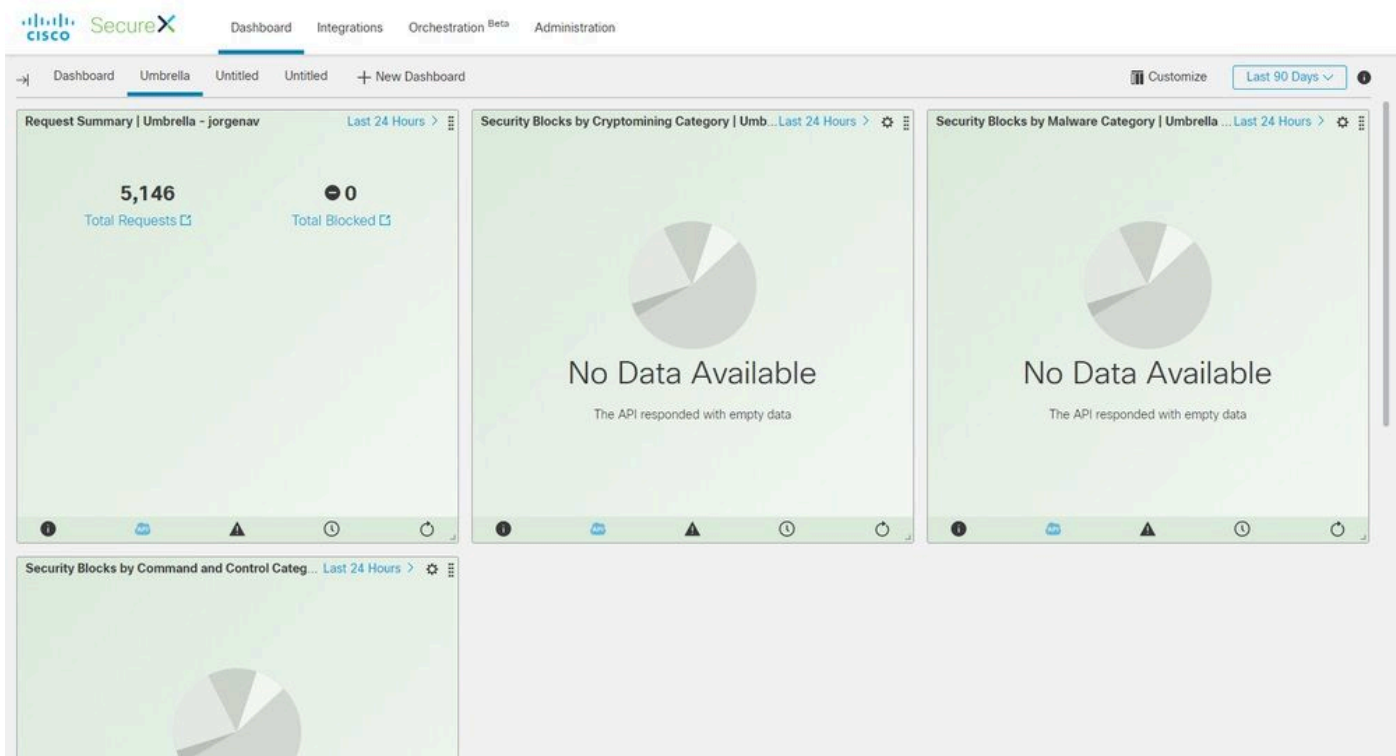
保存模块

1. 在Umbrella模块中填写API信息，然后单击Save。



创建SecureX控制面板

1. 添加模块后，可以导航到Secure X并创建新控制面板。
2. 在可用控制面板下，选择您的Umbrella模块并添加您感兴趣的类别。
3. 单击保存，然后查看通过API填充的信息。



验证

使用本部分可确认配置能否正常运行。

调查

Investigate API允许您向CTR调查添加源，查看域的处置情况并使用其他模块丰富调查。

1. 为了验证此集成，请在[思科威胁响应](#)中进行新的调查。通过搜索已知域(例如cisco.com)可以找到Umbrella提供的处置情况。
2. 如果单击“关系图”中的域下方，则还可以从那里旋转透视到Umbrella中的“调查仪表板”。

Investigation: 1 of 1 enrichments complete

domain: cisco.com

Investigate Clear Reset What can I search for?

Relations Graph - Dispositions: All - Types: All - Mode: Simplified - Showing 4 of 73 nodes

3 IPs Clean Domain cisco.com 2 SHA-256s

Sightings

Observables

cisco.com Clean Domain

My Environment Global

0 Sightings in My Environment

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

实施

通过实施API，您可以阻止或取消阻止域直接来自调查。

1. 为了验证API是否有效，您可以阻止调查中发现的域，并将该域添加到Umbrella中的策略阻止列表。
2. 要验证URL是否已添加到阻止列表，请导航到策略>策略组件>集成。选择您的SecureX集成，然后点击查看域。此时会出现一个窗口，显示CTR中添加的域。

Relations Graph - Dispositions: All - Types: All - Mode: Expanded - Showing 1 node

Domain malicioushacke.

malicioushackers.com

- Domain
- KEVIN TG
- Submit URL to Threat Grid
- Brandon Plays with Teams
- vivings4_Perimeter Block
- Move Computer to AMP Triage Group
- Perimeter Block
- Talos Intelligence
- Search for this domain
- ThreatGrid_jesum2
- Browse malicioushackers.com
- Search malicioushackers.com
- Umbrella - jorgenav
- Domain view for malicioushackers.c...
- Block this domain**

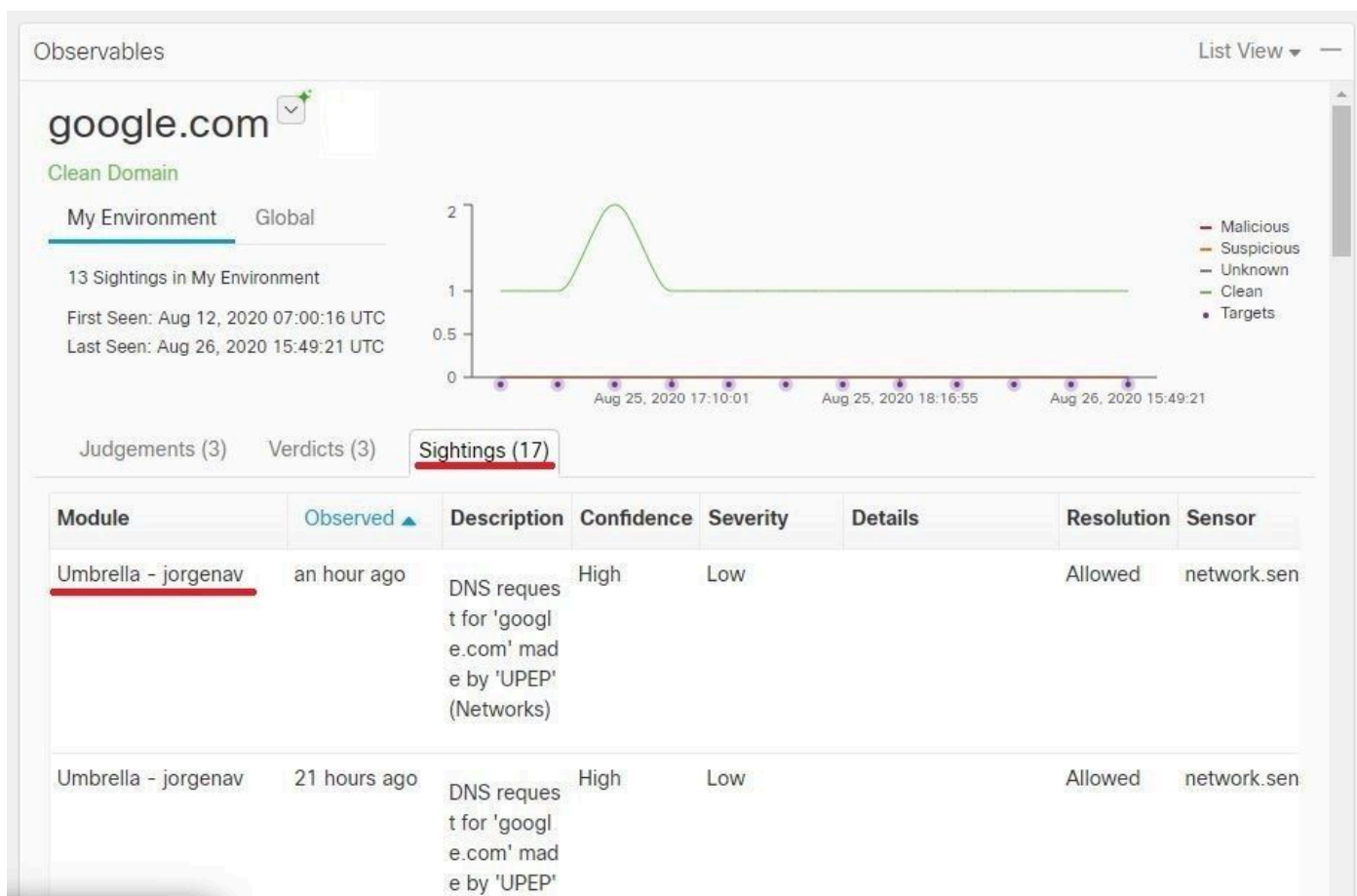
3. 如果未阻止域，请在Umbrella控制面板上导航到策略>策略组件>安全设置。在集成下，确保已应用所需的列表。

报告

报告API允许您查看SecureX中Umbrella部署的信息。

您可以验证与已知CTR环境中已发现的域的调查的集成。

在CTR调查中，已访问特定域的计算机的列表显示在“Sightings”下。



视频

您可以在此视频中找到本文中包含的配置信息。

相关信息

- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。