將Cisco SecureX與Cisco Umbrella整合

目錄

簡介

本文檔介紹使用3個可用API配置和驗證Umbrella與SecureX整合的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 思科資安防護傘
- Cisco Secure X
- 思科威脅響應

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 具有DNS Advantage許可證的Umbrella帳戶
- 安全X

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

為了完整配置此整合及其所有功能，您需要訪問以下3個API

- 報告API（包含在所有許可證中）
- 實施API
- 調查API

要配置Umbrella整合，您必須首先從Umbrella例項收集一些資訊，然後完成增加新的Umbrella模組表單。

設定

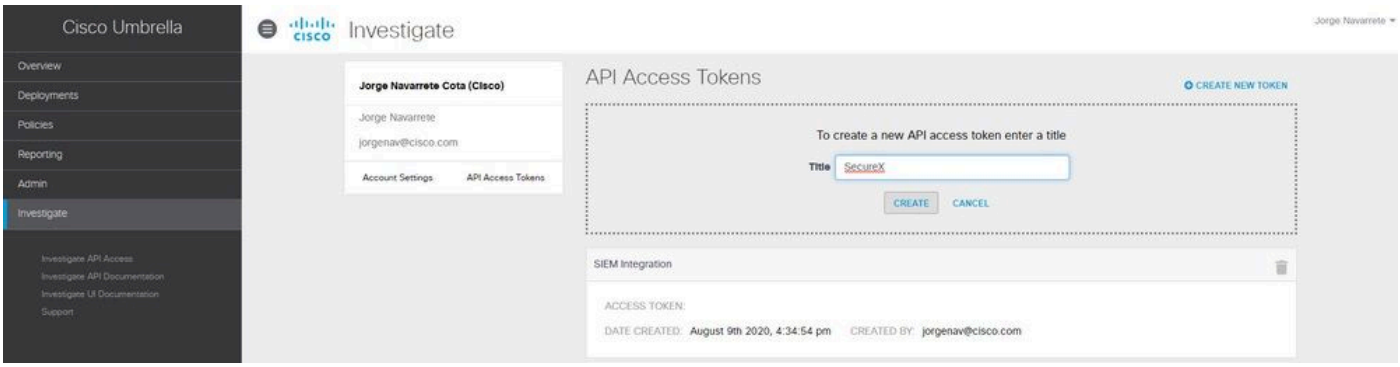
建立模組

1. 登入您的Secure X帳戶。如果您還沒有帳戶，則可以用Cisco安全登入建立一個帳戶。
2. 導航到整合>增加新模組。在Available Integrations頁中，向下滾動到Umbrella選項，然後按一下Add New Module。

使用以下步驟，從您的Umbrella帳戶收集必要資訊，以在增加新的Umbrella模組表單中提交。

調查API

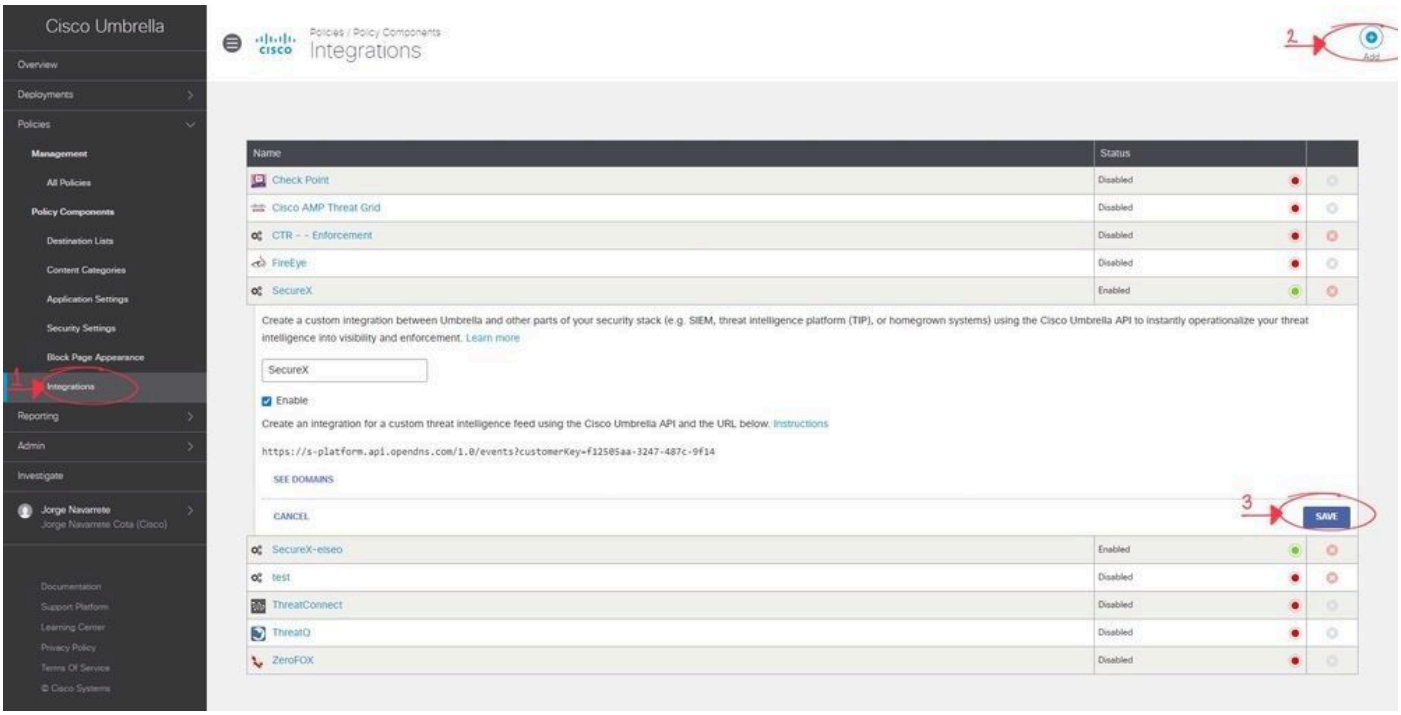
1. 在Umbrella中，導航到調查>調查API訪問，點選建立新令牌並輸入令牌標題，然後再次點選建立新令牌。
2. 將訪問令牌值複製到「增加新的Umbrella模組」窗體上的「API令牌」欄位中。



實施API

1. 在Umbrella中，導航到策略>策略元件>整合，點選增加，輸入名稱，然後點選建立。
2. 按一下新建立的整合名稱連結，選中Enablecheck框，然後進行儲存。

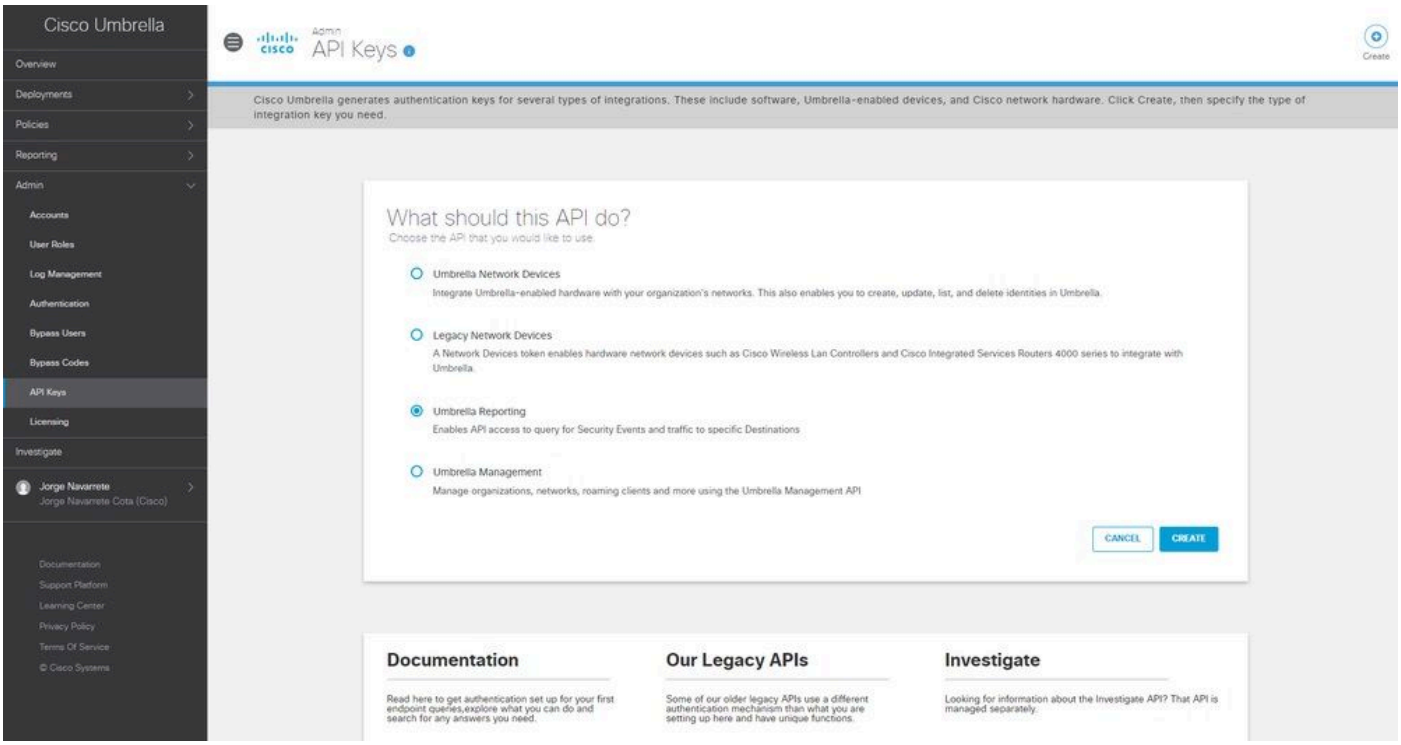
3. 按一下integration name以顯示整合URL。將整合URL複製到Add New Umbrella Module 表單上的Custom Umbrella Integration URL欄位。



注意：要整合Umbrella實施API，您必須是Umbrella獨立組織或子組織中的管理員，而不是Umbrella控制檯中的管理員。

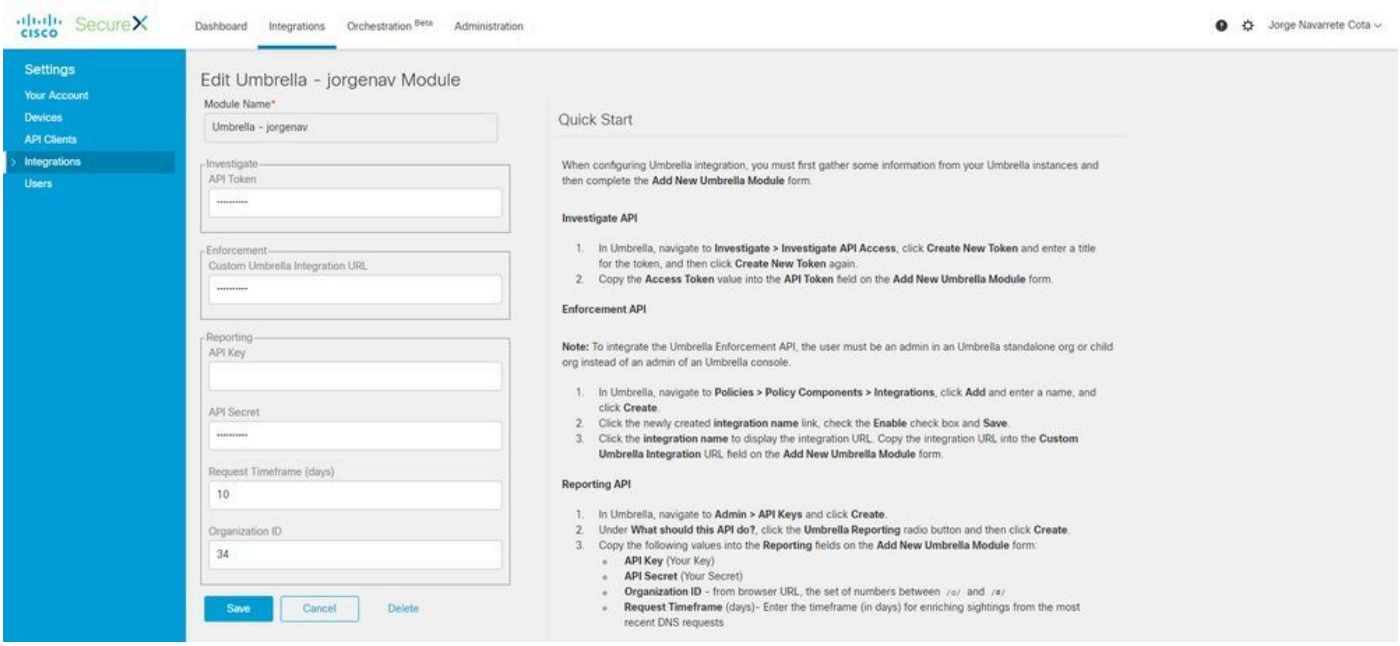
報告API

1. 在Umbrella中，導航到管理> API金鑰，然後按一下建立。
2. 在此API應做什麼？下，按一下Umbrella Reporting 單選按鈕，然後按一下Create。
3. 將以下值複製到Add New Umbrella Module 窗體上的Reporting欄位中：
    - API金鑰（您的金鑰）
    - API密碼（您的密碼）
    - 組織ID - 來自瀏覽器URL的/o/和/#/之間的數字集
    - 請求時間範圍（天）-輸入從最近的DNS請求中豐富所見資訊的時間範圍（以天為單位）



儲存模組

1. 在Umbrella模組中填寫API資訊，然後按一下Save。

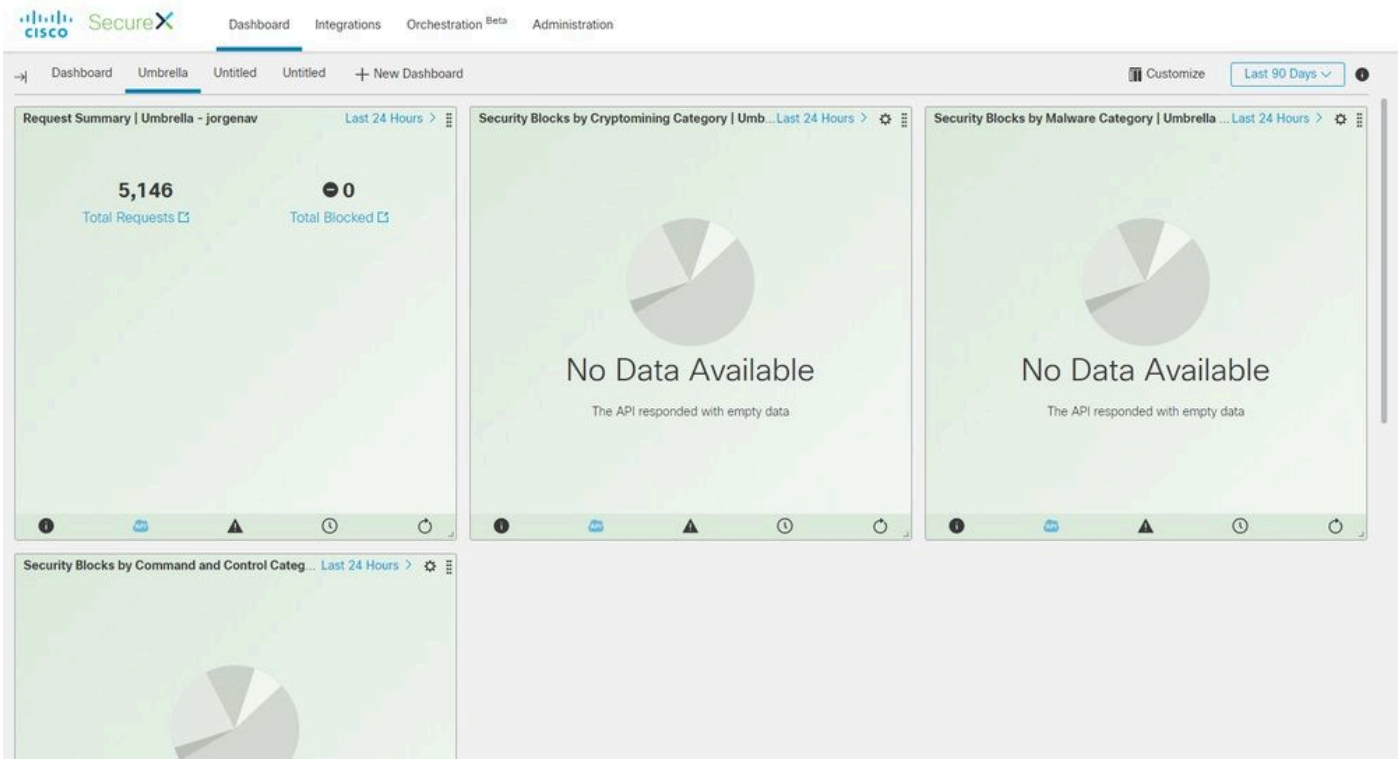


建立SecureX儀表板

1. 增加模組後，您可以導航到Secure X並建立新控制台。

2. 在可用控制台下，選擇您的Umbrella模組並增加您感興趣的「類別」。

3. 按一下儲存，然後檢視透過API填充的資訊。



驗證

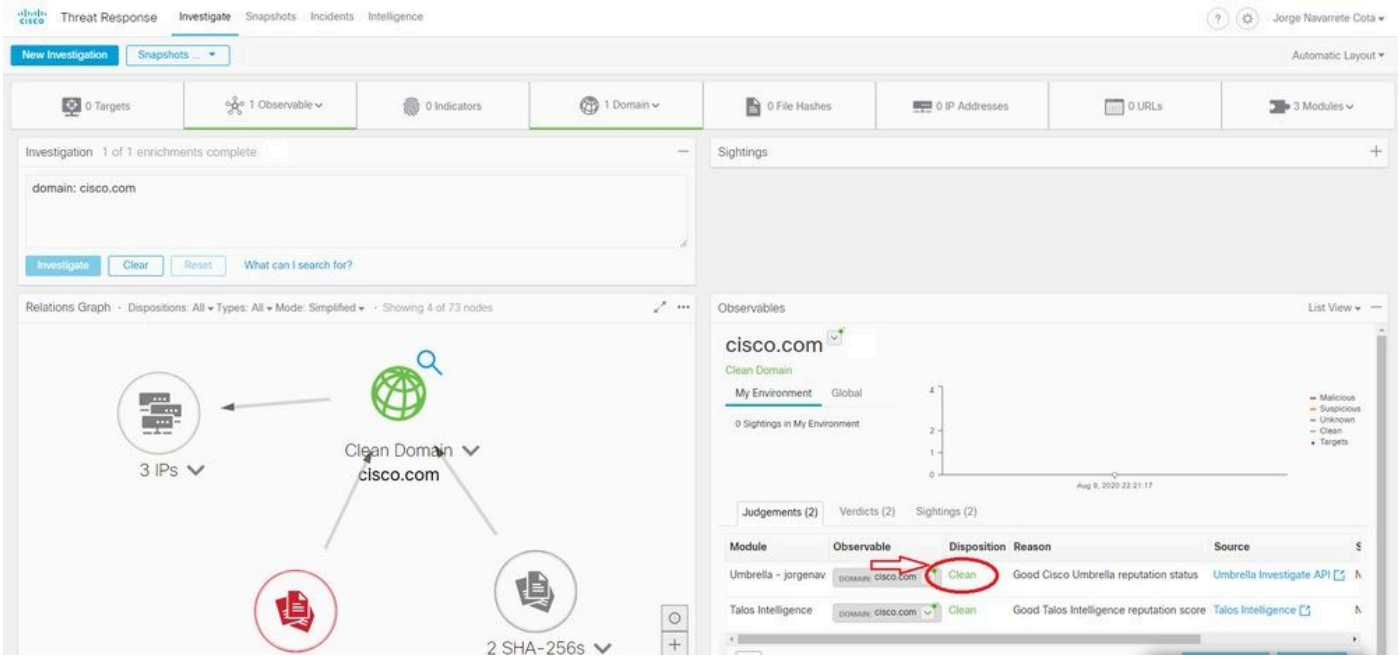
使用本節內容，確認您的組態是否正常運作。

調查

「調查API」允許您向CTR調查增加源，檢視域的處置情況並使用其他模組豐富調查。

1. 要驗證此整合，請在思科威脅響應中進行新的調查。Umbrella提供的處置可在搜尋已知域(例如cisco.com)時找到。

2. 如果您按一下「關係圖」中的領域下方，也可以從那裡樞紐分析至Umbrella中的「調查儀表板」。

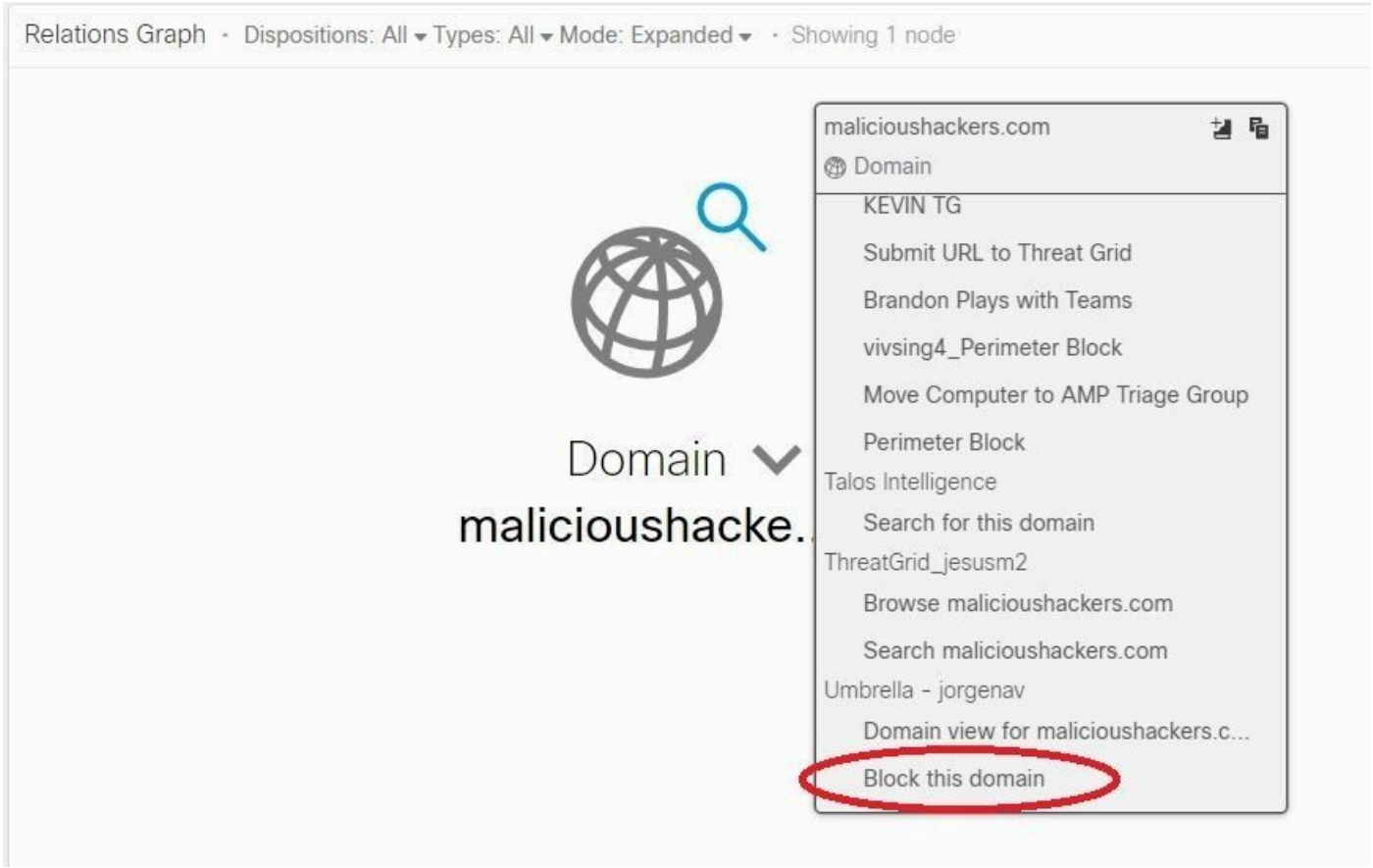


強制執行

透過實施API，您可以直接阻止或取消阻止調查中的域。

1. 為了驗證API是否有效，您可以阻止調查中發現的域，並將該域增加到Umbrella中的策略阻止清單。

2. 要驗證URL是否已增加到阻止清單，請導航到策略>策略元件>整合。選擇您的SecureX整合，然後按一下檢視域。 一個窗口顯示來自CTR的已增加域。



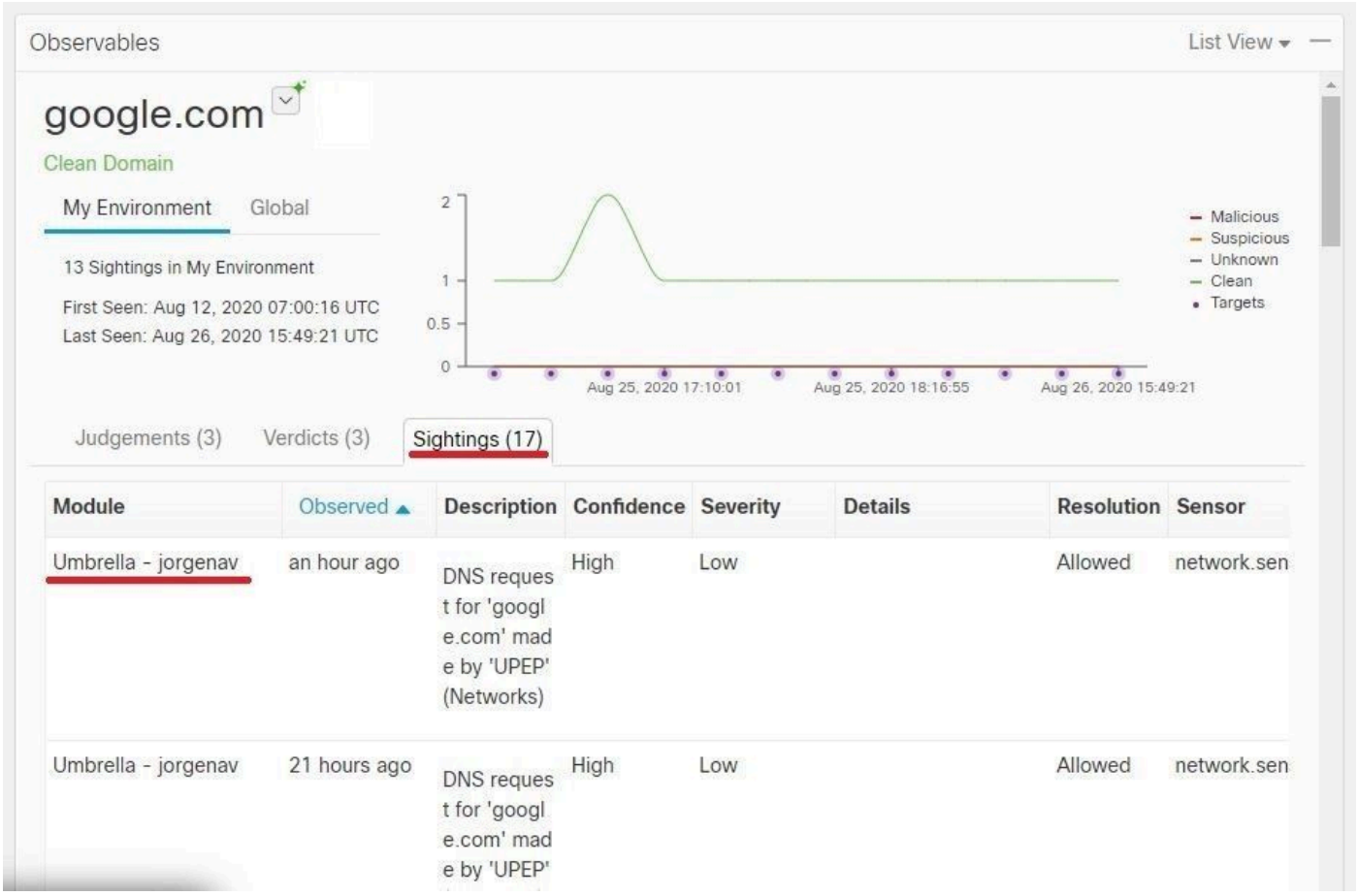
3. 如果未阻止域，請在Umbrella控制台上導航到策略>策略元件>安全設定。 在Integrations 下，確保已應用了所需清單。

報告

報告API允許您檢視SecureX中Umbrella部署的資訊。

您可以驗證與您已知已在CTR的環境中發現的域調查是否整合。

在CTR調查中，已訪問特定域的電腦清單顯示在Sighings下。



影片

您可以在本影片中找到本文中包含的配置資訊。

相關資訊

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。