整合CTR和Threat Grid雲

目錄

簡介

本文檔介紹將思科威脅響應(CTR)與Threat Grid(TG)雲整合以執行CTR調查的步驟。

作者：Jesus Javier Martinez，編輯者：Yeraldin Sanchez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 思科威脅回應
- Threat Grid

採用元件

本檔案中的資訊是根據以下軟體版本：

- CTR控制檯（具有管理員許可權的使用者帳戶）
- Threat Grid控制檯（具有管理員許可權的使用者帳戶）

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco Threat Grid是一種高級且自動化的惡意軟體分析和惡意軟體威脅情報平台，可在其中觸發可疑檔案或網路目標，而不會影響使用者環境。

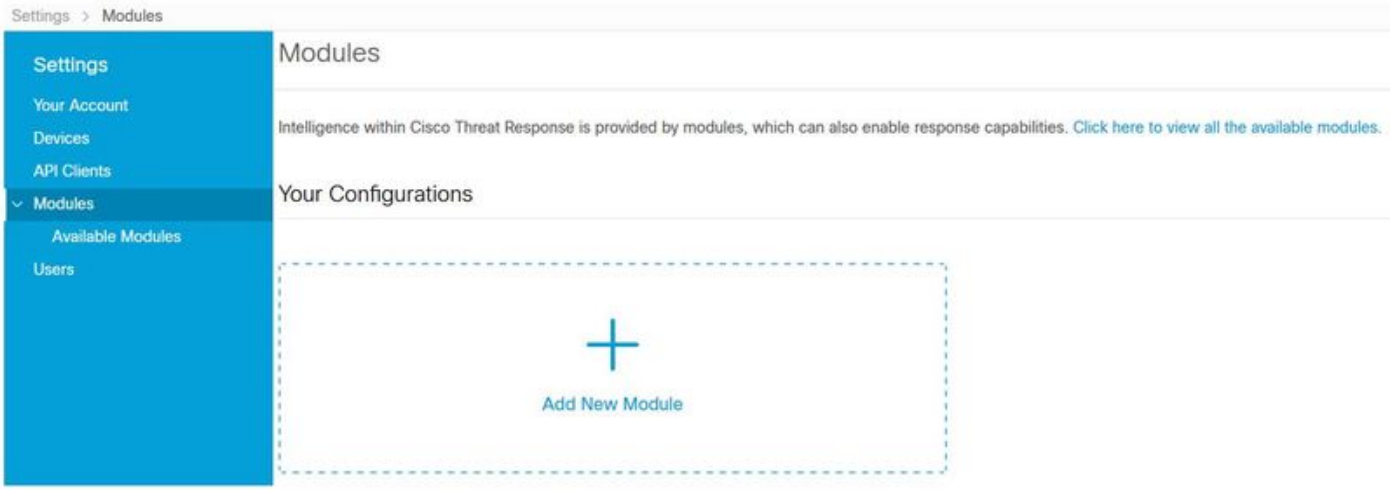
在與Cisco Threat Response的整合中，Threat Grid是一個參考模組，能夠透視到Threat Grid Portal中，以便收集有關Threat Grid知識庫中的檔案雜湊、IP、域和URL的其他情報。

設定

CTR控制檯 — 配置Threat Grid模組

步驟1.使用管理員憑證登入到思科威脅響應。

步驟2.導覽至Modules標籤，選擇**Modules > Add New Module**，如下圖所示。



步驟3.在「Available Modules」頁面上，在Threat Grid module窗格中選擇**Add New Module**，如下圖所示。

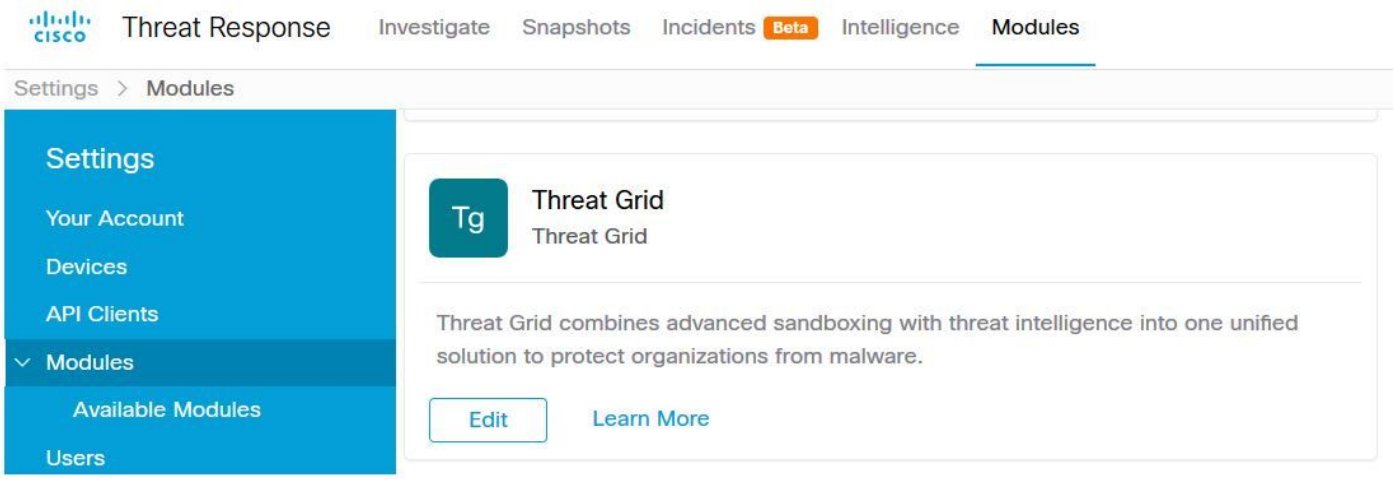
步驟4.打開**Add New Module**表格。完成如下圖所示的表格。

- **模組名**稱 — 保留預設名稱或輸入對您有意義的名稱。
- **URL** — 從下拉選單中，為Threat Grid帳戶所在位置（北美或歐洲）選擇適當的URL。 暫時忽略**Other**選項。

步驟5.選擇**Save**以完成Threat Grid模組配置。

步驟6. Threat Grid現在顯示在「模塊」頁面上**的**配置下，如下圖所示。

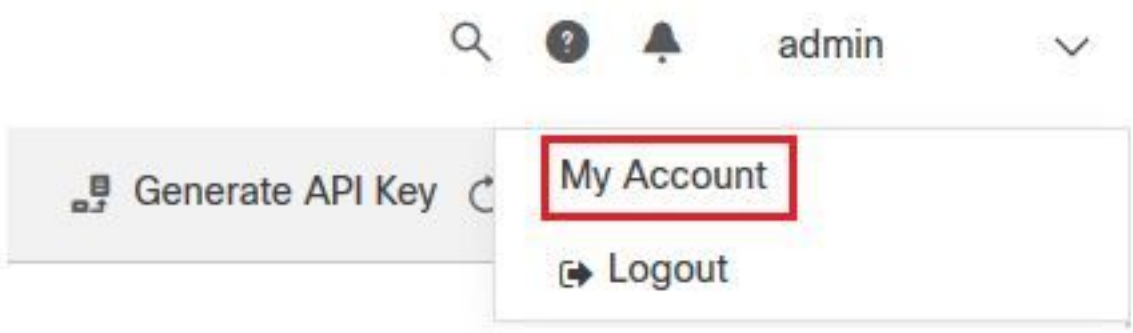
（可從旋轉選單和案例手冊中獲取TG，以改進威脅調查）。



Threat Grid控制檯 — 授權Threat Grid訪問威脅響應

步驟1.使用管理員憑據登入到Threat Grid。

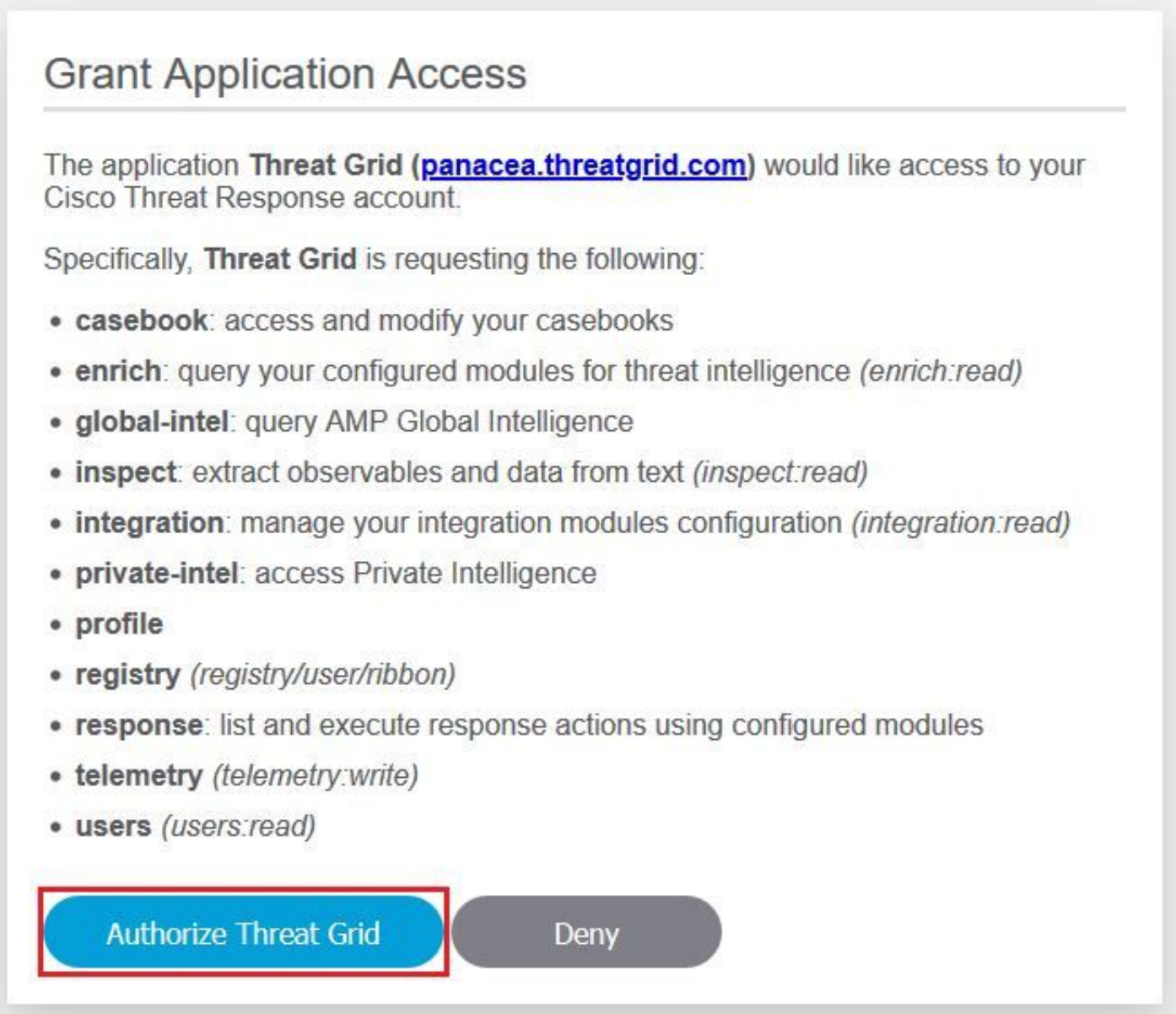
步驟2.導覽至**My Account**一節，如下圖所示。



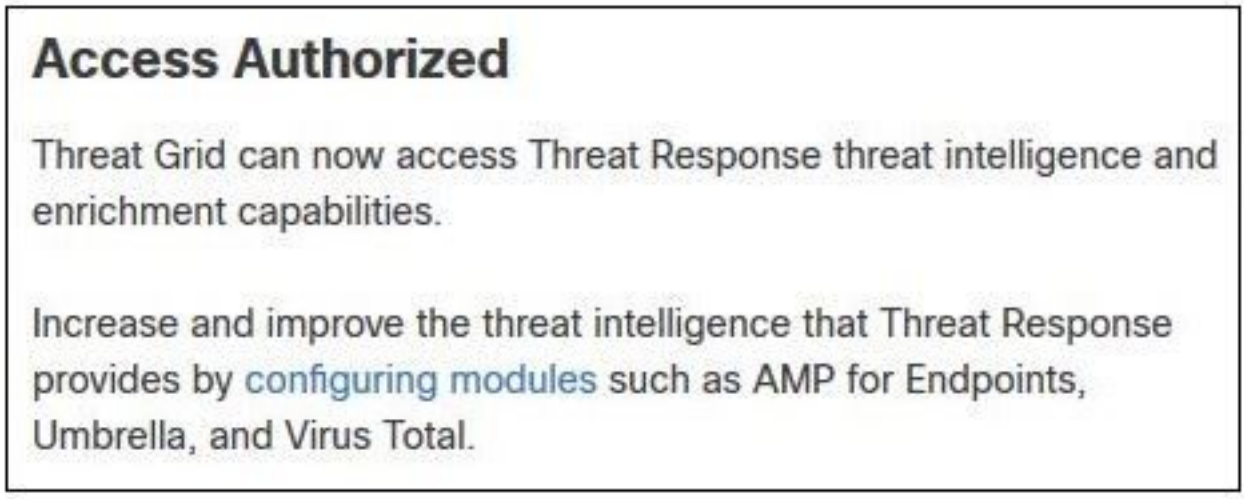
步驟3.導覽至Connections部分並選擇**Connect Threat Response選項，如下圖所示。**

步驟4.選擇Authorize選項以允許Threat Grid訪問思科威脅響應，如下圖所示。

步驟5.選擇Authorize Threat Grid選項以授予應用程式訪問許可權，如下圖所示。



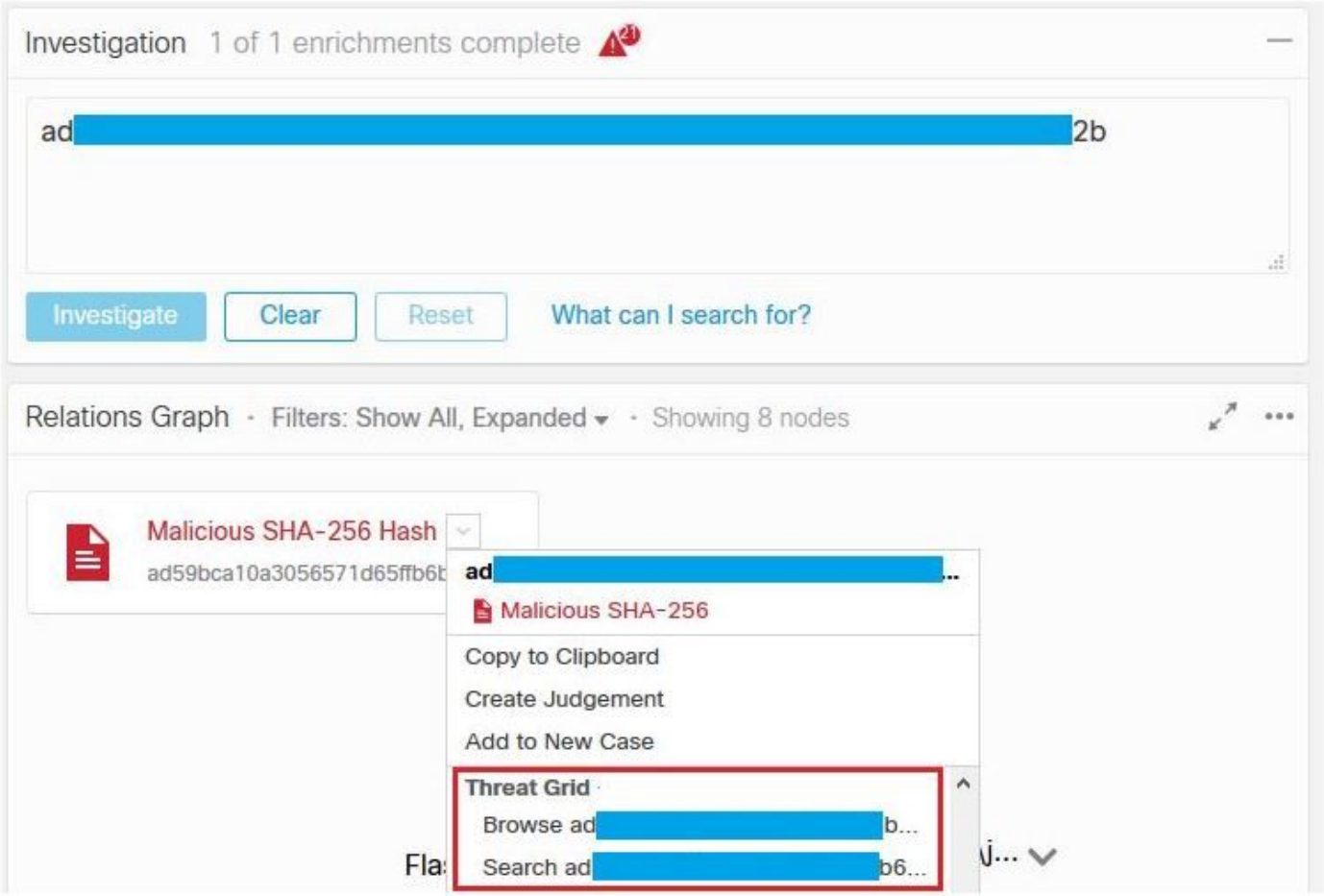
步驟6.出現「Access Authorized（訪問授權）」消息，以驗證Threat Grid是否可以訪問威脅響應威脅情報和增強功能，如下圖所示。



驗證

使用本節內容，確認您的組態是否正常運作。

為了驗證CTR和TG整合，您可以在CTR控制檯上執行**Investigation**，當所有**Investigation**詳細資訊顯示時，您可以看到Threat Grid選項，如下圖所示。



您可以選擇Browse或Search Threat Grid選項，並將其重定向到Threat Grid Portal中，以收集有關Threat Grid知識庫中的檔案/雜湊/IP/域/URL的其他資訊，如下圖所示。