CTRとThreat Gridクラウドの統合

内容

概要

このドキュメントでは、CTR調査を実行するために、Cisco Threat Response(CTR)をThreat Grid(TG)クラウドに統合する手順について説明します。

著者：Cisco TACエンジニア、Yeraldin Sanchez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Threat Response
- Threat Grid

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- CTRコンソール（管理者権限を持つユーザアカウント）
- Threat Gridコンソール（管理者権限を持つユーザアカウント）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Threat Gridは、高度で自動化されたマルウェア分析およびマルウェア脅威インテリジェンスプラットフォームで、ユーザ環境に影響を与えることなく、疑わしいファイルやWeb宛先を爆

発的に増加させることができます。

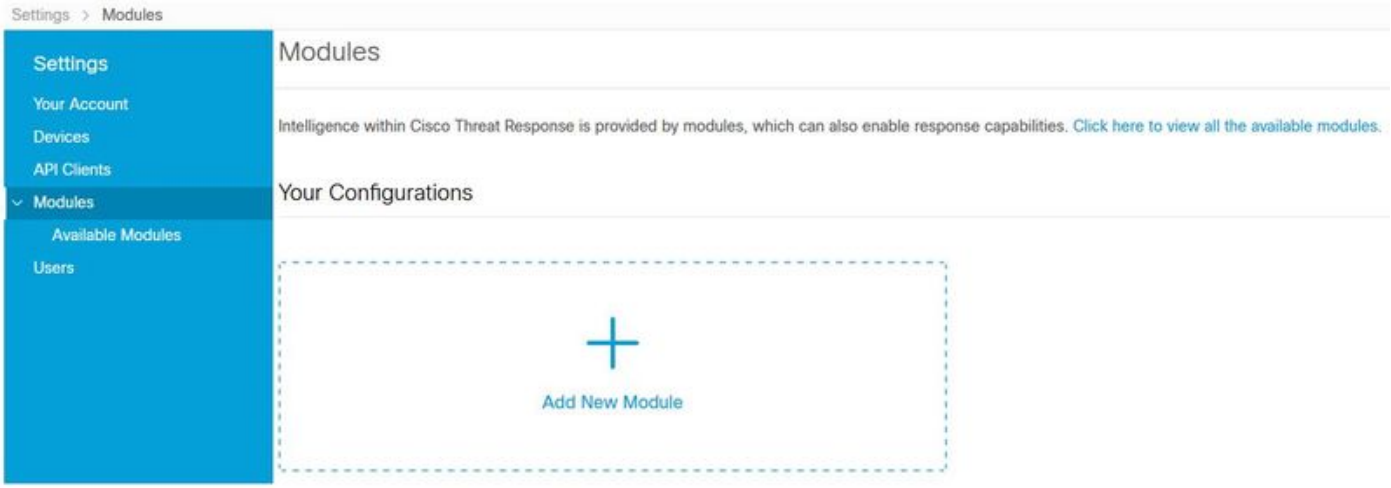
Cisco Threat Responseとの統合では、Threat Gridはリファレンスモジュールであり、Threat Gridポータルにピボットして、ファイルハッシュ、IP、ドメイン、およびURLに関する追加情報をThreat Gridナレッジストアに収集する機能を提供します。

設定

CTRコンソール：Threat Gridモジュールの設定

ステップ1：管理者の資格情報を使用して[Cisco Threat Responseに](#)ログインします。

ステップ2：図に示すように、[Modules]タブに移動し、**[Modules] > [Add New Module]**を選択します。



ステップ3：図に示すように、[Available Modules（利用可能なモジュール）]ページの[Threat Grid(脅威グリッドモジュール)]ペインで[Add New Module（新しいモジュールの追加）]を選択します。

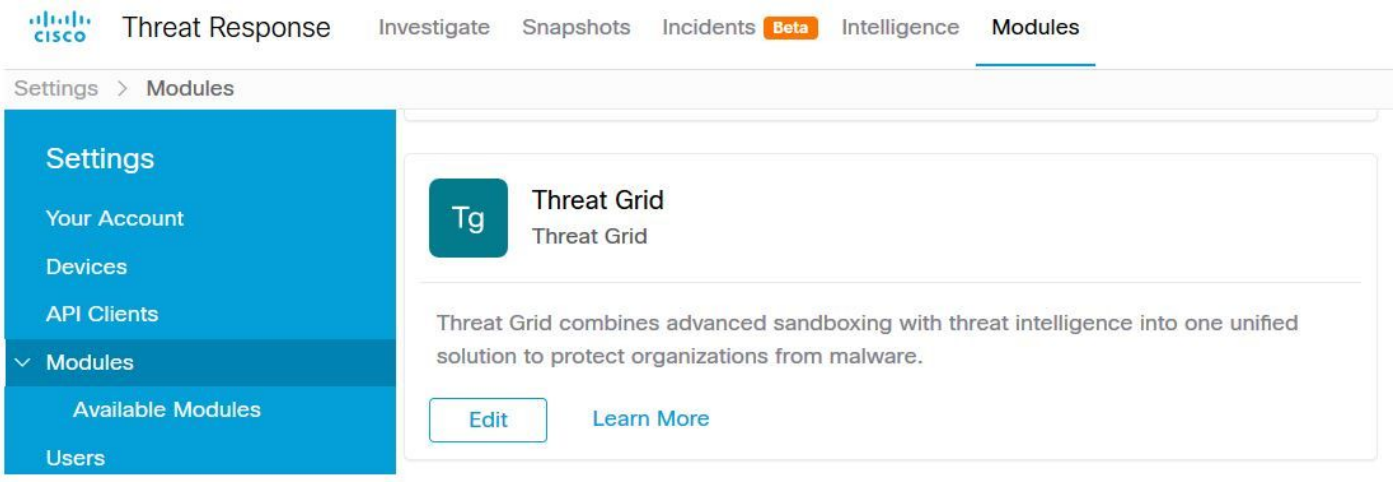
ステップ4:[Add **New Module]フォームが**開きます。図に示すように、フォームに入力します。

- **モジュール名**：デフォルトの名前をそのまま使用するか、わかりやすい名前を入力します。
- **URL**：ドロップダウンリストから、Threat Gridアカウントのベースとなる場所（北米またはヨーロッパ）に適したURLを選択します。 [その他]**オプション**は無視してください。

ステップ5:[保存]を選択し、Threat Gridモジュールの構成を完了します。

ステップ6：図に示すように、Threat Gridが構成の下の[モジュー]ページに表示されます。

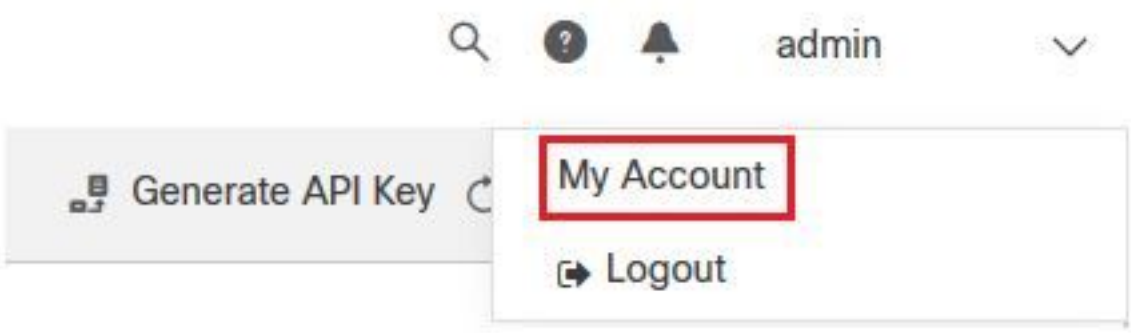
（TGはピボットメニューおよびケースブックから利用でき、脅威の調査が改善されます）。



Threat Gridコンソール – Authorize Threat Grid to access Threat response

ステップ1：管理者の資格情報を使用して Threat Grid**に**ログインします。

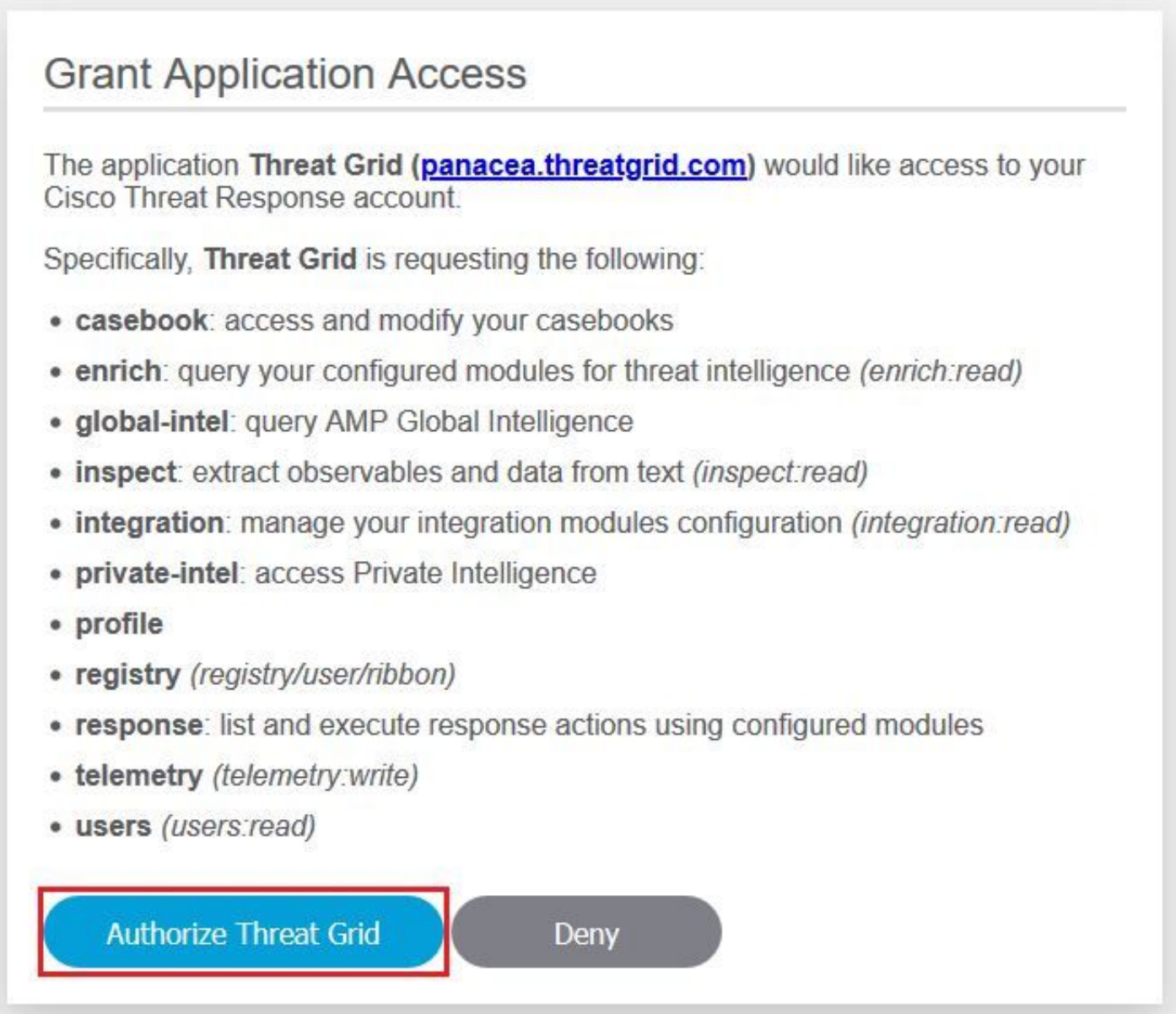
ステップ2：図に示すように、[マイアカウント]セクションに移動します。



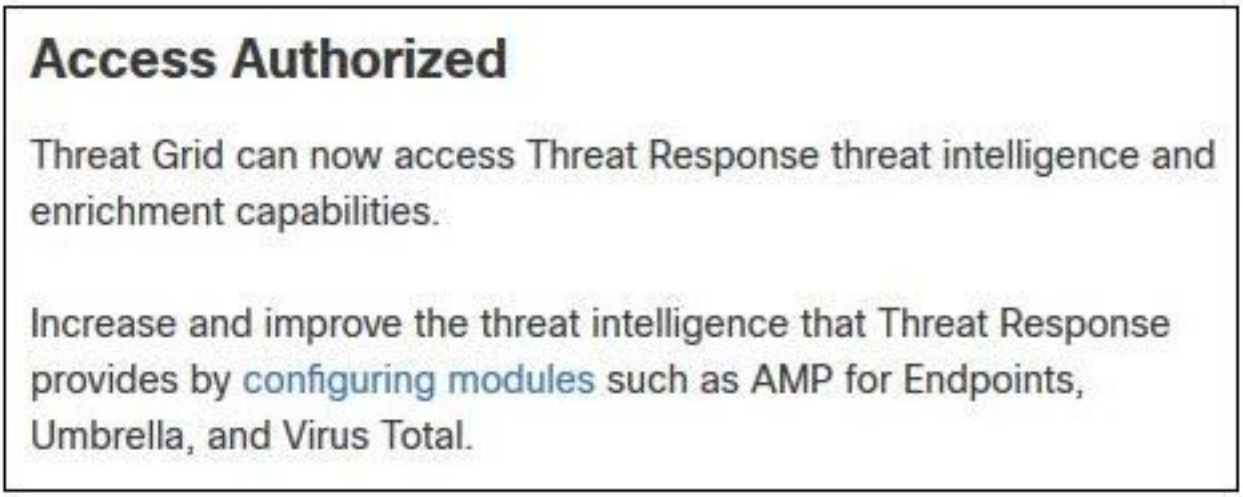
ステップ3：図に示すように、[接続]セクションに移動し、[脅威への接続]オプションを選択します。

ステップ4：図に示すように、Threat GridがCisco Threat Responseにアクセスできるようにするために、[Authorize]オプションを選択します。

ステップ5：図に示すように、アプリケーションアクセスを許可するには、[Authorize Threat Grid]オプションを選択します。



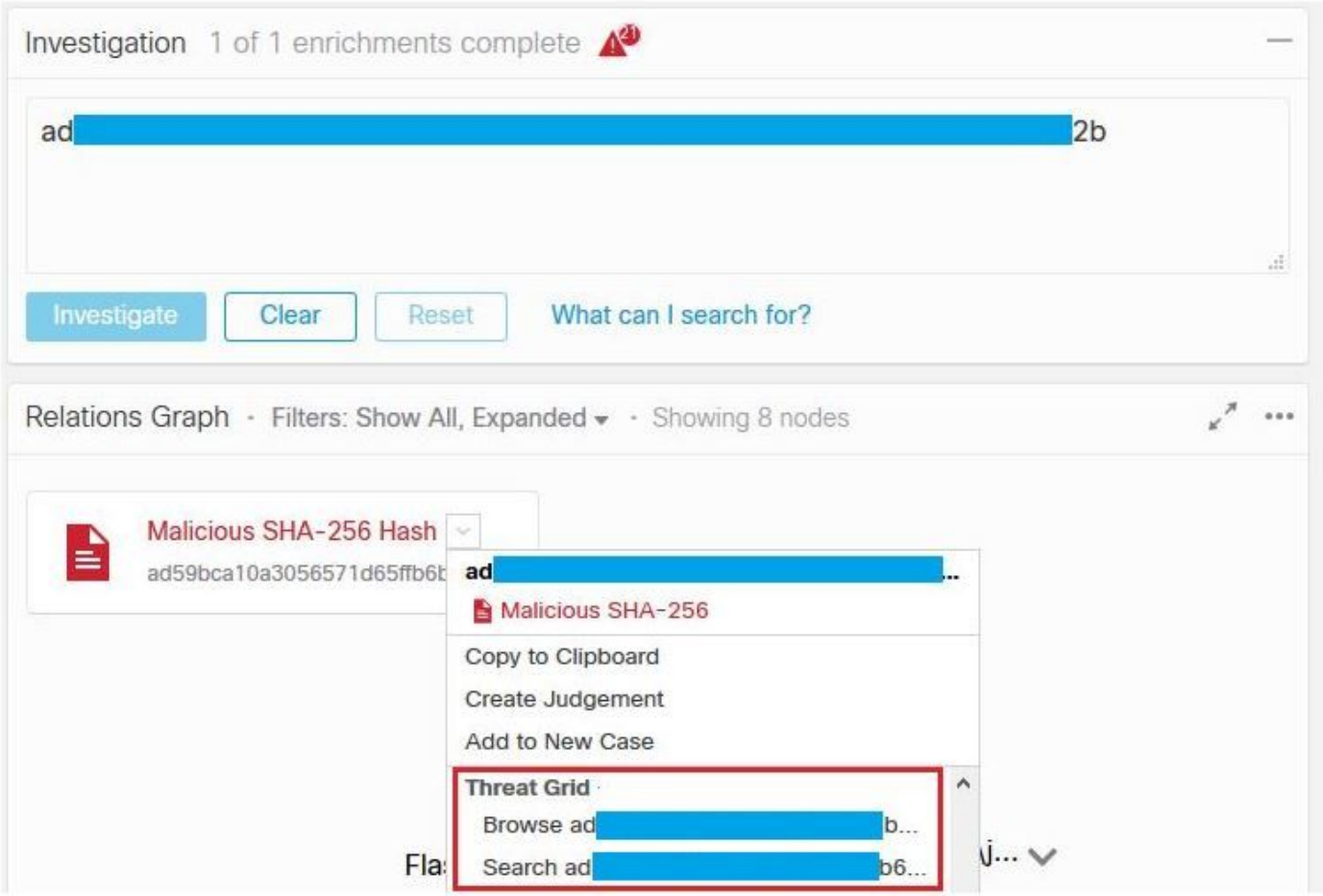
ステップ6：アクセス認可メッセージは、図に示すように、Threat GridがThreat Response脅威インテリジェンスおよびエンリッチメント機能にアクセスできることを確認するために表示されます。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

CTRとTGの統合を確認するには、CTRコンソールで調査を実行します。すべての調査の詳細が表示されれば、図のように[Threat Grid]オプションを表示できます。



[Browse or Search Threat Grid]オプションを選択すると、Threat Gridポータルにリダイレクトされ、図に示すように、Threat Gridナレッジストアのファイル、ハッシュ、IP、ドメイン、URLに関する追加情報を収集できます。