CTRをUmbrellaにリンクする方法を理解する

内容

はじめに

このドキュメントでは、Cisco Threat Response(CTR)ポータルをCisco Umbrellaに接続する方法と、必要なすべての前提条件について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

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、クリアな（デフォルト）設定で作業を開始しています。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。

概要

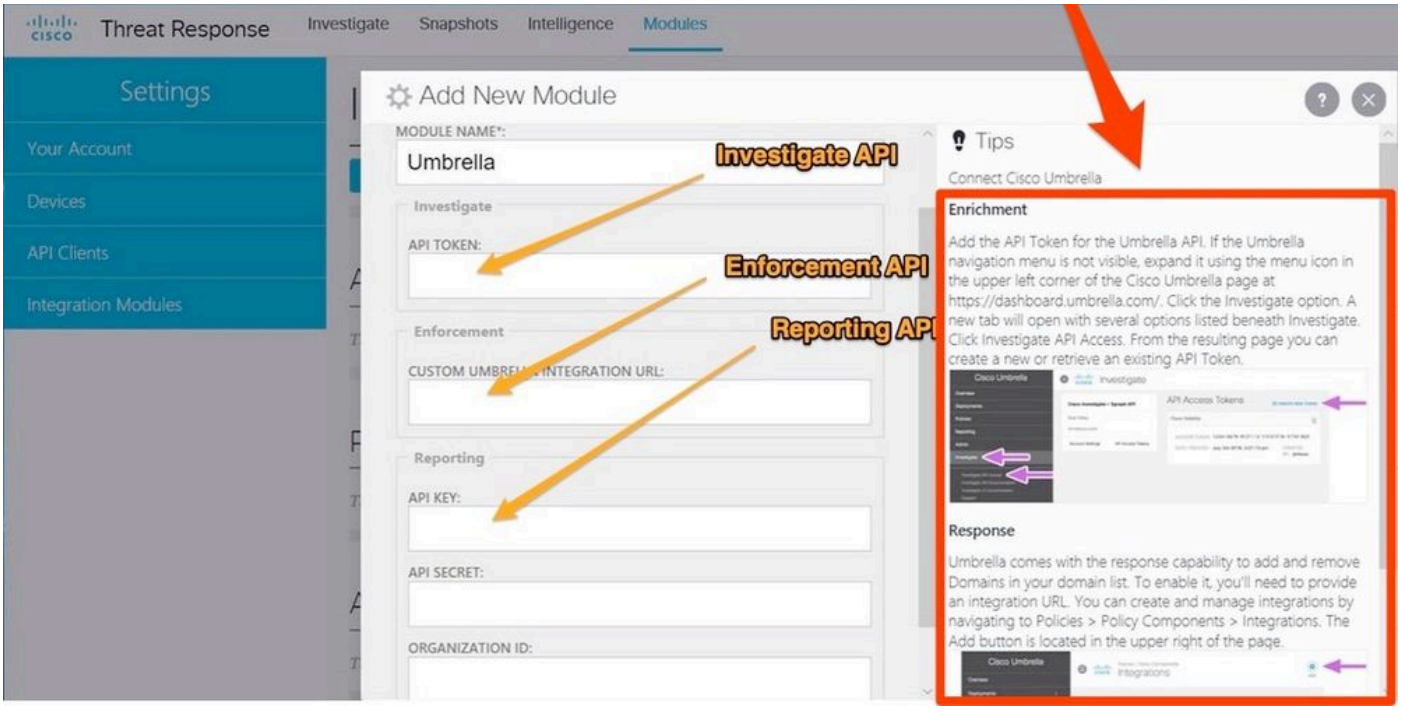
この記事では、CTRポータルをUmbrellaに接続する方法と、この接続を行うために必要なすべての前提条件について説明します。CTRは、次の3つのUmbrellaコンポーネントでリンクします。

- 調査(Cisco Umbrellaサブスクリプションが必要)
- 適用(Enforcement APIにアクセスできるCisco Umbrellaサブスクリプションへの昇格が必要)

- レポート

UmbrellaへのCTRリンクの設定

CTRをUmbrellaにリンクするには、Umbrellaサブスクリプションのレベルに応じて最大3つの手順を実行します。リンクページは次のスクリーンショットのようになります。



360034168072

CTRへのUmbrellaレポートのリンク

すべてのUmbrellaユーザは、レポートAPIにアクセスできます。開始するには、APIキーとシークレットが必要です。API認証の詳細を調べる方法については、Umbrella APIのドキュメントを参照してください。最後に、CTRにリンクするUmbrella組織の組織IDを入力します。

要件

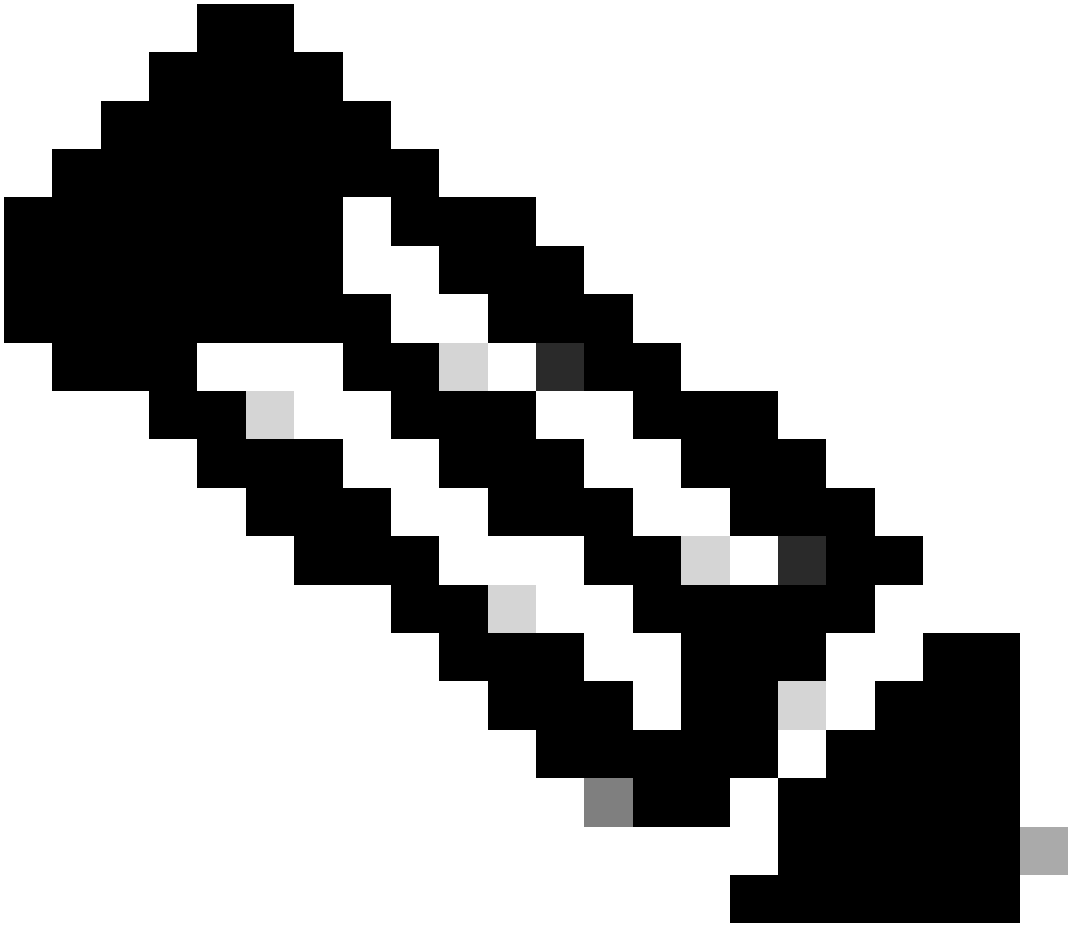
- Umbrellaサービスに登録します。

CTRへのUmbrella強制のリンク

Umbrella Enforcement APIは、セキュリティ適用リストへの新しいドメインの自動追加を可能にする機能です。詳細については、Umbrellaのドキュメントを参照してください。

要件

- ダッシュボードのEnforcement APIにアクセスして、Umbrellaサービスに登録します。



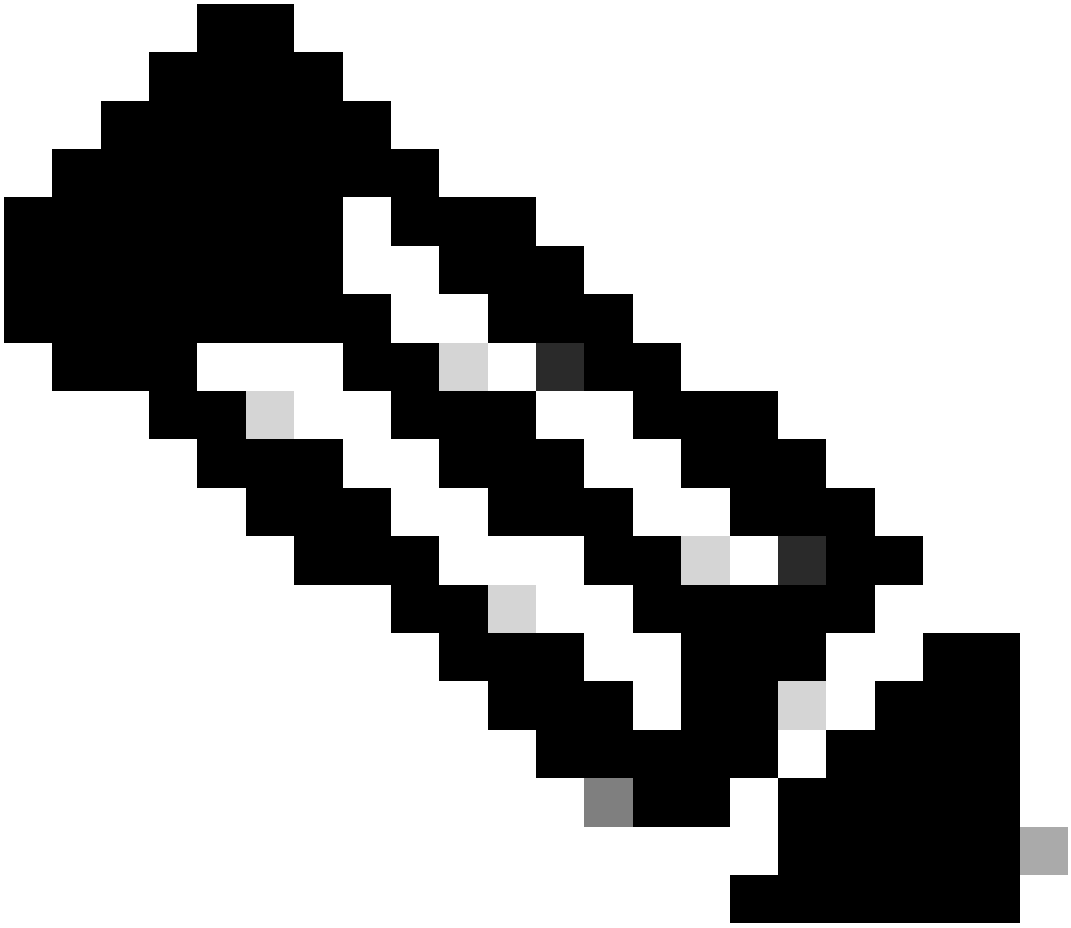
注:Umbrellaダッシュボードにカスタム統合用のUmbrella Enforcement APIがなく、アクセス権が必要な場合は、Cisco Umbrellaの担当者にお問い合わせください。

Umbrella InvestigateからCTRへのリンク

Umbrella Investigate APIは、Investigate Webポータルの外部でCisco Umbrella Investigateシステムに対するクエリを可能にする機能です。APIアクセスは制限されています。詳細については、Umbrellaのドキュメントを参照してください。

要件

- Cisco Umbrella Investigate(https://investigate.umbrella.com)に登録します。
  - Investigate APIのパッケージまたはアドオンがアクティブである必要があります。
  - 一部の権限では、少量のクエリを実行できます。CTRは、クエリーの上限に達するまで機能し続けることができます。



注:Umbrellaダッシュボードにカスタム統合用のUmbrella Enforcement APIがなく、アクセス権が必要な場合は、Cisco Umbrellaの担当者にお問い合わせください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。