ThreatConnectとUmbrellaの統合

内容

はじめに

このドキュメントでは、ThreatConnectをCisco Umbrellaと統合する方法について説明します。

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。

- 統合用にURLを更新するためのアクセス権を持つThreatConnectダッシュボード
- Umbrellaダッシュボードの管理者権限
- Umbrellaダッシュボードでは、ThreatConnect統合が有効になっている必要があります。

使用するコンポーネント

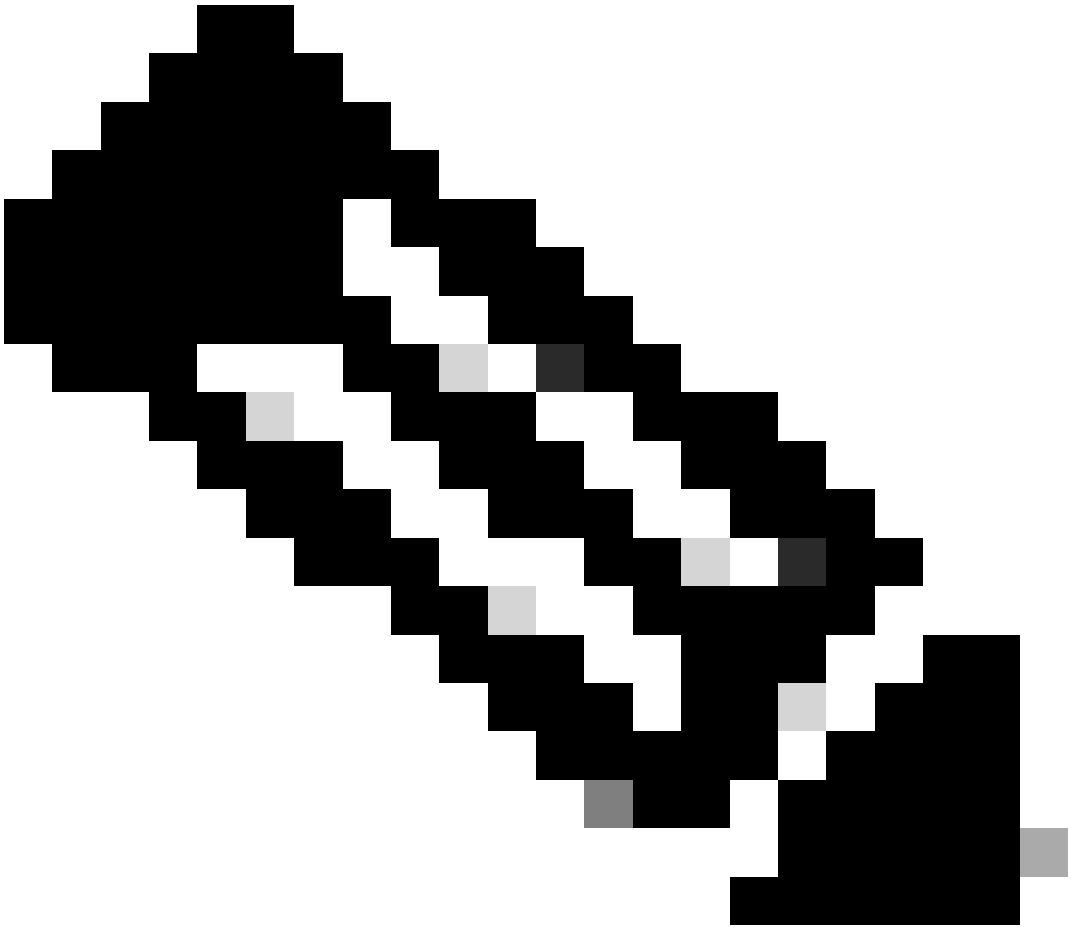
このドキュメントの情報は、Cisco Umbrellaに基づくものです。

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。

ThreatConnectとCisco Umbrellaの統合の概要

ThreatConnectをCisco Umbrellaと統合することで、セキュリティ担当者と管理者は、分散した企業ネットワークに別の適用レイヤを提供しながら、ローミングするラップトップ、タブレット、または電話に対する高度な脅威に対する保護を拡張できます。

このガイドでは、Cisco Umbrellaと通信するようにThreatConnectを設定し、ThreatConnect TIPからのセキュリティイベントを、Cisco Umbrellaによって保護されているクライアントに適用可能なポリシーに統合する方法について説明します。



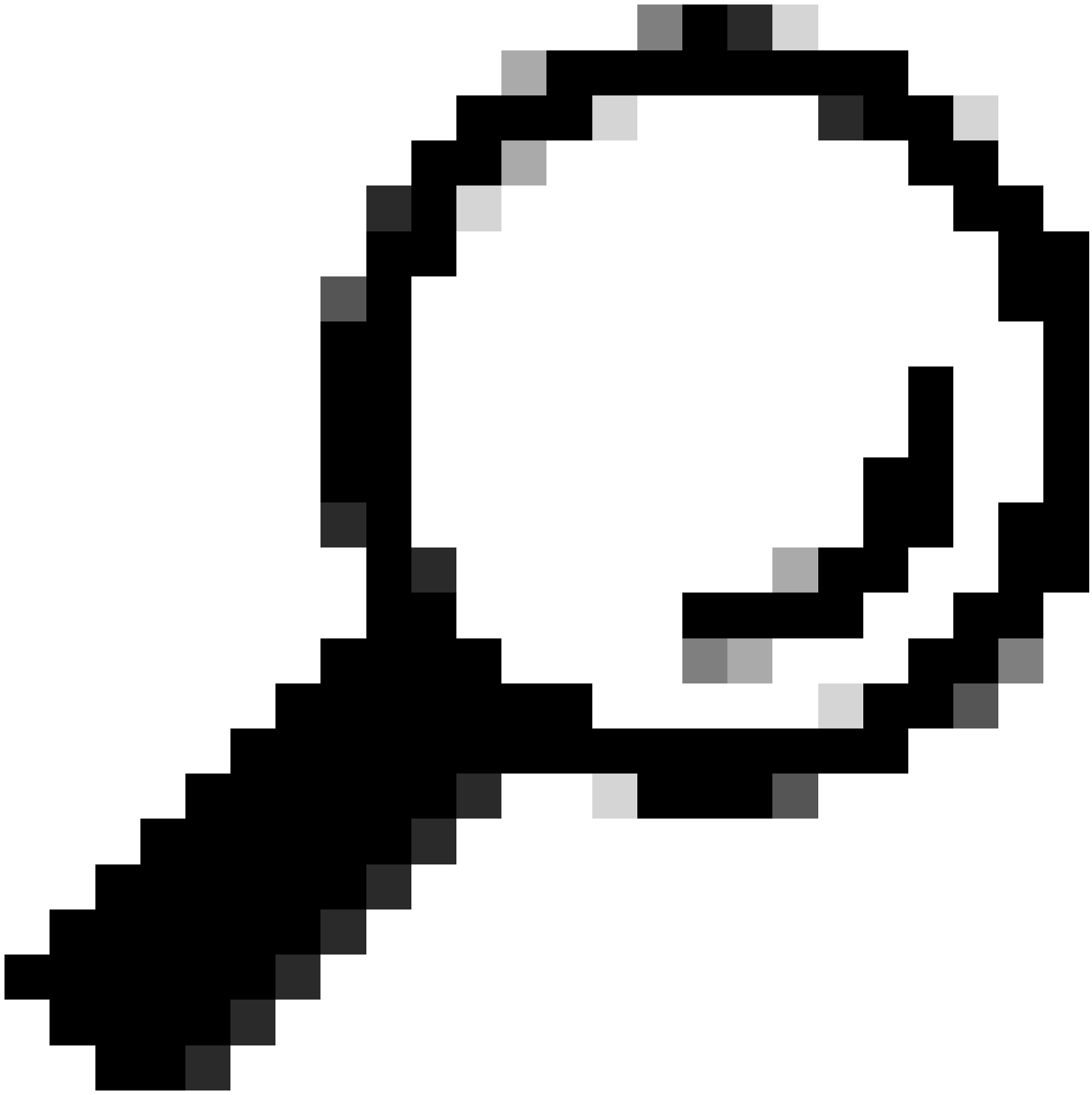
注:ThreatConnectの統合は、特定のCisco Umbrellaパッケージにのみ含まれています。この統合を含むパッケージがない場合は、Cisco Umbrellaの担当者に連絡して入手してくだ

さい。正しいパッケージがあっても、ダッシュボードの統合としてThreatConnectが表示されない場合は、Cisco Umbrellaサポートにお問い合わせください。

ThreatConnectプラットフォームはまず、検出されたサイバー脅威インテリジェンス（マルウェアをホストするドメイン、ボットネットまたはフィッシングサイトのコマンドと制御など）をUmbrellaに送信します。

その後、Umbrellaは脅威を検証し、ポリシーに追加できることを確認します。ThreatConnectからの情報が脅威であることが確認されると、任意のUmbrellaポリシーに適用できるセキュリティ設定の一部として、ドメインアドレスがThreatConnect宛先リストに追加されます。このポリシーは、ThreatConnect宛先リストのポリシーを使用してデバイスから行われるすべての要求に即座に適用されます。

今後、UmbrellaはThreatConnectのアラートを自動的に解析し、悪意のあるサイトをThreatConnectの接続先リストに追加します。これにより、すべてのリモートユーザとデバイスに対してThreatConnectの保護が拡張され、企業ネットワークに対して新たな適用レイヤが提供されます。



ヒント:Umbrellaは、一般的に安全であることが知られているドメイン（GoogleやSalesforceなど）を検証して許可するために最善を尽くしますが、意図しない中断を避けるために、Umbrellaはポリシーに従ってブロックされないようにするドメインをグローバル許可リストまたはその他の宛先リストに追加することを提案しています。次に例を示します。

- 組織のホームページ。たとえば、mydomain.comなどです。
- 内部レコードと外部レコードの両方を持つことができる、提供するサービスを表すドメイン。たとえば、mail.myservicedomain.comやportal.myotherservicedomain.comなどです。
- あまり知られていないクラウドアプリケーションに大きく依存しているが、Umbrellaが認識していない、または自動ドメイン検証に含まれていない。たとえば、localcloudservice.comなどです。

グローバル許可リストは、UmbrellaのPolicies > Destination Listsにあります。詳細につい

ては、次のドキュメントを参照してください。通知先リストの管理

ThreatConnectからイベントを受信するためのUmbrellaダッシュボードの設定

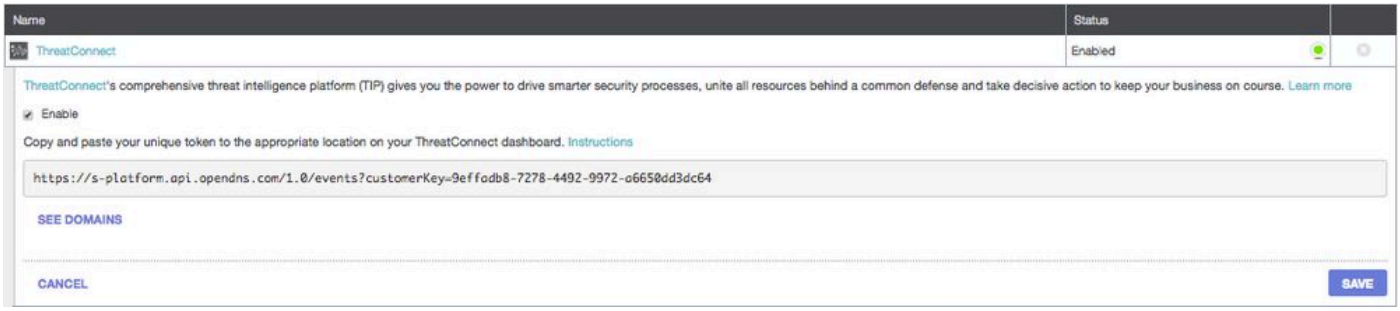
まず、ThreatQアプライアンスと通信するための固有のURLをUmbrellaで検索します。

1. Umbrellaダッシュボードにログインします。

2. 「ポリシー」>「統合」 にナビゲートします。

3. テーブルで、ThreatConnectを選択して展開します。

4. Enableを選択し、次にSaveを選択します。これにより、Umbrella内の組織に固有の固有のURLが生成されます。



データをUmbrellaに送信するようにThreatConnectを設定する場合は、この記事の後半で説明するURLが必要です。

Umbrellaと通信するためのThreatConnectの設定

ThreatConnectからUmbrellaへのトラフィックの送信を開始するには、この記事の最初のセクションで生成されたURL情報を使用してThreatConnectを設定する必要があります。

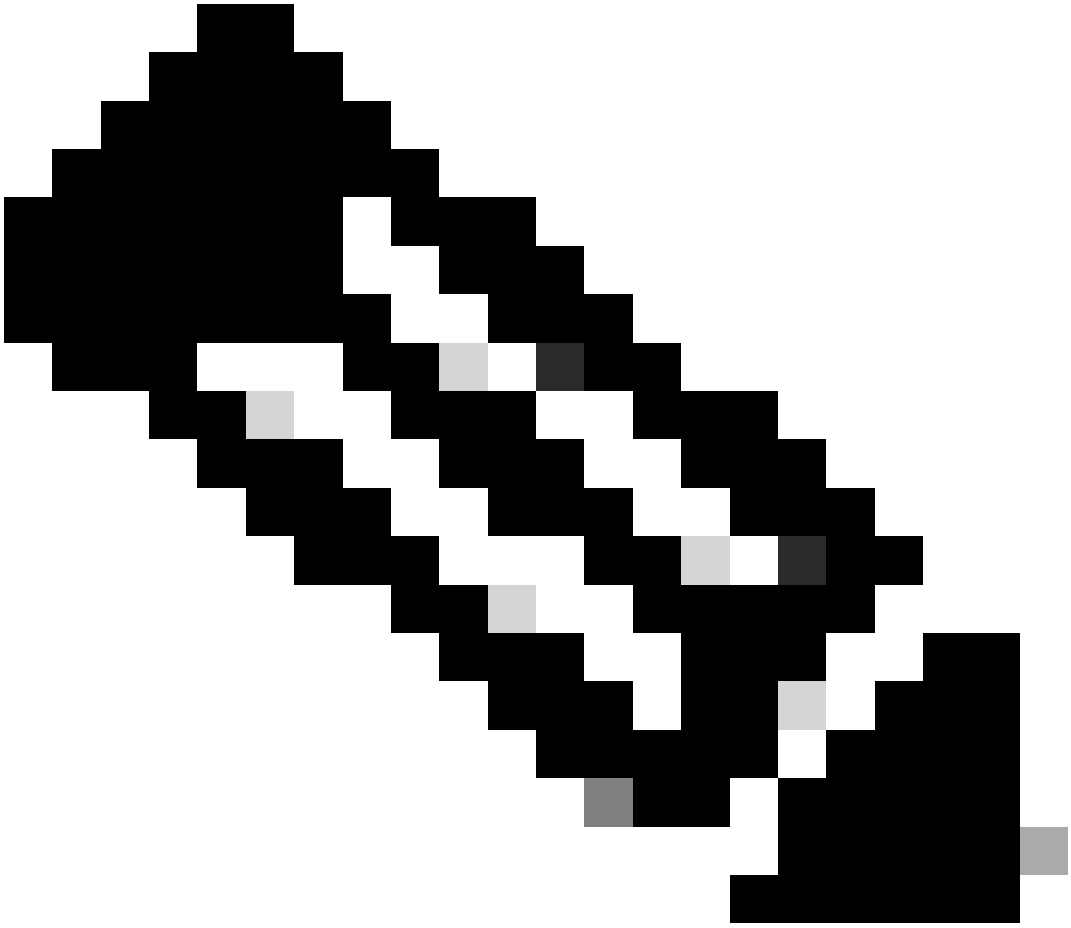
1. ThreatConnectダッシュボードにログインします。

2. Umbrellaに接続するための適切なエリアにURLを追加します。

正確な手順は異なるため、ThreatConnect内でAPI統合を設定する方法や場所が不明な場合は、UmbrellaからThreatConnectサポートに連絡することをお勧めします。

監査モードでThreatConnectセキュリティカテゴリに追加されたイベントを確認する

ThreatConnectダッシュボードからのイベントは、時間の経過とともに、ThreatConnectセキュリティカテゴリとしてポリシーに適用できる特定の宛先リストへの入力を開始できます。デフォルトでは、宛先リストとセキュリティカテゴリは監査モードになっています。これは、これらのリストがポリシーに適用されず、既存のUmbrellaポリシーが変更されないことを意味します。



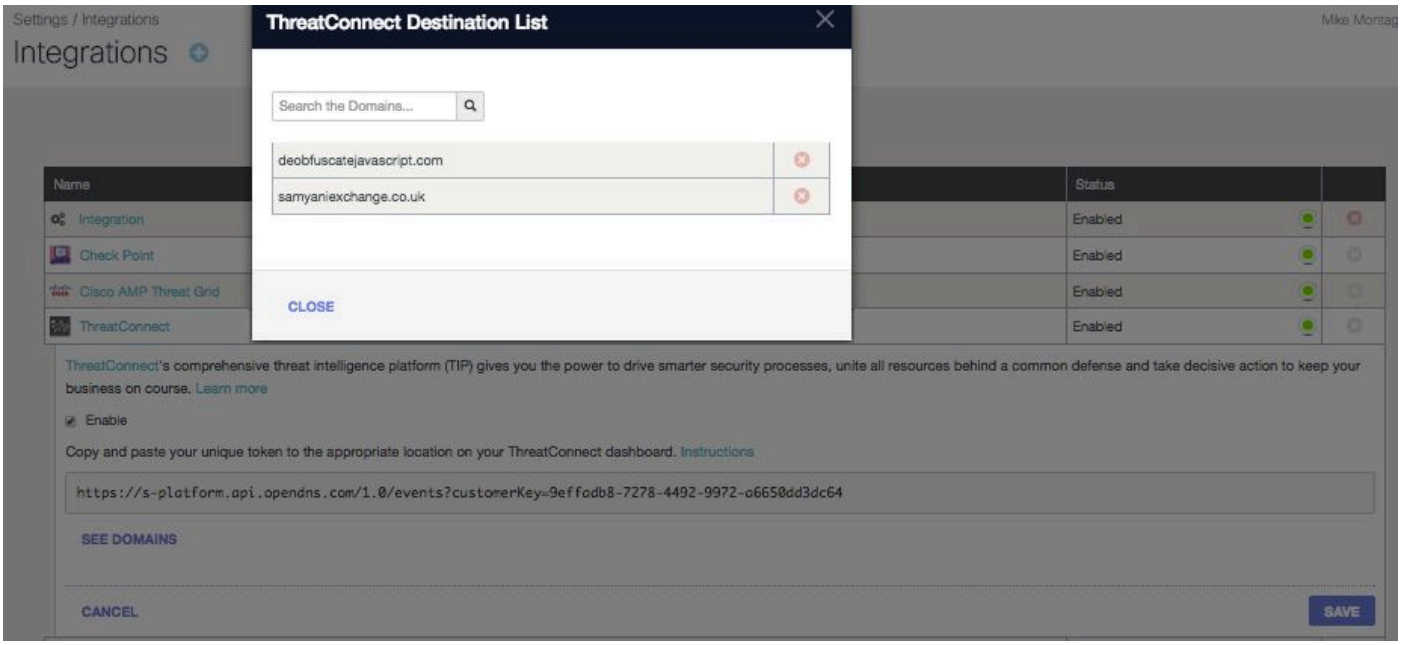
注：監査モードは、導入プロファイルとネットワーク設定に基づいて、必要な期間だけ有効にできます。

宛先リストの確認

UmbrellaのThreatConnect宛先リストは、次の操作を行うことによって、いつでも確認できます。

1. Umbrellaダッシュボードで、Policies > Integrationsの順に移動します。

2. テーブルで、ThreatConnectを展開し、See Domainsを選択します。



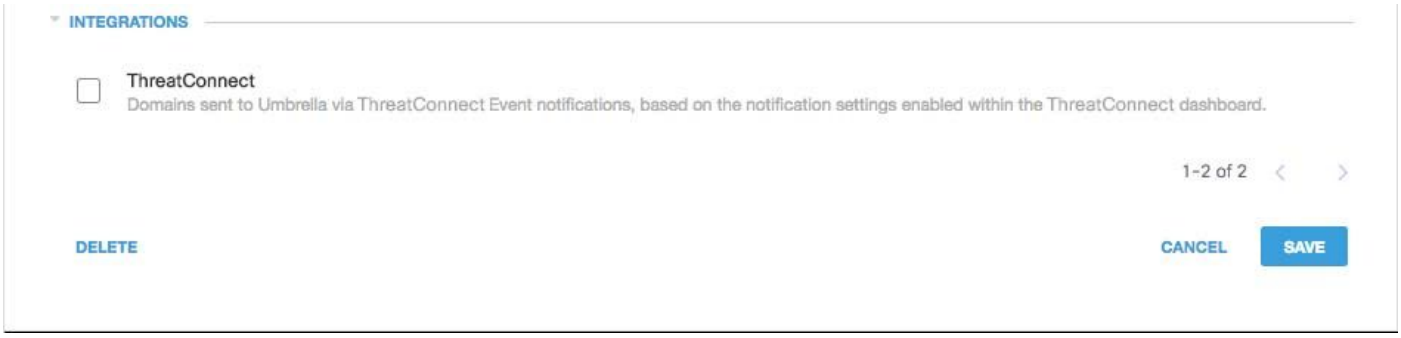
ポリシーのセキュリティ設定の確認

ポリシーに対して有効にできるセキュリティ設定は、いつでも確認できます。

1. Umbrellaダッシュボードで、Policies > Security Settingsの順に移動します。

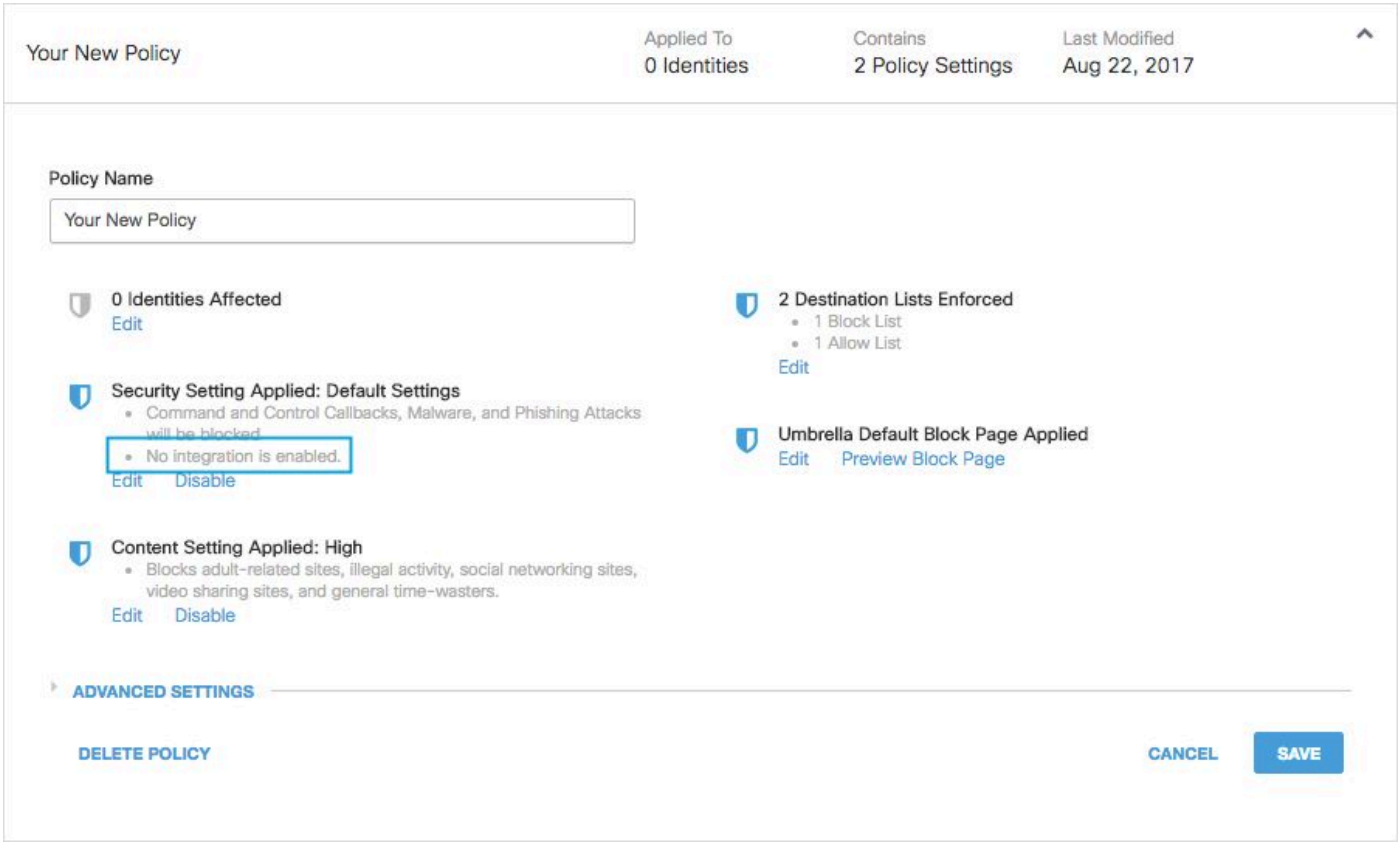
2. 表内のセキュリティ設定を選択して展開します。

3. Integrationsまでスクロールし、ThreatConnect 設定を見つけます。



115014036566

4. 「セキュリティ設定の概要」ページで統合情報を確認することもできます。



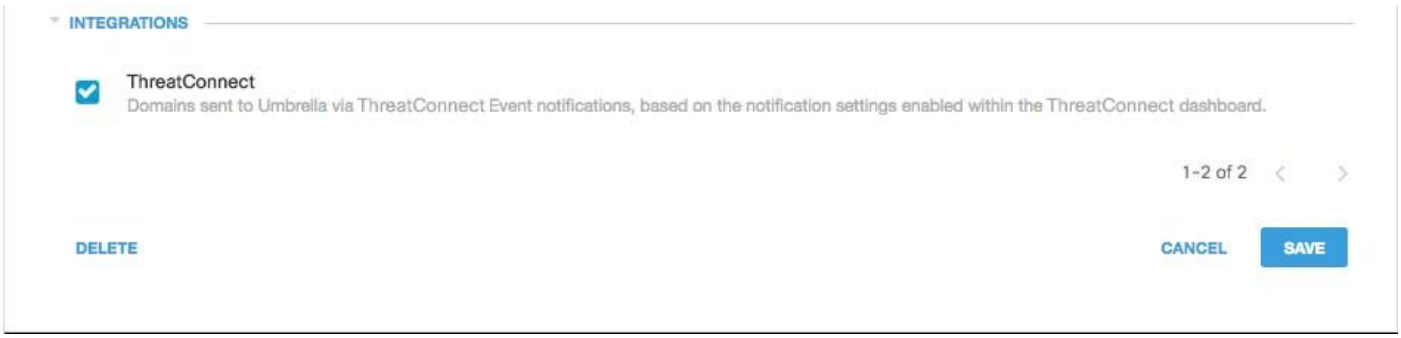
25464103885972

ブロックモードでのThreatConnectセキュリティ設定の管理対象クライアント用ポリシーへの適用

Umbrellaによって管理されるクライアントによってこれらの追加のセキュリティ脅威を適用する準備ができたら、既存のポリシーのセキュリティ設定を変更するか、最初に確実に適用されるようにデフォルトポリシーの上に配置する新しいポリシーを作成します。

1. [ポリシー] > [セキュリティの設定] に移動します。

2. Integrationsで、ThreatConnectを選択し、Saveを選択します。



115014203703

次に、ポリシーウィザードで、編集中のポリシーにセキュリティ設定を追加します。

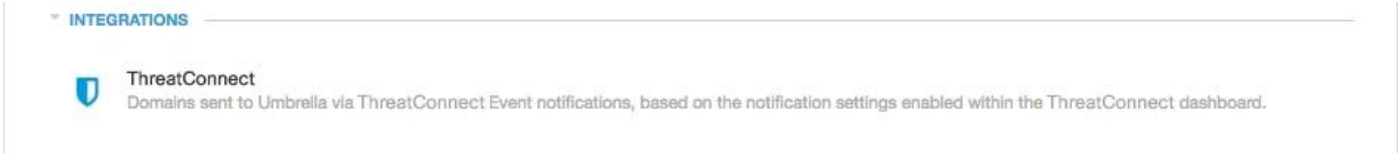
1. Policies > Policy Listの順に移動します。

2. ポリシーを展開します。Security Setting Appliedの下で、Editを選択します。

3. [セキュリティの設定] ドロップダウンで、ThreatConnect 設定を含むセキュリティ設定を選択します。

25464103908884

Integrationsの下のシールドアイコンが青色に更新されます。



115014037666

4. Set & Returnを選択します。

その後、ThreatConnectのセキュリティ設定内に含まれるThreatConnectドメインは、ポリシーを使用してIDに対してブロックされます。

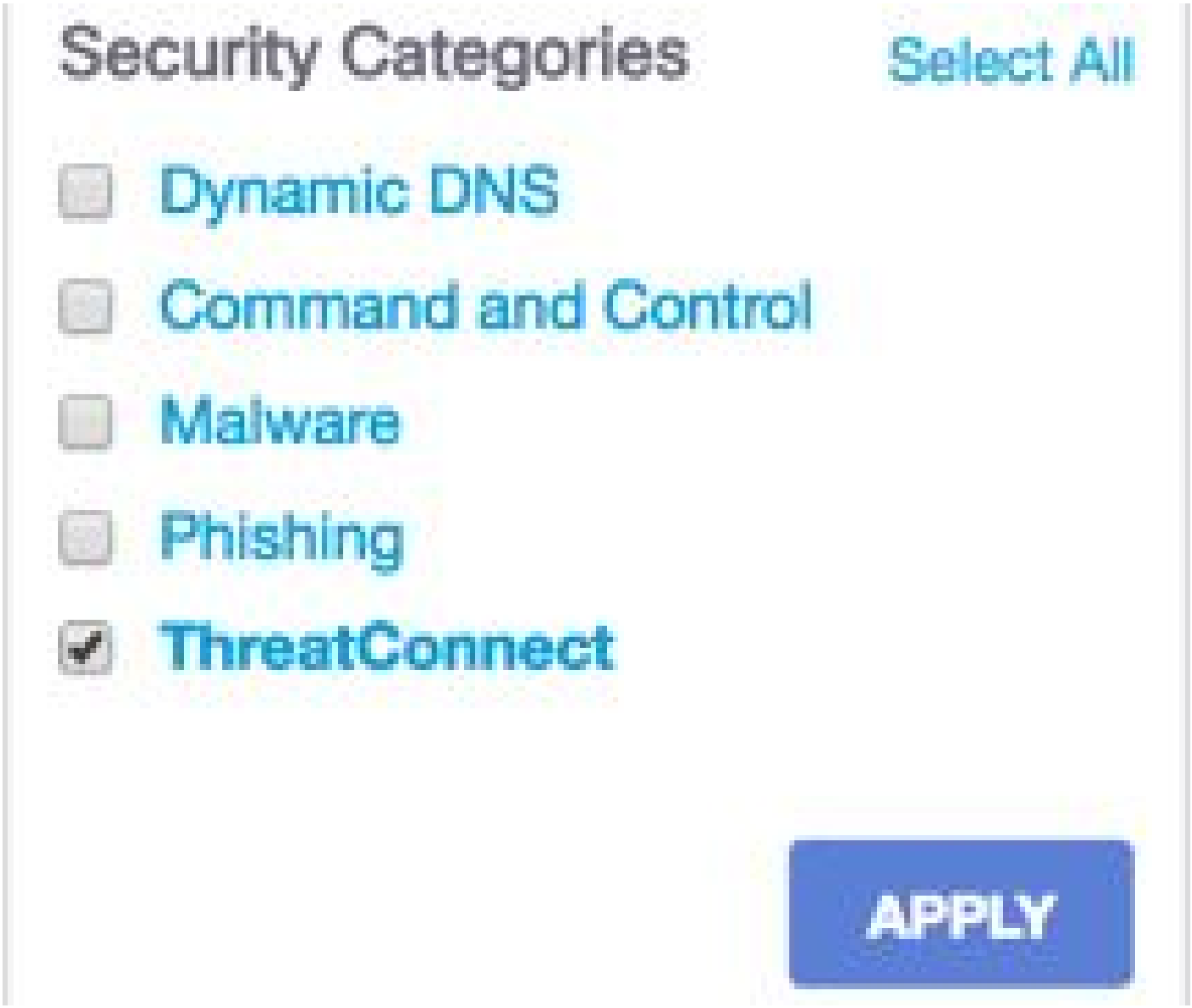
ThreatConnectイベントの包括的なレポート

ThreatConnectセキュリティイベントのレポート

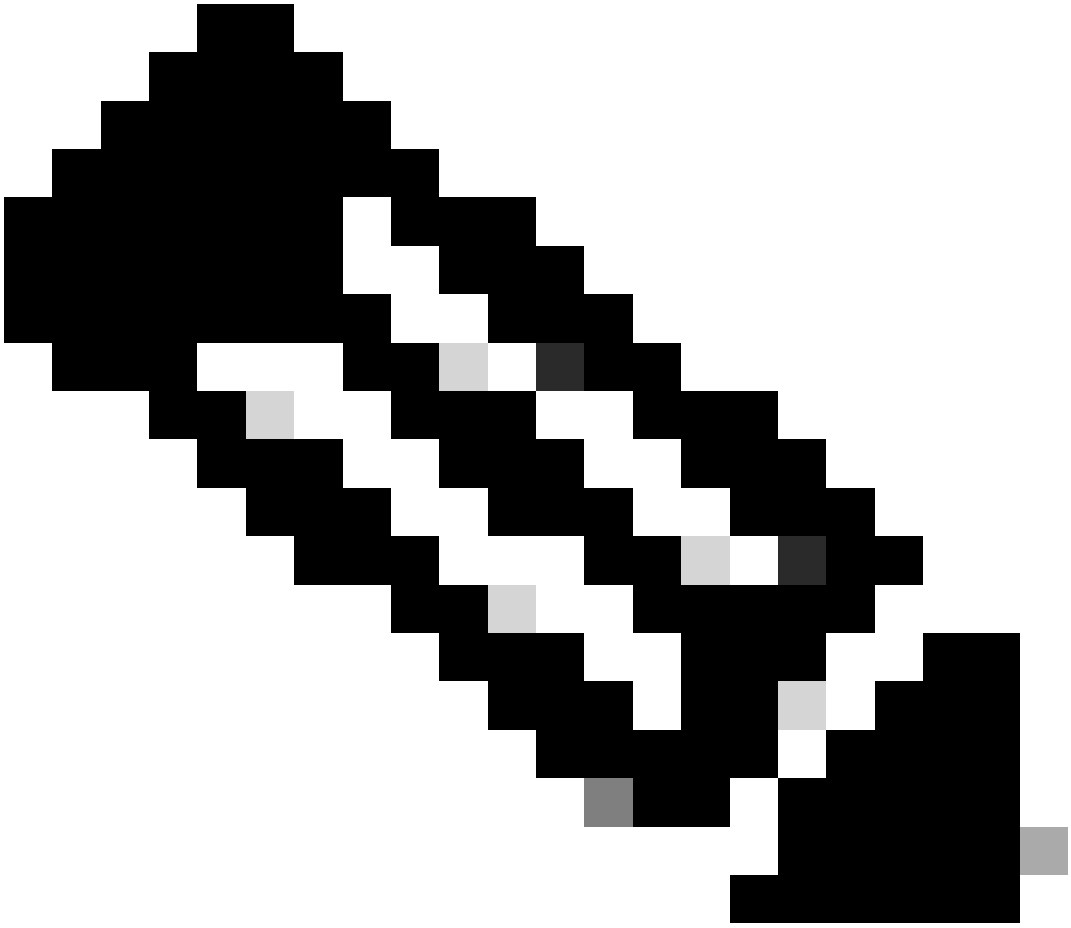
ThreatConnectの宛先リストは、レポートを作成できるセキュリティカテゴリリストの1つです。ほとんどのレポートまたはすべてのレポートでは、セキュリティカテゴリがフィルタとして使用されます。 たとえば、セキュリティカテゴリをフィルタリングして、ThreatConnect関連のアクティビティのみを表示できます。

1.「レポート」 >「活動検索」にナビゲートします。

2. Security Categoriesの下で、ThreatConnectを選択して、ThreatConnectのセキュリティカテゴリのみを表示するようにレポートをフィルタリングします。



115014206603



注:ThreatConnect統合が無効になっている場合、セキュリティカテゴリフィルタには表示されません。

3. Applyを選択します。

ドメインがThreatConnect宛先リストに追加されたときのレポート

管理監査ログには、宛先リストにドメインを追加する際のThreatConnectダッシュボードからのイベントが含まれます。ThreatConnectロゴが付いた「ThreatConnectアカウント」という名前のユーザがイベントを生成します。これらのイベントには、追加されたドメインと追加時刻が含まれます。

「ThreatConnectアカウント」ユーザのフィルタを適用することで、ThreatConnectの変更のみを含めるようにフィルタリングできます。

不要な検出や誤検出の処理

許可リスト

まれに、ThreatConnectによって自動的に追加されたドメインによって不要なブロックがトリガーされ、ユーザが特定のWebサイトにアクセスできなくなる可能性があります。このような状況では、Umbrellaは許可リストにドメインを追加することを推奨します。許可リストは、セキュリティ設定を含む他のすべてのタイプのブロックリストよりも優先されます。

このアプローチが望ましい理由は、次の2つです。

- まず、ThreatConnectダッシュボードが削除された後にドメインを再度追加した場合、許可リストは、さらなる問題を引き起こすものから保護します。
- また、許可リストには、調査または監査レポートに使用できる問題のあるドメインの履歴レコードが表示されます。

デフォルトでは、すべてのポリシーに適用されるグローバル許可リストがあります。グローバル許可リストにドメインを追加すると、ドメインはすべてのポリシーで許可されます。

ブロックモードのThreatConnectセキュリティ設定が、管理されているUmbrellaのIDのサブセットにのみ適用される場合（たとえば、ローミングコンピューターやモバイルデバイスにのみ適用される場合）、それらのIDまたはポリシーの特定の許可リストを作成できます。

許可リストを作成するには、次の手順を実行します。

1. Policies > Destination Listsの順に移動し、Add (+)アイコンを選択します。

2. Allowを選択して、ドメインをリストに追加します。

3. Saveを選択します。

宛先リストを保存したら、不要なブロックの影響を受けるクライアントをカバーする既存のポリシーに追加できます。

ThreatConnect宛先リストからのドメインの削除

ThreatConnect宛先リストの各ドメイン名の横には削除アイコンが表示されています。ドメインを削除すると、不必要な検出が発生した場合にThreatConnect宛先リストをクリーンアップできます。ただし、ThreatConnectダッシュボードがドメインをUmbrellaに再送信する場合、この削除は永続的にはありません。

ドメインを削除するには

1.「ポリシー」>「統合」にナビゲートします。

2. ThreatConnectを選択して展開します。

3.「ドメインを表示」を選択します。

4. 削除するドメイン名を検索します。

5. 「削除」アイコンを選択します。

6. 「Close」を選択し、次に「Save」を選択します。

不必要な検出または誤検出が発生した場合、Umbrellaは、Umbrellaで許可リストを即座に作成し、ThreatConnectダッシュボード内で誤検出を修復することをお勧めします。後で、ThreatConnectの宛先リストからドメインを削除できます。

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。