ThreatQとUmbrellaの統合

内容

はじめに

このドキュメントでは、ThreatQ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ThreatQ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、ThreatQ統合を有効にする必要があります。

使用するコンポーネント

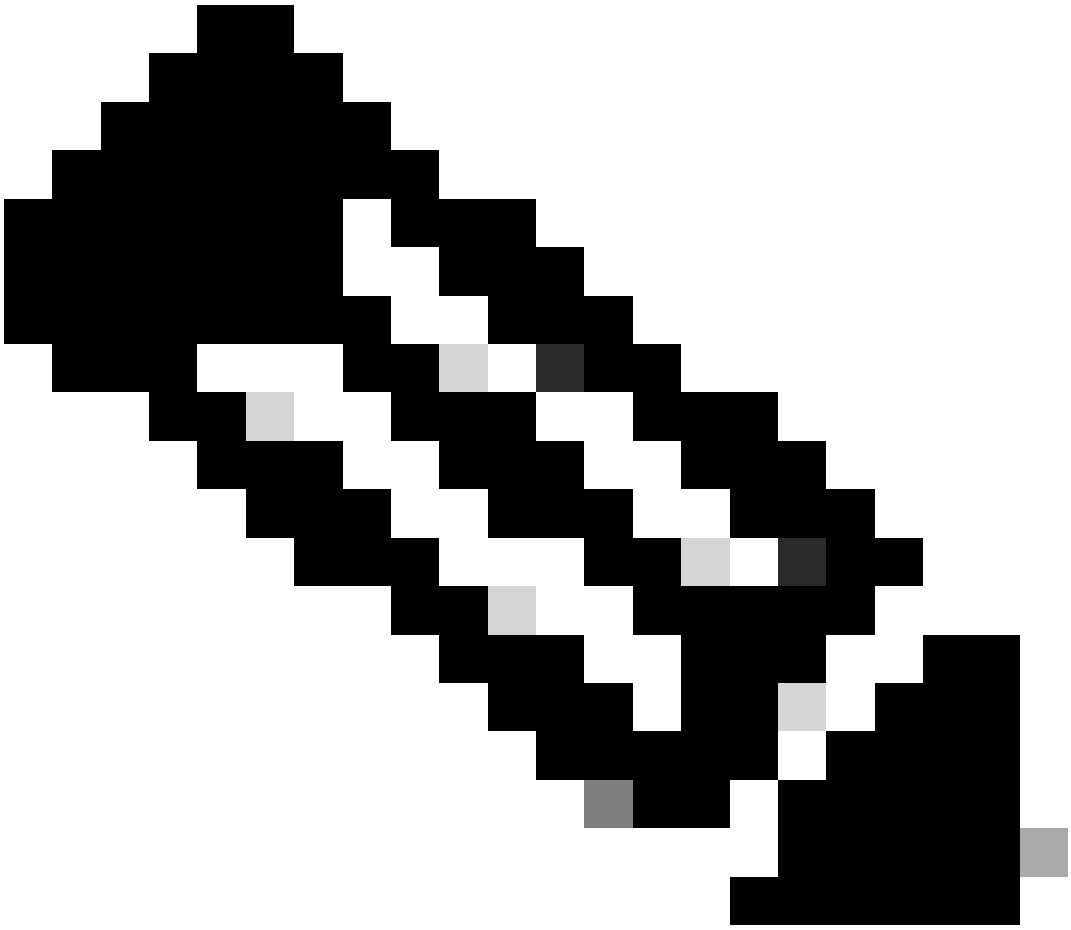
このドキュメントの情報は、Cisco Umbrellaに基づくものです。

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。

ThreatQとCisco Umbrellaの統合の概要

ThreatQ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、ThreatQ 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できるように、ThreatQをUmbrellaと通信するように設定する方法について説明します。



注:ThreatQ統合は、特定のCisco Umbrellaパッケージにのみ含まれます。必要なパッケージがなく、ThreatQの統合が必要な場合は、Cisco Umbrellaの担当者にお問い合わせくだ

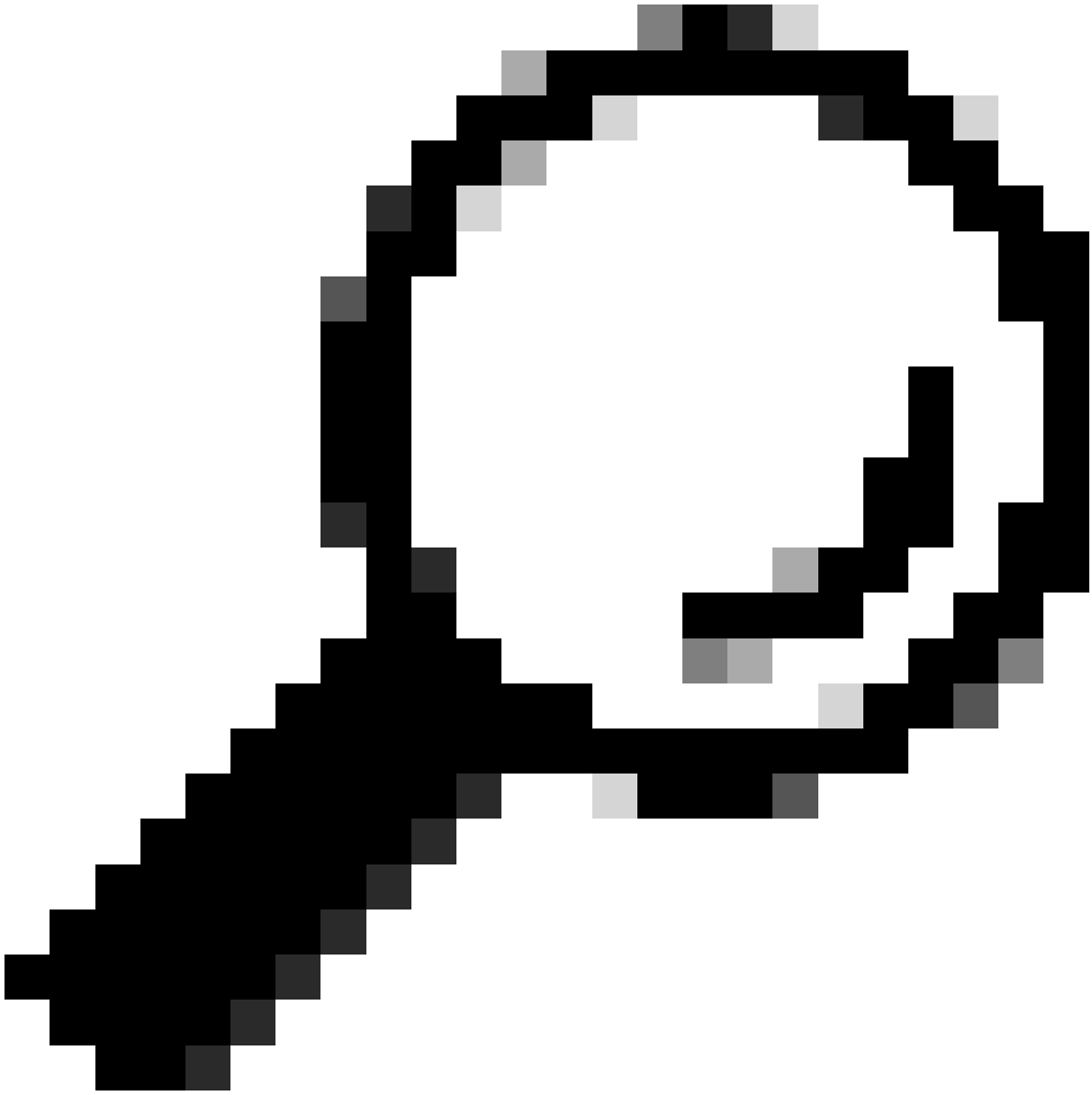
さい。正しいCisco Umbrellaパッケージがあっても、ダッシュボードの統合としてThreatQが表示されない場合は、Cisco Umbrellaサポートにお問い合わせください。

統合機能

ThreatQプラットフォームはまず、検出されたCyber Threat Intelligence（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。ThreatQ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ThreatQ宛先リストに追加されます。このポリシーは、ThreatQ宛先リストを持つ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ただちに適用されます。

今後、UmbrellaはThreatQアラートを自動的に解析し、悪意のあるサイトをThreatQ宛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ThreatQ保護が拡張され、企業ネットワークに適用の新たなレイヤが提供されます。



ヒント:Cisco 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）の検証と許可に最善を尽くしますが、望ましくない中断を避けるために、ポリシーに従って、ブロックしたことがない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お勧めします。次に例を示します。

- 組織のホームページ
- 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。
- Cisco Umbrellaに依存しているあまり知られていないクラウドベースのアプリケーションは、ドメインの自動検証に含まれません。例：「localcloudservice.com」。

これらのドメインは、Cisco UmbrellaのPolicies > Destination ListsにあるGlobal Allow Listに追加できます。

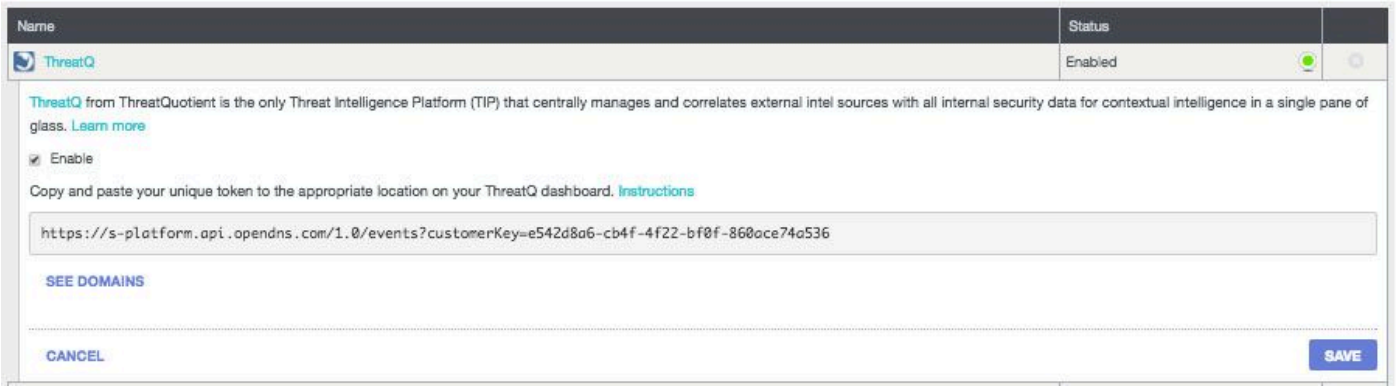
UmbrellaスクリプトとAPIトークンの生成

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. Settings > Integrationsの順に移動し、テーブル内でThreatQを選択して展開します。

3. Enableを選択してから、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。



後でThreatQを設定してUmbrellaにデータを送信するときにURLが必要になるため、URLをコピーしてThreatQダッシュボードに移動します。

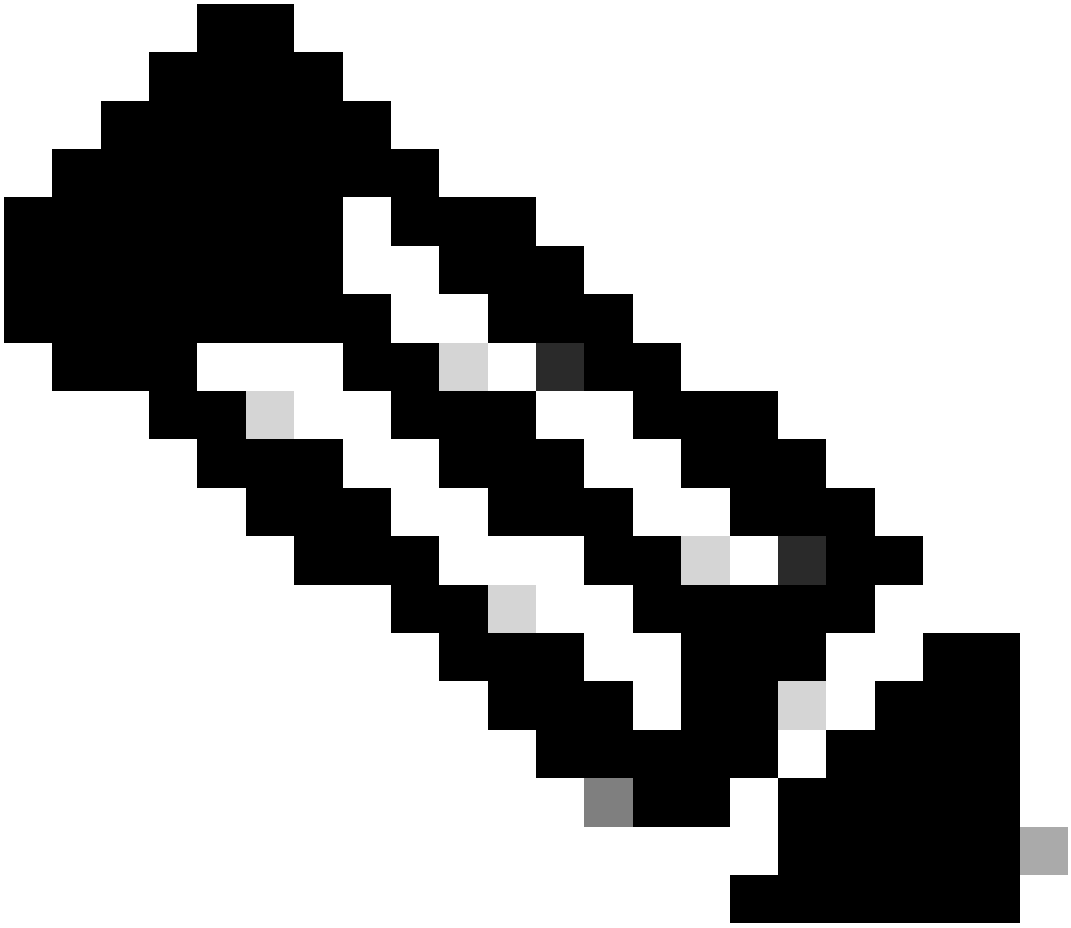
Umbrellaと通信するためのThreatQの設定方法

ThreatQダッシュボードにログインし、URLを適切なエリアに追加してUmbrellaに接続します。

正確な手順は異なりますが、ThreatQ内でAPI統合を構成する方法や場所が不明な場合は、UmbrellaからThreatQサポートに問い合わせることをお勧めします。

監査モードでThreatQ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

時間の経過とともに、ThreatQダッシュボードからのイベントは、ThreatQ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します。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、これらのリストがどのポリシーにも適用されず、既存のUmbrellaポリシーを変更できないことを意味します。



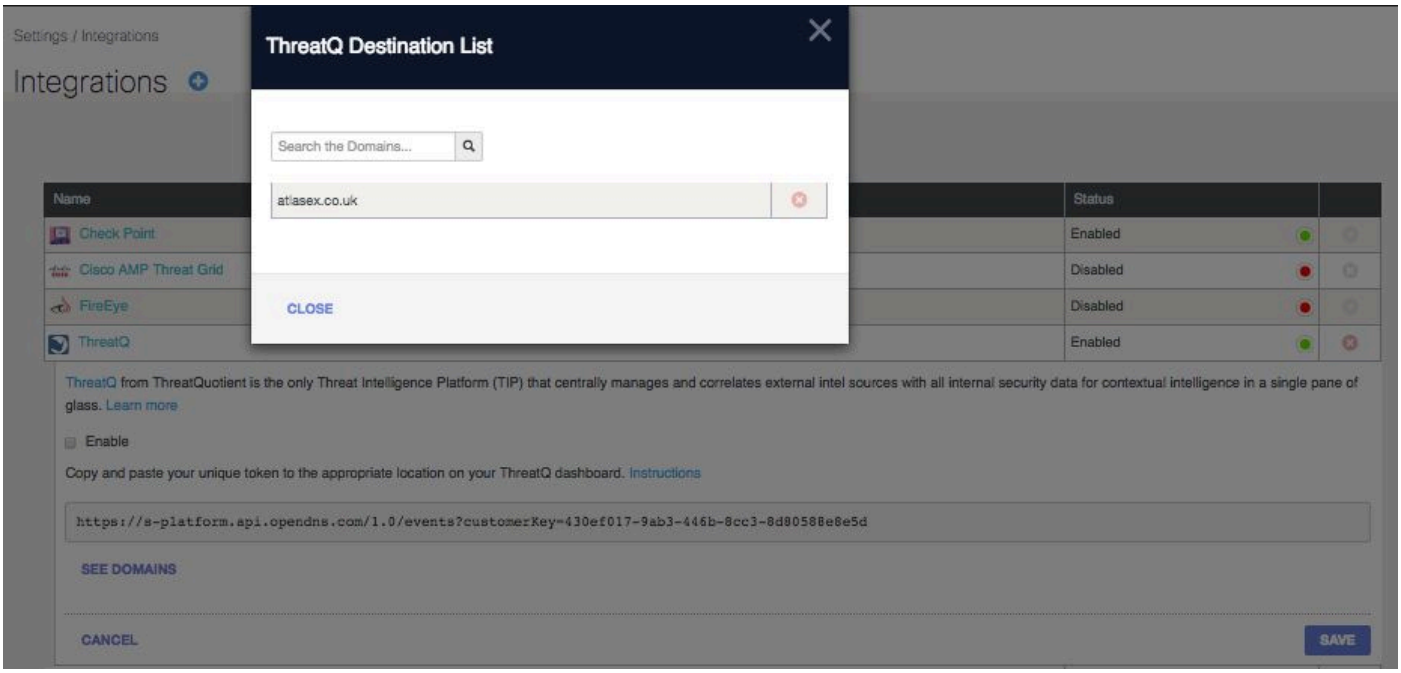
注：監査モードは、導入プロファイルとネットワーク設定に基づいて、必要な期間だけ有効にできます。

宛先リストの確認

UmbrellaのThreatQ宛先リストは、次の手順でいつでも確認できます。

1. 「設定」>「統合」にナビゲートします。

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



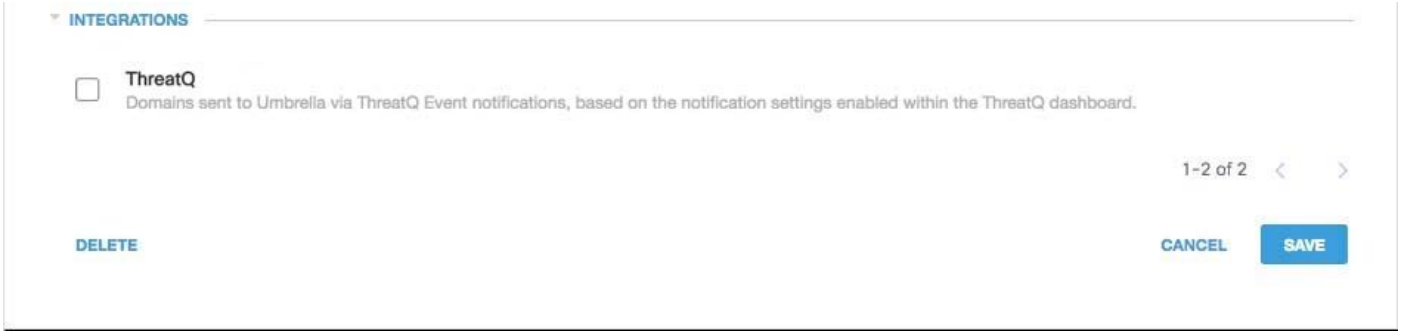
ポリシーのセキュリティ設定の確認

Umbrellaの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. [ポリシー] > [セキュリティの設定] に移動します。

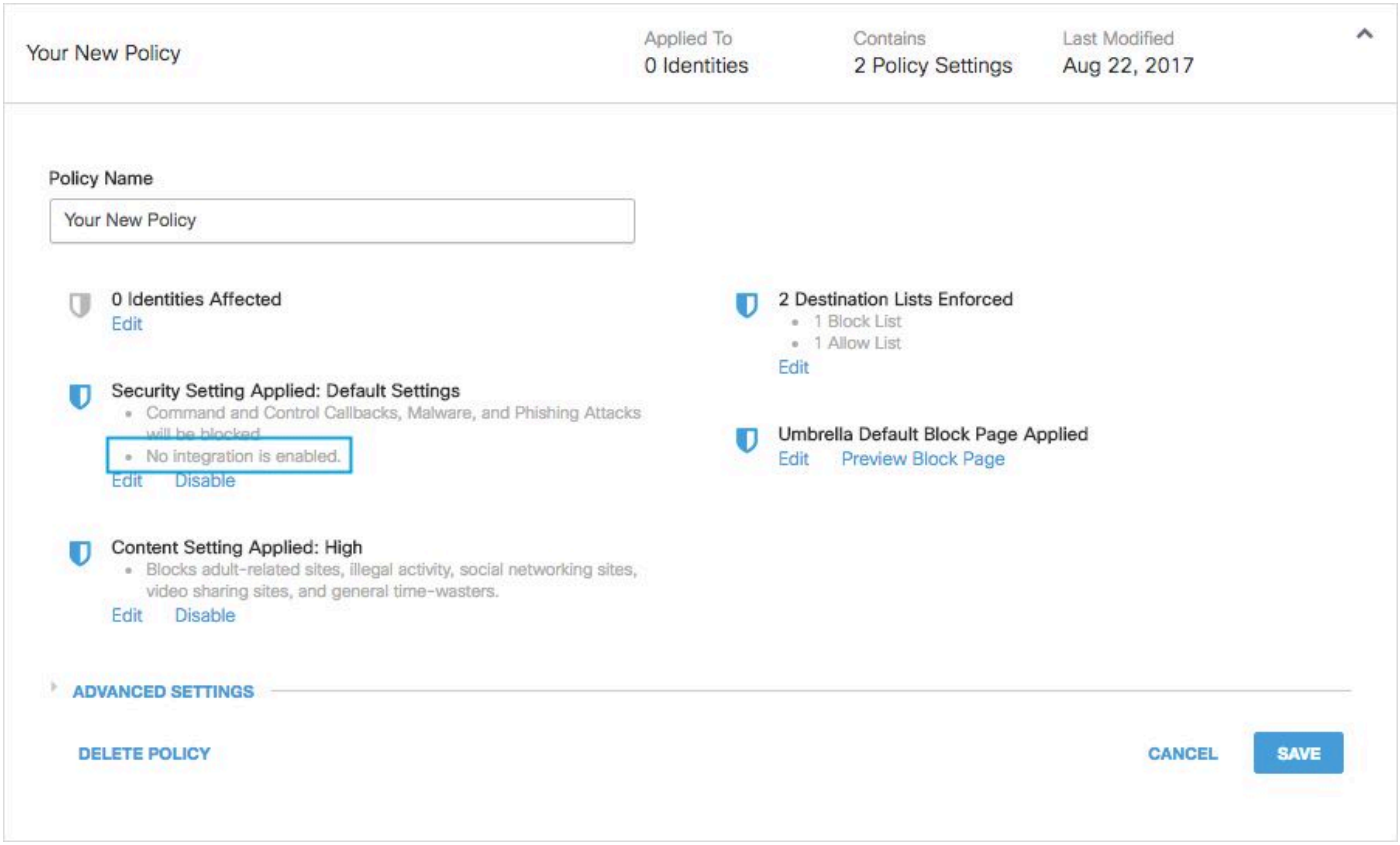
2. 表内のセキュリティ設定を選択して展開します。

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



115014040286

統合情報は、「セキュリティ設定の概要」ページで確認することもできます。



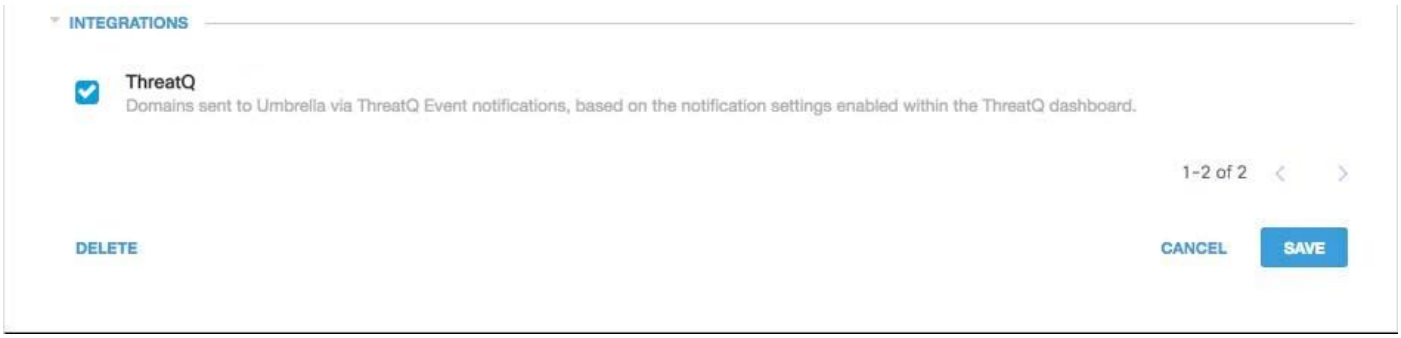
25464141748116

ブロックモードでのThreatQ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の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、デフォルトのポリシーよりも上位に配置される新しいポリシーを作成して、最初に確実に適用されるようにします。

1.Policies > Security Settingsの順に移動します。

2. Integrationsの下で、ThreatQを選択し、Saveを選択します。



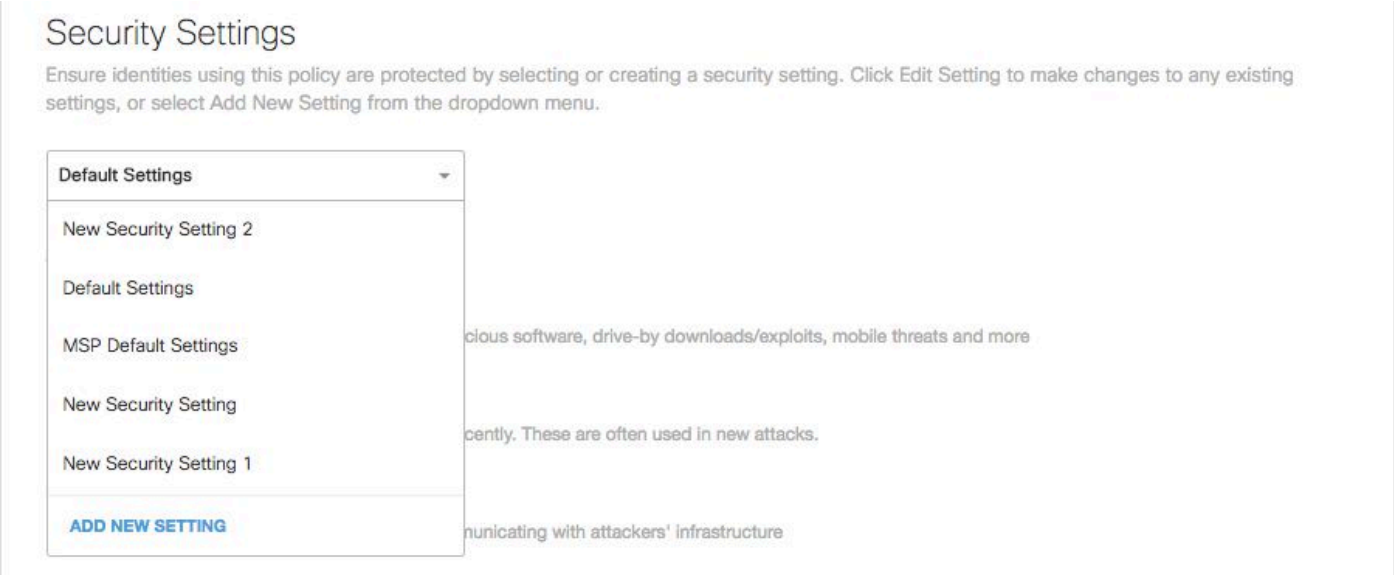
115014207403

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。

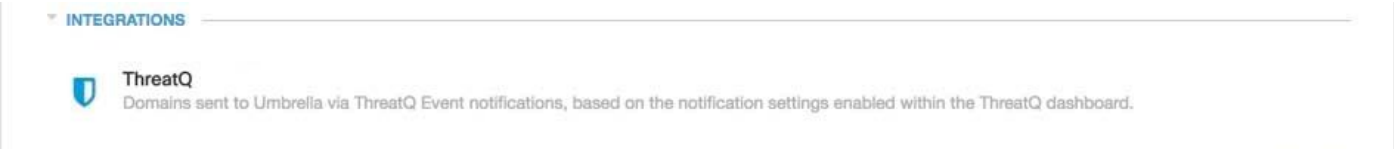
2. ポリシーを展開し、Security Setting Appliedの下でEditを選択します。

3. Security Settingsプルダウンから、ThreatQ設定を含むセキュリティ設定を選択します。



25464141787668

「統合」の下のシールドアイコンが青色に更新されます。



115014040506

4. Set & Returnを選択します。

ThreatQのセキュリティ設定内に含まれるThreatQ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るようになりました。

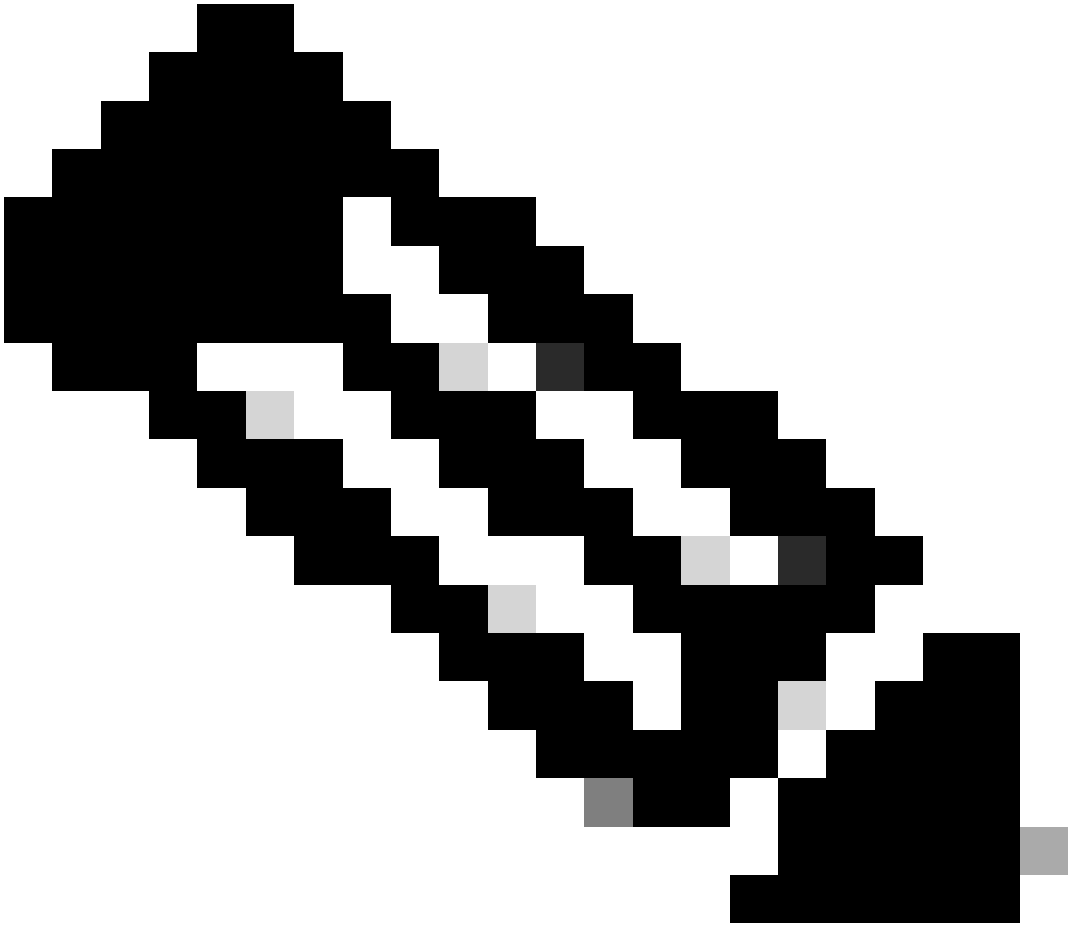
ThreatQイベントの包括的なレポート

ThreatQセキュリティイベントのレポート

ThreatQ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、ThreatQ関連のアクティビティだけを表示できます。

1. 「レポート」 > 「活動検索」にナビゲートします。

2. Security Categoriesの下でThreatQを選択し、ThreatQ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。



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

115014207603

3. Applyを選択します。

ドメインがThreatQ宛先リストに追加された際のレポート

Umbrella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ThreatQダッシュボードからのイベントが含まれます。「ThreatQ Account」という名前のユーザ（ThreatQロゴも付いている）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。Umbrella管理監査ログは、「Reporting > Admin Audit Log」で確認できます。

ThreatQアカウントユーザのフィルタを適用することで、ThreatQ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、ThreatQ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、ThreatQダッシュボードを削除した後にドメインを再度追加する場合、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。
- 2番目に、許可リストは、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を示します。

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ThreatQ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、リストにドメインを追加します。

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。

ThreatQ宛先リストからのドメインの削除

ThreatQの宛先リストでは、各ドメイン名の横に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ThreatQ宛先リストをクリーンアップできます。ただし、ThreatQダッシュボードがドメインをCisco 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.設定>統合に移動し、ThreatQを選択して展開します。

2.「ドメインを表示」を選択します。

3. 削除するドメイン名を検索します。

4.「削除」アイコンを選択します。

5. Closeを選択します。

6. 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、ThreatQ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、ThreatQ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。