ZeroFOXとUmbrellaの統合

内容

はじめに

このドキュメントでは、ZeroFOX EnterpriseをUmbrellaと統合して、Umbrellaによって保護されているクライアントにセキュリティイベントを適用できるようにする方法について説明します。

ZeroFOX EnterpriseとCisco Umbrellaの統合の概要

ZeroFOX EnterpriseをCisco Umbrellaと統合することで、セキュリティ担当者や管理者は、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今日のソーシャルメディアベースの脅威に対する保護を拡張し、分散型企業ネットワークに別の層の適用を提供できます。

Cisco UmbrellaとZeroFoxの統合：仕組み

ZeroFOX Enterpriseは、ソーシャルメディアベースのサイバー脅威（標的型マルウェア、フィッシング、ソーシャルエンジニアリング、なりすまし、その他の不正または悪意のある活動など）を検出した脅威をCisco Umbrellaにプッシュして、グローバルに適用します。

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。ZeroFOX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ZeroFOX宛先リストに追加されます。このポリシーは、そのポリシーに割り当てられたデバイスから行われたすべての要求に対して即座に適用されます。

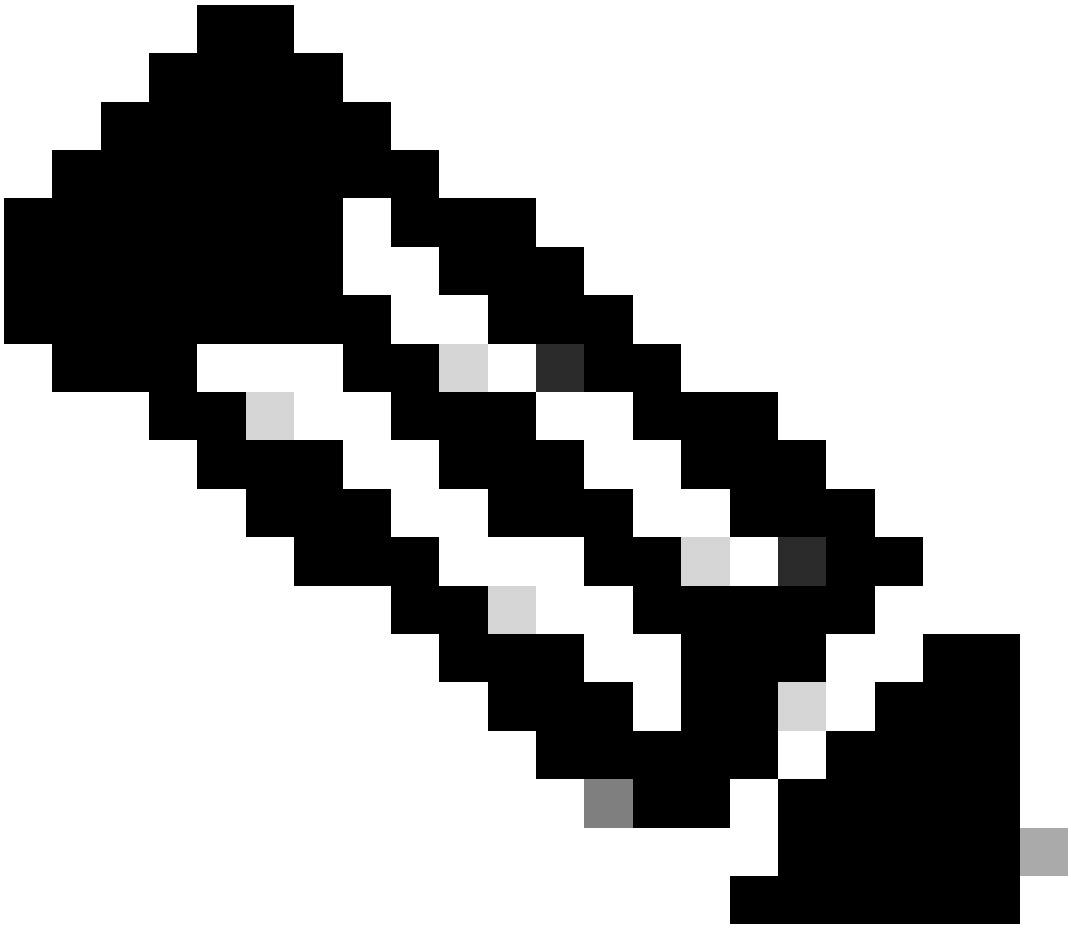
Cisco Umbrellaは、ZeroFOXのアラートを自動的に解析し、悪意のあるサイトをZeroFOXの宛先リストに追加します。これにより、すべてのリモートユーザとデバイスにZeroFOXのインテリジェンスが拡張され、企業ネットワークに対する新たな適用レイヤが提供されます。

これは、次の簡単な設定手順で実現できます。

1. Umbrellaでの統合を有効にして、APIトークンを生成します。
2. そのAPIトークンをZeroFOXアカウントに貼り付けます。
3. 目的のポリシーのセキュリティ設定でブロックするようにZeroFOXを設定します

前提条件

- ZeroFOX Enterprise管理者権限
- Umbrellaダッシュボードの管理者権限
- UmbrellaダッシュボードでZeroFOX統合を有効にする必要があります



注:ZeroFOX統合は、Umbrella Platformパッケージにのみ含まれています。Platformパッケージを所有しておらず、ZeroFOX統合を希望する場合は、Cisco Umbrellaの担当者にお問い合わせください。プラットフォームパッケージがあっても、ダッシュボードの統合としてZeroFOXが表示されない場合は、Umbrellaサポートにお問い合わせください。

重要： Umbrellaは、一般的に安全であると知られているドメイン（GoogleやSalesforceなど）を検証して許可するよう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、ブロックしたく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。

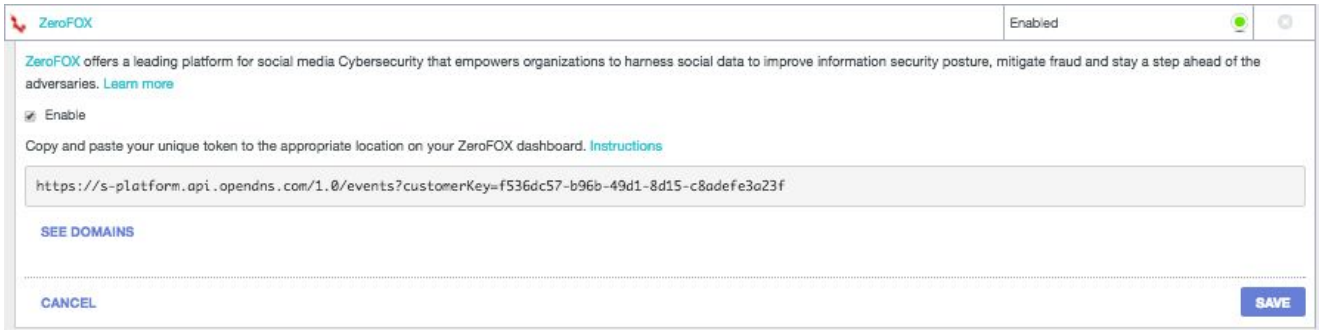
- 組織のホームページ。たとえば、mydomain.comなどです。
- 内部レコードと外部レコードの両方を持つことができる、提供するサービスを表すドメイン。たとえば、mail.myservicedomain.comやportal.myotherservicedomain.comなどです。
- Umbrellaが認識できない、または自動ドメイン検証に含めることができない、あまり知られていないクラウドアプリケーションに大きく依存しています。たとえば、localcloudservice.comなどです。

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、ドキュメント「宛先リストの管理」を参照してください。

ステップ1: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ダッシュボードに管理者としてログインし、設定>統合に移動して、テーブルで「ZeroFOX」をクリックして展開します。
2. Enableにチェックマークを入れてから、Saveをクリックする。これにより、カスタマーキーを含む一意のURLが生成されます。

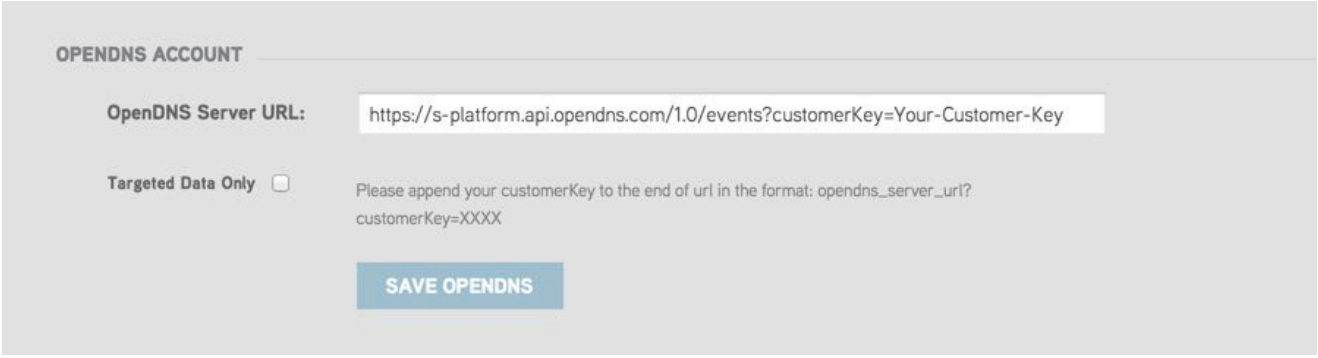


後でZeroFOXを設定する際にURLが必要になるため、URLをコピーしてThreatQダッシュボードに移動します。

ステップ2:Umbrellaに情報を送信するようにZeroFOX Enterpriseダッシュボードをセットアップする

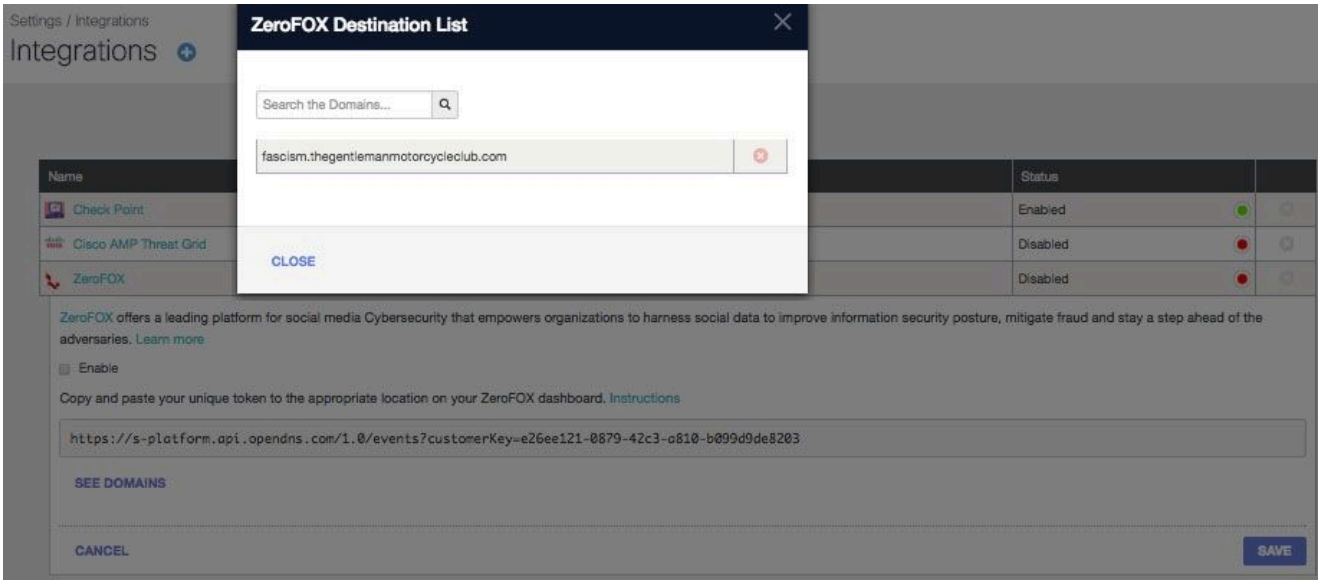
次に、ステップ1でコピーしたURLをZeroFOXダッシュボードに追加します。

1. Zerofoxダッシュボードの歯車アイコンをクリックし、Account Settingsを選択します。
2. OpenDNSアカウント情報が表示されるまで統合リストをスクロールし、UmbrellaのURLをOpenDNS Server URLフィールドに貼り付けます。
3. 統合を最初に有効化する際には、ターゲットデータのみを確認することをお勧めします。



ステップ3:ZeroFOXイベントをUmbrella内でブロックするように設定する

1. Umbrellaダッシュボードに管理者として再度ログインします。
2. Settings > Integrationsの順に移動し、表内の「ZeroFOX」をクリックして展開します。
3. See Domainsをクリックします。
   これにより、ZeroFOXアカウントの最近の数時間のイベントを含むドメインのリストが展開されます。その時点から、検索可能なリストにデータが入力され始め、リストが拡大し始めます。

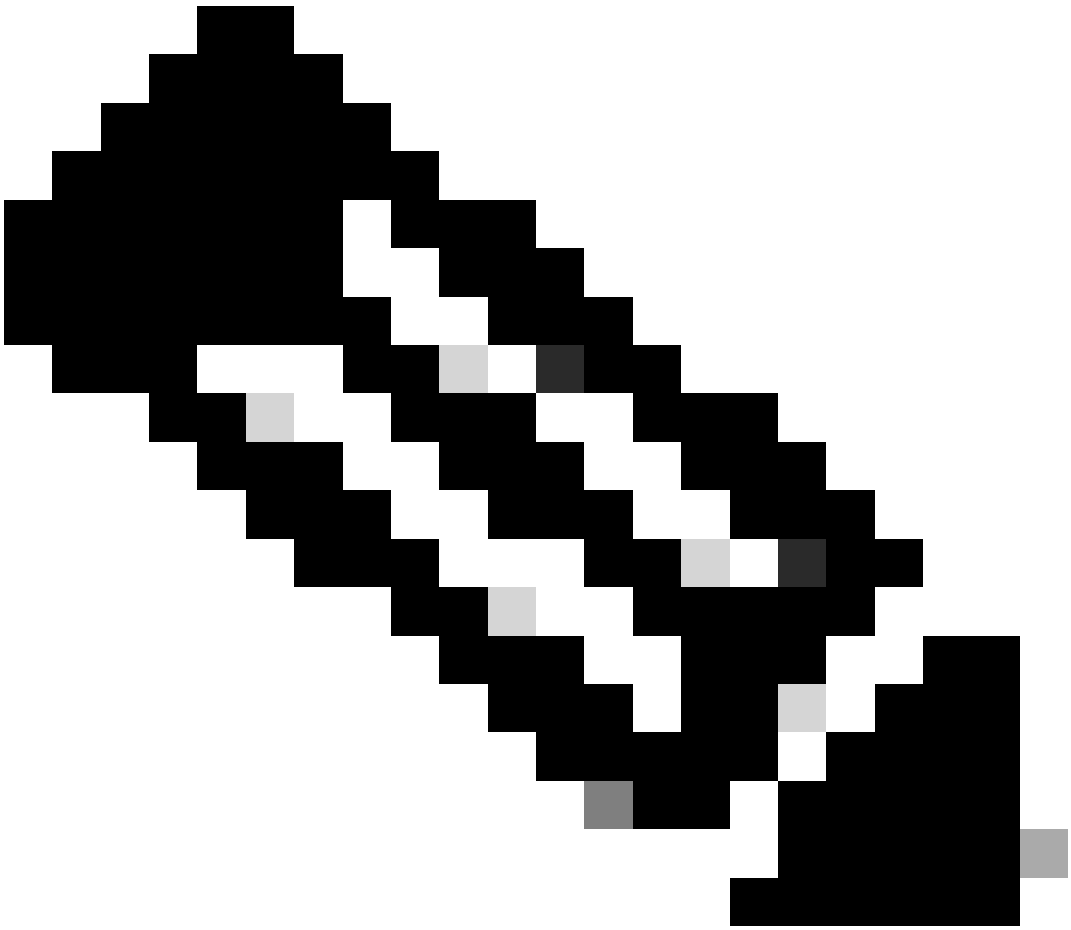


次のステップは、新しいZeroFOXセキュリティカテゴリに追加されたイベントを確認して監査することです。

監査モードでZeroFOXセキュリティカテゴリに追加されたイベントの監視

ZeroFOX Enterpriseからのイベントは、ZeroFOX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であり、どのポリシーにも適用されず、既存のUmbrellaポリシーは変更されませ

ん。



> 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

ZeroFox Destination Listはいつでも確認できます。

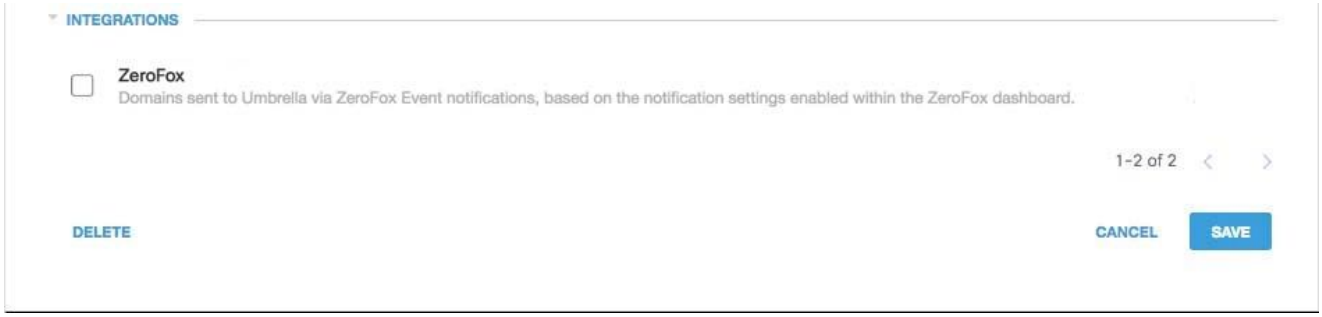
1. Settings > Integrationsの順に移動します。
2. テーブルで「ZeroFOX」を展開し、「ドメインを表示」をクリックします。

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。

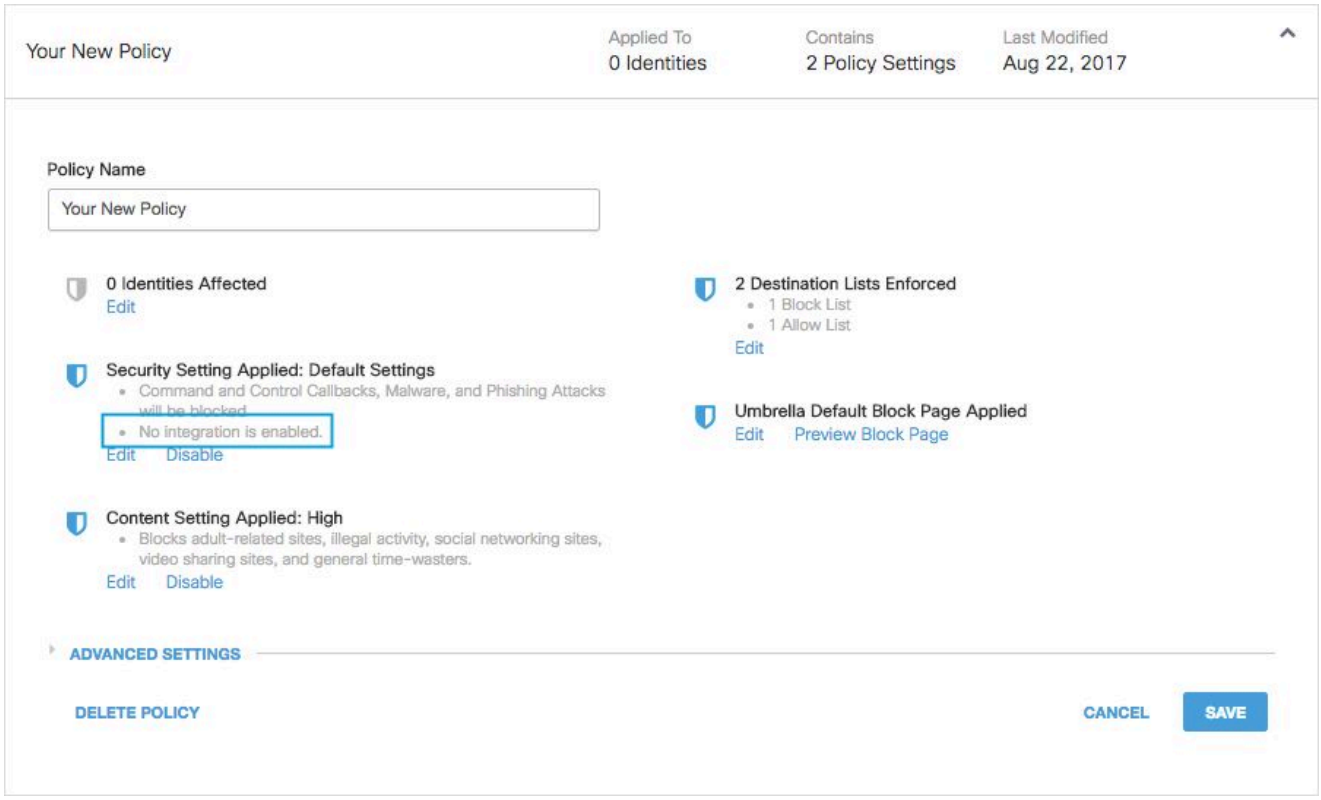
1. Policies > Security Settingsの順に移動します。

2. 表内のセキュリティ設定をクリックして展開し、「統合」までスクロールしてZeroFOX設定を見つけます。



115014041606

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。



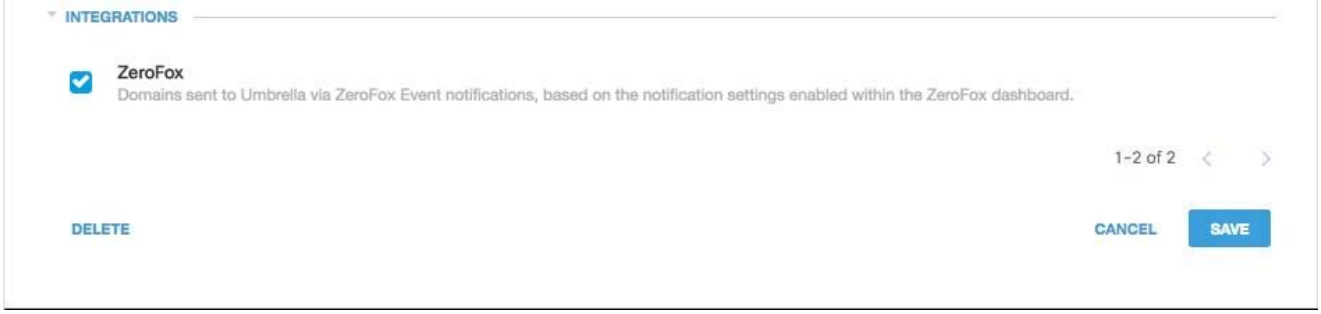
25464154913556

ブロックモードでのZeroFOXセキュリティ設定の管理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、デフォルト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、Integrationsの下で、ZeroFOXにチェックマーク

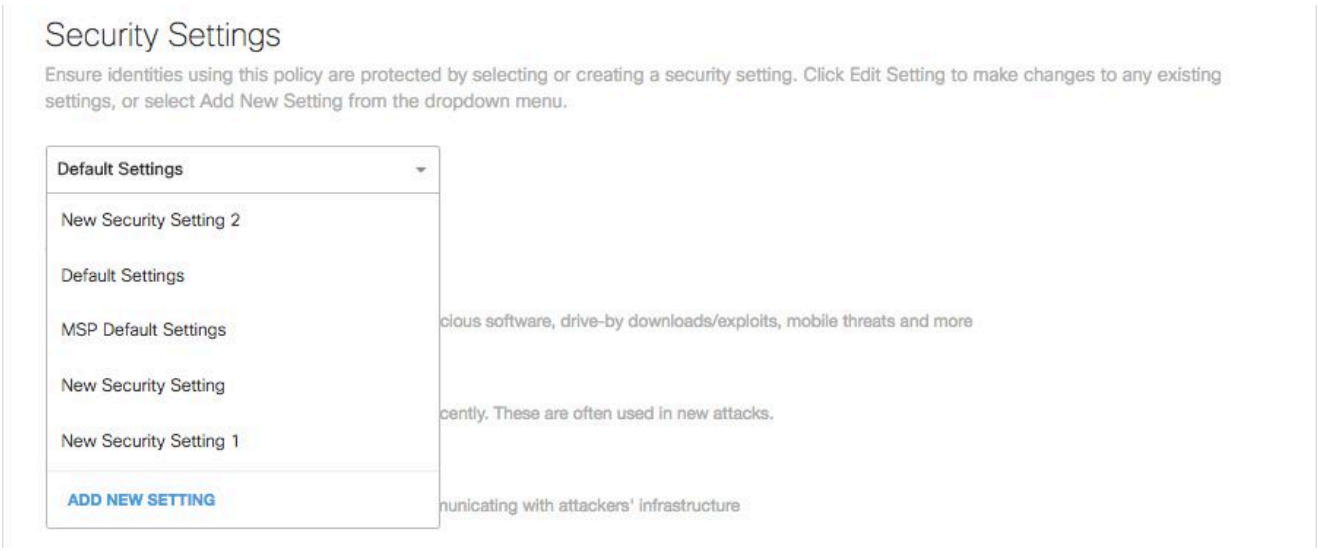
を入れて、Saveをクリックします。



115014042806

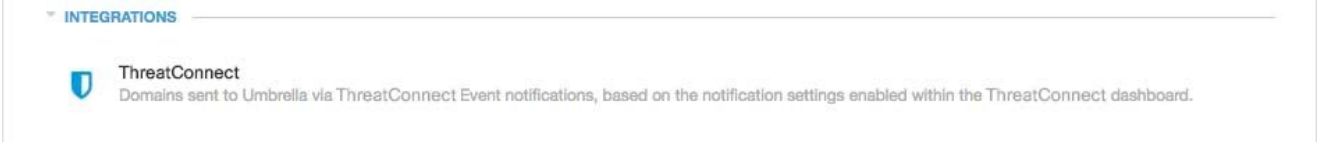
次に、ポリシーウィザードで、編集中のポリシーにセキュリティ設定を追加します。

1. Policies > Policy Listの順に移動します。
2. ポリシーを展開し、Security Setting Appliedの下にあるEditをクリックします。
3. Security Settingsプルダウンから、ThreatConnect設定を含むセキュリティ設定を選択します。



25464147943700

Integrationsの下のシールドアイコンが青色に更新されます。



25464147957652

4. Set & Returnをクリックします。

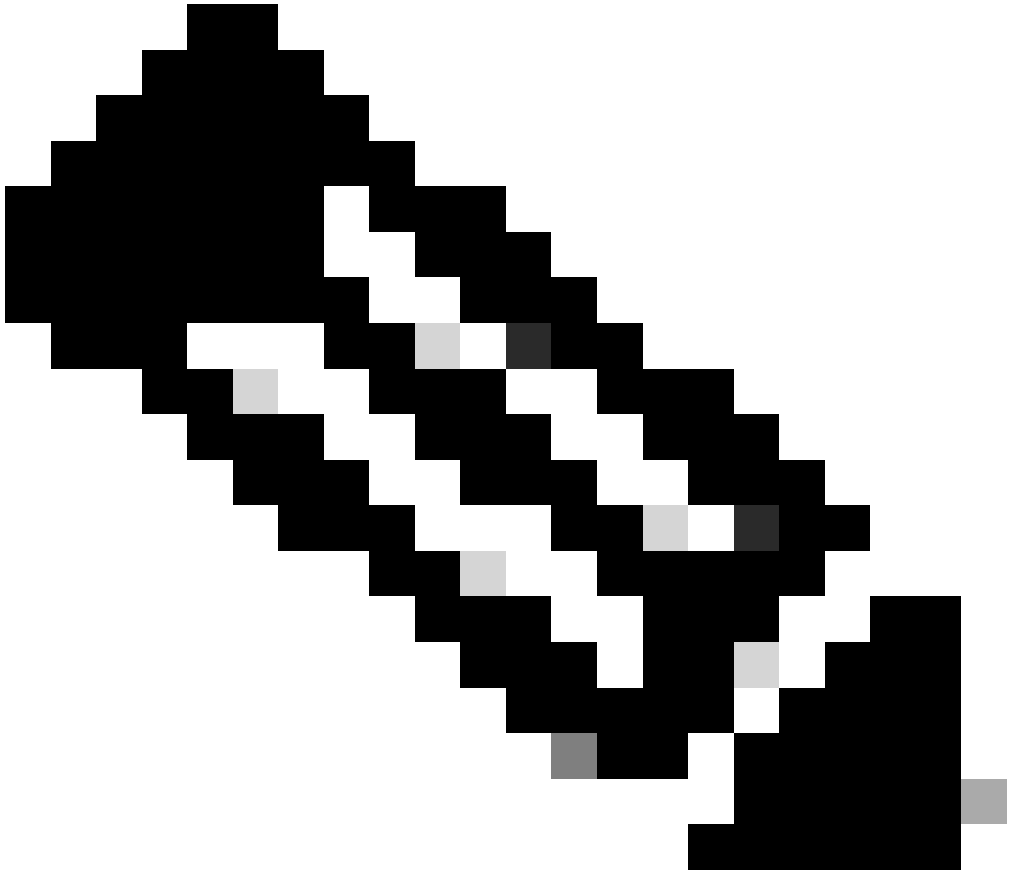
ZeroFOXのセキュリティ設定内に含まれるZeroFOXドメインは、そのポリシーを使用してこれらのIDに対してブロックされます。

ZeroFOXイベントのUmbrellaでのレポート

ZeroFOXセキュリティイベントのレポート

ZeroFOX Destination List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して、ZeroFOX関連のアクティビティのみを表示できます。

1. Reporting > Activity Search に移動し、Security Categoriesの下でZeroFOXを選択して、ZeroFOXのセキュリティカテゴリだけを表示するようにレポートをフィルタリングします。



注:ZeroFOX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。

115014043046

2. [APPLY] をクリックします。

ZeroFOX宛先リストにドメインが追加された場合のレポート

Umbrella管理監査ログには、ZeroFOXアカウントが宛先リストにドメインを追加するときに生成されたイベントが含まれます。

Umbrella管理監査ログは、「レポート」 >「管理監査ログ」で確認できます。ドメインがいつ追加されたかをレポートするには、ZeroFox宛先リストのIDと設定にフィルタを適用して、ZeroFOXの変更のみを含めるようにフィルタします。

レポートを実行すると、ZeroFOX宛先リストが統合からに追加されたときに行われた変更のリストが表示されます。

不要な検出や誤検出の処理

不要な検出の許可リストの管理

まれに、ZeroFOXによって自動的に追加されたドメインが、ユーザによる特定のWebサイトへのアクセスを妨げる不要なブロックをトリガーする可能性があります。このような状況では、許可リストにドメインを追加することをお勧めします。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。ドメインが両方に存在する場合、許可リストは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2つあります。まず、ZeroFOXアプライアンスが削除された後にドメインを再度追加する場合、許可リストは、この問題を引き起こすさらなる問題に対する保護策となります。次に、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ZeroFOX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。

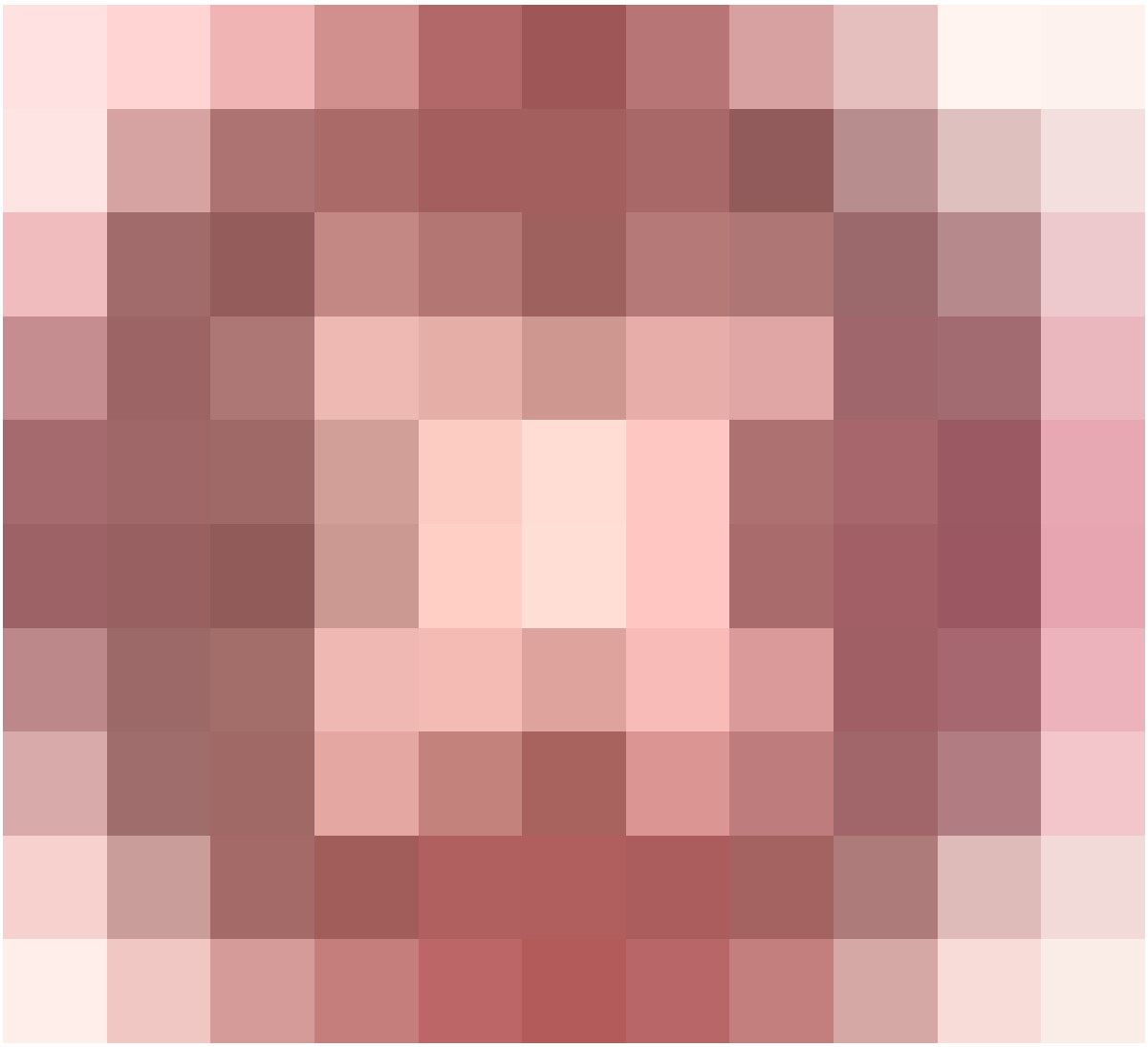
1. Policies > Destination Listsの順に移動し、

   25464155856404

   Addアイコン。
2. Allowを選択し、リストにドメインを追加します。
3. [Save] をクリックします。

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。

ZeroFOX宛先リストからのドメインの削除



この例では、(削除)アイコンをクリックします。ドメインを削除すると、不要な検出が発生した場合にZeroFOX宛先リストをクリーンアップできます。

ただし、ZeroFOXがUmbrellaにドメインを再送信する場合、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. Settings > Integrationsの順に移動し、ZeroFOXをクリックして展開します。
2. See Domainsをクリックします。
3. 削除するドメイン名を検索します。
4. Delete アイコンをクリックします。

5. [Close] をクリックします。
6. [Save] をクリックします。

不要な検出や誤検出が発生した場合は、Umbrellaで許可リストを即座に作成し、ZeroFOX内で誤検出を修復することをお勧めします。後で、ZeroFOX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。