カスタム統合のための包括的な適用APIの理解

内容

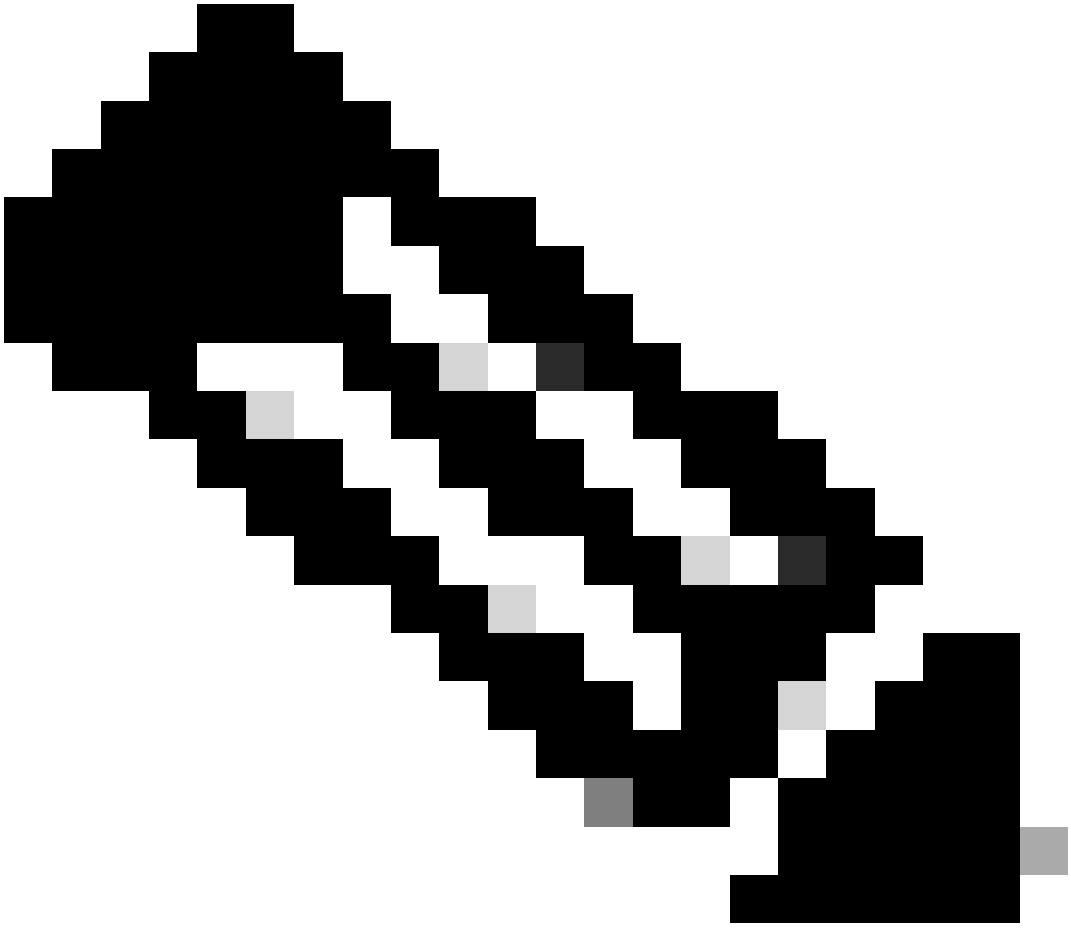
はじめに

このドキュメントでは、カスタム統合用のUmbrella Enforcement APIについて説明します。

Umbrella Enforcement APIとは何ですか。

Umbrella Enforcement APIを使用すると、自社開発のSIEM/脅威インテリジェンスプラットフォーム(TIP)環境を持つパートナーやお客様は、Umbrella環境にイベントや脅威インテリジェンスを注入できます。これらのイベントは、即座に可視性に変換され、境界を越えて適用されます。したがって、これらのイベントや脅威インテリジェンスを生成した可能性のあるシステムの範囲も拡大されます。

Enforcement APIは、このAPIドキュメントで説明されている汎用イベント形式でイベントを取り込むことができ、ADD、DELETE、またはLIST関数をサポートできます。



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。

なぜ使用する必要があるのですか。

すでに独自の脅威インテリジェンスシステムやプロセスを処理、管理、およびキュレートしている可能性があり、その結果、悪意のあるドメインや疑わしいドメインに対してアクションを実行したいという要望が生じています。その場合、イベントにアクションを実行する必要があることを決定したら（たとえば、保護に変換する）、Umbrellaに保護を手動で追加して適用するのではなく、Enforcement APIを使用してこのプロセスを自動化し、イベントに関連づけられたドメインに基づいて保護を即座に適用できます。

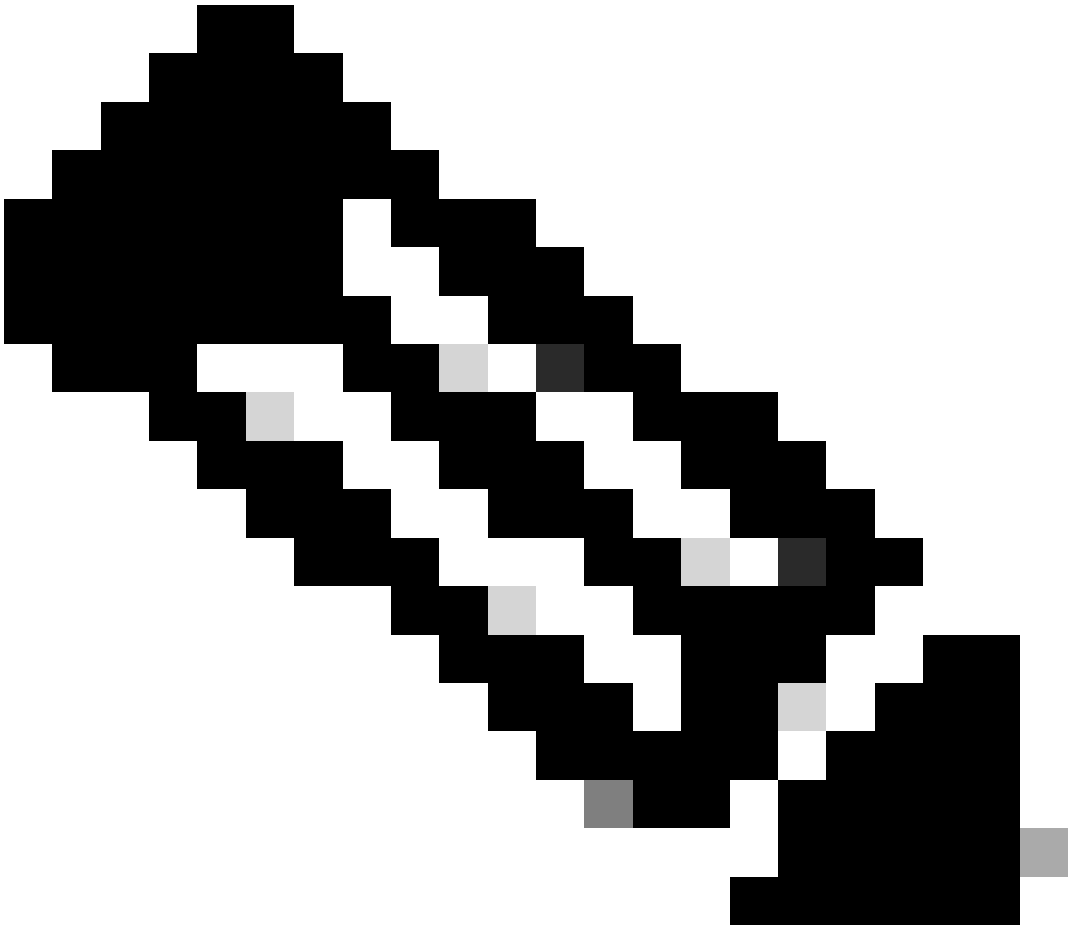
これにより、セキュリティチームは、Umbrellaの継続的な設定ではなく、調査に時間と労力を集中させることができます。これにより、セキュリティチームはUmbrellaダッシュボードに飛び込んで宛先リストを更新する必要がなくなり、ツールやプロセス内に留まることができます。基本的に、APIを介して直接管理する外部ソースからUmbrellaで宛先リストを作成し、Umbrella内の

IDに対してこれらの宛先をブロックするように選択できます。

どのように使用すればよいですか。

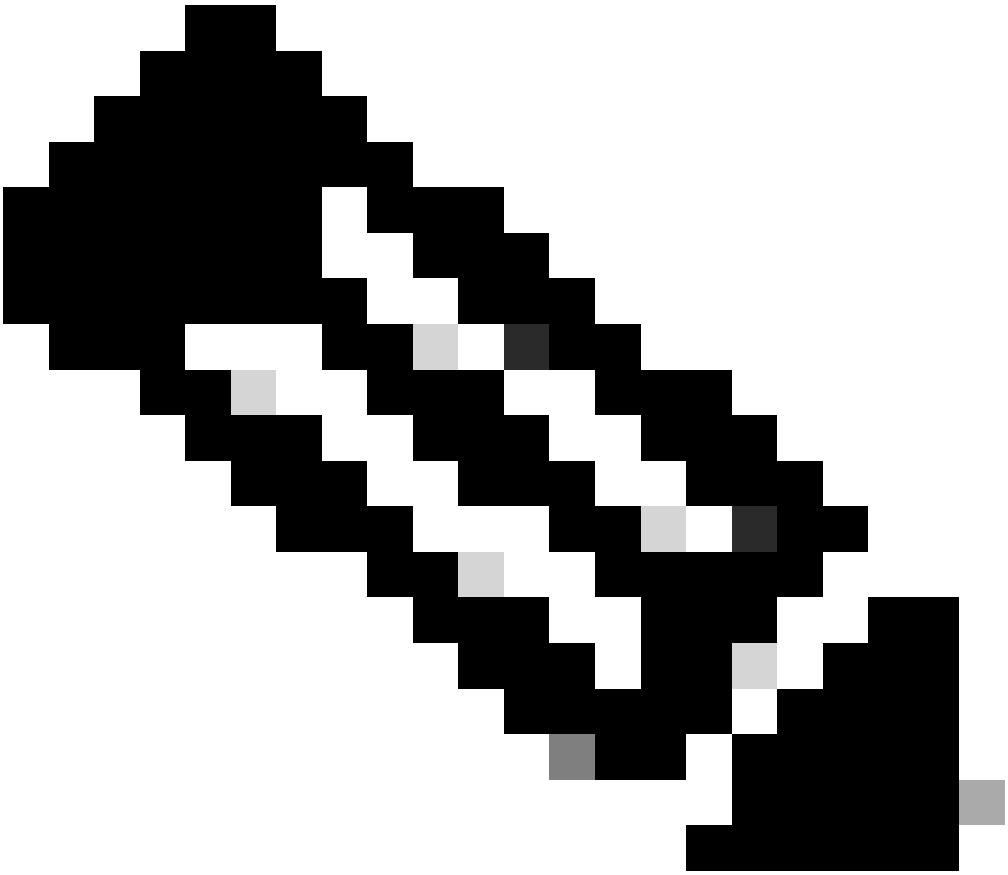
適用APIへのイベントの追加

イベントが追加されると、エンフォースメントはイベントからドメインを抽出しようとします。



注:IPアドレスとURLのサポートは今後追加されます。

- イベントには元のイベントの詳細情報をいくらでも含めることができますが、APIのドキュメントに記載されている仕様に準拠する必要があります。



注:Umbrellaダッシュボード内のサーフェシングイベントの詳細のサポートは今後追加される可能性があります。

- 抽出されたドメインは、Cisco Umbrellaセキュリティグラフで検証され、誤検出の原因となる可能性が高い、既知の適切なドメインでないか、またはCisco Umbrellaセキュリティグラフですでに悪意があると判断されているかどうかを確認します。
- 検証に合格した場合（たとえば、ブロックが不明で安全な場合など）、そのカスタム統合に関連付けられた宛先リストに追加され、カスタムセキュリティカテゴリとしてUmbrellaダッシュボード内に表示されます。
- カスタムセキュリティカテゴリは、ポリシー単位でブロックまたは許可することができ、疑わしい要求のアクティブな適用とパッシブな「監査」の両方を可能にします。

適用APIリストのLISTドメイン

- 以前に挿入されたイベントによってブロックされたドメインのブロック解除がワークフローに含まれている場合、LIST要求は、その統合に関連付けられた宛先リストに現在含まれているすべてのドメインを提供します。

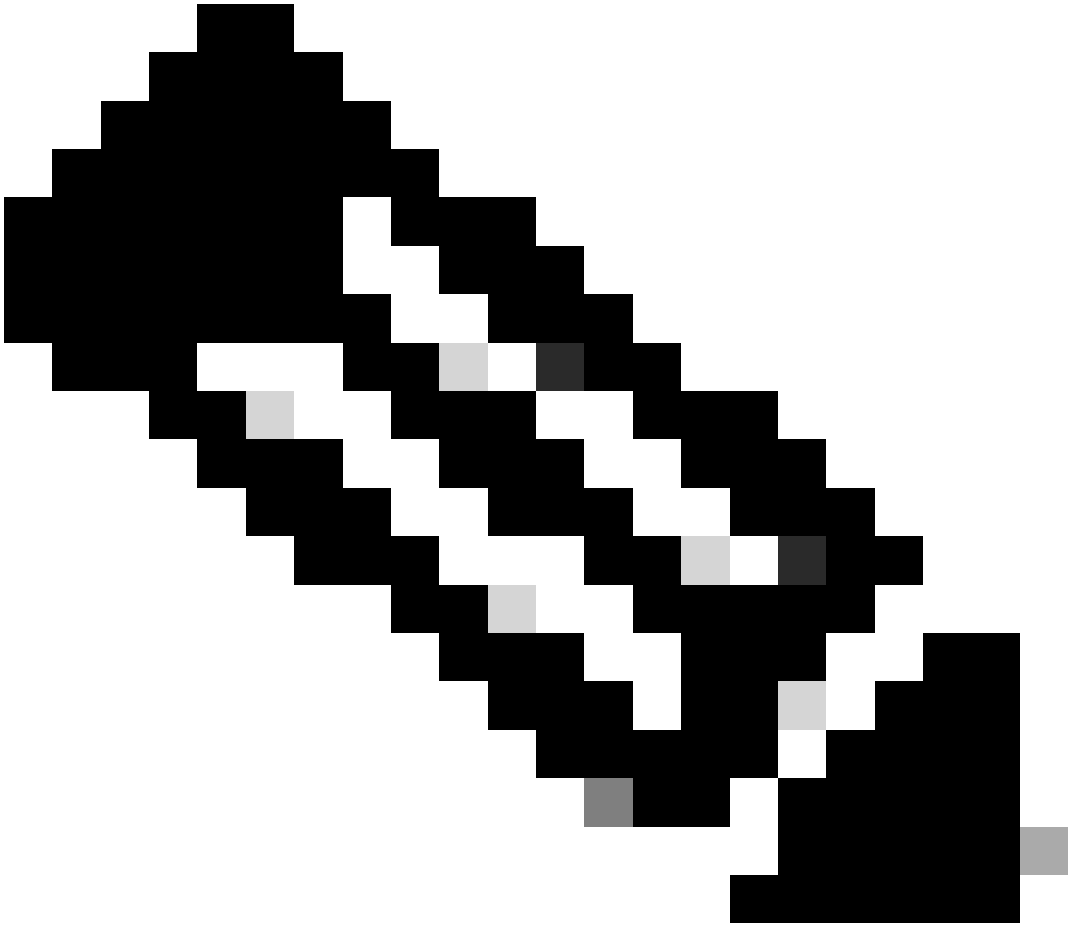
強制APIリストからのドメインの削除

- 以前に挿入されたイベントによってブロックされたドメインのブロック解除がワークフローに含まれている場合は、DELETE要求を使用して、その統合に関連付けられた宛先リストからドメインを削除できます。
- Umbrella IDのいずれかからの着信DNS要求が、カスタム統合先リスト内のドメイン宛である場合、要求をトリガーしたポリシーに関連付けられているカスタム統合のセキュリティ設定に応じて、要求はブロックまたは許可されます。
- 結果は他のすべてのUmbrellaイベントと一緒にログに記録され、アクティビティ検索またはS3統合を使用したAmazon S3経由でアクセスできます。したがって、カスタム統合に関連付けられたトラフィックをオプションでSIEM/TIPに取り込んで、フィードバックループを閉じることができます。

Enforcement APIの使用に関するチュートリアル

ステップ1：カスタム統合の作成

一度に最大10個のカスタム統合を実行できます。



注：組織がUmbrella MSP、MSSP、またはMOCの子組織である場合、子組織レベルで作成される統合の前に、コンソールレベルから共有されるカスタム統合が表示されます。

1. Umbrellaで、Policies > Policy Components > Integrationsの順に移動し、Addをクリックします。
2. カスタム統合の名前を追加し、Createをクリックします。
3. 新しいカスタム統合を展開し、Enableにチェックマークを付け、統合URLをコピーしてSaveをクリックします。

ステップ2：カスタムスクリプトを作成します。

1. このドキュメントの付録にあるgenerate_eventとdelete_domainのサンプルスクリプトを参照するか、APIのマニュアルを使用して独自のスクリプトを作成し、イベントの生成やドメインの削除または一覧表示を行う際に正しい形式のリクエストを生成します。今後は、これらのスクリプトでカスタム統合URLを使用する必要があります。

ステップ3：サンプルイベントを挿入する

1. 作成したスクリプトを使用して、カスタム統合にイベントを挿入します。この例では、ドメイン「creditcards.com」を含むイベントを挿入しました。

ステップ4:Umbrellaダッシュボードの宛先リストを確認します。

1. Settings > Integrationsの順に選択し、テーブルでカスタム統合を展開します。
2. See Domainsをクリックします。追加したドメインの検索可能なリストが表示され、ステップ4のサンプルイベントがリストに表示されます。

手順5：管理監査ログを確認します。

1. カスタム統合に関連するアクティビティを確認するもう1つの方法は、管理監査ログを確認することです。
2. Reporting > Admin Audit Logの順に移動します。
3. Filtersの下で、Filter by Identities & Settingsにカスタム統合の名前を入力し、Run Filterをクリックします。

エントリを展開すると、サンプルイベント(creditcards.com)がカスタム統合に追加されたイベントが表示されます。

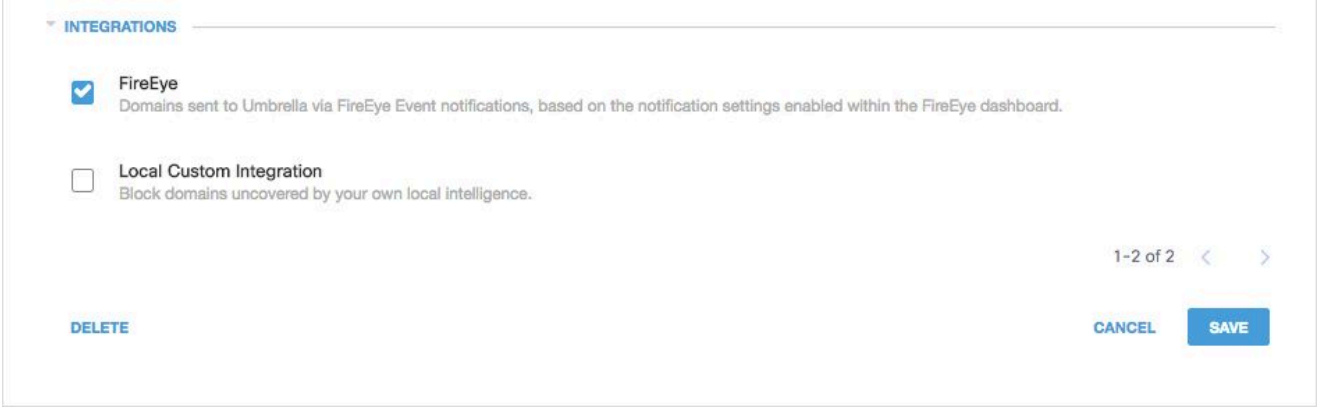
オプションの手順：ドメインの一覧表示または削除

また、ドメインに対して強制しない場合や、統合にドメインが含まれていない場合に、カスタム統合にドメインをリストし、ドメインを削除できることをテストすることもできます。ドメインを一覧表示および削除するには、『APIのドキュメント』に記載されている手順を使用します。

セキュリティ設定の構成

イベントを挿入（およびオプションでドメインの一覧表示と削除）できることを確認したら、カスタム統合のセキュリティカテゴリのドメイン宛てのIDからのDNS要求に対して行う操作を構成できます。

1. Policies > Security Settingsの順に移動し、Integrationsの下で、有効になっている統合（この例ではFireEye）を確認し、Saveをクリックします。

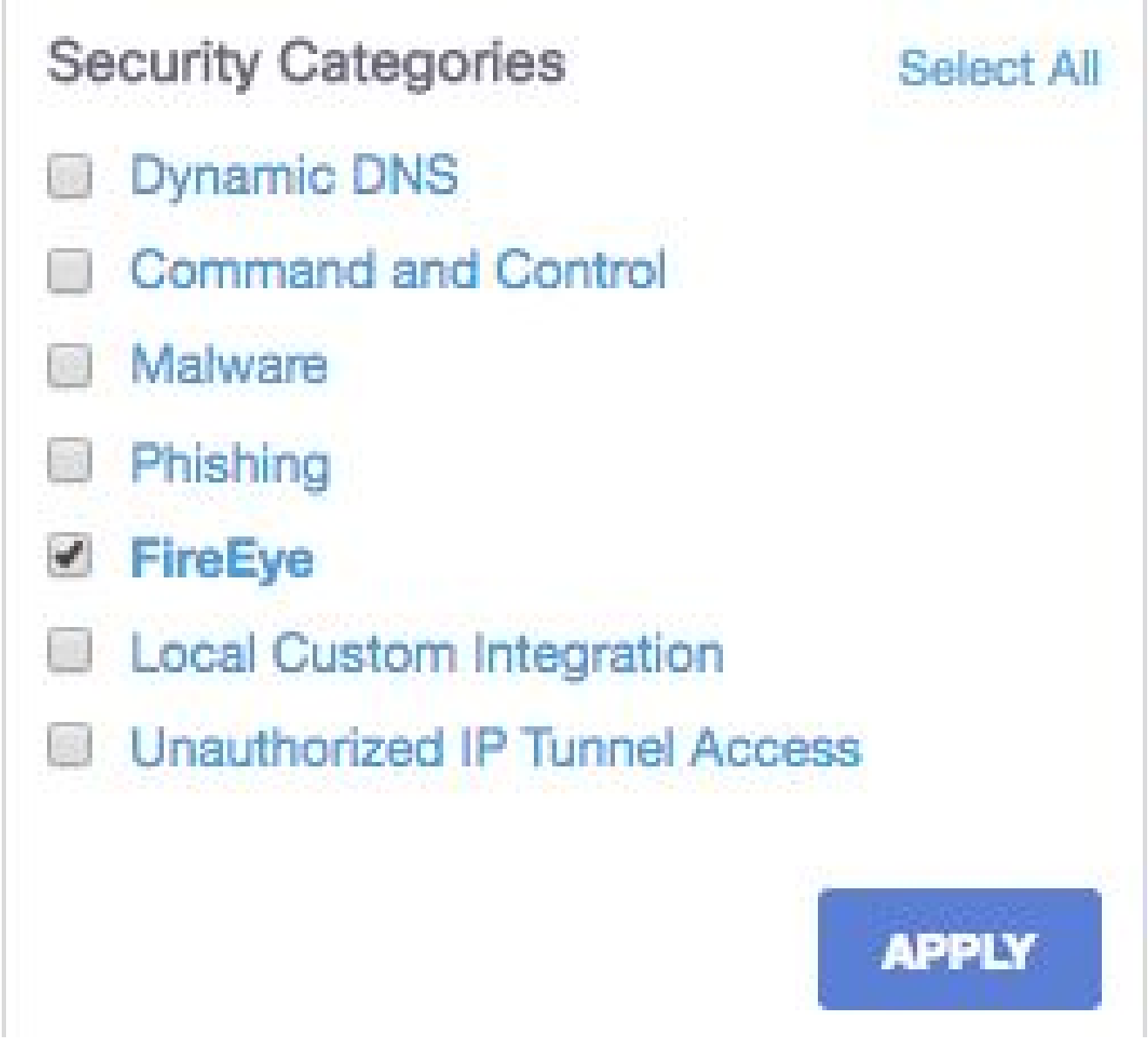


115014145103

カスタム統合のレポートの表示

IDの1つ（たとえば、ネットワークまたはローミングコンピュータ）から、カスタム統合のドメイン（この例では「creditcards.com」）宛てにDNS要求を生成します。 クライアントの観点からは、セキュリティ設定の設定方法に応じて、適切なブロックまたは許可の結果が表示されます。

1. Reporting > Activity Searchに移動し、Security Categoriesでカスタム統合（この例ではFireEye）を選択して、FireEyeのセキュリティカテゴリのみが表示されるようにレポートをフィルタリングします。

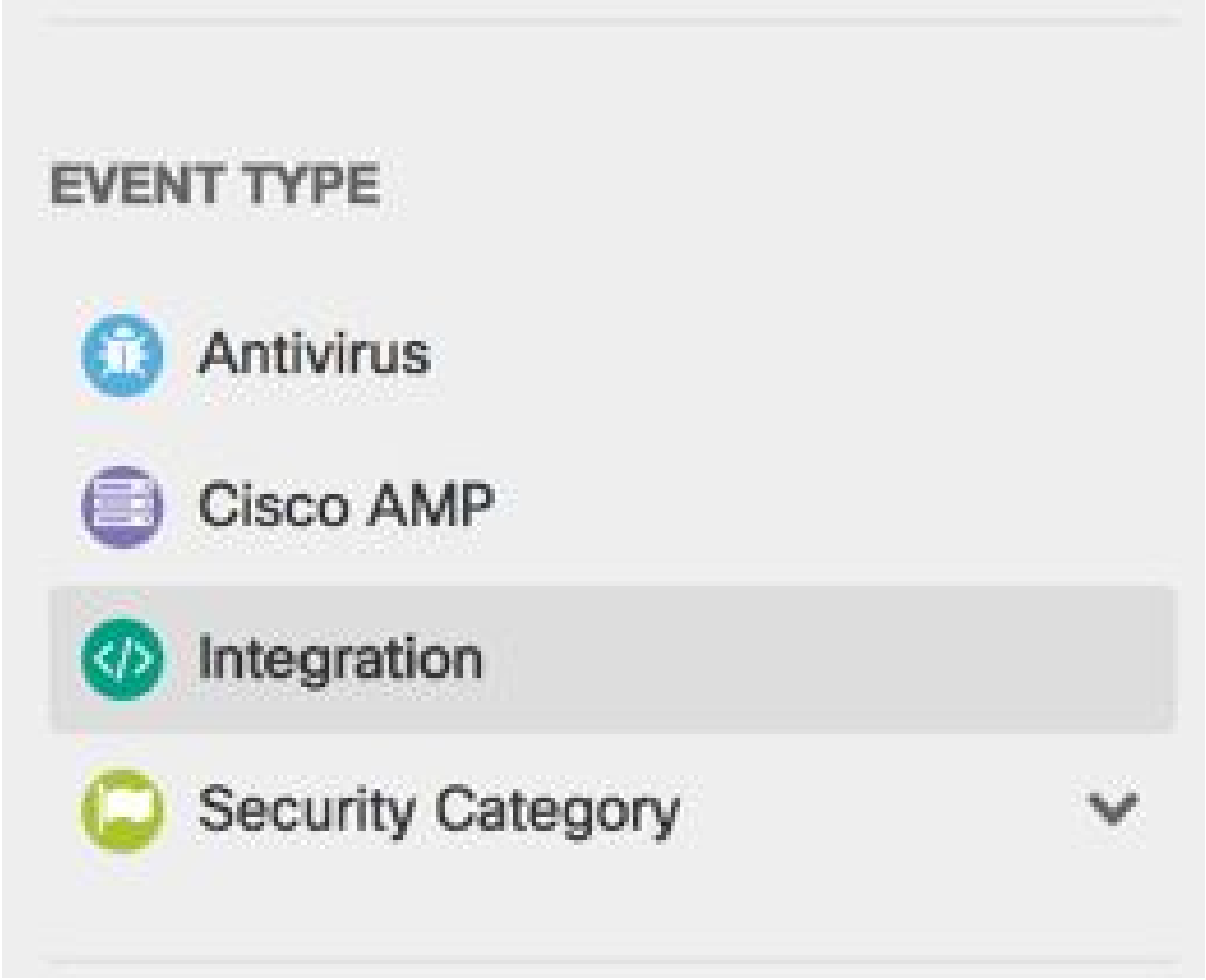


115013981706

2. Applyをクリックして、レポートで選択された期間のアクティビティを表示します。

また、アクティビティボリュームレポートを表示して、カスタム統合を含むスナップショットまたは経時的な傾向の集計レポートを確認することもできます。

1. 「レポート」>「セキュリティ活動ボリューム」にナビゲートします。
2. Event TypeでIntegrationを選択します。



115013982286

ログの保存と使用のためにS3統合を構成します（オプション）

環境に対するすべての要求を含むUmbrellaのログをSIEM/TIP環境にフィードバックする場合は、S3統合を使用して行うことができます。これにより、DNSアクティビティイベントをストリームバックできます。

付録：スクリプトの例

これらのperlスクリプトは、カスタム統合のイベントを生成する方法に関するガイダンスを提供します。両方のスクリプトで、統合のcustomerKey値を置き換えてください。これらのスクリプトは例として提供されており、カスタマイズや更新が必要になる場合があることに注意してください。

generate_event.pl:

```
#!/usr/bin/perl -w

# Custom integration - ADD EVENT URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/events?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $json_blob = "{
    \"alertTime\" : \"2013-02-08T11:14:26.0Z\",
    \"deviceId\" : \"ba6a59f4-e692-4724-ba36-c28132c761de\",
    \"deviceVersion\" : \"13.7a\",
    \"dstDomain\" : \"$domain\",
    \"dstUrl\" : \"http://$domain/a-bad-url\",
    \"eventTime\" : \"2013-02-08T09:30:26.0Z\",
    \"protocolVersion\" : \"1.0a\",
    \"providerName\" : \"Security Platform\"
}";

my $curl_request = "curl '" . $cust_key . "' -v -X POST -H 'Content-Type: application/json' -d '" . $js

my $results = exec($curl_request);
```

delete_domain.pl:

```
#!/usr/bin/perl -w

# Custom integration - DELETE URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/domains?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $curl_request = "curl '" . $cust_key . "&where[name]=" . $domain . "' -v -i -g -X DELETE -H 'Content
my $results = exec($curl_request);
```

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。