Secure Malware Analytics（以前のThreat Grid）とUmbrellaの統合の設定

内容

はじめに

このドキュメントでは、Secure Malware Analytics（以前のThreat Grid）をUmbrellaと統合する方法について説明します。

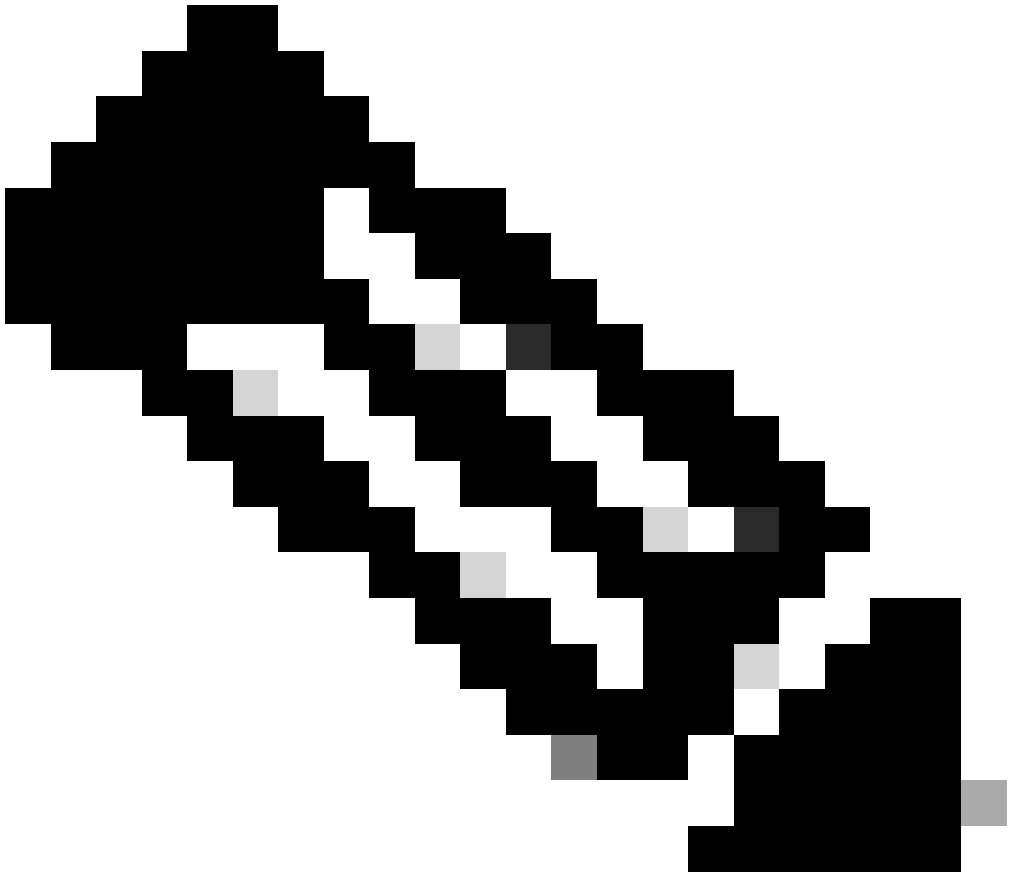
Cisco Secure Malware Analytics(Threat Grid)Integration for Cisco Umbrellaの概要

Cisco Secure Malware Analytics（以前のThreat Grid）とCisco Umbrellaの統合により、セキュリティチームは可視性を拡張し、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高度な脅威に対して保護を適用しながら、分散型企業ネットワークに別の適用レイヤを提供できます。

このガイドでは、Cisco Secure Malware Analytics(Threat Grid)によって生成された脅威インテリジェンスを、Cisco Umbrellaでクライアントを保護できるポリシーに自動的に統合できるように、Cisco Secure Malware Analytics(Threat Grid)をCisco Umbrellaと通信するように設定する方法について説明します。

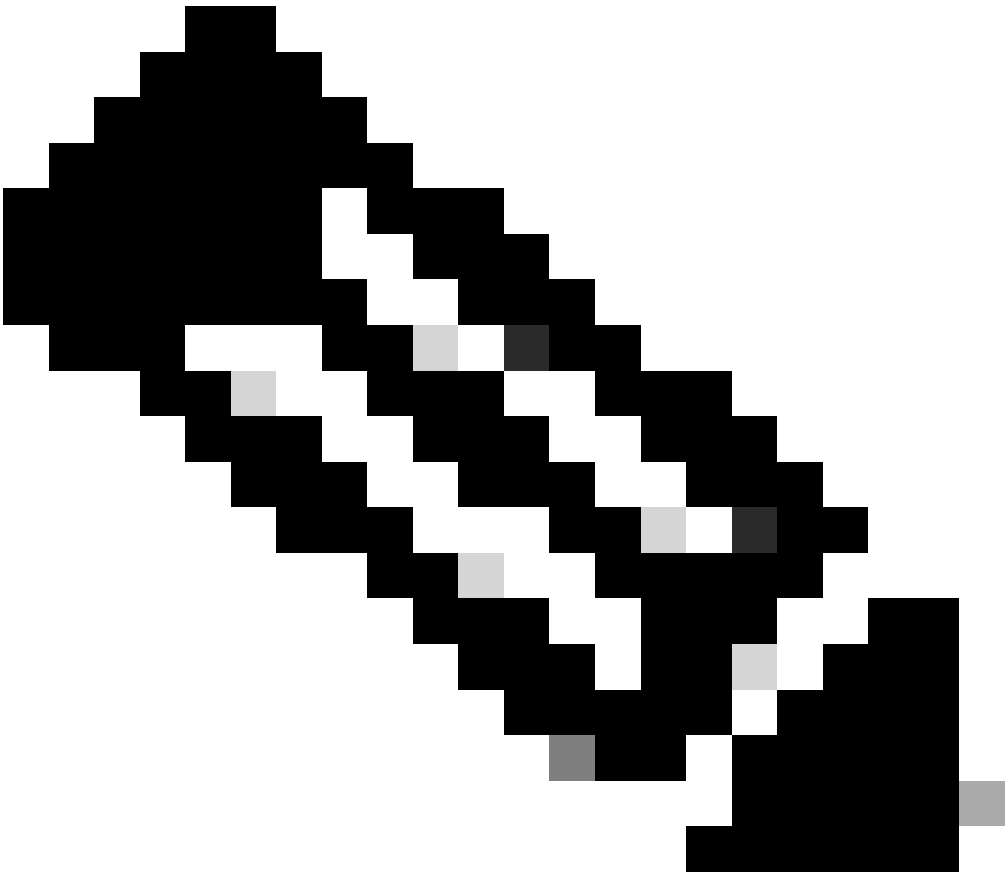
前提条件

- お客様のアカウントのAPIキーにアクセスできる、機能的なCisco Secure Malware Analytics(Threat Grid)ダッシュボード



> 注:Cisco Secure Malware Analytics(Threat Grid)アプライアンスおよびエンドポイントは、現時点ではサポートされていません。

- Cisco Umbrellaダッシュボードの管理者権限
- Cisco Umbrellaダッシュボードでは、Cisco Secure Malware Analytics(Threat Grid)統合を有効にする必要があります。



注:Cisco Secure Malware Analytics(Threat Grid)の統合は、DNS Essentials、DNS Advantage、SIG Essentials、SIG AdvantageなどのCisco Umbrellaパッケージにのみ含まれています。Cisco Umbrellaパッケージを所有しておらず、この統合を希望される場合は、Cisco Umbrellaアカウントマネージャにお問い合わせください。Cisco Umbrellaパッケージを所有しているが、ダッシュボードの統合としてCisco Secure Malware Analytics(Threat Grid)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。

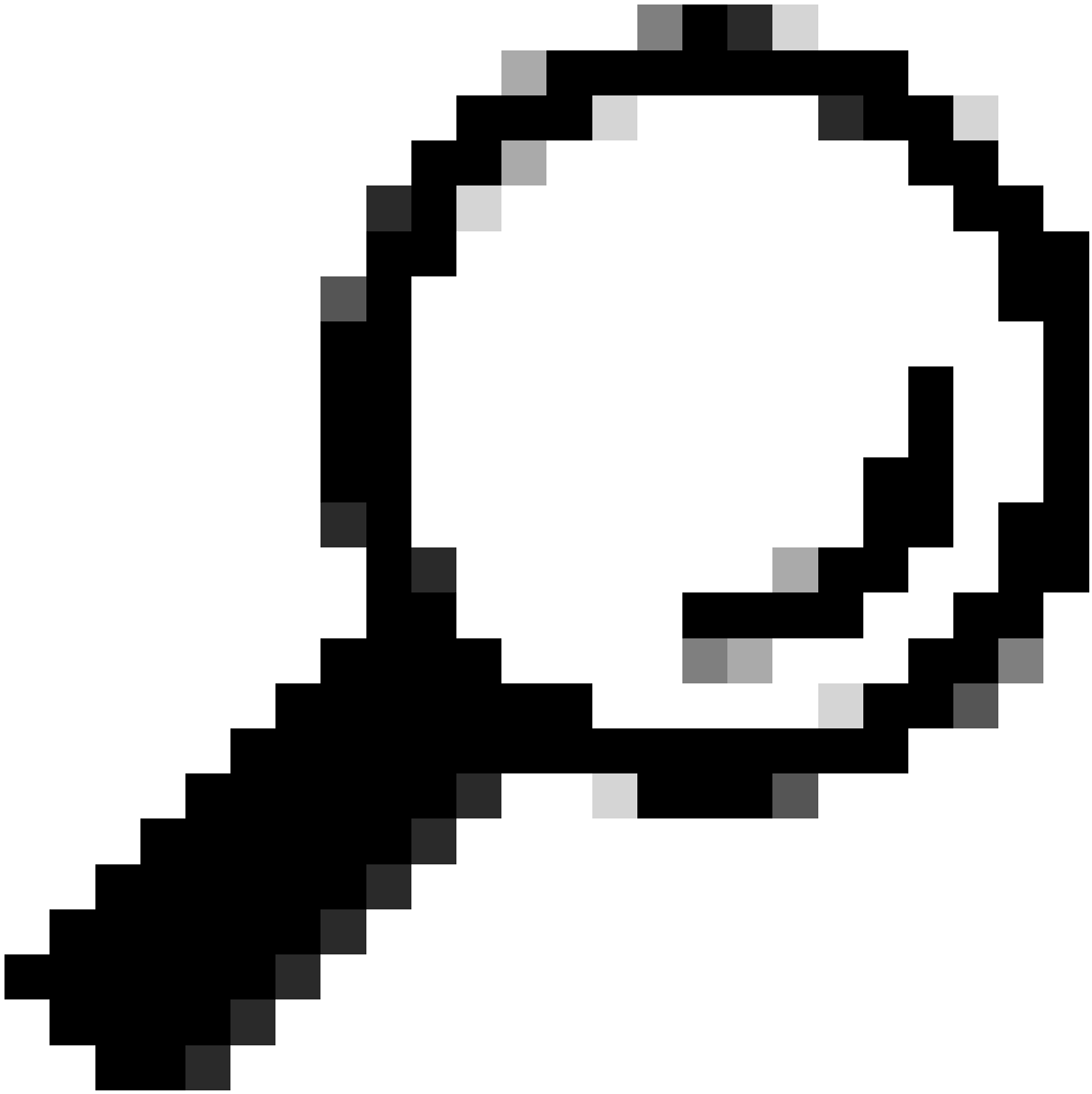
この統合の仕組みを教えてください。

Cisco Umbrellaは、Cisco Secure Malware Analytics(Threat Grid)APIにアクセスし、悪意のあるサンプルの分析から生成されたドメインリストを取得します。Cisco Umbrellaは、Cisco Umbrella Enforcement APIを介してこのリストをインポートします。このアプローチは、Cisco Umbrellaサービスに脅威インテリジェンスをプッシュする他のシステムからのインシデントを受け入れるのではなく、Cisco UmbrellaがCisco Secure Malware Analytics(Threat Grid)APIにAPIクエリを実行して脅威インテリジェンスをプルするという、他の統合の仕組みとは異なります。

その後、Cisco 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。Cisco

Secure Malware Analytics(Threat Grid)からの情報が脅威であることが確認された場合、または既知の適切なドメインでない場合、ドメインアドレスは、任意のCisco Umbrellaポリシーに適用可能なセキュリティ設定の一部として、Cisco Secure Malware Analytics(Threat Grid)宛先リストに追加されます。このポリシーは、Cisco Secure Malware Analytics(Threat Grid)の統合を利用するポリシーを使用してデバイスから行われたすべての要求に即座に適用されます。

Cisco Umbrellaは、Cisco Secure Malware Analytics(Threat Grid)から、パブリック（グローバル）フィードとカスタマー専用（プライベート、1つのカスタマー専用）フィードの2つの個別のフィードを取得します。



ヒント:Cisco Umbrellaは、一般的に安全であることが確認されているドメイン（GoogleやSalesforceなど）を検証および許可するために最善を尽くしますが、不要な中断を避けるために、ブロックしたくないすべてのドメインをポリシーに従ってGlobal Allow List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。
- 提供するサービスを表すドメインで、内部レコードと外部レコードの両方を持つ可能性があります。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ため、Cisco Umbrellaがドメインの自動検証を認識していない、または自動検証に含まれていない可能性があります。例：「localcloudservice.com」。

これらのドメインは、Cisco UmbrellaのPolicies > Destination ListsにあるGlobal Allow Listに追加する必要があります。

Cisco Secure Malware Analytics(Threat Grid)から情報を取得するためのCisco Umbrellaダッシュボードの設定

最初のステップは、Cisco Secure Malware Analytics(Threat Grid)ダッシュボードでAPIキーを見つけるか、生成することです。

1. Cisco Secure Malware Analytics(Threat Grid)ダッシュボードにログインし、アカウントの詳細を選択します。
2. すでにAPIキーを作成している場合は、アカウントの詳細にAPIキーがすでに表示されている可能性があります。まだ作成していない場合は、[新しいAPIキーの生成]を選択します。

   これで、APIキーがUser Details > API Keyの下に表示されます。

次に、Cisco UmbrellaダッシュボードにAPIキーを追加して、Cisco Secure Malware Analytics(Threat Grid)からデータを取得します。

1. Cisco Umbrellaダッシュボードに管理者としてログインします。
2. Policies > Policy Components > Integrations の順に移動し、テーブルで「Cisco AMP Threat Grid」(Cisco Secure Malware Analytics(Threat Grid))を選択して展開します。
3. Enableを選択し、API KeyボックスにAPI Keyをペーストしてから、Saveを選択します。

この時点でエラーが発生した場合は、APIキーまたはサービス間の通信に問題がある可能性があります。APIキーを確認して再試行し、それでも失敗する場合は、Cisco Umbrellaサポートに連絡してください。

成功のメッセージが表示された場合は、Cisco UmbrellaサービスがAPIキーを使用してCisco Secure Malware Analytics(Threat Grid)APIに最初に接続できたことが示されています。Cisco Umbrellaサービスは、5分のポーリング間隔を使用して、Cisco Secure Malware Analytics(Threat Grid)からデータを取得します。

5分インターバルの後でも、Cisco Umbrellaダッシュボードによってプルされる有効なデータまたは有効な脅威イベントがない場合、情報が表示されないことがあります。統合が最初に有効にされたときには、5分前までさかのぼってグローバルフィードと組織のみのフィードの両方のデータを取得し、最初にデータを取得したのは次の5分インターバルであるため、データがすぐに表示さ

れない可能性があります。

Cisco Secure Malware Analytics(Threat Grid)側のAPIキーが無効化または削除されると、統合は無効になります。統合を復元するには、Cisco Umbrellaダッシュボードで新しいAPIキーを指定する必要があります。Cisco UmbrellaとCisco Secure Malware Analytics(Threat Grid)の間でタイムアウトまたは内部サービスエラーが発生した場合、異なる種類の例外が発生し、統合は無効になりませんが、接続は通常の状態と同様に5分ごとに試行され続けます。

技術詳細

Cisco Secure Malware Analytics(Threat Grid)から情報を取得するために使用される正確なAPIクエリを次に示します。重大度が90より大きく、信頼度が90より大きく、タイプがDomainsのイベントだけが収集されていることに注意してください。この例では、時間は5分の範囲で、次のクエリに対してインクリメントされます。Cisco Umbrellaで提供されている`api_key`は、`<key>`変数の代わりに使用されます。

- パブリック (グローバルフィード) :

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- お客様のみ (プライベートフィード) :

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

または

- パブリック (グローバルフィード) :

```
 hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

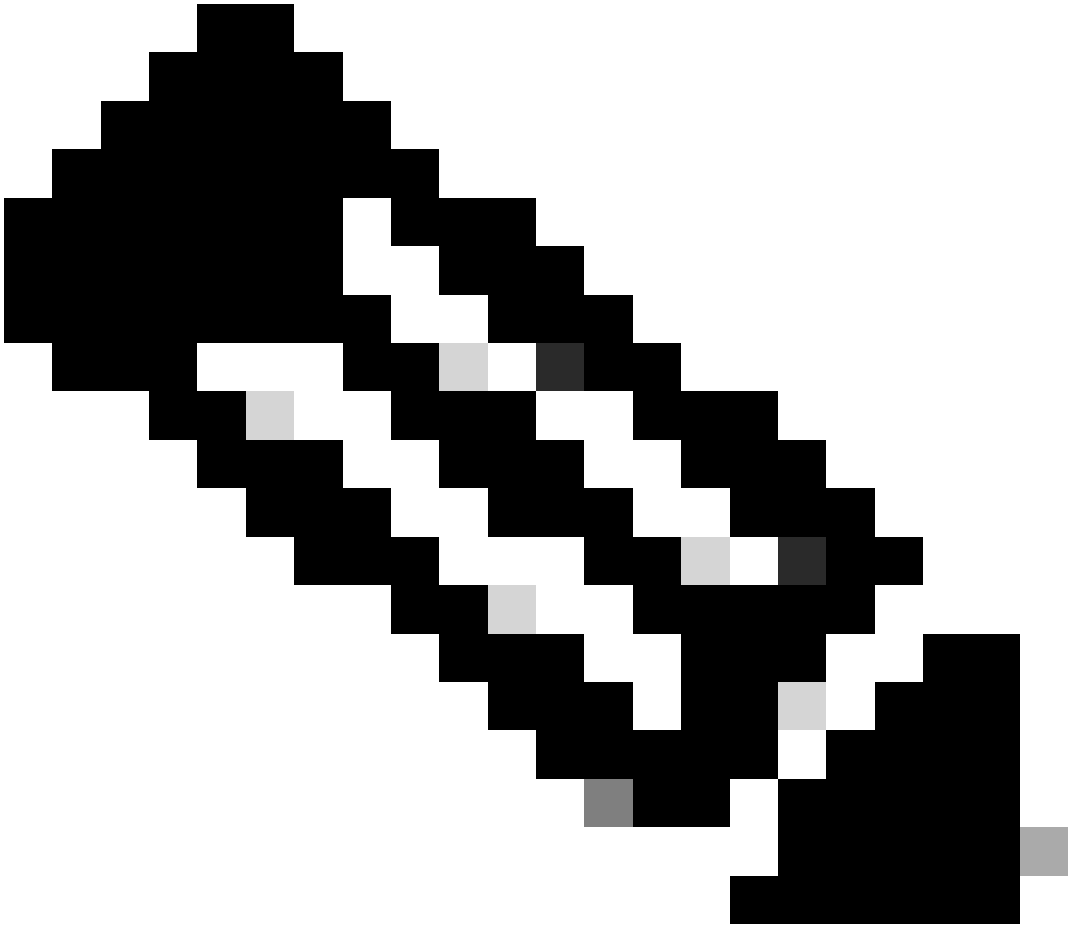
- お客様のみ (プライベートフィード) :

```
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence=
```

「監査モード」でCisco Secure Malware Analytics(Threat Grid)に追加されたイベントの監視

Cisco Secure Malware Analytics(Threat Grid)からのイベントは、時間の経過とともに、Cisco Secure Malware Analytics(Threat Grid)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」であり、ポリシーには適用されません。そのため、要求がブロックされることはありません。ただし、Cisco AMP Threat Gridセキュリティカテゴリに関連付けられている（ブロックされている可能性がある）要求を確認できます。



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応じて、必要な期間だけ、または無期限に有効にできます。

宛先リストの確認

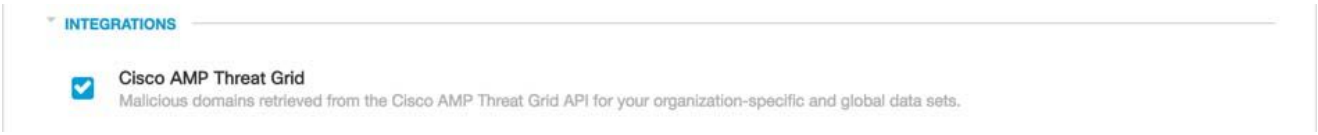
Cisco Secure Malware Analytics(Threat Grid)Destination Listはいつでも確認できます。

1. Policies > Policy Components > Integrationsの順に移動します。
2. テーブルで「Cisco AMP Threat Grid」(Cisco Secure Malware Analytics(Threat Grid))を展開し、「ドメインを表示」を選択します。

ポリシーのセキュリティ設定の確認

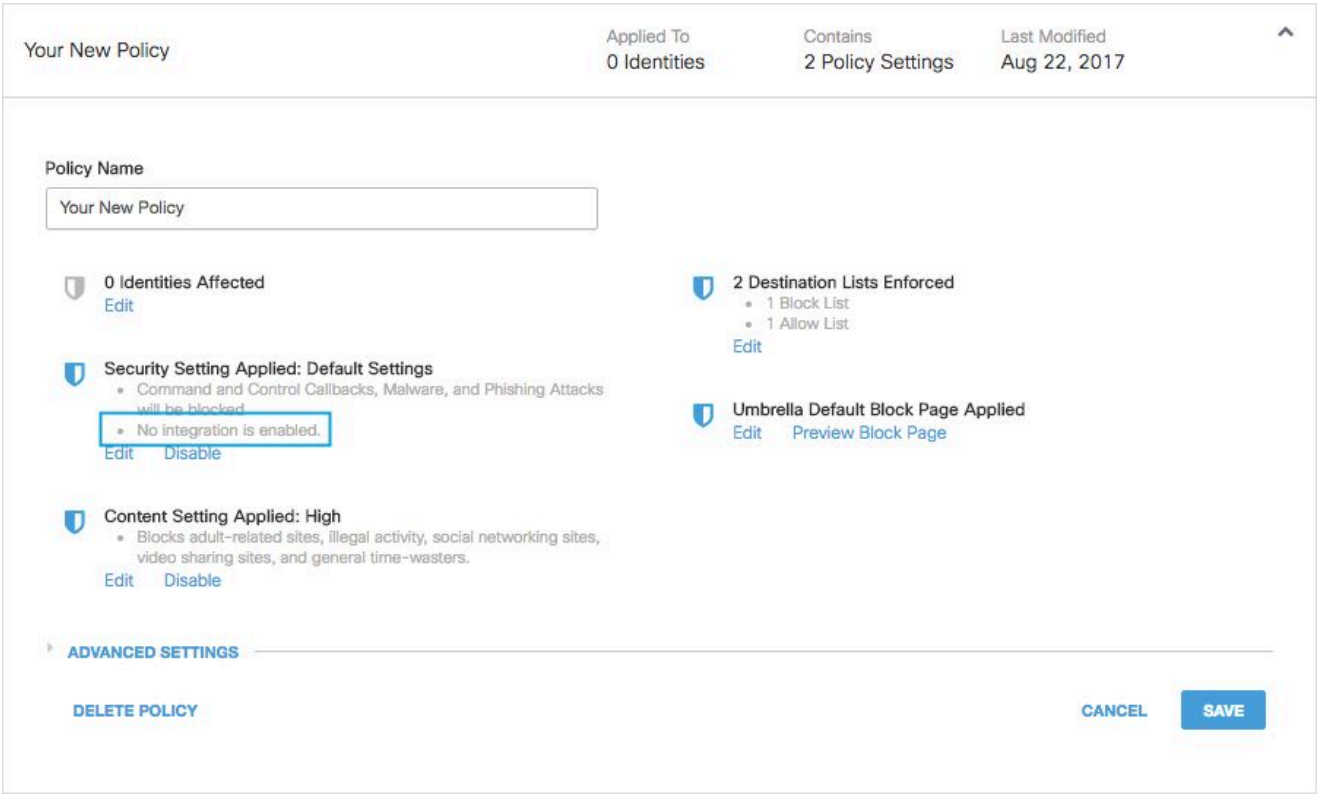
ポリシーに対して有効にできるセキュリティ設定は、Cisco Umbrellaでいつでも確認できます。

1. Policies > Policy Components > Security Settingsの順に移動します。
2. 表のセキュリティ設定をクリックして展開します。
3. 統合セクションまでスクロールし、セクションを展開して、Cisco AMP Threat Grid(Cisco Secure Malware Analytics(Threat Grid))統合を表示します。
4. Cisco AMP Threat Grid統合(Cisco Secure Malware Analytics(Threat Grid))のボックスを選択し、Saveを選択します。

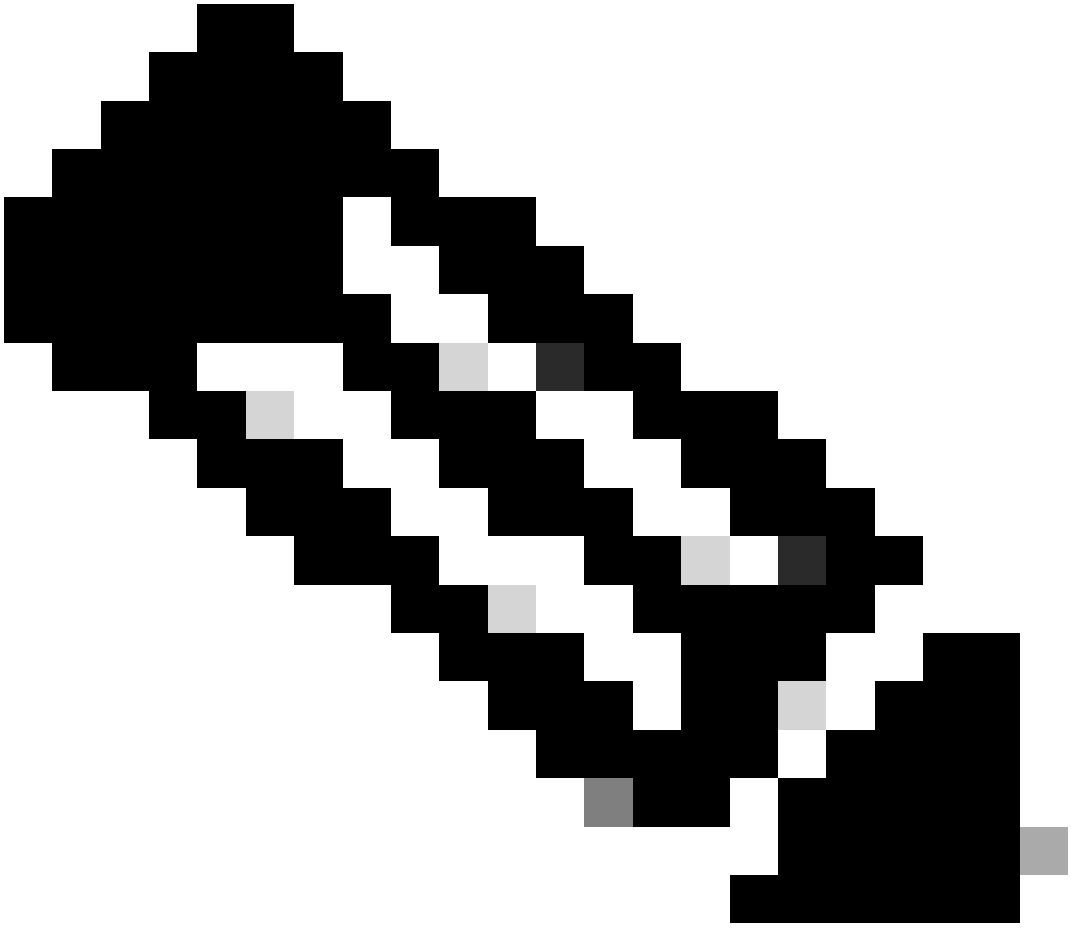


115014151543

統合情報は、[セキュリティ設定の概要]ページでも確認できます。



20993269073556

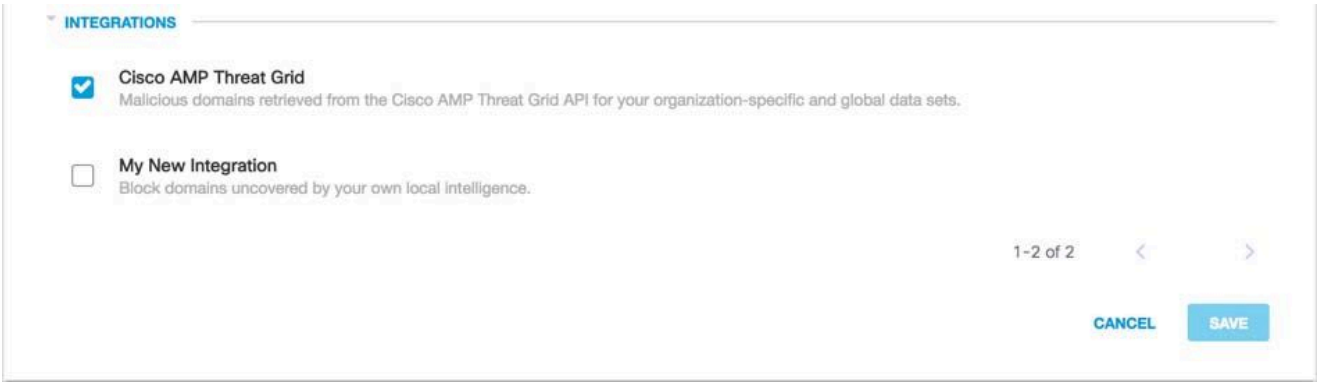


注：設定の適用には最大5分かかります。新しいイベントがCisco Secure Malware Analytics(Threat Grid)システムに挿入されない場合、統合に新しいドメインが追加されない可能性があります。

「ブロックモード」でのCisco Secure Malware Analytics(Threat Grid)セキュリティ設定のマネージドクライアントのポリシーへの適用

Cisco Umbrellaによって管理されるクライアントに対してこれらのドメインをブロック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、または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。

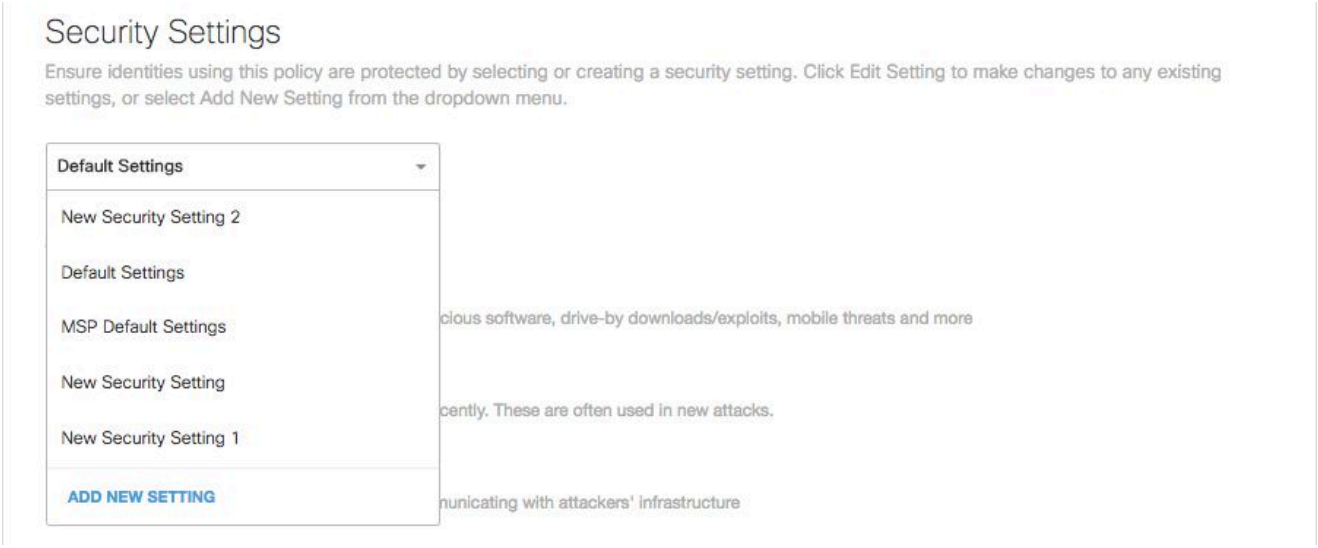
1. Policies > Policy Components > Security Settingsの順に移動します。
2. Integrationsの下で、「Cisco AMP Threat Grid」ボックスが選択されていることを確認します。そうでない場合は、ボックスを選択して、Saveを選択します。



115013987086

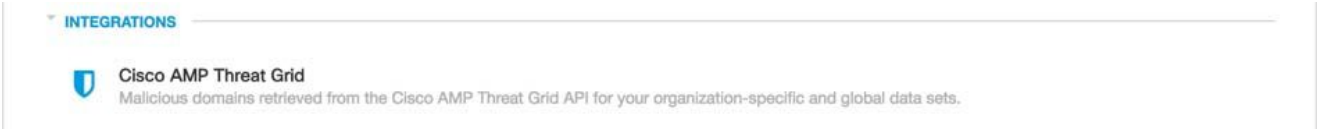
次に、Cisco Umbrellaポリシーウィザードで、編集中のポリシーにセキュリティ設定を追加します。

1. Policies > Management > All Policies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、「Cisco AMP Threat Grid」を含むセキュリティ設定を選択します。



20993282642708

「統合」の下のシールドアイコンが青色に更新されます。



115013987446

4. Set & Returnを選択します。

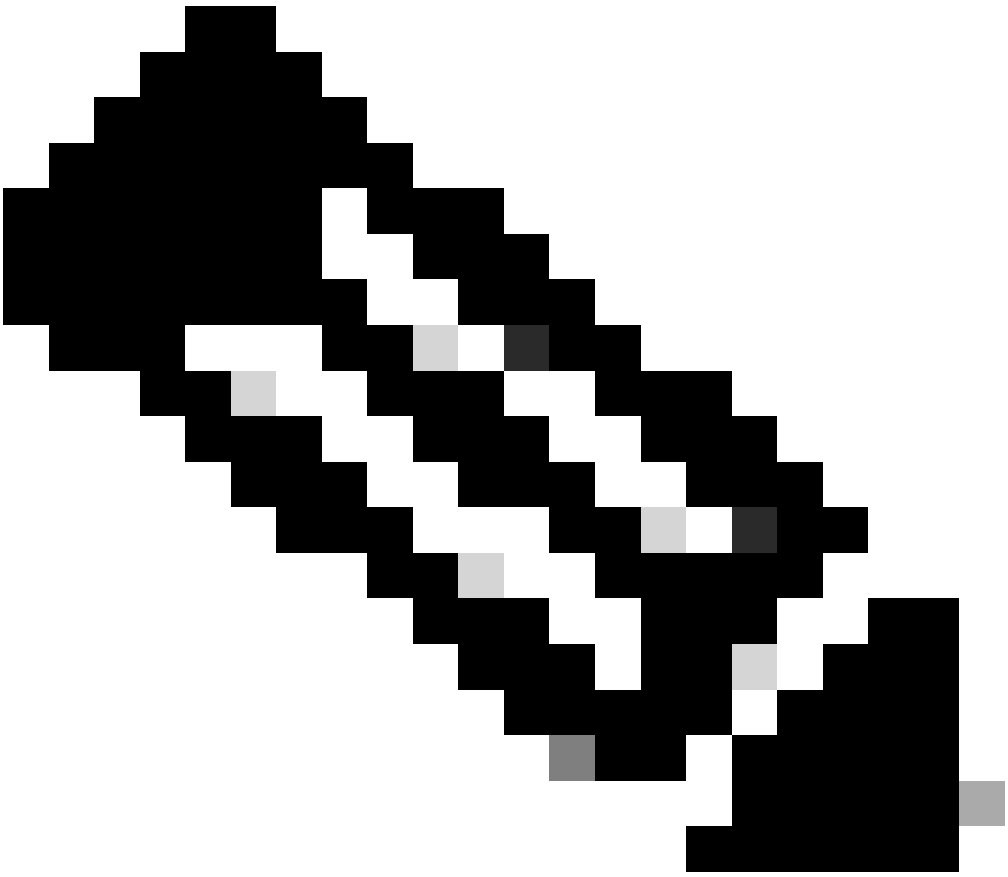
   Cisco Secure Malware Analytics(Threat Grid)のセキュリティ設定内に含まれるCisco Secure Malware Analytics(Threat Grid)ドメインは、ポリシーを使用してこれらのIDに対してブロックされます。

Cisco Secure Malware Analyticsイベントに関するCisco Umbrella内のレポート

Cisco Secure Malware Analytics(Threat Grid)セキュリティイベントに関するレポート

Cisco Secure Malware Analytics(Threat Grid)の宛先リストは、レポート対象の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、Cisco Secure Malware Analytics(Threat Grid)関連のアクティビティのみを表示できます。

1. レポート>コアレポート>アクティビティ検索に移動し、セキュリティカテゴリで「Cisco AMP Threat Grid」(Cisco Secure Malware Analytics(Threat Grid))を選択してレポートをフィルタリングし、Cisco Secure Malware Analytics(Threat Grid)のセキュリティカテゴリのみが表示されるようにします。



注:Cisco AMP Threat Grid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。

115014210123

2. Applyを選択します。

Cisco Secure Malware Analytics(Threat Grid)の宛先リストにドメインが追加された日時のレポート

Cisco 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Cisco Secure Malware Analytics(Threat Grid)ダッシュボードからのイベントが含まれます。「Cisco AMP Threat Gridドメインリスト」という名前のユーザが、イベントを生成します。このユーザはシスコのロゴも使用しています。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。

Admin Audit Logエントリを選択すると、エントリが展開され、追加された特定のドメインを含む詳細が表示されます。

「Cisco AMP Threat Gridドメインリスト」ユーザのフィルタを適用すると、Cisco Secure Malware Analytics(Threat Grid)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

2種類のCisco Secure Malware Analytics(Threat Grid)検出および2つの解決策

現在、Cisco Secure Malware Analytics(Threat Grid)ブロックには2つのタイプがあります。1つは可能な解決策を1つ、もう1つは不要な検出に対する現在の解決策を1つ持ちます。

1. Global Threat Gridエントリ（パブリック）:現時点では、ドメインを許可する唯一の方法は、許可リストにドメインを追加することです。
2. カスタマー専用フィード（プライベート）:許可リストのエントリまたはAMP Threat Grid統合リストからの削除で対処できます。

許可リスト

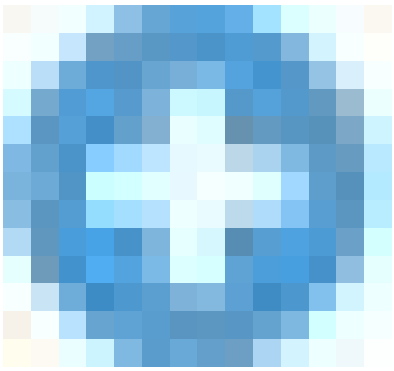
まれに、Cisco Secure Malware Analytics(Threat Grid)の統合によって自動的に追加されたドメインが、ユーザによる特定のWebサイトへのアクセスをブロックする望ましくない検出をトリガーする可能性があります。このような状況では、許可リスト(Policies > Destination Lists)にドメインを追加することを推奨します。この許可リストは、セキュリティ設定を含め、他のすべてのタイプのブロックリストよりも優先されます。

このアプローチが推奨される理由は2つあります。まず、Cisco Secure Malware Analytics(Threat Grid)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、この問題がさらに発生する可能性を防ぎます。次に、許可リストには、調査レポート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Cisco Secure Malware Analytics(Threat Grid)セキュリティ設定が、管理対象のCisco Umbrellaアイデンティティのサブセットにのみ適用される（たとえば、ローミングコンピュータとモバイルデバイスにのみ適用される）場合、これらのアイデンティティ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 > Policy Components > Destination Listsの順に移動し、

   25463394696852

   （「追加」）。

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。

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。

Cisco Secure Malware Analytics(Threat Grid)の宛先リストからのドメインの削除

Cisco Secure Malware Analytics(Threat Grid)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Cisco Secure Malware Analytics(Threat Grid)の宛先リストをクリーンアップできます。

Cisco Secure Malware Analytics(Threat Grid)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。

1. Policies > Policy Components > Integrations の順に移動し、「Cisco AMP Threat Grid」(Cisco Secure Malware Analytics(Threat Grid))を選択して展開します。
2. See Domains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。

不要な検出や誤検出が発生した場合は、Cisco Umbrellaで許可リストを即座に作成し、Cisco Secure Malware Analytics(Threat Grid)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、Cisco Secure Malware Analytics(Threat Grid)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。