セキュリティ インテリジェンス

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。ここでは、セキュリティ インテリジェンスの実装方法について説明します。

- セキュリティ インテリジェンスについて （1 ページ）
- セキュリティ インテリジェンスのためのライセンス要件 （3 ページ）
- セキュリティ インテリジェンスの設定 （3 ページ）
- セキュリティ インテリジェンスのモニタリング （5 ページ）
- セキュリティ インテリジェンスの例 （5 ページ）

セキュリティ インテリジェンスについて

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。システムは、ブラックリストに登録されたこのトラフィックをアクセス コントロール ポリシーで評価する前にドロップすることにより、使用されるシステム リソースの量を減らします。

次に基づいてトラフィックをブラックリストに登録できます。

- Cisco Talos Intelligence Group（Talos） フィード：Talos定期的に更新されるセキュリティ インテリジェンス フィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。システムはフィードの更新を定期的にダウンロードするため、設定を再導入する必要なく新しい脅威インテリジェンスを利用できます。

（注） Talos フィードはデフォルトで 1 時間ごとに更新されます。**[デバイス（Device）] > [更新（Updates）]** ページからは、更新頻度を変更するだけでなく、オンデマンドでフィードを更新することもできます。

- ネットワークおよびURL オブジェクト：ブロック対象の IP アドレスまたは URL が既知の場合は、それらのオブジェクトを作成し、それらをブラックリスト（またはホワイトリストとも呼ばれる例外リスト）に追加できます。

IP アドレス（ネットワーク）と URL で別のブラックリストを作成します。

ブラックリストの例外の作成

各ブラックリストには関連付けられた例外リストを作成でき、これはホワイトリストとも呼ばれます。例外リストの唯一の目的は、ブラックリストに表示される IP アドレスまたは URL を除外することです。つまり、使用する必要があり、安全であることがわかっているアドレスや URL が、ブラックリストに設定されているフィードにある場合、ブラックリストから完全にカテゴリを削除せずに、そのネットワーク/URL を除外できます。

除外された、またはホワイトリストに登録されたトラフィックは、以後アクセス コントロール ポリシーによって評価されます。接続が許可またはドロップされたかどうかの最終決定は、接続に一致するアクセス制御ルールに基づきます。また、アクセス ルールは接続に侵入やマルウェア検査を適用するかどうかも判断します。

セキュリティ インテリジェンス フィード カテゴリ

次の表では、Cisco Talos Intelligence Group（Talos） フィードで使用可能なカテゴリについて説明します。これらのカテゴリは、ネットワークと URL のブラックリストの両方に使用できます。

表 *1 : Talos* フィードのカテゴリ

カテゴリ	説明
attackers	アウトバウンドの悪意のあるアクティビティで知られている、アクティブなスキャナとブラックリストに登録されたホスト。
bogon	bogon ネットワークと未割り当て IP アドレス。
bots	バイナリ マルウェア ドロッパーをホストするサイト。
CnC	ボットネットの指示管理サーバをホストするサイト。
dga	指示管理サーバでランデブーポイントとして動作する多数のドメイン名の生成に使用されるマルウェア アルゴリズム。
exploitkit	クライアントでのソフトウェアの脆弱性を識別するために設計されたソフトウェア キット。
malware	マルウェア バイナリまたはエクスプロイト キットをホストするサイト。
open_proxy	匿名での Web ブラウジングを許可するオープン プロキシ。

カテゴリ	説明
open_relay	スパムに使用されることが知られているオープン メール リレー。
phishing	フィッシング詐欺のページをホストするサイト。
response	悪意のある、または不審なアクティビティに積極的に参加している IP アドレスおよび URL。
spam	スパムの送信で知られているメール ホスト。
suspicious	疑わしく、既知のマルウェアのような特性を持っていると思われるファイル。
tor_exit_node	Tor の出口ノード。

セキュリティインテリジェンスのためのライセンス要件

セキュリティ インテリジェンスを使用するには、**脅威**ライセンスを有効にする必要があります。オプション ライセンスの有効化と無効化を参照してください。

セキュリティ インテリジェンスの設定

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティインテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[セキュリティインテリジェンス（Security Intelligence）]** の順に選択します。

ステップ 2 ポリシーが有効になっていない場合は、[セキュリティインテリジェンスの有効化（Enable Security Intelligence）] ボタンをクリックします。

[セキュリティインテリジェンス（Security Intelligence）] をクリックして [オフ（Off）] にすることで、いつでもポリシーを無効にできます。設定は維持されるため、ポリシーを再度有効にするときに再設定する必要はありません。

ステップ 3 セキュリティ インテリジェンスを設定します。

ネットワーク（IP アドレス）と URL には別々のブラック リストがあります。

a) [ネットワーク（Network）] または [URL] タブをクリックして、構成するブラックリストを表示します。

b) [ブラックリスト（Blacklist）] で、[+] をクリックして接続をすぐにドロップするオブジェクトまたはフィードを選択します。

オブジェクトセレクタは、種類によってオブジェクトおよびフィードを別々のタブに整理します。希望するオブジェクトがまだ存在しない場合、リストの下部にある [新しいオブジェクトの作成（Create New Object）] リンクをクリックして作成します。Cisco Talos Intelligence Group（Talos）フィードの説明については、フィードの横にある [i] ボタンをクリックしてください。セキュリティ インテリジェンス フィード カテゴリ （2 ページ）も参照してください。

（注） セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。これには、any-ipv4 と any-ipv6 のネットワーク オブジェクトが含まれます。ネットワークのブラックリストにこれらのオブジェクトを選択しないでください。

c) [ブロックしない（Do Not Block）] リストで、[+] をクリックしてブラックリストの例外をすべて選択します。

このリストを構成する唯一の理由は、ブラックリストにある IP アドレスまたは URL を例外にすることです。適用除外された接続は、その後アクセス制御ポリシーによって評価され、いずれにしても破棄される可能性があります。

d) 他のブラックリストを構成するには上記の手順を繰り返します。

ステップ 4 （オプション）[ログ設定の編集（Edit Logging Settings）] ボタン（ ）をクリックしてログを設定します。

ロギングを有効にした場合は、ブラックリストのエントリに一致するものが記録されます。ロギングを有効にして、除外された接続がアクセス制御ルールに一致した場合、ログ メッセージは取得しますが例外エントリに一致するものは記録されません。

次を設定します。

- [接続イベントロギング（Connection Events Logging）]：クリックしてロギングを有効または無効に切り替えます。
- [Syslog]：外部の syslog サーバにイベントのコピーを送信するには、このオプションを選択して、syslog サーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトが存在しない場合は、[新しいSyslogサーバの追加（Add Syslog Server）] をクリックして作成します。

  デバイスのイベント ストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

セキュリティ インテリジェンスのモニタリング

セキュリティ インテリジェンス ポリシーのログ記録を有効にすると、システムはブラックリストに追加された接続ごとにセキュリティ インテリジェンス イベントを生成します。これらの接続に一致する接続イベントがあります。

ブラックリストに追加されたドロップされた接続の統計情報は、[モニタリング（Monitoring）] ページの、使用可能なさまざまなダッシュボードに表示されます。

[モニタリング（Monitoring）] > [アクセスおよびSIルール（Access and SI Rules）] ダッシュボードに、トラフィックと一致する、上位のアクセス ルールとセキュリティ インテリジェンスに相当するルールが表示されます。

さらに、**[モニタリング（Monitoring）] > [イベント（Events）]**、次に [セキュリティインテリジェンス（Security Intelligence）] を選択して、セキュリティ インテリジェンス イベントと、関連する接続イベントを [接続（Connection）] タブに表示できます。

- イベントの [SIカテゴリID（SI Category ID）] フィールドは、ネットワークまたは URL オブジェクトあるいはフィードなど、ブラックリストに一致するオブジェクトを示します。
- 接続イベントの [理由（Reason）] フィールドは、イベントに表示されたアクションが適用された理由について説明します。たとえば、ブロック アクションは、IP ブロックまたは URL ブロックなどの理由と組み合わされて、接続がブラックリストに追加され、セキュリティ インテリジェンスによってドロップされたことを示します。

セキュリティ インテリジェンスの例

使用例の章には、セキュリティ インテリジェンス ポリシーの実装例が含まれています。脅威をブロックする方法を参照してください。