セキュリティ インテリジェンス

以下のトピックでは、セキュリティインテリジェンスの概要（トラフィックのブロックリストと許可リストの使用、基本設定など）を示します。

セキュリティ インテリジェンスについて

悪意のあるインターネットコンテンツに対する防御の前線として、セキュリティインテリジェンスは疑わしい IP アドレス、URL、ドメイン名が関連する接続をレピュテーション インテリジェンスを使用して迅速にブロックします。これは、セキュリティ インテリジェンス ブロック リストと呼ばれます。

セキュリティインテリジェンスはアクセス制御の初期のフェーズであり、大量のリソースを消費する評価をシステムが実行する前に行われます。ブロックリストにより、インスペクションの必要がないトラフィックを迅速に除外できるため、パフォーマンスが向上します。

（注） ブロックリストを使用して、高速パストラフィックをブロックすることはできません。プレフィルタ評価の実行は、セキュリティインテリジェンスによるフィルタリングの前に行われます。FastPath が適用されたトラフィックは、セキュリティ インテリジェンスを含め、以降のすべての評価をバイパスします。

カスタムのブロックリストを設定できますが、シスコでは定期的に更新されるインテリジェンスフィードへのアクセスを提供しています。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。

ブロックしないリストとモニター専用ブロックリストを使用して、セキュリティインテリジェンスブロックリスト機能の精度を上げることができます。これらのメカニズムは、ブロックリストによりトラフィックがブロックされないようにしますが、一致するトラフィックを自動的に信頼したり FastPath を適用したりすることは**しません**。ブロックしないリストに追加されたトラフィックや、セキュリティインテリジェンスの段階でモニターされるトラフィックは、意図的に残りのアクセスコントロールによる分析が適用されます。

関連トピック

セキュリティ インテリジェンス

セキュリティ インテリジェンスのベストプラクティス

- システムが提供するセキュリティ インテリジェンス フィードによって検出されたすべての脅威をブロックするようにアクセス コントロール ポリシーを設定します。設定例：セキュリティインテリジェンスブロック （12 ページ）を参照してください。
- シスコが提供するセキュリティ インテリジェンス フィードをカスタム脅威データで補足する場合、または新しい脅威を手動でブロックする場合は、次のようにします。
  - IP アドレスの場合は、カスタムのセキュリティ インテリジェンスのリストおよびフィードか、ネットワークオブジェクトまたはグループを使用します。これらを作成するには、セキュリティインテリジェンスおよびネットワークとそのサブトピックを参照してください。これらをセキュリティインテリジェンスに使用するには、セキュリティ インテリジェンスの設定 （5 ページ）を参照してください。セキュリティ インテリジェンス ポリシーで使用されるネットワークオブジェクトには、IPS ライセンスが必要です。
  - IP とドメインの場合は、カスタムのセキュリティ インテリジェンスのリストおよびフィードを使用し、オブジェクトまたはグループは使用しません。詳細については、手動 URL フィルタリングオプションを参照してください。
  - イベントからブロックリストにエントリを追加することもできます。グローバルおよびドメインのセキュリティインテリジェンスリストを参照してください。
- 新しいフィードをテストする場合、またはパッシブ展開の場合は、アクションをブロックからモニターのみに設定します。セキュリティ インテリジェンス モニタリング （13 ページ）を参照してください。
- 特定のサイトまたはアドレスをセキュリティインテリジェンスのブロッキングから除外する必要がある場合は、セキュリティ インテリジェンス ブロッキングのオーバーライド （14 ページ）を参照してください。

- Firepower 展開が SecureX または関連ツールの SecureX Threat Response（以前は Cisco Threat Response または CTR と呼ばれていました）と統合されていて、カスタムのセキュリティ インテリジェンスのリストおよびフィードを使用している場合は、そのリストとフィードで Security Services Exchange を必ず更新します。詳細については、Security Services Exchange のオンラインヘルプでイベントの自動プロモーションを設定するための手順を参照してください。この統合に関する一般的な情報については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Integrate with Cisco SecureX」を参照してください。
- システムで提供されるセキュリティ インテリジェンスのカテゴリは、時間の経過とともに通知なしに変更される場合があります。定期的に変更を確認し、それに応じてポリシーを変更することを計画する必要があります。
- また、悪意のあるサイトからの保護を強化するために、URL フィルタリング（個別のライセンス要件がある個別の機能）を設定する必要もあります。URL フィルタリング を参照してください。

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

Threat Defense ライセンス

IPS

従来のライセンス

保護

セキュリティ インテリジェンスの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

重要 SIポリシーを正常に適用するには、デバイスにネットワーク検出ポリシーを適用する必要があります。

セキュリティ インテリジェンス送信元

- システムが提供するフィード

  シスコは、ドメイン、URL、およびIPアドレスについて定期的に更新されるインテリジェンスフィードへのアクセスを提供します。詳細については、セキュリティインテリジェンスを参照してください。

  名前に「TID」が含まれるフィードがある場合、このフィードはセキュリティ インテリジェンスによって使用されません。代わりに、このフィードは、Secure Firewall Threat Intelligence Directorで説明されている機能によって使用されます。

- サードパーティフィード

  オプションで、Cisco 提供のフィードをサードパーティのフィードで補完できます。これらのフィードは、Secure Firewall Management Center が定期的にインターネットからダウンロードする動的リストです。カスタム セキュリティ インテリジェンス フィードを参照してください。

- カスタムブロックリストまたはフィード（またはオブジェクトまたはグループ）

  手動で作成したリストまたはフィードを使用して、特定の IP アドレス、URL、またはドメイン名をブロックします（IPアドレスの場合、ネットワークオブジェクトまたはグループを使用することもできます）。

  たとえば、フィードによってまだブロックされていない悪意のあるサイトまたはアドレスに気付いた場合は、これらのサイトをカスタム セキュリティ インテリジェンス リストに追加し、このカスタムリストをアクセス コントロール ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブでブロックリストに追加します。カスタムセキュリティ インテリジェンス リストおよびセキュリティ インテリジェンスの設定 （5 ページ）を参照してください。

  IPアドレスの場合、リストやフィードではなく、オプションでネットワークオブジェクトをこの目的に使用できます。詳細については、ネットワークを参照してください（URLの場合、他の方法よりもリストとフィードを使用することを強くお勧めします）。

- カスタムのブロックしないリストまたはフィード

  特定のサイトまたはアドレスのセキュリティインテリジェンスブロックを無効にします。セキュリティ インテリジェンス ブロッキングのオーバーライド （14 ページ）を参照してください。

- グローバルブロックリスト（ネットワーク、URL、DNS ごとに 1 つ）

イベントの確認中に、セキュリティインテリジェンスがそのソースからの今後のトラフィックを処理する場合は、イベントの IP アドレス、URL、またはドメインを該当するグローバルブロックリストにすぐに追加できます。グローバルおよびドメインのセキュリティインテリジェンスリストを参照してください。

- グローバルブロックしないリスト（ネットワーク、URL、DNS ごとに 1 つ）

  イベントの確認中に、セキュリティインテリジェンスがそのソースからの今後のトラフィックをブロックしたくない場合は、イベントの IP アドレス、URL、またはドメインを該当するグローバルブロックしないリストにすぐに追加できます。グローバルおよびドメインのセキュリティインテリジェンスリスト 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

各アクセス コントロール ポリシーには、セキュリティ インテリジェンス オプションがあります。ネットワークオブジェクト、URL オブジェクトとリスト、およびセキュリティ インテリジェンスフィードとリストをブロックリストまたはブロックしないリストに追加でき、これらはすべてセキュリティゾーンによって制約できます。アクセス コントロール ポリシーに DNS ポリシーを関連付け、ドメイン名をブロックリストまたはブロックしないリストに追加することもできます。

ブロックしないリストに含まれるオブジェクトの数とブロックリストに含まれるオブジェクトの数の合計が、125 個のネットワークオブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

始める前に

- ヒント：推奨される最小構成については、設定例：セキュリティインテリジェンスブロック （12 ページ）も参照してください。
- すべてのオプションを選択できるようにするには、少なくとも 1 つの管理対象デバイスを Management Center に追加します。
- パッシブ展開の場合、またはモニター専用にセキュリティ インテリジェンス フィルタリングを設定する場合は、ロギングを有効にします。『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Logging Connections with Security Intelligence」を参照してください。
- ドメインのセキュリティ インテリジェンス アクションを実行する DNS ポリシーを設定します。詳細については、「DNS ポリシー」を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 次の選択肢があります。

- [ネットワーク（Networks）] をクリックして、ネットワークオブジェクト（IP アドレス）を追加します。

  （注） セキュリティ インテリジェンス ポリシーで使用されるネットワークオブジェクトには、IPS ライセンスが必要です。

- [URL（URLs）] をクリックして、URL オブジェクトを追加します。

ステップ 3 ブロックしないリストまたはブロックリストに追加する [Available Objects] を検索します。次の選択肢があります。

- [名前または値で検索（Search by name or value）] フィールドに入力して、利用可能なオブジェクトを検索します。**[Reload]**（）または[クリア（Clear）]（  ）をクリックして、検索文字列をクリアします。

- 既存のリストまたはフィードがニーズを満たしていない場合は、**Add**（  ）をクリックし、[新規ネットワークリスト（New Network List）] または [新規 URL リスト（New URL List）] を選択し、セキュリティ インテリジェンス フィードの作成または新しいセキュリティ インテリジェンス リストの Secure Firewall Management Center へのアップロードの説明に従って続行します。

- 既存のオブジェクトがニーズを満たしていない場合は、**Add**（）をクリックし、[新規ネットワークオブジェクト（New Network Object）] または [新規 URL オブジェクト（New URL Object）] を選択し、ネットワーク オブジェクトの作成の説明に従って続行します。

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。

ステップ 4 追加する 1 つ以上の**利用可能なオブジェクト**を選択します。

ステップ 5 （オプション）[利用可能なゾーン（Available Zone）] を選択して、選択したオブジェクトをゾーンごとに制約します。

システムが提供するセキュリティ インテリジェンス リストをゾーンで制約することはできません。

（注） SI リストの [すべて（Any）] ゾーンは、セキュリティゾーンの一部であるインターフェイスにのみ適用されます。ただし、例外として、セキュリティゾーンに関連付けられたインターフェイスがデバイスにない場合、[すべて（Any）] ゾーンはどのインターフェイスにも一致します。

たとえば、デバイスに 5 つのインターフェイスがあり、それらのどれもセキュリティゾーンに関連付けられていない場合、[すべて（Any）] ゾーンに割り当てられた SI リストは、デバイスのすべてのインターフェイスのトラフィックに対して検査されます。そのデバイスのセキュリティゾーンに 1 つのインターフェイスを追加すると、ゾーンが SI リストに対して [すべて（Any）] に設定されている他の 4 つのインターフェイスの SI 検査が効果的に削除されます。他の 4 つのインターフェイスをセキュリティゾーンに追加すると、それらは [すべて（Any）] ゾーンにアタッチされている SI リストによって評価されます。

ステップ 6 [Add to Do Not Block list] または [Add to Block list] をクリックするか、選択したオブジェクトをクリックしていずれかのリストにドラッグします。

ブロックしないリストまたはブロックリストからオブジェクトを削除するには、[削除（Delete）]（） をクリックします。複数のオブジェクトを削除するには、オブジェクトを選択し、右クリックして [Delete Selected] を選択します。

ステップ 7 （オプション）ブロックリストのオブジェクトをモニター専用に設定するには、[ブロックリスト（Block List）] にリストされている該当するオブジェクトを右クリックし、[モニター専用（ブロックしない）（Monitor-only (do not block)）] を選択します。

システムが提供するグローバル セキュリティ インテリジェンス リストをモニター専用に設定することはできません。

ステップ 8 [DNS ポリシー（DNS Policy）] ドロップダウン リストから DNS ポリシーを選択します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

関連トピック

セキュリティ インテリジェンス
Snort 再起動のシナリオ

セキュリティ インテリジェンス オプション

アクセス制御ポリシーエディタの [セキュリティ インテリジェンス（Security Intelligence）] タブを使用して、ネットワーク（IP アドレス）と URL セキュリティ インテリジェンスを構成し、ドメインにセキュリティ インテリジェンスを設定した DNS ポリシーにアクセス制御ポリシーを関連付けます。

使用可能なオブジェクト

使用可能なオブジェクトは次のとおりです。

- システム提供のフィードによって入力されたセキュリティインテリジェンスのカテゴリ。

  詳細については、セキュリティ インテリジェンス カテゴリ （9 ページ）を参照してください。

- システム提供のグローバルのブロックリストとブロックしないリスト。

  説明については、セキュリティ インテリジェンス送信元 （4 ページ）を参照してください。

- [オブジェクト（Object）] > [オブジェクト管理（Object Management）] > [セキュリティインテリジェンス（Security Intelligence）] で作成するセキュリティインテリジェンスのリストとフィード。

  説明については、セキュリティ インテリジェンス送信元 （4 ページ）を参照してください。

- [オブジェクト（Object）] > [オブジェクト管理（Object Management）] の各ページで設定されている、ネットワークと URL のオブジェクトとグループ。これらは、前の箇条書きのセキュリティ インテリジェンス オブジェクトとは異なります。

  ネットワークオブジェクトの詳細については、ネットワークを参照してください。（URL には、オブジェクトやグループではなく、セキュリティインテリジェンスのリストまたはフィードを使用します。）

使用可能なゾーン

システムが提供するグローバルリストを除いて、ゾーンごとにセキュリティインテリジェンスフィルタリングを制約できます。

例：パフォーマンスを向上させるために、ターゲットの適用が必要になる場合があります。より具体的な例として、電子メールトラフィックを処理するセキュリティゾーンでのみ、スパムをブロックできます。

複数のゾーンでオブジェクトのセキュリティ インテリジェンス フィルタリングを適用するには、ゾーンのそれぞれについて、オブジェクトをブロックリストまたはブロックしないリストに追加する必要があります。

DNS ポリシー

セキュリティ インテリジェンスを使用して DNS トラフィックを照合するには、セキュリティインテリジェンス設定の DNS ポリシーを選択する必要があります。

ブロックリストまたはブロックしないリストの使用、または DNS リストまたはフィードに基づくトラフィックのモニタリングには、以下の条件もあります。

- DNS セキュリティ インテリジェンスのリストとフィードを設定します。セキュリティ インテリジェンスを参照してください。

- DNS ポリシーを作成します。詳細については、基本的な DNS ポリシーの作成を参照してください。
- DNS リストまたはフィードを参照する DNS ルールを設定します。詳細については、DNS ルールの作成と編集を参照してください。
- DNS ポリシーはアクセス コントロール ポリシーの一部として展開するため、両方のポリシーを関連付ける必要があります。詳細については、DNS ポリシーの導入を参照してください。

ブロックしないリスト

セキュリティ インテリジェンス ブロッキングのオーバーライド（14 ページ）を参照してください。

リスト内のすべてのオブジェクトを選択するには、オブジェクトを右クリックします。

ブロックリスト

設定例：セキュリティインテリジェンスブロック （12 ページ）およびこの章の他のトピックを参照してください。

ブロックリストのビジュアルインジケータの説明については、ブロックリストのアイコン（11 ページ）を参照してください。

リスト内のすべてのオブジェクトを選択するには、オブジェクトを右クリックします。

ログ

デフォルトで有効になっているセキュリティ インテリジェンス ロギングは、アクセス制御ポリシー対象のデバイスが処理するブロックされ、監視対象である接続はすべてロギングされます。ただし、システムはブロックしないリストの一致はロギングしません。ブロックしないリストの接続のロギングは、その接続の最終的な傾向によって異なります。ブロックリストの接続については、ブロックリストのオブジェクトをモニターのみに設定する前にロギングを有効にする必要があります。

ロギング設定を有効化、無効化、または表示するには、ブロックリストでオブジェクトを右クリックします。

関連トピック

グローバルおよびドメインのセキュリティインテリジェンスリスト
セキュリティ インテリジェンス リストとマルチテナンシー

セキュリティ インテリジェンス カテゴリ

セキュリティ インテリジェンスのカテゴリは、セキュリティ インテリジェンスで説明されているシステム提供のフィードによって決定されます。

これらのカテゴリは、次の場所で使用されます。

- アクセス コントロール ポリシーの [Security Intelligence] タブの [Networks] サブタブ
- アクセス コントロール ポリシーの [Security Intelligence] タブの [Networks] タブの横にある [URLs] サブタブ
- [DNS rule configuration] ページの [DNS] タブの DNS ポリシー
- トラフィックが上記の場所のブロック設定またはモニター設定と一致する場合に生成されるイベント

（注） 組織で Secure Firewall Threat Intelligence Directorを使用している場合：イベントを表示すると、アクションが TID によって実行されたことを示すカテゴリ（`TID URL ブロック`など）が表示されることがあります。

カテゴリはクラウドから Talos によって更新されます。このリストは、Firepower リリースとは無関係に変更される場合があります。

表 *1 : Cisco Talos Intelligence Group*（*Talos*） フィードカテゴリ

セキュリティインテリジェンス カテゴリ	説明
Attackers	悪意のある発信アクティビティが知られているアクティブスキャナやホスト
Banking_fraud	電子バンキングに関連する詐欺行為を行うサイト
Bogon	Bogon ネットワークおよび割り当てられていない IP アドレス
Bots	バイナリ マルウェア ドロッパを有するサイト
CnC	botnets 用のホスト C & C サーバーを有するサイト
Cryptomining	プールと財布へのリモートアクセスを提供するホスト (cryptocurrency のマイニングのため)
Dga	C & C サーバのランデブー ポイントとして機能するさまざまなドメイン名を生成するために使用されるマルウェア アルゴリズム
Exploitkit	クライアントのソフトウェアの脆弱性を特定するために設計されたソフトウェア キット
High_risk	セキュリティグラフからの OpenDNS 予測セキュリティアルゴリズムと一致するドメインとホスト名
Ioc	侵害の兆候（IOC）に関与していることが観察されているホスト
Link_sharing	権限のないファイルを共有する web サイト

セキュリティインテリジェンス カテゴリ	説明
Malicious	他のより詳細な脅威カテゴリに必ずしも適合しているわけではない、悪意のある動作を示しているサイト
マルウェア	マルウェアバイナリまたはエクスプロイト キットを有するサイト
Newly_seen	最近登録されたドメイン、またはテレメトリでまだ認識されていないドメイン **注目** 現在、このカテゴリにはアクティブなフィードがなく、将来の使用のために予約されています。
Open_proxy	匿名の web ブラウジングが可能な公開プロキシ
Open_relay	スパム用に使用されることが既知のオープン メール リレー
Phishing	フィッシング ページを有するサイト
応答	悪意があるか疑わしいアクティブに積極的に参加している IP アドレスと URL
Spam	スパムを送信することが知られているメール ホスト
Spyware	スパイウェアおよびアドウェアのアクティビティを含む、提供する、またはサポートすることが知られているサイト
Suspicious	疑いがあり、既知のマルウェアと同様の特性を持つようなファイル
Tor_exit_node	Torアノニマイザー ネットワークの出口ノードサービスを提供することが知られているホスト

ブロックリストのアイコン

アクセス コントロール ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブの [ブロックリスト（Block list）] に、次のビジュアルインジケータが表示される場合があります。

アイコンまたはビジュアルインジケータ	説明
Block ( )	オブジェクトはブロックするように設定されています。
	オブジェクトは監視専用に設定されています。 セキュリティ インテリジェンス モニタリング（13 ページ）を参照してください

アイコンまたはビジュアルインジケータ	説明
オブジェクトが取り消し線付きのテキストで表示される	同じオブジェクトがブロックをオーバーライドする [ブロックしない（Do Not Block）] リストにもあります。

設定例：セキュリティインテリジェンスブロック

システムにより定期的に更新されるセキュリティ インテリジェンス フィードによって検出可能なすべての脅威をブロックするようにアクセス コントロール ポリシーを設定します。

ブロックしないリストに含まれるオブジェクトの数とブロックリストに含まれるオブジェクトの数の合計が、125 個のネットワークオブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

始める前に

- すべてのオプションを選択できるようにするには、少なくとも 1 つの管理対象デバイスを Management Center に追加します。
- ドメインのセキュリティ インテリジェンスの脅威カテゴリをすべてブロックするように DNS ポリシーを設定します。詳細については、DNS ポリシーを参照してください。
- ブロックするエンティティのカスタムリストがある場合、または設定する予定がある場合は、各タイプ（URL、DNS、ネットワーク）のセキュリティ インテリジェンス オブジェクトを作成します。「セキュリティ インテリジェンス」を参照してください。

手順

ステップ 1 [ポリシー（Policies）] > [アクセスコントロール（Access Control）] をクリックします。

ステップ 2 新しいアクセス コントロール ポリシーを作成するか、既存のポリシーを編集します。

ステップ 3 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 4 [Networks] をクリックして、IP アドレスのブロック条件を追加します。

a) [Networks] リストを下にスクロールし、[Global] リストの下にリストされているすべての脅威カテゴリを選択します。
b) これらの脅威をブロックするセキュリティゾーンを選択します（該当する場合）。
c) [Add to Block List] をクリックします。
d) ブロックするアドレスを含むカスタムリストまたはフィードを作成している場合は、上記と同じ手順を使用してブロックリストに追加します。

ステップ 5 [URL] をクリックして URL のブロック条件を追加し、[Networks] で実行した手順を繰り返します。

ステップ 6 [DNS ポリシー（DNS Policy）] ドロップダウン リストから DNS ポリシーを選択します。DNS ポリシーの概要 を参照してください。

ステップ 7 [保存（**Save**）] をクリックします。

次のタスク

- これらの接続のロギングを有効にします。『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Logging Connections with Security Intelligence」を参照してください。
- 設定変更を展開します設定変更の展開を参照してください。
- 保護を強化するには、悪意のある URL をブロックするように URL フィルタリングを設定します。URL フィルタリング を参照してください。

セキュリティ インテリジェンス モニタリング

モニタリングでは、セキュリティインテリジェンスによってブロックされるはずのトラフィックの接続イベントをログに記録しますが、トラフィックをブロックすることはありません。モニタリングは、特に次の場合に役立ちます。

- 実装する前のフィードテスト。

  たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニター専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

- パフォーマンスを最適化するためのパッシブ展開。

  パッシブに展開された管理対象デバイスはトラフィック フローに影響を与えることができないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

（注） 構成されている場合、Secure Firewall Threat Intelligence Director は実行されるアクション（モニターまたはブロック）に影響を与える可能性があります。詳細については、Threat Intelligence Director-Management Center のアクションの優先順位付けを参照してください。

セキュリティ インテリジェンス モニタリングを設定するには：

設定例：セキュリティインテリジェンスブロック （12 ページ）の手順に従ってセキュリティインテリジェンス ブロックを設定したら、ブロックリストで該当する各オブジェクトを右クリックし、[モニターのみ（Monitor-only）] を選択します。システムが提供するセキュリティインテリジェンス リストをモニター専用に設定することはできません。

セキュリティ インテリジェンス ブロッキングのオーバーライド

必要に応じて、ブロックしないリストを使用して、特定のドメイン、URL、または IP アドレスが、セキュリティ インテリジェンスのリストまたはフィードによってブロックされないようにすることができます。

たとえば、以下を行うことができます。

- 信頼できるセキュリティ インテリジェンス フィードで時折発生する誤検出ブロックをオーバーライドする
- レピュテーションに基づいて早期にブロックするのではなく、特定のトラフィックを詳細に検査する
- セキュリティ インテリジェンス ブロッキングからのゾーンに基づいて、該当しなければ制限されたトランザクションを免除する

  たとえば、不適切に分類された URL をブロックしないリストに追加した後、組織内でそれらの URL にアクセスする必要があるユーザーが使用しているセキュリティゾーンによりブロックしないリストのオブジェクトを制限するという方法が考えられます。この方法では、ビジネスニーズを持つユーザーだけが、ブロックしないリスト上の URL にアクセスできます。

（注） Do Not Block リストのエントリは、ブロックリストから除外されるだけです。セキュリティ インテリジェンス ポリシーを通過する接続には、アクセスコントロールルールが適用されます。したがって、Do Not Block リストのエントリは、その後、アクセスコントロールルールまたは侵入ポリシーによってブロックされる可能性があります。Do Not Block エントリは、常にブロックリストから除外する必要があります。

手順

ステップ 1 オプション 1：イベントの IP アドレス、URL、またはドメインを、グローバルのブロックしないリストに追加します。グローバルおよびドメインのセキュリティインテリジェンスリストを参照してください。

ステップ 2 オプション2：カスタムのセキュリティ インテリジェンスのリストまたはフィードを使用します。

a) カスタムのセキュリティ インテリジェンスのリストまたはフィードを作成します。カスタム セキュリティ インテリジェンス リストまたはセキュリティ インテリジェンス フィードの作成を参照してください。

b) IP アドレス（ネットワーク）と URL の場合：アクセス コントロール ポリシーを編集し、[セキュリティインテリジェンス（Security Intelligence）] タブをクリックしてから、[ネットワーク（Networks）] または [URL（URLs）] サブタブでカスタムのリストまたはフィードをクリックし、[ブロックしないリストに追加（Add to Do Not Block List）] をクリックします。

c) 変更を保存します。

d) ドメイン（DNS）の場合：セキュリティ インテリジェンス オプション （7 ページ）トピックの「DNS ポリシー」セクションを参照してください。

e) 変更を展開します。

セキュリティ インテリジェンスのトラブルシューティング

セキュリティインテリジェンスのトラブルシューティングについては、次の項を参照してください。

セキュリティインテリジェンスのカテゴリが使用可能なオプションのリストに表示されない

症状：アクセスコントロールポリシーの[セキュリティインテリジェンス（Security Intelligence）] タブで、[利用可能なオプション（Available Options）] の下にある [ネットワーク（Networks）] タブにセキュリティ インテリジェンス カテゴリ（CnC や Exploitkit など）が表示されない。

原因：

- Management Center に少なくとも 1 つの管理対象デバイスが追加されるまで、これらのカテゴリは表示されません。すべての TALOS フィードを取得するには、デバイスを追加する必要があります。
- URL フィルタリング機能は、セキュリティ インテリジェンス機能とは異なる一連のカテゴリを使用します。表示されると予想されるカテゴリは、URL フィルタリングカテゴリである可能性があります。URL フィルタリングカテゴリを表示するには、アクセスコントロールルールの [URL] タブを調べます。

セキュリティ インテリジェンス ブロック リストへの登録の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
新しいセキュリティインテリジェンスカテゴリ	すべて	任意（Any）	Talos では、次の新しいセキュリティ インテリジェンス カテゴリを追加しました。 • banking_fraud • ioc • high_risk • link_sharing • malicious • newly_seen • spyware 新しいカテゴリに対応するようにアクセス制御と DNS ポリシーを更新し、定期的に将来の変更を確認する必要があります。 新規/変更されたページ：[セキュリティインテリジェンス（Security Intelligence）] タブの [ネットワーク（Network）] および [URL（URLs）] サブタブ、[DNSポリシー（DNS policies）] の [DNSルール（DNS rules）] サポートされているプラットフォーム： Management Center

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。