セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録

悪意のあるインターネット コンテンツに対する第一の防衛ラインとして、FireSIGHT システムにはセキュリティ インテリジェンス機能があります。これを使用すると、接続を最新のレピュテーション インテリジェンスに基づいて即座にブラックリスト登録(ブロック)することができるため、リソースを集中的に消費する詳細な分析が不要になります。セキュリティ インテリジェンスのフィルタリングには、Protectionライセンスが必要で、シリーズ 2 を除くすべての管理対象デバイスでサポートされます。

セキュリティ インテリジェンスは、既知の好ましくないレピュテーションが含まれる IP アドレスを送信元/宛先とするトラフィックをブロックすることにより機能します。このトラフィック フィルタリングは、他のどのポリシー ベースのインスペクション、分析、またはトラフィック処理よりも**先**に行われます(ただし高速パスなどのハードウェア レベルの処理の後に発生します)。

IP アドレスでトラフィックを手動で制限することで、セキュリティ インテリジェンス フィルタリングと同様の機能を実行するアクセス コントロール ルールを作成することができます。ただし、アクセス コントロール ルールは対象範囲が広く、設定の難易度が高いだけでなく、動的フィードを使用した自動更新に対応できません。

セキュリティ インテリジェンスによってブラックリスト登録されたトラフィックは即座にブロックされるため、他のさらなるインスペクションの対象にはなりません(侵入、エクスプロイト、マルウェアなどの有無だけでなくネットワーク検出についても)。オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されたであろう接続をシステムが分析できるだけでなく、ブラックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

注意 シリーズ 3 デバイスによって処理されるトラフィックの場合は、システムはアクセス 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 ブラックリストの前に特定の信頼ルールを処理します。これによって、ブラックリスト登録されたトラフィックは検査されないまま通過することができます。詳細については、シリーズ 3 デバイスを使用したトラフィックの信頼またはブロックへの制限事項(14-13 ページ)を参照してください。

便宜上、シスコは*インテリジェンス フィード*(時に *Sourcefire インテリジェンス フィード*とも呼ばれます)を提供します。これは、VRT によってレピュテーションに欠けると判断された IP アドレスのコレクションからなり、これらのコレクションは定期的に更新されます。インテリジェンス フィードは、オープン リレー、既知の攻撃者、偽の IP アドレス(bogon)などを追跡します。この機能を組織の固有のニーズに適するようにカスタマイズできます。例を次に示します。

- **サードパーティ フィード**:インテリジェンス フィードをサードパーティのレピュテーション フィードで補足できます。そのフィードはシステムが シスコ フィードと同様に自動的に更新できます。
- **カスタム ブラックリスト**:システムは、ユーザが自身のニーズに応じてさまざまな方法で特定の IP アドレスを手動でブラックリスト登録することを許可します。
- **セキュリティ ゾーンによるブラックリスト登録の強制**:パフォーマンスを向上させるには、スパムのブラックリスト登録を電子メール トラフィックを処理するゾーンに制限するなどして、強制を適用することができます。
- **ブラックリスト登録の代わりにモニタリング**:特にパッシブ展開で、展開を実装する前のフィードのテストに有用です。違反しているセッションをブロックする代わりに単にモニタして、接続終了イベントを生成できます。
- **誤検出をなくすためのホワイトリスト登録**:ブラックリストの範囲が広すぎる場合、または(たとえば、重要なリソースに)許可するトラフィックを誤ってブロックした場合、ブラックリストをカスタム ホワイトリストで上書きできます。

セキュリティ インテリジェンス フィルタリングを実行するためにアクセス コントロール ポリシーを設定する方法、およびこのフィルタリングが生成するイベント データを表示する方法については、次の項を参照してください。

- セキュリティ インテリジェンス戦略の選択(13-2 ページ)
- セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成(13-4 ページ)
- セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング(38-13 ページ)
- 接続およびセキュリティ インテリジェンスのデータの使用(39-1 ページ)

セキュリティ インテリジェンス戦略の選択

ライセンス: Protection

サポートされるデバイス:すべて(シリーズ 2 を除く)

サポートされる防御センター:DC500 を除くいずれか

ブラックリストを作成する最も簡単な方法は、オープン リレーとなることが分かっている IP アドレス、既知の攻撃者、不正な IP アドレス(bogon)などを追跡する、インテリジェンス フィードを使用することです。インテリジェンス フィードは定期的に更新されるため、インテリジェンス フィードを使用することで、システムがネットワーク トラフィックのフィルタリングに最新の情報を使用することが保証されます。ただし、セキュリティに対する脅威(マルウェア、スパム、ボットネット、フィッシングなど)を表す不正な IP アドレスが現れては消えるペースが速すぎて、新しいポリシーを更新して適用するには間に合わないこともあります。

したがって、インテリジェンス フィードを補完するために、次の場合にサードパーティの IP アドレスのリストとフィードを使用してセキュリティ インテリジェンス フィルタリングを実行できるようになっています。

- *リスト*とは、ユーザが Defense Center にアップロードする IP アドレスの静的リストのことです。
- *フィード*とは、Defense Center が定期的にインターネットからダウンロードする、IP アドレスの動的リストのことです。インテリジェンス フィードは、特殊なタイプのフィードです。

高可用性およびインターネット アクセス要件を含め、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する方法の詳細については、セキュリティ インテリジェンス リストとフィードの操作（3-5 ページ）を参照してください。

セキュリティ インテリジェンスのグローバル ブラックリストの使用

分析の過程で、イベント ビュー、Context Explorer、またはダッシュボードで任意の IP アドレスを選択して*グローバル ブラックリスト*を作成することができます。たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な IP アドレスのセットに気付いた場合、それらの IP アドレスを即時にブラックリストに入れることができます。Defense Center ではすべてのアクセス コントロール ポリシーで、このグローバル ブラックリスト（および関連する*グローバル ホワイトリスト*）を使用してセキュリティ インテリジェンス フィルタリングを行います。これらのグローバル リストを管理する方法の詳細については、グローバル ホワイトリストおよびブラックリストの操作（3-7 ページ）を参照してください。

（注）　グローバル ブラックリスト（またはグローバル ホワイトリスト。以下を参照）のフィードの更新および追加では、展開環境全体にわたって自動的にその変更が実装されますが、セキュリティ インテリジェンス オブジェクトに対するその他の変更には、アクセス コントロール ポリシーの再適用が必要になります。詳細については、表 3-1（3-7 ページ）を参照してください。

ネットワーク オブジェクトの使用

さらに、ブラックリストを作成するもう 1 つの簡単な方法として、IP アドレス、IP アドレス ブロック、あるいは IP アドレスのコレクションを表す*ネットワーク オブジェクト*または*ネットワーク オブジェクト グループ*を使用することもできます。ネットワーク オブジェクトの作成および変更の詳細については、ネットワーク オブジェクトの操作（3-4 ページ）を参照してください。

セキュリティ インテリジェンスのホワイトリストの使用

ブラックリストに加え、各アクセス コントロール ポリシーにはホワイトリストが関連付けられます。ホワイトリストにも、セキュリティ インテリジェンス オブジェクトを取り込むことができます。ポリシーでは、ホワイトリストがブラックリストをオーバーライドします。つまり、システムは、送信元または宛先の IP アドレスがホワイトリストに登録されているトラフィックは、たとえそれらの IP アドレスがブラックリストにも登録されているとしても、そのトラフィックをアクセス コントロール ルールを使用して評価します。通常、ブラックリストがまだ有用であっても、その適用範囲があまりにも広く、インスペクション対象のトラフィックを誤ってブロックする場合には、ホワイトリストを使用してください。

たとえば、信頼できるフィードにより、重要なリソースへのアクセスが不適切にブロックされたが、そのフィードが全体としては組織にとって有用である場合は、そのフィード全体をブラックリストから削除するのではなく、不適切に分類された IP アドレスだけをホワイトリストに登録するという方法を取ることができます。

セキュリティ ゾーンを基準としたセキュリティ インテリジェンス フィルタリングの適用

さらに細かく制御するには、接続の送信元または宛先 IP アドレスが特定のセキュリティ ゾーン内にあるかどうかに基づいて、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ことができます。

上述のホワイトリストの例を拡張するとしたら、不適切に分類された IP アドレスをホワイトリストに登録した後、組織でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティ ゾーンを使用して、ホワイト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だけが、ホワイトリストに登録された IP アドレスにアクセスできます。別の例として、サードパーティのスパム フィードを使用して、電子メール サーバのセキュリティ ゾーンのトラフィックをブラックリスト登録することができます。

接続のモニタリング（ブラックリスト登録ではなく）

特定の IP アドレスまたはアドレス一式をブラックリスト登録する必要があるかどうかわからない場合は、「モニタ専用」設定を使用できます。この設定では、システムが一致する接続をアクセス コントロール ルールに渡せるだけでなく、ブラックリストと一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。注意する点として、グローバル ブラックリストをモニタ専用に設定することはできません。詳細については、次を参照してください。

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。

パッシブ展開環境では、パフォーマンスを最適化するために、シスコでは常にモニタ専用の設定を使用することを推奨しています。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。

セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成

ライセンス：Protection

サポートされるデバイス：すべて（シリーズ 2 を除く）

サポートされる防御センター：DC500 を除くいずれか

ホワイトリストとブラックリストを作成するには、ネットワーク オブジェクトとグループの任意の組み合わせに加え、セキュリティ ゾーン別に制約することができる、セキュリティ インテリジェンスのフィードとリストを入力します。

注意　右クリック メニューで [今すぐホワイトリスト（Whitelist Now）] または [今すぐブラックリスト（Blacklist Now）] オプションを選択した場合を除き、セキュリティ インテリジェンス リストを変更すると、Snort プロセスが再開され、構成変更を適用する際、一時的にトラフィック インスペクション（検査）が中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

デフォルトでは、アクセス コントロール ポリシーは、どのゾーンにも適用される Defense Center のグローバル ホワイトリストおよびブラックリストを使用します。これらのリストはアナリストによって入力されます。アナリストは、コンテキスト メニューを使用して、簡単に個々の IP アドレスを追加できます。ポリシーのそれぞれについて、これらのグローバル リストを使用しないように選択することができます。

(注)　入力したグローバル ホワイトリストまたはブラックリストを使用するアクセス コントロール ポリシーを シリーズ 2 デバイス（または Protection のライセンスがない他のデバイス）に適用することはできません。いずれかのグローバル リストに IP アドレスを追加した場合は、ポリシーのセキュリティ インテリジェンス設定から空でないリストを削除**してからでないと**、ポリシーを適用できません。詳細については、グローバル ホワイトリストおよびブラックリストの操作 (3-7 ページ) を参照してください。

ホワイトリストとブラックリストを作成した後は、ブラックリスト登録された接続のロギングが可能になります。フィードとリストを含め、ブラックリスト登録された個々のオブジェクトをモニタ専用に設定することもできます。この設定では、システムがブラックリスト登録された IP アドレスを使用する接続をアクセス コントロールによって処理できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。

ホワイトリスト、ブラックリスト、およびロギング オプションを設定するには、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）] タブを使用します。このページには、ホワイトリストまたはブラックリストのいずれかで使用できるオブジェクトのリスト（[使用可能なオブジェクト（Available Objects）]）と、ホワイトリスト登録およびブラックリスト登録されたオブジェクトを制約するために使用できるゾーンのリスト（[利用可能なゾーン（Available Zones）]）が表示されます。オブジェクトまたはゾーンのタイプは、異なるアイコンによって見分けられるようになっています。シスコ アイコン（  ）でマークされたオブジェクトは、インテリジェンス フィードの各種カテゴリを表します。

セキュリティ インテリジェンスのカテゴリ	カテゴリ定義
攻撃者	悪意のあるアウトバウンド アクティビティが認識されているアクティブなスキャナおよびブラックリスト ホスト
Malware	マルウェアのバイナリをホストまたはキットをエクスプロイトするサイト
フィッシング	フィッシング ページをホストするサイト
スパム	スパム送信が認識されているメール ホスト
BOT	バイナリ マルウェア ドロッパをホストするサイト
CnC	ボットネットのコマンド サーバと制御サーバをホストするサイト
OpenProxy	匿名 Web ブラウジングを許可するオープン プロキシ
OpenRelay	スパムに使用されることが認識されているオープン メール リレー
TorExitNode	Tor 終了ノード
Bogon	Bogon ネットワークおよび未割り当ての IP アドレス

ブラックリストでは、ブロックするように設定されたオブジェクトはブロック アイコン( )でマークされ、モニタ専用オブジェクトはモニタ アイコン( )でマークされます。ホワイトリストがブラックリストをオーバーライドするため、両方のリストに同じオブジェクトを追加すると、ブラックリスト登録されたオブジェクトに取り消し線が表示されます。

ホワイトリストとブラックリストには、最大 255 個のオブジェクトを追加できます。つまり、ホワイトリストのオブジェクトとブラックリストのオブジェクトを合計した数は 255 以下でなければなりません。

ネットマスク /0 のネットワーク オブジェクトはホワイトリストまたはブラックリストに追加できますが、ネットマスク /0 を使用したアドレス ブロックは無視され、これらのアドレスに基づいたホワイトリストおよびブラックリスト フィルタリングは行われないことに注意してください。セキュリティ インテリジェンス フィードからのネットマスク /0 のアドレス ブロックも無視されます。すべてのトラフィックをモニタまたはブロックする場合は、セキュリティ インテリジェンス フィルタリングの代わりに、[モニタ(Monitor)] または [ブロック(Block)] ルール アクションでアクセス コントロール ルールを使用し、[送信元ネットワーク(Source Networks)] および [宛先ネットワーク(Destination Networks)] のデフォルト値 **any** をそれぞれ使用します。

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 ホワイトリストおよびブラックリストを作成する方法:

アクセス: Admin/Access Admin/Network Admin

手順 1　[ポリシー(Policies)] > [アクセス制御(Access Control)] を選択します。

[アクセス コントロール ポリシー(Access Control Policy)] ページが表示されます。

手順 2　設定するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[セキュリティ インテリジェンス(Security Intelligence)] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

手順 4　オプションで、ブラックリスト登録された接続をログに記録するには、ロギング アイコン( )をクリックします。

ロギングを有効にしてからでないと、ブラックリスト登録されたオブジェクトをモニタ専用に設定することはできません。詳細は、セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング(38-13 ページ)を参照してください。

手順 5　1 つ以上の**使用可能なオブジェクト**を選択して、ホワイトリストおよびブラックリストの作成を開始します。

複数のオブジェクトを選択するには、Shift キーまたは Ctrl キーを使用するか、右クリックして [すべて選択(Select All)] を選択します。

ヒント　リストに含める既存のオブジェクトを検索できます。組織のニーズを満たす既存のオブジェクトがない場合は、その場でオブジェクトを作成することもできます。詳細については、ホワイトリストまたはブラックリストに追加するオブジェクトの検索(13-7 ページ)およびホワイトリストまたブラックリストに追加するオブジェクトの作成(13-8 ページ)を参照してください。

手順 6　オプションで、**利用可能なゾーン**を選択して、選択したオブジェクトをゾーンを基準に制約します。

デフォルトでは、オブジェクトは制約されません。つまり、オブジェクトのゾーンは [任意（Any）] に設定されます。[任意（Any）] を使用しない場合、制約の基準にできるゾーンは 1 つだけです。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、オブジェクトをホワイトリストまたはブラックリストに追加する必要があります。また、グローバル ホワイトリストまたはブラックリストをゾーンによって制約することはできません。

手順 7　[ホワイトリストに追加（Add to Whitelist）] または [ブラックリストに追加（Add to Blacklist）] をクリックします。

また、オブジェクトをクリックして選択し、いずれかのリストにドラッグすることもできます。

選択したオブジェクトは、ホワイトリストまたはブラックリストに追加されます。

ヒント　オブジェクトをリストから削除するには、そのオブジェクトの削除アイコン（ ）をクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択した後、右クリックして [選択対象を削除（Delete Selected）] を選択します。グローバル リストを削除する場合は、選択した操作を確認する必要があります。ホワイトリストまたはブラックリストからオブジェクトを削除しても、そのオブジェクトは、Defense Center からは削除されません。

手順 8　オブジェクトをホワイトリストまたはブラックリストに追加し終わるまで、ステップ 5 ～ 7 を繰り返します。

手順 9　オプションで、ブラックリスト登録されたオブジェクトをモニタ専用に設定するには、[ブラックリスト（Blacklist）] 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、[モニタ専用（ブロックしない（Monitor-only (do not block)] を選択します。

パッシブ展開環境の場合、シスコではすべてのブラックリスト登録されたオブジェクトをモニタ専用に設定することを推奨します。ただし、グローバル ブラックリストをモニタ専用に設定することはできません。

手順 10　[保存（Save）] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ） を参照してください。

ホワイトリストまたはブラックリストに追加するオブジェクトの検索

ライセンス：Protection

サポートされるデバイス：すべて（シリーズ 2 を除く）

サポートされる防御センター：DC500 を除くいずれか

複数のネットワーク オブジェクト、グループ、フィード、およびリストを使用する場合は、検索機能を使用して、ブラックリストまたはホワイトリストに追加するオブジェクトを絞り込むことができます。

ブラックリストまたはホワイトリストに追加するオブジェクトを検索する方法:

アクセス: Admin/Access Admin/Network Admin

手順 1　[名前または値で検索(Search by name or value)] フィールドにクエリを入力します。

検索文字列を入力すると、[使用可能なオブジェクト(Available Objects)] リストが更新されて、検索文字列と一致する項目が表示されます。検索文字列をクリアするには、検索フィールドの上のリロード アイコン( )をクリックするか、検索フィールド内のクリア アイコン( )をクリックします。

ネットワーク オブジェクトの名前、またはネットワーク オブジェクトに設定されている値を基準に検索できます。たとえば `Texas Office` という名前の個別ネットワーク オブジェクトがあり、`192.168.3.0/24` という値が設定されていて、`US Offices` というグループ オブジェクトに含まれる場合、`Tex` などの部分的または完全な検索文字列を入力するか、または `3` などの値を入力することにより、両方のオブジェクトを表示できます。

ホワイトリストまたブラックリストに追加するオブジェクトの作成

ライセンス: Protection

サポートされるデバイス:すべて(シリーズ 2 を除く)

サポートされる防御センター:DC500 を除くいずれか

アクセス コントロール ポリシーの編集中に、ホワイトリストやブラックリストで使用するオブジェクト(ネットワーク オブジェクトや、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)をその場で作成できます。ネットワーク オブジェクトをグループ化する場合、またはネットワーク オブジェクト グループを作成する場合は、オブジェクト マネージャを使用する必要があります。

ホワイトリストまたはブラックリストに追加するオブジェクトを作成する方法:

アクセス: Admin/Access Admin/Network Admin

手順 1　追加アイコン( )をクリックして、作成するオブジェクトのタイプを選択します。

- 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する場合は、[IP リストの追加(Add IP List)] を選択します。セキュリティ インテリジェンス リストとフィードの操作(3-5 ページ)を参照してください。
- ネットワーク オブジェクトを追加する場合は、[ネットワーク オブジェクトの追加(Add Network Object)] を選択します。ネットワーク オブジェクトの操作(3-4 ページ)を参照してください。