ネットワーク資産に応じた侵入防御の調整

以下のトピックでは、Cisco 推奨ルールの使用方法について説明します。

シスコ推奨ルールについて

侵入ルールの推奨事項を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアント アプリケーション プロトコルを、それらのアセットを保護するために作成されたルールに関連付けることができます。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

システムは、侵入ポリシーごとに個別の推奨事項のセットを作成します。これにより、通常、標準テキストルールと共有オブジェクトルールのルール状態の変更が推奨されます。ただし、プリプロセッサおよびデコーダのルールの変更も推奨されます。

ルール状態の推奨事項を生成する場合は、デフォルト設定を使用するか、詳細設定を指定できます。詳細設定では次の操作が可能です。

- システムが脆弱性をモニタするネットワーク上のホストを再定義する。
- ルール オーバーヘッドに基づき、システムが推奨するルールに影響を与える。
- ルールを無効にする推奨事項を生成するかどうかを指定する。

推奨事項をすぐに使用するか、推奨事項（および影響を受けるルール）を確認してから受け入れることができます。

推奨ルール状態を使用することを選択すると、読み取り専用のシスコ推奨レイヤが侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないことを選択すると、そのレイヤが削除されます。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。

システムは、手動で設定されたルール状態を変更しません。

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる。
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる。

ヒント 侵入ポリシー レポートには、推奨状態と異なるルール状態を持つルールのリストを含めることができます。

推奨が絞り込まれた [ルール（Rules）] ページを表示している最中に、あるいは、ナビゲーション パネルまたは [ポリシー情報（Policy Information）] ページから [ルール（Rules）] ページに直接アクセスした後に、手動で、ルール状態を設定したり、ルールをソートしたり、[ルール（Rules）] ページで可能なその他の操作（ルールの抑制やルールしきい値の設定など）を実行することができます。

（注） Talos インテリジェンスグループ は、システム提供のポリシーでの各ルールの適切な状態を決定します。システムによって提供されるポリシーをベースポリシーとして使用し、システムがルールをシスコの推奨ルール状態に設定できるようにすると、侵入ポリシーのルールは、シスコが推奨するネットワークアセットの設定と一致します。

Cisco 推奨のデフォルト設定

Cisco 推奨を生成すると、システムがネットワーク資産に関連付けられた脆弱性から保護するルールの基本ポリシーを検索して、その基本ポリシー内のルールの現在の状態を特定します。システムによってルールの状態が推奨されますが、自身で設定する場合はルールを推奨される状態に設定します。

システムによって次の基本的な分析が実行され、推奨が生成されます。

表 *1*: 脆弱性に基づく ルール状態推奨

検出された資産がルールにより保護されるか	基本ポリシー ルール状態	推奨ルール状態
はい	無効	イベントを生成する（Generate Events）
	イベントを生成する（Generate Events）	イベントを生成する（Generate Events）
	ドロップおよびイベントの生成	ドロップおよびイベントの生成（Drop and Generate Events）
いいえ	任意	無効

表の次の点に注意してください。

- ベース ポリシーでルールが無効になっているか、または[イベントの生成（Generate Events）] に設定されている場合、推奨される状態は常に[イベントの生成（Generate Events）] です。

  たとえば、ベース ポリシーが [アクティブなルールなし（No Rules Active）] の場合（すべてのルールが無効になっている）、[ドロップしてイベントを生成する（Drop and Generate Events）] は推奨されません。

- [ドロップしてイベントを生成する（Drop and Generate Events）] は、ベース ポリシーですでに[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されているルールにのみ推奨します。

  ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定して、そのルールを無効にするか、またはベース ポリシーで [イベントの生成（Generate Events）] に設定した場合は、ルールの状態を手動でリセットする必要があります。

Cisco 推奨ルールの詳細設定を変更せずに推奨を生成する場合は、システムが検出対象のネットワーク全体のすべてのホストのルール状態の変更を推奨します。

デフォルトで、システムは、オーバーヘッドが低または中のルールに対してのみ推奨を生成し、ルールを無効にする推奨を生成します。

システムは、Impact Qualification 機能を使用して無効にされた脆弱性に基づく侵入ルールのルール状態を推奨しません。

システムは、常に、ホストにマップされたサードパーティの脆弱性に関連付けられたローカル ルールを有効にするように推奨します。

マップされていないローカル ルールに対する状態推奨は生成されません。

関連トピック

サードパーティ製品のマッピング

Cisco 推奨事項の詳細設定

推奨とルール状態とのすべての差をポリシー レポートに含める（Include all differences between recommendations and rule states in policy reports）

デフォルトで、侵入ポリシー レポートには、ポリシーで有効になっているルール、つまり、[イベントを生成する（Generate Events）] と [ドロップしてイベントを生成する（Drop and Generate Events）] のいずれかに設定されているルールが表示されます。また、[すべての差を含める（Include all differences）] オプションを有効にすると、推奨されている状態が保存されている状態と異なるルールが一覧表示されます。ポリシー レポートの詳細については、設定の展開についてを参照してください。

検査対象のネットワーク（Networks to Examine）

モニタ対象のネットワークまたは推奨について検査する個々のホストを指定します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

指定したホスト内のアドレスのリストは、否定以外の OR 演算でリンクされ、すべての OR 演算の実行後に AND 演算でリンクされます。

ホスト情報に基づいて特定のパケットのアクティブ ルール処理を動的に適応させる場合は、adaptive profile updates を有効にすることもできます。

推奨しきい値（ルール オーバーヘッドの指定）（Recommendation Threshold (By Rule Overhead)）

選択したしきい値をオーバーヘッドが超える侵入ルールが推奨または自動的に有効にされないようにします。

オーバーヘッドは、システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率に基づいています。オーバーヘッドが高いルールを許可すると、通常、より多くの推奨が生成されるようになりますが、システム パフォーマンスに影響を及ぼす可能性があります。[侵入ルール（Intrusion Rules）] ページのルール詳細ビューでルールのオーバーヘッドの評価を確認できます。

ただし、ルールを無効にする推奨ではルール オーバーヘッドが考慮されません。また、ローカル ルールは、サードパーティの脆弱性にマップされていない限り、オーバーヘッドがないものと見なされます。

特定の設定のオーバーヘッド評価のルールについて推奨を生成した場合でも、別のオーバーヘッドの推奨を生成してから、再び元のオーバーヘッド設定の推奨を生成することができます。推奨を生成する回数や生成時に使用する異なるオーバーヘッド設定の数に関係なく、同じルールセットについては、推奨を生成するたびに、オーバーヘッド設定ごとに同じルール状態の推奨が生成されます。たとえば、オーバーヘッドを「中」に設定して推奨を生成し、次に「高」にして推奨を生成してから、再び「中」にして推奨を生成することができます。ネットワーク上のホストとアプリケーションが変更されていなければ、オーバーヘッドが「中」の推奨は、どちらも、そのルール セットに対して同じになります。

ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）

Cisco の推奨に基づいて侵入ルールを無効にするかどうかを指定します。

ルールを無効にする推奨を受け入れると、ルールの適用範囲が制限されます。ルールを無効にする推奨を無視すると、ルールの適用範囲が拡大されます。

関連トピック

アダプティブプロファイルの更新とシスコの推奨ルール

Cisco 推奨事項の生成と適用

Cisco の推奨事項の使用を開始または停止する場合、ネットワークのサイズと侵入ルールセットに応じて、数分かかる場合があります。

始める前に

- Cisco の推奨事項には、次の要件があります。
  - Threat Defense ライセンス：IPS
  - 従来のライセンス：保護
  - ユーザの役割 ～ 管理者 または 侵入管理者
- 手順を開始する前に、ネットワーク検出ポリシーを設定します。Cisco の推奨事項が適切になるように、ネットワーク検出ポリシーを設定して内部ホストを定義します。ネットワーク検出のカスタマイズを参照してください。

手順

ステップ 1 Snort 2 侵入ポリシーエディタのナビゲーションウィンドウで、[Cisco推奨事項（Cisco Recommendations）] をクリックします。

ステップ 2 （オプション）詳細設定を設定します。Cisco 推奨事項の詳細設定 （4 ページ）を参照してください。

ステップ 3 推奨事項を生成して適用します。

- **推奨事項の生成および使用（Generate and Use Recommendations）**：推奨事項を生成して、一致するようにルール状態を変更します。これまでに推奨事項を生成したことがない場合にのみ使用できます。
- **推奨事項の生成（Generate Recommendations）**：推奨事項を使用しているかどうかに関係なく、新しい推奨事項を生成しますが、一致するようにルールの状態を変更しません。
- **推奨事項の更新（Update Recommendations）**：推奨事項を使用している場合は、推奨事項を生成してルールの状態を一致するように変更します。それ以外の場合は、ルールの状態を変更することなく、新しい推奨事項を生成します。

- **推奨事項の使用（Use Recommendations）**：ルールの状態を未実装の推奨事項に一致するように変更します。
- **推奨事項を使用しない（Do Not Use Recommendations）**：推奨事項の使用を停止します。推奨事項の適用前にルールの状態を手動で変更した場合、ルールの状態は指定した値に戻ります。それ以外の場合、ルールの状態はデフォルト値に戻ります。

推奨事項の生成時に、システムは推奨される変更の概要を表示します。システムによって状態の変更が推奨されるルールのリストを表示するには、新しく提案されたルール状態の横にある[表示（View）] をクリックします。

ステップ 4 実装した推奨事項を評価して調整します。

ほとんどの Cisco の推奨事項を承認する場合でも、ルールの状態を手動で設定することで、推奨事項を個別に上書きできます。侵入ルール状態の設定を参照してください。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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。

スクリプト検出

スクリプト検出は、部分的な検査で Snort ブロックの手遅れになった侵入による障害を防ぎます。HTML ファイルがクライアントとサーバーの間で転送されるときに、これらのファイルに悪意のあるスクリプト（攻撃を開始するための JavaScript など）が含まれている可能性があります。このような悪意のあるスクリプトが検出された場合、部分的な検査により任意の IPS ルールを悪意のあるスクリプトと照合することができ、インスペクタが検査と検出を通じてそのデータセグメントをフラッシュします。悪意のあるファイルが宛先に到達することはありません。この機能は、HTTP/1 と HTTP/2 の両方のトラフィックをサポートしています。

この機能はデフォルトで常に有効になっています。オフにするには、**`http_inspect.script_detection=true`** を false に設定します。

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。