ネットワーク資産に応じた侵入防御の調整

「ネットワークアセットに対する侵入保護の調整」の章では、Firepowerが推奨するルールと、Firepower 推奨ルールの生成と適用についての洞察を提供します。

LSP 更新での Snort 3 ルールの変更

通常のSnort 3侵入ルール（LSP）の更新中に、既存のシステム定義の侵入ルールが新しい侵入ルールに置き換えられることがあります。1 つのルールが複数のルールに置き換えられたり、または複数のルールが1つのルールに置き換えられたりする可能性があります。これは、結合または拡張されたルールに対してより適切な検出が可能な場合に発生します。管理を向上させるために、既存のシステム定義ルールの一部をLSPアップデートの一部として削除することもできます。

LSP更新中にオーバーライドされたシステム定義ルールの変更に関する通知を受け取るには、[削除されたSnort 3ルールのユーザオーバーライドの保持（Retain user overrides for deleted Snort 3 rules）] チェックボックスがオンになっていることを確認します。システムのデフォルトでは、このチェックボックスはオンになっています。このチェックボックスをオンにすると、LSP更新の一部として追加される新しい置換ルールのルールオーバーライドが保持されます。通知は、[歯車（Cog）]（⚙）の横にある [通知（Notification）] アイコンの下にある [タスク（Task）] タブに表示されます。

[削除されたSnort 3ルールのユーザオーバーライドの保持（Retain user overrides for deleted Snort 3 rules）] チェックボックスに移動するには、**[歯車（Cog）]**（⚙）をクリックして、**[設定（Configuration）] > [侵入ポリシー設定（Intrusion Policy Preferences）]** を選択します。

Firepower 推奨ルールについて

Firepower 侵入ルールの推奨事項を使用して、ネットワークで検出されたホストアセットに関連付けられている脆弱性を対象にすることができます。たとえば、オペレーティングシステ

ム、サーバ、クライアント アプリケーション プロトコルなどです。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、インスペクタやデコーダのルールの変更も推奨されています。

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 Firepower 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） Cisco Talos Intelligence Group（Talos）は、システムによって提供される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 Firepower 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。

Snort 2 で生成された Firepower 推奨事項の Snort 3 への移行

Firepower 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。

Firepower の推奨事項は、Snort 3 バージョンでは直接生成できません。侵入ポリシーの Snort 2 バージョンの Firepower 推奨事項を生成し、ここに記載されている手順に従って、推奨されたルール設定を Snort 3 に移行します。

始める前に

Firepower の推奨事項には、次の要件があります。

- FTD ライセンス：Threat
- クラシックライセンス：保護
- ユーザロール：管理者または侵入管理者
- 推奨を生成するホストがシステムに存在することを確認します。

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 侵入ポリシーの [Snort 2 バージョン（Snort 2 Version）] ボタンをクリックします。

ステップ 3 侵入ポリシーの Snort 2 バージョンで推奨事項を生成して適用します。

最新バージョンの『*Firepower Management Center Configuration Guide*』の「*Generate and Applying Firepower Recommendations*」のトピックを参照し、そのトピックに記載されている手順を実行します。

ステップ 4 Snort 2 のルール変更を Snort 3 と同期します。

手順については、Snort 2 のルールと Snort 3 の同期を参照してください。

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。