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、Firepower 推奨ルールの使用方法について説明します。

Firepower 推奨ルールについて

Firepowerの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、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 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 Security Intelligence and Research Group（Talos）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。システム提供のポリシーを基本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場合、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。

推奨ルールおよびマルチテナンシー

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

Firepower 推奨のデフォルト設定

Firepower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 *Firepower* ルール状態推奨

基本ポリシー ルール状態	ルールは検出された資産を保護するか	推奨ルール状態
イベントの生成または無効化	Yes	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	Yes	ドロップおよびイベントの生成（Drop and Generate Events）
任意	No	無効（Disable）

Firepower 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

個々の脆弱性の非アクティブ化
サードパーティ製品のマッピング

Firepower 推奨の詳細設定

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、ポリシー レポート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、アダプティブ プロファイル 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）

Firepower 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

Firepower システムの IP アドレス表記法
アダプティブプロファイルおよび Firepower 推奨ルール

Firepower の推奨事項の生成と適用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

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。

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、先祖ドメインの侵入ポリシーでこの機能を有効にすると、システムはすべての子孫のリーフ ドメインからのデータを使用して、推奨事項を生成します。これにより、侵入ルールをすべてのリーフ ドメインに存在しない可能性があるアセットに調整することができ、パフォーマンスに影響を与えることができます。

手順

ステップ 1 侵入ポリシー エディタのナビゲーション ウィンドウで、[Firepower の推奨事項（Firepower 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。Firepower 推奨の詳細設定, （3 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 Firepower 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、個別の推奨事項を上書きできます。侵入ルール状態の設定を参照してください。

ステップ 5 最後のポリシーの確定以降に、このポリシーに加え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、別のポリシーを編集すると、最後に確定してから加えた変更は廃棄されます。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

関連トピック

Firepower の推奨ルールの自動化