Snort 3 侵入ポリシーでの MITRE フレームワークを使用した脅威の軽減

MITRE ATT&CK フレームワークについて

MITRE ATT&CK フレームワークは、攻撃者がシステムを侵害するために使用する戦術、手法、および手順（TTP）の概要を示す包括的なナレッジベースです。これらの TTP をさまざまなオペレーティングシステムとプラットフォームのマトリックスに編成し、各攻撃段階（戦術）を特定の方法（手法）にマッピングします。各手法には、実行、手順、防御、検出、および実際の例に関する情報が含まれています。

（注） MITRE ATT&CK に関するその他の情報については、https://attack.mitre.org [英語] を参照してください。

Management Center では、MITRE ATT&CK フレームワークを使用して脅威検出と対応が強化されており、次の機能が組み込まれています。

- 侵入イベントには TTP が含まれます。これにより、管理者は、脆弱性タイプ、ターゲットシステム、または脅威カテゴリに従ってルールをグループ化して、より緻密にトラフィックを管理できるようになります。
- TTP を使用するマルウェアイベントを選択して、脅威を検出して対応する機能を強化できます。

- 統合イベントビューアとクラシックイベントビューアには、Talos 分類による戦術、手法、攻撃のライフサイクルグラフ、およびコンテキストに応じたエンリッチメントが表示されます。これらのエンリッチメントには、MITRE タグと、関連する戦術、手法、およびサブ手法の階層ビューが含まれます。MITRE 識別子を使用してイベントをフィルタ処理することもできます。

MITRE フレームワークの利点

- MITRE の戦術、手法、および手順（TTP）が侵入イベントに追加されることで、管理者は MITRE ATT&CK フレームワークに基づいてトラフィックに対処できるようになります。これにより、管理者はトラフィックをより細かく表示および処理でき、脆弱性タイプ、ターゲットシステム、または脅威カテゴリ別にルールをグループ化することができます。
- MITRE ATT&CK フレームワークに従って侵入ルールを編成できます。これにより、特定の攻撃者の戦術と手法に応じてポリシーをカスタマイズできます。

MITRE ネットワークのビジネスシナリオの例

大規模な企業ネットワークで、主要な侵入検知および防御システムとして Snort 3 を使用しているとします。セキュリティへの脅威が急速に進化する状況では、堅牢なネットワークセキュリティ対策の採用が必要かつ重要です。ネットワーク管理者は、設定されたポリシーで対象のトラフィックが検出されているかどうかと、既知の攻撃グループがトラッキングされているかどうかを知る必要があります。たとえば、攻撃者がシステムまたはアプリケーションの弱点を利用して、予期しない動作を引き起こそうとしているかどうかを知る必要がある場合があります。考えられるシステムの弱点には、バグ、グリッチ、または設計上の脆弱性があります。考えられるアプリケーションには、Web サイト、データベース、サーバーメッセージブロック（SMB）やセキュアシェル（SSH）などの標準サービス、ネットワークデバイスの管理プロトコル、または Web サーバーや関連サービスなどのアプリケーションがあります。

MITRE フレームワークによって提供されるインサイトにより、管理者は特定の資産の保護を指定し、特定の脅威グループからネットワークを保護するための、より適切な機会を得ることができます。

MITRE フレームワークの前提条件

- Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense バージョン 7.3.0 以降を Snort 3 とともに実行している必要があります。
- 少なくとも 1 つの侵入ポリシーが必要です。「カスタム Snort 3 侵入ポリシーの作成」を参照してください。

Snort 3 侵入ポリシーの表示と編集

手順

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

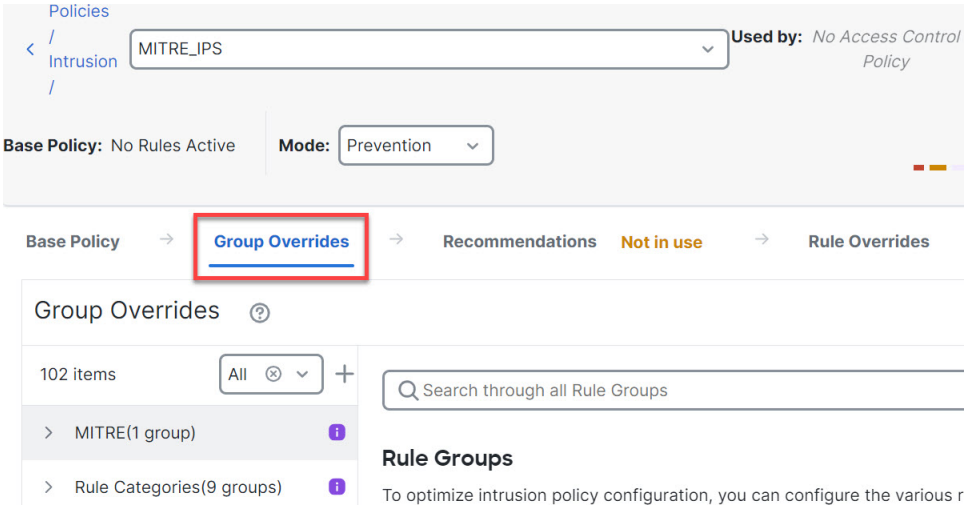
ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 表示または編集する侵入ポリシーの横にある [Snort 3バージョン（Snort 3 Version）] をクリックします。

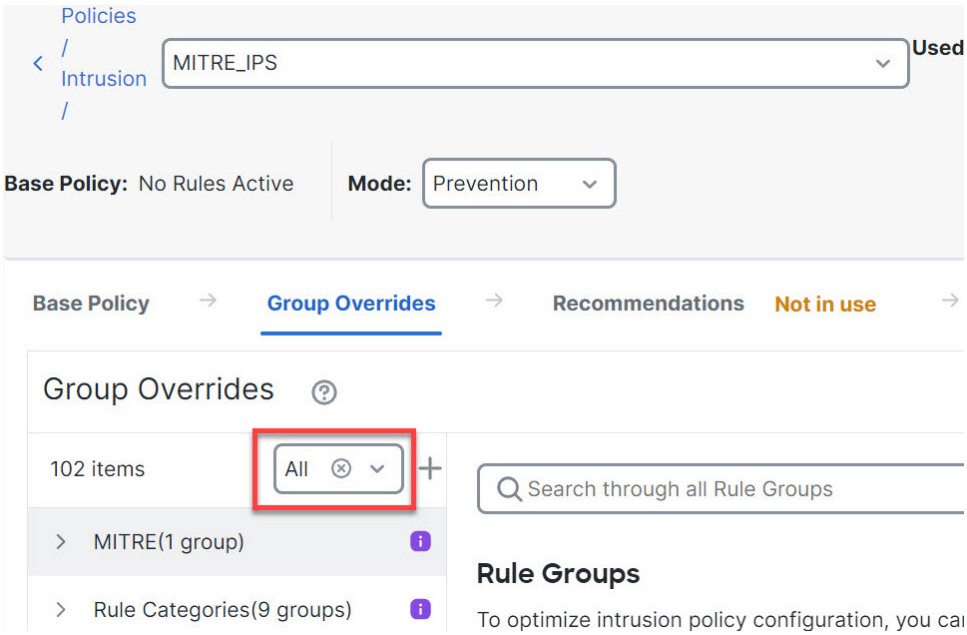
ステップ 4 表示された Snort ヘルパーガイドを閉じます。

ステップ 5 [グループのオーバーライド（Group Overrides）] レイヤをクリックします。

このレイヤには、ルールグループのすべてのカテゴリが階層構造で一覧表示されます。各ルールグループで、最後のリーフルールグループまでドリルダウンできます。

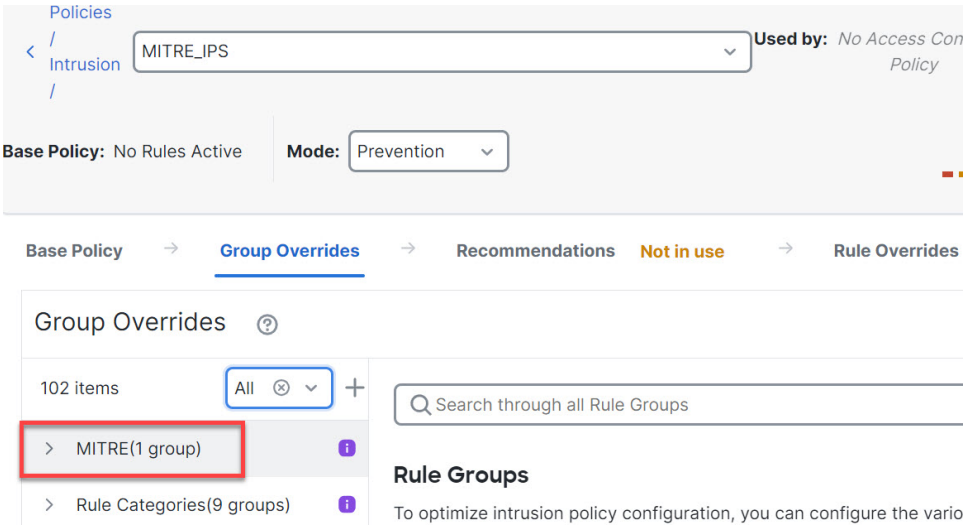


ステップ 6 [グループのオーバーライド（Group Overrides）] で、ドロップダウンリストで [すべて（All）] が選択されていることを確認します。これにより、対応する侵入ポリシーのすべてのルールグループが左側のペインに表示されます。

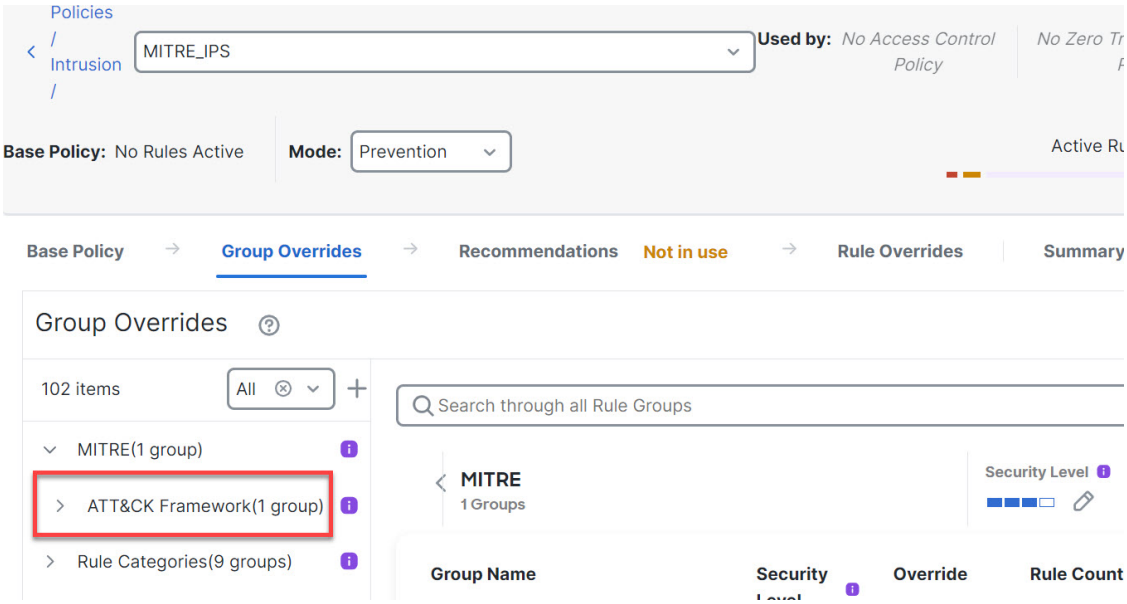


ステップ 7 左側のペインで、[MITRE] をクリックします。

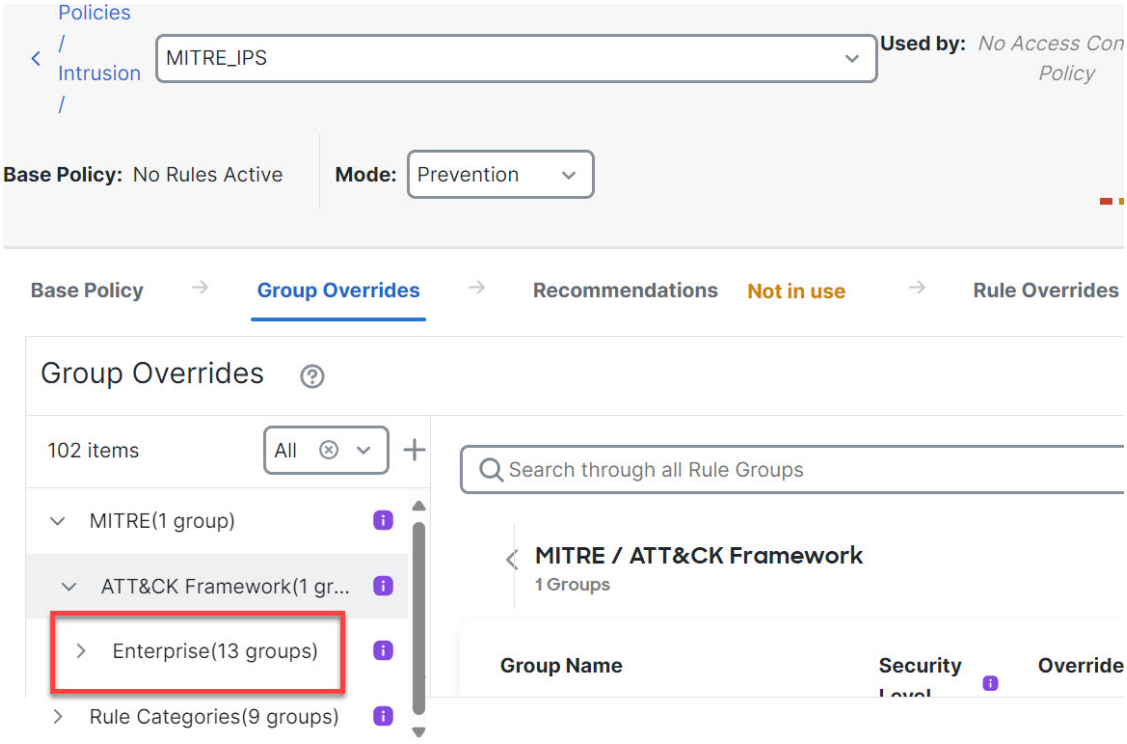
（注）
特定の要件に応じて、[ルールカテゴリ（Rule Categories）] ルールグループまたはその他のルールグループと、その下のサブルールグループを選択できます。すべてのルールグループで MITRE フレームワークが使用されます。



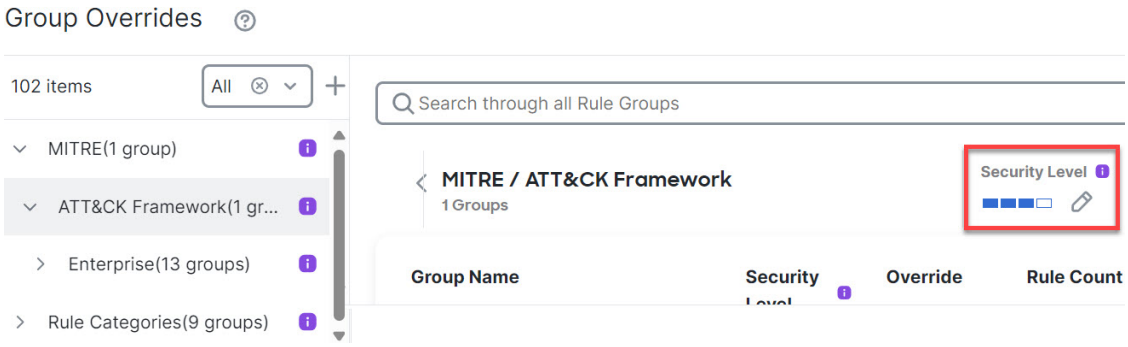
ステップ 8 [MITRE] で、[ATT&CKフレームワーク（ATT&CK Framework）] をクリックしてドリルダウンします。



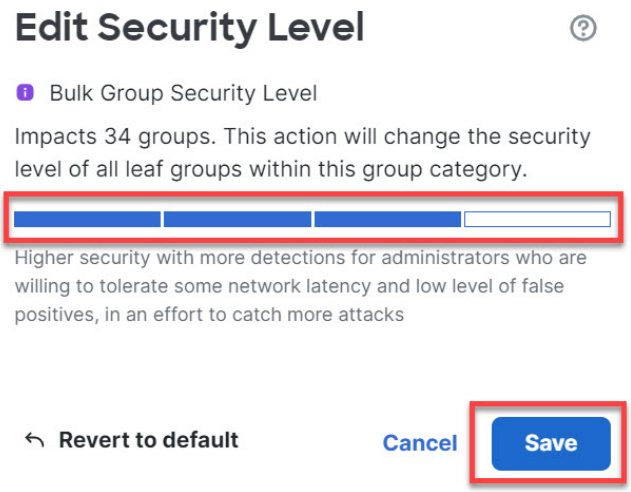
ステップ 9 [ATT&CKフレームワーク（ATT&CK Framework）] の下で、[エンタープライズ（Enterprise）] をクリックして展開します。



ステップ 10 ルールグループの **[セキュリティレベル（Security Level）]** の横にある **Edit** (✎) アイコンをクリックすると、**[エンタープライズ（Enterprice）]** ルールグループカテゴリのすべての関連ルールグループのセキュリティレベルに一括変更を適用できます。

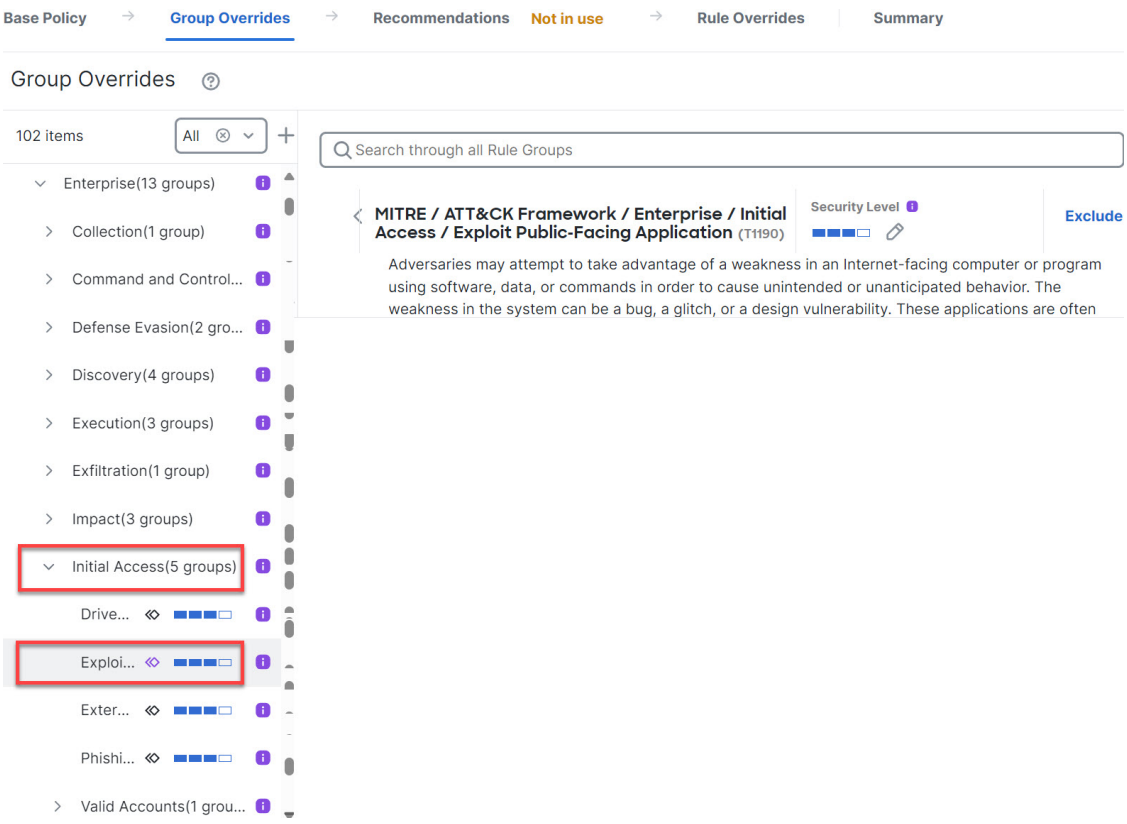


ステップ 11 [セキュリティレベルの編集（Edit Security Level）] ウィンドウで**セキュリティレベル**（この例では **3**）を選択し、[保存（Save）] をクリックします。

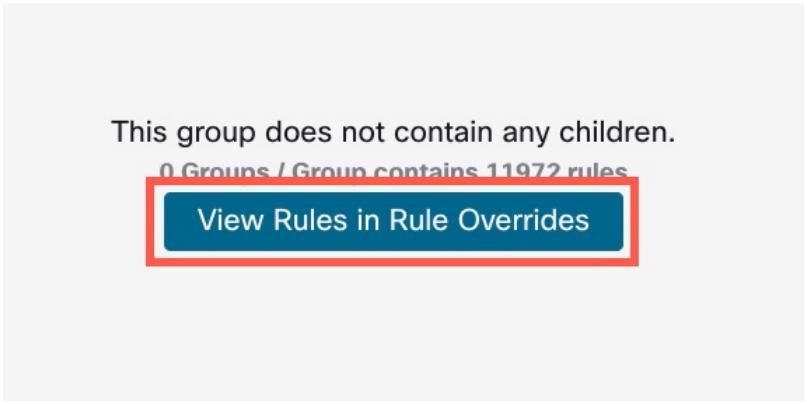


ステップ 12 [エンタープライズ（Enterprise）] の下で、[初期アクセス（Initial Access）] をクリックして展開します。

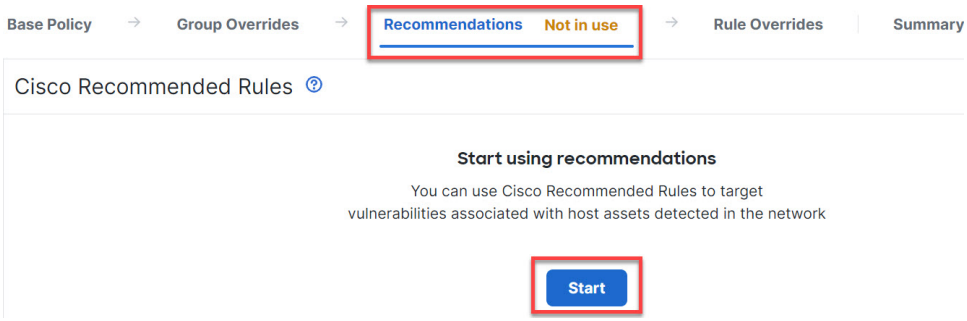
ステップ 13 [初期アクセス（Initial Access）] で、最後のリーフグループである [外部公開されたアプリケーションへの攻撃（Exploit Public-Facing Application）] をクリックします。



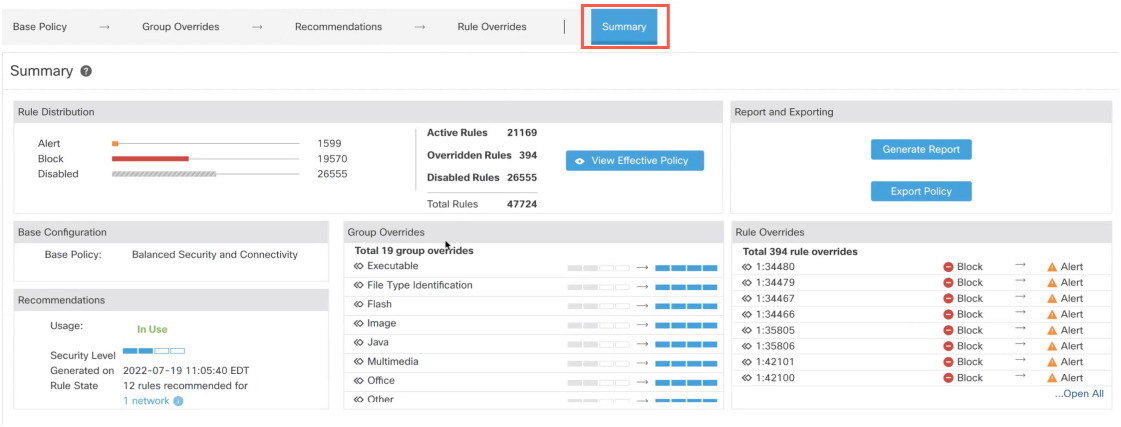
ステップ 14 [ルールのオーバーライドでルールを表示する（View Rules in Rule Overrides）] をクリックして、さまざまなルール、およびさまざまなルールのルール詳細やルールアクションなどを表示します。[ルールのオーバーライド（Rule Overrides）] レイヤで、1 つまたは複数のルールのルールアクションを変更できます。



ステップ 15 [推奨事項（Recommendations）] レイヤをクリックしてから [開始（Start）] をクリックして、シスコが推奨するルールの使用を開始します。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。詳細については、「Snort 3 での新しい Cisco Secure Firewall 推奨事項の生成」を参照してください。



ステップ 16 ポリシーに対する現在の変更の全体像を表示するには、[概要（Summary）] レイヤをクリックします。ルールのオーバーライド、セキュリティレベルの変更、およびシスコが推奨するルールの生成に基づいて、ポリシーのルール配分、グループのオーバーライド、ルールのオーバーライド、ルールの推奨事項などを表示して、変更を確認することができます。



次のタスク

侵入ポリシーを展開し、Snort ルールによってトリガーされたイベントを検出してログに記録します。「設定変更の展開」を参照してください。

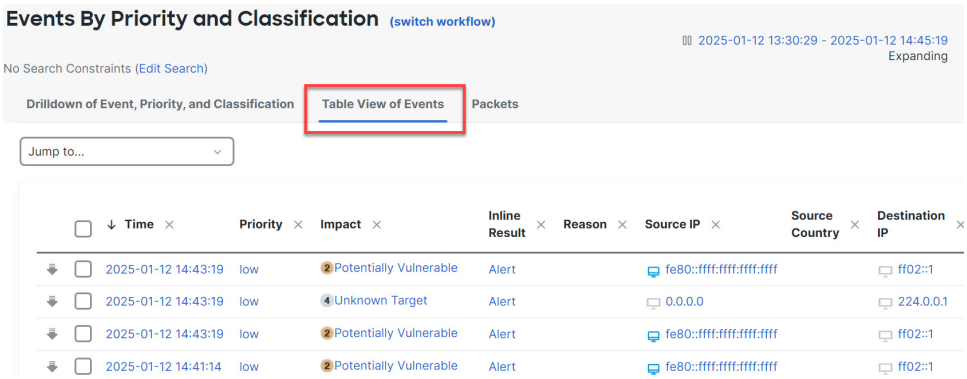
侵入イベントの表示

[クラシックイベントビューア（Classic Event Viewer）] ページと [統合イベントビューア（Unified Event Viewer）] ページで、侵入イベントの MITRE ATT&CK の手法とルールグループを表示できます。Talos により、Snort ルール（GID:SID）から MITRE ATT&CK の手法とルールグループへのマッピングが提供されます。これらのマッピングは、Lightweight Security Package（LSP）の一部としてインストールされます。

手順

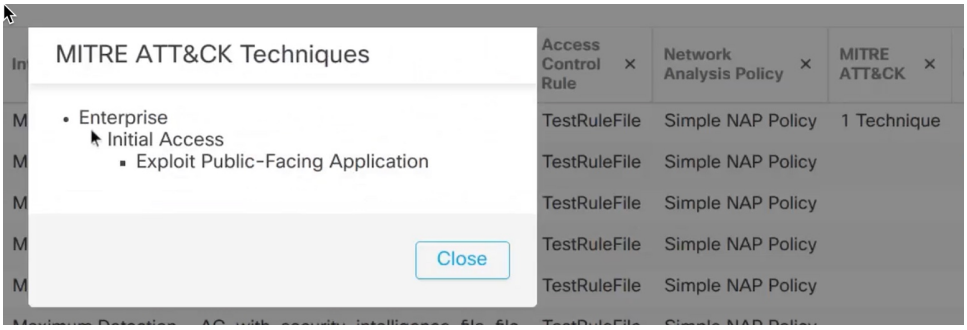
ステップ 1 [分析（Analysis）] をクリックし、[侵入（Intrusions）] で [イベント（Events）] を選択します。

ステップ 2 [イベントのテーブルビュー（Table View of Events）] タブをクリックします。



ステップ 3 [MITRE ATT&CK] で、侵入イベント用の手法を確認できます。[1件の手法（1 Technique）] をクリックして、MITRE ATT&CK の手法を表示します。

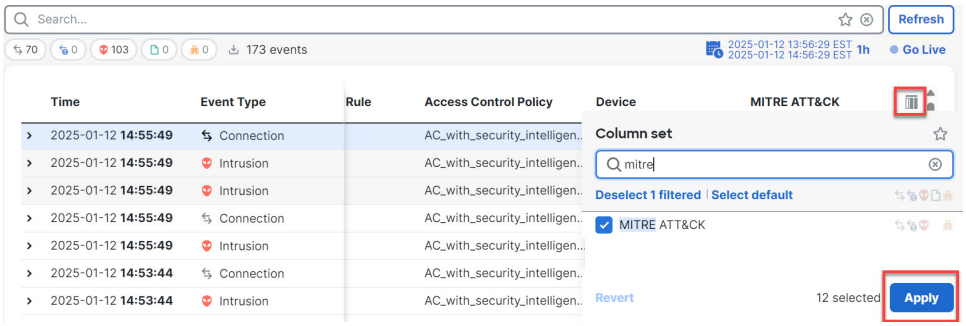
この例では、手法は [外部公開されたアプリケーションへの攻撃（Exploit Public-Facing Application）] です。



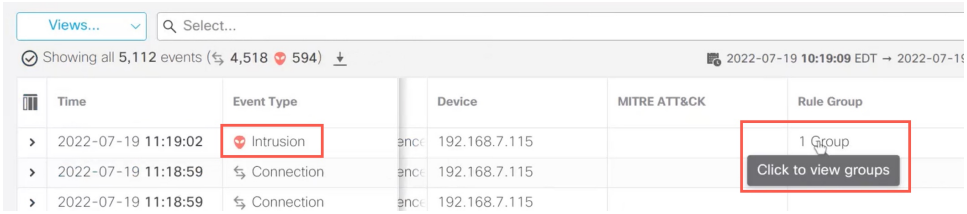
ステップ 4 [閉じる（Close）] をクリックします。

ステップ 5 [分析（Analysis）] をクリックして [統合イベント（Unified Events）] を選択します。

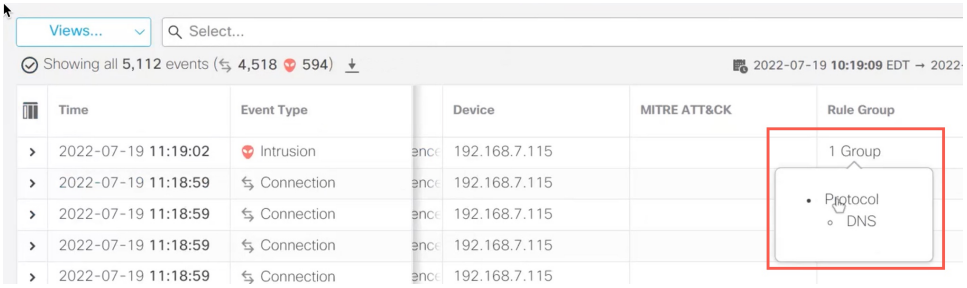
ステップ 6 [MITRE ATT&CK] 列と [ルールグループ（Rule Group）] 列が有効になっていない場合は、列セレクタアイコンをクリックして有効にします。



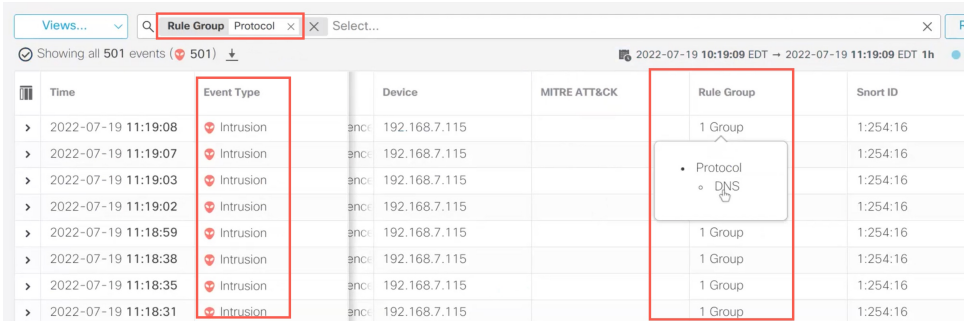
ステップ 7 この例では、侵入イベントは、1 つのルールグループにマッピングされたイベントによってトリガーされます。[ルールグループ（Rule Group）] 列の下にある [1つのグループ（1 Group）] をクリックします。



ステップ 8 親ルールグループである [プロトコル（Protocol）] と、その下の [DNS] ルールグループを表示できます。**[プロトコル（Protocol）]>[DNS]** を選択して、少なくとも 1 つのルールグループを持つすべての侵入イベントを検索します。



検索結果が表示されます。



その他の参考資料

- Intrusion Policy in Snort 3
- Snort 3 侵入ポリシーの編集
- MITRE Information in Malware Events

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。