MITERフレームワークを使用したSecure FMCでの潜在的な脅威の表示と対処

内容

[はじめに](#)

[バックグラウンド情報](#)

[前提条件](#)

- [要 件](#)
- [使用するコンポーネント](#)

[MITERフレームワークの利点](#)

- [侵入ポリシーのMITERフレームワークを表示する](#)
- [侵入イベントの表示](#)

はじめに

このドキュメントでは、MITERフレームワークを使用して、セキュアなFirepower Management Center(FMC)で潜在的な脅威を表示して対処する方法について説明します。

バックグラウンド情報

MITER ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge)フレームワークは、システムに損害を与えることを目的として脅威アクターによって配布される戦術、手法、手順(TTP)に関する洞察を提供する広範なナレッジベースおよび手法です。ATT&CKは、それぞれオペレーティングシステムまたは特定のプラットフォームを表すマトリックスにコンパイルされます。「戦術」と呼ばれる攻撃の各ステージは、「手法」と呼ばれる、これらのステージを達成するために使用される特定の方法にマッピングされます。

ATT&CKフレームワークの各テクニックには、テクニック、関連する手順、考えられる防御と検出、および実際の例に関する情報が付随しています。また、MITER ATT&CKフレームワークには、使用している一連の戦術および手法に基づいて脅威グループ、活動グループ、または脅威アクターを指すグループも組み込まれています。このフレームワークでは、グループを使用して動作を分類および文書化できます。

MITERの詳細については、https://attack.mitre.orgを参照してください。

前提条件

要 件

次の項目に関する知識があることが推奨されます。

- Snortに関する知識
- セキュアFMC
- セキュアなFirepower Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- このドキュメントは、すべてのFirepowerプラットフォームに適用されます
- ソフトウェアバージョン7.3.0を実行するセキュアFTD
- ソフトウェアバージョン7.3.0を実行するSecure Firepower Management Center Virtual(FMC)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

MITERフレームワークの利点

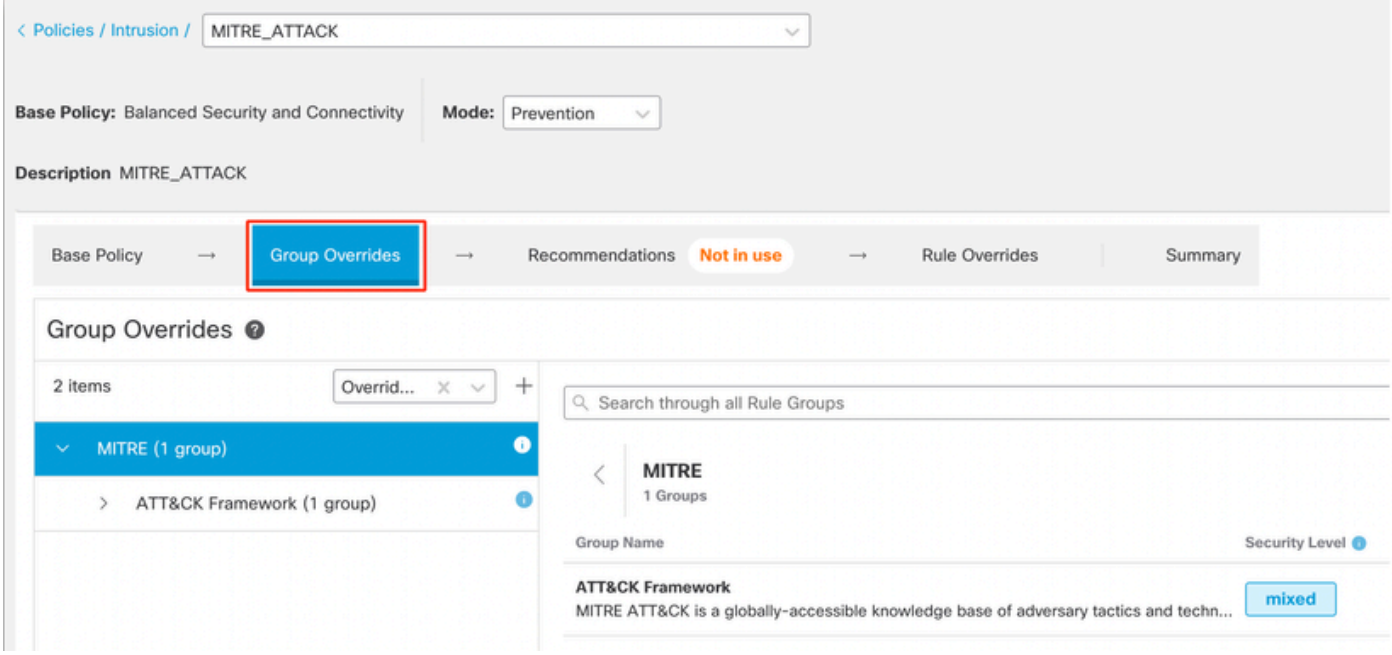
- MITER ATT&CK(Adversary Tactics Techniques and Common Knowledge)フレームワークに基づいて管理者がトラフィックに対して行動できるようにする侵入イベントに、MITER Tactics, Techniques, and Procedures(TTP)が追加されました。これにより、管理者はより詳細にトラフィックを表示および処理でき、脆弱性タイプ、ターゲットシステム、または脅威カテゴリ別にルールをグループ化できます。
- MITER ATT&CKフレームワークに従って侵入ルールを編成できます。これにより、特定の攻撃者の戦術と手法に従ってポリシーをカスタマイズできます。

侵入ポリシーのMITERフレームワークを表示する

MITERフレームワークを使用すると、侵入ルールをナビゲートできます。MITERは、ルールグループのもう1つのカテゴリであり、Talosルールグループの一部です。複数レベルのルールグループに対するルールナビゲーションがサポートされており、ルールの柔軟性と論理的なグループ化が向上します。

1. Policies > Intrusionの順に選択します。
2. 侵入ポリシーが選択されていることを確認します。
3. 表示または編集する侵入ポリシーの横にあるSnort 3バージョンをクリックします。ポップアップ表示されたSnortヘルパーガイドを閉じます。
4. Group Overrideslayerをクリックします。

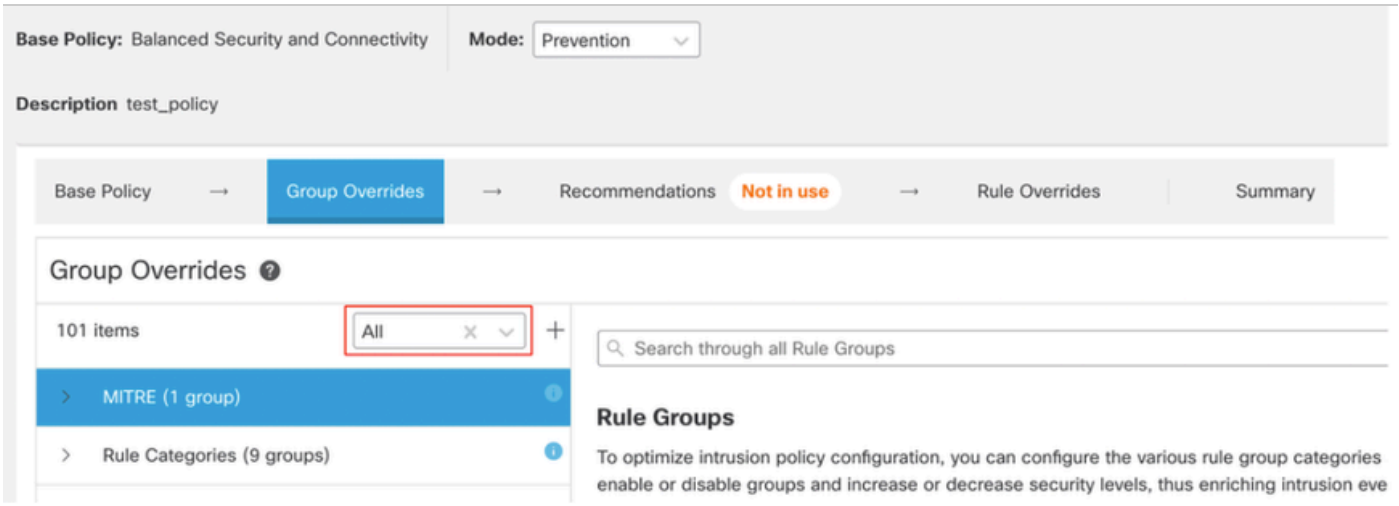
グループオーバーライド層は、階層構造のルールグループのすべてのカテゴリをリストします。各ルールグループの最後のリーフルールグループに移動できます。



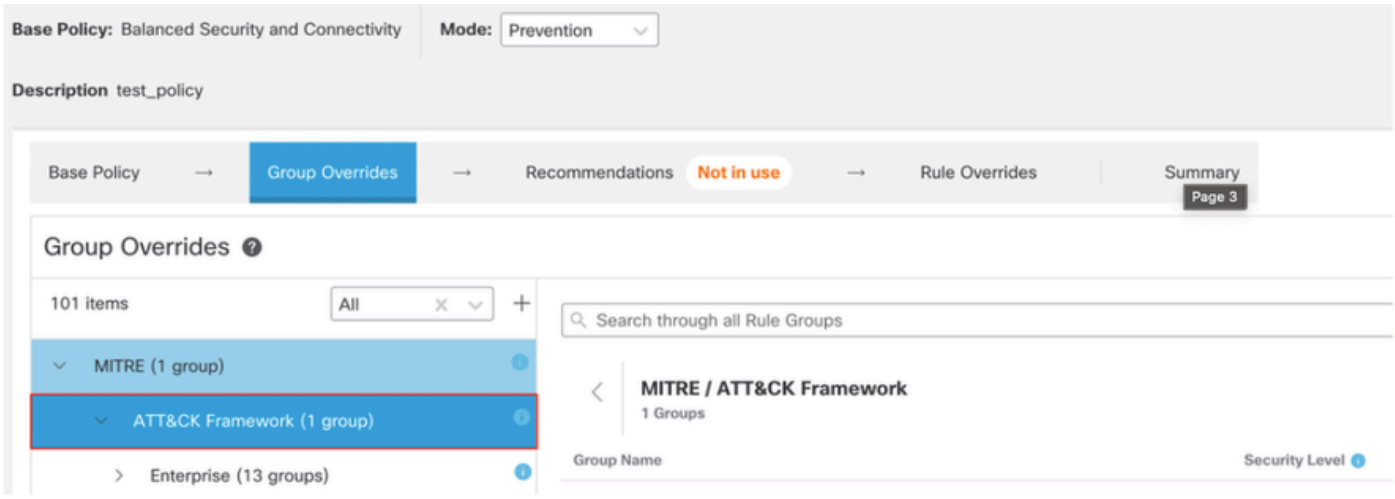
6. Group Overridesの下で、Allがドロップダウンリストで選択されているため、侵入ポリシーのすべてのルールグループが左側のペインに表示されます。

7. マイタをクリックします左側のペインに表示されます。

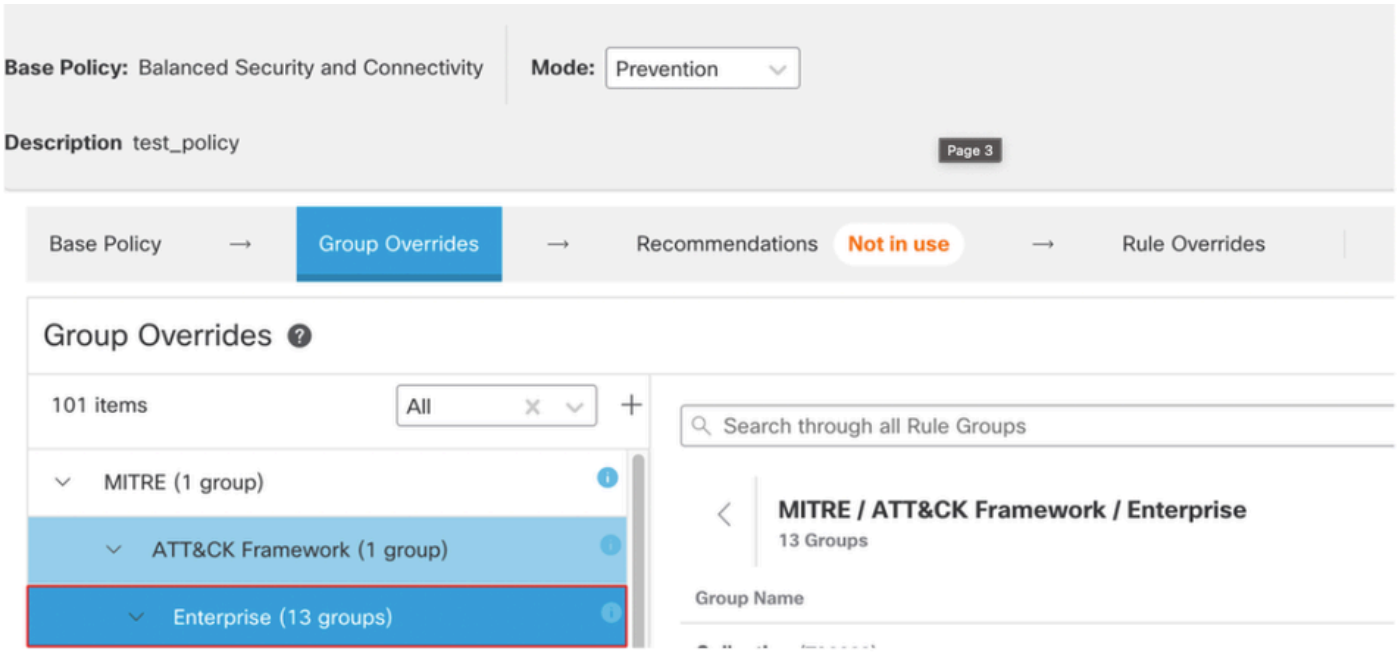
注意：この例では「MITER」が選択されていますが、特定の要件に応じて「ルール・カテゴリ」ルール・グループ、または他のルール・グループとその下にある後続のルール・グループを選択できます。すべてのルールグループはMITERフレームワークを使用します。



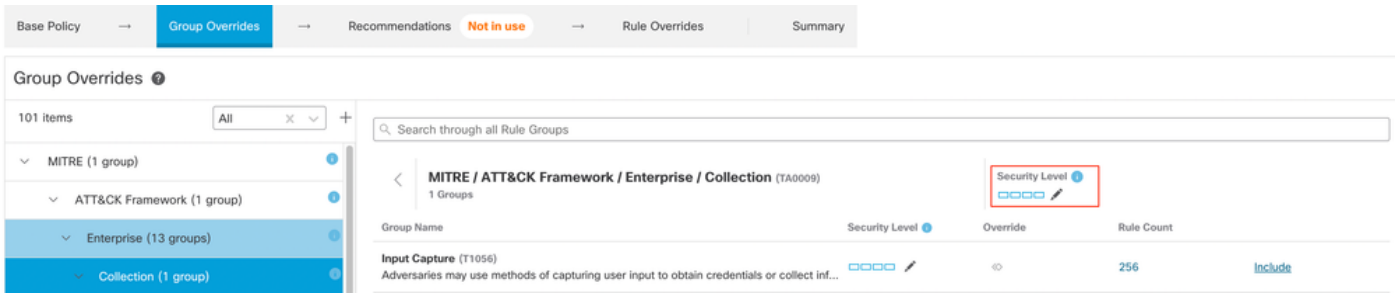
8. 「MITER」の下の「ATT&CK Framework」をクリックして展開します。



9. 「ATT&CK Framework」で「Enterprise」をクリックして展開します。

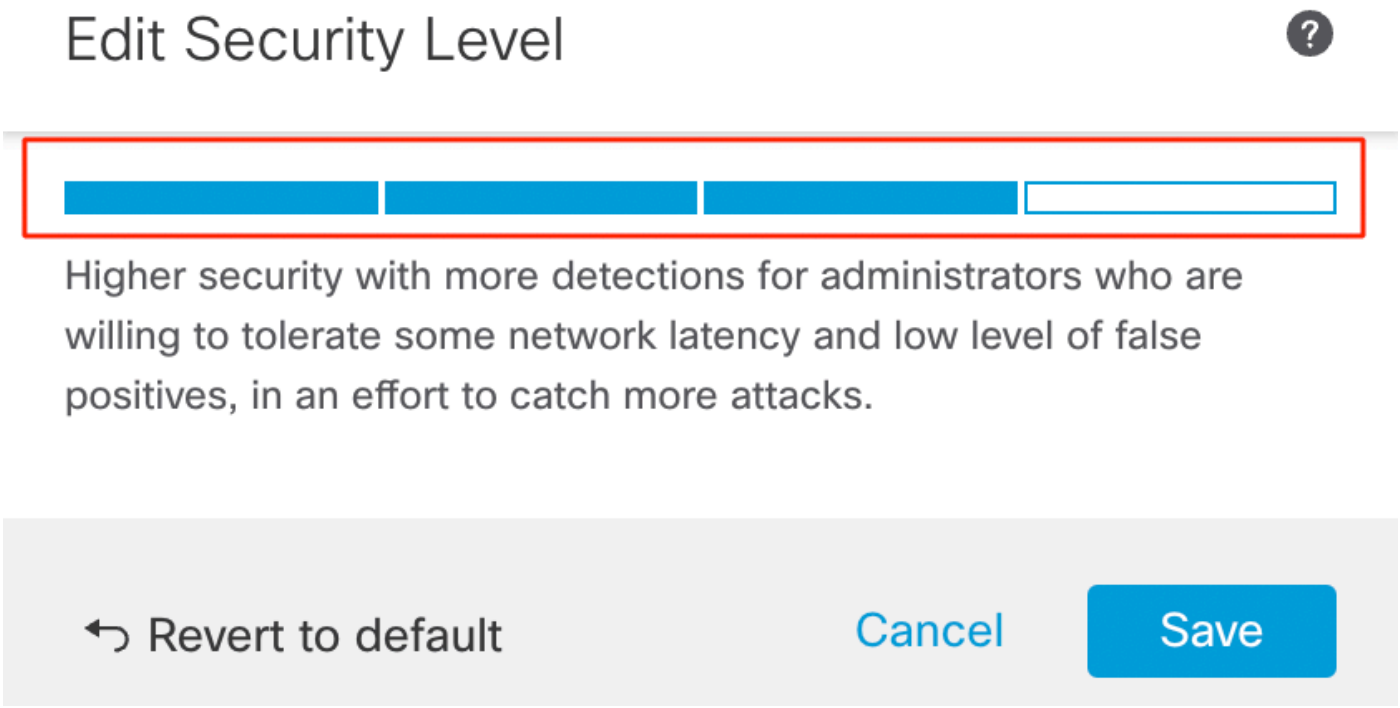


10. ルールグループのセキュリティレベルの横にある編集( )をクリックして、エンタープライズ内の関連付けられているすべてのルールグループのセキュリティレベルを一括して変更しますルールグループカテゴリ。



セキュリティ規則グループの編集

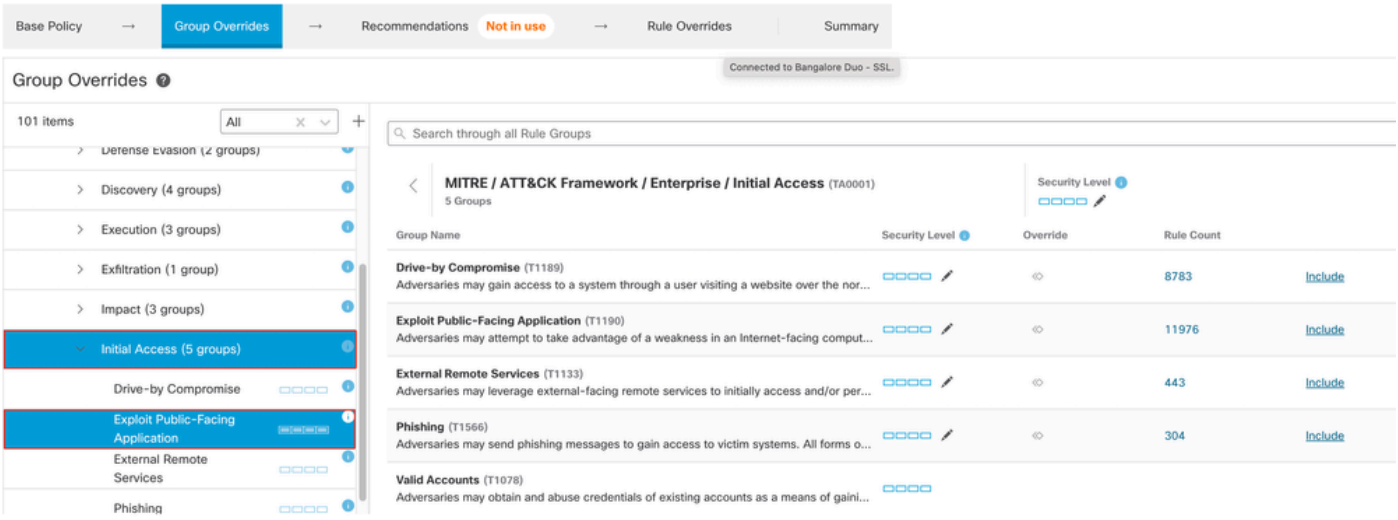
11. 例として、Edit Security Levelウィンドウでsecurity level 3を選択して、Saveをクリックします。



セキュリティレベル

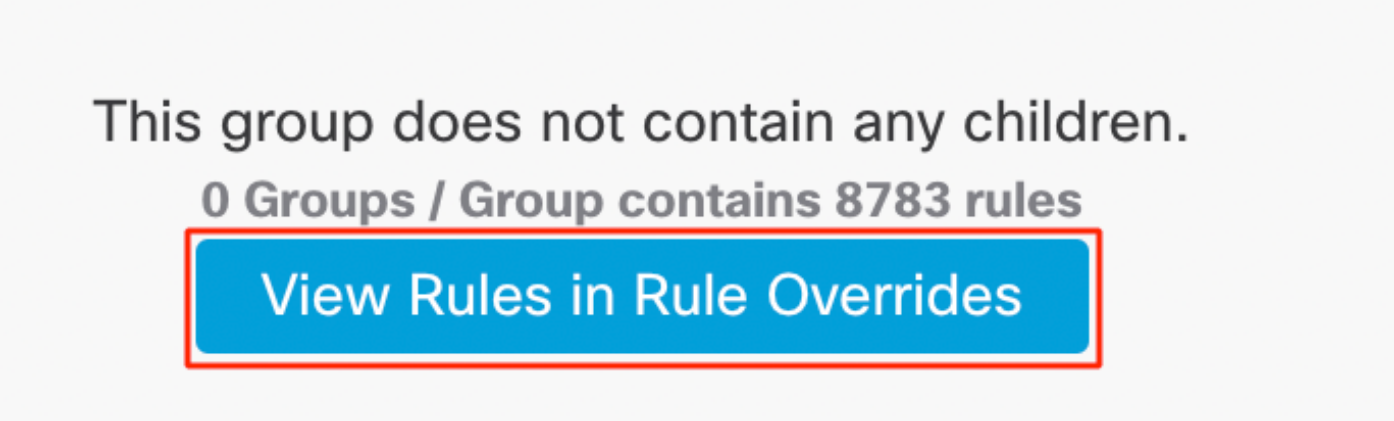
12. 「Enterprise」の下の「Initial Access」をクリックして展開します。

13. Initial Accessの下で、最後のリーフグループであるExploit Public-Facing Applicationをクリックします。



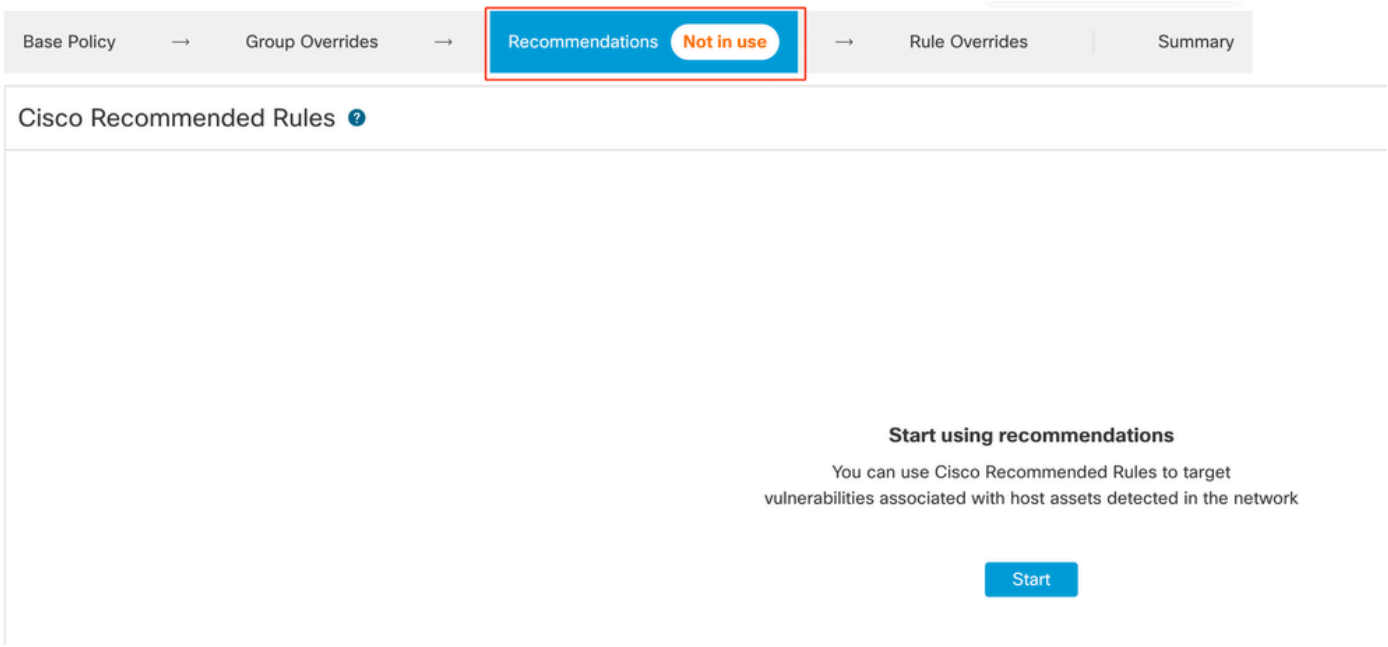
初期アクセスグループ

14. 「ルールの上書き」で「ルールの表示」をクリックしますボタンをクリックして、各ルールの各種ルール、ルールの詳細、ルールの処理などを表示します。

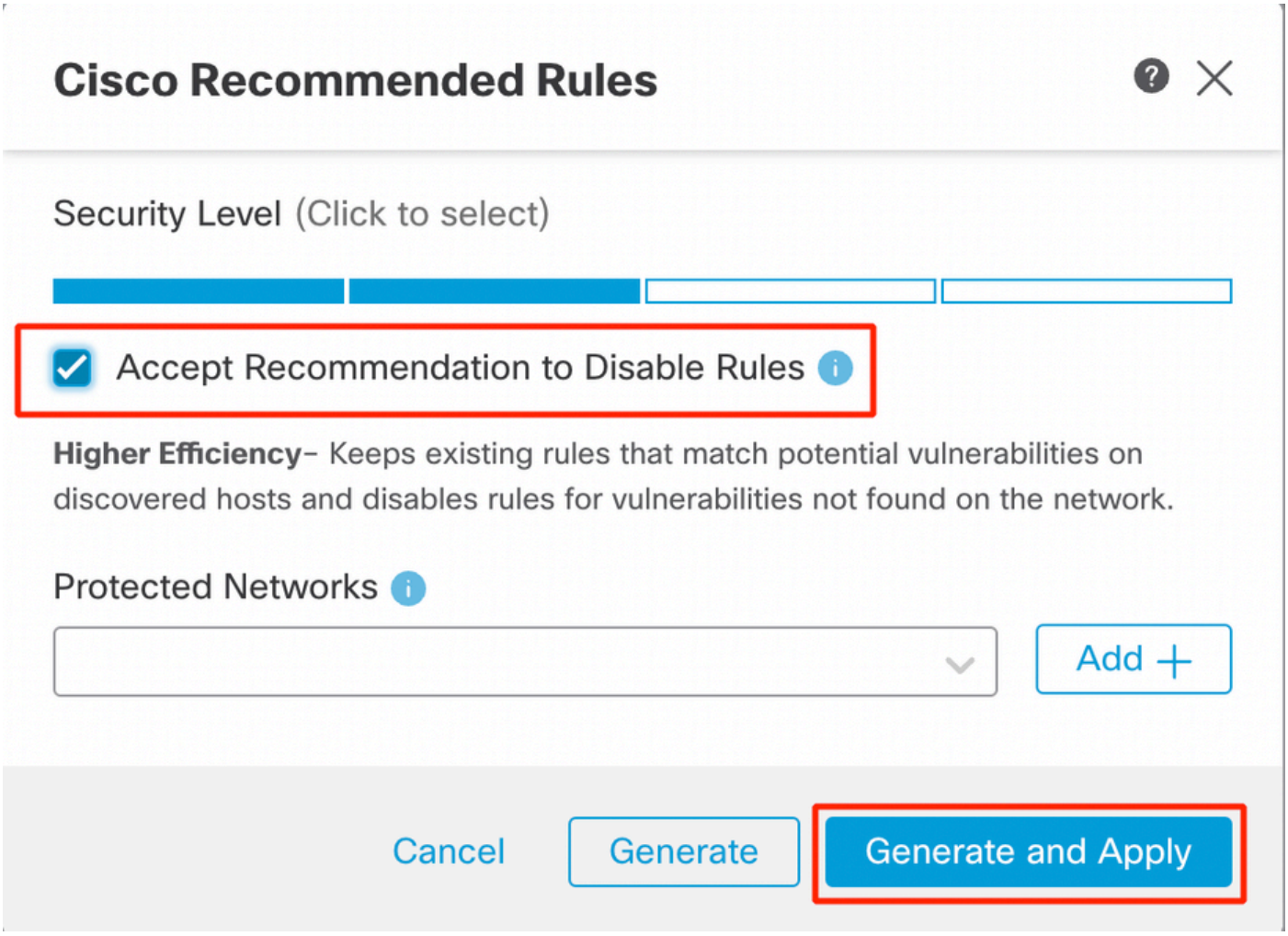


ルールの上書きのルール

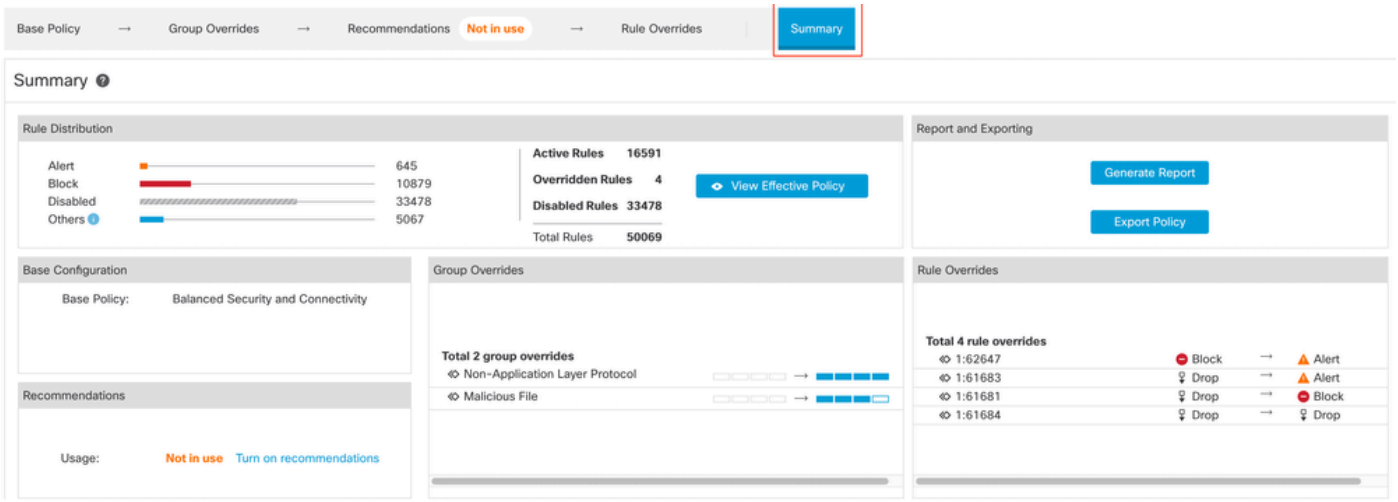
15. 「推奨事項」をクリックしますレイヤを選択し、Startをクリックして、シスコが推奨するルールの使用を開始します。侵入ルールの推奨事項を使用して、ネットワークで検出されたホスト資産に関連する脆弱性を対象にすることができます。参照してください。



推奨事項



16. Summaryをクリックしますポリシーに対する現在の変更の全体像を把握するためのレイヤ。ポリシーのルール配布、グループの上書き、ルールの上書きなどを表示できます。



ポリシーサマリー

侵入イベントの表示

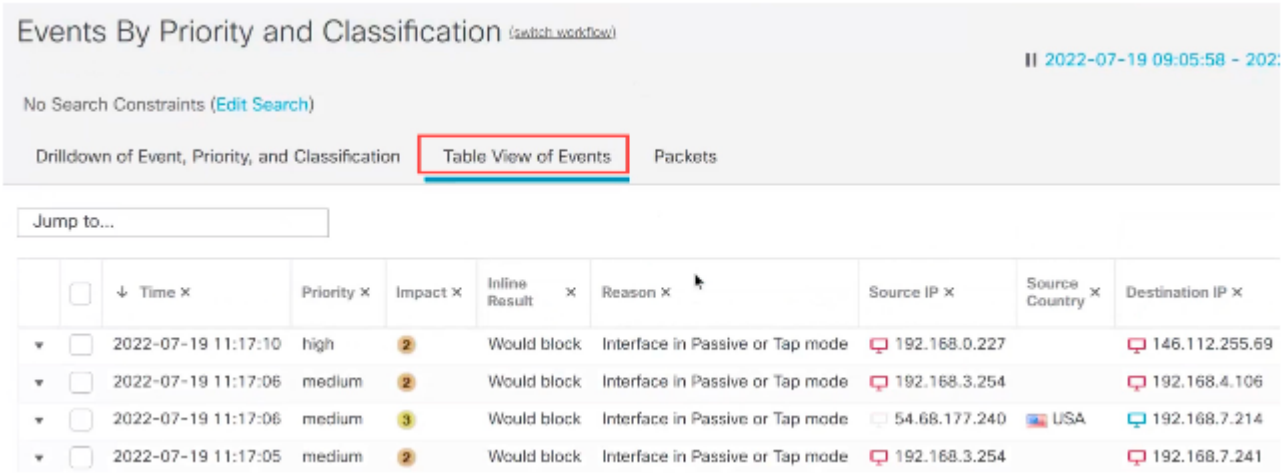
MITER ATT&CKテクニックおよびルールグループは、クラシックイベントビューアおよびユニファイドイベントビューアの侵入イベントで表示できます。Talosは、Snortルール(GID:SID)からMITER ATT&CKテクニックおよびルールグループへのマッピングを提供します。これらのマッピ

ングは、Lightweight Security Package(LSP)の一部としてインストールされます。

開始する前に、Snortルールによってトリガーされるイベントを検出してログに記録するために、侵入およびアクセスコントロールポリシーを導入する必要があります。

1. 「分析」>「侵入」>「イベント」の順にクリックします。

2.イベントのテーブルビューをクリックしますタブをクリックします（図を参照）。

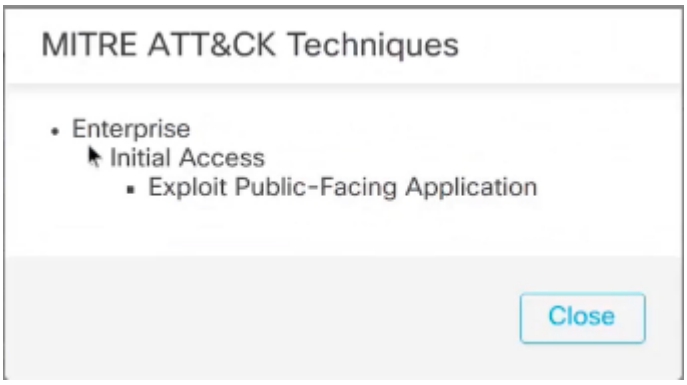


イベント

3.マイターATT&CKカラムのヘッダーを調べると、侵入イベントの手法を確認できます。

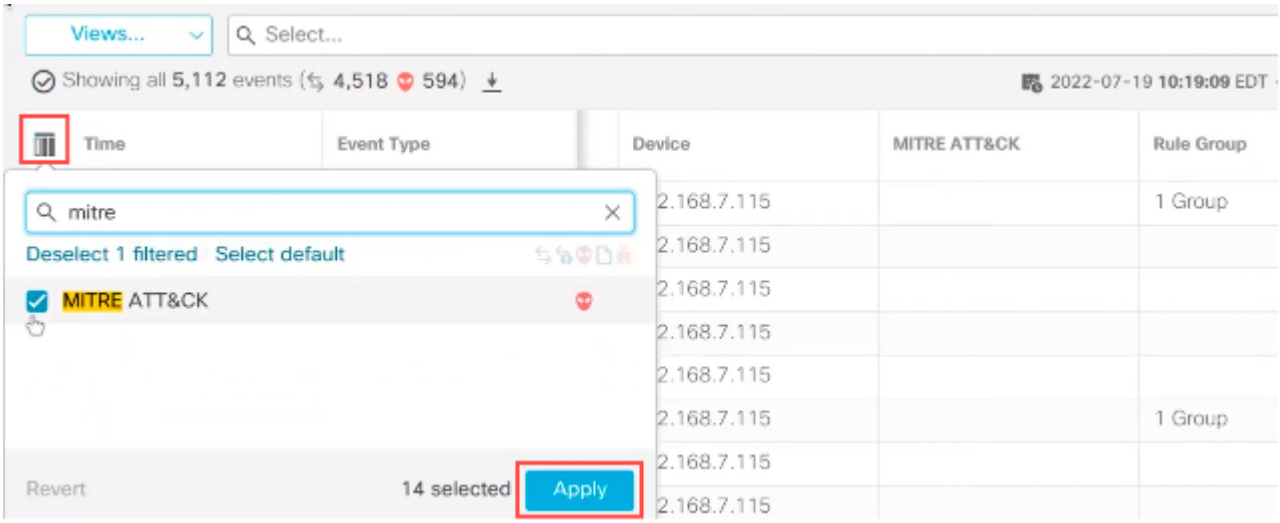
マイター列ヘッダー

4. クリック 1テクニックをクリックして、次の図に示すようにMITER ATT&CK Techniquesを表示します。この例では、公開アプリケーションを不正利用します手法です



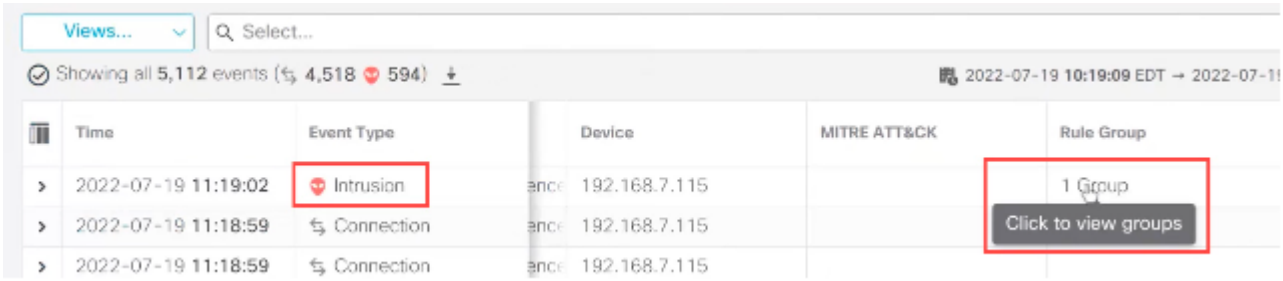
マイターATT&CKテクニック

5. Closeをクリックします。
6. Analysis > Unified Eventsの順にクリックします。
7. 列セレクタアイコンをクリックすると、MITER ATT&CKand Rule Groupcolumnsを有効にできます。



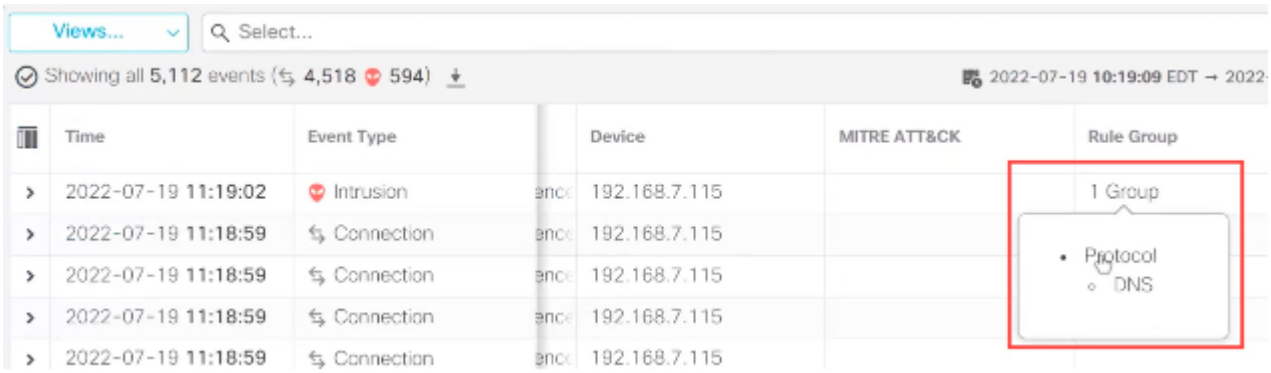
マイター攻撃を有効にする

8. 次の例に示すように、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した。Rule Groupの下にある1 Groupをクリックします。カラム.



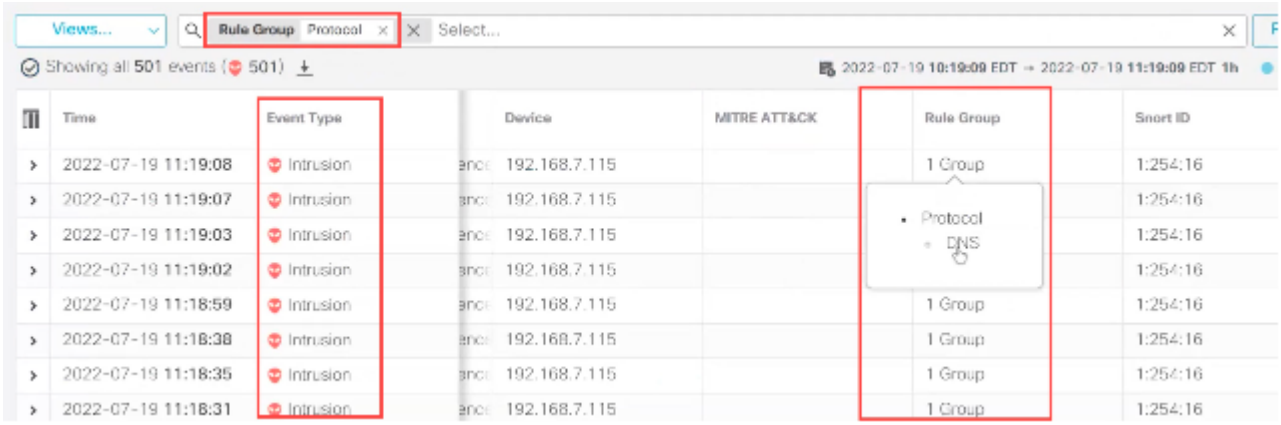
[ルール]領域

9. 例として、親ルールグループであるProtocolとその下のDNSルールグループを表示できます。



プロトコルの表示

10. Protocolをクリックすると、少なくとも1つのルールグループ(Protocol > DNS)を持つすべての侵入イベントを検索できます。次の例に示すように、検索結果が表示されます。



ルールグループプロトコル

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。