Use a estrutura MITER para visualizar e agir sobre possíveis ameaças no FMC seguro

Contents

Introdução

Este documento descreve como usar a estrutura MITER para visualizar e agir sobre possíveis ameaças em um Firepower Management Center (FMC) seguro.

Informações de Apoio

O MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework é uma base de conhecimento e metodologia extensiva que fornece insights sobre táticas, técnicas e procedimentos (TTPs) distribuídos por agentes de ameaças com o objetivo de prejudicar sistemas. O ATT&CK é compilado em matrizes que representam cada sistema operacional ou uma plataforma específica. Cada estágio de um ataque, conhecido como "táticas", é mapeado para os métodos específicos usados para alcançar esses estágios, conhecidos como "técnicas".

Cada técnica na estrutura da ATT&CK é acompanhada de informações sobre a técnica, procedimentos associados, defesas e detecções prováveis e exemplos reais. A estrutura MITER ATT&CK também incorpora grupos para se referir a grupos de ameaças, grupos de atividades ou agentes de ameaças com base no conjunto de táticas e técnicas que empregam. Usando Grupos, a estrutura ajuda a categorizar e documentar comportamentos.

Para obter mais informações sobre o MITER, consulte https://attack.mitre.org.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Snort
- FMC seguro
- Defesa contra ameaças (FTD) Secure Firepower

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Este documento se aplica a todas as plataformas Firepower
- FTD seguro executando a versão de software 7.3.0
- Secure Firepower Management Center Virtual (FMC) executando a versão de software 7.3.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Benefícios do MITER Framework

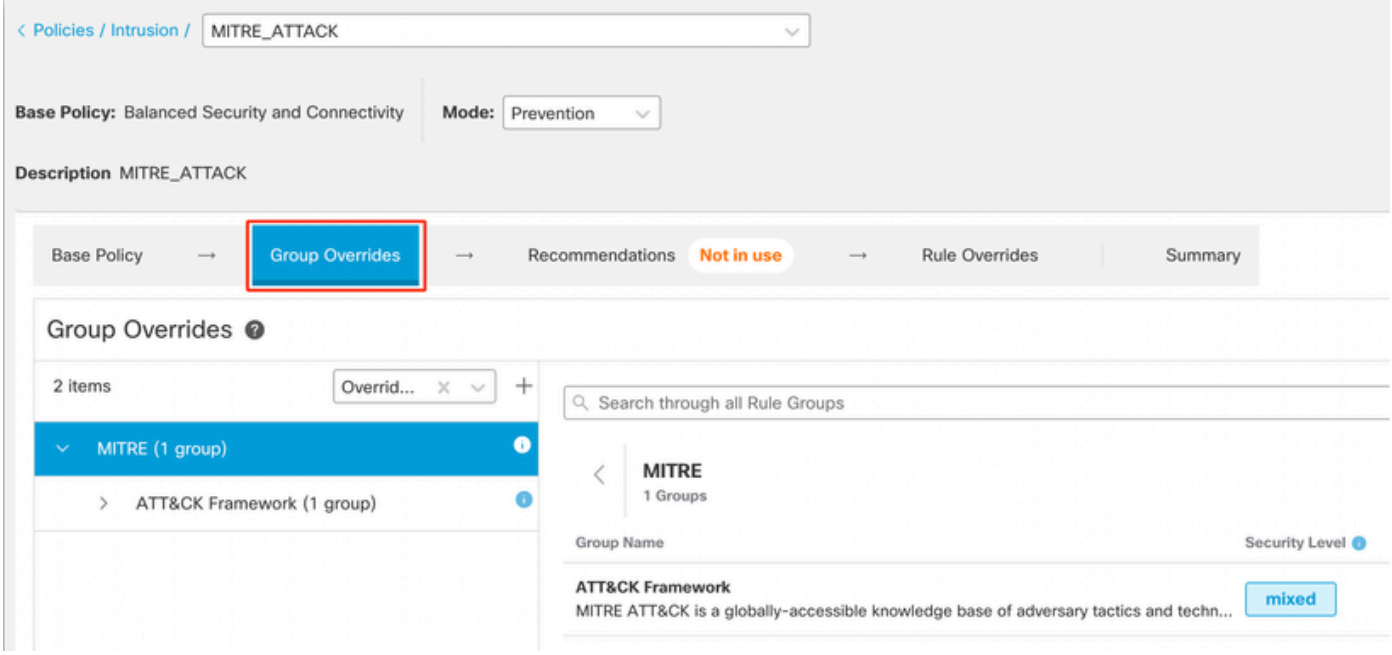
- As Táticas, Técnicas e Procedimentos (TTPs) MITER são adicionadas a eventos de invasão que permitem que os administradores atuem no tráfego com base na estrutura MITER ATT&CK (Adversary Tactics Techniques and Common Knowledge). Isso permite que os administradores visualizem e lidem com o tráfego com mais granularidade e possam agrupar regras por tipo de vulnerabilidade, sistema de destino ou categoria de ameaça.
- Você pode organizar as regras de intrusão de acordo com a estrutura MITER ATT&CK. Isso permite que você personalize políticas de acordo com táticas e técnicas específicas do invasor.

Visualize a estrutura MITER em sua política de intrusão

A estrutura MITER permite que você navegue pelas suas regras de intrusão. MITRE é apenas outra categoria de grupos de regras e faz parte dos grupos de regras do Talos. A navegação de regras para vários níveis de grupos de regras é suportada, o que fornece mais flexibilidade e agrupamento lógico de regras.

1. Escolha Policies > Intrusion.
2. Certifique-se de que a Intrusion Policiesguia seja escolhida.
3. Clique em Snort 3 Versionpróximo à política de intrusão que deseja exibir ou editar. Feche o guia auxiliar do Snort que aparece.
4. Clique na Group Overridescamada.

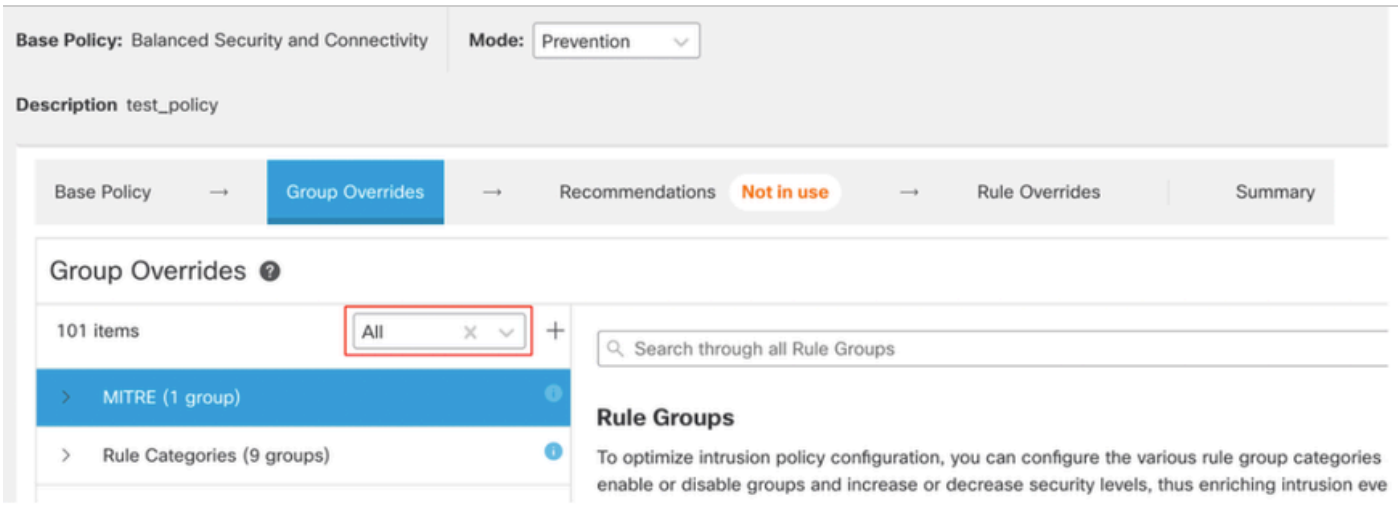
A Group Overridescamada lista todas as categorias de grupos de regras em uma estrutura hierárquica. Você pode passar para o último grupo de regras folha em cada grupo de regras.



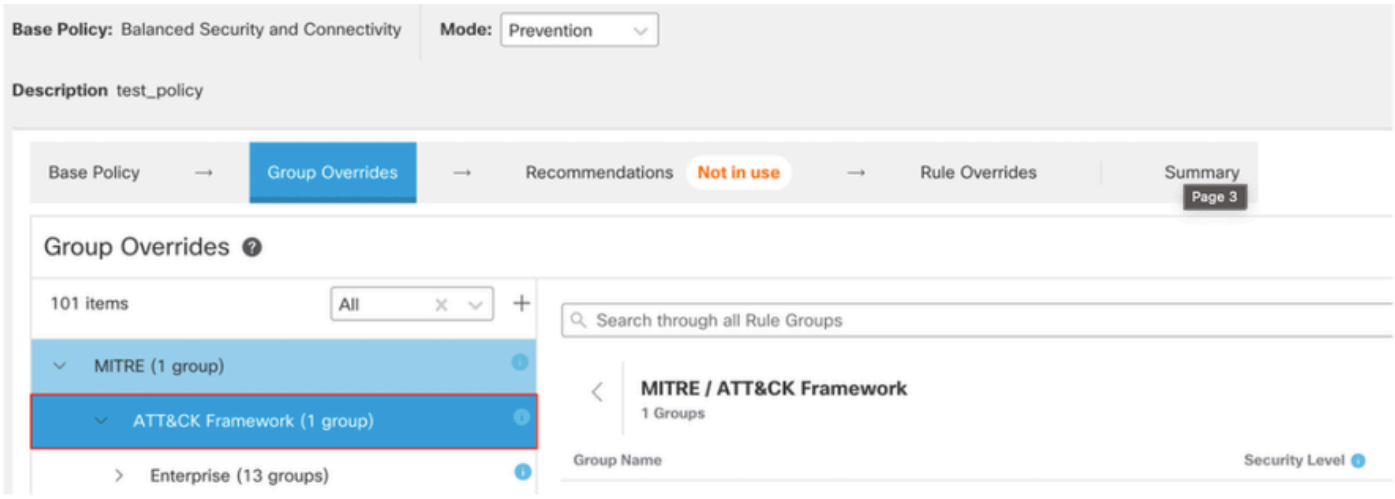
6. Nos termos Group Overridesdo Allé escolhido na lista suspensa, para que todos os grupos de regras da política de intrusão fiquem visíveis no painel esquerdo.

7. Clique em MITREno painel esquerdo.

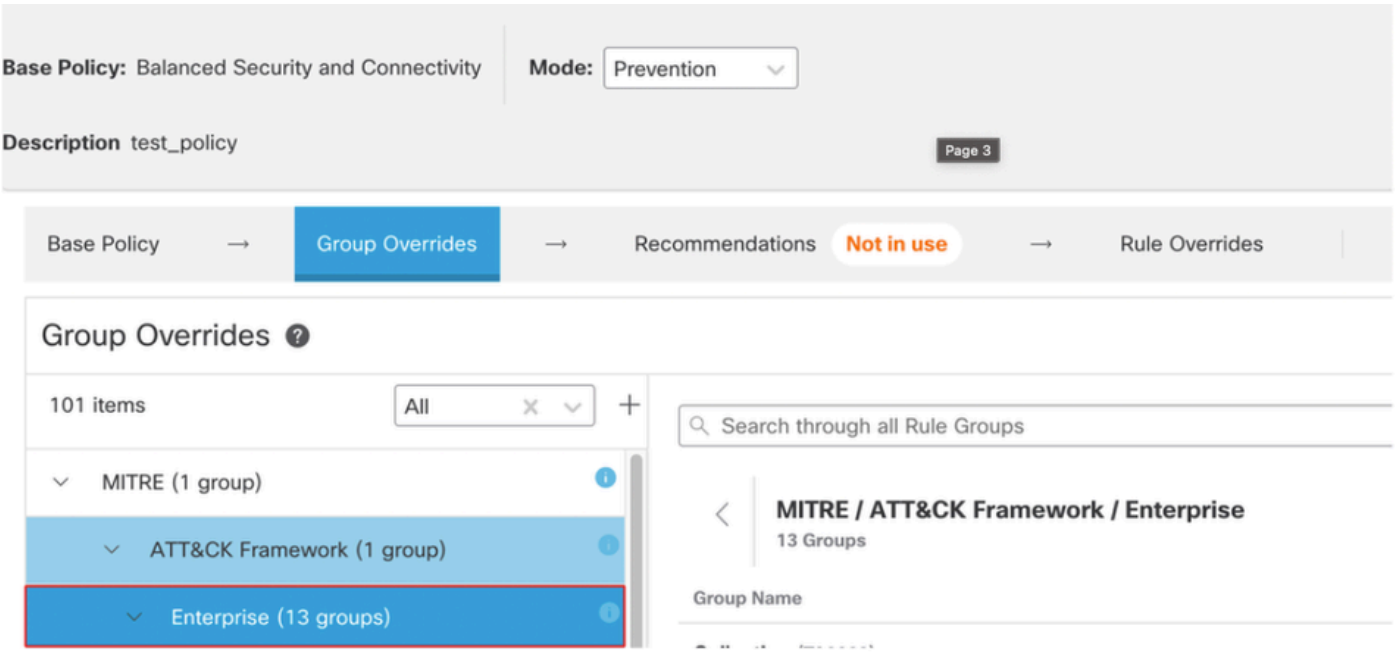
Note: Para este exemplo, MITRE é selecionado, mas dependendo de seus requisitos específicos, você pode escolher o grupo de regras Categorias de Regras ou qualquer outro grupo de regras e grupos de regras subsequentes sob ele. Todos os grupos de regras usam a estrutura MITER.



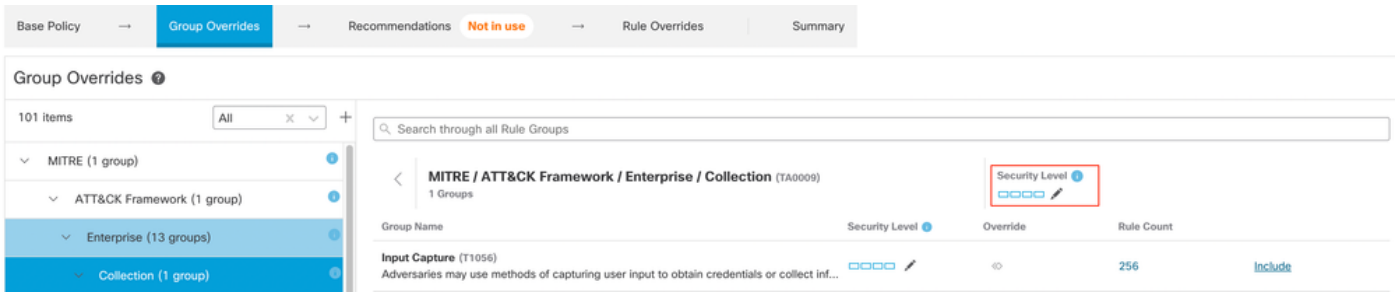
8. EmMITRE, clique em ATT&CK Framework para expandi-lo.



9. Em ATT&CK Framework, clique em Corporativo para expandi-lo.

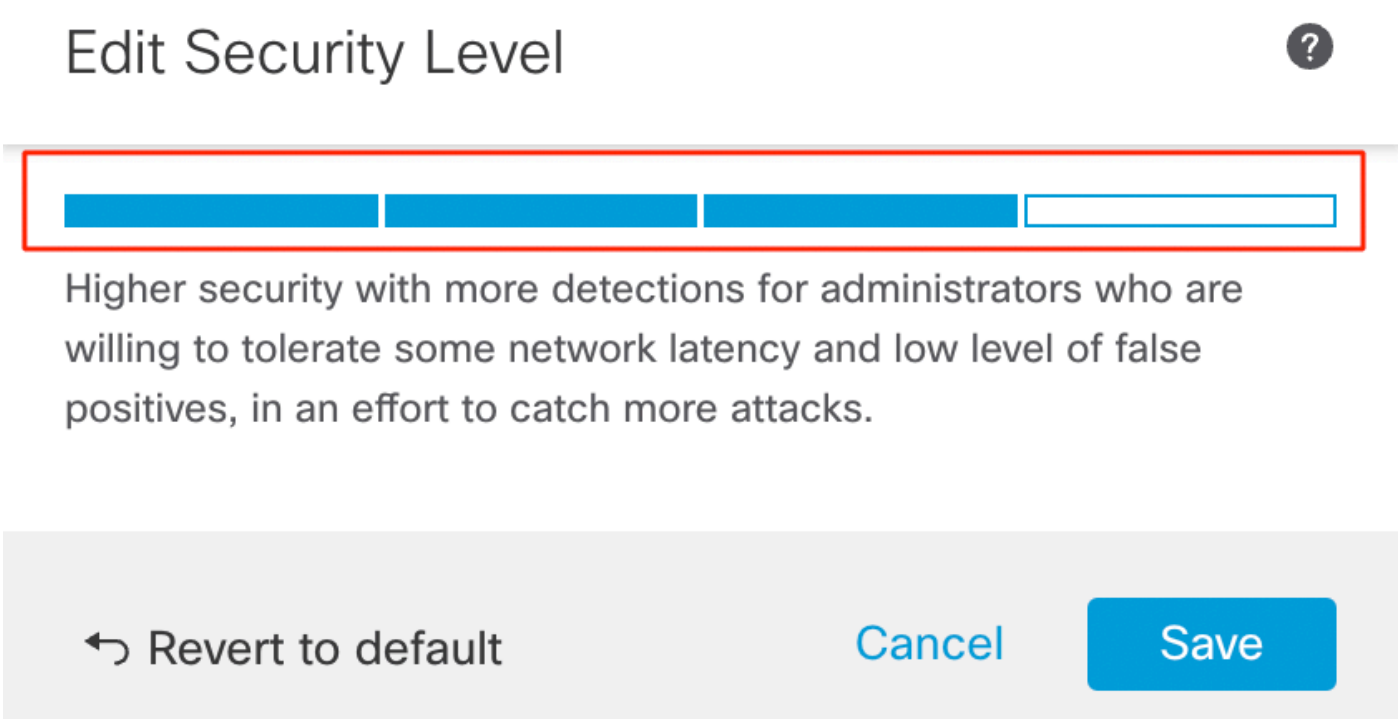


10. Clique em Edit ( ) próximo ao Nível de Segurança do grupo de regras para fazer alterações em massa no nível de segurança de todos os grupos de regras associados na Enterprisecategoria do grupo de regras.



Editar grupo de regras de segurança

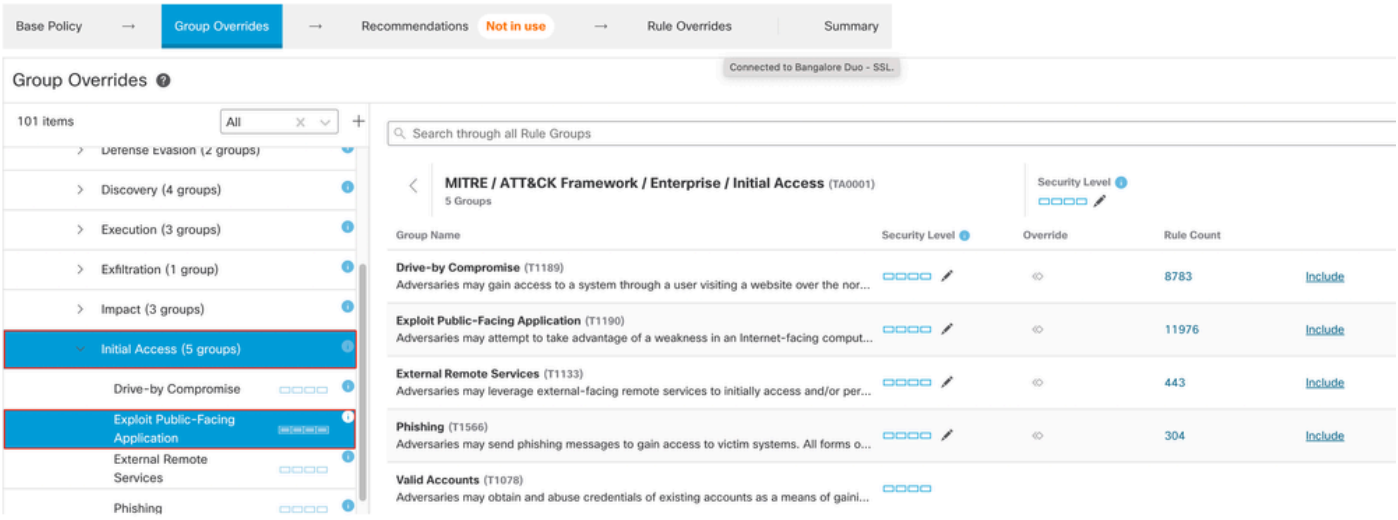
11. Por exemplo, escolha o nível de segurança 3 na Edit Security Level janela e clique em **Save**.



Nível de segurança

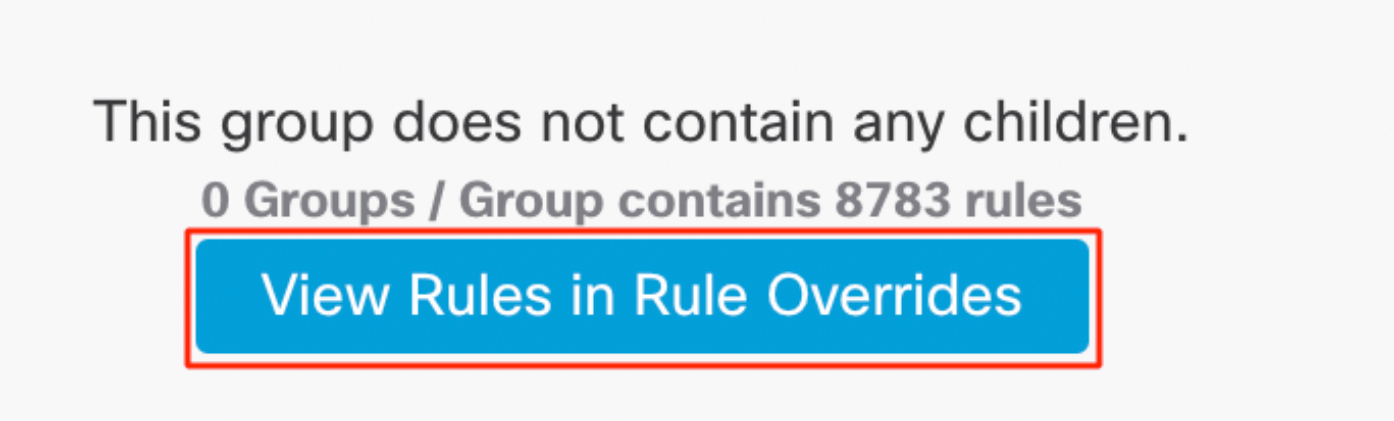
12. EmEnterprise, clique Initial Accesspara expandi-lo.

13. Em Initial Access, clique emExploit Public-Facing Application, que é o último grupo de folhas.



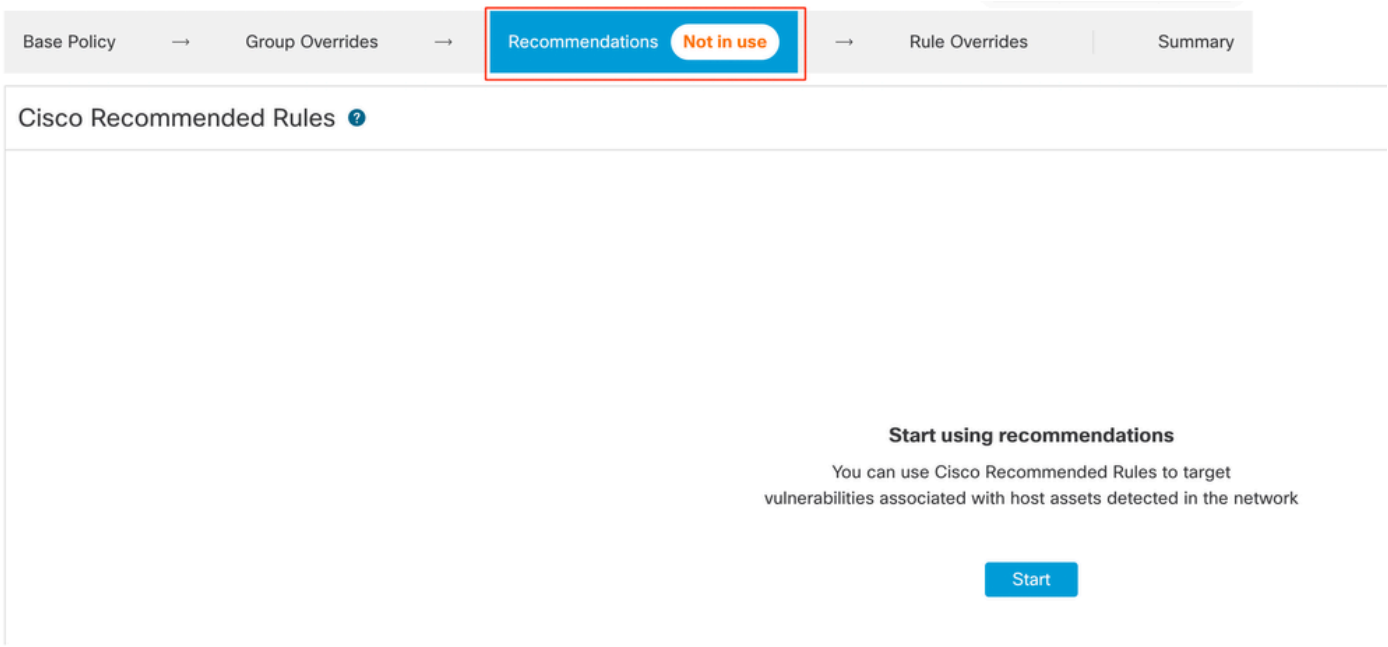
Grupo de acesso inicial

14. Clique no botão **View Rules in Rule Overrides**para exibir as diferentes regras, detalhes da regra, ações da regra etc. para as diferentes regras.

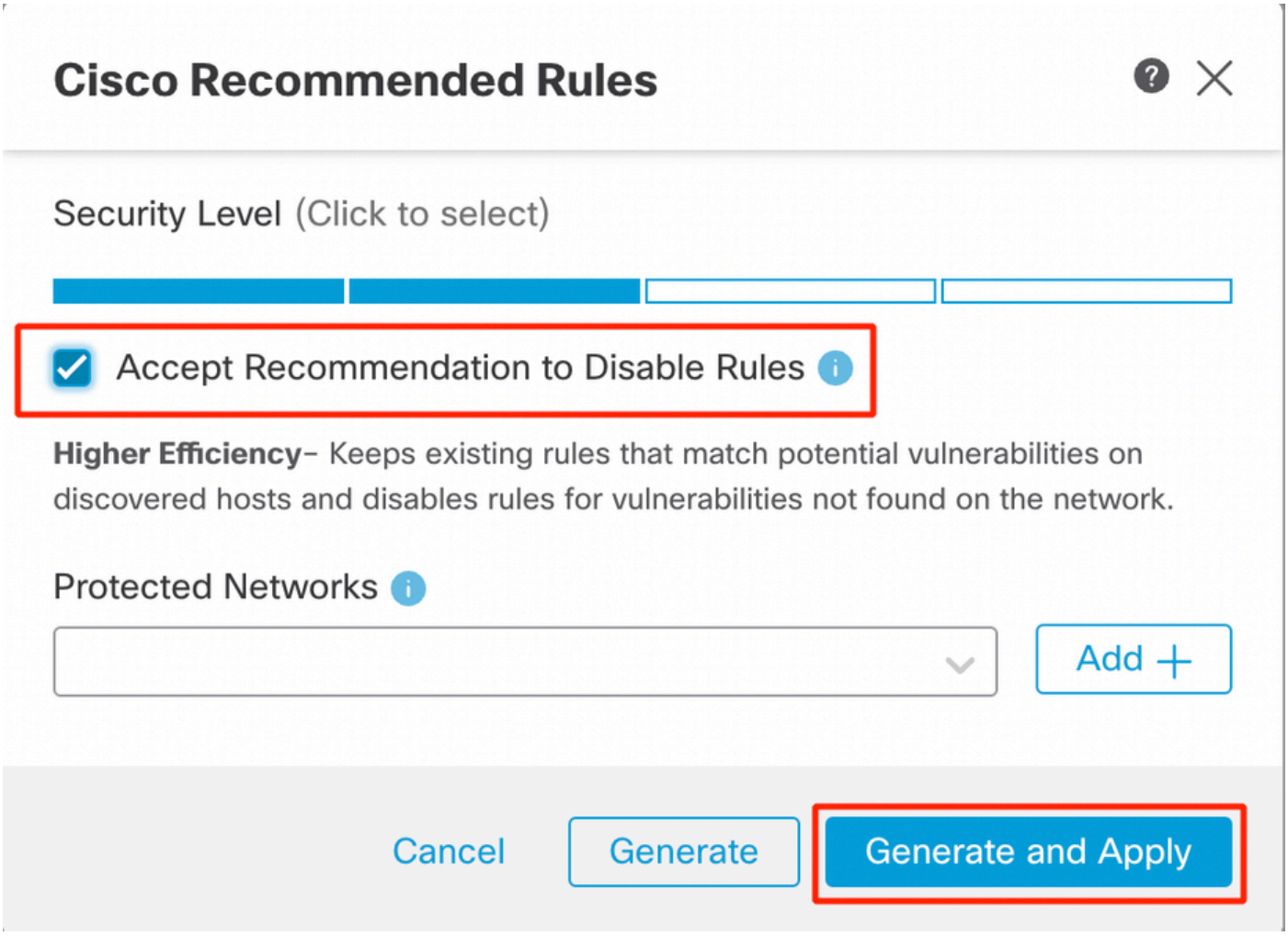


Regras em Substituições de Regra

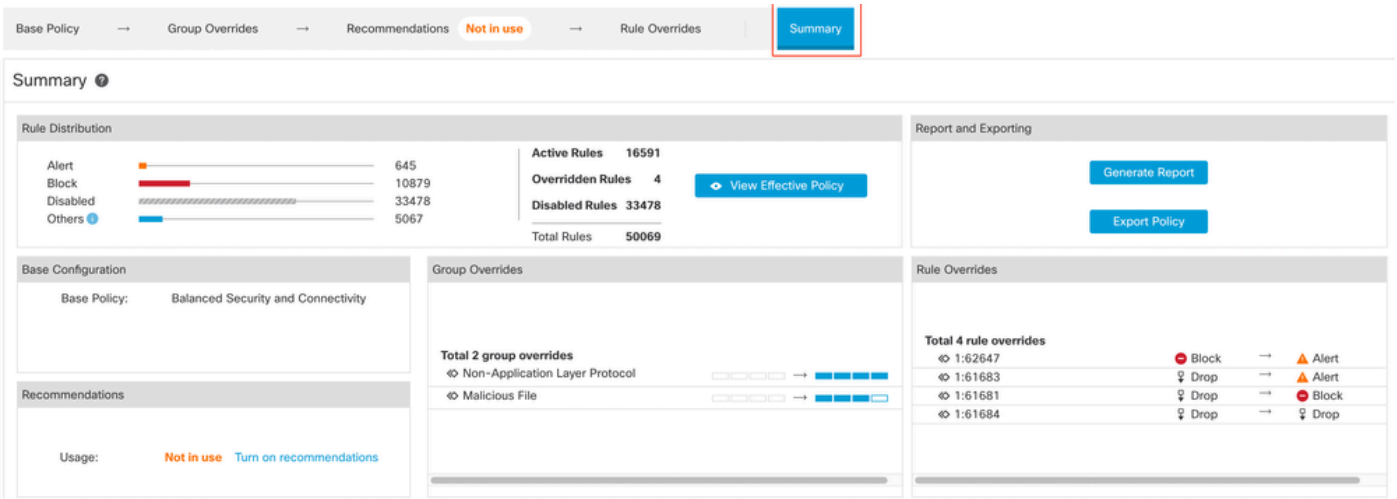
15. Clique no botão Recommendationse cliqueStartpara começar a usar as regras recomendadas pela Cisco. Você pode usar as recomendações de regras de intrusão para identificar vulnerabilidades associadas a ativos de host detectados na rede. Para obter mais informações.



Recomendações



16. Clique no botão Summarypara obter uma visão holística das alterações atuais na política. Você pode exibir a distribuição da regra da política, sobreposições de grupo, sobreposições de regra e assim por diante.



Resumo da política

Visualizar eventos de invasão

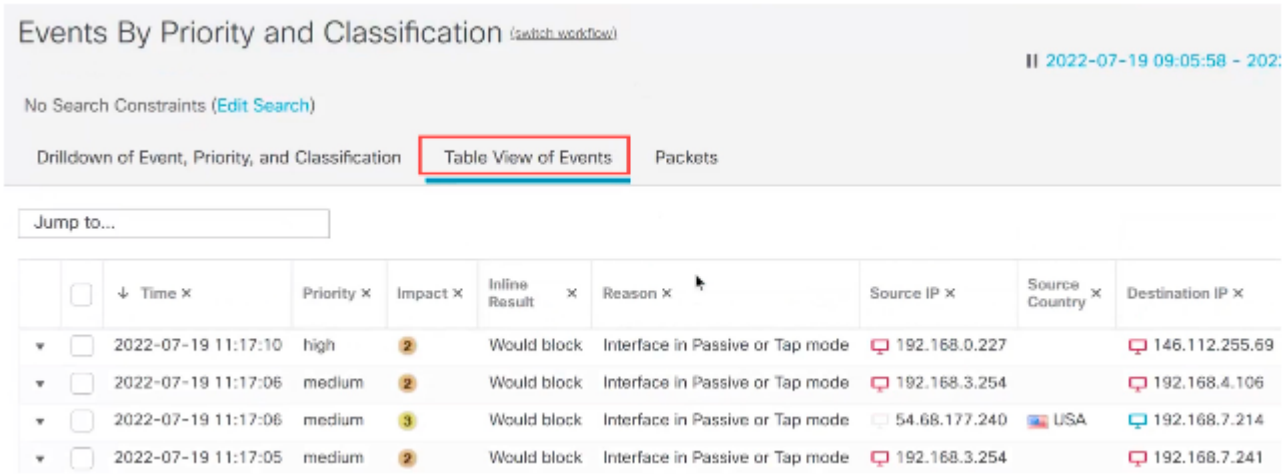
Você pode visualizar as técnicas MITER ATT&CK e os grupos de regras nos eventos de invasão no Visualizador de eventos clássico e no Visualizador de eventos unificado. O Talos fornece

mapeamentos de regras Snort (GID:SID) para técnicas MITER ATT&CK e grupos de regras. Esses mapeamentos são instalados como parte do LSP (Lightweight Security Package).

Antes de começar, as políticas de intrusão e controle de acesso devem ser implantadas para detectar e registrar eventos disparados pelas regras do Snort.

1. Clique em Analysis > Intrusions > Events.

2. Clique no botão **Table View of Events**conforme mostrado na imagem.



Events

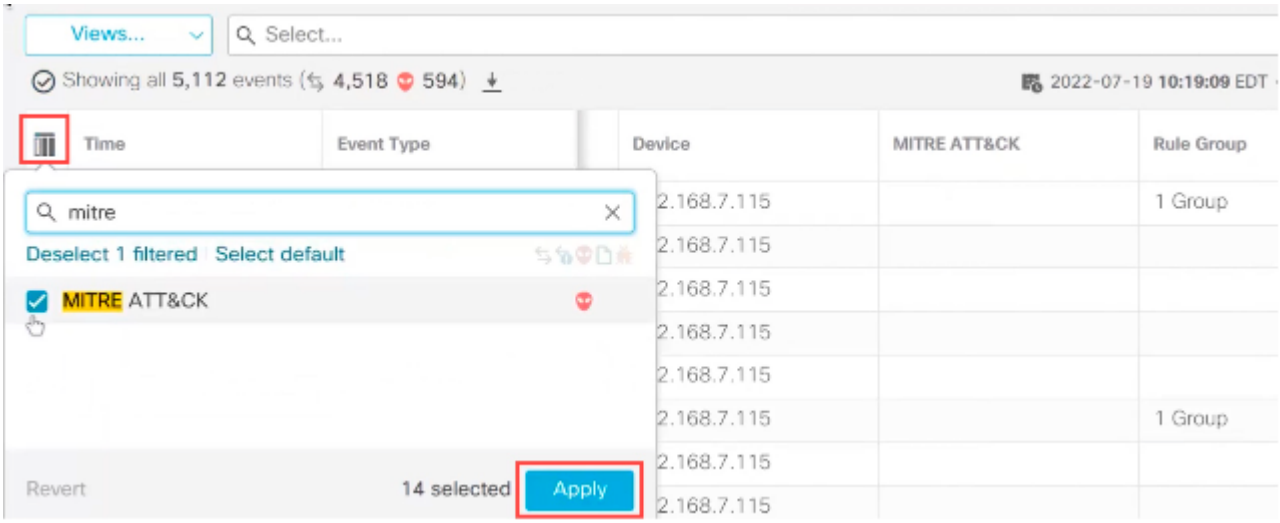
3. No MITRE ATT&CKcabeçalho da coluna, você poderá ver as técnicas para um evento de intrusão.

Cabeçalho de coluna central

4. Clique em 1 Techniquepara visualizar as Técnicas MITER ATT&CK, como mostrado na figura. Neste exemplo, Exploit Public-Facing Applicationé a técnica.

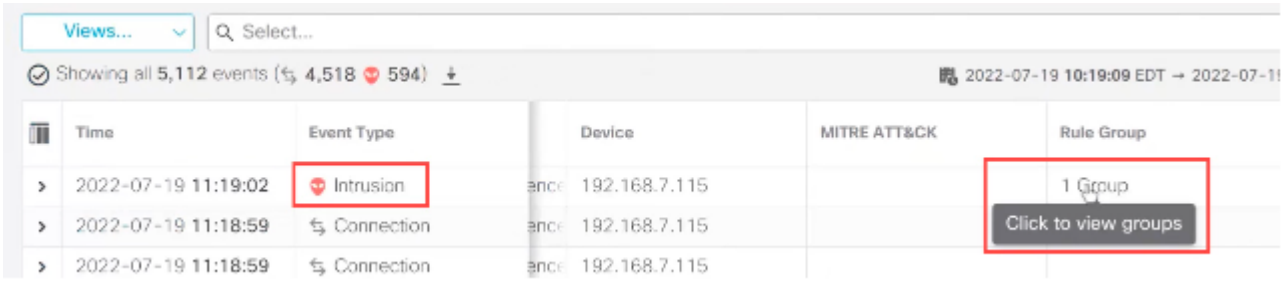
Técnicas de MITRA&TCK

5. Clique emClose.
6. Clique em Analysis > Unified Events.
7. Você pode clicar no ícone do seletor de colunas para ativar as colunas MITRE ATT&CKe Rule Group.



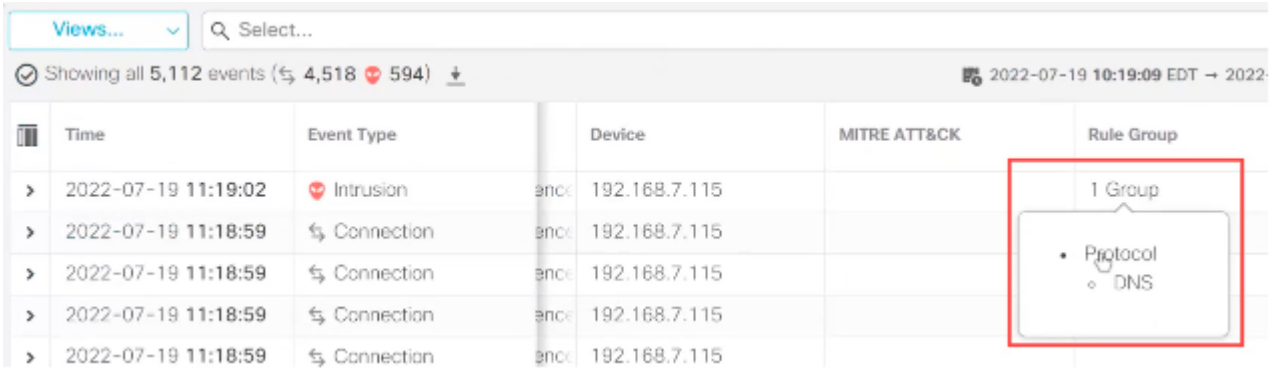
Ativar o ataque de mitre

8. Como mostrado no exemplo aqui, o evento de intrusão foi disparado por um evento mapeado para um grupo de regras. Clique 1 Group em Rule Groupcoluna.



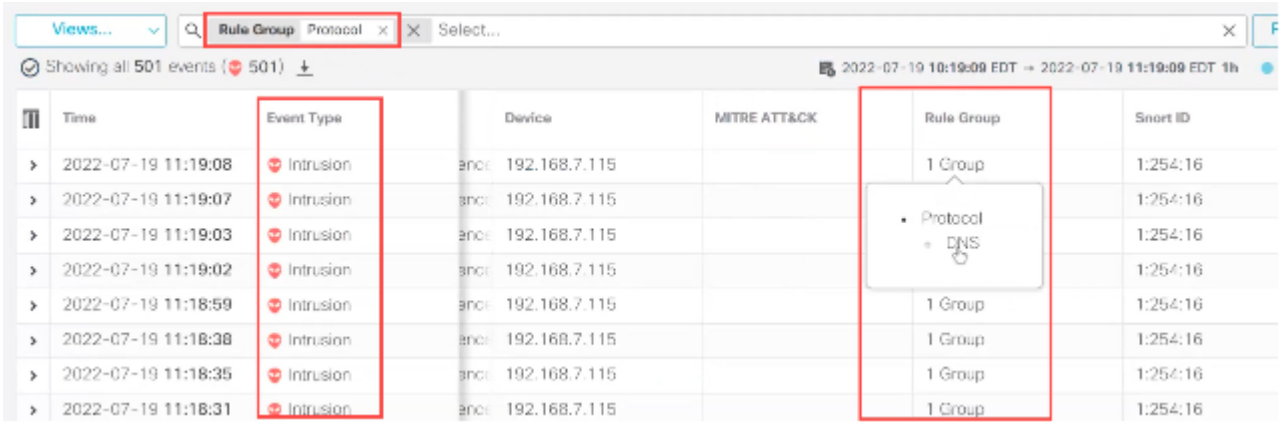
Grupo de regras

9. Por exemplo, você pode exibir o Protocolo, que é o grupo de regras pai, e o grupo de regras DNS abaixo dele.



Exibir protocolo

10. Você pode clicarProtocolpara procurar todos os eventos de intrusão que tenham pelo menos um grupo de regras, isto é, Protocol > DNS . Os resultados da pesquisa são exibidos, como mostrado no exemplo aqui.



Protocolo de grupo de regras

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.