

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

Contents

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Benefícios do MITER Framework](#)

[Visualize a estrutura MITER em sua política de intrusão](#)

[Visualizar eventos de invasão](#)

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 Policies** guia seja escolhida.
3. Clique em **Snort 3 Version** próximo à política de intrusão que deseja exibir ou editar. Feche o guia auxiliar do Snort que aparece.
4. Clique na **Group Overrides** camada.

A **Group Overrides** camada 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.

< Policies / Intrusion / MITRE_ATTACK

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description MITRE_ATTACK

Base Policy → **Group Overrides** → Recommendations **Not in use** → Rule Overrides | Summary

Group Overrides ?

2 items x v +

MITRE (1 group) 1

ATT&CK Framework (1 group) 1

Search through all Rule Groups

MITRE 1 Groups

Group Name Security Level

ATT&CK Framework mixed

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techn...

6. Nos termos `Group Overrides` do `All` é escolhido na lista suspensa, para que todos os grupos de regras da política de intrusão fiquem visíveis no painel esquerdo.

7. Clique em `MITRE` no 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.

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description test_policy

Base Policy → **Group Overrides** → Recommendations **Not in use** → Rule Overrides | Summary

Group Overrides ?

101 items x v +

MITRE (1 group) 1

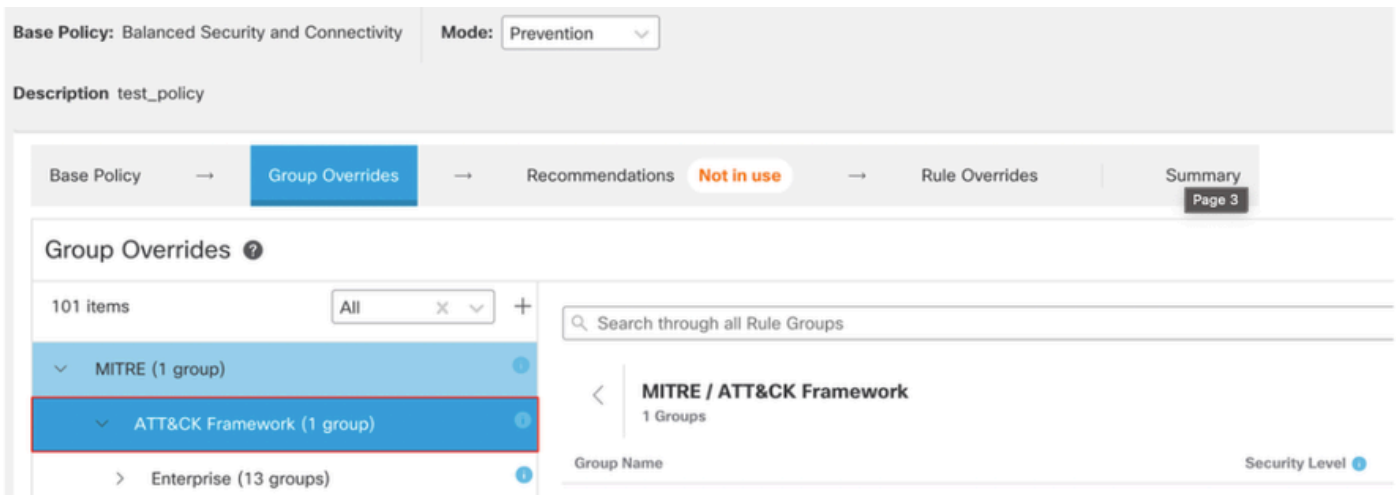
Rule Categories (9 groups) 1

Search through all Rule Groups

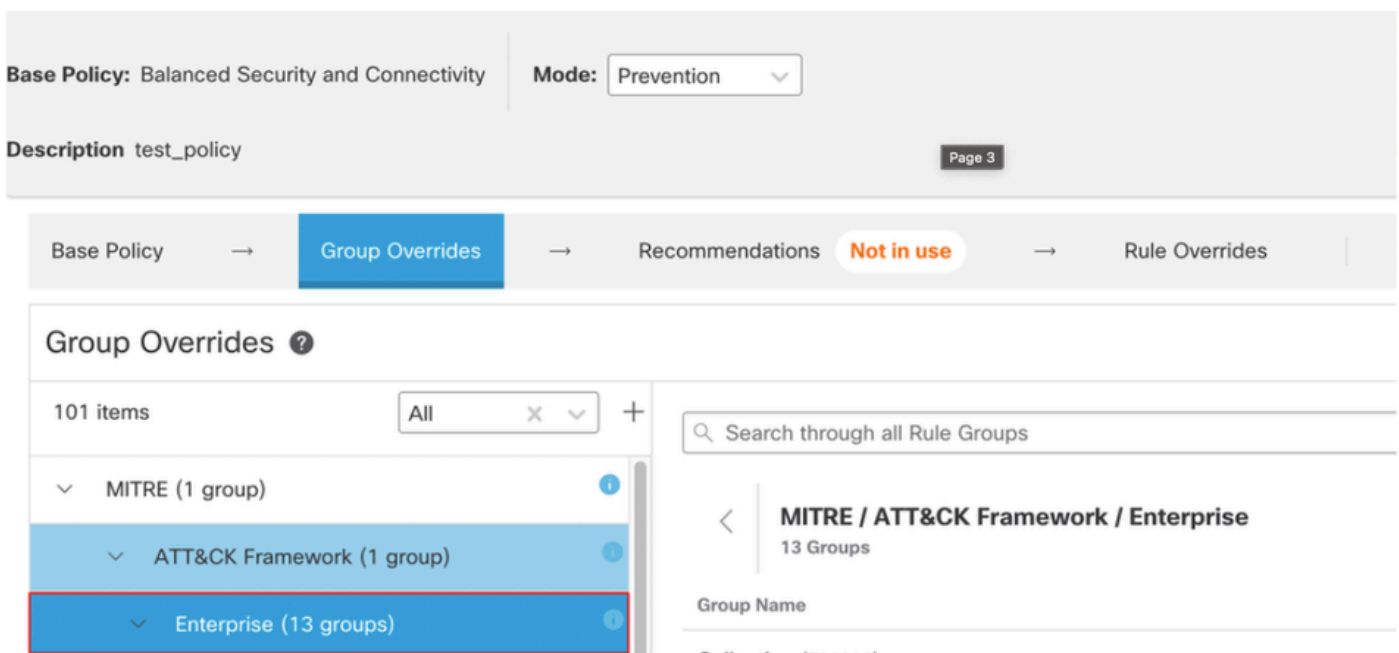
Rule Groups

To optimize intrusion policy configuration, you can configure the various rule group categories enable or disable groups and increase or decrease security levels, thus enriching intrusion eve

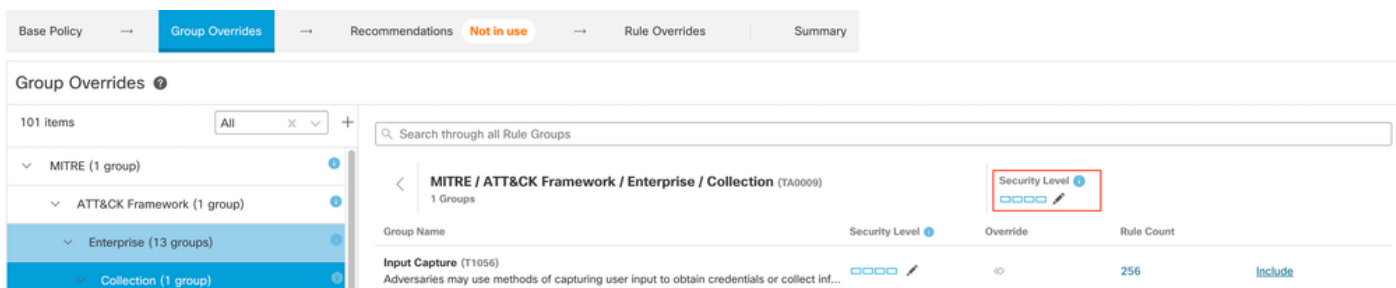
8. Em `MITRE`, clique em `ATT&CK Framework` para expandi-lo.



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 Enterprise categoria 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.

Edit Security Level



Higher security with more detections for administrators who are willing to tolerate some network latency and low level of false positives, in an effort to catch more attacks.

↶ Revert to default

Cancel

Save

Nível de segurança

12. Em Enterprise, clique **Initial Access** para expandi-lo.

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

The screenshot shows the 'Group Overrides' section of a security console. The breadcrumb trail is: Base Policy → Group Overrides → Recommendations (Not in use) → Rule Overrides → Summary. The 'Group Overrides' section shows a list of 101 items. The 'Initial Access' group (5 groups) is selected and expanded, showing sub-groups: Drive-by Compromise, Exploit Public-Facing Application, External Remote Services, and Phishing. The 'Exploit Public-Facing Application' group is highlighted. The right pane shows details for the 'MITRE / ATT&CK Framework / Enterprise / Initial Access (TA0001)' group, listing rules with their security levels, override status, and rule counts.

Group Name	Security Level	Override	Rule Count	
Drive-by Compromise (T1189) Adversaries may gain access to a system through a user visiting a website over the nor...	○○○○	⊖	8783	Include
Exploit Public-Facing Application (T1190) Adversaries may attempt to take advantage of a weakness in an Internet-facing comput...	○○○○	⊖	11976	Include
External Remote Services (T1133) Adversaries may leverage external-facing remote services to initially access and/or per...	○○○○	⊖	443	Include
Phishing (T1566) Adversaries may send phishing messages to gain access to victim systems. All forms o...	○○○○	⊖	304	Include
Valid Accounts (T1078) Adversaries may obtain and abuse credentials of existing accounts as a means of gaini...	○○○○			

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.

This group does not contain any children.

0 Groups / Group contains 8783 rules

[View Rules in Rule Overrides](#)

Regras em Substituições de Regra

15. Clique no botão **Recommendations** e clique **Start** para 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.

Base Policy → Group Overrides → **Recommendations** Not in use → Rule Overrides | Summary

Cisco Recommended Rules ⓘ

Start using recommendations

You can use Cisco Recommended Rules to target vulnerabilities associated with host assets detected in the network

[Start](#)

Recomendações

Cisco Recommended Rules



Security Level (Click to select)

Accept Recommendation to Disable Rules

Higher Efficiency– Keeps existing rules that match potential vulnerabilities on discovered hosts and disables rules for vulnerabilities not found on the network.

Protected Networks

Add +

Cancel

Generate

Generate and Apply

16. Clique no botão **Summary** para 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.

Base Policy → Group Overrides → Recommendations **Not in use** → Rule Overrides | **Summary**

Summary

Rule Distribution

Alert	645
Block	10879
Disabled	33478
Others	5067

Active Rules 16591
Overridden Rules 4 [View Effective Policy](#)
Disabled Rules 33478
Total Rules 50069

Report and Exporting

[Generate Report](#)
[Export Policy](#)

Base Configuration

Base Policy: Balanced Security and Connectivity

Recommendations

Usage: **Not in use** [Turn on recommendations](#)

Group Overrides

Total 2 group overrides

- Non-Application Layer Protocol
- Malicious File

Rule Overrides

Total 4 rule overrides

1:62647	Block	→	Alert
1:61683	Drop	→	Alert
1:61681	Drop	→	Block
1:61684	Drop	→	Drop

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 By Priority and Classification (switch workflow) || 2022-07-19 09:05:58 - 202

No Search Constraints (Edit Search)

Drilldown of Event, Priority, and Classification Table View of Events Packets

Jump to...

	Time ×	Priority ×	Impact ×	Inline Result ×	Reason ×	Source IP ×	Source Country ×	Destination IP ×
▼	2022-07-19 11:17:10	high	2	Would block	Interface in Passive or Tap mode	192.168.0.227		146.112.255.69
▼	2022-07-19 11:17:06	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.4.106
▼	2022-07-19 11:17:06	medium	3	Would block	Interface in Passive or Tap mode	54.68.177.240	USA	192.168.7.214
▼	2022-07-19 11:17:05	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.7.241

Events

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

Access Control Policy ×	Access Control Rule ×	Network Analysis Policy ×	MITRE ATT&CK ×	Rule Group ×
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

Cabeçalho de coluna central

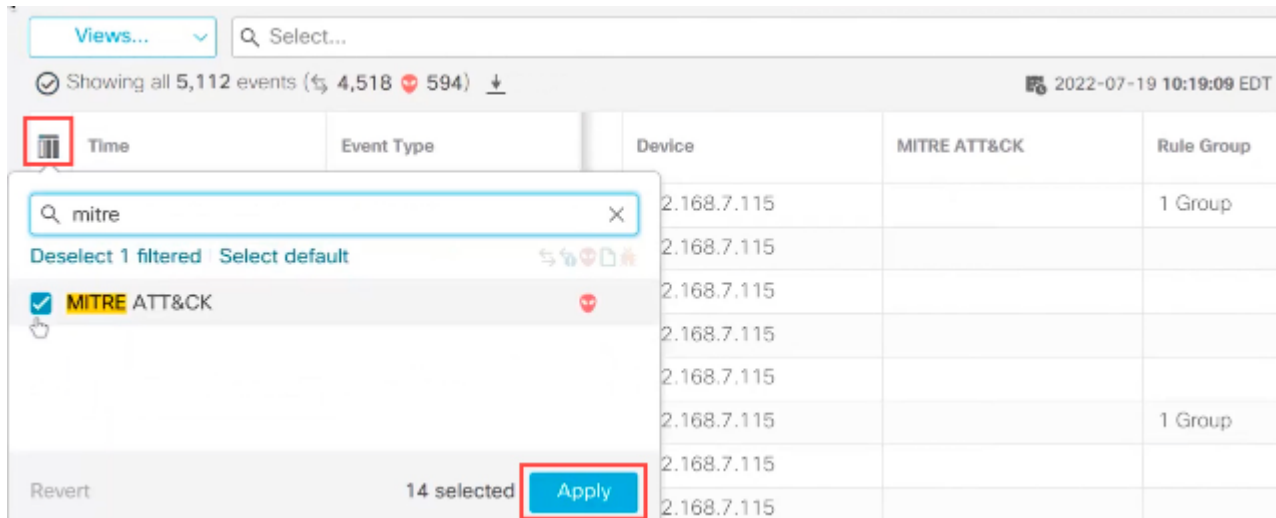
4. Clique em **1 Technique** para visualizar as Técnicas MITER ATT&CK, como mostrado na figura. Neste exemplo, **Exploit Public-Facing Application** é a técnica.

MITRE ATT&CK Techniques

- Enterprise
 - Initial Access
 - Exploit Public-Facing Application

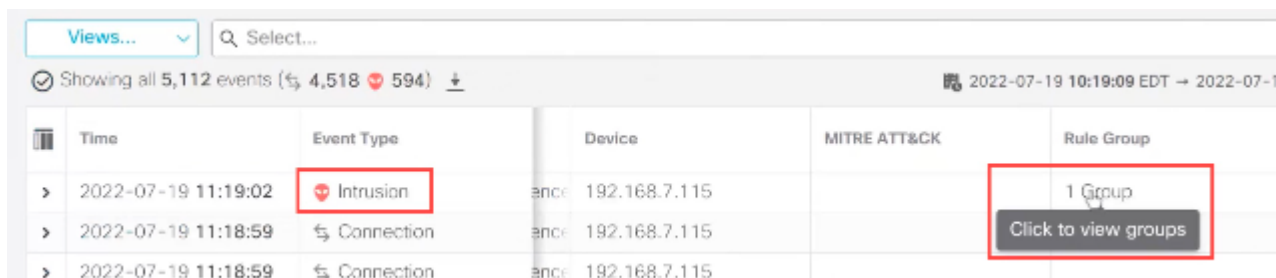
Close

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



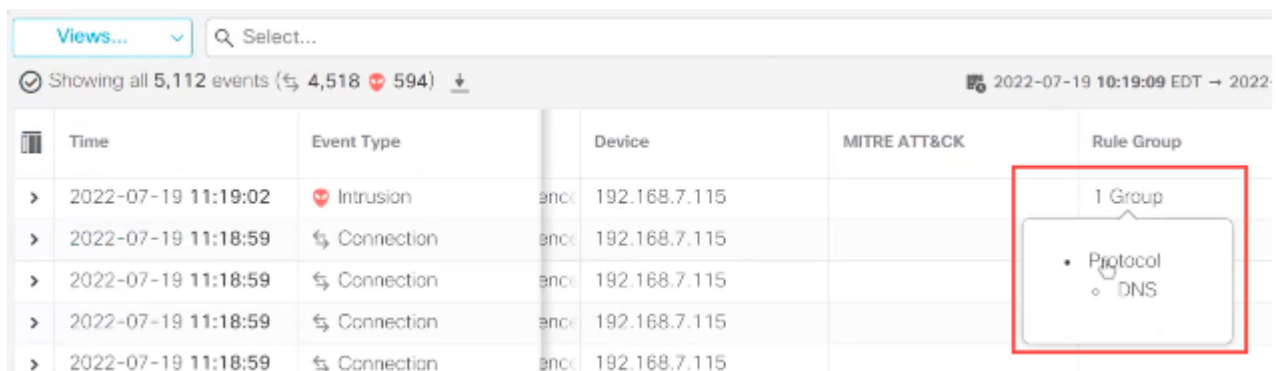
Ativar o ataque de mitre

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 Group** coluna.



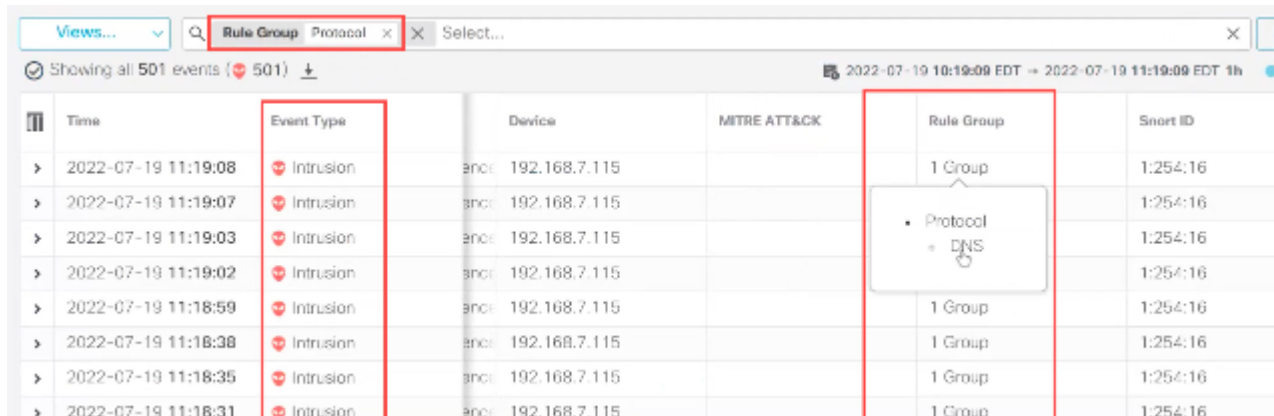
Grupo de regras

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 clicar Protocolo para 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.



The screenshot shows a security event viewer interface with a search filter 'Protocol > DNS' applied. The table displays several intrusion events. A dropdown menu is open over the 'Rule Group' column, showing 'Protocol > DNS' selected.

Time	Event Type	Device	MITRE ATT&CK	Rule Group	Smart ID
2022-07-19 11:19:08	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:07	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:03	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:02	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:59	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:38	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:35	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:31	Intrusion	enc: 192.168.7.115		1 Group	1:254:16

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.