Use the MITRE Framework to View and Act on Potential Threats in Secure FMC

Contents

Introduction

This document describes how to use the MITRE framework to view and act on potential threats in a secure Firepower Management Center (FMC).

Background Information

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework is an extensive knowledge base and methodology that provides insights into the tactics, techniques, and procedures (TTPs) distributed by threat actors aiming to harm systems. ATT&CK is compiled into matrices that each represent operating systems or a particular platform. Each stage of an attack, known as "tactics", is mapped to the specific methods used to achieve those stages, known as "techniques".

Each technique in the ATT&CK framework is accompanied by information about the technique, associated procedures, probable defences and detections, and real-world examples. The MITRE ATT&CK framework also incorporates Groups to refer to threat groups, activity groups, or threat actors based on the set of tactics and techniques they employ. By using Groups, the framework helps categorize and document behaviors.

For more information about MITRE Please refer https://attack.mitre.org.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Snort
- Secure FMC
- Secure Firepower Threat Defense (FTD)

Components Used

The information in this document is based on these software and hardware versions:

- This document applies to all Firepower platforms
- Secure FTD running software version 7.3.0
- Secure Firepower Management Center Virtual (FMC) running software version 7.3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Benefits of MITRE Framework

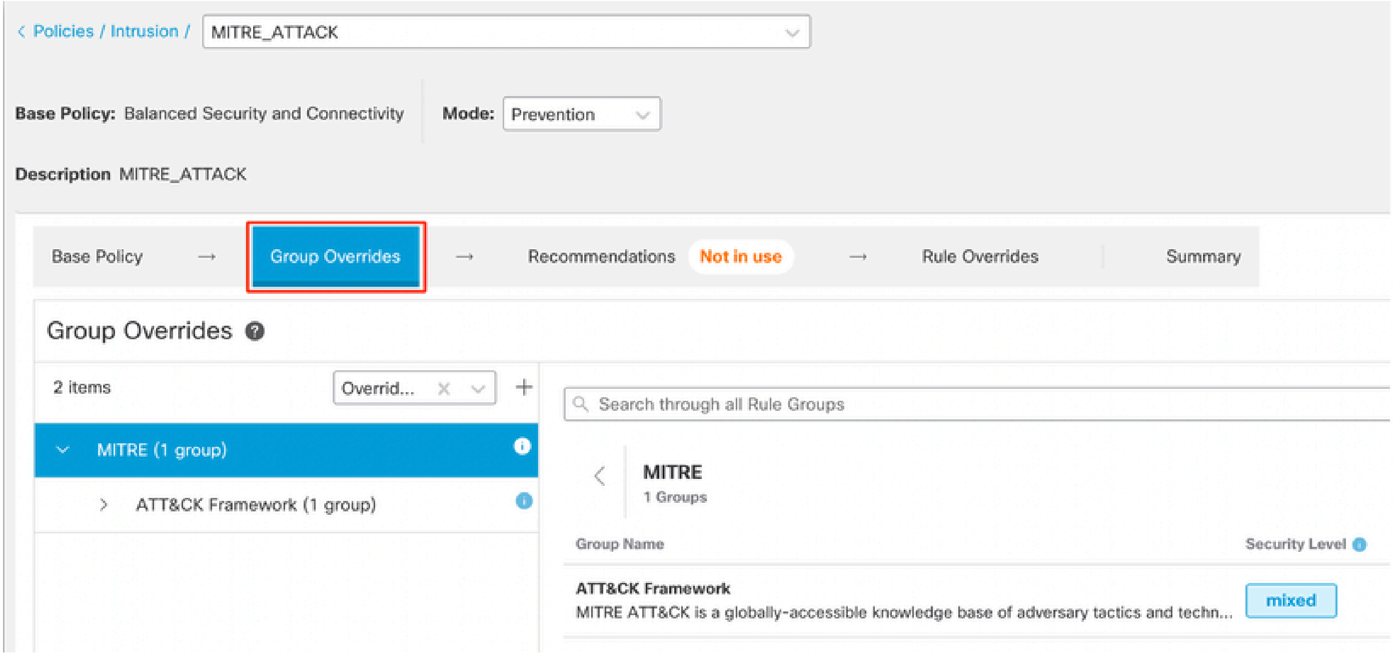
- MITRE Tactics, Techniques, and Procedures (TTPs) are added to intrusion events that enable administrators to act on traffic based on the MITRE ATT&CK (Adversary Tactics Techniques and Common Knowledge) framework. This enables administrators to view and handle traffic with more granularity, and they can group rules by vulnerability type, target system, or threat category.
- You can organize intrusion rules according to the MITRE ATT&CK framework. This allows you to customize policies according to specific attacker tactics and techniques.

View the MITRE Framework in your Intrusion Policy

The MITRE framework enables you to navigate through your intrusion rules. MITRE is just another category of rule groups and is part of the Talos rule groups. Rule navigation for several levels of rule groups is supported which provides more flexibility and logical grouping of rules.

1. Choose Policies > Intrusion.
2. Ensure that the Intrusion Policiestab is chosen.
3. Click Snort 3 Versionnext to the intrusion policy you want to view or edit. Close the Snort helper guide that pops up.
4. Click the Group Overrideslayer.

The Group Overrideslayer lists all the categories of rule groups in a hierarchical structure. You can traverse to the last leaf rule group in each rule group.



< Policies / Intrusion / MITRE_ATTACK

Base Policy: Balanced Security and Connectivity **Mode:** Prevention

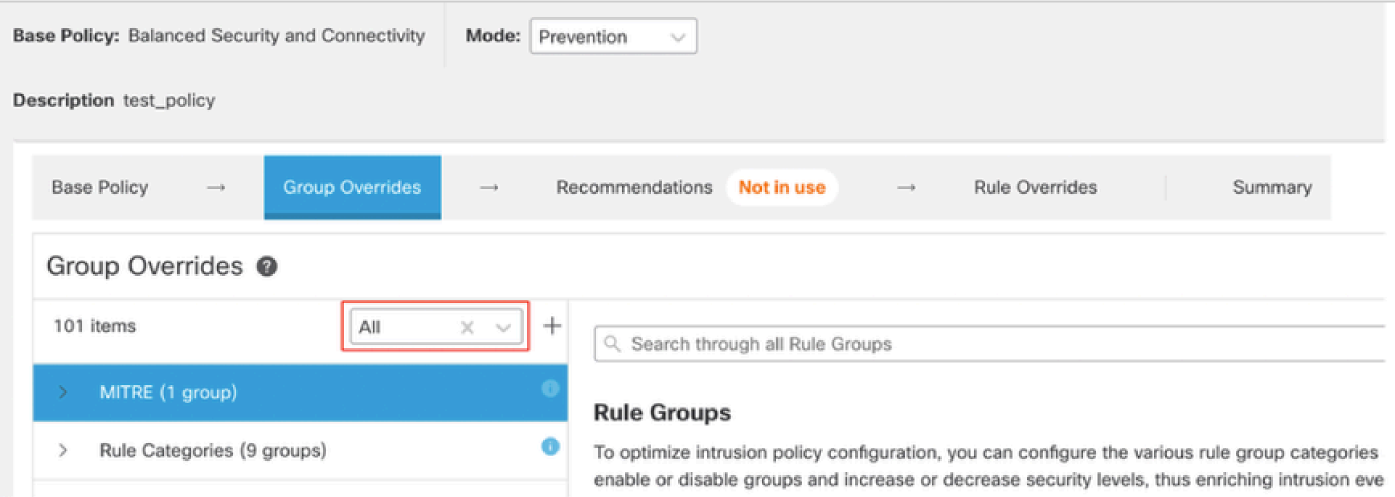
Description MITRE_ATTACK

Group Name	Security Level
ATT&CK Framework MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techn...	mixed

6. Under Group Overrides, ensure that Allis chosen in the drop-down list, so that all the rule groups for the intrusion policy are visible in the left pane.

7. Click MITREin the left pane.

Note: For this example, MITRE is selected, but depending on your specific requirements, you can choose the Rule Categories rule group or any other rule group and subsequent rule groups under it. All the rule groups use the MITRE framework.



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 All

MITRE (1 group)

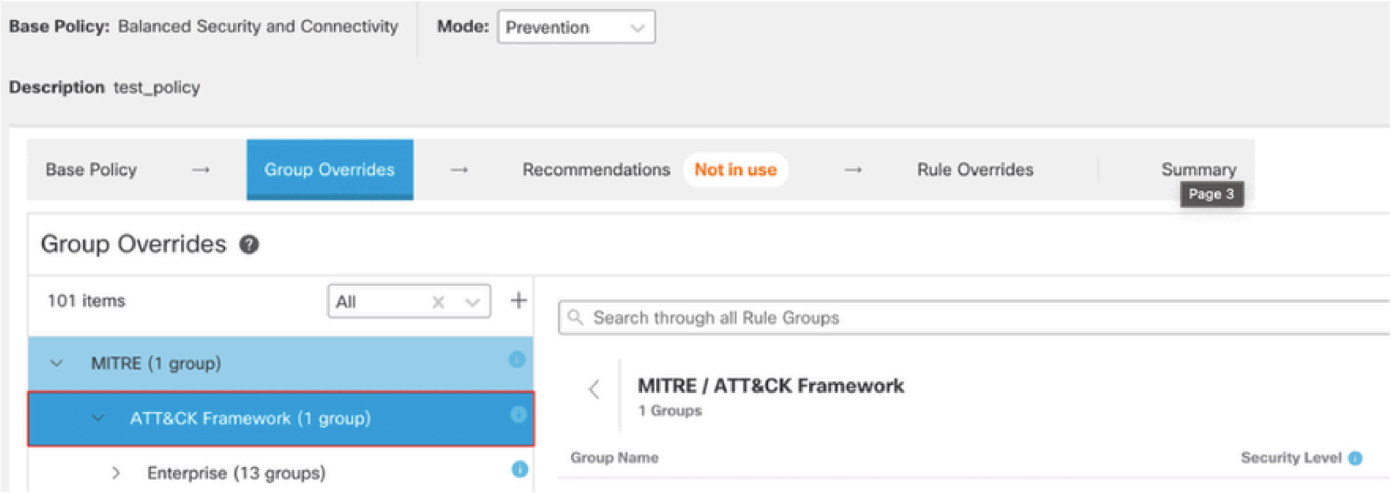
Rule Categories (9 groups)

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

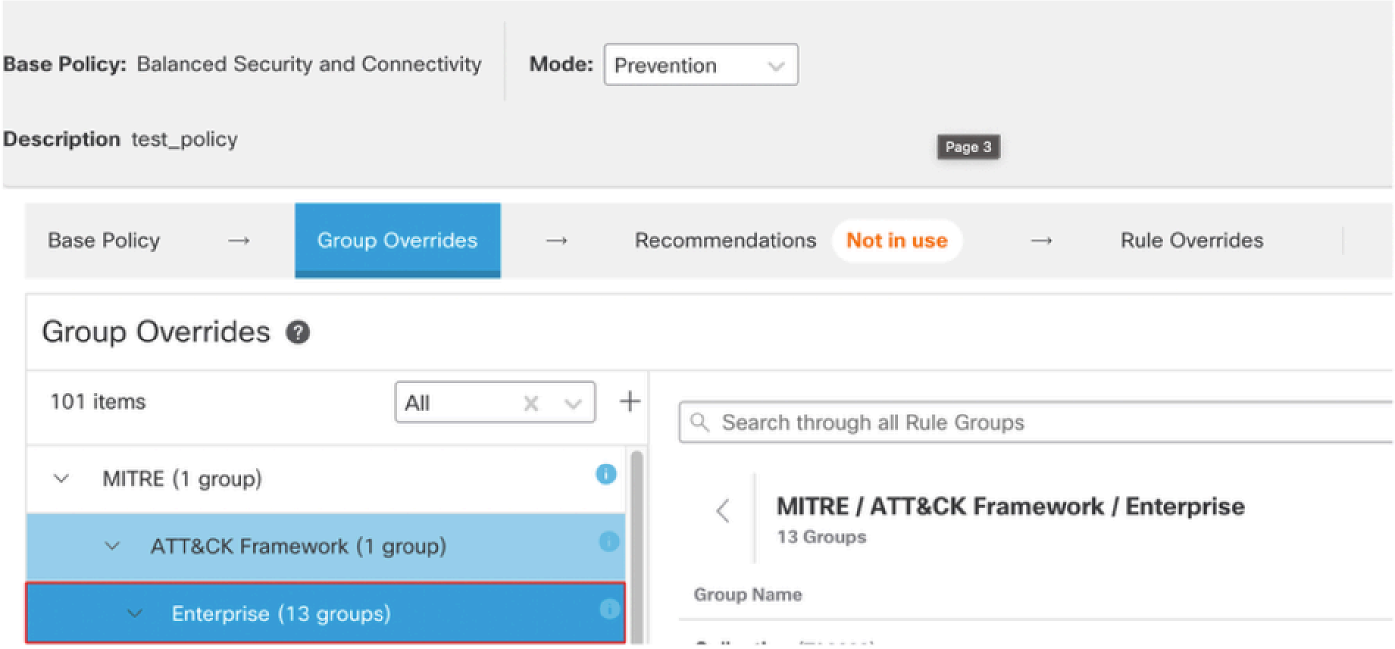
8. Under MITRE, click ATT&CK Framework to expand it.


Base Policy: Balanced Security and Connectivity

Mode: Prevention

Description test_policy

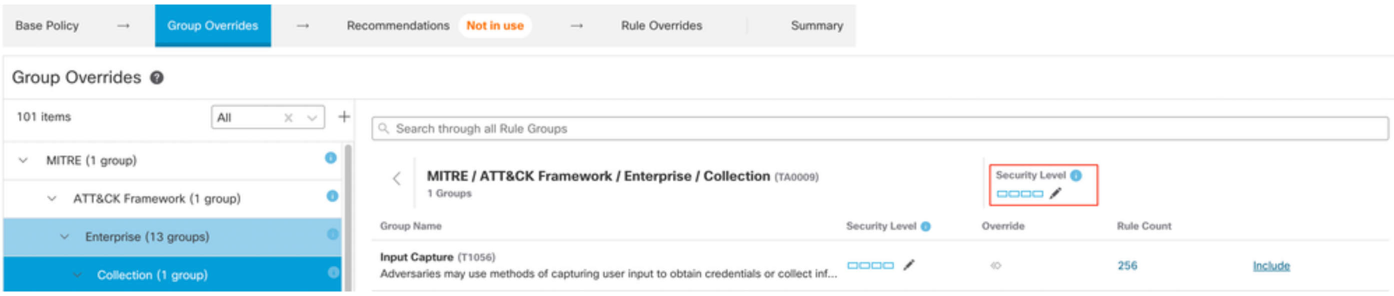
9. Under ATT&CK Framework, click Enterprise to expand it.


Base Policy: Balanced Security and Connectivity

Mode: Prevention

Description test_policy

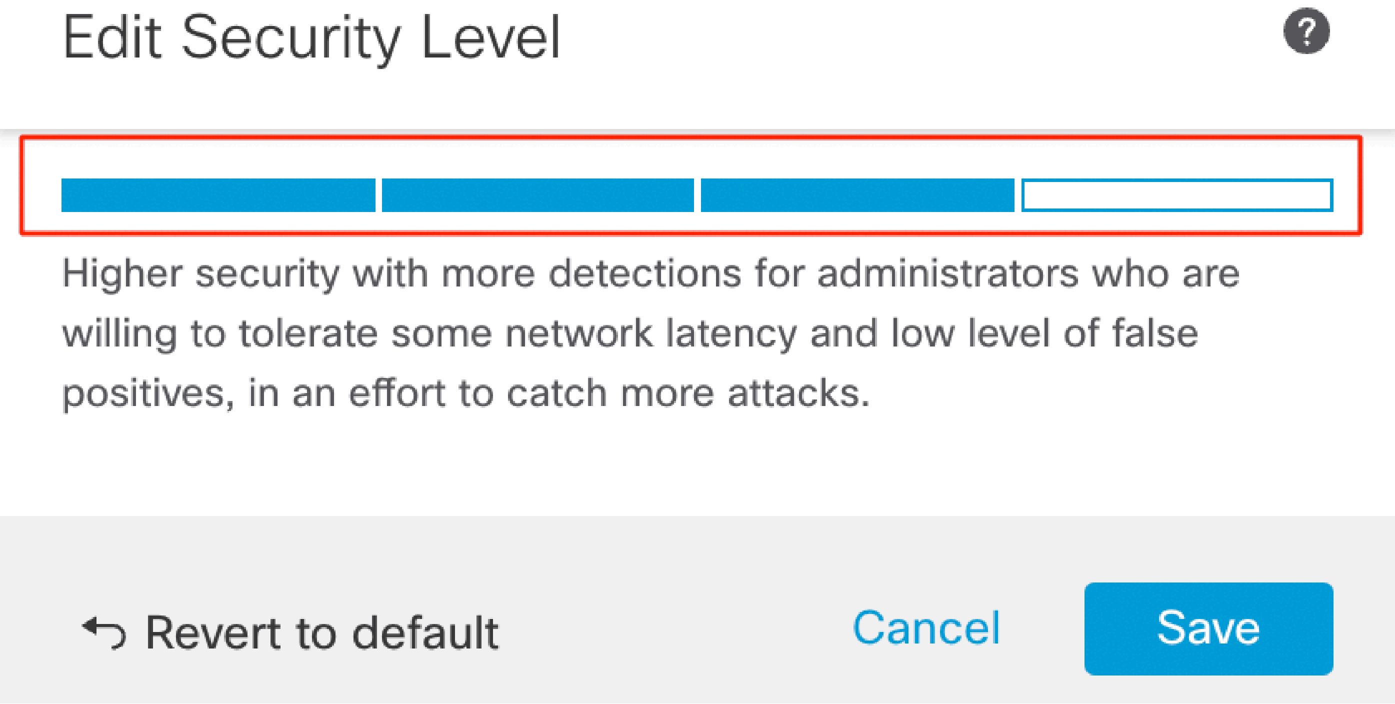
10. Click Edit ( ) next to the Security Level of the rule group to make bulk changes to the security level for all the associated rule groups under the Enterpriserule group category.



Group Name	Security Level	Override	Rule Count	
Input Capture (T1056) Adversaries may use methods of capturing user input to obtain credentials or collect inf...	□□□□		256	Include

Edit security rule group

11. As an example, choose security level 3 in the Edit Security Level window and click **Save.**



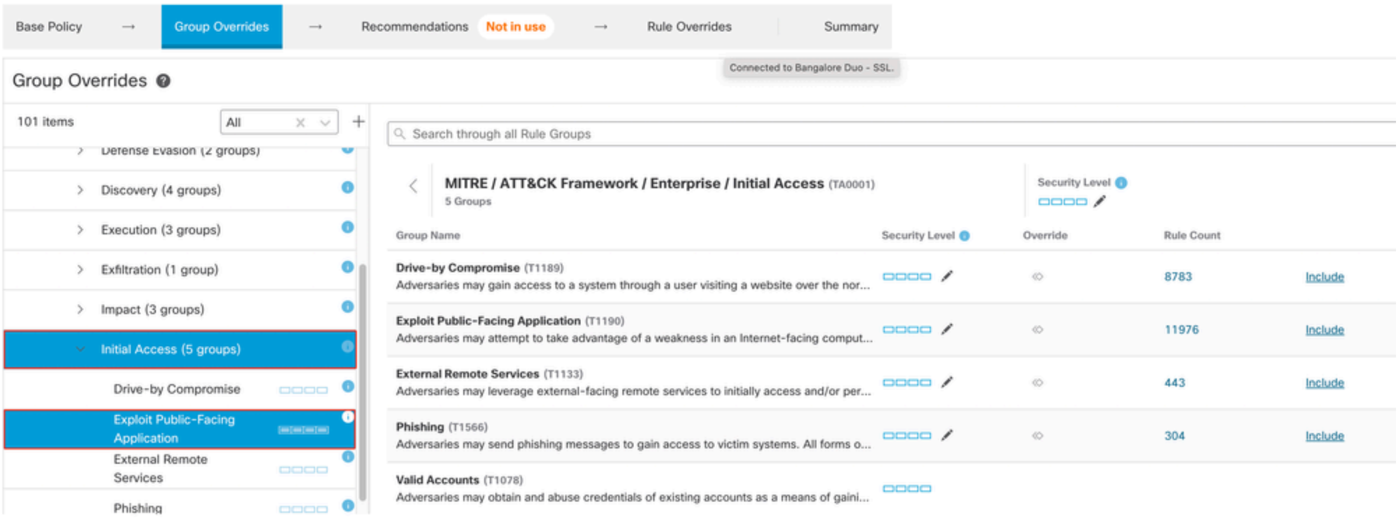
Edit Security Level

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.

Security level

12. Under Enterprise, click Initial Accessto expand it.

13. Under Initial Access, click Exploit Public-Facing Application, which is the last leaf group.



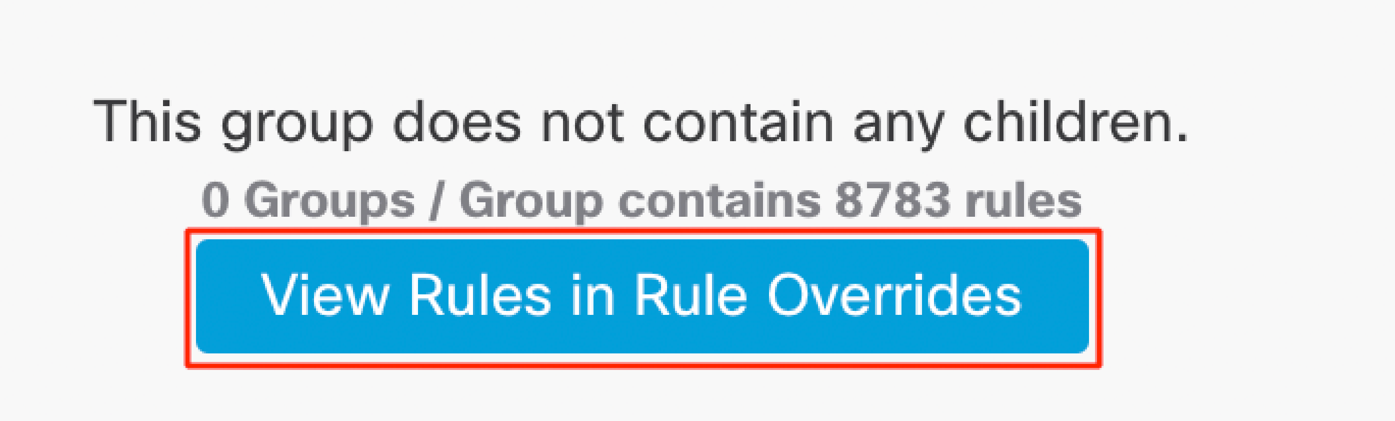
MITRE / ATT&CK Framework / Enterprise / Initial Access (TA0001)
5 Groups

Security Level

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...	□□□□			

Initial access group

14. Click the **View Rules in Rule Overrides**button to view the different rules, rule details, rule actions, and so on for the different rules.

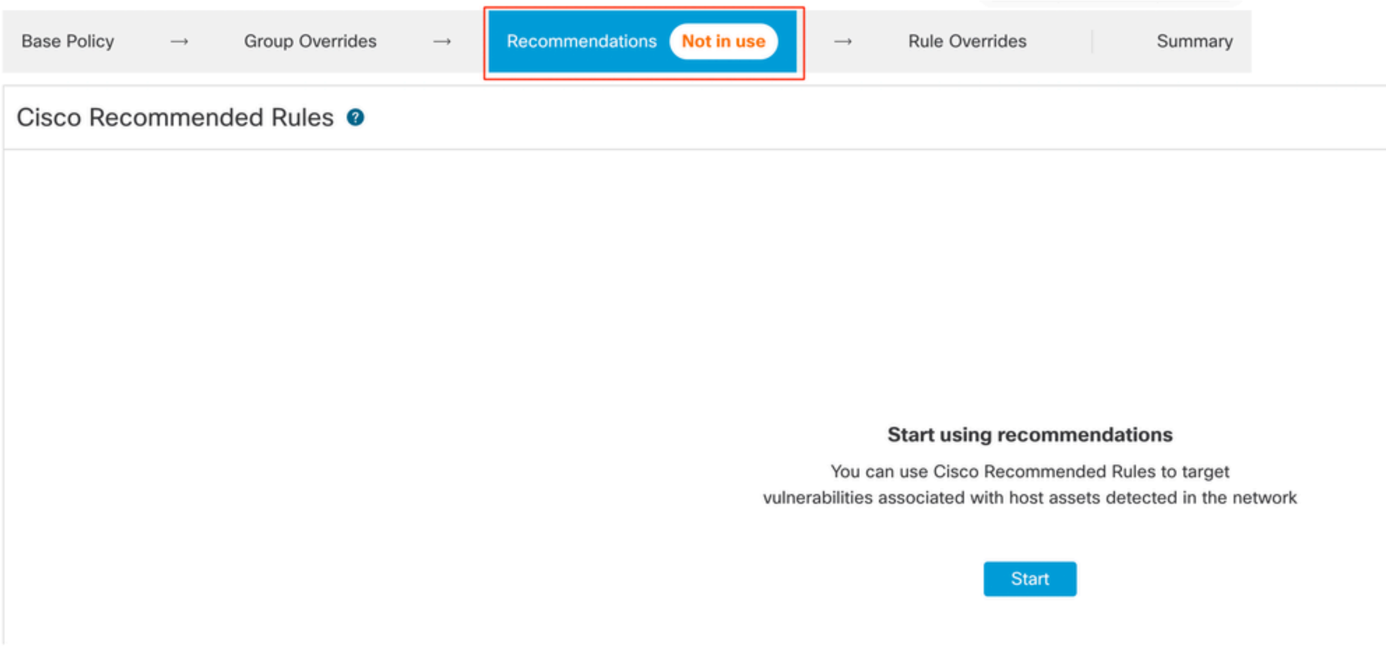


This group does not contain any children.

0 Groups / Group contains 8783 rules

Rules in Rule Overrides

15. Click the Recommendationslayer and then click Start to start using Cisco-recommended rules. You can use the intrusion rule recommendations to target vulnerabilities associated with host assets detected in the network. For more information.

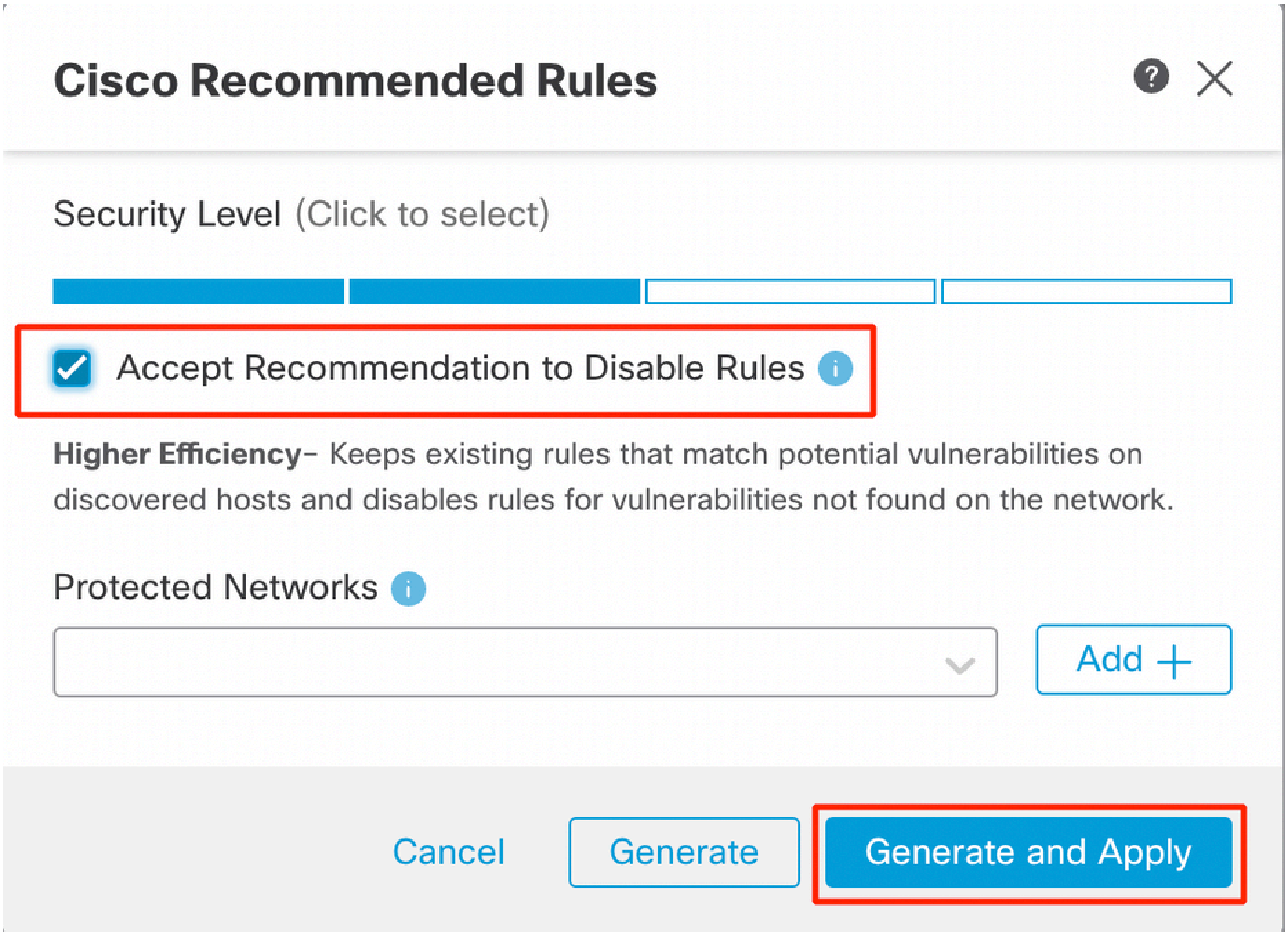


Cisco Recommended Rules

Start using recommendations

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

Recommendations



Cisco Recommended Rules

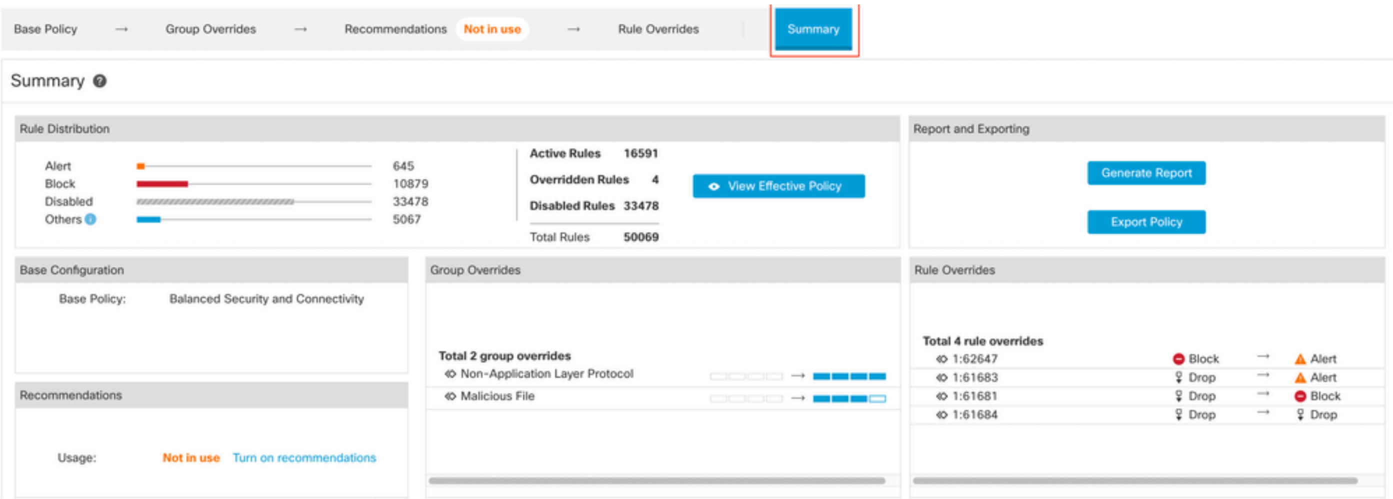
Security Level (Click to select)

☑ 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

16. Click the Summarylayer for a holistic view of the current changes to the policy. You can view the rule distribution of the policy, group overrides, rule overrides, and so on.



Summary

Rule Distribution

Alert	645
Block	10879
Disabled	33478
Others	5067

Active Rules	16591
Overridden Rules	4
Disabled Rules	33478
Total Rules	50069

Report and Exporting

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

Policy summary

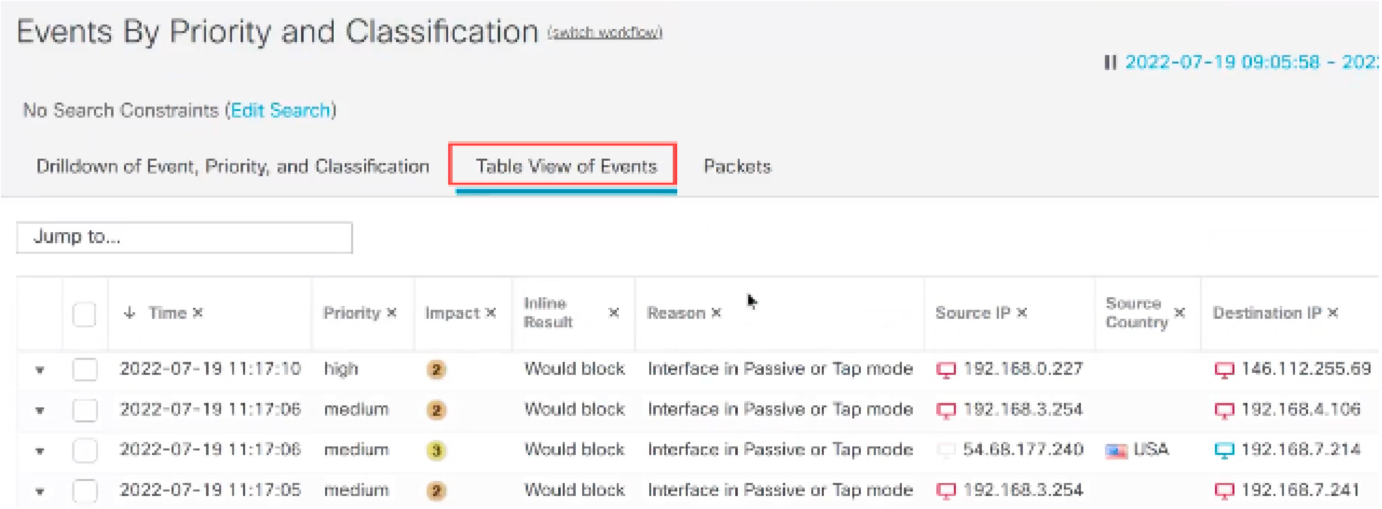
View Intrusion Events

You can view the MITRE ATT&CK techniques and rule groups in the intrusion events in the Classic Event Viewer and Unified Event Viewer. Talos provides mappings from Snort rules (GID:SID) to MITRE ATT&CK techniques and rule groups. These mappings are installed as part of the Lightweight Security Package (LSP).

Before you begin, Intrusion and access control policies must be deployed to detect and log events triggered by Snort rules.

1. Click Analysis > Intrusions > Events.

2. Click the **Table View of Events**tab as shown in the image.



Events By Priority and Classification (switch workflow)

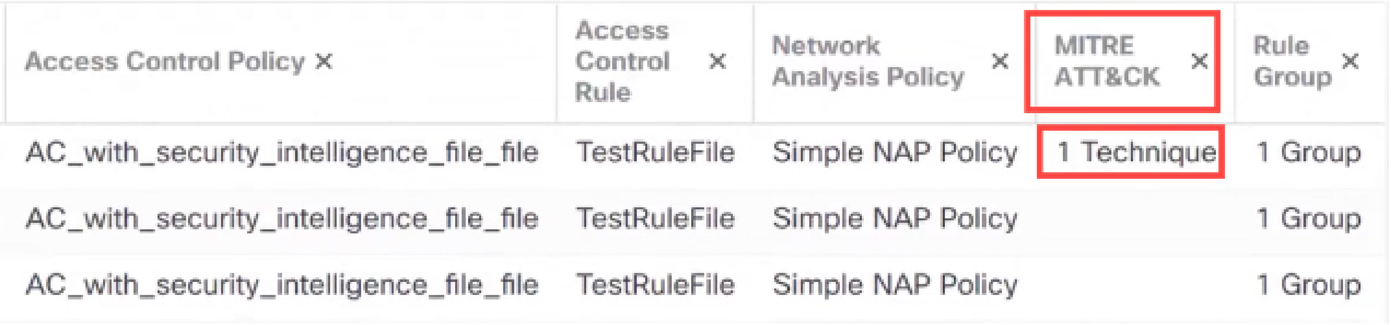
II 2022-07-19 09:05:58 - 202

No Search Constraints (Edit Search)

	□	↓ 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

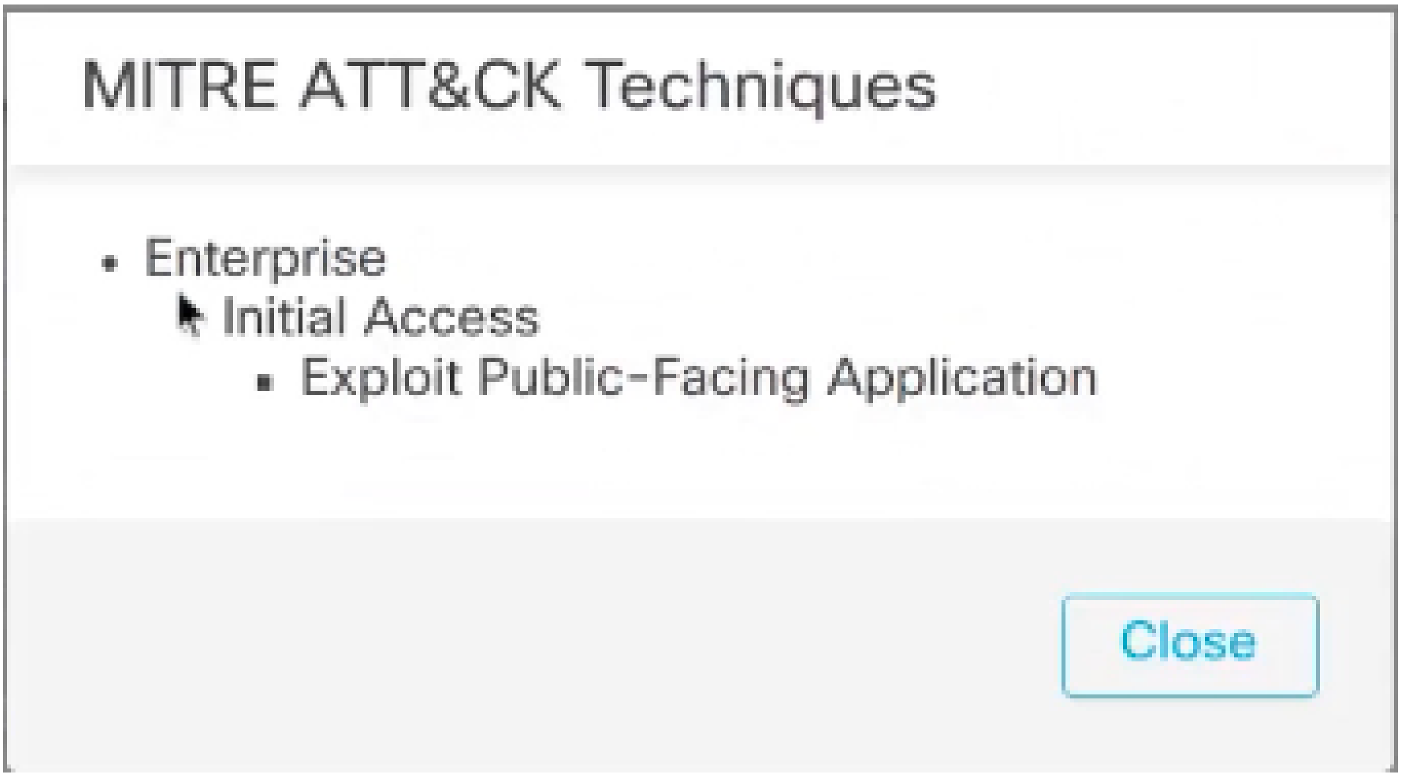
3. In the MITRE ATT&CKcolumn header, you can see the techniques for an intrusion event.



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

Mitre column header

4. Click 1 Techniqueto view the MITRE ATT&CK Techniques, as shown in this figure. In this example, Exploit Public-Facing Applicationis the technique.



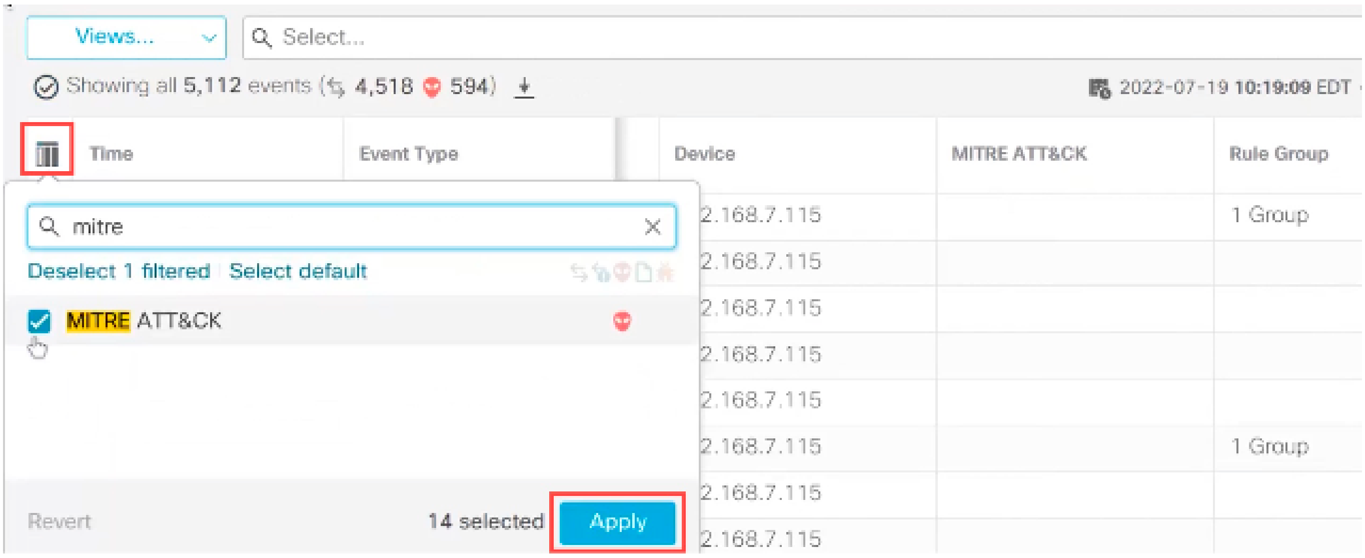
MITRE ATT&CK Techniques

- Enterprise
  - Initial Access
    - Exploit Public-Facing Application

Close

MITRE ATT&CK Techniques

5. Click Close.
6. Click Analysis > Unified Events.
7. You can click the column selector icon to enable the MITRE ATT&CKand Rule Groupcolumns.



Views... Select...

Showing all 5,112 events (4,518 594) 2022-07-19 10:19:09 EDT

mitre

Deselect 1 filtered Select default

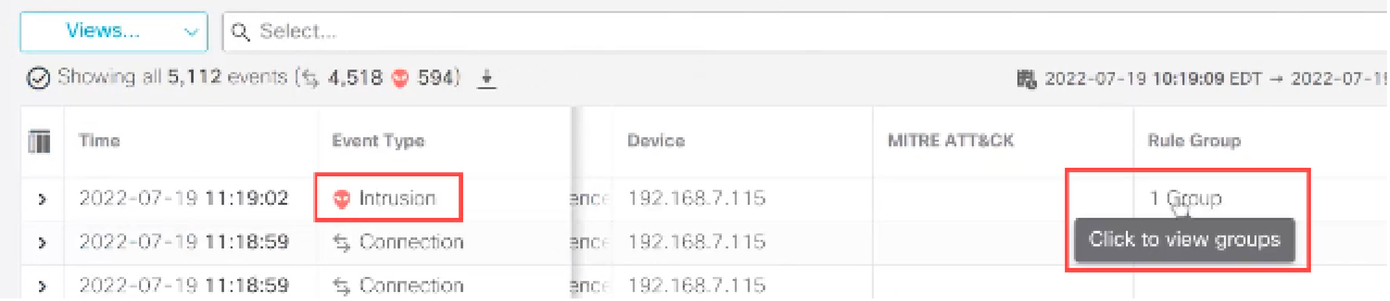
☑ MITRE ATT&CK

Revert 14 selected Apply

Time	Event Type	Device	MITRE ATT&CK	Rule Group
		2.168.7.115		1 Group
		2.168.7.115		
		2.168.7.115		
		2.168.7.115		
		2.168.7.115		
		2.168.7.115		1 Group
		2.168.7.115		
		2.168.7.115		

Enable the Mitre Attack

8. As shown in the example here, the intrusion event was triggered by an event that is mapped to one rule group. Click 1 Group under the Rule Groupcolumn.



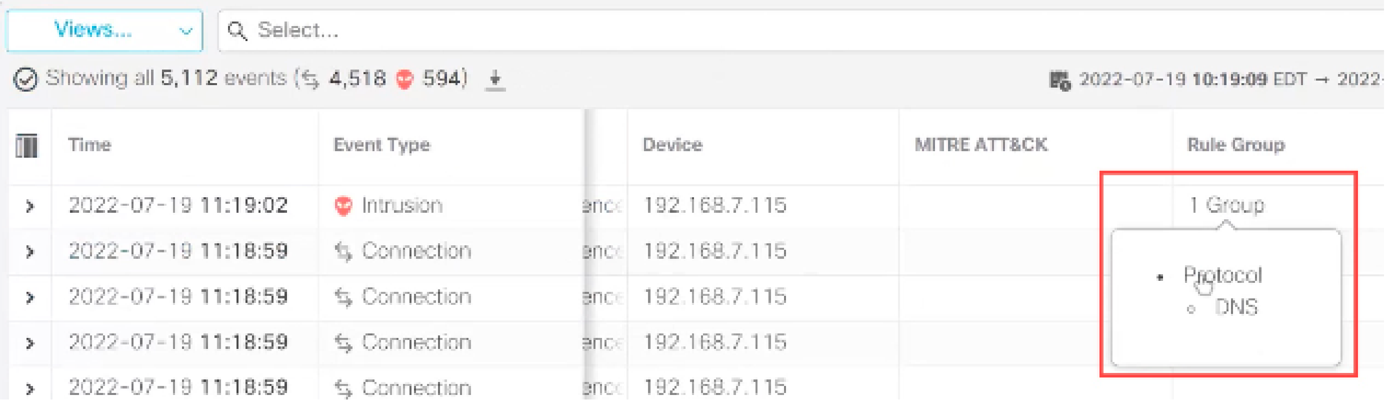
Showing all 5,112 events (4,518 594)

2022-07-19 10:19:09 EDT → 2022-07-1

	Time	Event Type		Device	MITRE ATT&CK	Rule Group
›	2022-07-19 11:19:02	Intrusion	ence	192.168.7.115		1 Group
›	2022-07-19 11:18:59	Connection	ence	192.168.7.115		
›	2022-07-19 11:18:59	Connection	ence	192.168.7.115		

Rule group

9. As an example, you can view Protocol, which is the parent rule group, and the DNS rule group under it.



Showing all 5,112 events (4,518 594)

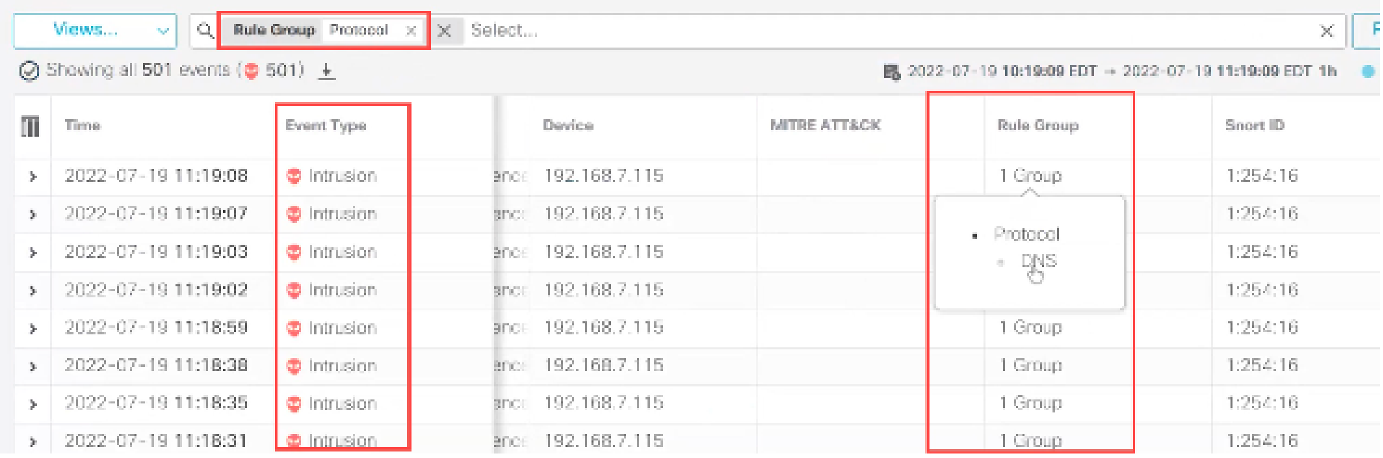
2022-07-19 10:19:09 EDT → 2022-

	Time	Event Type		Device	MITRE ATT&CK	Rule Group
›	2022-07-19 11:19:02	Intrusion	ence	192.168.7.115		1 Group
›	2022-07-19 11:18:59	Connection	ence	192.168.7.115		
›	2022-07-19 11:18:59	Connection	ence	192.168.7.115		
›	2022-07-19 11:18:59	Connection	ence	192.168.7.115		
›	2022-07-19 11:18:59	Connection	ence	192.168.7.115		

- Protocol
  - DNS

View protocol

10. You can click Protocol to search for all the intrusion events that have at least one rule group, that is Protocol > DNS . The search results are displayed, as shown in the example here.



Showing all 501 events (501)

2022-07-19 10:19:09 EDT → 2022-07-19 11:19:09 EDT 1h

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

- Protocol
  - DNS

Rule group protocol