Mitigate Threats Using MITRE Framework in Snort 3 Intrusion Policies

About MITRE ATT&CK Framework

The MITRE ATT&CK Framework is a comprehensive knowledge base that outlines the tactics, techniques, and procedures (TTPs) used by threat actors to compromise systems. It organizes these TTPs into matrices for different operating systems and platforms, mapping each attack stage (tactics) to specific methods (techniques). Each technique includes information about execution, procedures, defenses, detections, and real-world examples.

Note See https://attack.mitre.org for additional information about MITRE ATT&CK.

The management center uses the MITRE ATT&CK Framework to enhance threat detection and response, incorporating the following capabilities:

- Intrusion events include TTPs, allowing administrators to manage traffic with greater granularity by grouping rules according to vulnerability type, target system, or threat category.
- Select malware events use TTPs, enhancing the ability to detect and respond to threats.
- Unified and Classic Event Viewers display tactics, techniques, attack lifecycle graphs, and contextual enrichments from the Talos taxonomy. These enrichments include MITRE tags and a hierarchical view of associated tactics, techniques, and sub-techniques. You can also filter events using MITRE identifiers.

Benefits of MITRE Framework

- MITRE Tactics, Techniques, and Procedures (TTPs) are added to intrusion events, which enable administrators to act on traffic, based on the MITRE ATT&CK framework. This enables administrators to view and handle traffic with more granularity, and 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.

Sample Business Scenario for MITRE Network

A large corporate network uses Snort 3 as its primary intrusion detection and prevention system. In a rapidly evolving threat landscape, adoption of robust network security measures is necessary and important. Network administrators need to know if the configured policies are finding traffic of interest and if they are tracking a known attack group. For example, you may want to know if adversaries are attempting to take advantage of a weakness in your systems or applications in order to cause unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. The applications may be websites, databases, standard services, such as Server Message Block (SMB) or Secure Shell (SSH), network device administration and management protocols or applications, such as web servers and related services.

The insights provided by the MITRE framework provides administrators with a more precise opportunity to specify protection for specific assets and protect their network from specific threat groups.

Prerequisites for MITRE Framework

- You must be running Secure Firewall Management Center and Secure Firewall Threat Defence Version 7.3.0 or later with Snort 3.
- You must have at least one intrusion policy. See Create a Custom Snort 3 Intrusion Policy.

View and Edit Your Snort 3 Intrusion Policy

Procedure

Step 1 Choose **Policies** > **Security policies** > **Intrusion**.

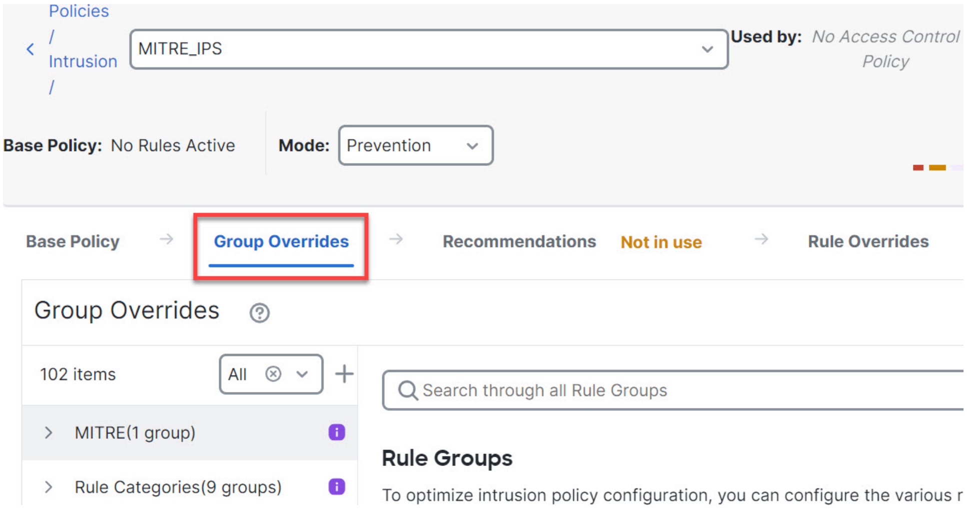
Step 2 Ensure that the **Intrusion Policies** tab is chosen.

Step 3 Click **Snort 3 Version** next to the intrusion policy that you want to view or edit.

Step 4 Close the Snort helper guide that is displayed.

Step 5 Click the **Group Overrides** layer.

This layer lists all the categories of rule groups in an hierarchical structure. You can drill down to the last leaf rule group under each rule group.



Policies / Intrusion / MITRE_IPS

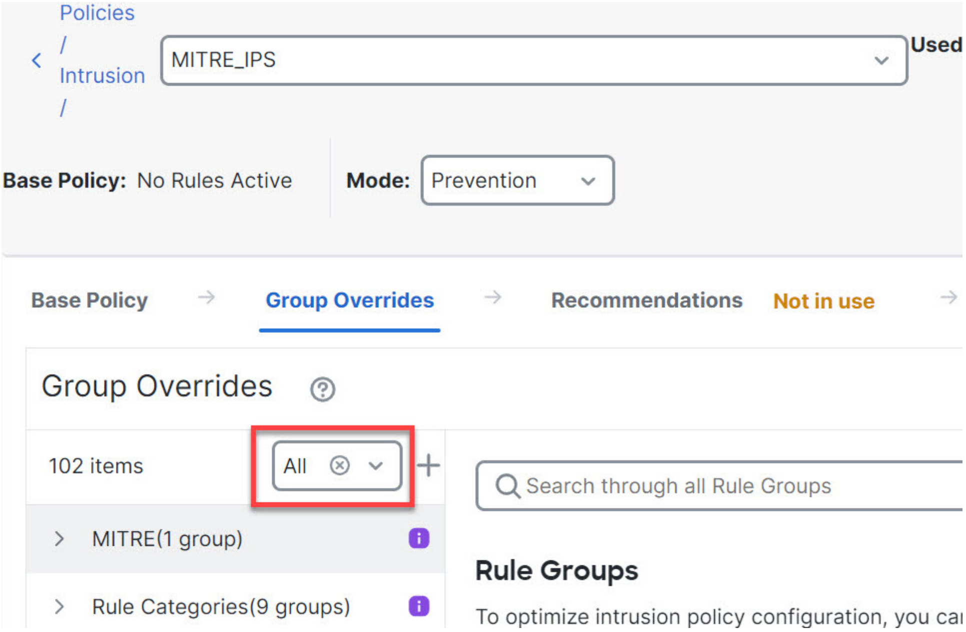
Used by: No Access Control Policy

Base Policy: No Rules Active

Mode: Prevention

Base Policy
Group Overrides
Recommendations
Not in use
Rule Overrides
Group Overrides
102 items
All
Search through all Rule Groups
MITRE(1 group)
Rule Categories(9 groups)
Rule Groups
To optimize intrusion policy configuration, you can configure the various r

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



Policies / Intrusion / MITRE_IPS

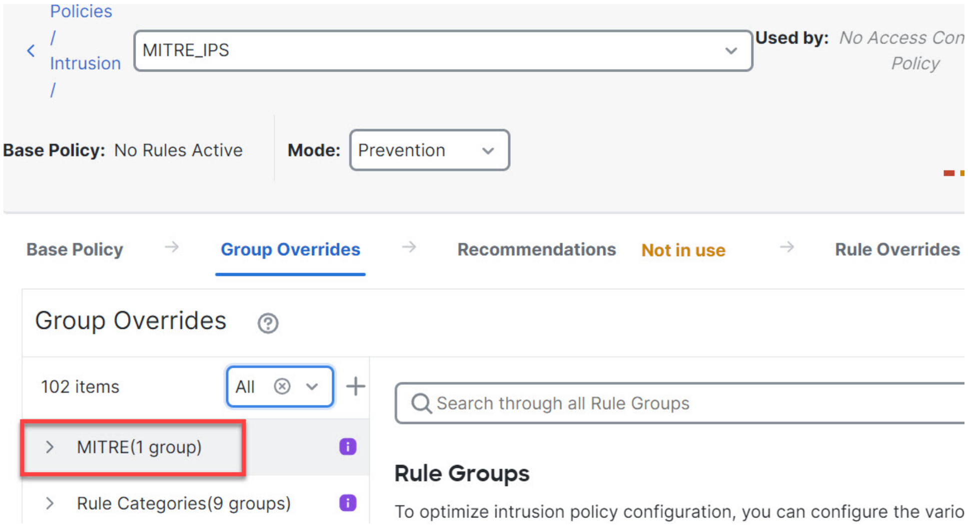
Base Policy: No Rules Active

Mode: Prevention

Step 7 Click **MITRE** in the left pane.

Note

Depending on your specific requirements, you can choose the **Rule Categories** rule group or any other rule group and subrule groups under it. All the rule groups use the MITRE framework.



Policies / Intrusion /

MITRE_IPS

Used by: *No Access Con Policy*

Base Policy: No Rules Active **Mode:** Prevention

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

Group Overrides

102 items All

MITRE(1 group)

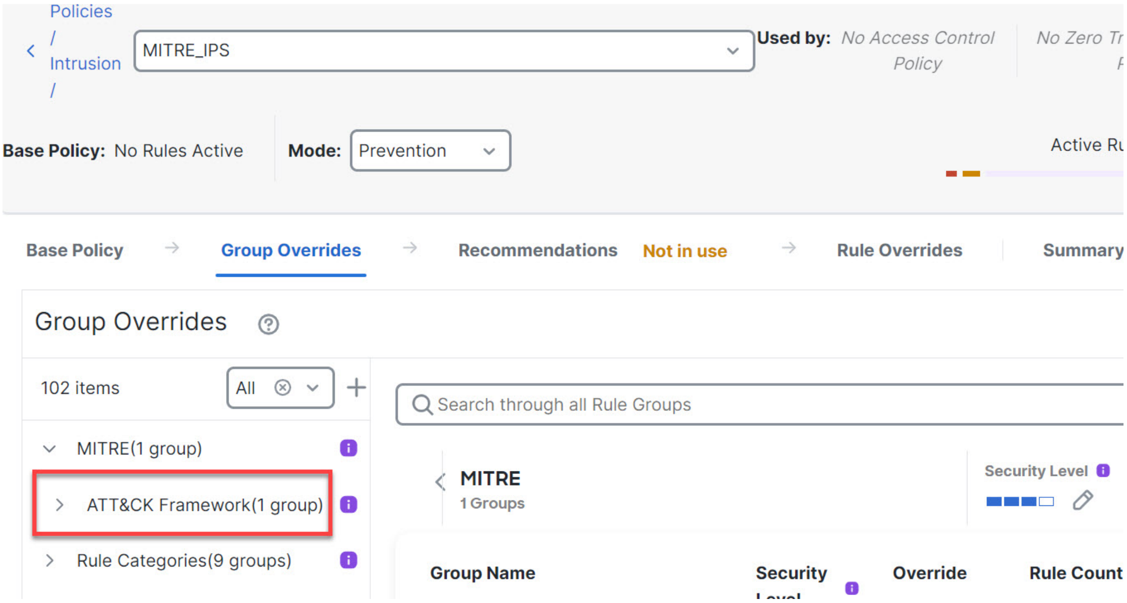
Rule Categories(9 groups)

Search through all Rule Groups

Rule Groups

To optimize intrusion policy configuration, you can configure the vario

Step 8 Under **MITRE**, click **ATT&CK Framework** to drill down.



Policies / Intrusion /

MITRE_IPS

Used by: *No Access Control Policy* *No Zero Tr P*

Base Policy: No Rules Active **Mode:** Prevention

Active Ru

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

Group Overrides

102 items All

MITRE(1 group)

ATT&CK Framework(1 group)

Rule Categories(9 groups)

Search through all Rule Groups

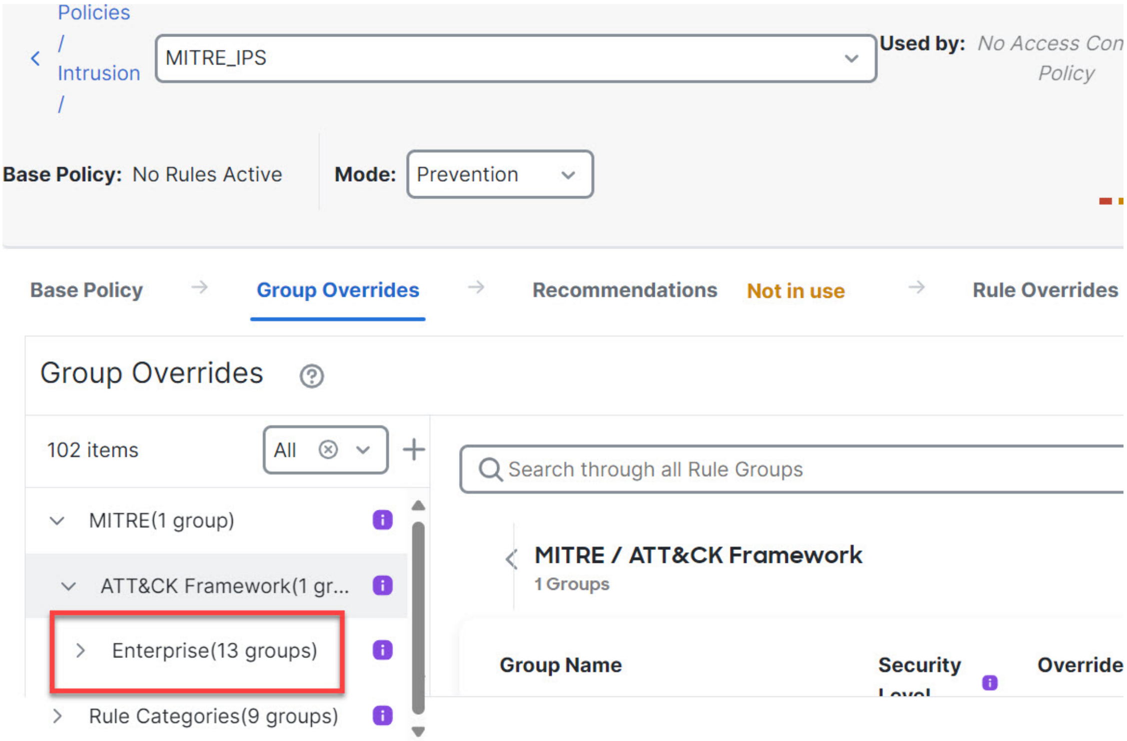
MITRE

1 Groups

Security Level

Group Name | Security Level | Override | Rule Count

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



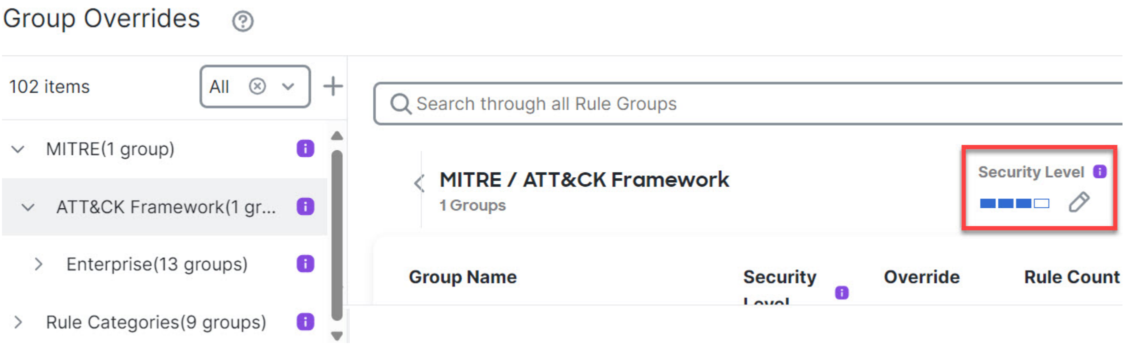
Policies / Intrusion / MITRE_IPS

Used by: No Access Con Policy

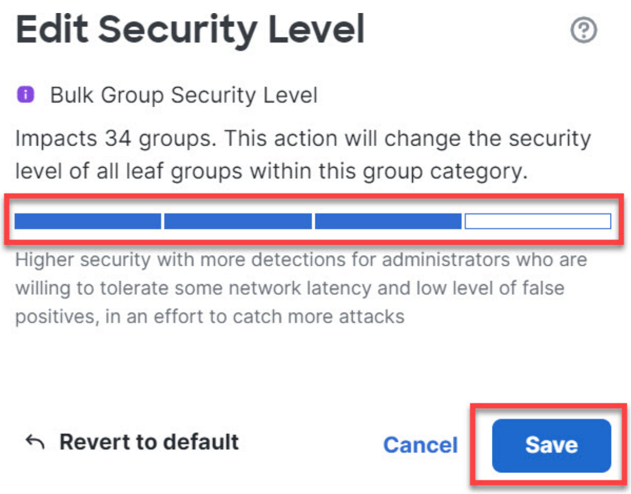
Base Policy: No Rules Active

Mode: Prevention

Step 10 Click the **Edit** (✎) icon next to the **Security Level** of the rule group to make bulk changes to the security level of all the associated rule groups under the **Enterprise** rule group category.



Step 11 In the **Edit Security Level** window, choose a **Security Level** (in this example, **3**), and click **Save**.



Edit Security Level

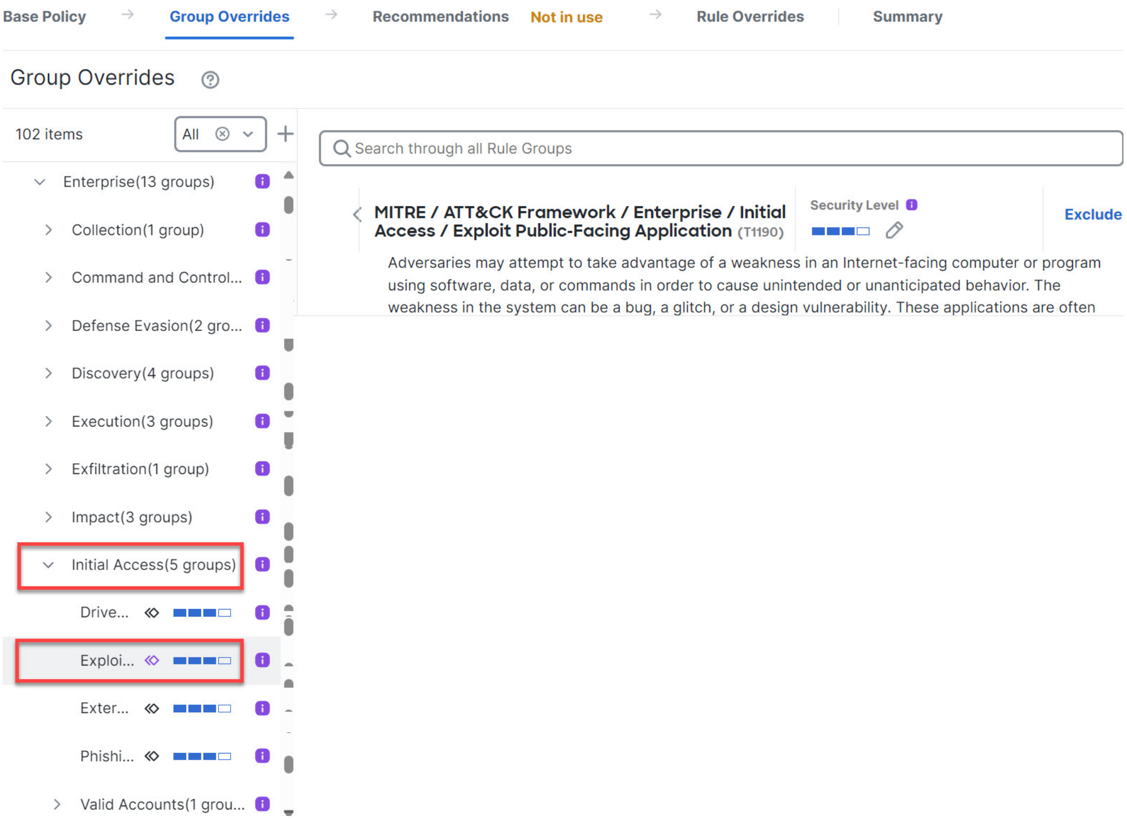
Bulk Group Security Level

Impacts 34 groups. This action will change the security level of all leaf groups within this group category.

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

Step 12 Under **Enterprise**, click **Initial Access** to expand it.

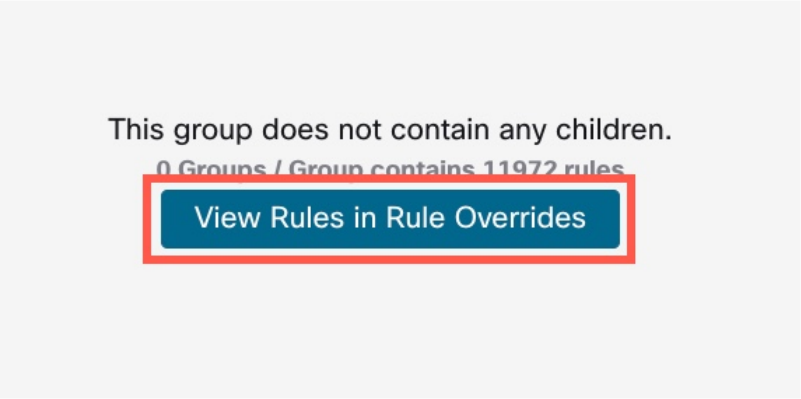
Step 13 Under **Initial Access**, click **Exploit Public-Facing Application**, which is the last leaf group.



MITRE / ATT&CK Framework / Enterprise / Initial Access / Exploit Public-Facing Application (T1190)

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often

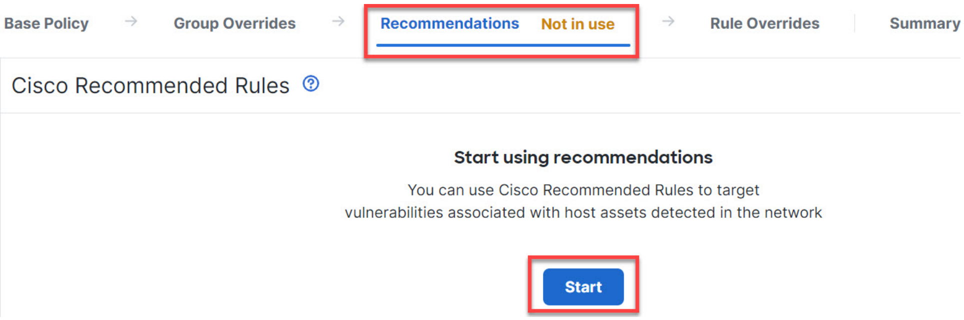
Step 14 Click **View Rules in Rule Overrides** to view the different rules, rule details, rule actions, and so on, for the different rules. You can change the rule actions for one or multiple rules in the **Rule Overrides** layer.



This group does not contain any children.

0 Groups / Group contains 11972 rules

Step 15 Click the **Recommendations** layer and then click **Start** to start using Cisco-recommended rules. You can use the intrusion rule recommendations to target the vulnerabilities that are associated with the host assets detected in the network. For more information, see Generate New Secure Firewall Recommendations in Snort 3.

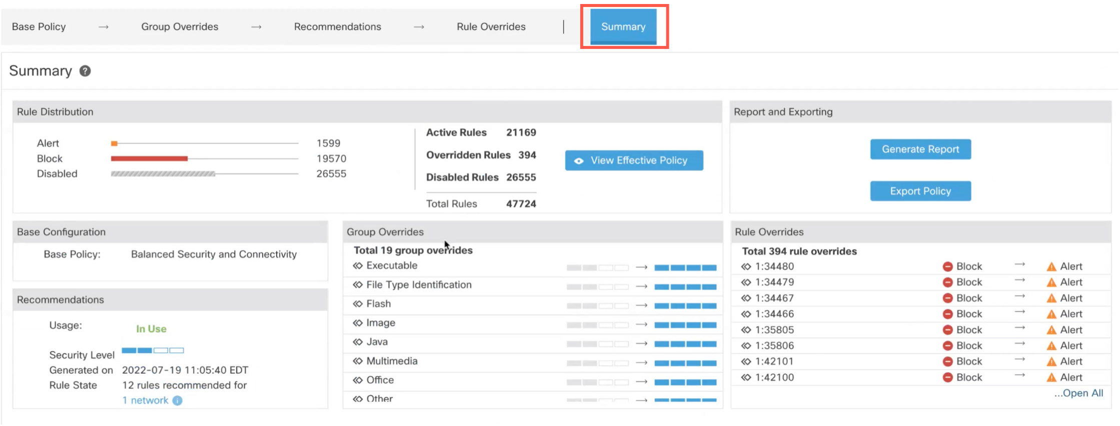


Cisco Recommended Rules

Start using recommendations

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

Step 16 Click the **Summary** layer for a holistic view of the current changes to the policy. Based on the rule overrides, security-level changes, and generation of Cisco-recommended rules, you can view the rule distribution of the policy, group overrides, rule overrides, rule recommendations, and so on, to verify your changes.



Summary

Rule Distribution

Alert	1599
Block	19570
Disabled	26555

Active Rules	**21169**
Overridden Rules	**394**
Disabled Rules	**26555**
Total Rules	**47724**

Report and Exporting

Base Configuration

Base Policy: Balanced Security and Connectivity

Recommendations

Usage: In Use

Security Level

Generated on 2022-07-19 11:05:40 EDT

Rule State 12 rules recommended for 1 network

Group Overrides

Total 19 group overrides

- Executable
- File Type Identification
- Flash
- Image
- Java
- Multimedia
- Office
- Other

Rule Overrides

Total 394 rule overrides

1:34480	Block	→	Alert
1:34479	Block	→	Alert
1:34467	Block	→	Alert
1:34466	Block	→	Alert
1:35805	Block	→	Alert
1:35806	Block	→	Alert
1:42101	Block	→	Alert
1:42100	Block	→	Alert

What to do next

Deploy your intrusion policy to detect and log events that are triggered by the Snort rules. See Deploy Configuration Changes.

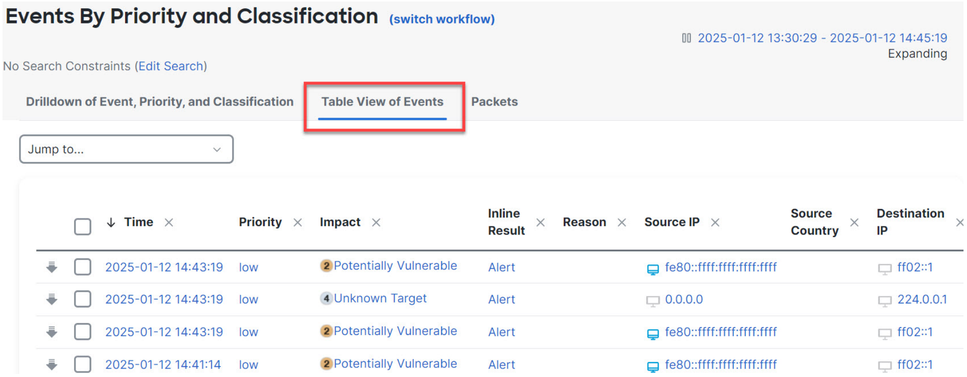
View Intrusion Events

You can view the MITRE ATT&CK techniques and rule groups in the intrusion events on the **Classic Event Viewer** and **Unified Event Viewer** pages. 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).

Procedure

Step 1 Click **Analysis** and select **Events** under **Intrusions**.

Step 2 Click the **Table View of Events** tab.



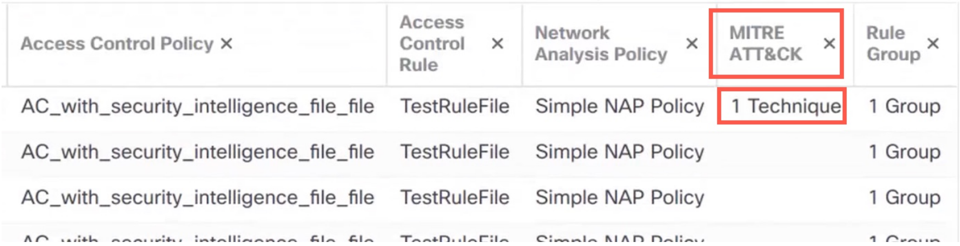
Events By Priority and Classification (switch workflow)

2025-01-12 13:30:29 - 2025-01-12 14:45:19
Expanding

No Search Constraints (Edit Search)

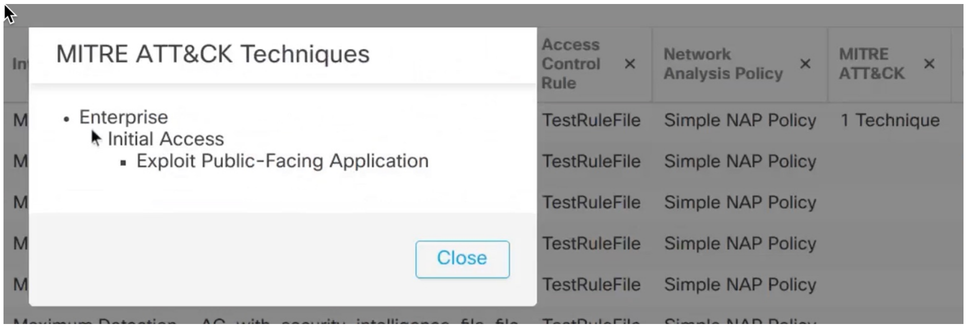
	□	↓ Time ×	Priority ×	Impact ×	Inline Result ×	Reason ×	Source IP ×	Source Country ×	Destination IP ×
	□	2025-01-12 14:43:19	low	2 Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1
	□	2025-01-12 14:43:19	low	4 Unknown Target	Alert		0.0.0.0		224.0.0.1
	□	2025-01-12 14:43:19	low	2 Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1
	□	2025-01-12 14:41:14	low	2 Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1

Step 3 Under **MITRE ATT&CK**, you can see the techniques for an intrusion event. Click **1 Technique** to view the MITRE ATT&CK techniques.



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
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

In this example, **Exploit Public-Facing Application** is the technique.



MITRE ATT&CK Techniques

- Enterprise
  - Initial Access
    - Exploit Public-Facing Application

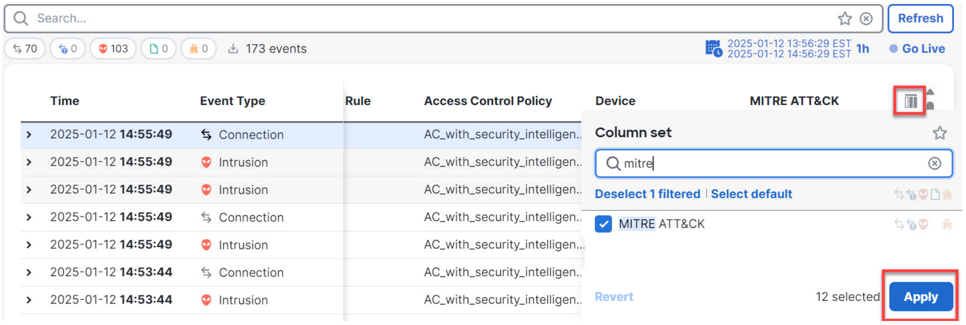
Close

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

Step 4 Click **Close**.

Step 5 Click **Analysis** and select **Unified Events**.

Step 6 If not enabled, click the column selector icon to enable the **MITRE ATT&CK** and **Rule Group** columns.



Time	Event Type	Rule	Access Control Policy	Device	MITRE ATT&CK
2025-01-12 **14:55:49**	Connection		AC_with_security_intelligen...		
2025-01-12 **14:55:49**	Intrusion		AC_with_security_intelligen...		
2025-01-12 **14:55:49**	Intrusion		AC_with_security_intelligen...		
2025-01-12 **14:55:49**	Connection		AC_with_security_intelligen...		
2025-01-12 **14:55:49**	Intrusion		AC_with_security_intelligen...		
2025-01-12 **14:53:44**	Connection		AC_with_security_intelligen...		
2025-01-12 **14:53:44**	Intrusion		AC_with_security_intelligen...		

Column set

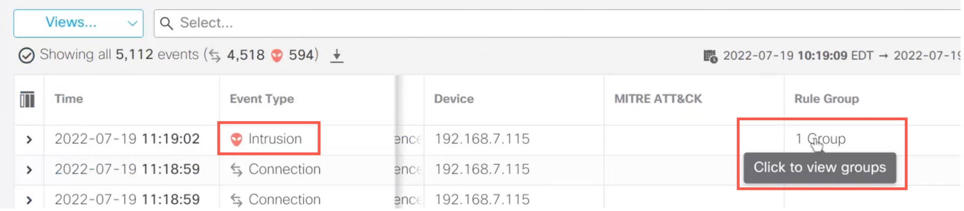
mitre

Deselect 1 filtered | Select default

☑ MITRE ATT&CK

Revert 12 selected Apply

Step 7 In this example, the intrusion event is triggered by an event that is mapped to one rule group. Click **1 Group** under the **Rule Group** column.



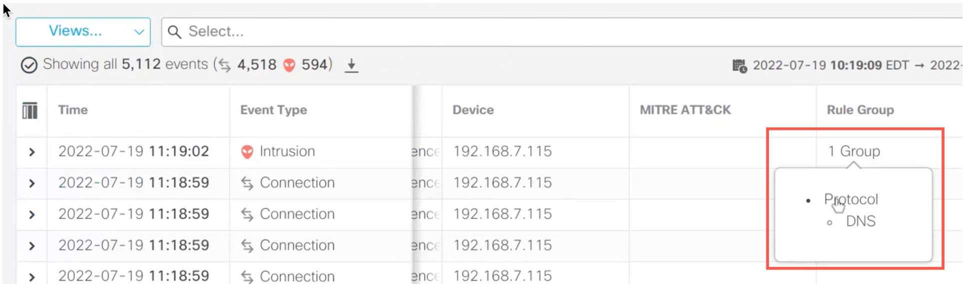
Showing all 5,112 events (4,518 594)

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		

Click to view groups

Step 8 You can view **Protocol**, which is the parent rule group, and the DNS rule group under it. Choose **Protocol** > **DNS** to search for all the intrusion events that have at least one rule group that is .



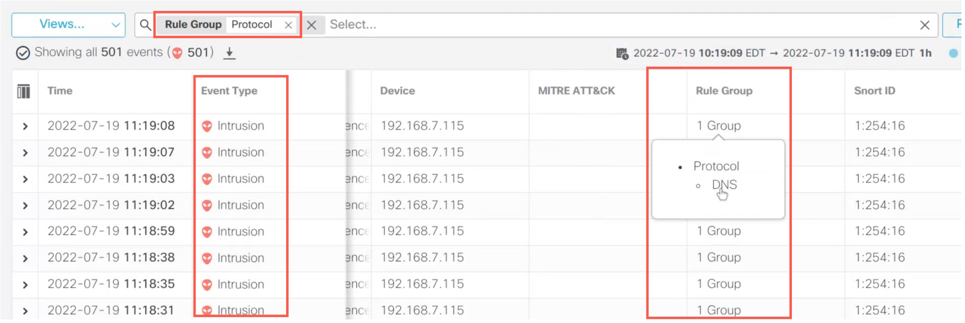
Showing all 5,112 events (4,518 594)

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

The search results are displayed.



Views... | Rule Group Protocol | Select...

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

Additional References

- Intrusion Policy in Snort 3
- Edit Snort 3 Intrusion Policies
- MITRE Information in Malware Events