

Configure Elephant Flow Detection Outcomes

- About MITRE Framework, on page 1
- Benefits of MITRE Framework, on page 1
- Prerequisites, on page 2
- Sample Business Scenario, on page 2
- View and Edit your Snort 3 Intrusion Policy, on page 2
- View Intrusion Events, on page 7
- Additional References, on page 9

About MITRE Framework

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."



Note See https://attack.mitre.org for information about MITRE.

Each technique in the ATT&CK framework is accompanied with information about the technique, associated procedures, probable defenses 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. Usage of groups in the framework helps categorize and document behaviors.

The MITRE framework enables you to navigate through your intrusion rules. MITRE is just another category of rule groups and are part of the Talos rule groups. In your Snort 3 intrusion policy, you can navigate through several levels of rule groups that provides more flexibility and logical grouping of rules.

Benefits of MITRE Framework

MITRE Tactics, Techniques, and Procedures (TTPs) are added to intrusion events that enables
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.

Prerequisites

- You must be running management center 7.3.0 or later with managed devices 7.3.0 or later using Snort 3.
- You must have at least one intrusion policy. See Create a Custom Snort 3 Intrusion Policy.

Sample Business Scenario

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 observing a known attack group.

As an example, you may want to know if adversaries are attempting to take advantage of a weakness in your systems or applications to cause unintended or 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 SMB or SSH, network device administration and management protocols, or applications, such as web servers and related services.

The insights provided by the MITRE framework, enables the administrators a more precise opportunity to specify protection for specific assets and protect themselves from specific threat groups.

View and Edit your Snort 3 Intrusion Policy

- **Step 1** Choose **Policies** > **Intrusion**.
- **Step 2** Ensure that the **Intrusion Policies** tab is chosen.
- **Step 3** Click **Snort 3 Version** next to the intrusion policy you want to view or edit.
- **Step 4** Close the Snort helper guide that pops up.
- **Step 5** Click the **Group Overrides** layer.

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



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

< Policies / Intrusion / MITRE_IPS			~
Base Policy: Balanced Security and Co	nnectivity	Mode: Prevention V	
Base Policy → Group	\rightarrow Overrides \rightarrow	Recommendations No	ot in use \rightarrow
Group Overrides @			
102 items	All	x v +	h through all Rule Gr
> MITRE(1 group)		Rule Gro	oups
> Rule Categories(9 groups)		 To optimiz or decrease 	e intrusion policy cor e security levels, thu

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

Note For this example, we have chosen MITRE, 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.

< Policies / Intrusion / MITRE_IPS			~		
Base Policy: Balanced Security and C	onnectivity	Mode: Preventio	n 🗸		
Base Policy → Grou	p Overrides \rightarrow	Recommenda	tions Not in use	\rightarrow Rule	Overrides
Group Overrides @					
102 items	All	× • +	${\bf Q}_{\rm c}$ Search through all	Rule Groups	
> MITRE(1 group)		0	Rule Groups		
> Rule Categories(9 groups)		()	To optimize intrusion po or decrease security lev	licy configuration, els, thus enriching	you can con intrusion ev

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

< Policies / Intrusion / MITRE_IPS	~
Base Policy: Balanced Security and Connectivity	Mode: Prevention
Base Policy \rightarrow Group Overrides \rightarrow	Recommendations Not in use \rightarrow Rule Overrides Summary
Group Overrides @	
102 items All	x v +
✓ MITRE(1 group)	
> ATT&CK Framework(1 group)	1 Groups
> Rule Categories(9 groups)	Government

Step 9

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

	< Policies / Intrusion / MITR	E_IPS		~	
Ba	ise Policy: Balanced Security	and Connectivity	Mode: Prevention	 Image: A set of the set of the	
	Base Policy \rightarrow	Group Overrides \rightarrow	Recommendations	Not in use \rightarrow	Rule Overrides
	Group Overrides	>			
	102 items	All	x v + ् ् Sea	arch through all Rule Groups	;
	✓ MITRE(1 group)		0	MITRE / ATT&CK Fra	mework
	\vee ATT&CK Framework(1	group)	0	1 Groups	
	> Enterprise(13 group	os)	Group	Name	
	> Rule Categories(9 group	energia (s)	Enterp Enterp	rise rise tactics represent the "why	y" of an ATT&CK technique or a

Step 10 Click **Edit** (*I*) 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 **Enterprise** rule group category.

K	Group Overrides @						
	102 items All	x ~ +	Q Sear	rch through all Rule Groups			
	✓ MITRE(1 group)	0	<	MITRE / ATT&CK Framework		Security Level 🕕	
	~ ATT&CK Framework(1 group)	•		1 Groups			
	> Enterprise(13 groups)	0	Group N	ame	Security Level	Override	Rule
	> Rule Categories(9 groups)	0	Enterpr Enterpri	ise ise tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversar			

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



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.

Figure 1: MITRE Tactics and Techniques

Base Policy \rightarrow Group Overrides \rightarrow	Recommendation	n use → Rule Overrides S	Summary		
Group Overrides @					
102 hours					
All X		hrough all Rule Groups			
V Enterprise(13 groups)	0	ITRE / ATT&CK Framework / Enterprise / Initial Ad Groups	CCESS (TA0001)		Security Level 🌖
> Collection(1 group)	G			Security Level	Override
> Command and Control(3 groups)	0				
> Defense Evasion(2 groups)	6 A	mpromise (T1189) may gain access to a system through a user visiting a website	over the normal course	/	<
> Discovery(4 groups)	0 E:	ic-Facing Application (T1190) may attempt to take advantage of a weakness in an Internet-fa	acing computer or progr	/	<
> Execution(3 groups)	i E	mote Services (T1133) may leverage external-facing remote services to initially acces	ss and/or persist within a		<<>
> Exfiltration(1 group)	0				
> Impact(3 groups)	0 A	(566) may send phishing messages to gain access to victim system.	s. All forms of phishing a		\diamond
✓ Initial Access(5 groups)	A	nts (T1078) may obtain and abuse credentials of existing accounts as a m	eans of gaining Initial Ac		
Drive-by Compromise 🚸 💴 💴	0				
Exploit Public-Facing Application 🗇 📃 🔲	•				
External Remote Services 🚸 🔲 💴	0				
Phishing 🗇 🔲	0				

Step 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. 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 View Rules in Rule Overrides

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 vulnerabilities associated with host assets detected in the network. For more information, see Generate New Secure Firewall Recommendations in Snort 3.



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.

Base Policy \rightarrow Group Overrides \rightarrow Recon	nmendations \rightarrow Rule Overrides	Summary			
Summary Ø					
Rule Distribution			Report and Exporting		
Alert 1 Biock 1 Disabled 2	Active Rules 21169 9570 Overridden Rules 394 6555 Disabled Rules 26555 Total Rules 47724	• View Effective Policy	Gene	erate Report	
Base Configuration	Group Overrides		Rule Overrides		
Base Policy: Balanced Security and Connectivity	Total 19 group overrides		Total 394 rule overrides (*) 1:34480 (*) 1:34479	Block	→ Alert
Recommendations	© Flash		< 1:34467	Block	→ 🔺 Alert
Usage: In Lies	« Image		♦ 1:34466	Block	Alert
iii ose	«> Java		© 1:35805	Block	→ Alert
Security Level	«> Multimedia		< 1:42101	Block	→ Alert
Rule State 12 rules recommended for	«> Office		< 1:42100	Block	→ ▲ Alert
1 network 🕕	«> Other	\longrightarrow			Open A

L

What to do next

Deploy your intrusion policy to detect and log events 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 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).

Step 1Click Analysis > Intrusions > Events.

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

Events	s By Priority ar	II 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	Jump to								
	↓ Time ×	Priority ×	Impact X	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	口 192.168.0.227		口 146.112.255.69	
•	2022-07-19 11:17:06	medium	2	Would block	Interface in Passive or Tap mode	口 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 🔤	口 192.168.7.214	
•	2022-07-19 11:17:05	medium	2	Would block	Interface in Passive or Tap mode	口 192.168.3.254		口 192.168.7.241	

Step 3 In the **MITRE ATT&CK** column 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 Techniq	ue 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 accurity intelligence file file	TeatDulaFile	Simple NAD Delieu	1 Croup

Step 4Click 1 Technique to view the MITRE ATT&CK Techniques, as shown in the following figure. In this example,
Exploit Public-Facing Application is the technique.

4					
In	MITRE ATT&CK Techniques	Access Control × Rule	Network Analysis Policy	MITRE ATT&CK ×	
М	Enterprise Initial Access	TestRuleFile	Simple NAP Policy	1 Technique	
М	Exploit Public-Facing Application	TestRuleFile	Simple NAP Policy		
М		TestRuleFile	Simple NAP Policy		
Μ	Close	TestRuleFile	Simple NAP Policy		
М		TestRuleFile	Simple NAP Policy		
		T			

Step 5 Click Close.

- **Step 6** Click **Analysis** > **Unified Events**.
- **Step 7** If not already enabled, click the column selector icon to enable the **MITRE ATT&CK** and **Rule Group** columns.

Showing all 5,112 e	vents (🔄 4,518 😨 594) 🛓		202	2-07-19 10:19:09 E
Time	Event Type	Device	MITRE ATT&CK	Rule Group
Q mitre		× 2.168.7.115		1 Group
eselect 1 filtered Sel	ect default	\$ \$0		
MITRE ATT&CK		2.168.7.115		
7		2.168.7.115		
		2.168.7.115		
		2.168.7.115		1 Group
	r.	2.168.7.115		
tevert	14 selected	Apply 2 168 7 115		

Step 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 Group** column.

	Views ~ Q Selec	t				
\odot	Showing all 5,112 events (🗦 4,518 🙄 594) 🗜			2	022-07-19 10:19:09 EDT → 2022-07-19
	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	S Connection	ence	192.168.7.115		Click to view groups
>	2022-07-19 11:18:59	S Connection	enc∈	192.168.7.115		

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

⊘ Showing all 5,112 events (≤ 4,518 ♀ 594) ± Bowing all 5,112 events (≤ 4,518 ♀ 594) ±								
	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	Sconnection ≤ Connection	ence	192.168.7.115		Destand		
>	2022-07-19 11:18:59	S Connection	ence	192.168.7.115		Protocol DNS		
>	2022-07-19 11:18:59	S Connection	ence	192.168.7.115				
>	2022-07-19 11:18:59	S Connection	ence	192.168.7.115	L			

Step 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 below.

	Views Views	Group Protocol X	X Select.				×		
OTT	Time	Event Type		Device	MITRE ATT&CK	Rule Group	Snort 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	ence	192.168.7.115		Protocol DNS	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		

Additional References

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