

Gebruik het MITER-framework om potentiële bedreigingen in Secure FMC te bekijken en ernaar te handelen

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Voordelen van het MITRE Framework](#)

[Bekijk het MITER Framework in uw Intrusion Policy](#)

[Inbraakgebeurtenissen bekijken](#)

Inleiding

In dit document wordt beschreven hoe u het MITER-framework kunt gebruiken om potentiële bedreigingen in een beveiligd Firepower Management Center (FMC) te bekijken en erop te reageren.

Achtergrondinformatie

Het MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework is een uitgebreide kennisbasis en methodologie die inzicht biedt in de tactieken, technieken en procedures (TTP's) die worden verspreid door dreigingsactoren die systemen willen schaden. ATT&CK wordt gecompileerd in matrices die elk besturingssystemen of een bepaald platform vertegenwoordigen. Elke fase van een aanval, bekend als "tactiek", wordt in kaart gebracht met de specifieke methoden die worden gebruikt om die fasen te bereiken, bekend als "technieken".

Elke techniek in het ATT & CK-framework gaat vergezeld van informatie over de techniek, bijbehorende procedures, waarschijnlijke verdedigingen en detecties en voorbeelden uit de echte wereld. Het MITRE ATT & CK-raamwerk bevat ook groepen om te verwijzen naar dreigingsgroepen, activiteitengroepen of dreigingsactoren op basis van de reeks tactieken en technieken die ze gebruiken. Door het gebruik van Groepen, het kader helpt categoriseren en documenteren gedrag.

Voor meer informatie over MITER verwijzen wij u naar <https://attack.mitre.org>.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van snort
- Beveiligde FMC
- Veilige bescherming tegen vuurkracht (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Dit document is van toepassing op alle Firepower-platforms
- Beveiligde FTD met softwareversie 7.3.0
- Secure Firepower Management Center Virtual (FMC) met softwareversie 7.3.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Voordelen van het MITRE Framework

- MITER Tactics, Techniques, and Procedures (TTP's) worden toegevoegd aan inbraakgebeurtenissen waarmee beheerders kunnen handelen op basis van het MITER ATT & CK-framework (Adversary Tactics Techniques and Common Knowledge). Hierdoor kunnen beheerders het verkeer gedetailleerder bekijken en afhandelen en kunnen ze regels groeperen op kwetsbaarheidstype, doelsysteem of bedreigingscategorie.
- U kunt inbraakregels organiseren volgens het MITRE ATT&CK-raamwerk. Hiermee kunt u het beleid aanpassen aan specifieke tactieken en technieken van aanvallers.

Bekijk het MITER Framework in uw Intrusion Policy

Met het MITER-framework kunt u door uw inbraakregels navigeren. MITER is gewoon een andere categorie van regelgroepen en maakt deel uit van de Talos-regelgroepen. Regelnavigatie voor verschillende niveaus van regelgroepen wordt ondersteund, wat meer flexibiliteit en logische groepering van regels biedt.

1. Kies **Policies > Intrusion** uit.
2. Zorg ervoor dat het **Intrusion Policies** tabblad is geselecteerd.
3. Klik **Snort 3 Version** naast het inbraakbeleid dat u wilt bekijken of bewerken. Sluit de Snort-hulprij die verschijnt.
4. Klik op de **Group Overrides** laag.

In de **Group Overrides** laag worden alle categorieën regelgroepen in een hiërarchische structuur weergegeven. U kunt naar de laatste bladregelgroep in elke regelgroep gaan.

< 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 Overrid... 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. Group Overrides Ervoor zorgen dat All Dit wordt in de vervolgkeuzelijst gekozen, zodat alle regelgroepen voor het inbraakbeleid in het linkerdeelvenster zichtbaar zijn.

7. Klik op MITRE in het linkerdeelvenster.



Opmerking: In dit voorbeeld is MITER geselecteerd, maar afhankelijk van uw specifieke vereisten kunt u de regelcategorieën of een andere regelgroep en daaropvolgende regelgroepen kiezen. Alle regelgroepen gebruiken het MITER-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 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. Klik onder MITRE op ATT&CK Raamwerk om het uit te vouwen.

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description test_policy

Base Policy → **Group Overrides** → Recommendations **Not in use** → Rule Overrides | Summary Page 3

Group Overrides ?

101 items All x v +

Search through all Rule Groups

MITRE (1 group)

ATT&CK Framework (1 group)

Enterprise (13 groups)

MITRE / ATT&CK Framework
1 Groups

Group Name Security Level

9. Klik onder ATT&CK Frameworkaan op Enterprise om het te vergroten.

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description test_policy Page 3

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

Group Overrides ?

101 items All x v +

Search through all Rule Groups

MITRE (1 group)

ATT&CK Framework (1 group)

Enterprise (13 groups)

MITRE / ATT&CK Framework / Enterprise
13 Groups

Group Name

10. Klik Edit () naast het beveiligingsniveau van de regelgroep om bulksgewijs wijzigingen aan te brengen in het beveiligingsniveau voor alle bijbehorende regelgroepen onder de EnterpriseRubriek Regelgroep.

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

Group Overrides ?

101 items All x v +

Search through all Rule Groups

MITRE (1 group)

ATT&CK Framework (1 group)

Enterprise (13 groups)

Collection (1 group)

MITRE / ATT&CK Framework / Enterprise / Collection (TA0009)
1 Groups

Security Level

Group Name	Security Level	Override	Rule Count
Input Capture (T1056) Adversaries may use methods of capturing user input to obtain credentials or collect inf...	0000	↔	256 Include

Groep beveiligingsregels bewerken

11. Kies bijvoorbeeld beveiligingsniveau 3 in het Edit Security Level venster en klik Saveop.

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

Beveiligingsniveau

12. Klik onder **Enterprise** om het **Initial Access** uit te vouwen.

13. Klik onder **Initial Access**, klik **Exploit Public-Facing Application**, dat is de laatste bladgroep.

The screenshot shows the 'Group Overrides' section of a security management console. The left sidebar lists various rule groups under 'Initial Access', with 'Exploit Public-Facing Application' selected. The main panel displays a table of rules for this group, including their names, descriptions, security levels, and 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...	○○○○			

Groep voor eerste toegang

14. Klik op **View Rules in Rule Overrides** knop om de verschillende regels, regeldetails, regelacties, enzovoort voor de verschillende regels te bekijken.

This group does not contain any children.

0 Groups / Group contains 8783 rules

[View Rules in Rule Overrides](#)

Regels in regeloverschrijvingen

15. Klik op de **Recommendations** laag en klik vervolgens **Start** om te beginnen met het gebruik van Cisco-aanbevolen regels. U kunt de aanbevelingen voor de inbraakregel gebruiken om kwetsbaarheden aan te pakken die zijn gekoppeld aan host-assets die in het netwerk zijn gedetecteerd. Meer informatie.

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](#)

Aanbevelingen

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. Klik op **Summary**laag voor een holistische weergave van de huidige wijzigingen in het beleid. U kunt de regelverdeling van het beleid, groepsoverschrijvingen, regeloverschrijvingen, enzovoort bekijken.

The screenshot shows the 'Summary' page in the Cisco interface. At the top, there is a navigation bar with tabs: Base Policy, Group Overrides, Recommendations (Not in use), Rule Overrides, and Summary (highlighted). Below the navigation bar, the 'Summary' section is divided into several panels:

- Rule Distribution:** A bar chart showing the distribution of rules. The data is as follows:

Category	Count
Alert	645
Block	10879
Disabled	33478
Others	5067
- Active Rules:** 16591
- Overridden Rules:** 4 (with a 'View Effective Policy' button)
- Disabled Rules:** 33478
- Total Rules:** 50069

On the right side, there is a 'Report and Exporting' section with buttons for 'Generate Report' and 'Export Policy'.

Below the main summary, there are three more panels:

- Base Configuration:** Base Policy: Balanced Security and Connectivity
- Recommendations:** Usage: Not in use (highlighted in orange) Turn on recommendations
- Group Overrides:** Total 2 group overrides:
 - Non-Application Layer Protocol
 - Malicious File
- Rule Overrides:** Total 4 rule overrides:

Rule ID	Action
1:62647	Block → Alert
1:61683	Drop → Alert
1:61681	Drop → Block
1:61684	Drop → Drop

Samenvatting van het beleid

Inbraakgebeurtenissen bekijken

U kunt de MITRE ATT&CK-technieken en regelgroepen bekijken in de inbraakgebeurtenissen in de Classic Event Viewer en Unified Event Viewer. Talos biedt mappings van Snort-regels (GID:

SID) naar MITRE ATT & CK-technieken en regelgroepen. Deze mappings worden geïnstalleerd als onderdeel van het Lightweight Security Package (LSP).

Voordat u begint, moet het beleid voor indringing en toegangscontrole worden geïmplementeerd om gebeurtenissen te detecteren en te registreren die zijn geactiveerd door de regels van Snort.

1. Klik **Analysis > Intrusions > Events** erop.
2. Klik op de **Table View of Events** tabblad zoals weergegeven in de afbeelding.

	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

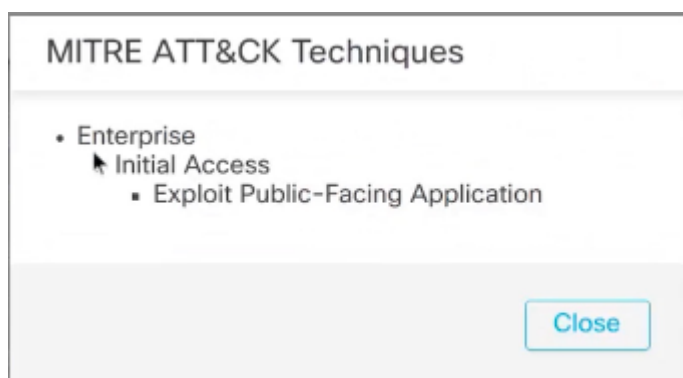
Gebeurtenissen

3. In de **MITRE ATT&CK** Column header, kunt u de technieken voor een inbraak evenement te zien.

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

Kolomkop mijter

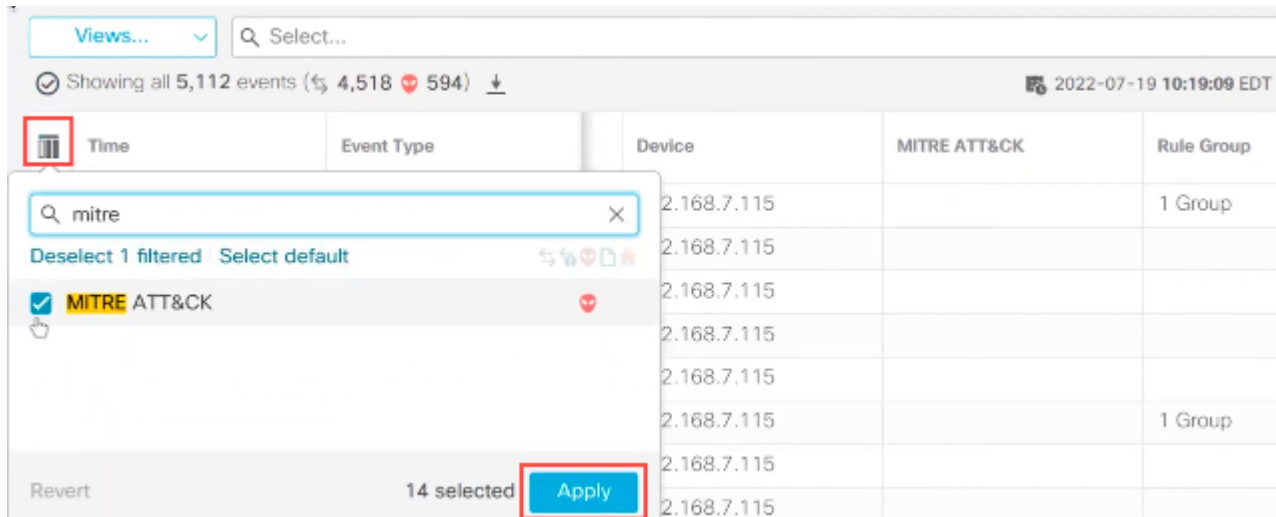
4. Klik op **1 Technique** om de MITER ATT&CK-technieken te bekijken, zoals weergegeven in deze figuur. In dit voorbeeld, **Exploit Public-Facing Application** is de techniek.



5. Klik **Close** erop.

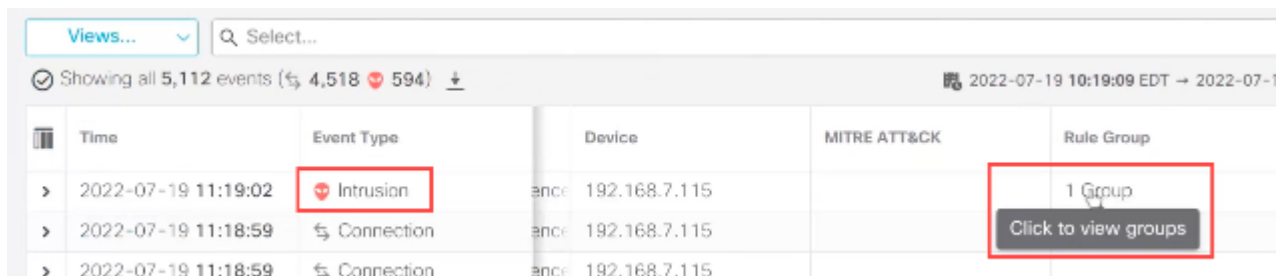
6. Klik **Analysis > Unified Events** erop.

7. U kunt op het kolomselectie pictogram klikken om de **MITRE ATT&CK** en **Rule Group** kolommen in te schakelen.



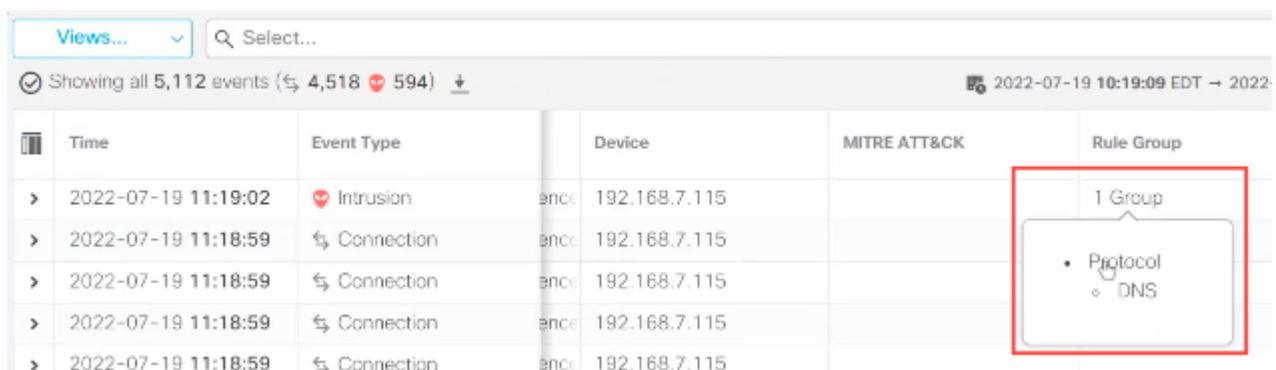
Schakel de Mitre-aanval in

8. Zoals in het voorbeeld hier wordt getoond, werd de inbreuk veroorzaakt door een gebeurtenis die aan één regelgroep is toegewezen. Klik **1 Group** onder de **Rule Group** kolom.



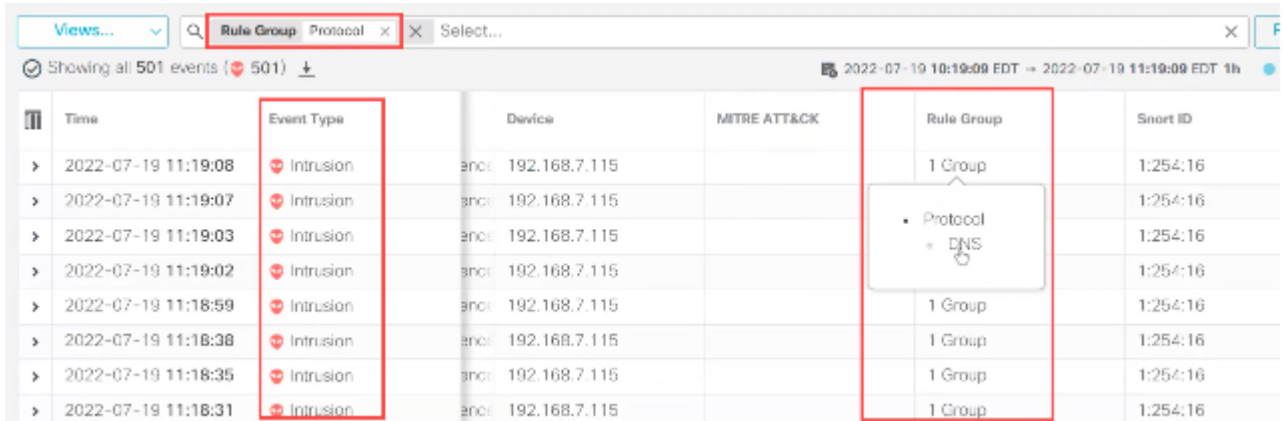
Regelgroep

9. Als voorbeeld kunt u **Protocol** bekijken, dat de bovenliggende regelgroep is, en de **DNS**-regelgroep eronder.



Bekijk protocol

10. U kunt klikken Protocol om te zoeken naar alle inbraakgebeurtenissen met ten minste één regelgroep, dat wil zeggen Protocol > DNS . De zoekresultaten worden weergegeven, zoals weergegeven in het voorbeeld hier.



The screenshot shows a security event log interface. At the top, there is a search bar with the text 'Rule Group Protocol' and a dropdown menu showing 'Protocol > DNS'. Below the search bar, there is a table with columns: Time, Event Type, Device, MITRE ATT&CK, Rule Group, and Smart ID. The table contains several rows of intrusion events. A red box highlights the 'Event Type' column, and another red box highlights the 'Rule Group' column. A dropdown menu is open over the 'Rule Group' column, showing 'Protocol > DNS'.

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

Regelgroepprotocol

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.