

MITER-Framework zum Anzeigen und Bekämpfen potenzieller Bedrohungen in sicheren FMCs

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Vorteile des MITER-Frameworks](#)

[Anzeigen des MITER-Frameworks in Ihrer Richtlinie für Sicherheitsrisiken](#)

[Angriffsereignisse anzeigen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie mithilfe des MITER-Frameworks potenzielle Bedrohungen in einem sicheren FirePOWER Management Center (FMC) anzeigen und darauf reagieren können.

Hintergrundinformationen

Das MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework ist eine umfassende Wissensbasis und Methodik, die Einblicke in die Taktiken, Techniken und Verfahren (TTPs) bietet, die von Angreifern verteilt werden, um Systeme zu beschädigen. ATT&CK ist in Matrizen zusammengefasst, die jeweils ein Betriebssystem oder eine bestimmte Plattform darstellen. Jede Stufe eines Angriffs wird als "Taktik" bezeichnet und den spezifischen Methoden zugeordnet, mit denen diese Stufen erreicht werden. Diese werden als "Techniken" bezeichnet.

Zu jeder Technik im ATT&CK-Framework gehören Informationen über die Technik, zugehörige Verfahren, mögliche Abwehrmechanismen und Erkennungen sowie Beispiele aus der Praxis. Das MITER ATT&CK-Framework umfasst auch Gruppen, die sich auf Bedrohungsgruppen, Aktivitätsgruppen oder Bedrohungsakteure beziehen, basierend auf den von ihnen verwendeten Taktiken und Techniken. Durch die Verwendung von Gruppen hilft das Framework, Verhaltensweisen zu kategorisieren und zu dokumentieren.

Weitere Informationen zu MITER finden Sie unter <https://attack.mitre.org>.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse von Snort
- Sicheres FMC
- Sicherer Schutz vor Bedrohungen mit Firepower (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Dieses Dokument gilt für alle FirePOWER-Plattformen
- Sichere FTD mit Softwareversion 7.3.0
- Secure FirePOWER Management Center Virtual (FMC) mit Softwareversion 7.3.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Vorteile des MITER-Frameworks

- MITER-Taktiken, -Techniken und -Prozeduren (TTPs) werden zu Angriffsversuchen hinzugefügt, die es Administratoren ermöglichen, auf Datenverkehr basierend auf dem MITER ATT&CK-Framework (Adversary Tactics Techniques and Common Knowledge) zu reagieren. So können Administratoren den Datenverkehr präziser anzeigen und behandeln und Regeln nach Schwachstellentyp, Zielsystem oder Bedrohungskategorie gruppieren.
- Sie können Intrusionsregeln nach dem MITER ATT&CK Framework organisieren. Auf diese Weise können Sie Richtlinien entsprechend der Taktiken und Techniken der Angreifer anpassen.

Anzeigen des MITER-Frameworks in Ihrer Richtlinie für Sicherheitsrisiken

Mit dem MITER-Framework können Sie durch Ihre Zugriffsregeln navigieren. MITER ist nur eine weitere Kategorie von Regelgruppen und Teil der Talos-Regelgruppen. Die Regelnavigation für mehrere Ebenen von Regelgruppen wird unterstützt, was mehr Flexibilität und eine logische Gruppierung von Regeln ermöglicht.

1. Wählen Sie `Policies > Intrusion`.
2. Stellen Sie sicher, dass die `Intrusion Policies` Registerkarte ausgewählt ist.
3. Klicken Sie `Snort 3 Version` neben der Richtlinie für Sicherheitsrisiken, die Sie anzeigen oder bearbeiten möchten. Schließen Sie das sich öffnende Snort-Hilfshandbuch.
4. Klicken Sie auf die `Group Overrides` Ebene.

Die `Group Overrides` Ebene listet alle Kategorien von Regelgruppen in einer hierarchischen Struktur

auf. Sie können zu der letzten Blattregelgruppe in jeder Regelgruppe wechseln.

< 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. unter Group Overrides: All wird in der Dropdown-Liste ausgewählt, sodass alle Regelgruppen für die Richtlinie für Sicherheitsrisiken im linken Bereich angezeigt werden.

7. Klicken Sie MITRE im linken Fensterausschnitt.



Anmerkung: Für dieses Beispiel ist MITER ausgewählt. Je nach Ihren spezifischen Anforderungen können Sie jedoch die Regelgruppe Regelkategorien oder eine andere Regelgruppe und die darunterliegenden nachfolgenden Regelgruppen auswählen. Alle Regelgruppen verwenden das 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 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. Klicken Sie unter MITRE auf Framework, um es zu erweitern ATT&CK.

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) 1

ATT&CK Framework (1 group) 1

Enterprise (13 groups) 1

MITRE / ATT&CK Framework 1 Groups

Group Name Security Level

9. Klicken Sie unter ATT&CK Framework auf Enterprise, um es zu erweitern.

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) 1

ATT&CK Framework (1 group) 1

Enterprise (13 groups) 1

MITRE / ATT&CK Framework / Enterprise 13 Groups

Group Name

10. Klicken Sie Edit () neben der Sicherheitsstufe der Regelgruppe, um Massenänderungen an der Sicherheitsstufe für alle zugeordneten Regelgruppen unter der Enterprise Regelgruppenkategorie

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) 1

ATT&CK Framework (1 group) 1

Enterprise (13 groups) 1

Collection (1 group) 1

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

Security Level **1**

Group Name	Security Level	Override	Rule Count
Input Capture (T1056) Adversaries may use methods of capturing user input to obtain credentials or collect inf...	1	⊞	256 Include

Sicherheitsregelgruppe bearbeiten

11. Wählen Sie als Beispiel Sicherheitsstufe 3 im Fenster aus Edit Security Level, und klicken Sie auf 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

Sicherheitsstufe

12. Unter Enterprise, klicken Sie, Initial Access um es zu erweitern.

13. Unter Initial Access, klicken Sie auf Exploit Public-Facing Application, die letzte Leaf-Gruppe ist.

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
Exploit Public-Facing Application (T1190) Adversaries may attempt to take advantage of a weakness in an Internet-facing comput...	○○○○	⊖	11976
External Remote Services (T1133) Adversaries may leverage external-facing remote services to initially access and/or per...	○○○○	⊖	443
Phishing (T1566) Adversaries may send phishing messages to gain access to victim systems. All forms o...	○○○○	⊖	304
Valid Accounts (T1078) Adversaries may obtain and abuse credentials of existing accounts as a means of gaini...	○○○○		

Erste Zugriffsgruppe

14. Klicken Sie auf **View Rules in Rule Overrides** um die verschiedenen Regeln, Regeldetails, Regelaktionen usw. für die verschiedenen Regeln anzuzeigen.

This group does not contain any children.

0 Groups / Group contains 8783 rules

[View Rules in Rule Overrides](#)

Regeln in Regelüberschreibungen

15. Klicken Sie auf **Recommendations** Ebene aus, und klicken Sie dann auf **Start**, um die von Cisco empfohlenen Regeln zu verwenden. Mithilfe der Empfehlungen für Angriffsregeln können Sie Schwachstellen identifizieren, die mit Hostressourcen im Netzwerk verbunden sind. finden Sie weitere Informationen.

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](#)

Empfehlungen

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. Klicken Sie auf `Summary` um einen ganzheitlichen Überblick über die aktuellen Richtlinienänderungen zu erhalten. Sie können die Regelverteilung der Richtlinie, Gruppenüberschreibungen, Regelüberschreibungen usw. anzeigen.

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

Richtlinienübersicht

Angriffseignisse anzeigen

Sie können die MITER ATT&CK-Techniken und Regelgruppen in der klassischen Ereignisanzeige und in der einheitlichen Ereignisanzeige in den Angriffseignissen anzeigen. Talos stellt

Zuordnungen von Snort-Regeln (GID:SID) zu MITER ATT&CK-Techniken und Regelgruppen bereit. Diese Zuordnungen werden als Teil des Lightweight Security Package (LSP) installiert.

Bevor Sie beginnen, müssen Richtlinien für Sicherheitsrisiken und die Zugriffskontrolle bereitgestellt werden, um von Snort-Regeln ausgelöste Ereignisse zu erkennen und zu protokollieren.

1. Klicken Sie auf `Analysis > Intrusions > Events`.
2. Klicken Sie auf das `Table View of Events` angezeigt, wie im Bild dargestellt.

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

No Search Constraints [\(Edit Search\)](#)

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

Jump to...

	<input type="checkbox"/>	Time ×	Priority ×	Impact ×	Inline Result ×	Reason ×	Source IP ×	Source Country ×	Destination IP ×
▼	<input type="checkbox"/>	2022-07-19 11:17:10	high	2	Would block	Interface in Passive or Tap mode	192.168.0.227		146.112.255.69
▼	<input type="checkbox"/>	2022-07-19 11:17:06	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.4.106
▼	<input type="checkbox"/>	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
▼	<input type="checkbox"/>	2022-07-19 11:17:05	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.7.241

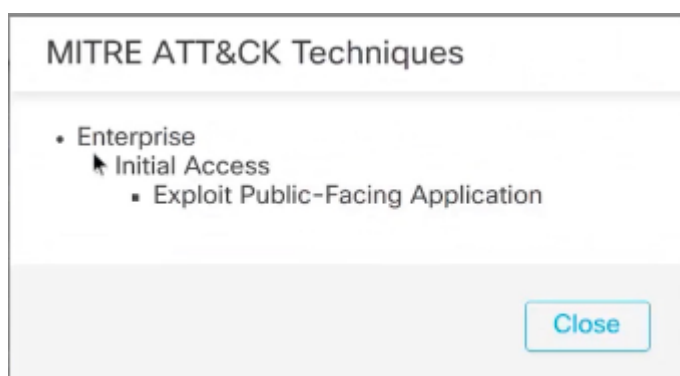
Events

3. Im `MITRE ATT&CK` Spaltenüberschrift finden Sie die Techniken für ein Angriffsereignis.

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

Gehungsspaltenüberschrift

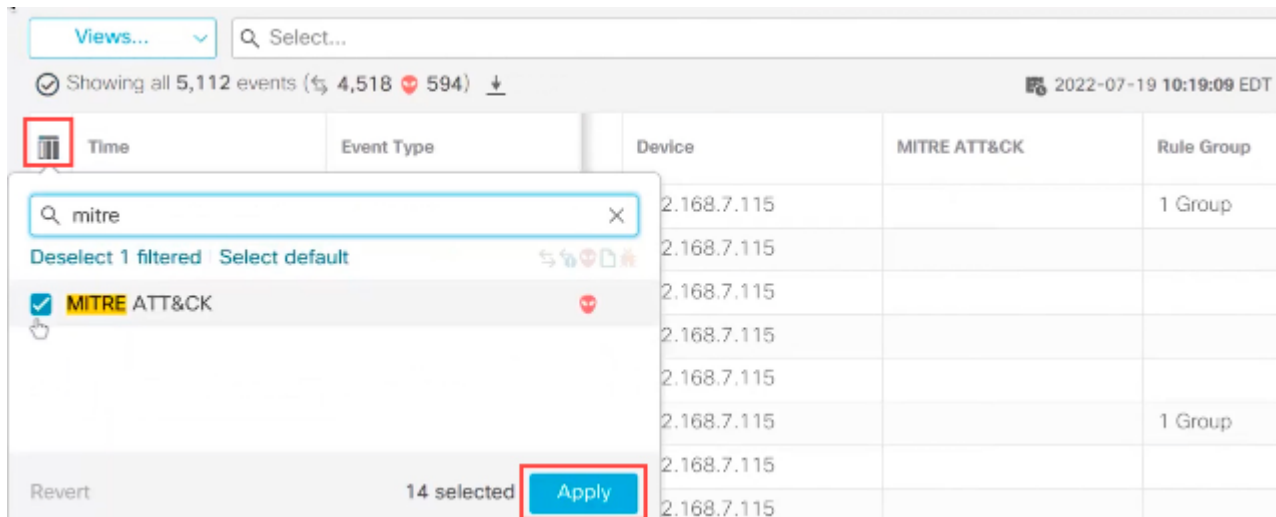
4. Klicken Sie `1 Technique` um die MITER ATT&CK-Techniken anzuzeigen, wie in dieser Abbildung dargestellt. In diesem Beispiel `Exploit Public-Facing Application` ist die Technik.



5. Klicken Sie auf **Close**.

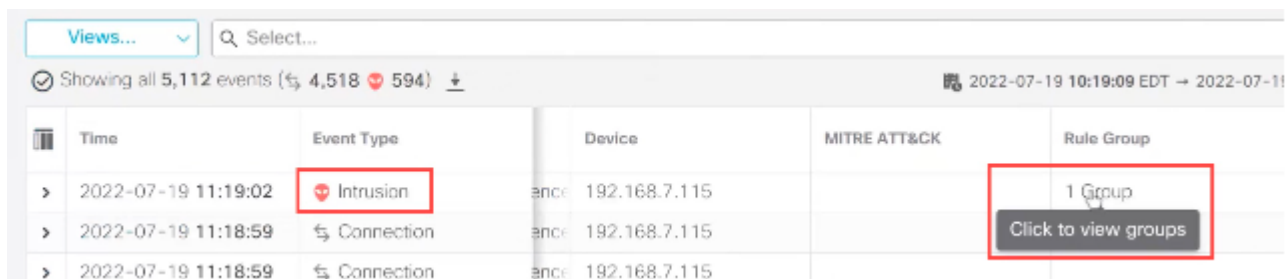
6. Klicken Sie auf **Analysis > Unified Events**.

7. Sie können auf das Symbol für die Spaltenauswahl klicken, um die **MITRE ATT&CK** und die **Rule Group** Spalten zu aktivieren.



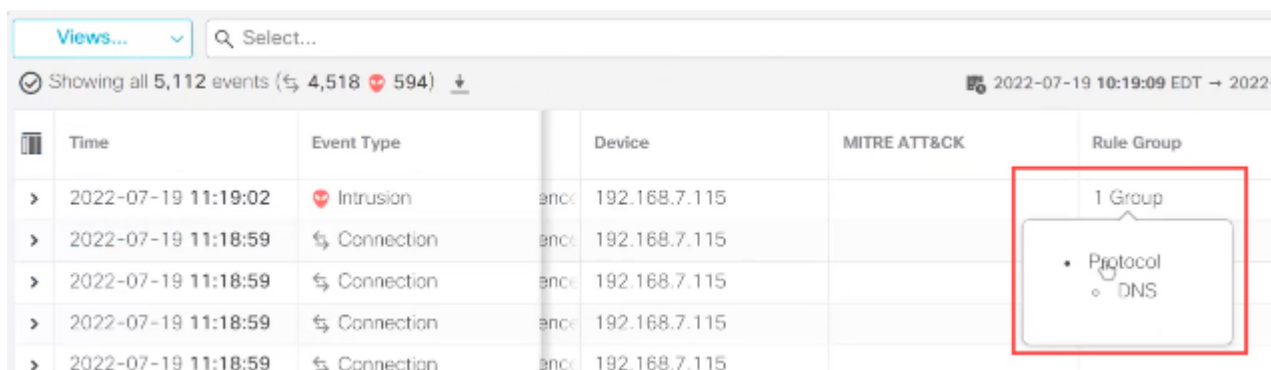
Gehrungsangriff aktivieren

8. Wie im vorliegenden Beispiel gezeigt, wurde das Angriffsereignis durch ein Ereignis ausgelöst, das einer Regelgruppe zugeordnet ist. Klicken Sie **1 Group** unter **Rule Group** Spalte.



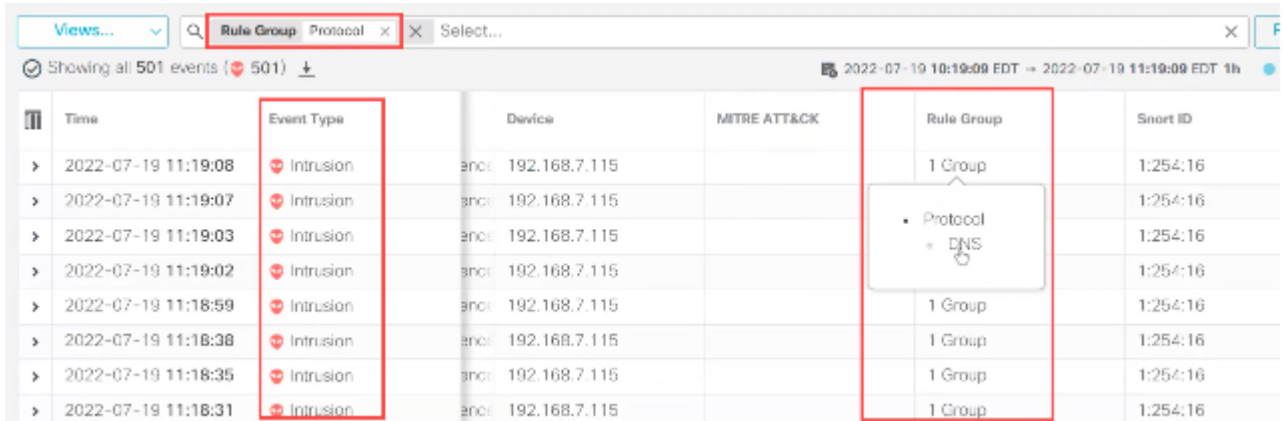
Regelgruppe

9. Als Beispiel können Sie das Protokoll, das die übergeordnete Regelgruppe darstellt, und die darunter liegende DNS-Regelgruppe anzeigen.



Protokoll anzeigen

10. Klicken Sie auf, Protocolum nach allen Angriffsereignissen zu suchen, die über mindestens eine Regelgruppe verfügen, d. h. Protocol > DNS . Die Suchergebnisse werden angezeigt, wie im Beispiel hier gezeigt.



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

Regelgruppenprotokoll

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.