

Utilizzare il framework MITER per visualizzare e agire sulle minacce potenziali in un FMC protetto

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Vantaggi del framework MITER](#)

[Visualizzare il framework MITER nei criteri per le intrusioni](#)

[Visualizza eventi di intrusione](#)

Introduzione

Questo documento descrive come utilizzare il framework MITER per visualizzare e agire su potenziali minacce in un centro di gestione sicura di Firepower (FMC).

Premesse

Il framework MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) è un'ampia base di conoscenze e metodologie che fornisce informazioni sulle tattiche, le tecniche e le procedure (TTP) distribuite da attori della minaccia che mirano a danneggiare i sistemi. ATT&CK viene compilato in matrici che rappresentano ciascuna sistema operativo o una particolare piattaforma. Ogni fase di un attacco, nota come "tattica", è mappata ai metodi specifici utilizzati per raggiungere quelle fasi, note come "tecniche".

Ogni tecnica nel framework ATT&CK è accompagnata da informazioni sulla tecnica, le procedure associate, le probabili difese e rilevamenti, ed esempi reali. La struttura MITER ATT&CK incorpora anche Gruppi per fare riferimento a gruppi di minacce, gruppi di attività o attori di minaccia in base alla serie di tattiche e tecniche impiegate. Tramite l'utilizzo dei gruppi, il framework semplifica la categorizzazione e la documentazione dei comportamenti.

Per ulteriori informazioni su MITER, visitare il sito Web all'indirizzo <https://attack.mitre.org>.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Snort
- Secure FMC
- Secure Firepower Threat Defense (FTD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Questo documento è valido per tutte le piattaforme Firepower
- Secure FTD con software versione 7.3.0
- Secure Firepower Management Center Virtual (FMC) con software versione 7.3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Vantaggi del framework MITER

- Tattiche, tecniche e procedure MITER (TTP) vengono aggiunte agli eventi di intrusione che consentono agli amministratori di agire sul traffico in base alla struttura ATT&CK (Adversary Tactics Techniques and Common Knowledge) di MITER. Ciò consente agli amministratori di visualizzare e gestire il traffico con maggiore granularità e di raggruppare le regole per tipo di vulnerabilità, sistema di destinazione o categoria di minaccia.
- È possibile organizzare le regole di intrusione in base al framework ATT&CK MITER. In questo modo è possibile personalizzare i criteri in base a tattiche e tecniche specifiche.

Visualizzare il framework MITER nei criteri per le intrusioni

Il framework MITER consente di spostarsi tra le regole di intrusione. MITER è solo un'altra categoria di gruppi di regole e fa parte dei gruppi di regole Talos. È supportata la navigazione tra le regole per diversi livelli di gruppi di regole, che offre maggiore flessibilità e raggruppamento logico delle regole.

1. Scegliere `Policies > Intrusion`.
2. Assicurarsi che la `Intrusion Policies` scheda sia selezionata.
3. Fare clic su `Snort 3 Version` accanto al criterio intrusione che si desidera visualizzare o modificare. Chiudere la guida di supporto Snort visualizzata.
4. Fare clic sul `Group Overrides` livello.

Il `Group Overrides` livello elenca tutte le categorie di gruppi di regole in una struttura gerarchica. È possibile passare all'ultimo gruppo di regole foglia in ogni gruppo di regole.

< 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. Nell'ambito Group Overrides, All è selezionato nell'elenco a discesa, in modo che tutti i gruppi di regole per il criterio intrusione siano visibili nel riquadro sinistro.

7. Fare clic su MITRE nel riquadro di sinistra.



Nota: Per questo esempio, è selezionato MITER, ma a seconda dei requisiti specifici, è possibile scegliere il gruppo di regole Categorie regole o qualsiasi altro gruppo di regole e i gruppi di regole successivi al suo interno. Tutti i gruppi di regole utilizzano il framework MITER.

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. In MITRE, fare clic su ATT&CK Framework per espanderlo.

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. In ATT&CK Framework, fare clic su Azienda per espanderla.

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. Fare clic su Edit () accanto al livello di protezione del gruppo di regole per apportare modifiche di massa al livello di protezione per tutti i gruppi di regole associati nel gruppo Enterprise categoria del gruppo di regole.

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 **3**

Group Name	Security Level	Override	Rule Count
Input Capture (T1056) Adversaries may use methods of capturing user input to obtain credentials or collect inf...	3	⊞	256 Include

Modifica gruppo di regole di sicurezza

11. Ad esempio, scegliere il livello di protezione 3 nella Edit Security Level finestra e fare clic su 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

Livello di protezione

12. In Enterprise, fare clic Initial Access per espanderlo.

13. In Initial Access, fare clic su Exploit Public-Facing Application, che è l'ultimo gruppo foglia.

The screenshot shows the 'Group Overrides' section of a security management console. The top navigation bar includes 'Base Policy', 'Group Overrides' (selected), 'Recommendations' (Not in use), 'Rule Overrides', and 'Summary'. A status indicator shows 'Connected to Bangalore Duo - SSL'. The left sidebar shows a tree view of rule groups under 'Group Overrides' (101 items). The 'Initial Access' group is expanded, showing sub-groups: 'Drive-by Compromise', 'Exploit Public-Facing Application' (selected), 'External Remote Services', and 'Phishing'. The main panel displays the details for the 'MITRE / ATT&CK Framework / Enterprise / Initial Access (TA0001)' group, which contains 5 groups. A table lists the rules within this group:

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...	○○○○			

Gruppo di accesso iniziale

14. Fare clic sul pulsante **View Rules in Rule Overrides** per visualizzare le diverse regole, i dettagli delle regole, le azioni delle regole e così via per le diverse regole.

This group does not contain any children.

0 Groups / Group contains 8783 rules

[View Rules in Rule Overrides](#)

Regole in sostituzioni regole

15. Fare clic sul pulsante **Recommendations** e quindi fare clic su **Start** per iniziare a utilizzare le regole consigliate da Cisco. È possibile utilizzare i suggerimenti per le regole di intrusione per individuare le vulnerabilità associate agli asset host rilevati nella rete. Ulteriori informazioni.

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](#)

Consigli

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. Fare clic sul pulsante **Summary** per una visualizzazione olistica delle modifiche correnti al criterio. È possibile visualizzare la distribuzione delle regole del criterio, le sostituzioni di gruppo, le sostituzioni di regola e così via.

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

Riepilogo criteri

Visualizza eventi di intrusione

È possibile visualizzare le tecniche e i gruppi di regole ATT&CK MITER negli eventi di intrusione nel Visualizzatore eventi classico e nel Visualizzatore eventi unificato. Talos fornisce i mapping

dalle regole di tipo Snort (GID:SID) alle tecniche e ai gruppi di regole ATT&CK MITER. Questi mapping vengono installati come parte del Lightweight Security Package (LSP).

Prima di iniziare, è necessario distribuire i criteri di controllo delle intrusioni e degli accessi per rilevare e registrare gli eventi attivati dalle regole Snort.

1. Fare clic su [Analysis > Intrusions > Events](#).

2. Fare clic sul pulsante **Table View of Events** come mostrato nell'immagine.

	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

Eventi

3. Nel MITRE ATT&CK nell'intestazione di colonna è possibile visualizzare le tecniche per un evento intrusione.

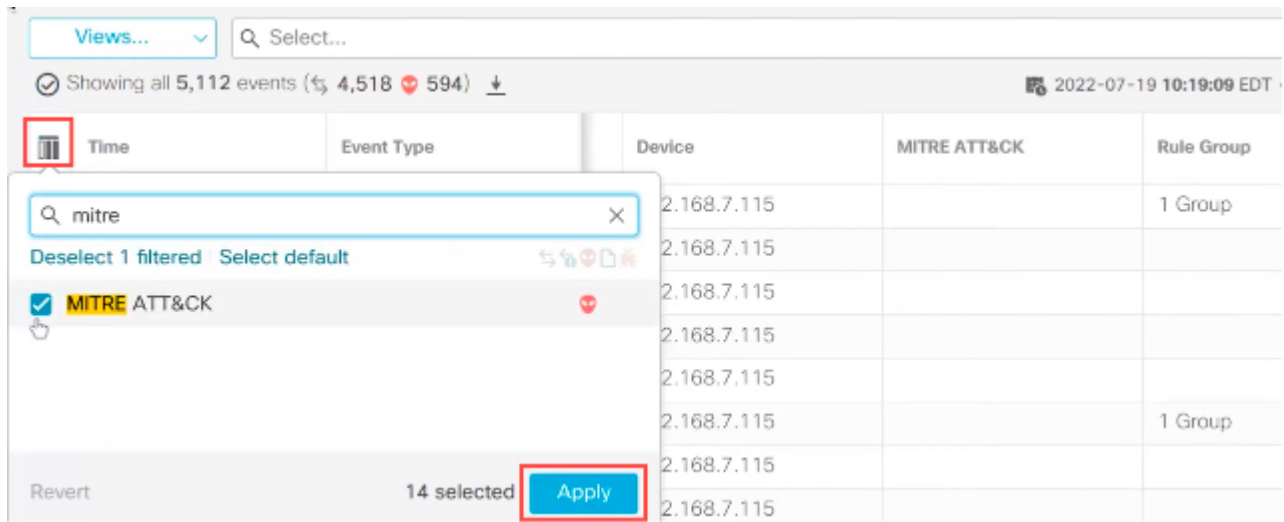
Access Control Policy	Access Control Rule	Network Analysis Policy	MITRE ATT&CK	Rule Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file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

Intestazione colonna Angoli

4. Fare clic **1 Technique** per visualizzare le tecniche ATT&CK di MITER, come illustrato nella figura riportata di seguito. In questo esempio, **Exploit Public-Facing Application** è la tecnica.

```
graph TD
  Enterprise[Enterprise] --> InitialAccess[Initial Access]
  InitialAccess --> ExploitPublicFacingApplication[Exploit Public-Facing Application]
```

- 5. Fare clic su Close.
- 6. Fare clic su Analysis > Unified Events.
- 7. È possibile fare clic sull'icona del selettore di colonne per abilitare le colonne MITRE ATT&CK e Rule Group.



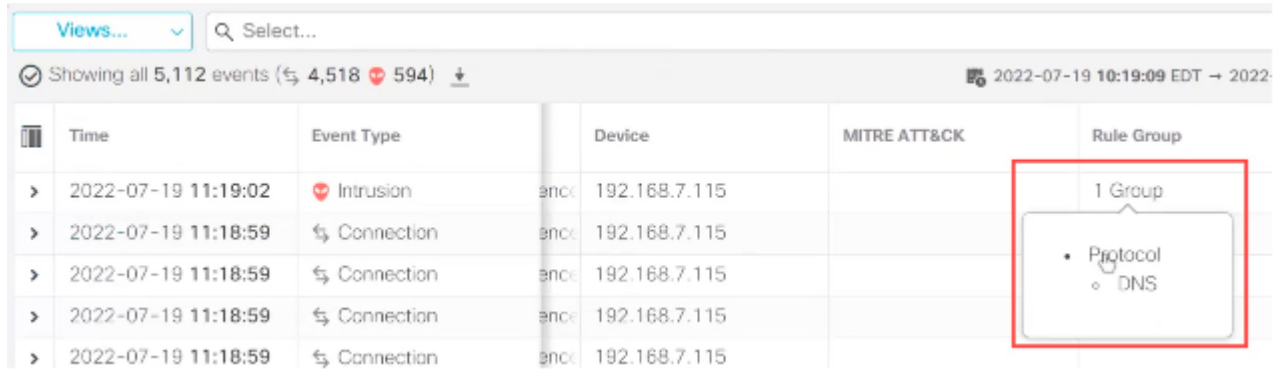
Abilita attacco a 45°

- 8. Come illustrato nell'esempio, l'evento intrusione è stato attivato da un evento mappato a un gruppo di regole. Fare clic 1 Group sotto Rule Group colonna.



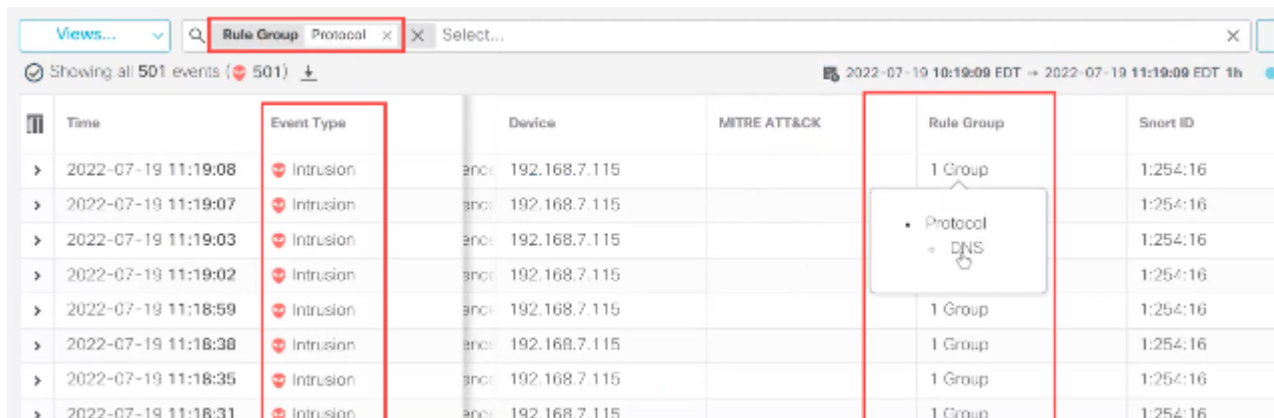
Gruppo di regole

- 9. Ad esempio, è possibile visualizzare il gruppo di regole Protocol, che è il gruppo di regole padre, e il gruppo di regole DNS sottostante.



Visualizza protocollo

10. È possibile fare clic su **Protocol** per cercare tutti gli eventi di intrusione che hanno almeno un gruppo di regole, ovvero **Protocol > DNS** . Vengono visualizzati i risultati della ricerca, come mostrato nell'esempio riportato di seguito.



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

Protocollo gruppo di regole

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).