

Utiliser le cadre MITER pour visualiser et agir sur les menaces potentielles dans Secure FMC

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Avantages du cadre MITER](#)

[Affichez l'infrastructure MITER dans votre politique d'intrusion](#)

[Afficher les événements d'intrusion](#)

Introduction

Ce document décrit comment utiliser le cadre MITER pour visualiser et agir sur les menaces potentielles dans un centre de gestion Firepower (FMC) sécurisé.

Informations générales

Le cadre MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) est une vaste base de connaissances et une méthodologie qui fournit des informations sur les tactiques, les techniques et les procédures (TTP) distribuées par les acteurs de la menace visant à nuire aux systèmes. ATT&CK est compilé en matrices qui représentent chacune des systèmes d'exploitation ou une plate-forme particulière. Chaque étape d'une attaque, appelée « tactique », est associée aux méthodes spécifiques utilisées pour atteindre ces étapes, appelées « techniques ».

Chaque technique du cadre ATT&CK est accompagnée d'informations sur la technique, les procédures associées, les défenses et détections probables, ainsi que des exemples concrets. Le cadre ATT&CK MITER intègre également des groupes pour désigner les groupes de menaces, les groupes d'activité ou les acteurs de la menace en fonction de l'ensemble des tactiques et des techniques qu'ils utilisent. En utilisant des groupes, l'infrastructure permet de catégoriser et de documenter les comportements.

Pour plus d'informations sur MITER, consultez la page <https://attack.mitre.org>.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de Snort
- FMC sécurisé
- Défense contre les menaces Firepower (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Ce document s'applique à toutes les plates-formes Firepower
- Secure FTD exécutant la version 7.3.0 du logiciel
- Secure Firepower Management Center Virtual (FMC) exécutant la version 7.3.0 du logiciel

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Avantages du cadre MITER

- Les Tactiques, Techniques et Procédures MITER sont ajoutées aux événements d'intrusion qui permettent aux administrateurs d'agir sur le trafic en fonction du cadre MITER ATT&CK (Adversary Tactics Techniques and Common Knowledge). Cela permet aux administrateurs d'afficher et de gérer le trafic avec plus de granularité, et ils peuvent regrouper les règles par type de vulnérabilité, système cible ou catégorie de menace.
- Vous pouvez organiser les règles d'intrusion en fonction de la structure ATT&CK MITER. Cela vous permet de personnaliser les stratégies en fonction des tactiques et des techniques spécifiques de l'attaquant.

Affichez l'infrastructure MITER dans votre politique d'intrusion

L'infrastructure MITER vous permet de naviguer dans vos règles d'intrusion. MITER n'est qu'une autre catégorie de groupes de règles et fait partie des groupes de règles Talos. La navigation des règles pour plusieurs niveaux de groupes de règles est prise en charge, ce qui offre plus de flexibilité et un regroupement logique des règles.

1. Sélectionnez `Policies > Intrusion`.
2. Assurez-vous que l'onglet `Intrusion Policies` est sélectionné.
3. Cliquez sur en regard de la stratégie d'intrusion que vous souhaitez afficher ou modifier. Fermez le guide d'aide Snort qui s'affiche.
4. Cliquez sur le `Group Overrides` calque.

La couche `Group Overrides` répertorie toutes les catégories de groupes de règles dans une structure hiérarchique. Vous pouvez passer au dernier groupe de règles feuille dans chaque groupe de règles.

< 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. En vertu de Group Overrides, veiller à ce All est sélectionné dans la liste déroulante, de sorte que tous les groupes de règles de la stratégie d'intrusion soient visibles dans le volet gauche.

7. Cliquez sur MITRE dans le volet de gauche.



Remarque : Dans cet exemple, MITER est sélectionné, mais selon vos besoins spécifiques, vous pouvez choisir le groupe de règles Catégories de règles ou tout autre groupe de règles et les groupes de règles suivants. Tous les groupes de règles utilisent le cadre 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

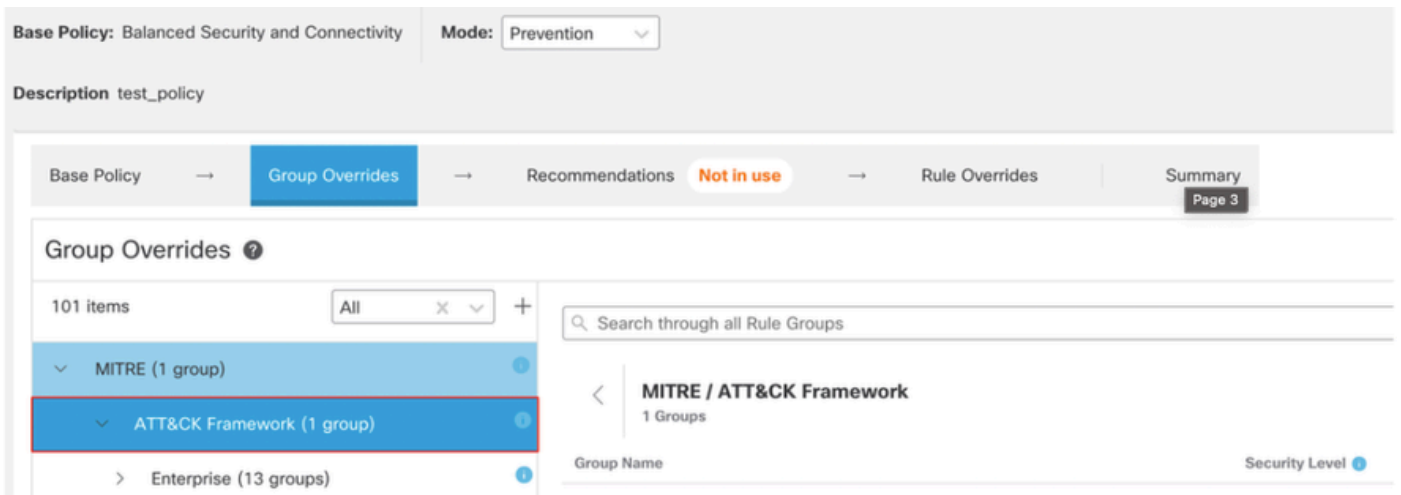
Rule Categories (9 groups) 1

Search through all Rule Groups

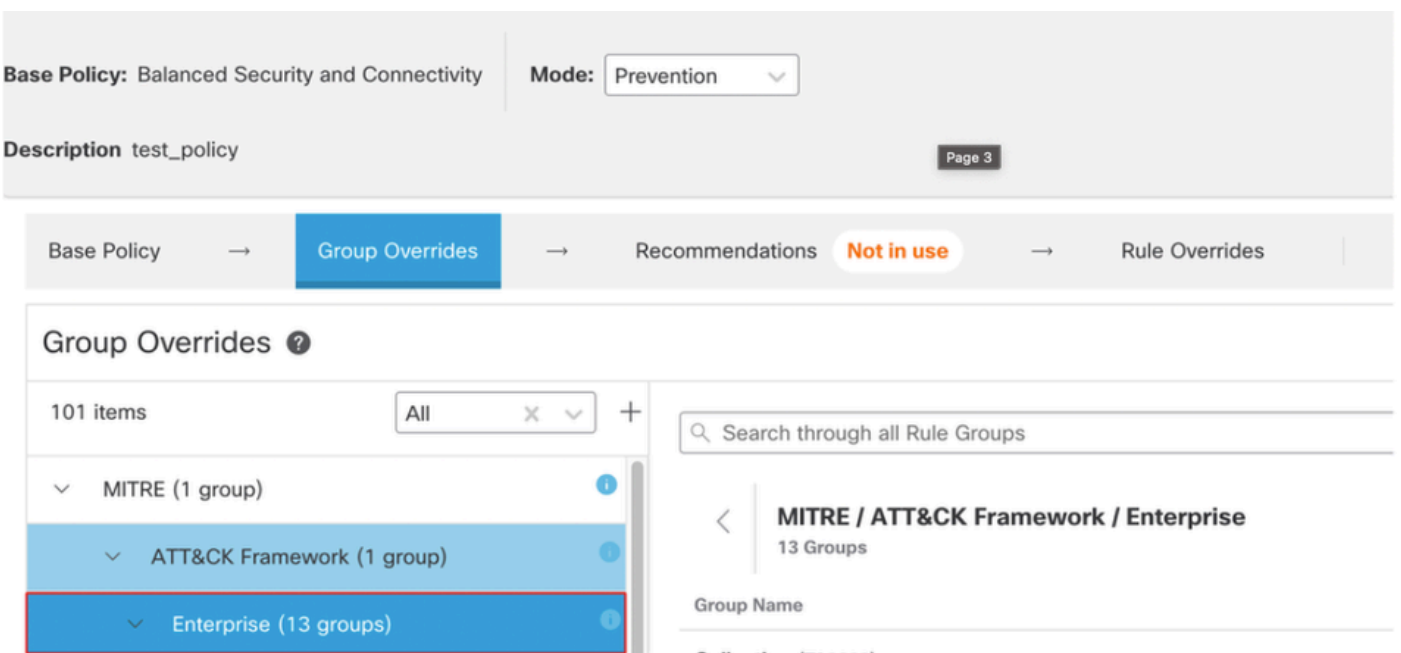
Rule Groups

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

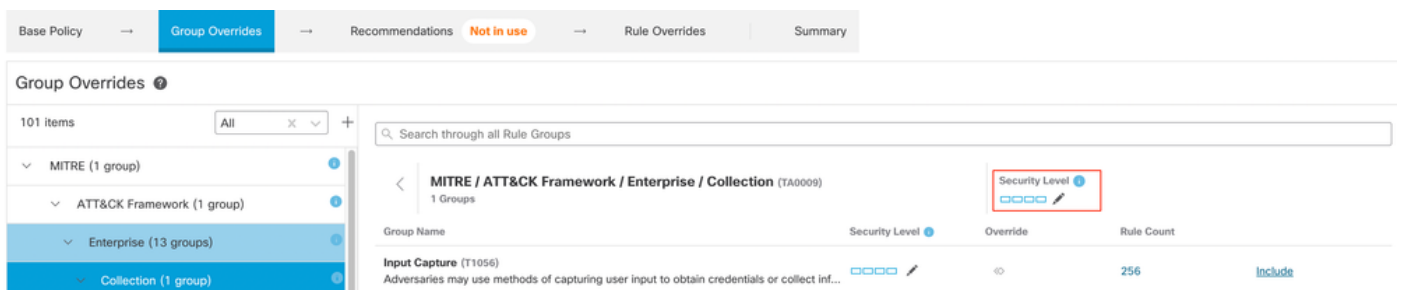
8. Sous MITRE, cliquez sur ATT&CK Framework pour le développer.



9. Sous ATT&CK Framework, cliquez sur Entreprise pour le développer.



10. Cliquez sur en Edit () regard du niveau de sécurité du groupe de règles pour apporter des modifications en bloc au niveau de sécurité de tous les groupes de règles associés sous l'onglet Enterprise catégorie de groupe de règles.



Modifier le groupe de règles de sécurité

11. Par exemple, choisissez le niveau de sécurité 3 dans la fenêtre, Edit Security Level puis cliquez sur 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

Niveau de sécurité

12. Sous Enterprise, cliquez Initial Access pour le développer.

13. Sous Initial Access, cliquez sur Exploit Public-Facing Application, qui est le dernier groupe de feuilles.

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...	□□□□			

Groupe d'accès initial

14. Cliquez sur le bouton **View Rules in Rule Overrides** pour afficher les différentes règles, les détails des règles, les actions de règle, etc. pour les différentes règles.

This group does not contain any children.

0 Groups / Group contains 8783 rules

[View Rules in Rule Overrides](#)

Règles dans les remplacements de règles

15. Cliquez sur le bouton **Recommendations** puis cliquez sur **Start** pour commencer à utiliser les règles recommandées par Cisco. Vous pouvez utiliser les recommandations de règles d'intrusion pour cibler les vulnérabilités associées aux ressources hôtes détectées sur le réseau. Pour plus d'informations.

The screenshot shows a navigation breadcrumb: Base Policy → Group Overrides → **Recommendations** (with a 'Not in use' status) → Rule Overrides → Summary. Below the breadcrumb, the page title is 'Cisco Recommended Rules'. The main content area contains the following text:

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

[Start](#)

Recommendations

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. Cliquez sur le bouton `Summary` pour une vue globale des modifications actuelles apportées à la stratégie. Vous pouvez afficher la répartition des règles de la stratégie, les remplacements de groupes, les remplacements de règles, etc.

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

Résumé de la stratégie

Afficher les événements d'intrusion

Vous pouvez afficher les techniques et les groupes de règles MITER ATT&CK dans les événements d'intrusion de l'Observateur d'événements classique et de l'Observateur

d'événements unifié. Talos fournit des mappages des règles Snort (GID:SID) aux techniques et groupes de règles MITER ATT&CK. Ces mappages sont installés dans le cadre du package de sécurité léger (LSP).

Avant de commencer, vous devez déployer des stratégies de contrôle d'accès et d'intrusion pour détecter et consigner les événements déclenchés par les règles Snort.

1. Cliquez sur `Analysis > Intrusions > Events`.
2. Cliquez sur le bouton `Table View of Events` comme illustré dans l'image.

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...

	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

Événements

3. Dans la `MITRE ATT&CK`, vous pouvez voir les techniques d'un événement d'intrusion.

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

En-tête de colonne mitre

4. Cliquez sur `1 Technique` pour afficher les techniques ATT&CK MITER, comme illustré dans cette figure. Dans cet exemple, `Exploit Public-Facing Application` est la technique.

MITRE ATT&CK Techniques

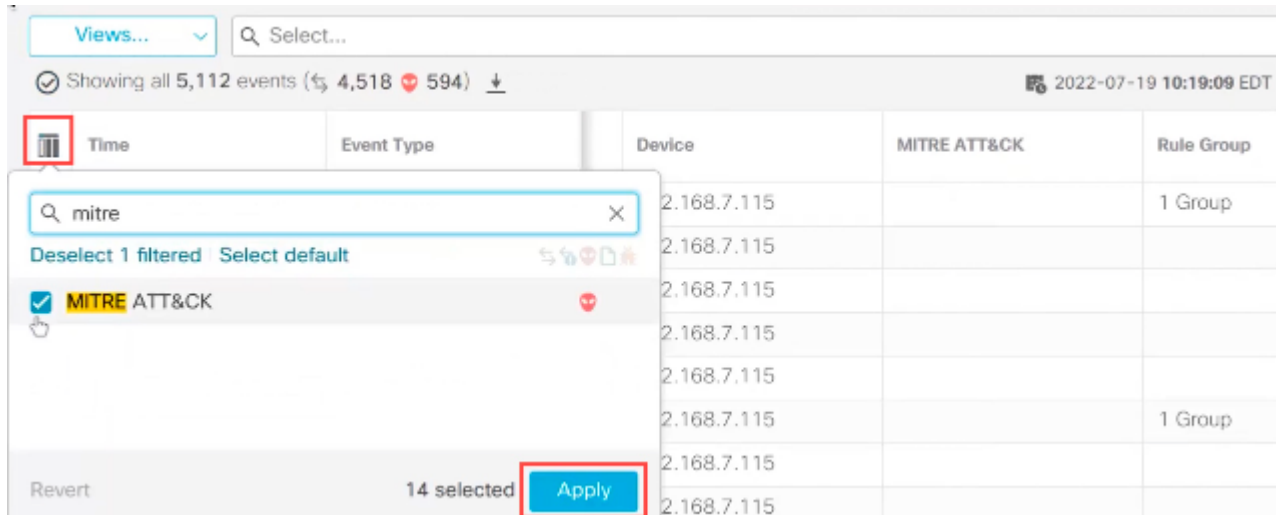
- Enterprise
 - Initial Access
 - Exploit Public-Facing Application

Close

5. Cliquez sur **Close**.

6. Cliquez sur **Analysis > Unified Events**.

MITRE ATT&CK 7. Vous pouvez cliquer sur l'icône de sélection de colonne pour activer les **Rule Group** colonnes et.



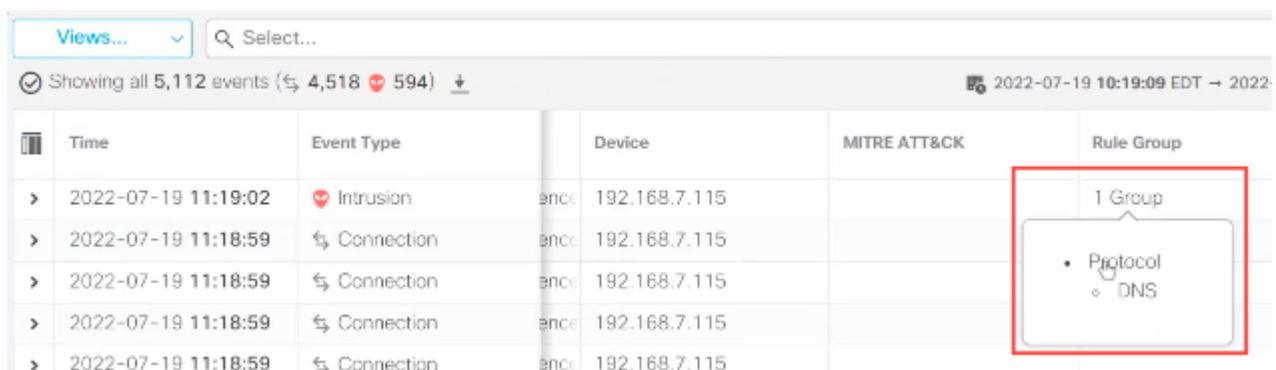
Activer l'attaque mitre

8. Comme l'illustre l'exemple ci-contre, l'événement d'intrusion a été déclenché par un événement mappé à un groupe de règles. Cliquez sur **1 Group** sous **Rule Group** colonne.



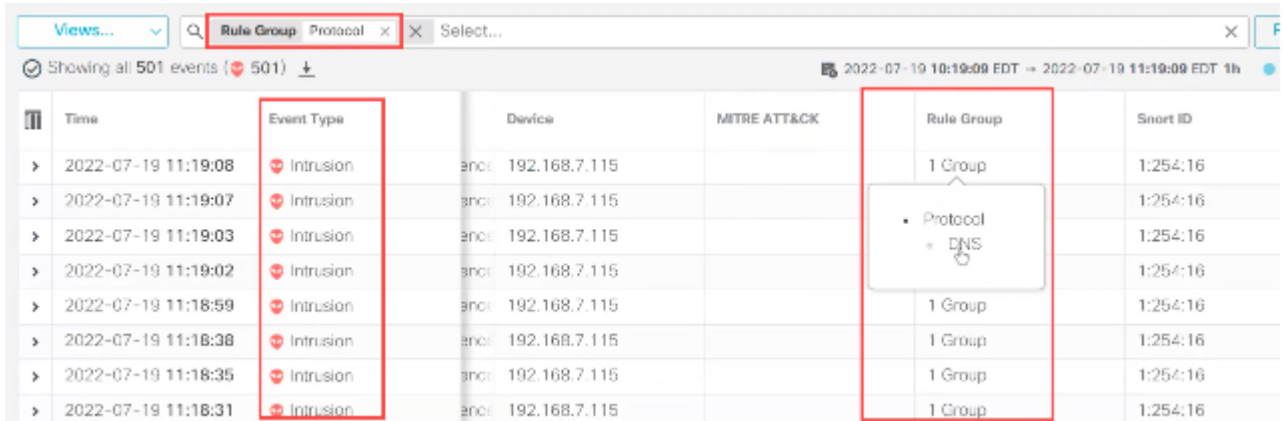
Groupe de règles

9. Par exemple, vous pouvez afficher le protocole, qui est le groupe de règles parent, et le groupe de règles DNS situé en dessous.



Afficher le protocole

10. Vous pouvez cliquer sur **Protocol** pour rechercher tous les événements d'intrusion qui ont au moins un groupe de règles, c'est-à-dire `Protocol > DNS`. Les résultats de la recherche s'affichent, comme illustré dans l'exemple ci-contre.



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

Protocole de groupe de règles

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.