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

Table des matières

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

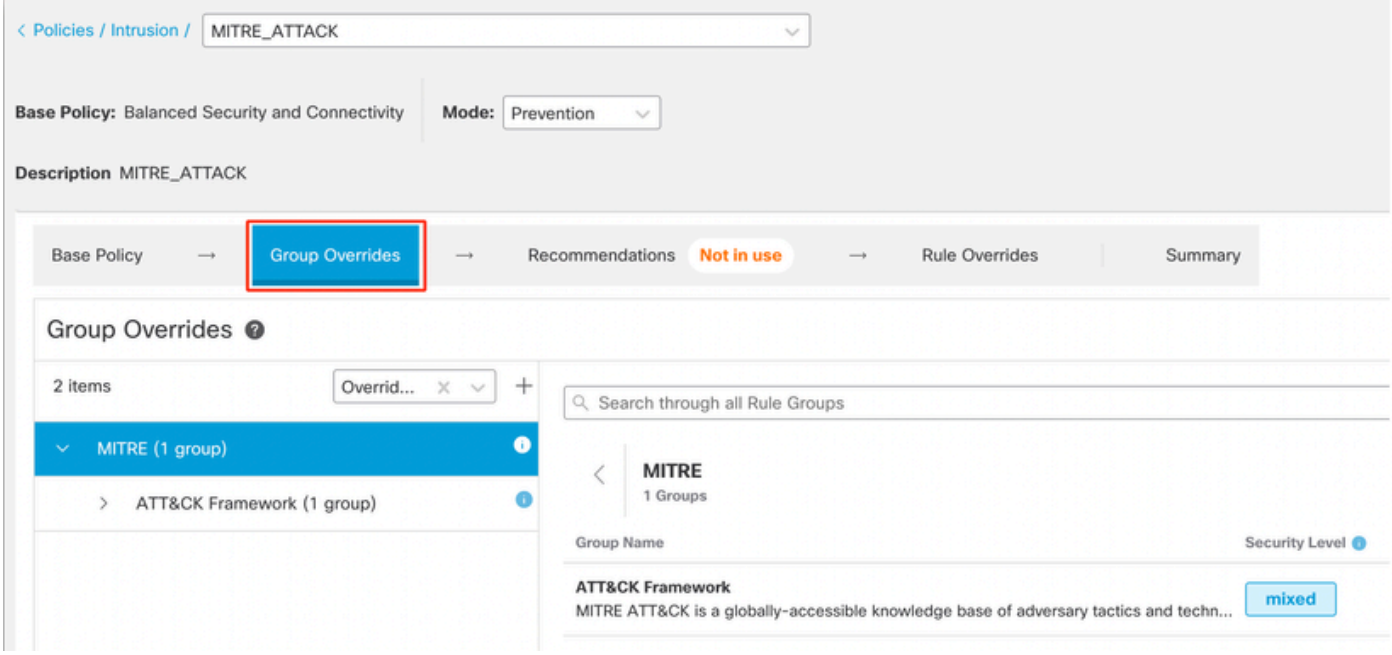
- Les Tactiques, Techniques et Procédures MITER sont ajoutées aux événements d'intrusion qui permettent aux administrateurs d'agir sur le trafic en fonction du cadre MITER ATT&CK (Adversary Tactics Techniques and Common Knowledge). Cela permet aux administrateurs d'afficher et de gérer le trafic avec 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' Intrusion Policiesonglet est sélectionné.
3. Cliquez sur en Snort 3 Versionregard 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 Overridescalque.

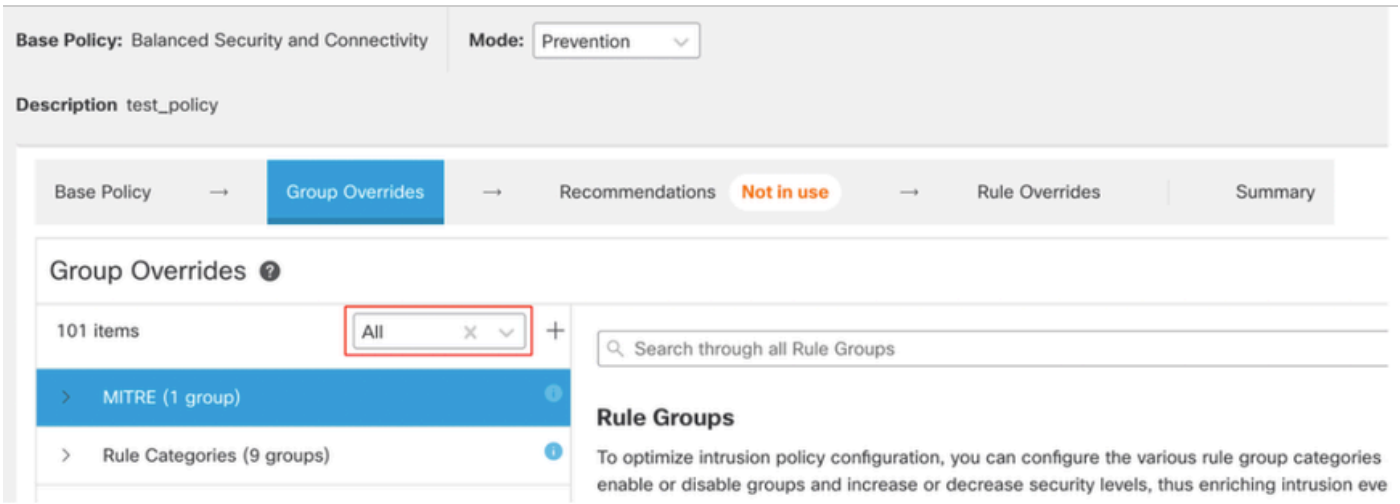
La Group Overridescouche répertorie toutes les catégories de groupes de règles dans une structure hiérarchique. Vous pouvez passer au dernier groupe de règles feuille dans chaque groupe de règles.



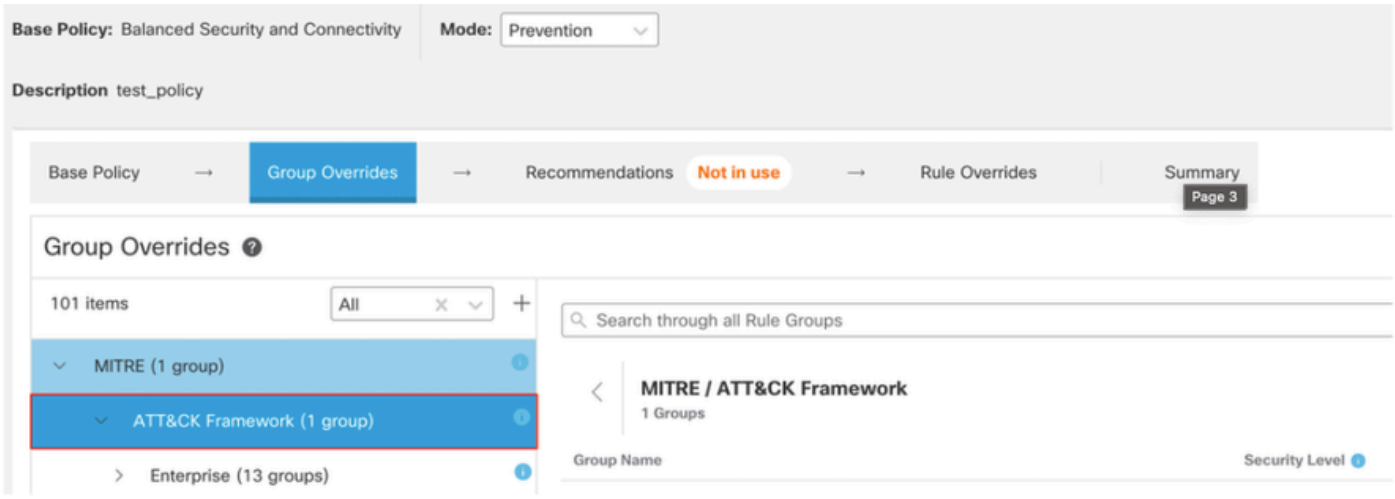
6. En vertu de Group Overrides, veiller à ce Allest sélectionné dans la liste déroulante, de sorte que tous les groupes de règles de la stratégie d'intrusion soient visibles dans le volet gauche.

7. Cliquez sur MITREdans le volet de gauche.

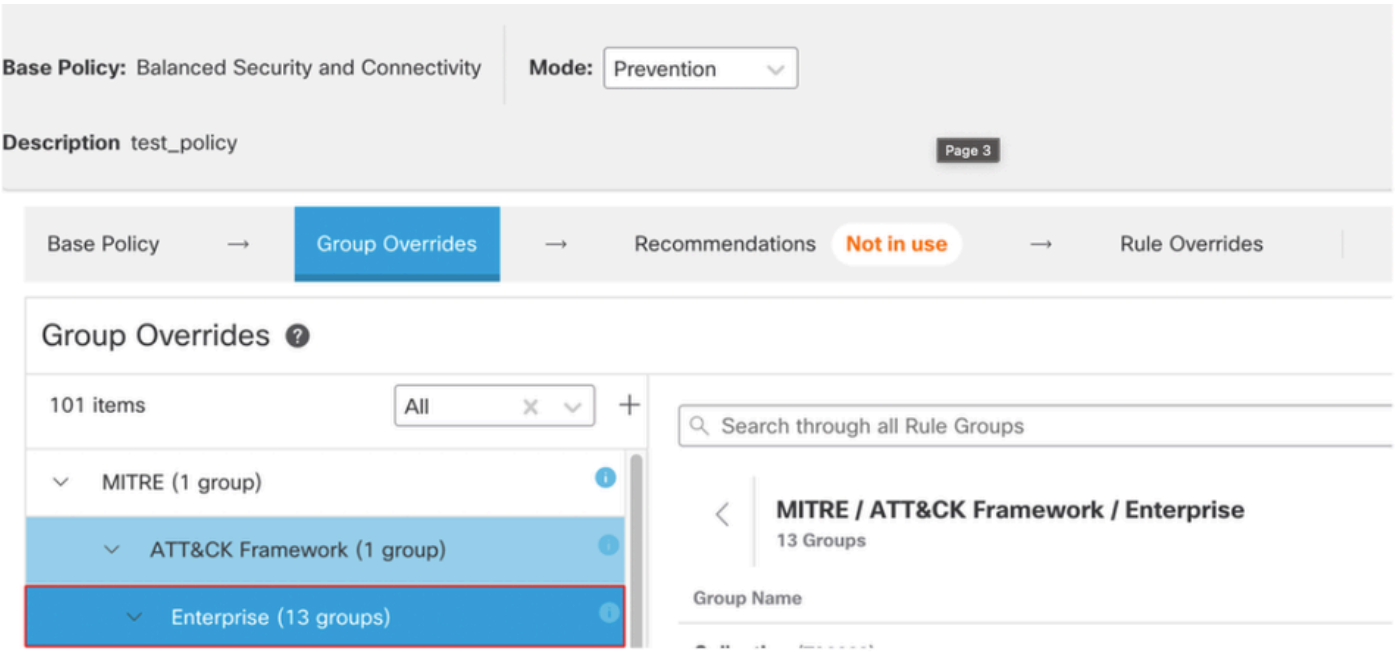
Remarque : Dans cet exemple, MITER est sélectionné, mais selon vos besoins spécifiques, vous pouvez choisir le groupe de règles Catégories de règles ou tout autre groupe de règles et les groupes de règles suivants. Tous les groupes de règles utilisent le cadre MITER.



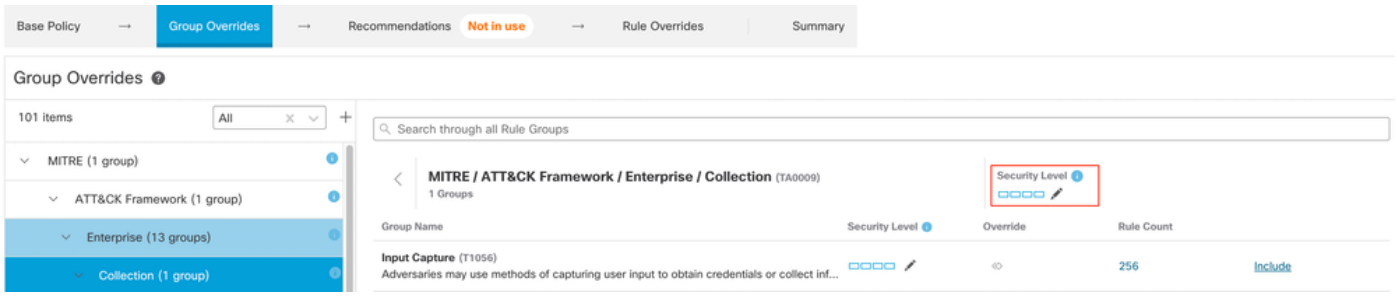
8. SousMITRE, cliquez sur ATT&CK Framework pour le développer.



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

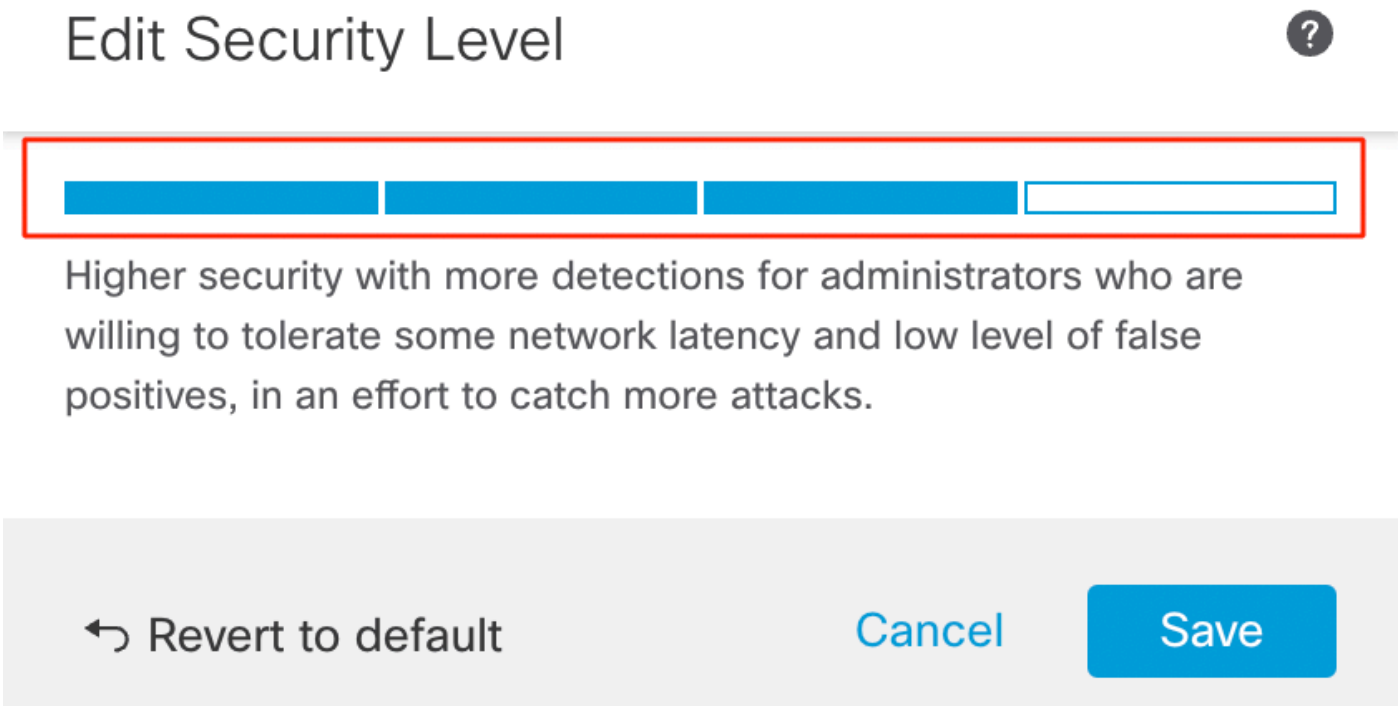


10. Cliquez sur en Edit ( ) regard du niveau de sécurité du groupe de règles pour apporter des modifications en bloc au niveau de sécurité de tous les groupes de règles associés sous l'onglet Enterprisecatégorie de groupe de règles.



Modifier le groupe de règles de sécurité

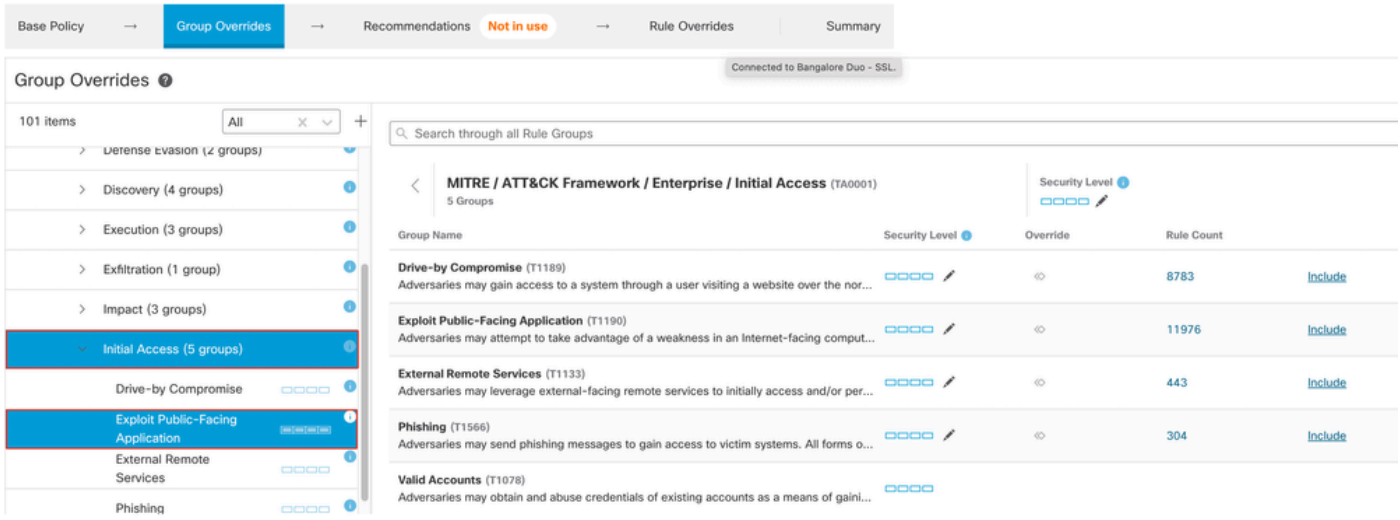
11. Par exemple, choisissez le niveau de sécurité 3 dans la fenêtre, Edit Security Level puis cliquez sur **Save.**



Niveau de sécurité

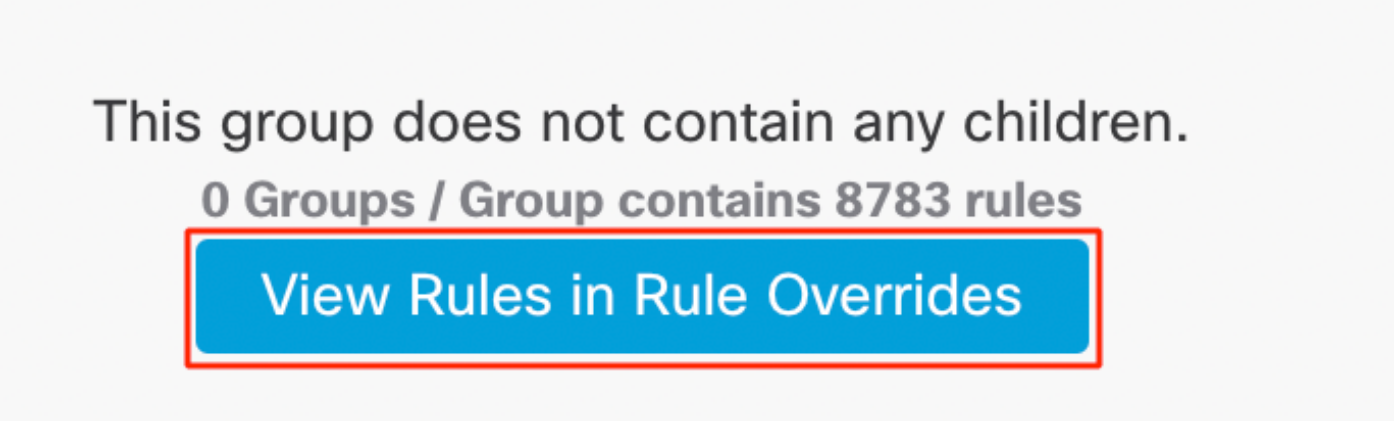
12. SousEnterprise, cliquez Initial Accesspour le développer.

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



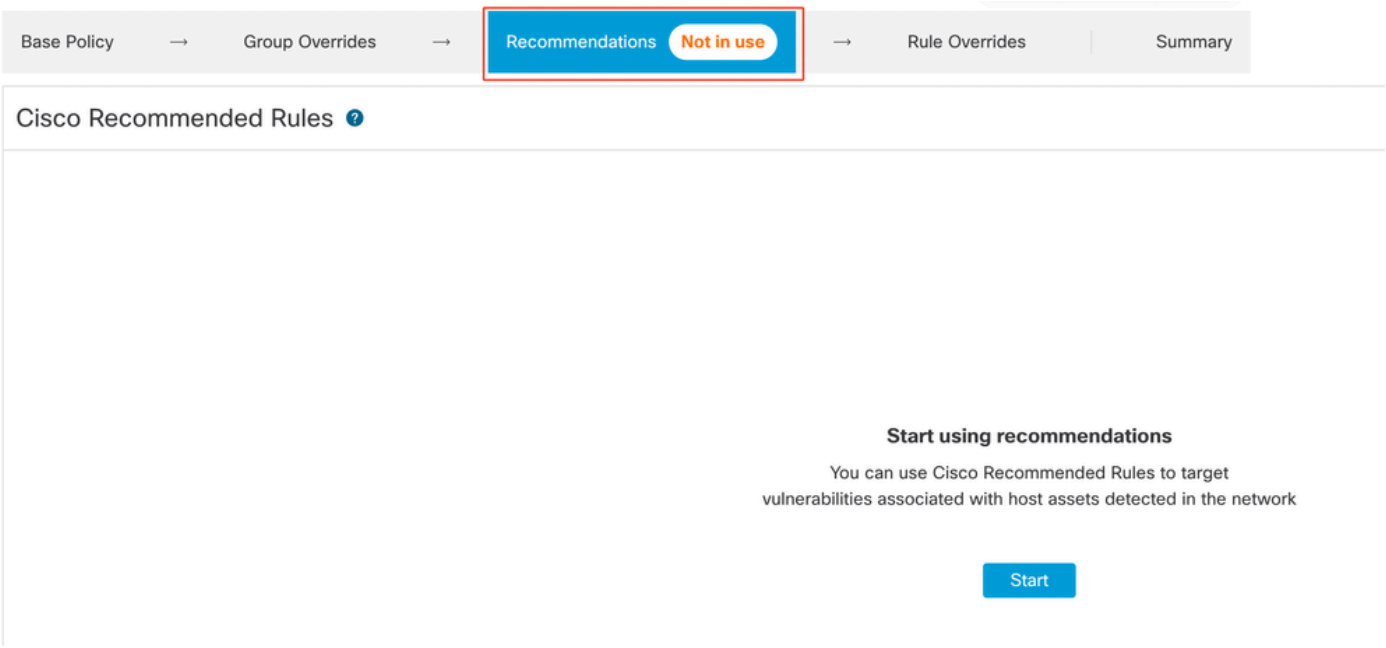
Groupe d'accès initial

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.

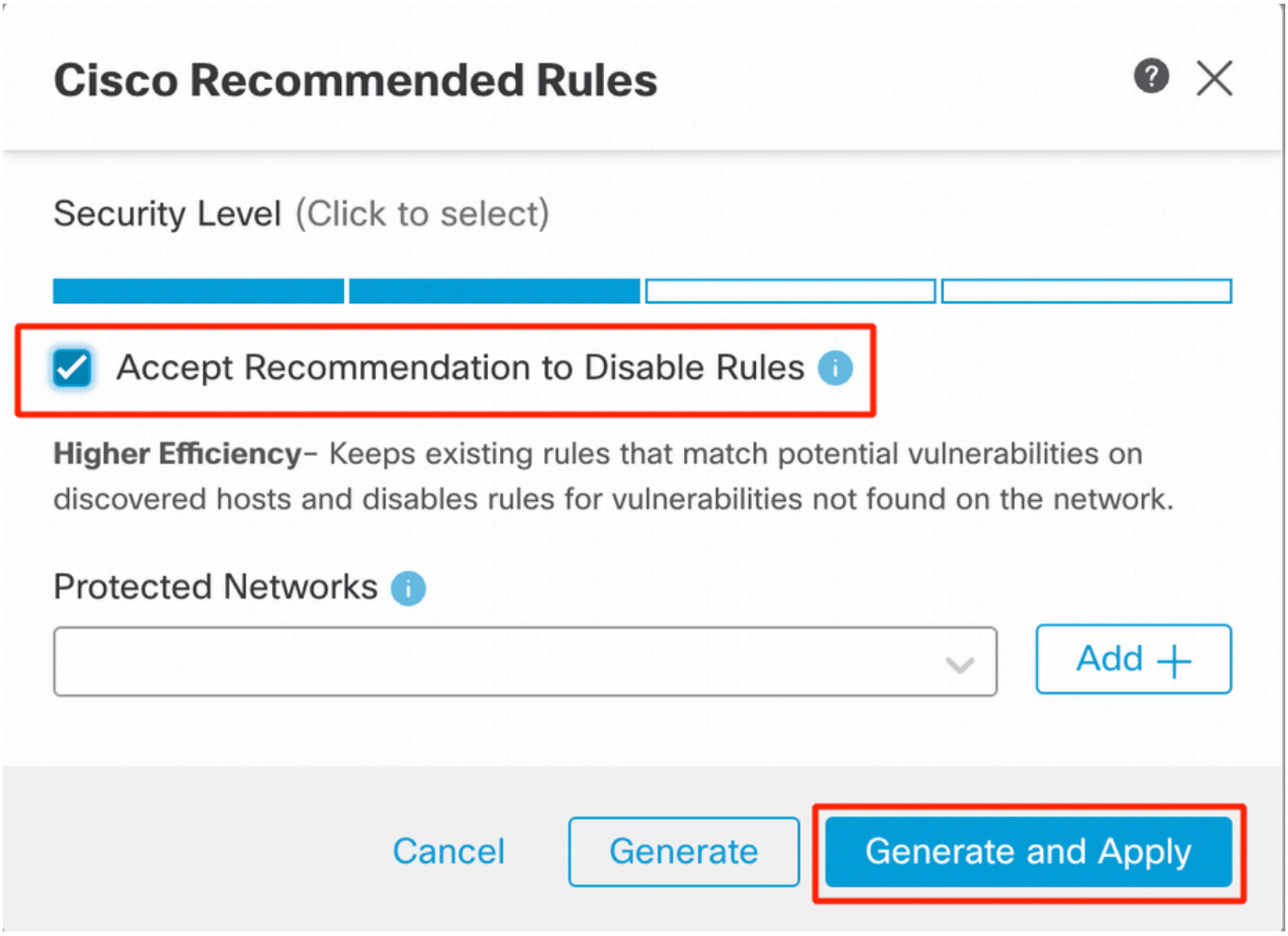


Règles dans les remplacements de règles

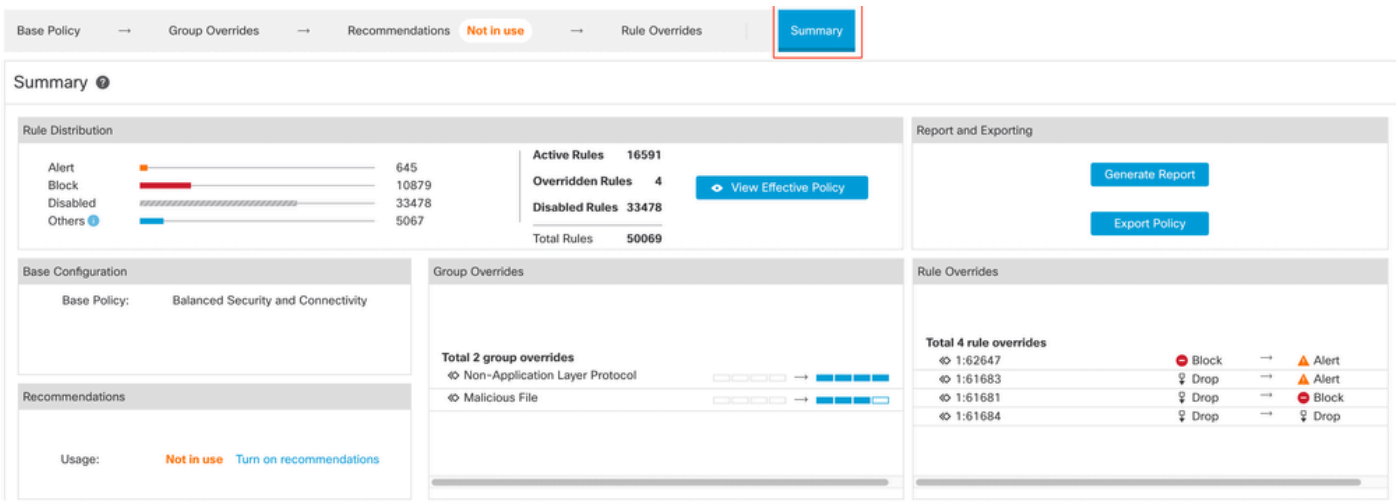
15. Cliquez sur le bouton Recommendationspuis cliquez surStartpour commencer à utiliser les règles recommandées par Cisco. Vous pouvez utiliser les recommandations de règles d'intrusion pour cibler les vulnérabilités associées aux ressources hôtes détectées sur le réseau. Pour plus d'informations.



Recommandations



16. Cliquez sur le bouton Summarypour 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.



Résumé de la stratégie

Afficher les événements d'intrusion

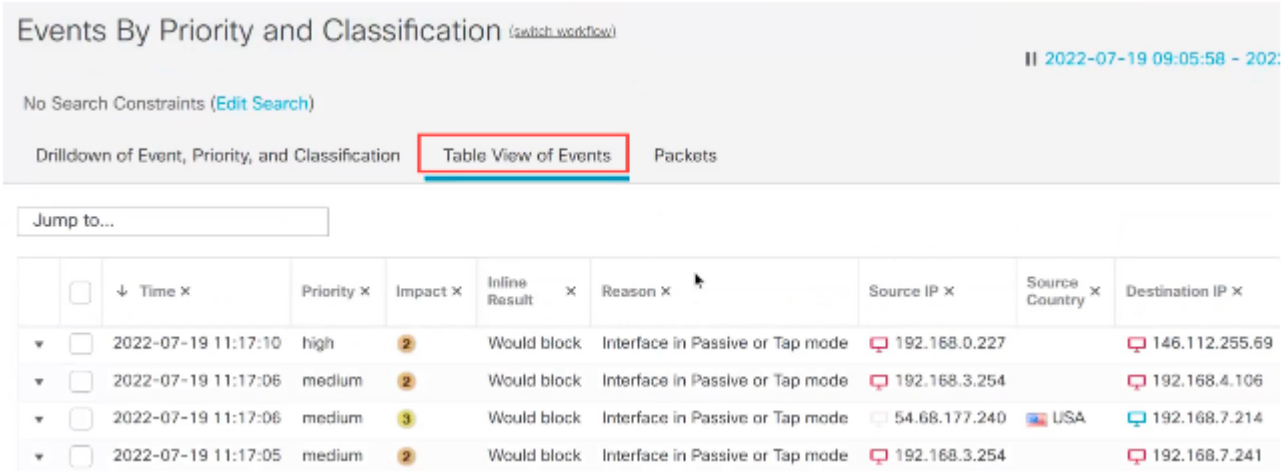
Vous pouvez afficher les techniques et les groupes de règles MITER ATT&CK dans les événements d'intrusion de l'Observateur d'événements classique et de l'Observateur

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.



Événements

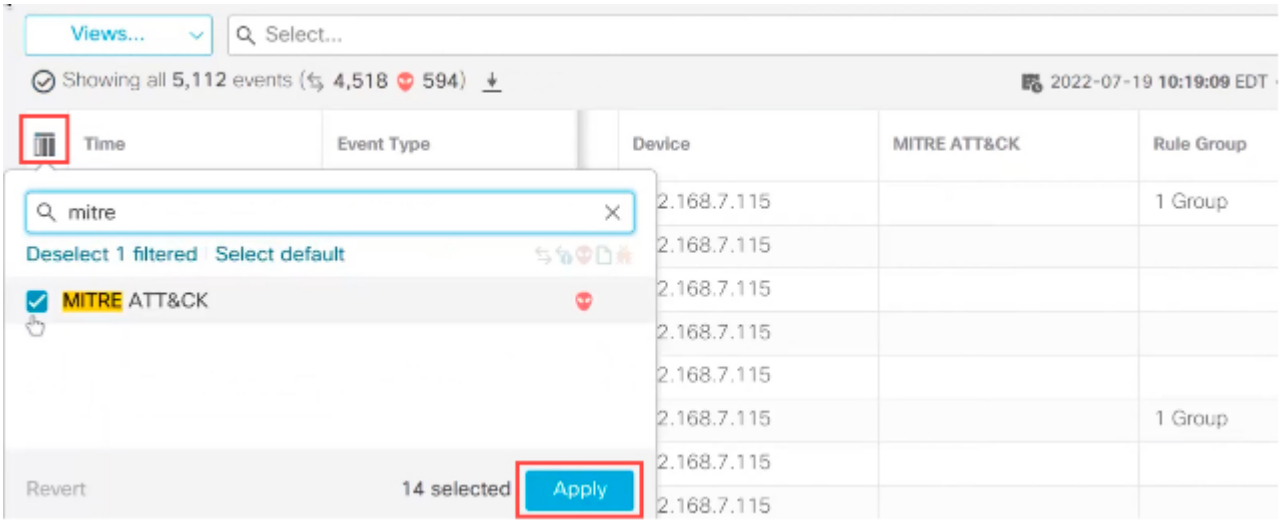
3. Dans la MITRE ATT&CK, vous pouvez voir les techniques d'un événement d'intrusion.

En-tête de colonne mitre

4. Cliquez sur 1 Techniquepour afficher les techniques ATT&CK MITER, comme illustré dans cette figure. Dans cet exemple, Exploit Public-Facing Applicationest la technique.

Techniques ATT&CK MITER

5. Cliquez surClose.
6. Cliquez sur Analysis > Unified Events.
MITRE ATT&CK7. Vous pouvez cliquer sur l'icône de sélection de colonne pour activer les Rule Groupcolonnes et.

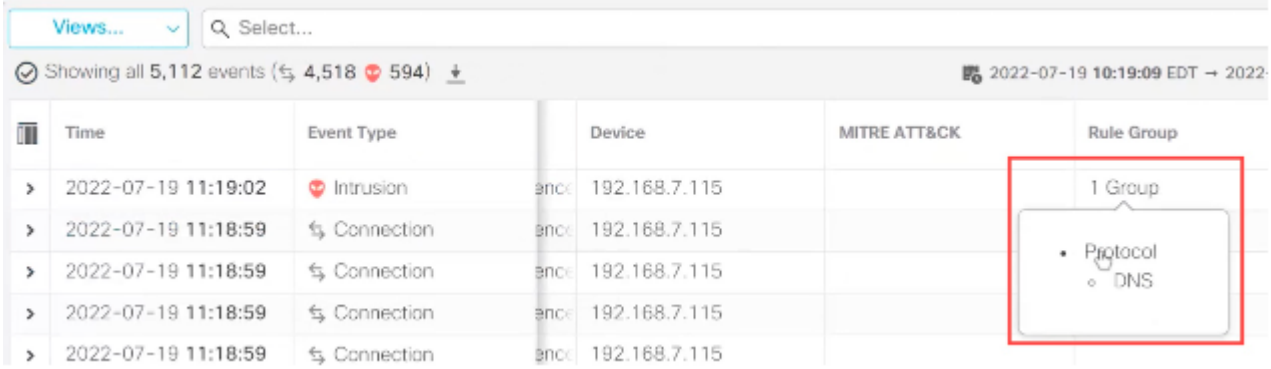


Activer l'attaque mitre

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 Groupcolonne.

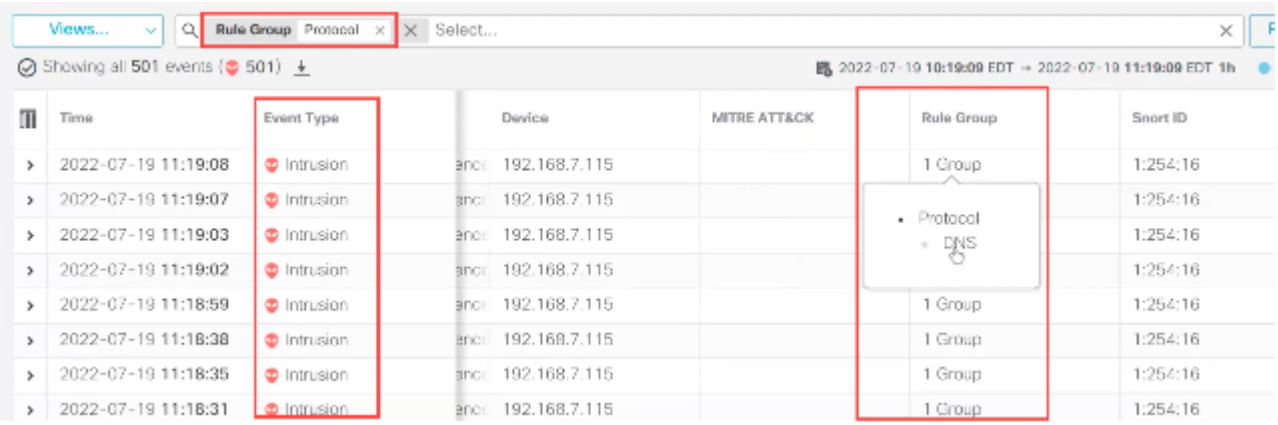
Groupe de règles

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 surProtocolpour 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.



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.