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

Inhoud

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

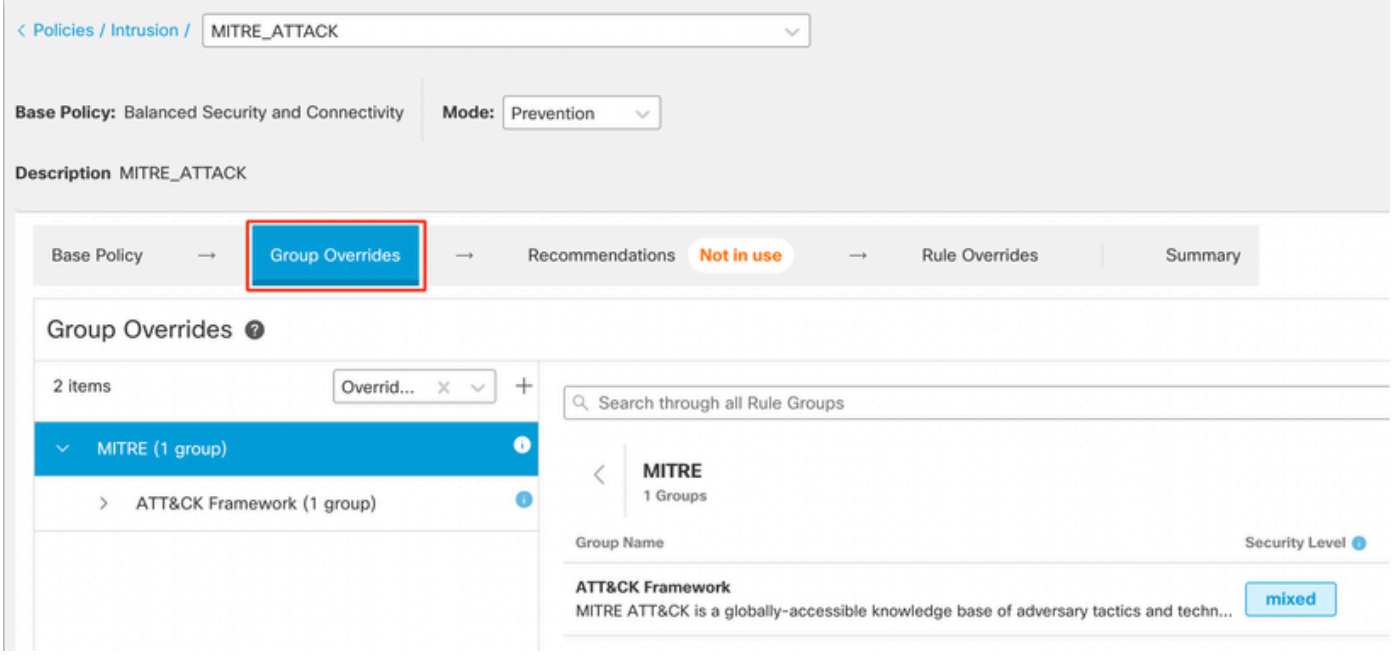
- MITER Tactics, Techniques, and Procedures (TTP's) worden toegevoegd aan inbraakgebeurtenissen waarmee beheerders kunnen handelen op basis van het MITER ATT & CK-framework (Adversary Tactics Techniques and Common Knowledge). Hierdoor kunnen beheerders het verkeer gedetailleerder bekijken en afhandelen 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 > Intrusionuit.
2. Zorg ervoor dat het Intrusion Policiestabblad is geselecteerd.
3. Klik Snort 3 Versionnaast het inbraakbeleid dat u wilt bekijken of bewerken. Sluit de Snort-hulplijn die verschijnt.
4. Klik op de Group Overrideslaag.

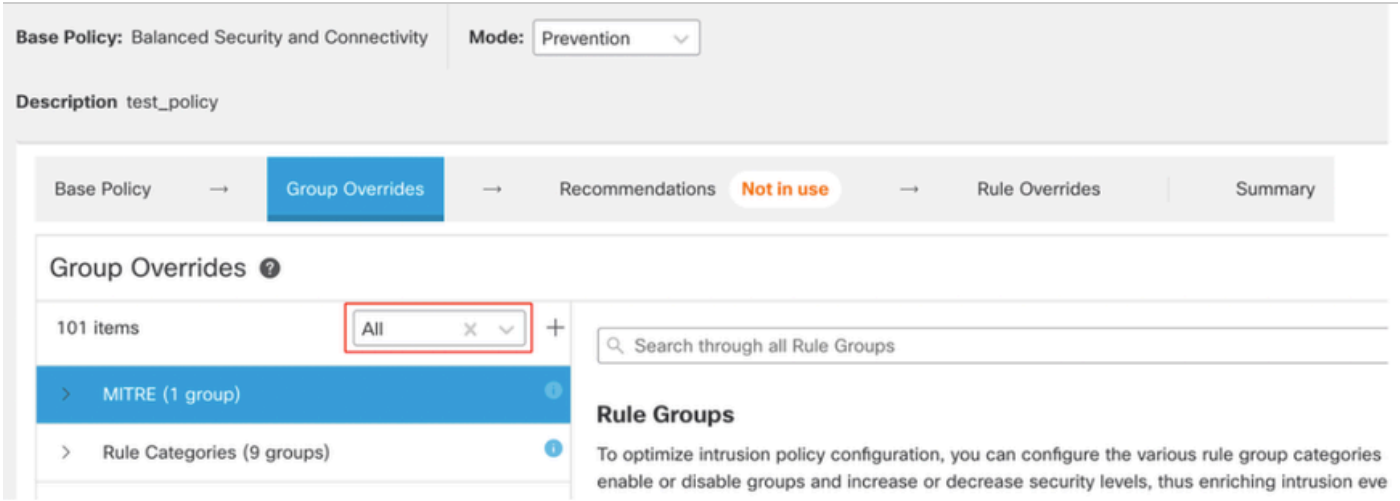
In de Group Overrideslaag worden alle categorieën regelgroepen in een hiërarchische structuur weergegeven. U kunt naar de laatste bladregelgroep in elke regelgroep gaan.



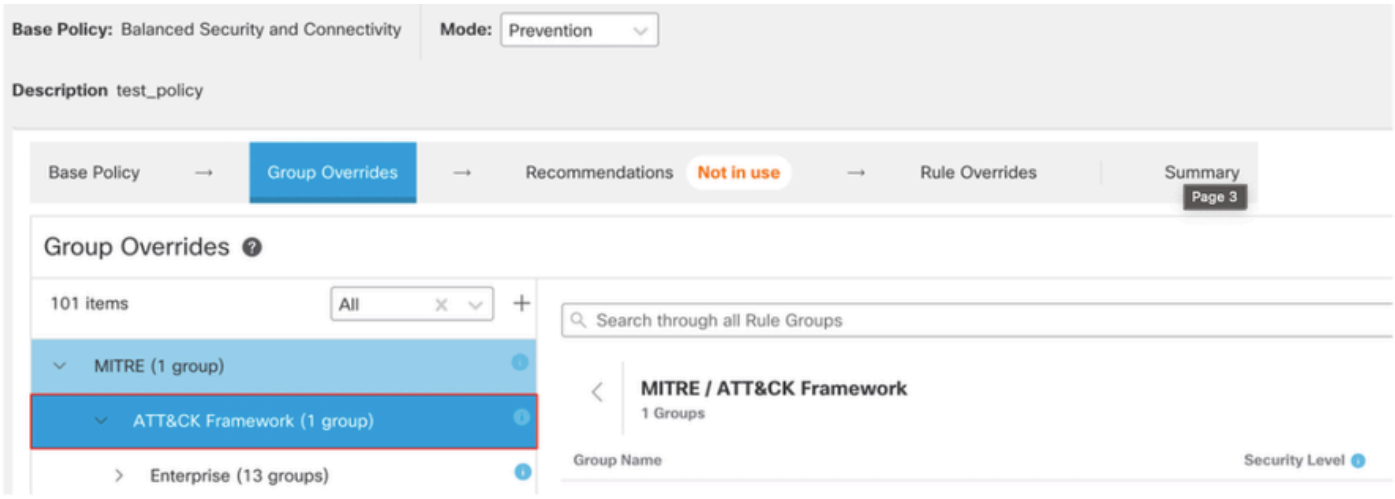
6. Group OverridesErvoor zorgen dat AllDit wordt in de vervolgkeuzelijst gekozen, zodat alle regelgroepen voor het inbraakbeleid in het linkerdeelvenster zichtbaar zijn.

7. Klik op MITREin het linkerdeelvenster.

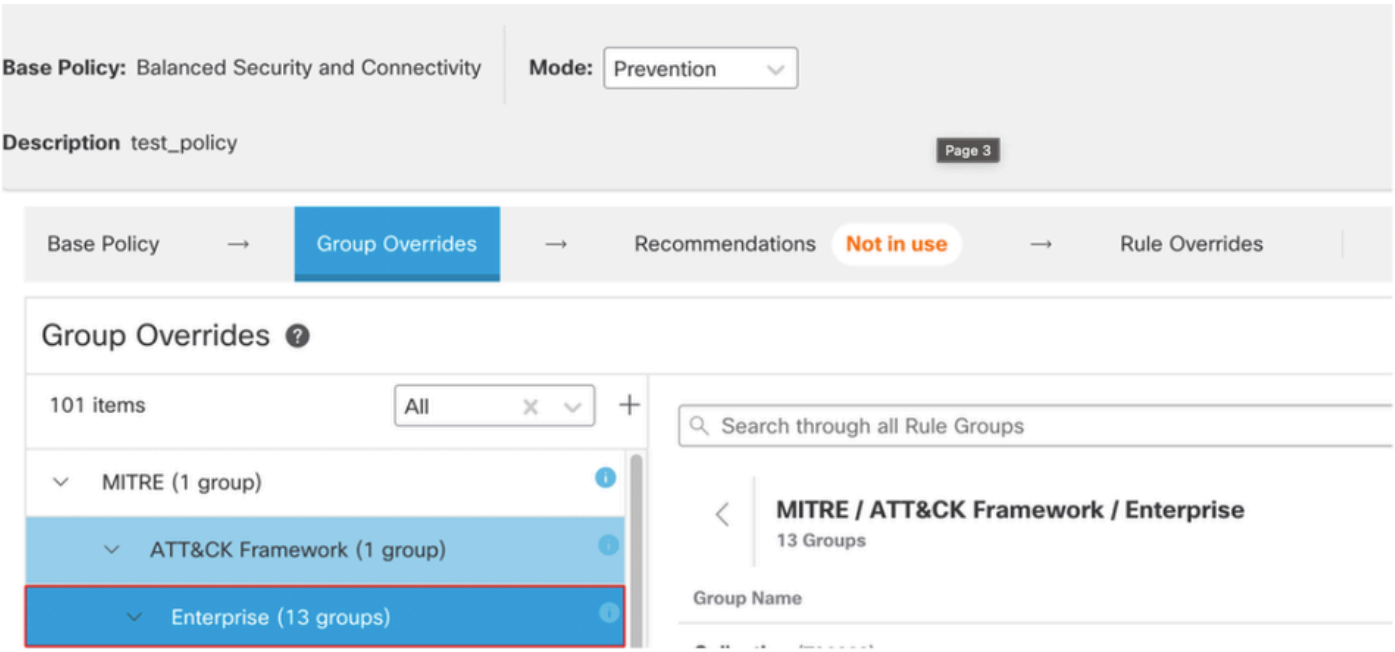
Opmerking: In dit voorbeeld is MITER geselecteerd, maar afhankelijk van uw specifieke vereisten kunt u de regelcategorieën of een andere regelgroep en daaropvolgende regelgroepen kiezen. Alle regelgroepen gebruiken het MITER-framework.



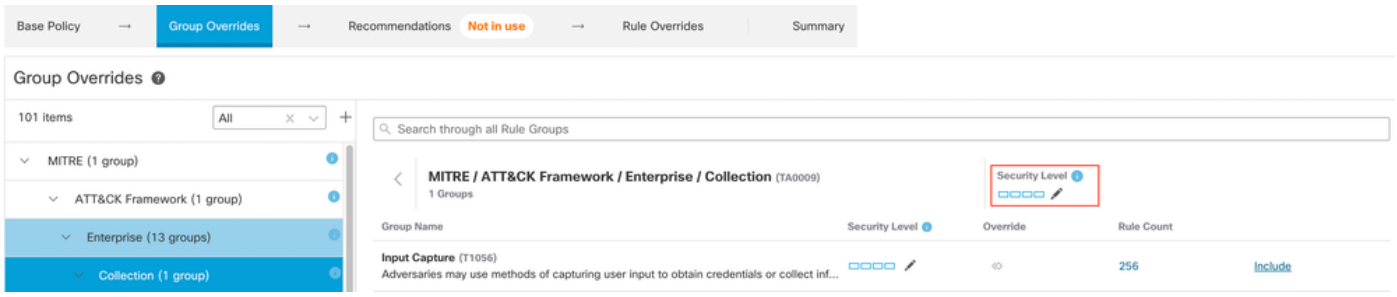
8. Klik onderMITREop ATT&CK Raamwerk om het uit te vouwen.



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

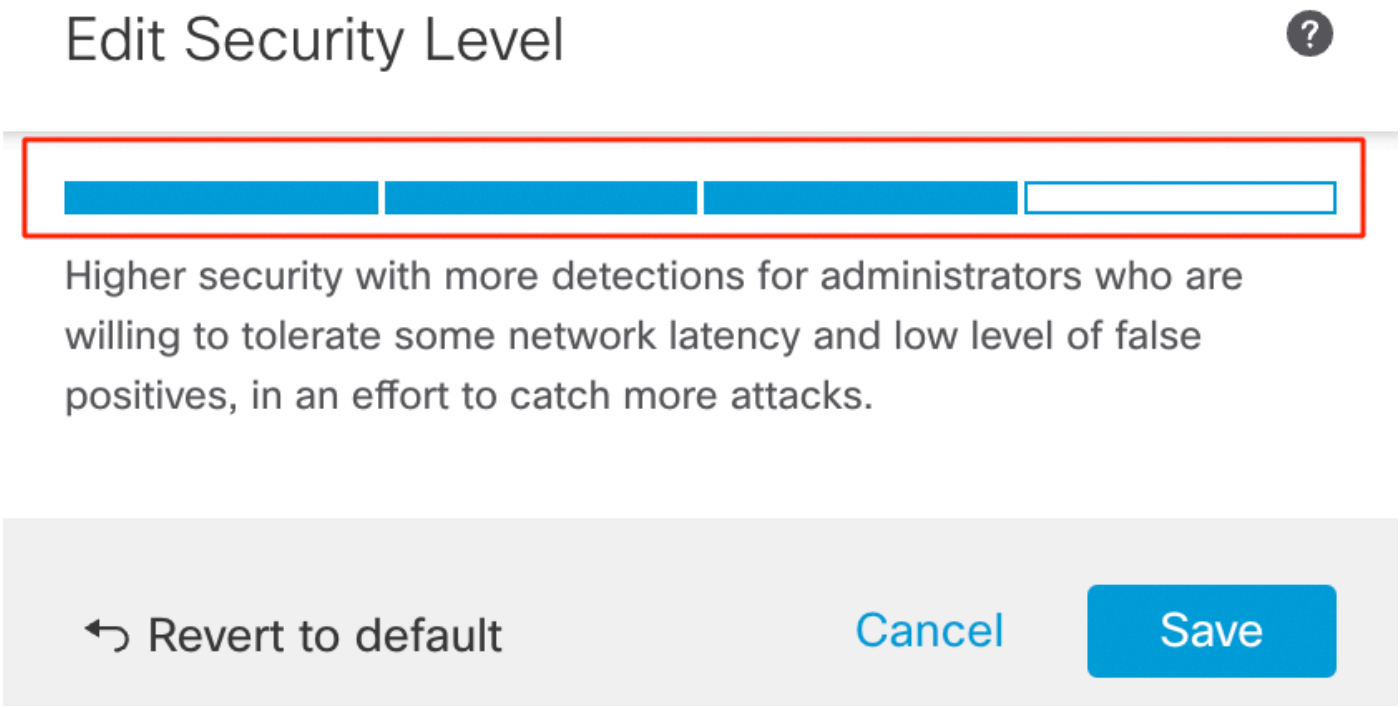


10. Klik Edit ( ) naast het beveiligingsniveau van de regelgroep om bulksgewijs wijzigingen aan te brengen in het beveiligingsniveau voor alle bijbehorende regelgroepen onder de EnterpriseRubriek Regelgroep.



Groep beveiligingsregels bewerken

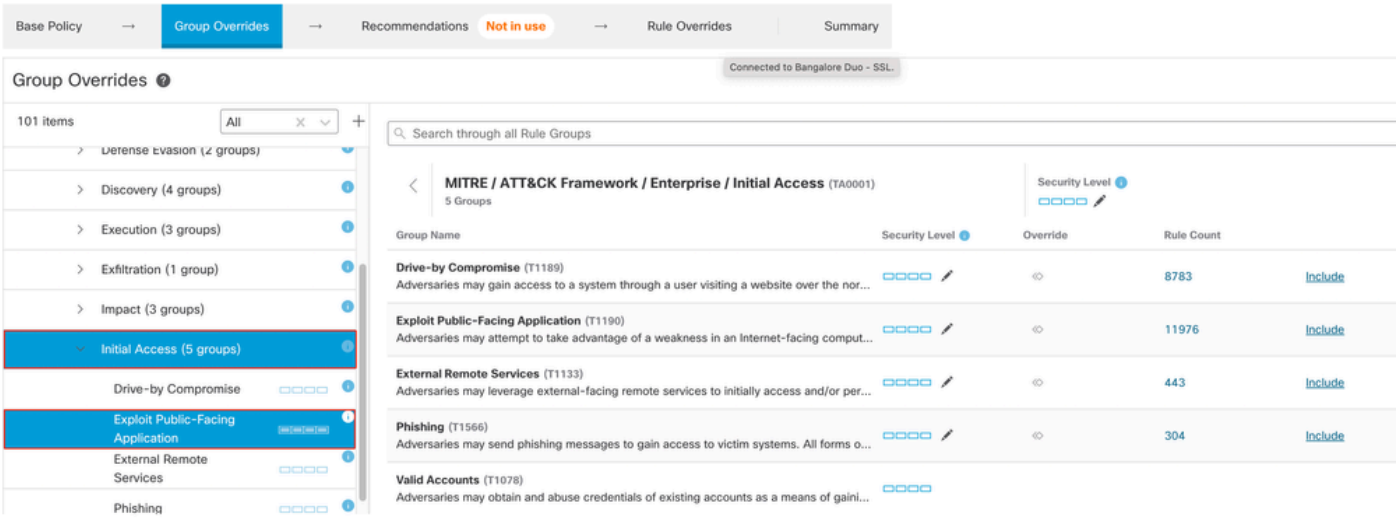
11. Kies bijvoorbeeld beveiligingsniveau 3 in het Edit Security Level venster en klik **Save**op.



Beveiligingsniveau

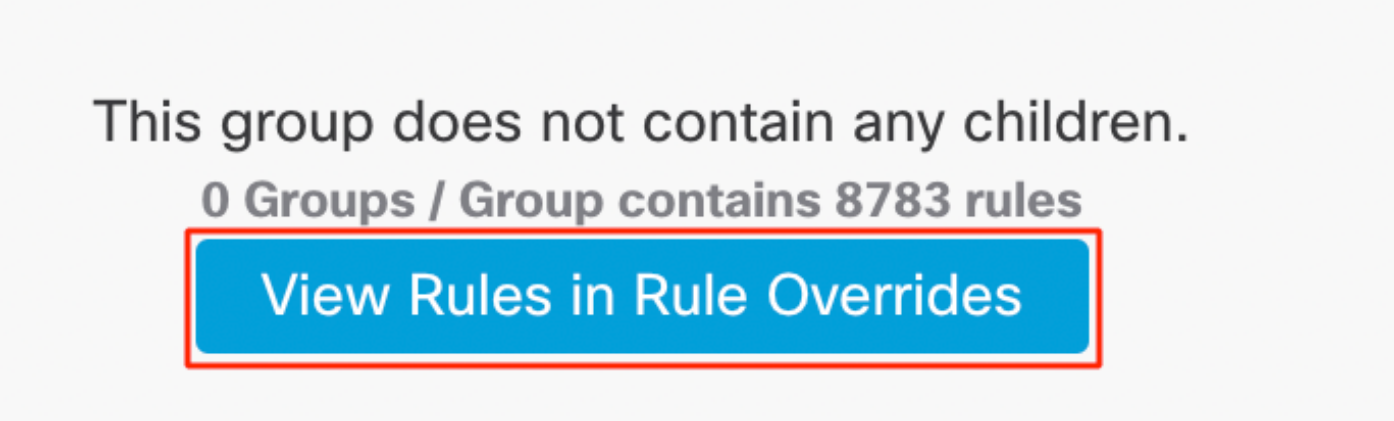
12. Klik onderEnterpriseom het Initial Accessuit te vouwen.

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



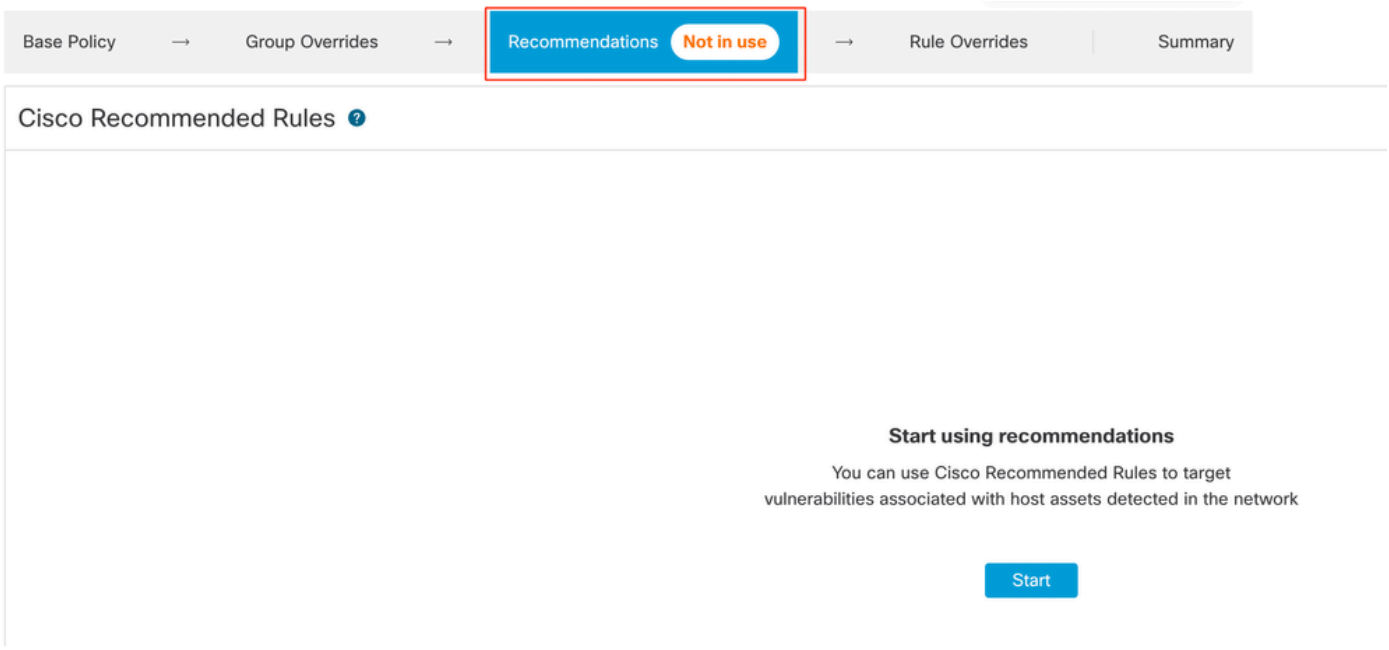
Groep voor eerste toegang

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

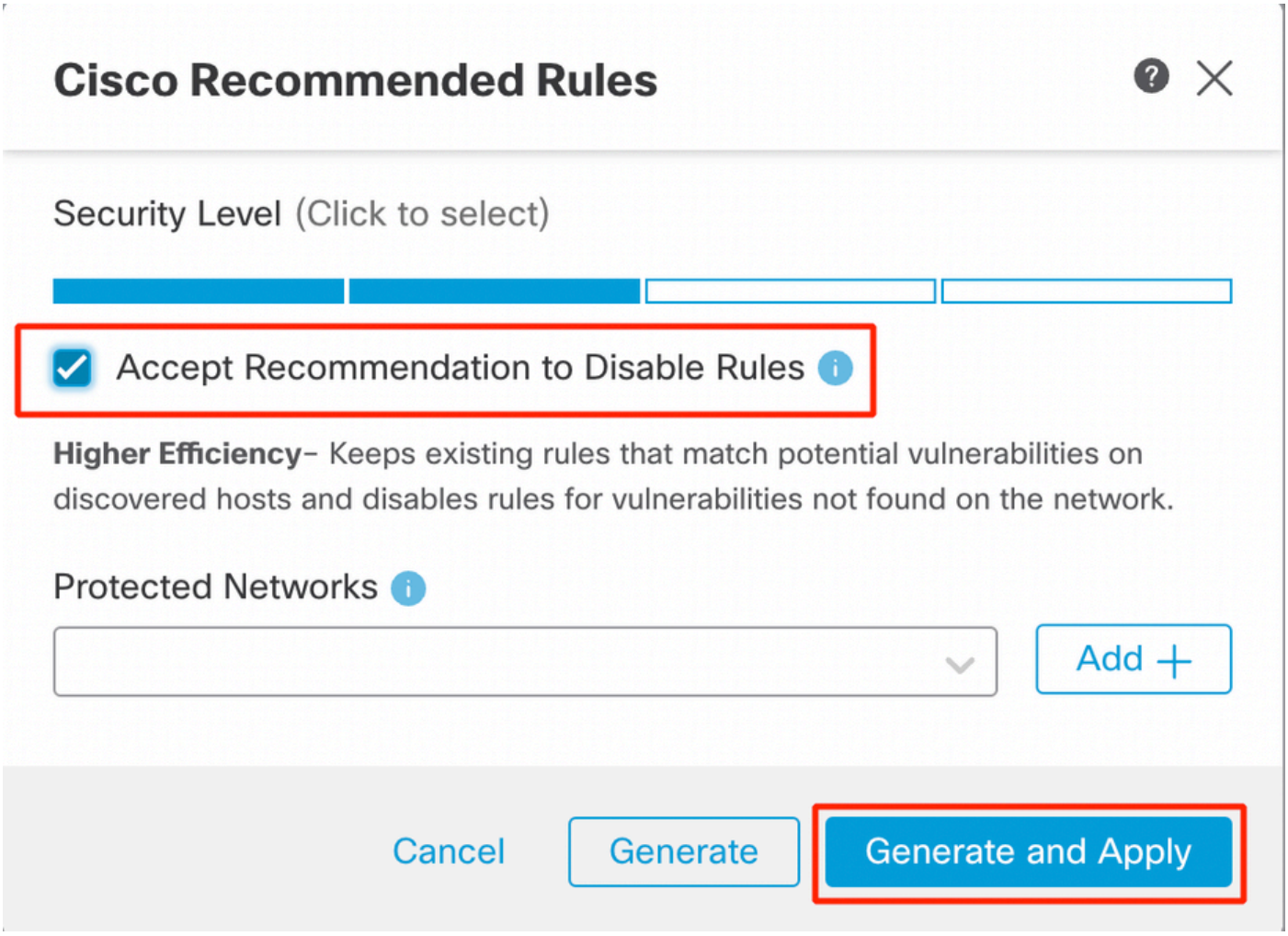


Regels in regeloverschrijvingen

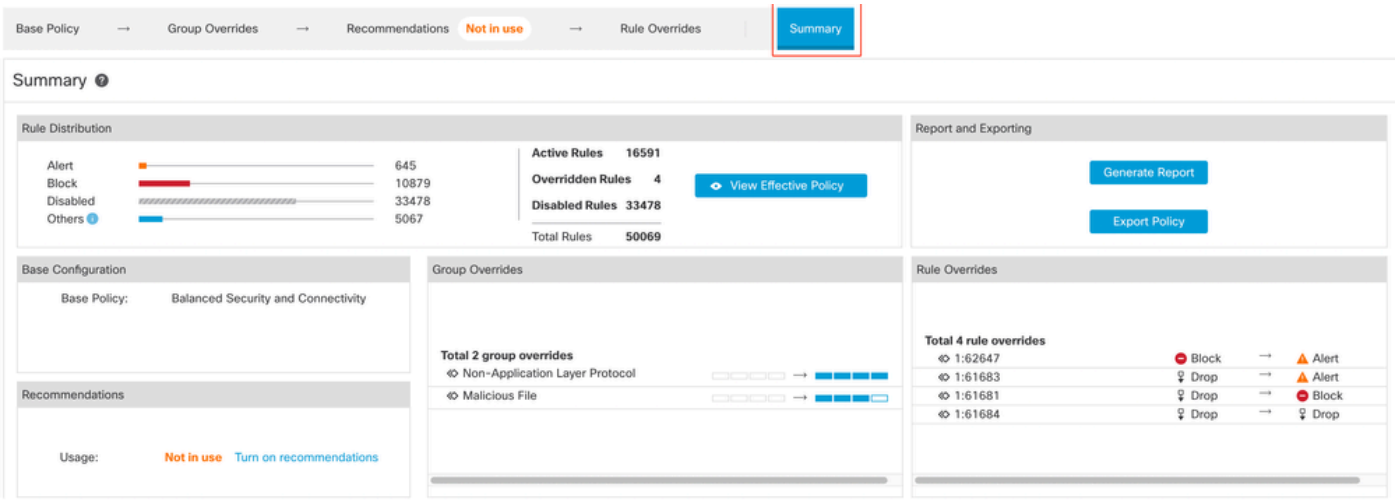
15. Klik op de Recommendationslaag en klik vervolgensStartom te beginnen met het gebruik van Cisco-aanbevolen regels. U kunt de aanbevelingen voor de inbraakregel gebruiken om kwetsbaarheden aan te pakken die zijn gekoppeld aan host-assets die in het netwerk zijn gedetecteerd. Meer informatie.



Aanbevelingen



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



Samenvatting van het beleid

Inbraakgebeurtenissen bekijken

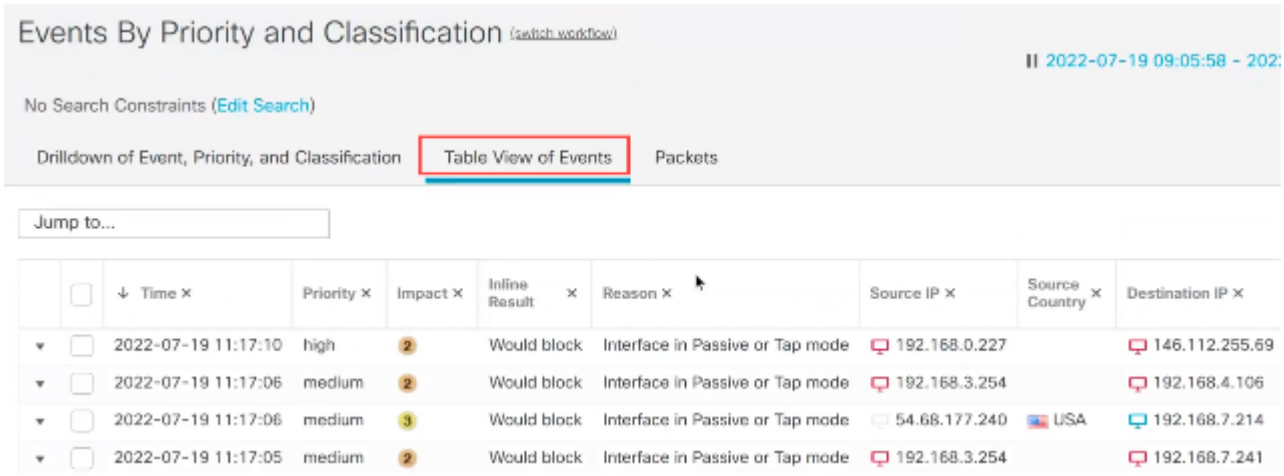
U kunt de MITRE ATT&CK-technieken en regelgroepen bekijken in de inbraakgebeurtenissen in de Classic Event Viewer en Unified Event Viewer. Talos biedt mappings van Snort-regels (GID:

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 > Eventserop.

2. Klik op de **Table View of Events**tabblad zoals weergegeven in de afbeelding.



Gebeurtenissen

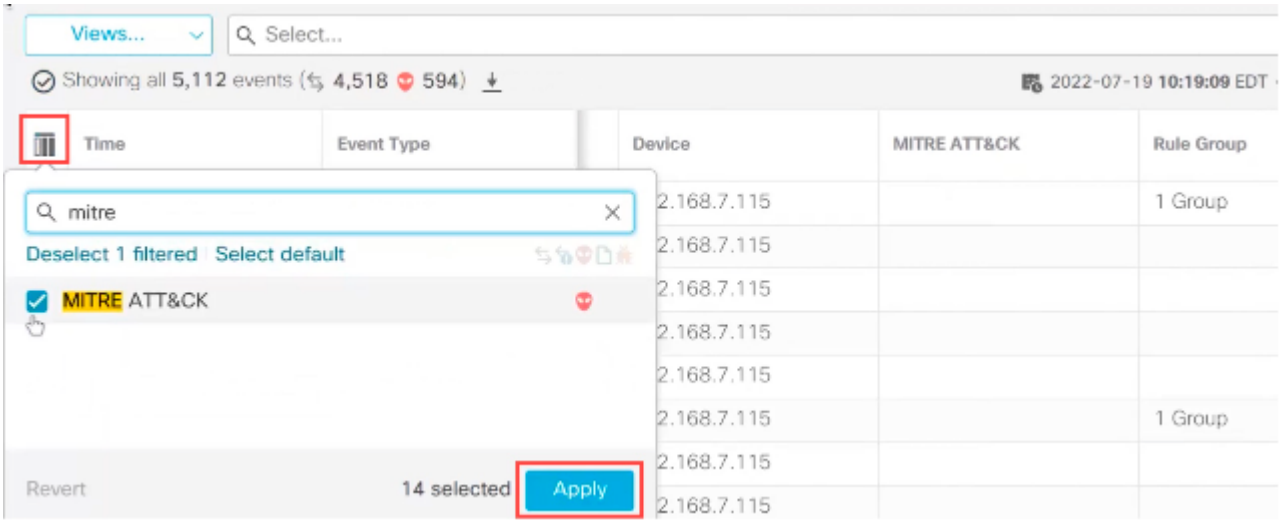
3. In de MITRE ATT&CKColumn header, kunt u de technieken voor een inbraak evenement te zien.

Kolomkop mijter

4. Klik op 1 Techniqueom de MITER ATT&CK-technieken te bekijken, zoals weergegeven in deze figuur. In dit voorbeeld, Exploit Public-Facing Applicationis de techniek.

MITRE ATT&CK Techniques

5. KlikCloseerop.
6. Klik Analysis > Unified Eventserop.
7. U kunt op het kolomselectiepictogram klikken om de MITRE ATT&CKen Rule Groupkolommen in te schakelen.

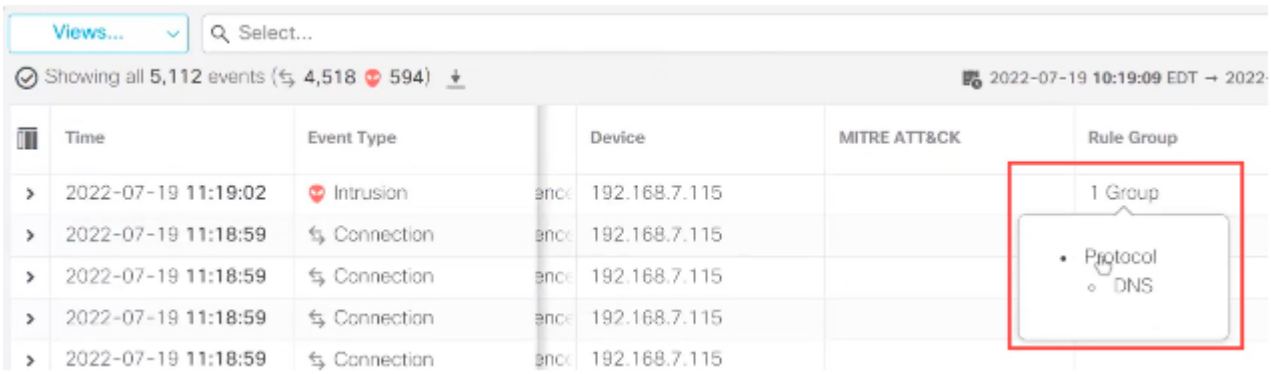


Schakel de Mitre-aanval in

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 Groupkolom.

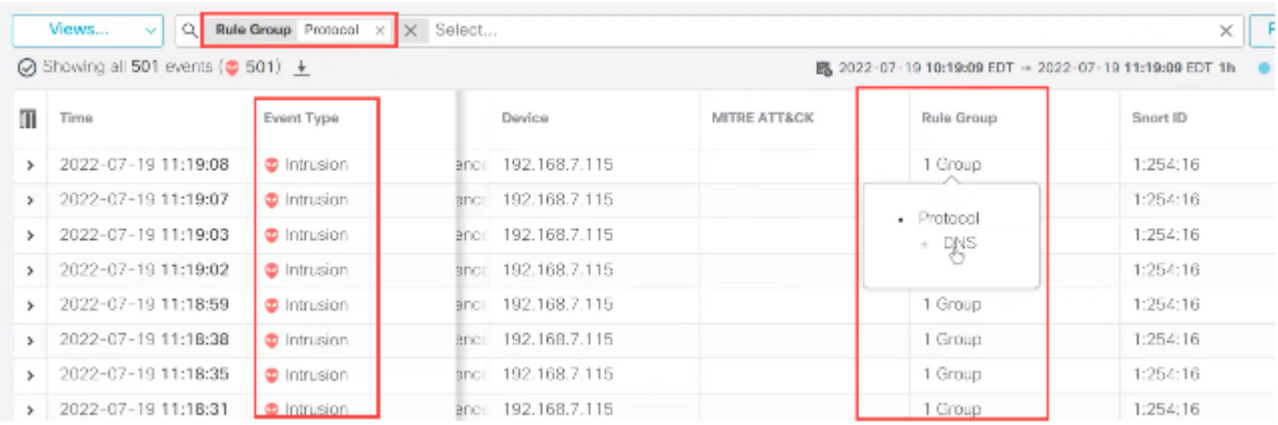
Regelgroep

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



Bekijk protocol

10. U kunt klikkenProtocolom 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.



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.