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

Inhalt

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.

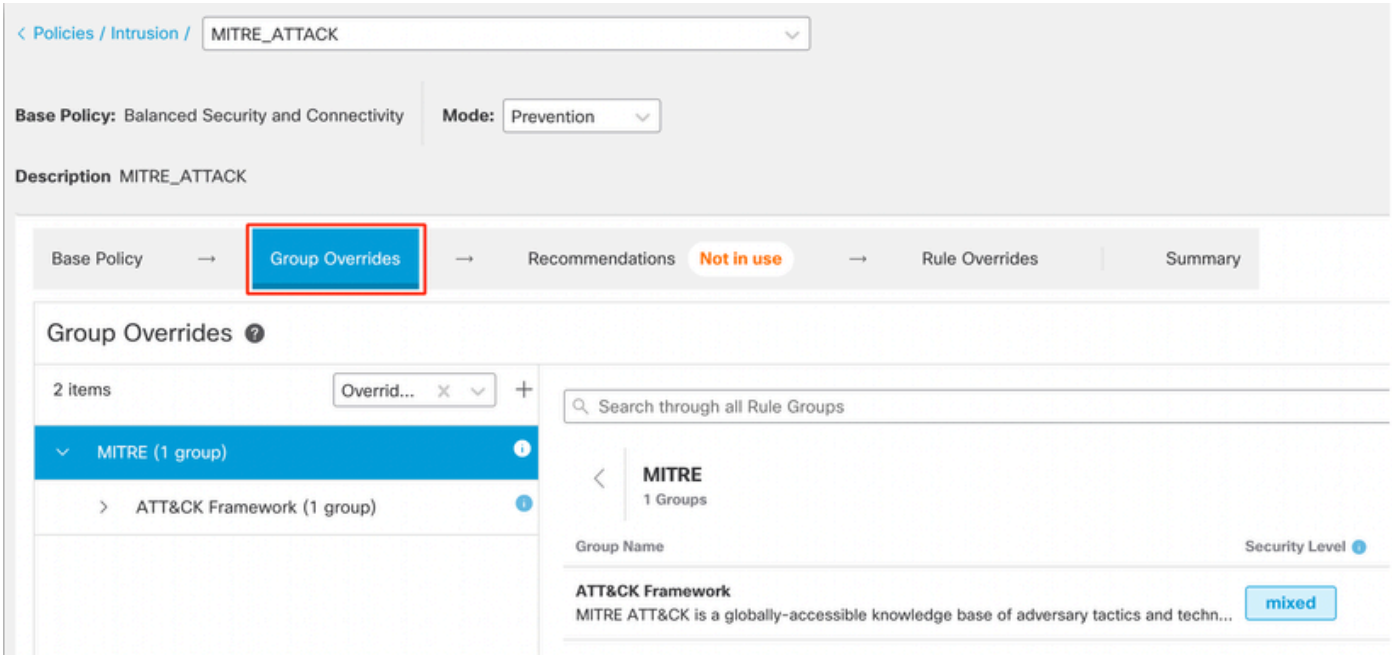
Anzeigen des MITER-Frameworks in Ihrer Richtlinie für Sicherheitsrisiken

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 PoliciesRegisterkarte ausgewählt ist.
3. Klicken Sie Snort 3 Versionneben der Richtlinie für Sicherheitsrisiken, die Sie anzeigen oder bearbeiten möchten. Schließen Sie das sich öffnende Snort-Hilfshandbuch.
4. Klicken Sie auf die Group OverridesEbene.

Die Group OverridesEbene listet alle Kategorien von Regelgruppen in einer hierarchischen Struktur

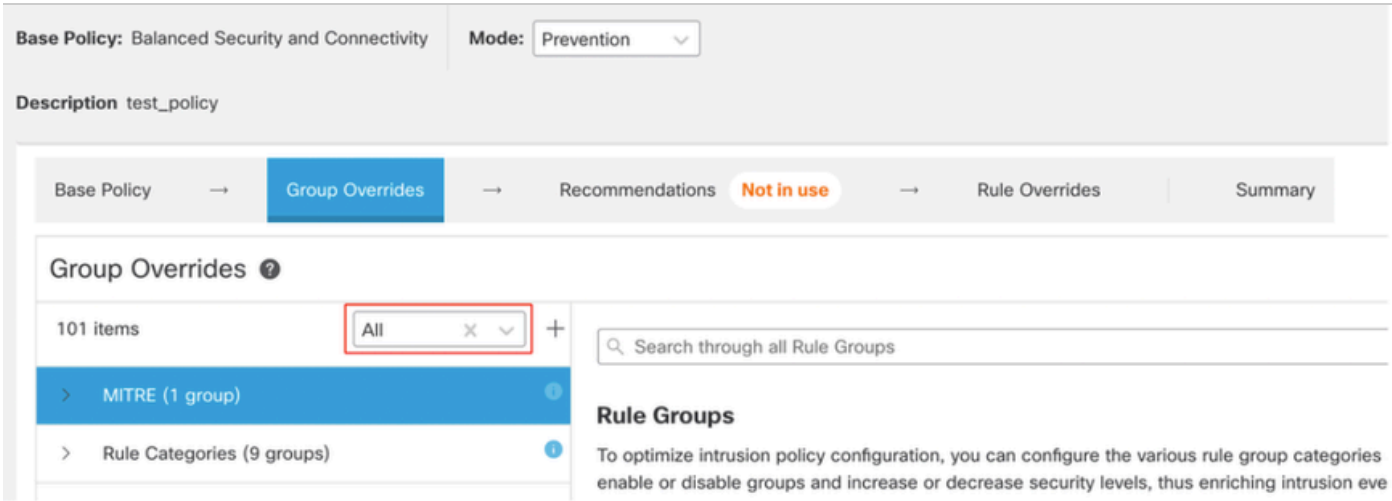
auf. Sie können zu der letzten Blattregelgruppe in jeder Regelgruppe wechseln.



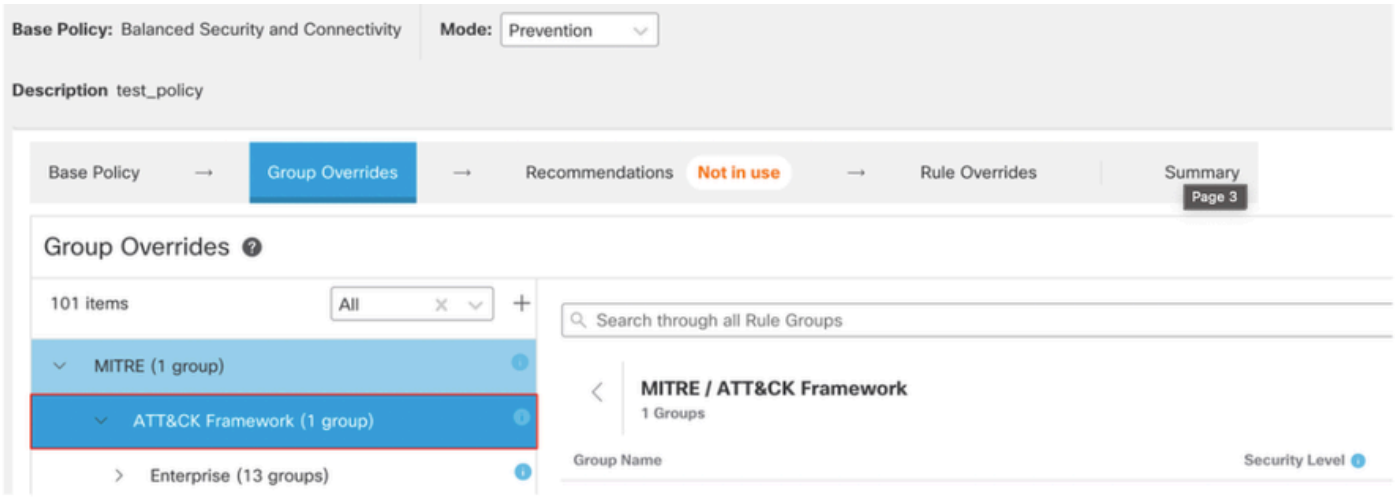
6. unter Group Overrides: Allwird in der Dropdown-Liste ausgewählt, sodass alle Regelgruppen für die Richtlinie für Sicherheitsrisiken im linken Bereich angezeigt werden.

7. Klicken Sie MITREim linken Fensterausschnitt.

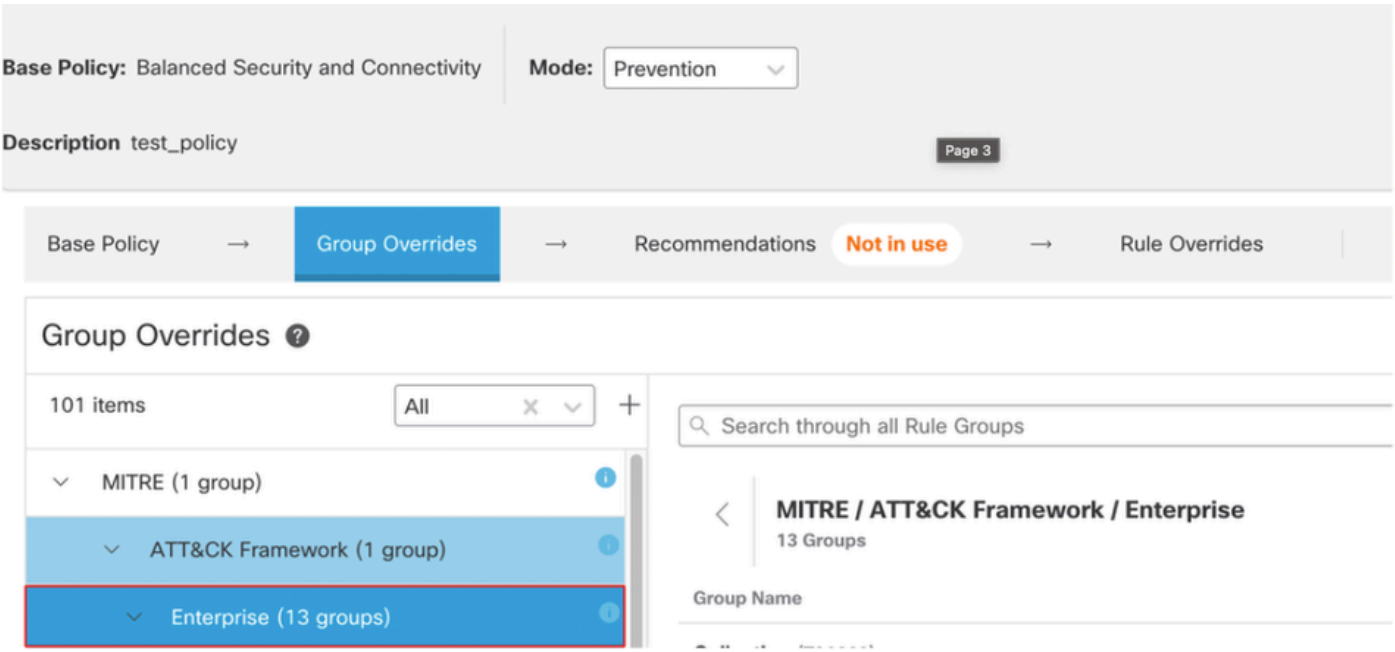
Anmerkung: Für dieses Beispiel ist MITER ausgewählt. Je nach Ihren spezifischen Anforderungen können Sie jedoch die Regelgruppe Regelkategorien oder eine andere Regelgruppe und die darunterliegenden nachfolgenden Regelgruppen auswählen. Alle Regelgruppen verwenden das MITER-Framework.



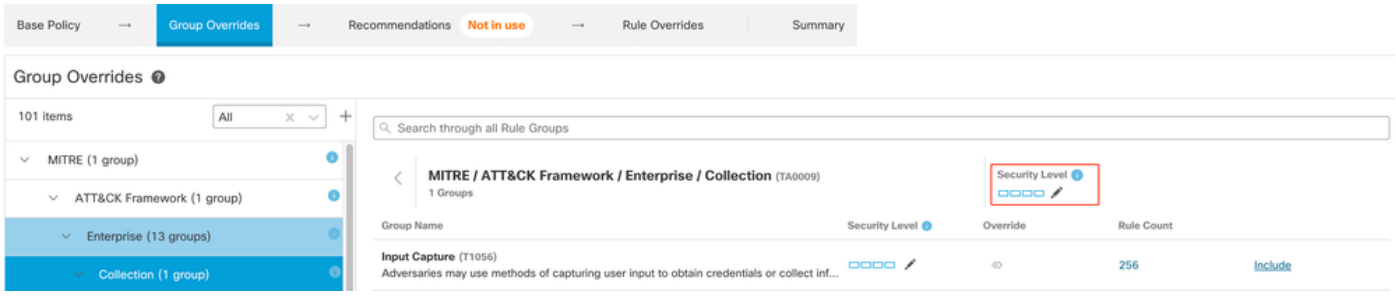
8. Klicken Sie unterMITREauf Framework, um es zu erweitern ATT&CK.



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

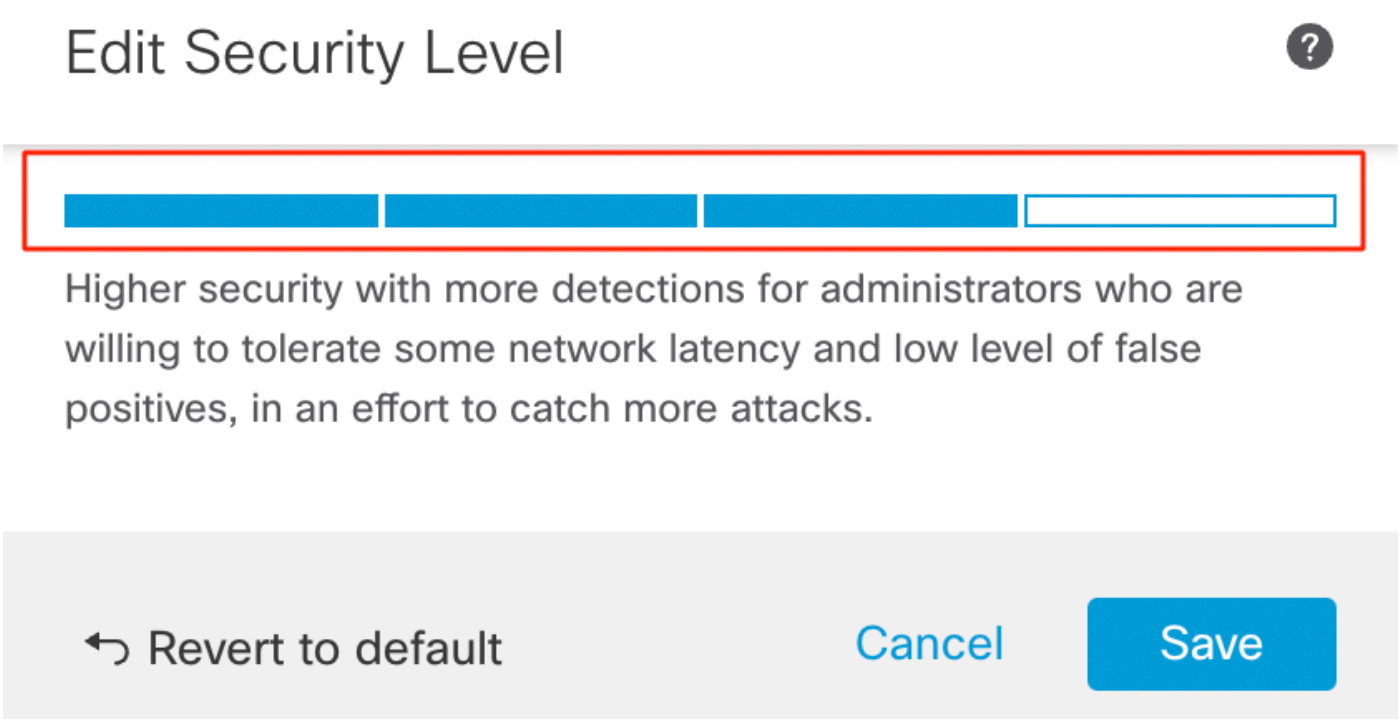


10. Klicken Sie Edit ( ) neben der Sicherheitsstufe der Regelgruppe, um Massenänderungen an der Sicherheitsstufe für alle zugeordneten Regelgruppen unter der EnterpriseRegelgruppenkategorie



Sicherheitsregelgruppe bearbeiten

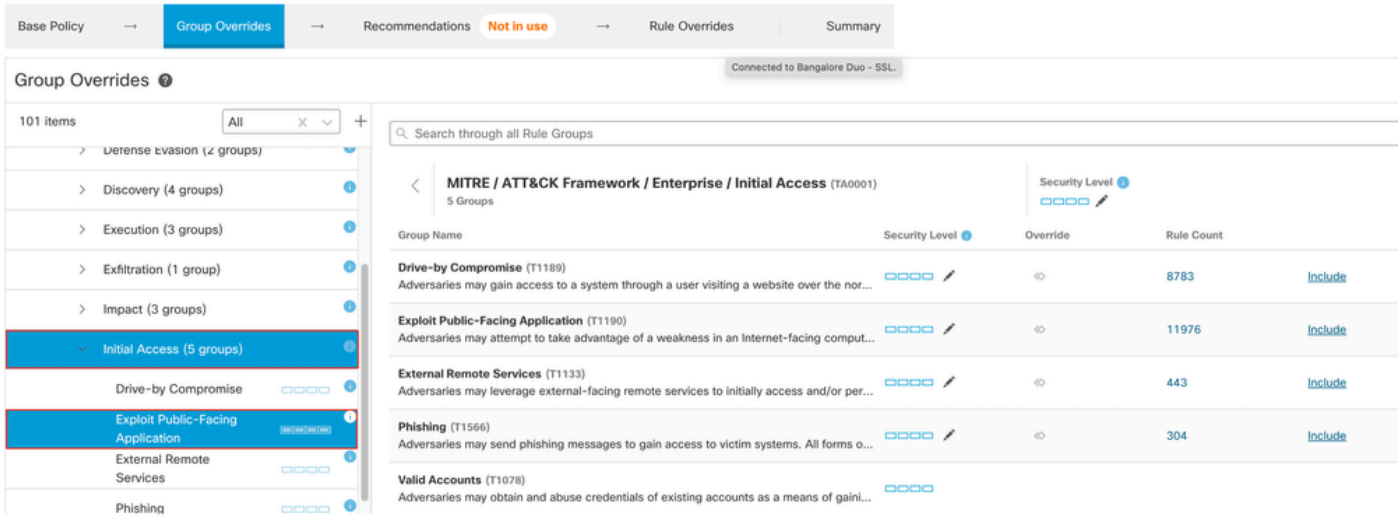
11. Wählen Sie als Beispiel Sicherheitsstufe 3 im Fenster aus Edit Security Level, und klicken Sie auf **Save**.



Sicherheitsstufe

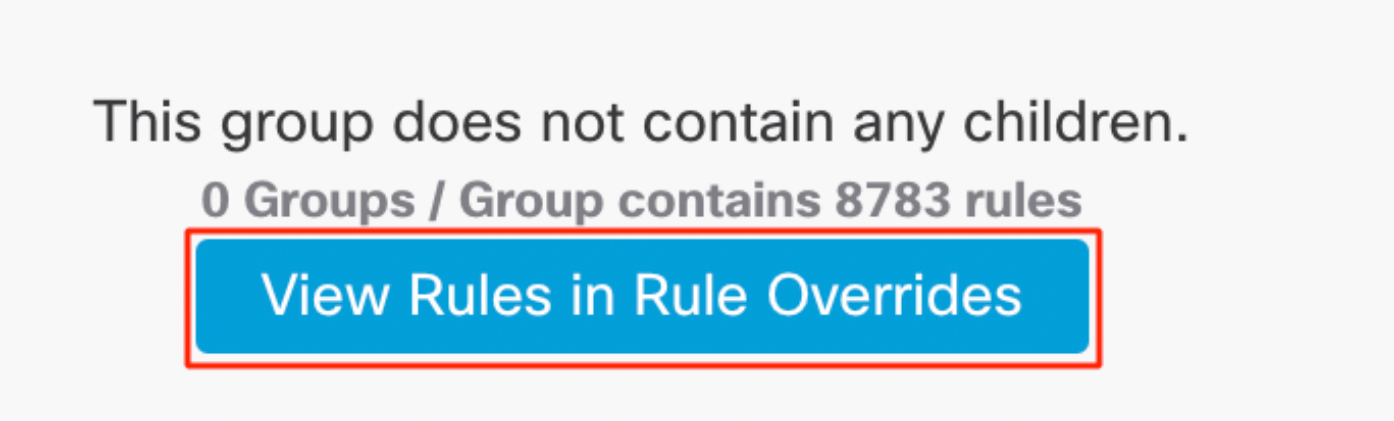
12. UnterEnterprise, klicken Sie, Initial Accessum es zu erweitern.

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



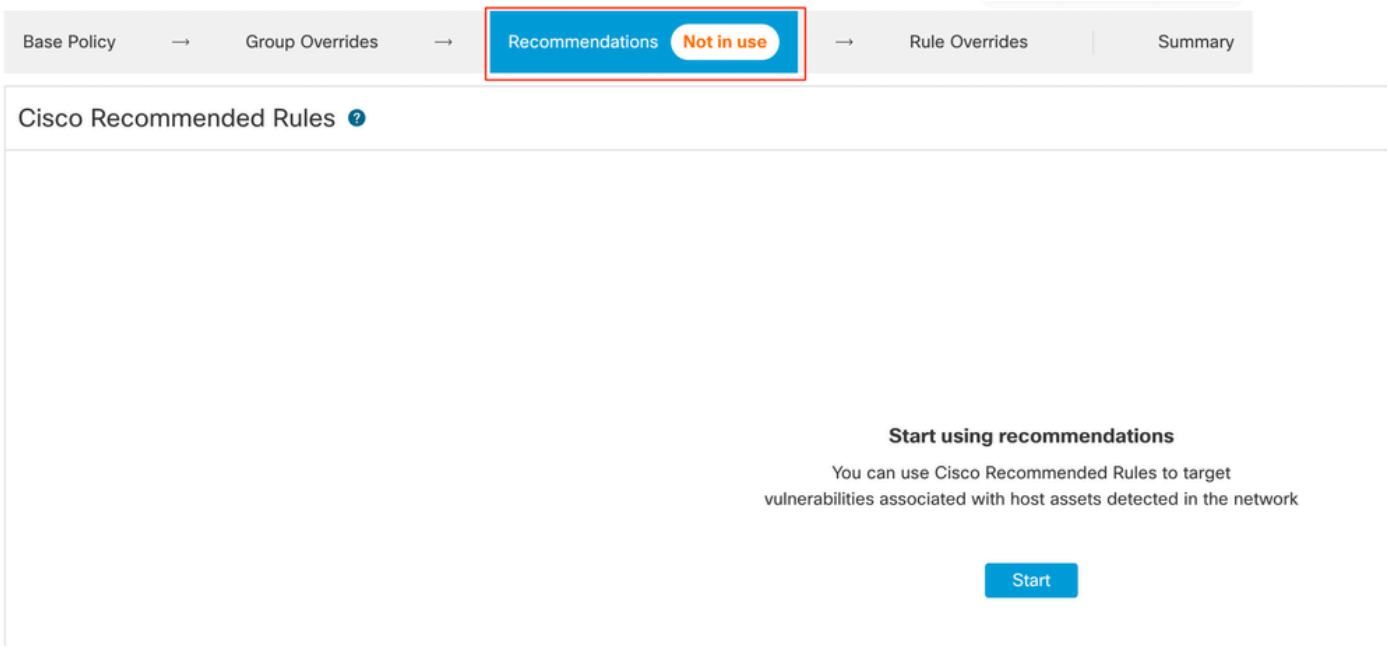
Erste Zugriffsgruppe

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

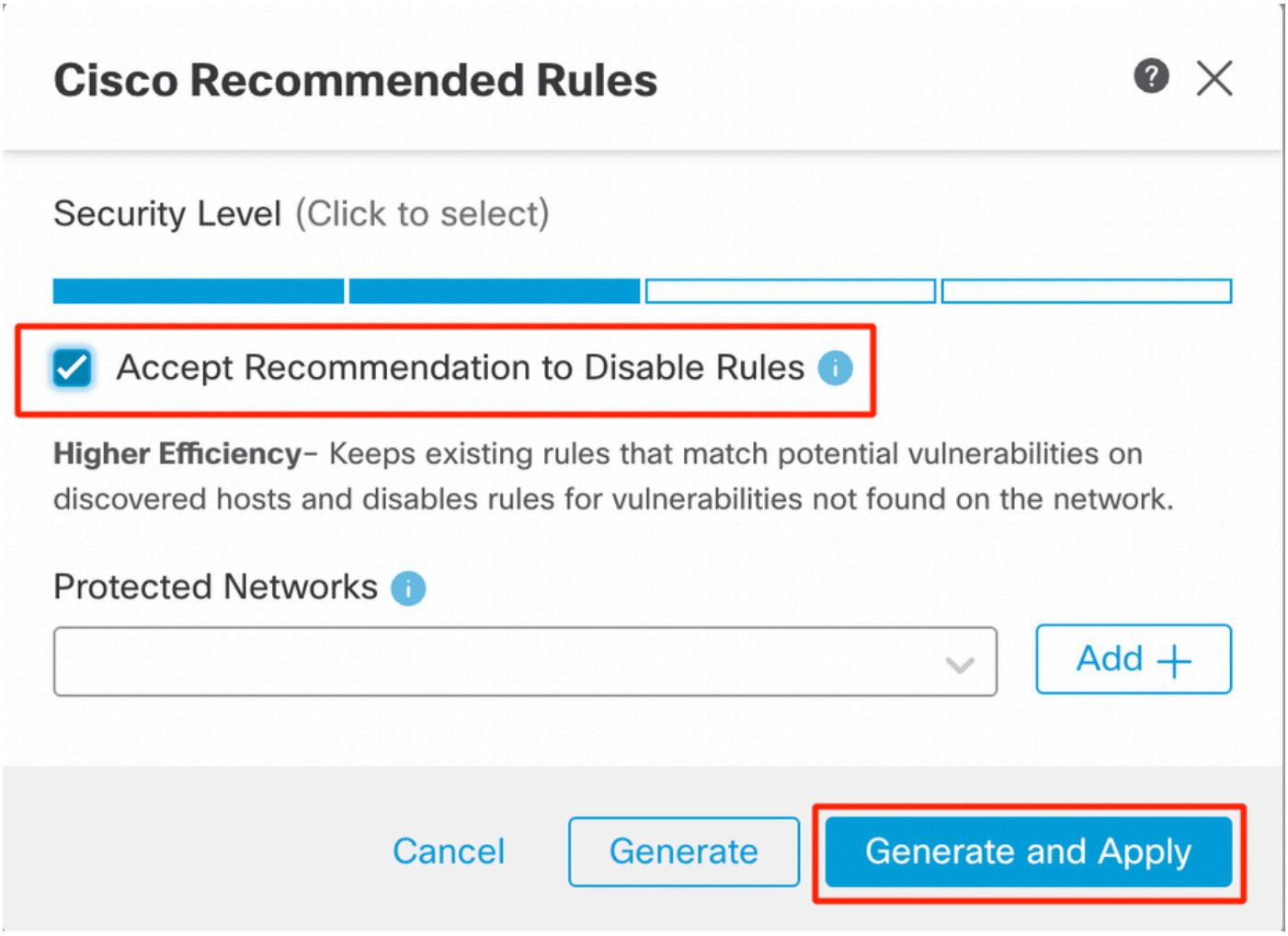


Regeln in Regelüberschreibungen

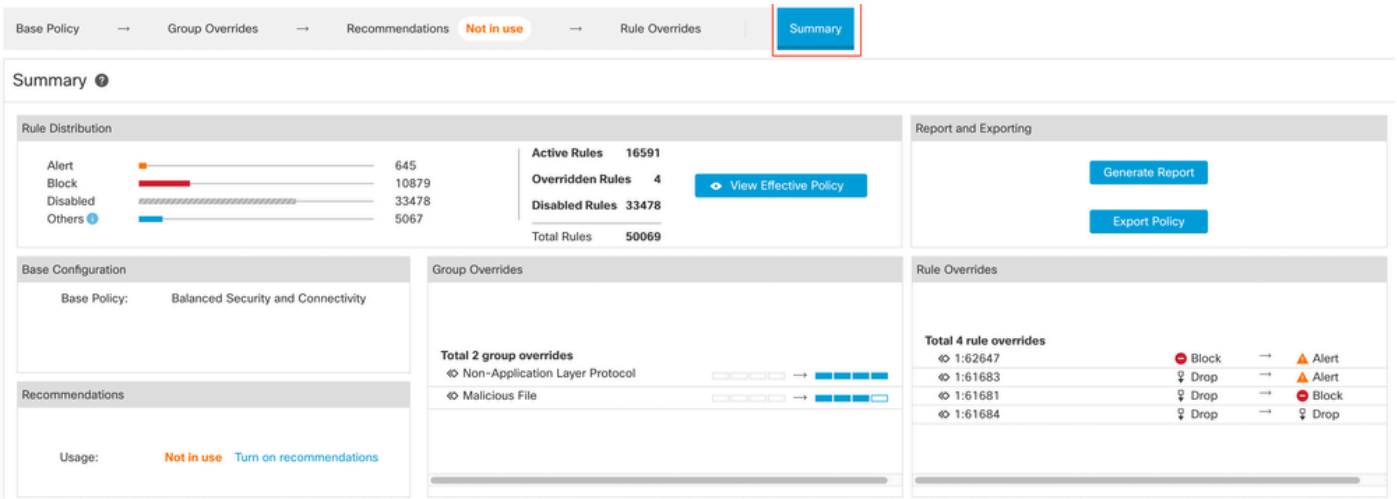
15. Klicken Sie auf RecommendationsEbene aus, und klicken Sie dann aufStart, um die von Cisco empfohlenen Regeln zu verwenden. Mithilfe der Empfehlungen für Angriffsregeln können Sie Schwachstellen identifizieren, die mit Hostressourcen im Netzwerk verbunden sind. finden Sie weitere Informationen.



Empfehlungen



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



Richtlinienübersicht

Angriffsereignisse anzeigen

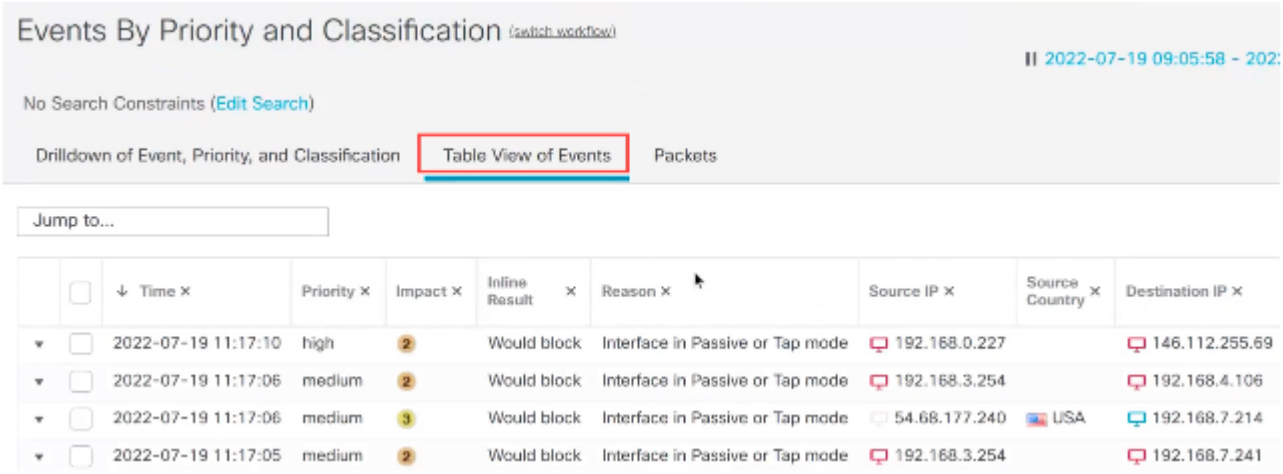
Sie können die MITER ATT&CK-Techniken und Regelgruppen in der klassischen Ereignisanzeige und in der einheitlichen Ereignisanzeige in den Angriffsereignissen anzeigen. Talos stellt

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

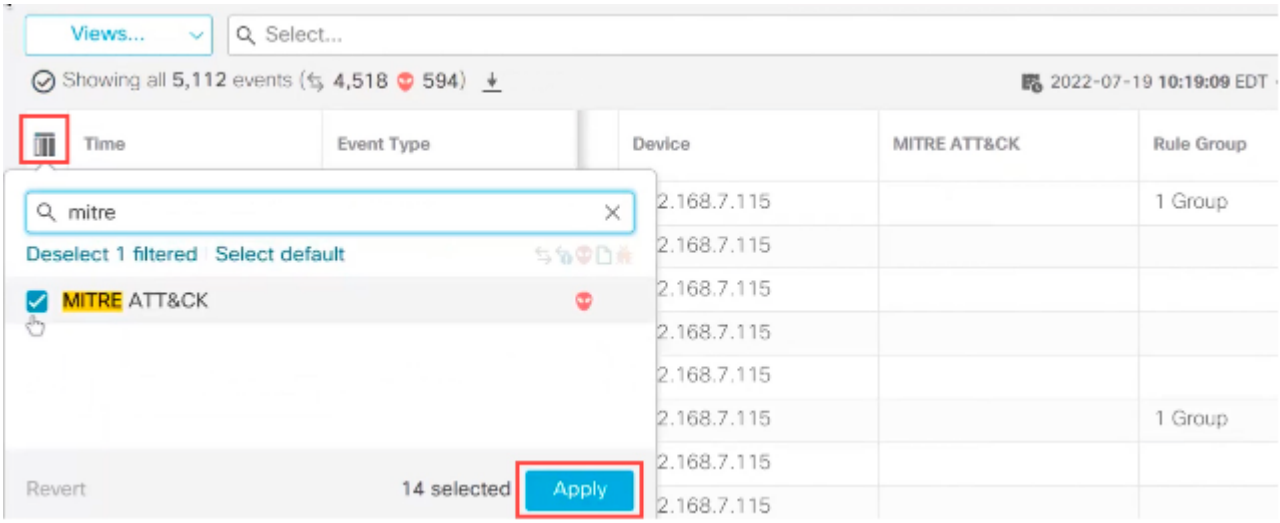
3. Im MITRE ATT&CKSpaltenüberschrift finden Sie die Techniken für ein Angriffsereignis.

Gehrungsspaltenüberschrift

4. Klicken Sie 1 Techniqueum die MITER ATT&CK-Techniken anzuzeigen, wie in dieser Abbildung dargestellt. In diesem Beispiel Exploit Public-Facing Applicationist die Technik.

MITER ATT&CK-Techniken

5. Klicken Sie aufClose.
6. Klicken Sie auf Analysis > Unified Events.
7. Sie können auf das Symbol für die Spaltenauswahl klicken, um die MITRE ATT&CKund die Rule GroupSpalten zu aktivieren.

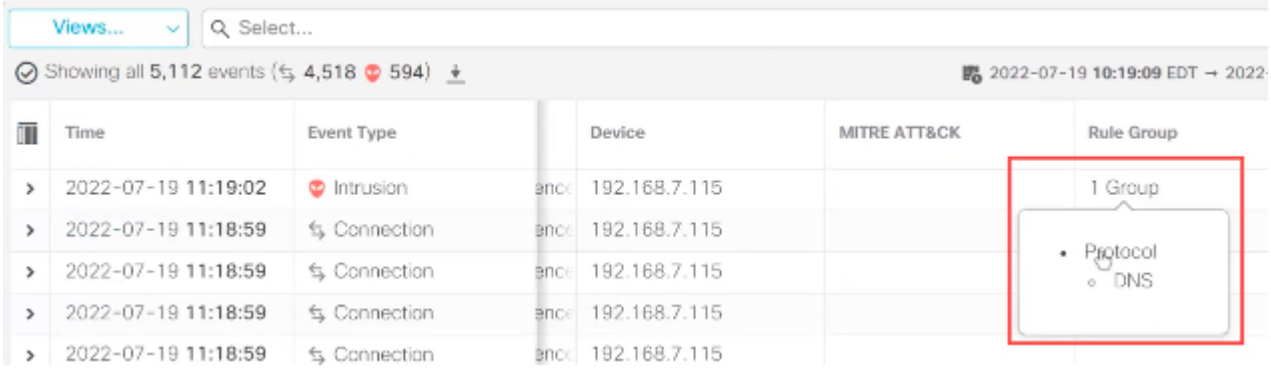


Gehrungsangriff aktivieren

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

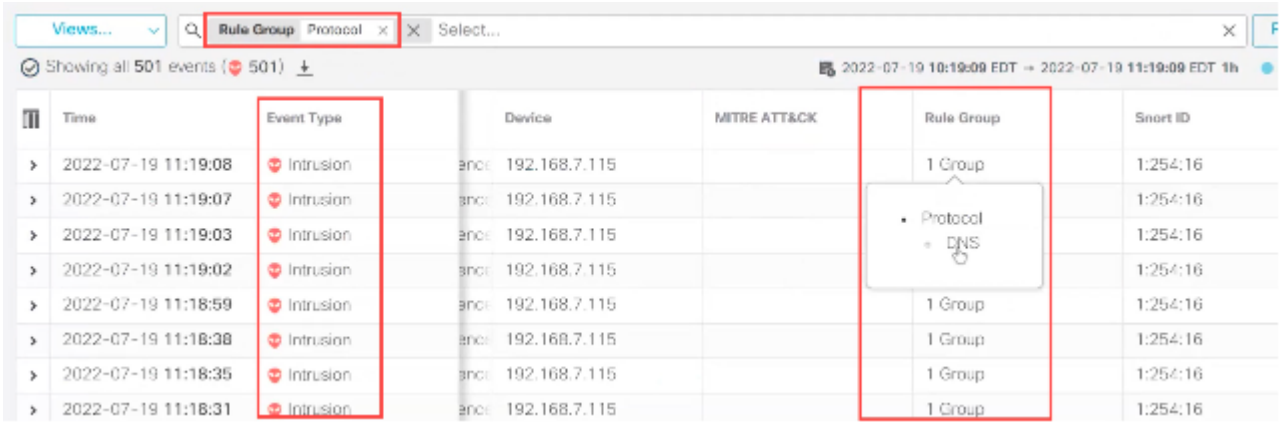
Regelgruppe

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.



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.