Utilice el marco MITER para ver y actuar ante las amenazas potenciales en FMC seguro

Contenido

Introducción

Este documento describe cómo utilizar la estructura MITER para ver y actuar sobre las amenazas potenciales en un Firepower Management Center (FMC) seguro.

Antecedentes

El marco MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es una amplia base de conocimientos y metodología que proporciona información sobre las tácticas, técnicas y procedimientos (TTP) distribuidos por los agentes de amenazas con el objetivo de dañar los sistemas. ATT&CK se compila en matrices que representan sistemas operativos o una plataforma en particular. Cada etapa de un ataque, conocida como "táctica", se asigna a los métodos específicos utilizados para lograr esas etapas, conocidas como "técnicas".

Cada técnica del marco de ATT&CK va acompañada de información sobre la técnica, procedimientos asociados, defensas probables y detecciones, y ejemplos reales. El marco de MITER ATT&CK también incorpora grupos para hacer referencia a grupos de amenazas, grupos de actividad o agentes de amenazas en función del conjunto de tácticas y técnicas que emplean. Mediante el uso de Grupos, el marco de trabajo ayuda a categorizar y documentar comportamientos.

Para obtener más información sobre MITER, consulte https://attack.mitre.org.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Snort
- FMC seguro
- Firepower Threat Defense (FTD) seguro

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Este documento se aplica a todas las plataformas Firepower
- FTD seguro con software versión 7.3.0
- Secure Firepower Management Center Virtual (FMC) con software versión 7.3.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Ventajas del marco MITER

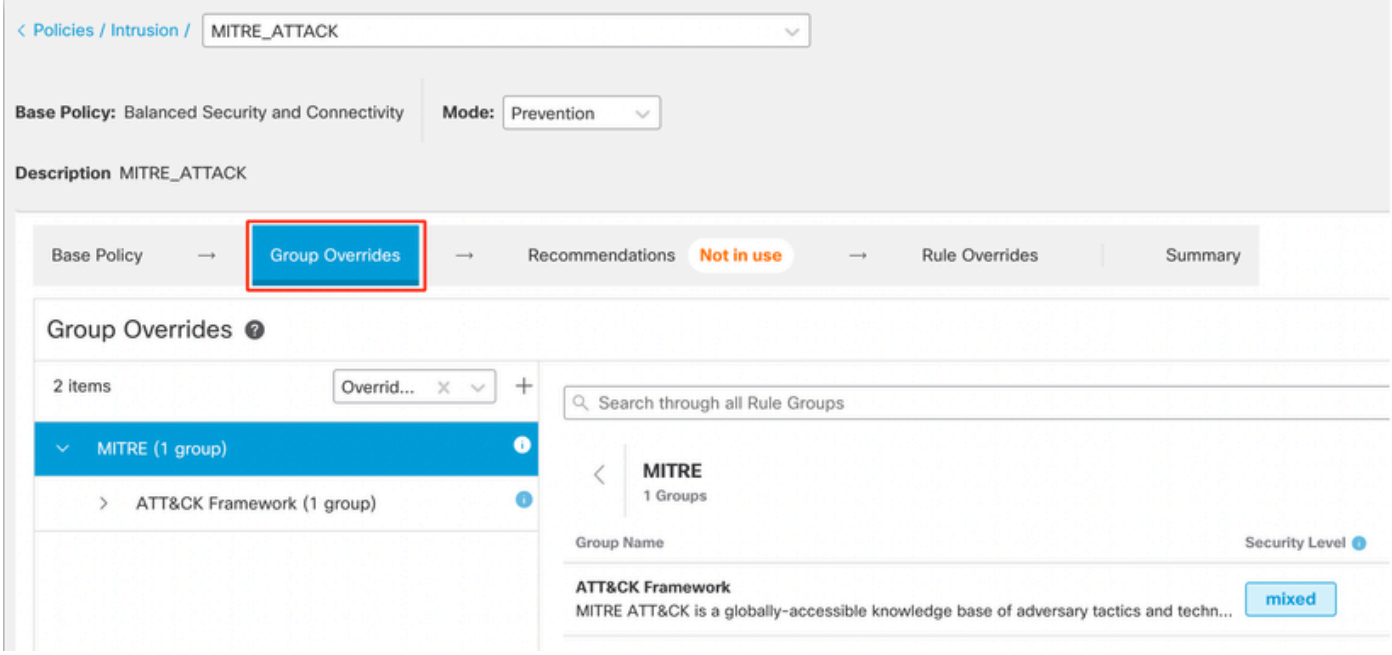
- Las Tácticas, Técnicas y Procedimientos (TTP) MITER se agregan a los eventos de intrusión que permiten a los administradores actuar sobre el tráfico basado en el marco MITER ATT&CK (Técnicas de Tácticas Adversarias y Conocimiento Común). Esto permite a los administradores ver y gestionar el tráfico con mayor granularidad, y pueden agrupar reglas por tipo de vulnerabilidad, sistema de destino o categoría de amenaza.
- Puede organizar las reglas de intrusión según el marco de MITER ATT&CK. Esto le permite personalizar las políticas en función de tácticas y técnicas específicas de los atacantes.

Ver el marco de MITER en su política de intrusiones

La estructura MITER le permite navegar a través de las reglas de intrusión. MITRE es solo otra categoría de grupos de reglas y forma parte de los grupos de reglas Talos. Se admite la exploración de reglas para varios niveles de grupos de reglas, lo que proporciona más flexibilidad y una agrupación lógica de las reglas.

1. Seleccione Policies > Intrusion.
2. Asegúrese de seleccionar la Intrusion Policiespestaña.
3. Haga clic Snort 3 Versionjunto a la política de intrusiones que desea ver o editar. Cierre la guía de ayuda de Snort que aparece.
4. Haga clic en la Group Overridescapa.

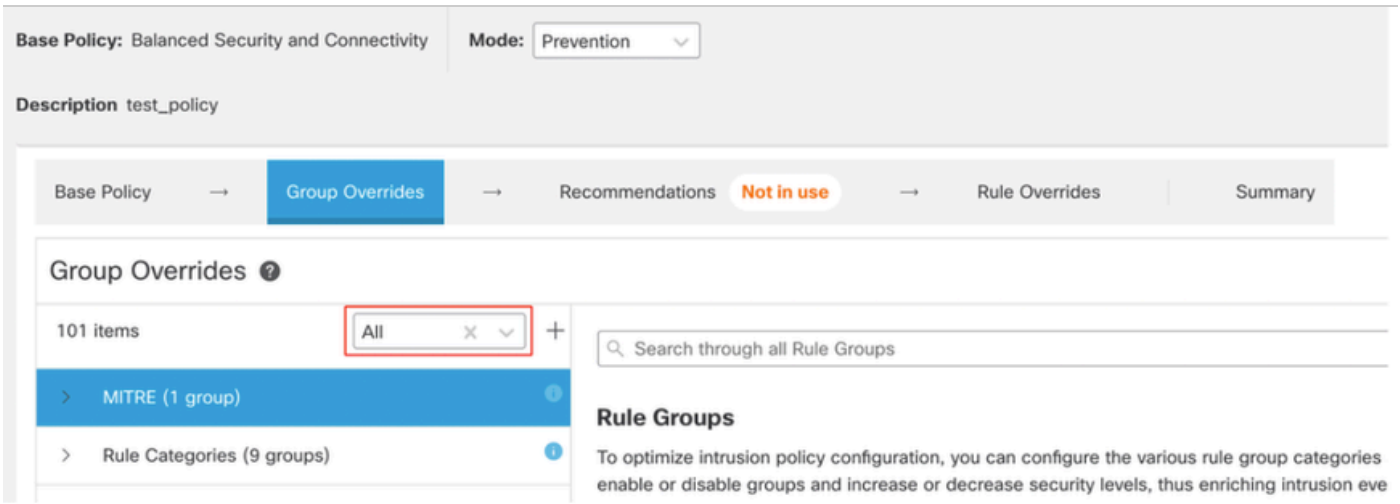
La Group Overridescapa muestra todas las categorías de grupos de reglas en una estructura jerárquica. Puede pasar al último grupo de reglas de hoja de cada grupo de reglas.



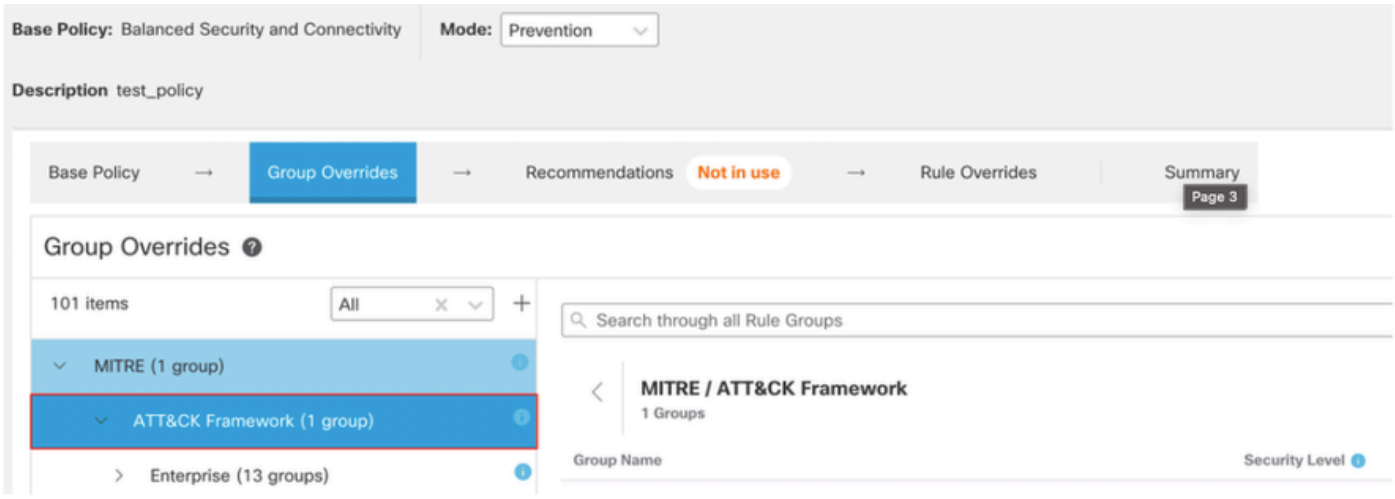
6. En Group Overrides, asegúrese de que Allse elige en la lista desplegable, de modo que todos los grupos de reglas de la directiva de intrusiones estén visibles en el panel izquierdo.

7. Haga clic MITREen el panel izquierdo.

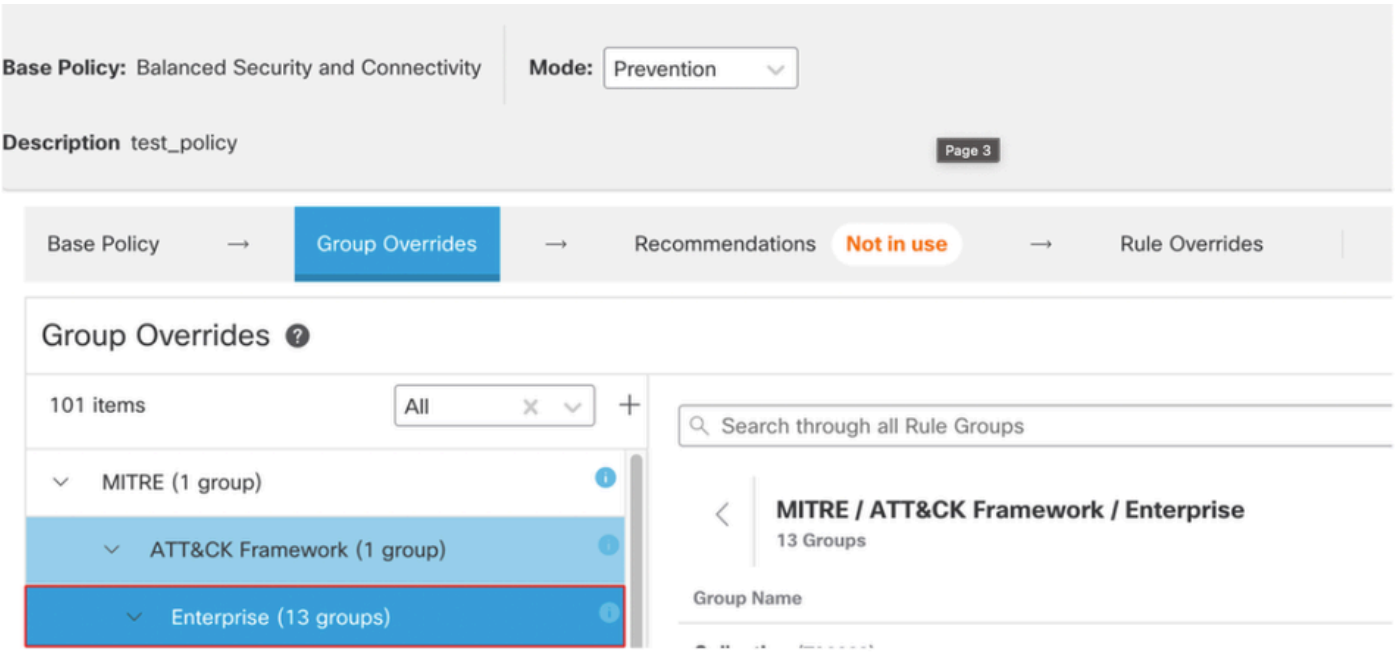
Nota: En este ejemplo, se selecciona MITRE, pero, en función de sus requisitos específicos, puede elegir el grupo de reglas Categorías de regla o cualquier otro grupo de reglas y los grupos de reglas subsiguientes bajo él. Todos los grupos de reglas utilizan la estructura MITER.



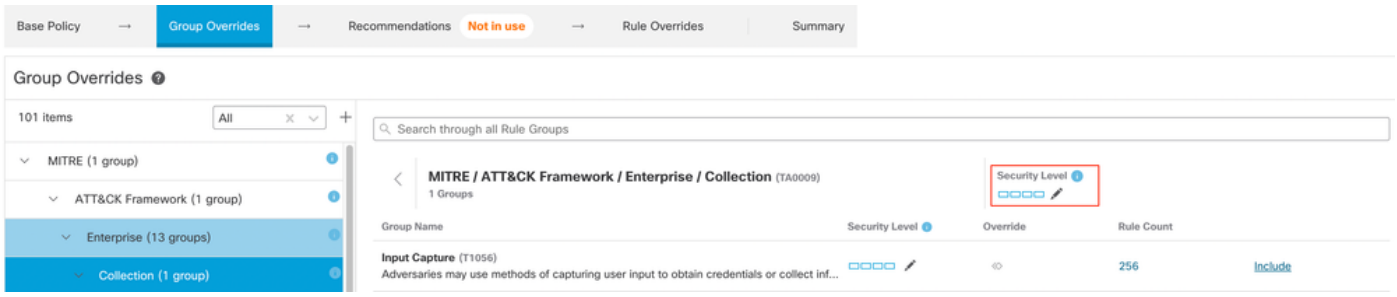
8. EnMITRE, haga clic en ATT&CK Marco conceptual para expandirlo.



9. En ATT&CK Framework, haga clic en Empresa para expandirla.

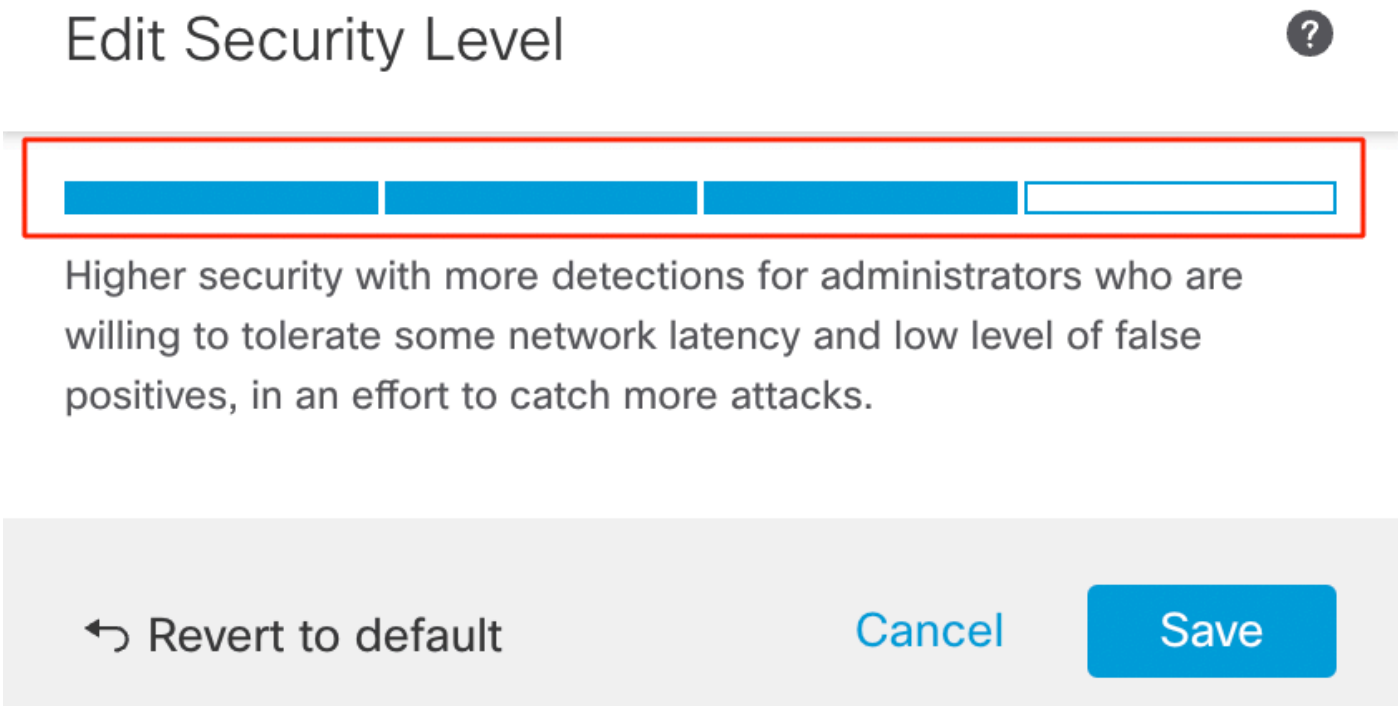


10. Haga clic Edit ( ) junto al nivel de seguridad del grupo de reglas para realizar cambios masivos en el nivel de seguridad de todos los grupos de reglas asociados en el Enterprisecategoría de grupo de reglas.



Editar grupo de reglas de seguridad

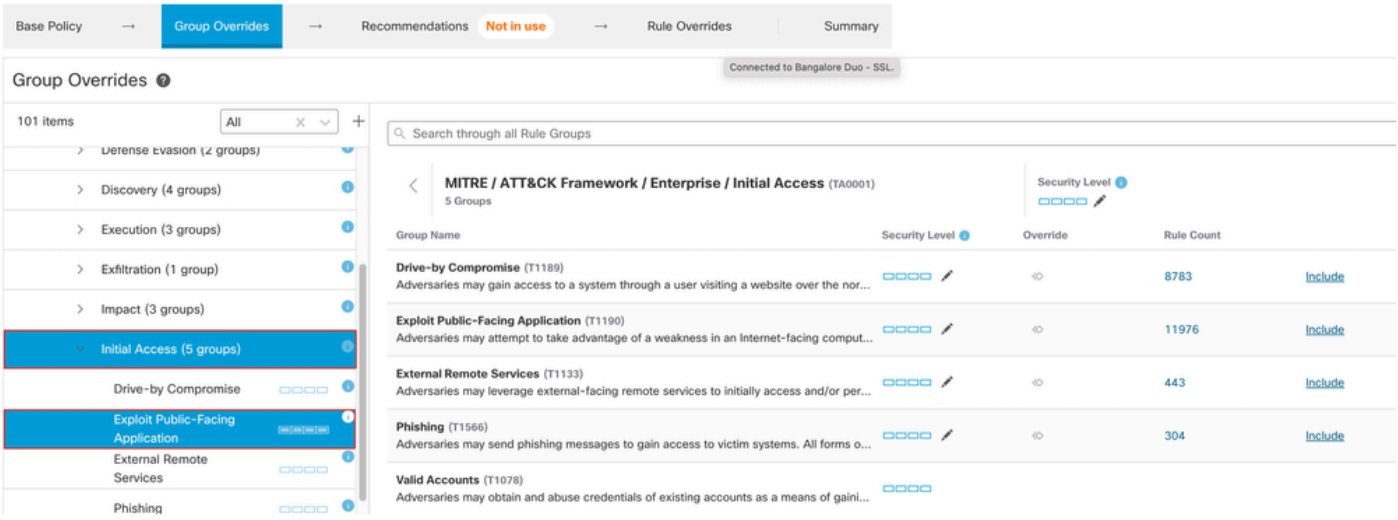
11. Por ejemplo, seleccione el nivel de seguridad 3 en la Edit Security Level ventana y haga clic en **Save**.



Nivel de seguridad

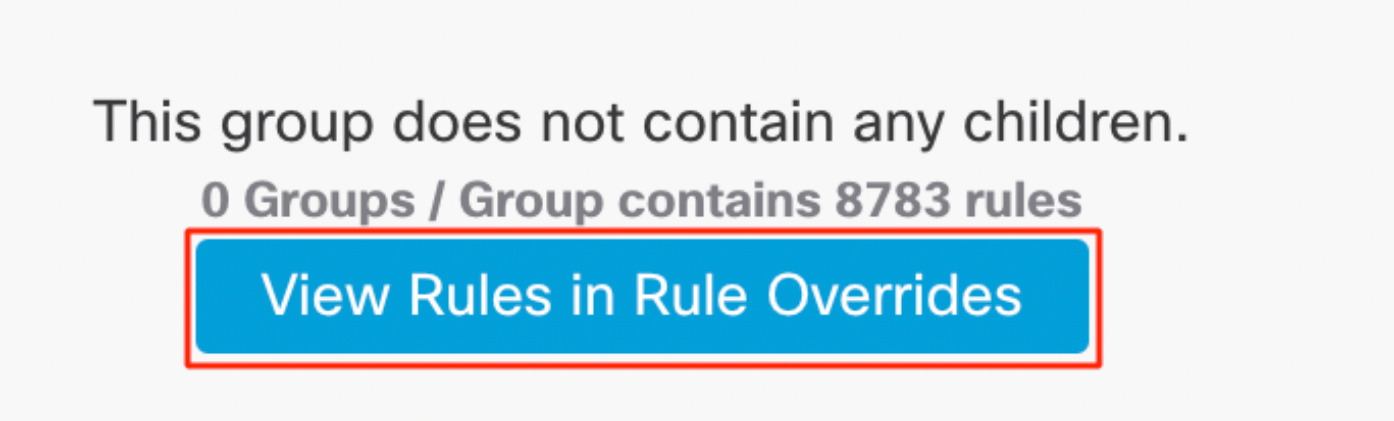
12. En Enterprise, haga clic Initial Accesspara expandirlo.

13. En Initial Access, haga clic en Exploit Public-Facing Application, que es el último grupo de hojas.



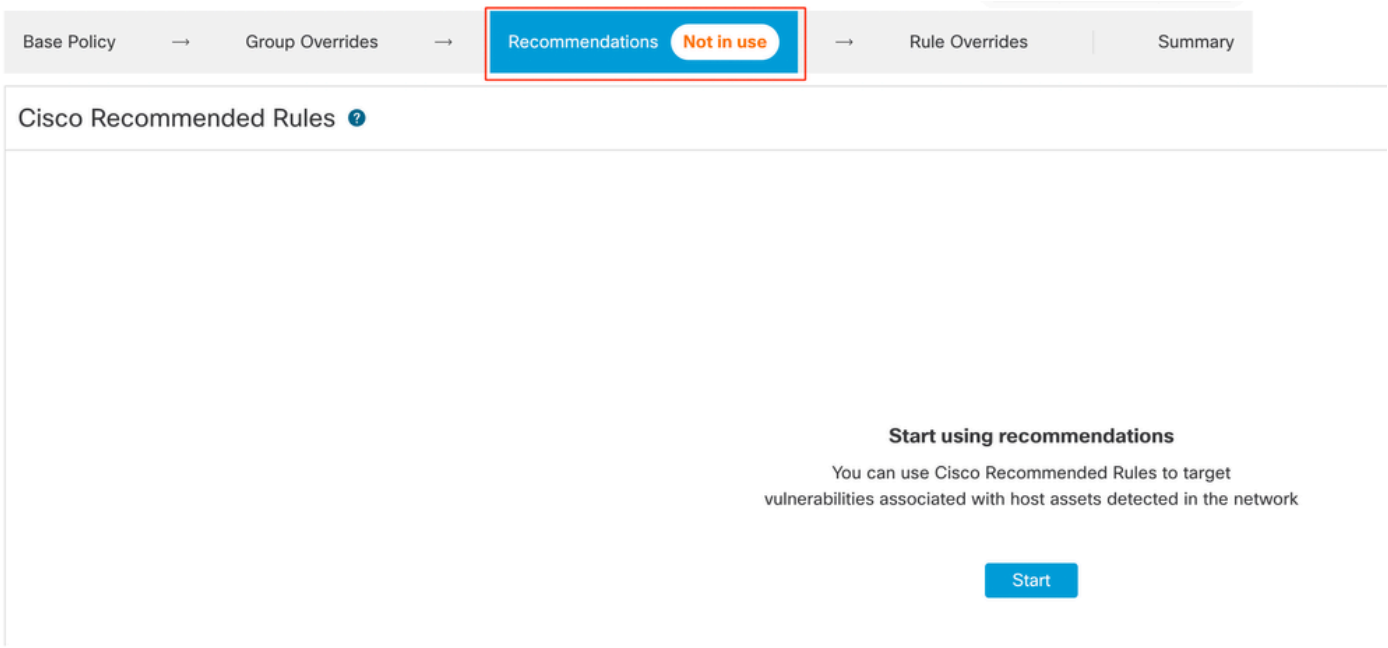
Grupo de acceso inicial

14. Haga clic en el botón **View Rules in Rule Overrides**para ver las distintas reglas, detalles de reglas, acciones de regla, etc. de las distintas reglas.

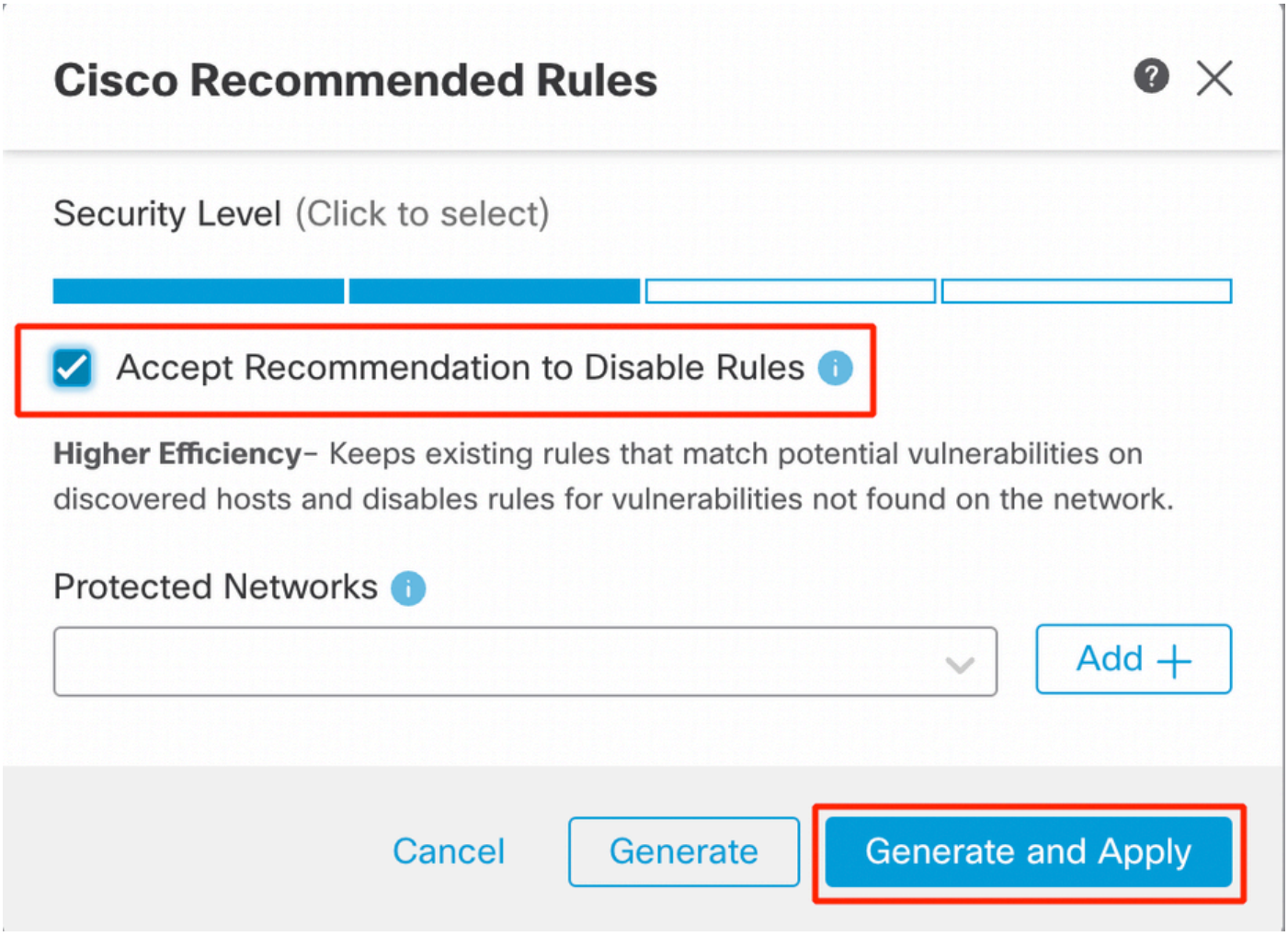


Reglas de anulaciones de reglas

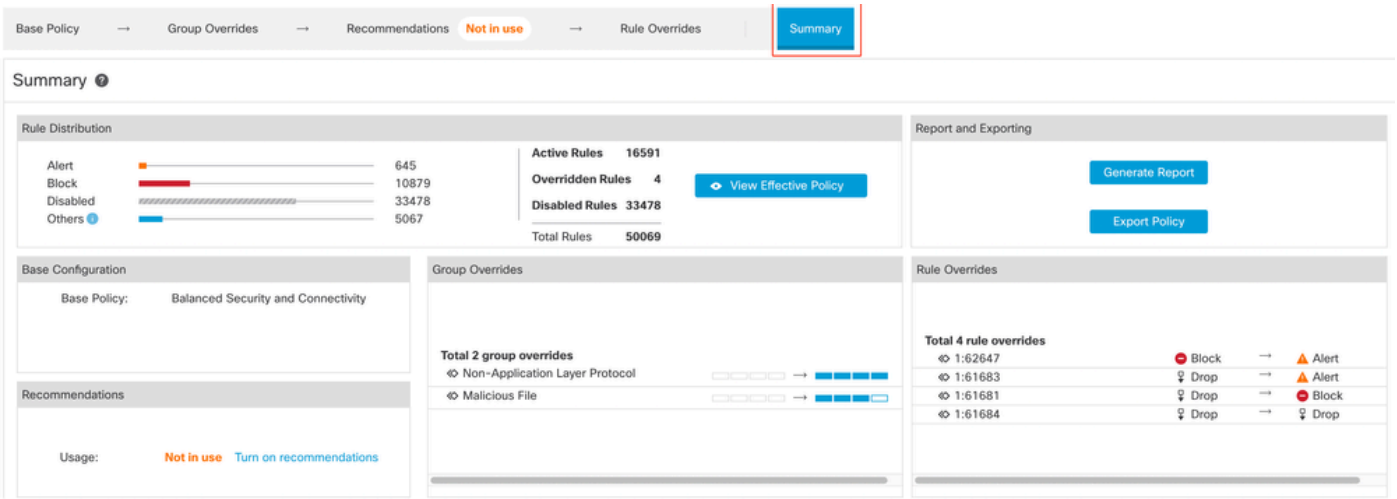
15. Haga clic en el botón Recommendationsy, a continuación, haga clicStartpara empezar a utilizar las reglas recomendadas por Cisco. Puede utilizar las recomendaciones de reglas de intrusión para identificar las vulnerabilidades asociadas con los activos de host detectados en la red. Para más información.



Recomendaciones



16. Haga clic en el botón Summarypara obtener una vista integral de los cambios actuales de la política. Puede ver la distribución de reglas de la directiva, las invalidaciones de grupos, las invalidaciones de reglas, etc.



Resumen de políticas

Ver eventos de intrusión

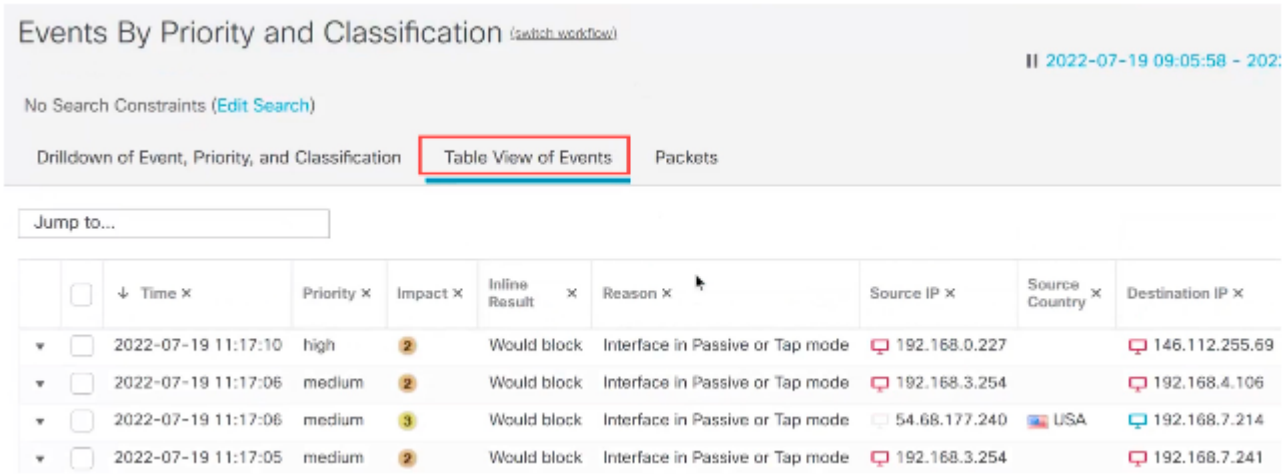
Puede ver las técnicas y grupos de reglas de MITER ATT&CK en los eventos de intrusión en el Visor de eventos clásico y el Visor de eventos unificado. Talos proporciona asignaciones de

reglas de Snort (GID:SID) a técnicas y grupos de reglas MITER AT&CK. Estas asignaciones se instalan como parte del paquete de seguridad ligero (LSP).

Antes de comenzar, deben implementarse las directivas de control de acceso e intrusiones para detectar y registrar los eventos desencadenados por las reglas de Snort.

1. Haga clic en Analysis > Intrusions > Events.

2. Haga clic en el botón **Table View of Events**como se muestra en la imagen.

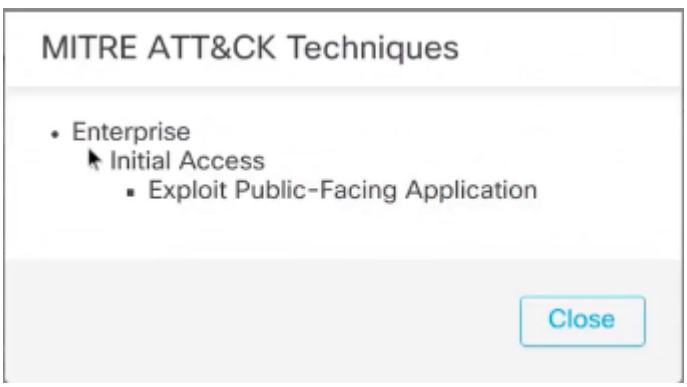


Events

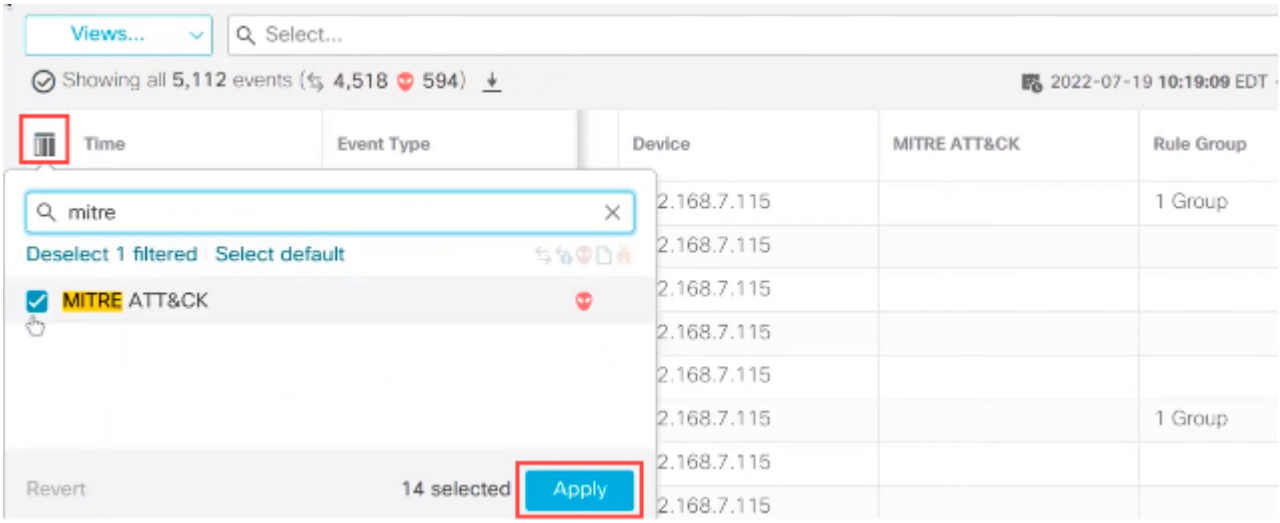
3. En el MITRE ATT&CKencabezado de columna, puede ver las técnicas para un evento de intrusión.

Encabezado de columna inglete

4. Haga clic 1 Techniquepara ver las Técnicas ATT&CK de MITER, como se muestra en esta figura. En este ejemplo, Exploit Public-Facing Applicationes la técnica.



5. Haga clic enClose.
6. Haga clic en Analysis > Unified Events.
7. Puede hacer clic en el icono selector de columna para activar las columnas MITRE ATT&CKy Rule Groupe.

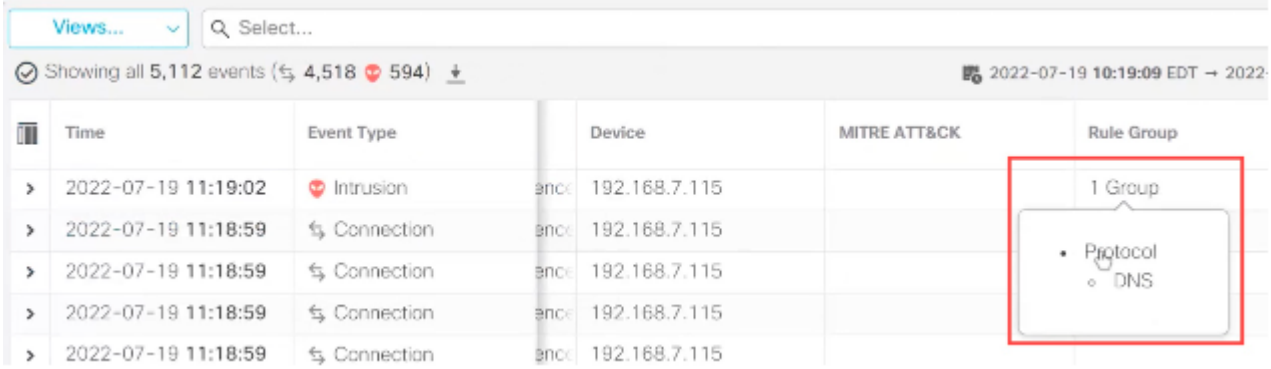


Habilitar el ataque de inglete

8. Como se muestra en el ejemplo, el evento de intrusión fue activado por un evento asignado a un grupo de reglas. Haga clic 1 Group en la Rule Groupcolumna.

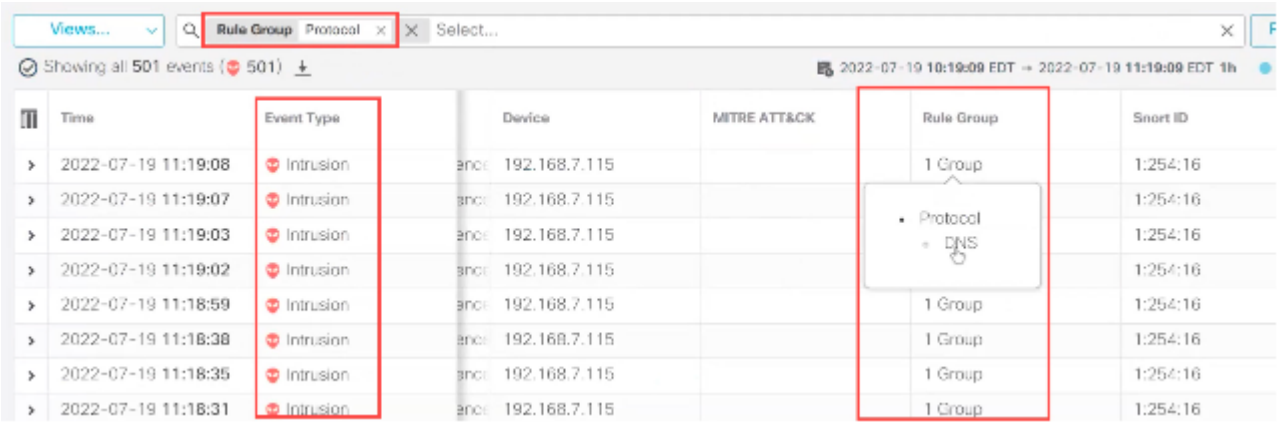
Grupo de reglas

9. Por ejemplo, puede ver Protocolo, que es el grupo de reglas principal, y el grupo de reglas DNS que se encuentra debajo.



Ver protocolo

10. Puede hacer clicProtocolpara buscar todos los eventos de intrusión que tienen al menos un grupo de reglas, es decir, Protocol > DNS . Se muestran los resultados de la búsqueda, como se muestra en el ejemplo siguiente.



Protocolo de grupo de reglas

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).