Utilizzare il framework MITER per visualizzare e agire sulle minacce potenziali in un FMC protetto

Sommario

Introduzione

Premesse

Prerequisiti

- Requisiti
- Componenti usati

Vantaggi del framework MITER

- Visualizzare il framework MITER nei criteri per le intrusioni
- Visualizza eventi di intrusione

Introduzione

Questo documento descrive come utilizzare il framework MITER per visualizzare e agire su potenziali minacce in un centro di gestione sicura di Firepower (FMC).

Premesse

Il framework MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) è un'ampia base di conoscenze e metodologie che fornisce informazioni sulle tattiche, le tecniche e le procedure (TTP) distribuite da attori della minaccia che mirano a danneggiare i sistemi. ATT&CK viene compilato in matrici che rappresentano ciascuna sistema operativo o una particolare piattaforma. Ogni fase di un attacco, nota come "tattica", è mappata ai metodi specifici utilizzati per raggiungere quelle fasi, note come "tecniche".

Ogni tecnica nel framework ATT&CK è accompagnata da informazioni sulla tecnica, le procedure associate, le probabili difese e rilevamenti, ed esempi reali. La struttura MITER ATT&CK incorpora anche Gruppi per fare riferimento a gruppi di minacce, gruppi di attività o attori di minaccia in base alla serie di tattiche e tecniche impiegate. Tramite l'utilizzo dei gruppi, il framework semplifica la categorizzazione e la documentazione dei comportamenti.

Per ulteriori informazioni su MITER, visitare il sito Web all'indirizzo https://attack.mitre.org.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Snort
- Secure FMC
- Secure Firepower Threat Defense (FTD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Questo documento è valido per tutte le piattaforme Firepower
- Secure FTD con software versione 7.3.0
- Secure Firepower Management Center Virtual (FMC) con software versione 7.3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Vantaggi del framework MITER

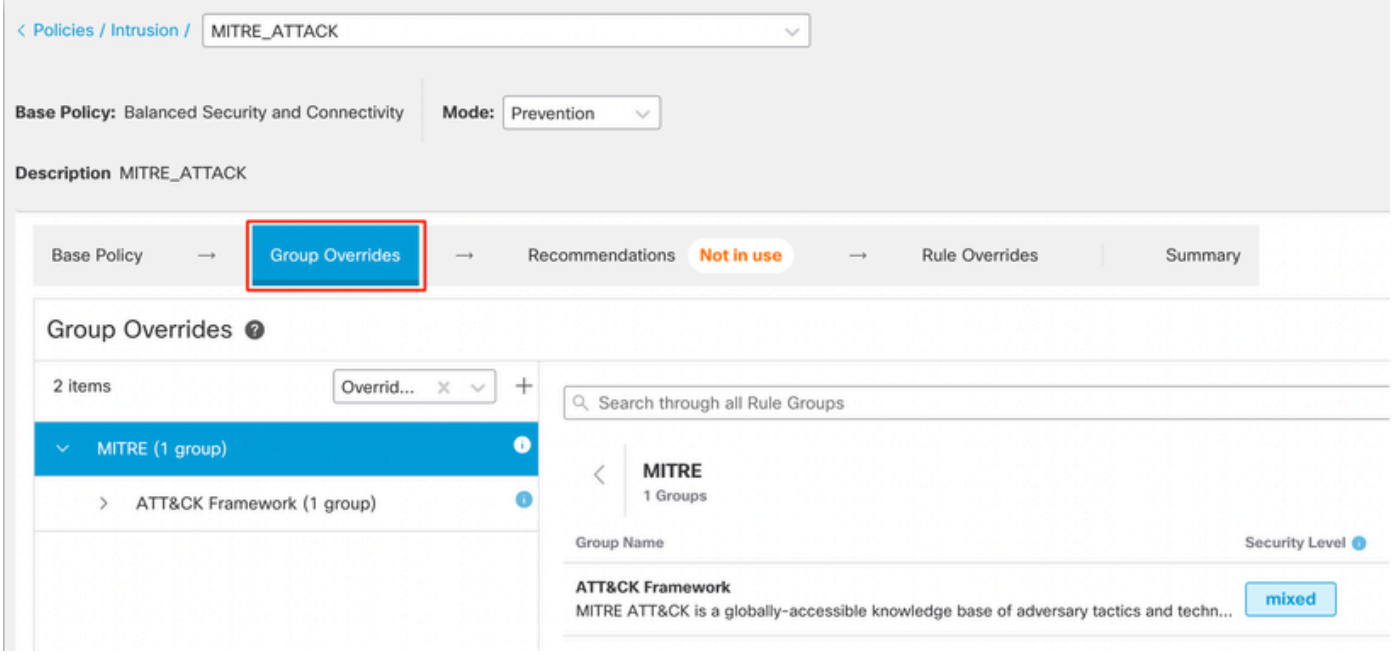
- Tattiche, tecniche e procedure MITER (TTP) vengono aggiunte agli eventi di intrusione che consentono agli amministratori di agire sul traffico in base alla struttura ATT&CK (Adversary Tactics Techniques and Common Knowledge) di MITER. Ciò consente agli amministratori di visualizzare e gestire il traffico con maggiore granularità e di raggruppare le regole per tipo di vulnerabilità, sistema di destinazione o categoria di minaccia.
- È possibile organizzare le regole di intrusione in base al framework ATT&CK MITER. In questo modo è possibile personalizzare i criteri in base a tattiche e tecniche specifiche.

Visualizzare il framework MITER nei criteri per le intrusioni

Il framework MITER consente di spostarsi tra le regole di intrusione. MITER è solo un'altra categoria di gruppi di regole e fa parte dei gruppi di regole Talos. È supportata la navigazione tra le regole per diversi livelli di gruppi di regole, che offre maggiore flessibilità e raggruppamento logico delle regole.

1. Scegliere Policies > Intrusion.
2. Assicurarsi che la Intrusion Policiesscheda sia selezionata.
3. Fare clic su Snort 3 Versionaccanto al criterio intrusione che si desidera visualizzare o modificare. Chiudere la guida di supporto Snort visualizzata.
4. Fare clic sul Group Overrideslivello.

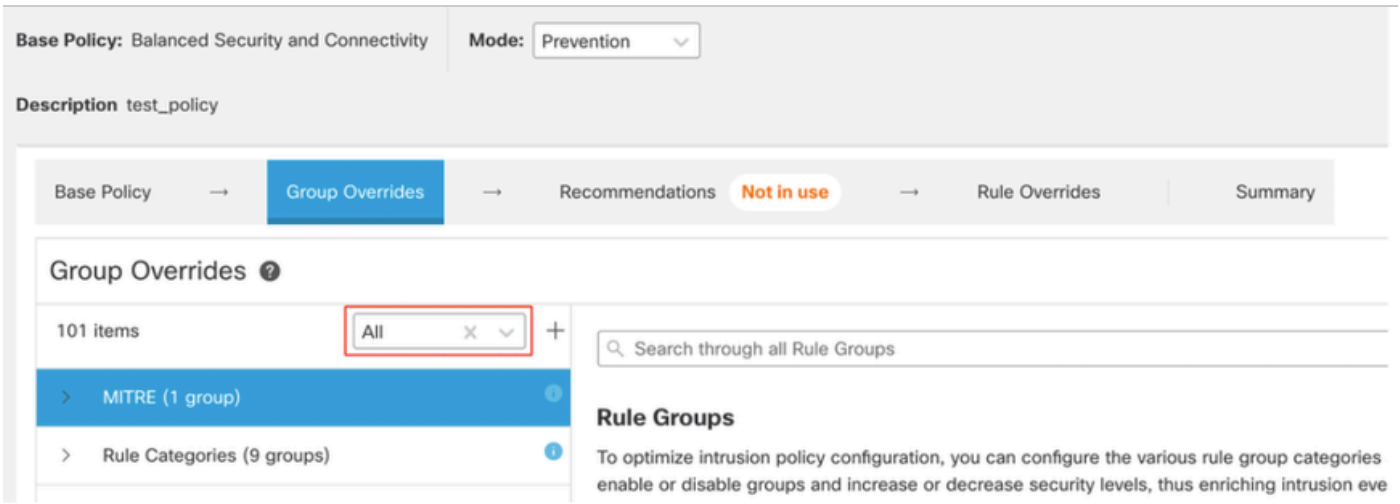
Il Group Overrideslivello elenca tutte le categorie di gruppi di regole in una struttura gerarchica. È possibile passare all'ultimo gruppo di regole foglia in ogni gruppo di regole.



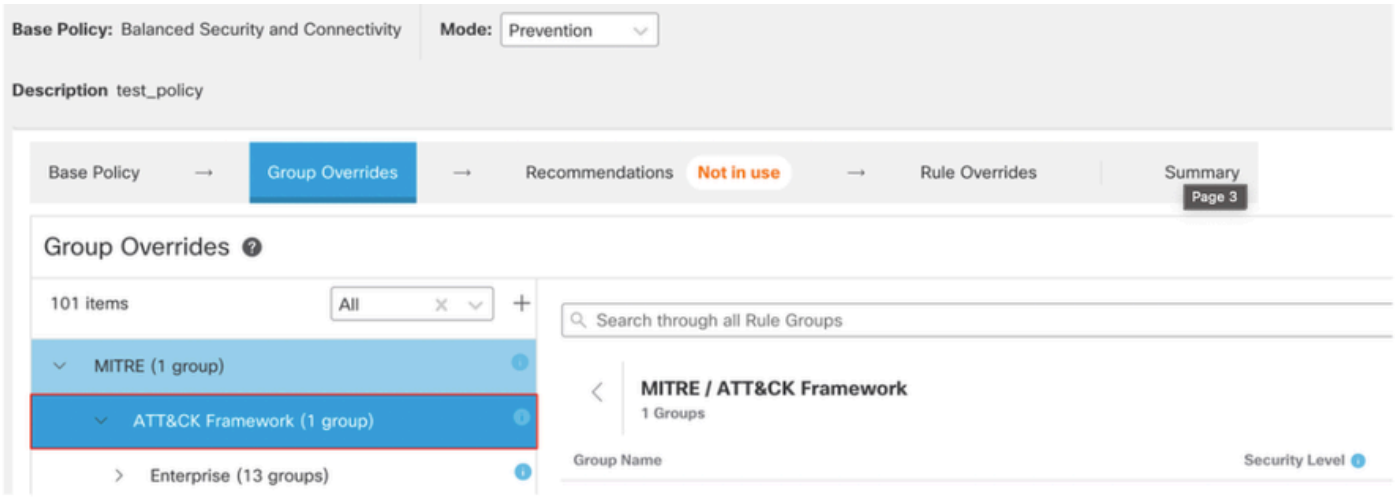
6. Nell'ambito Group Overrides, Allè selezionato nell'elenco a discesa, in modo che tutti i gruppi di regole per il criterio intrusione siano visibili nel riquadro sinistro.

7. Fare clic su MITREnel riquadro di sinistra.

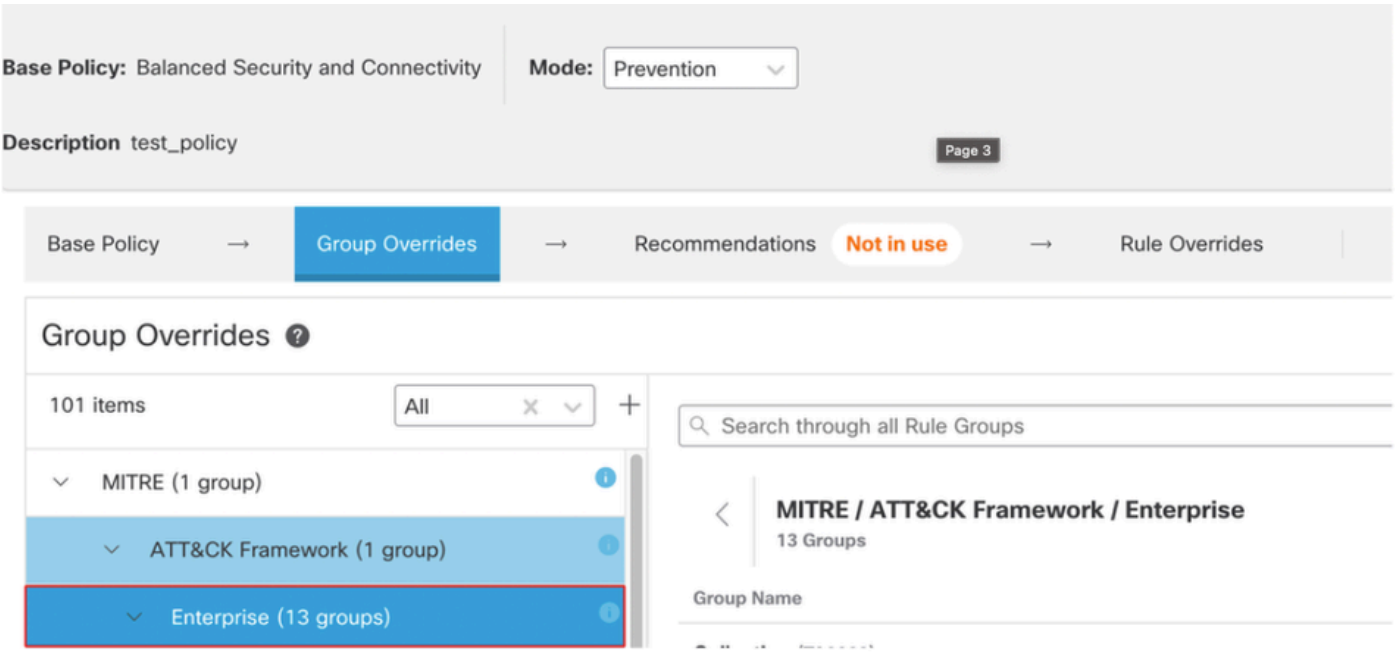
Nota: Per questo esempio, è selezionato MITER, ma a seconda dei requisiti specifici, è possibile scegliere il gruppo di regole Categorie regole o qualsiasi altro gruppo di regole e i gruppi di regole successivi al suo interno. Tutti i gruppi di regole utilizzano il framework MITER.



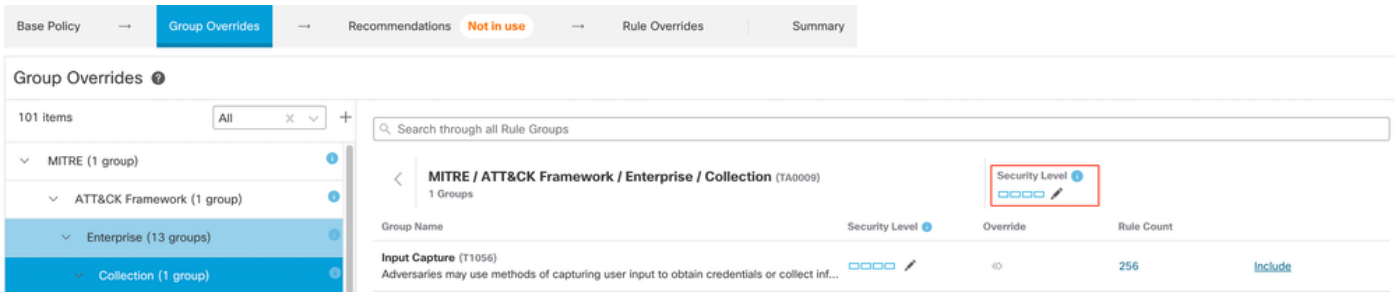
8. InMITRE, fare clic su ATT&CK Framework per espanderlo.



9. In ATT&CK Framework, fare clic su Azienda per espanderla.

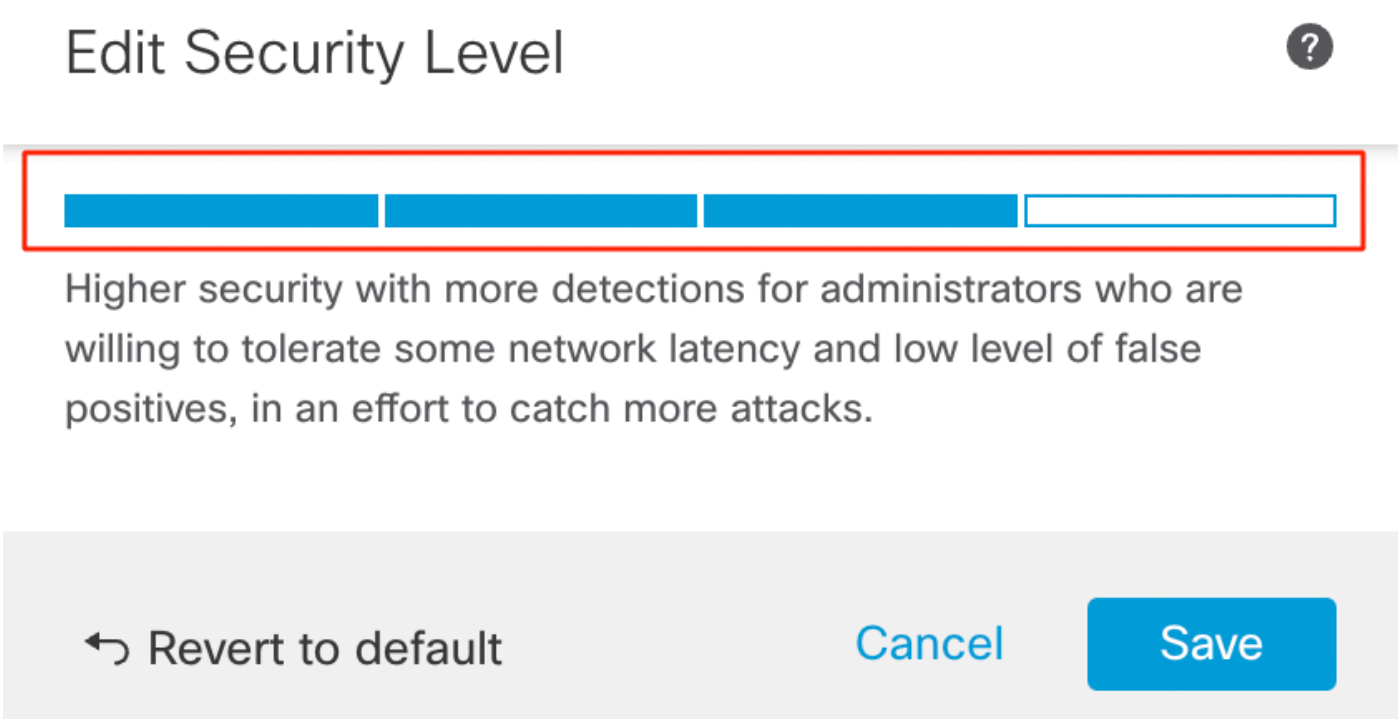


10. Fare clic su Edit ( ) accanto al livello di protezione del gruppo di regole per apportare modifiche di massa al livello di protezione per tutti i gruppi di regole associati nel gruppo Enterprisecategoria del gruppo di regole.



Modifica gruppo di regole di sicurezza

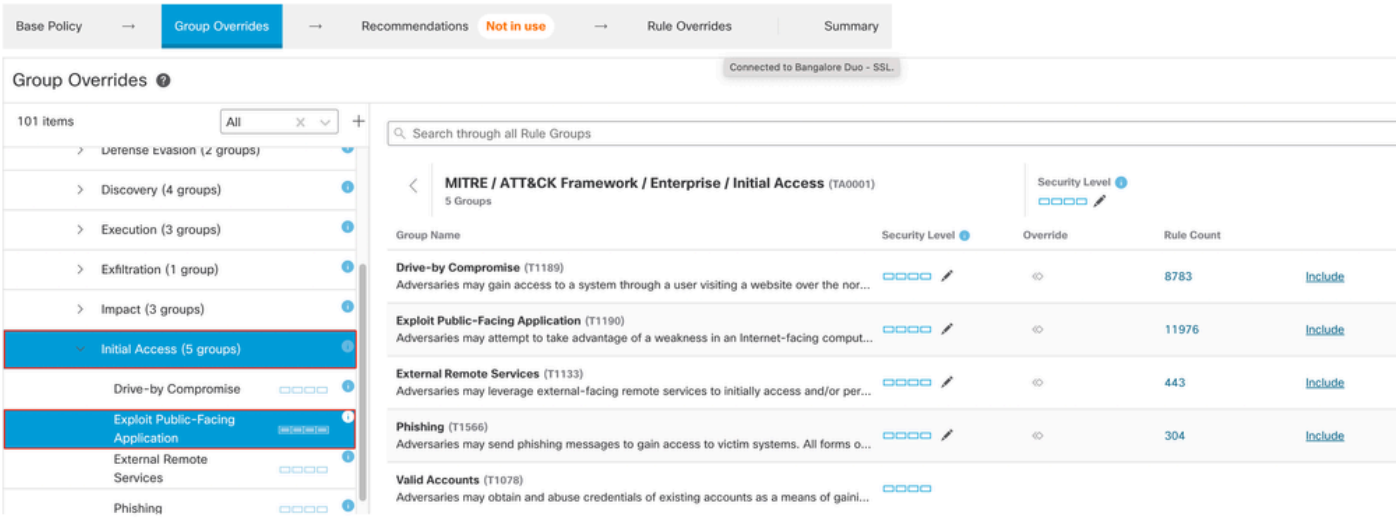
11. Ad esempio, scegliere il livello di protezione 3 nella Edit Security Level finestra e fare clic su **Save**.



Livello di protezione

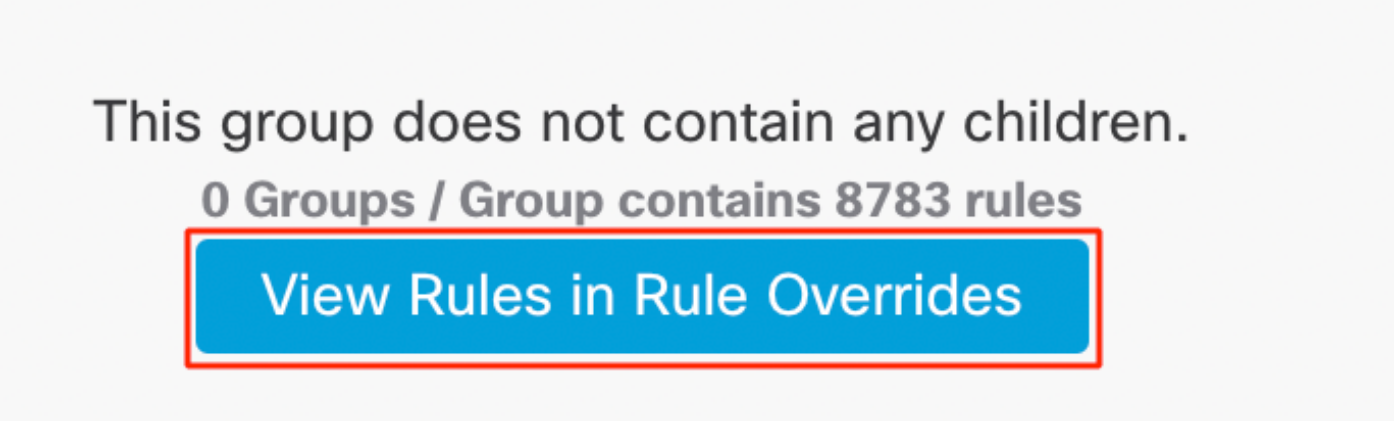
12. In Enterprise, fare clic Initial Accessper espanderlo.

13. In Initial Access, fare clic su Exploit Public-Facing Application, che è l'ultimo gruppo foglia.



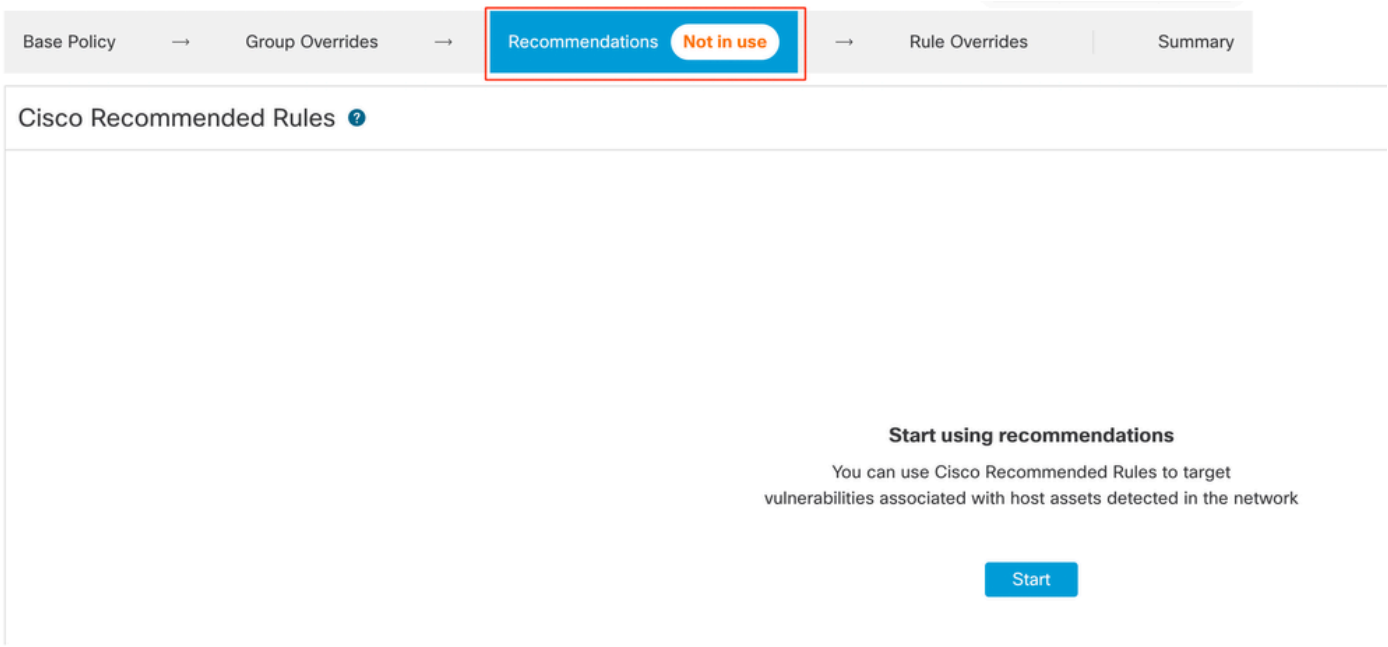
Gruppo di accesso iniziale

14. Fare clic sul pulsante **View Rules in Rule Overrides**per visualizzare le diverse regole, i dettagli delle regole, le azioni delle regole e così via per le diverse regole.

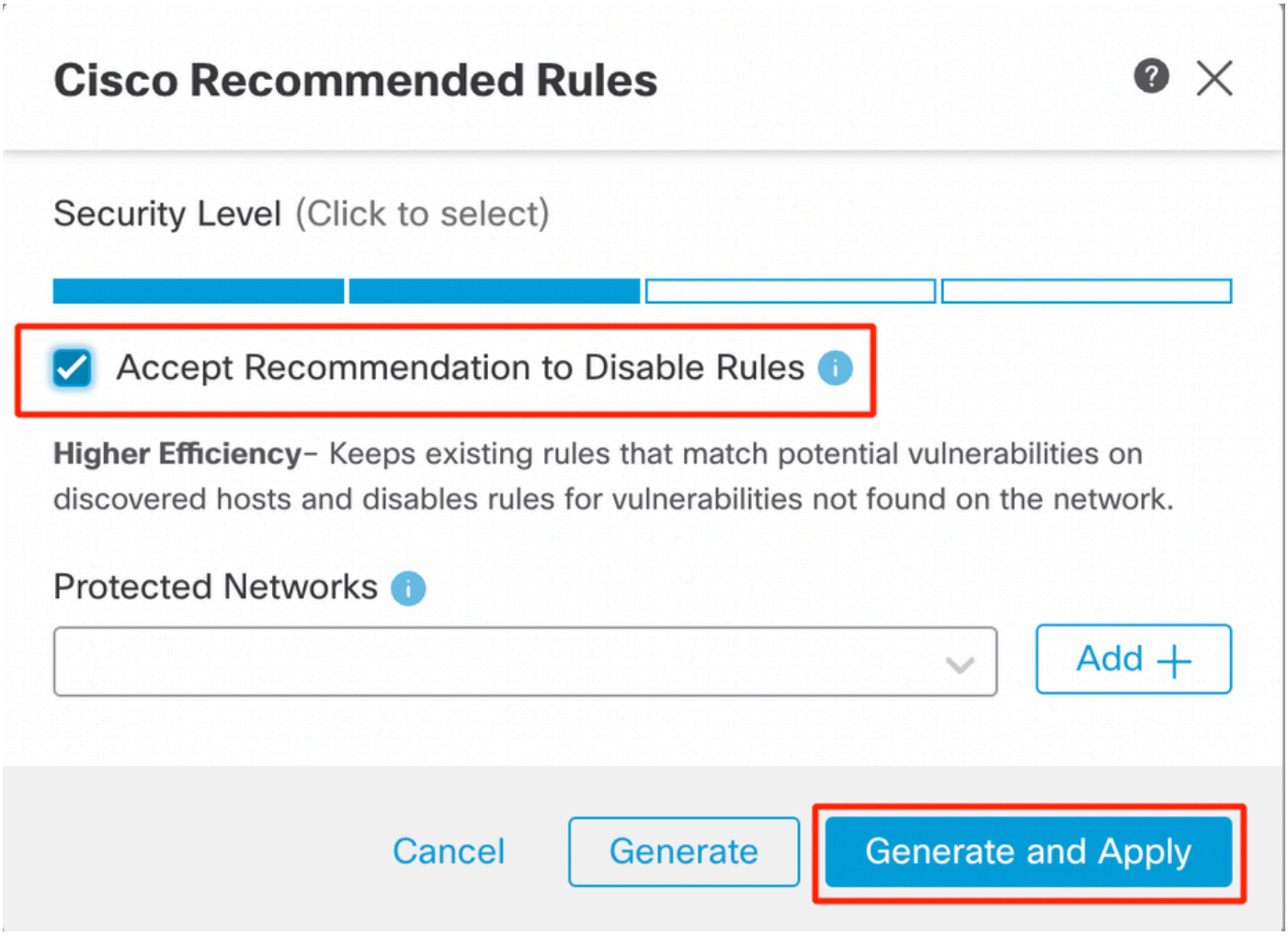


Regole in sostituzioni regole

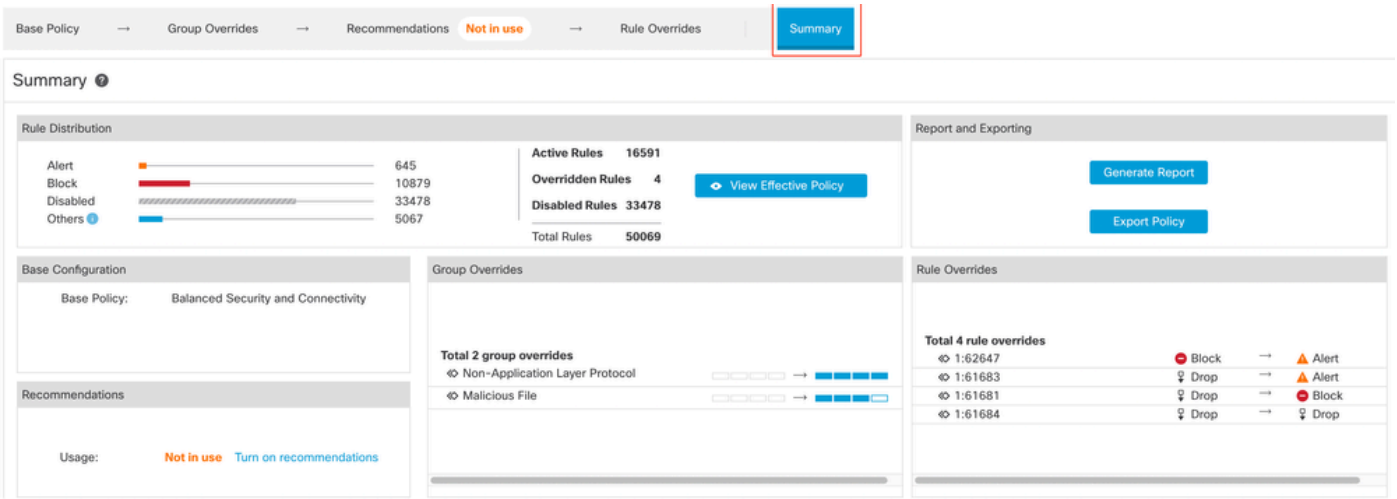
15. Fare clic sul pulsante Recommendationse quindi fare clic suStartper iniziare a utilizzare le regole consigliate da Cisco. È possibile utilizzare i suggerimenti per le regole di intrusione per individuare le vulnerabilità associate agli asset host rilevati nella rete. Ulteriori informazioni.



Consigli



16. Fare clic sul pulsante Summaryper una visualizzazione olistica delle modifiche correnti al criterio. È possibile visualizzare la distribuzione delle regole del criterio, le sostituzioni di gruppo, le sostituzioni di regola e così via.



Riepilogo criteri

Visualizza eventi di intrusione

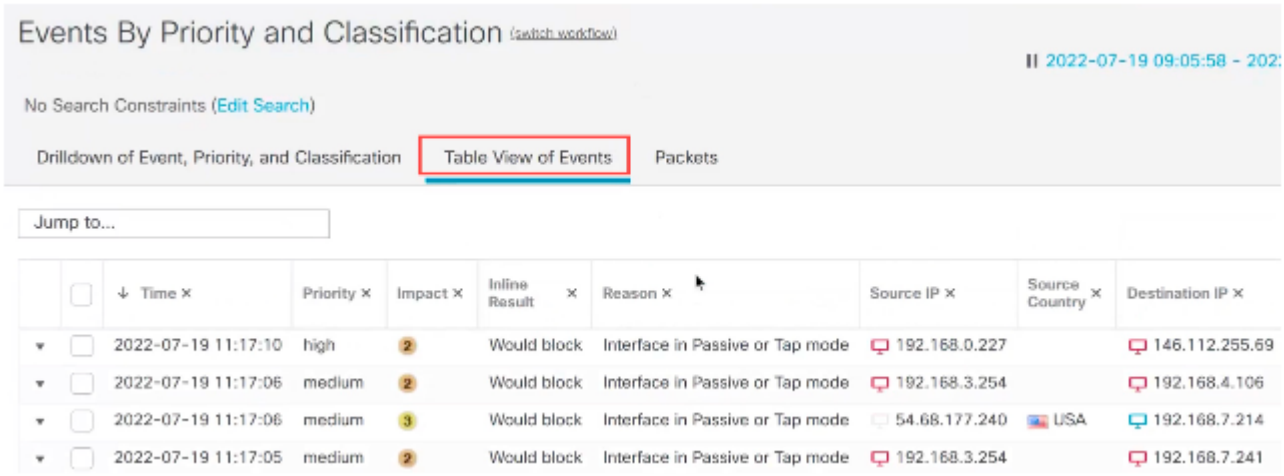
È possibile visualizzare le tecniche e i gruppi di regole ATT&CK MITER negli eventi di intrusione nel Visualizzatore eventi classico e nel Visualizzatore eventi unificato. Talos fornisce i mapping

dalle regole di tipo Snort (GID:SID) alle tecniche e ai gruppi di regole ATT&CK MITER. Questi mapping vengono installati come parte del Lightweight Security Package (LSP).

Prima di iniziare, è necessario distribuire i criteri di controllo delle intrusioni e degli accessi per rilevare e registrare gli eventi attivati dalle regole Snort.

1. Fare clic su Analysis > Intrusions > Events.

2. Fare clic sul pulsante **Table View of Events**come mostrato nell'immagine.

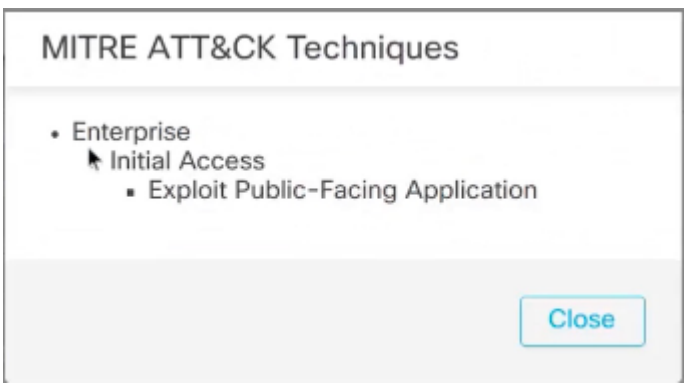


Eventi

3. Nel MITRE ATT&CKnell'intestazione di colonna è possibile visualizzare le tecniche per un evento intrusione.

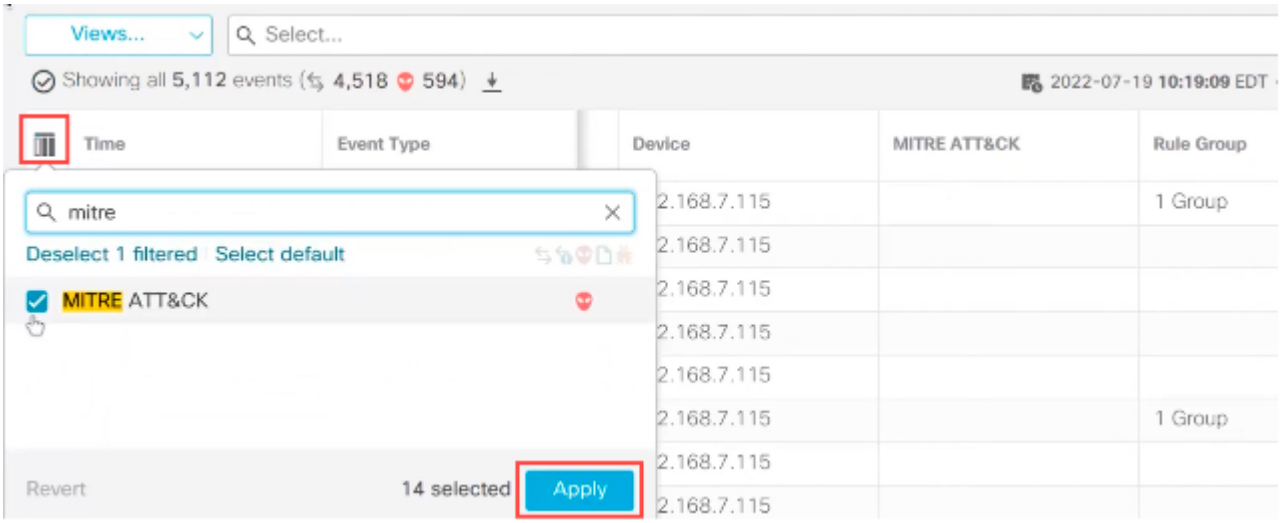
Intestazione colonna Angoli

4. Fare clic 1 Techniqueper visualizzare le tecniche ATT&CK di MITER, come illustrato nella figura riportata di seguito. In questo esempio, Exploit Public-Facing Applicationè la tecnica.



Tecniche ATT&CK MITER

5. Fare clic suClose.
6. Fare clic su Analysis > Unified Events.
7. È possibile fare clic sull'icona del selettore di colonne per abilitare le colonne MITRE ATT&CKe Rule Groupdi.

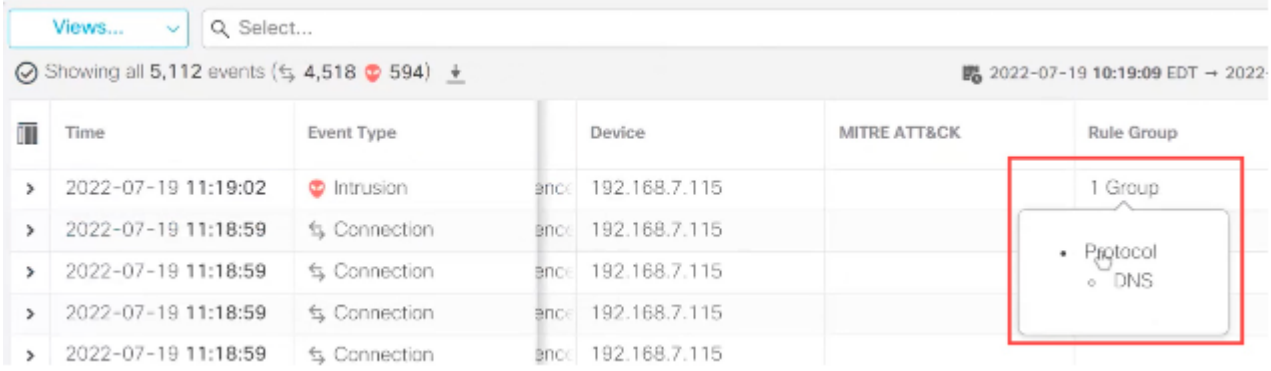


Abilita attacco a 45°

8. Come illustrato nell'esempio, l'evento intrusione è stato attivato da un evento mappato a un gruppo di regole. Fare clic 1 Group sotto Rule Groupcolonna.

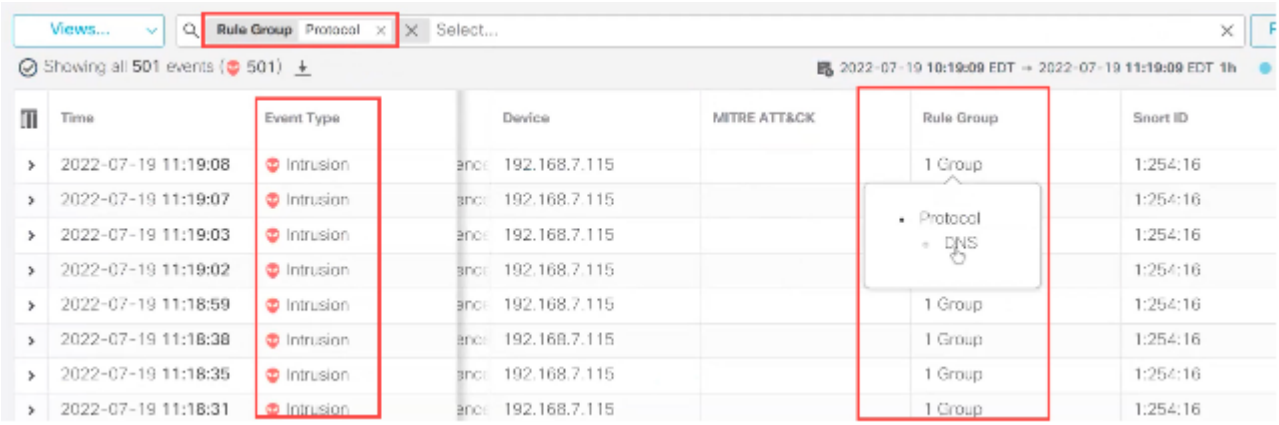
Gruppo di regole

9. Ad esempio, è possibile visualizzare il gruppo di regole Protocol, che è il gruppo di regole padre, e il gruppo di regole DNS sottostante.



Visualizza protocollo

10. È possibile fare clic suProtocolper cercare tutti gli eventi di intrusione che hanno almeno un gruppo di regole, ovvero Protocol > DNS . Vengono visualizzati i risultati della ricerca, come mostrato nell'esempio riportato di seguito.



Protocollo gruppo di regole

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).