使用MITER框架檢視安全FMC中的潛在威脅並採取相應措施

目錄

簡介

本文檔介紹如何使用MITER框架檢視安全Firepower管理中心(FMC)中的潛在威脅並對其執行操作。

背景資訊

MITER ATT&CK(Anagarial Tactics， Technique， and Common Knowledge)框架是一個廣泛的知識庫和方法，提供對威脅發起者針對威脅系統分發的策略、技術和程式(TTP)的洞察。ATT&CK編譯成矩陣，每個矩陣表示作業系統或特定平台。攻擊的每個階段（稱為「戰術」）都對應到用於實現這些階段的特定方法（稱為「技術」）。

ATT&CK框架中的每個技術都附帶有關技術、相關程式、可能的防禦和檢測以及真實世界例項的資訊。MITER ATT&CK框架還包含多個組，這些組根據使用的戰術和技術來指代威脅組、活動組或威脅實施者。通過使用組，框架可幫助分類和記錄行為。

有關MITER的詳細資訊，請參閱https://attack.mitre.org。

必要條件

需求

思科建議您瞭解以下主題：

- Snort知識
- 安全FMC
- 安全Firepower威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 本檔案適用於所有Firepower平台
- 執行軟體版本7.3.0的安全FTD
- 運行軟體版本7.3.0的安全Firepower管理中心虛擬(FMC)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

MITER框架的優勢

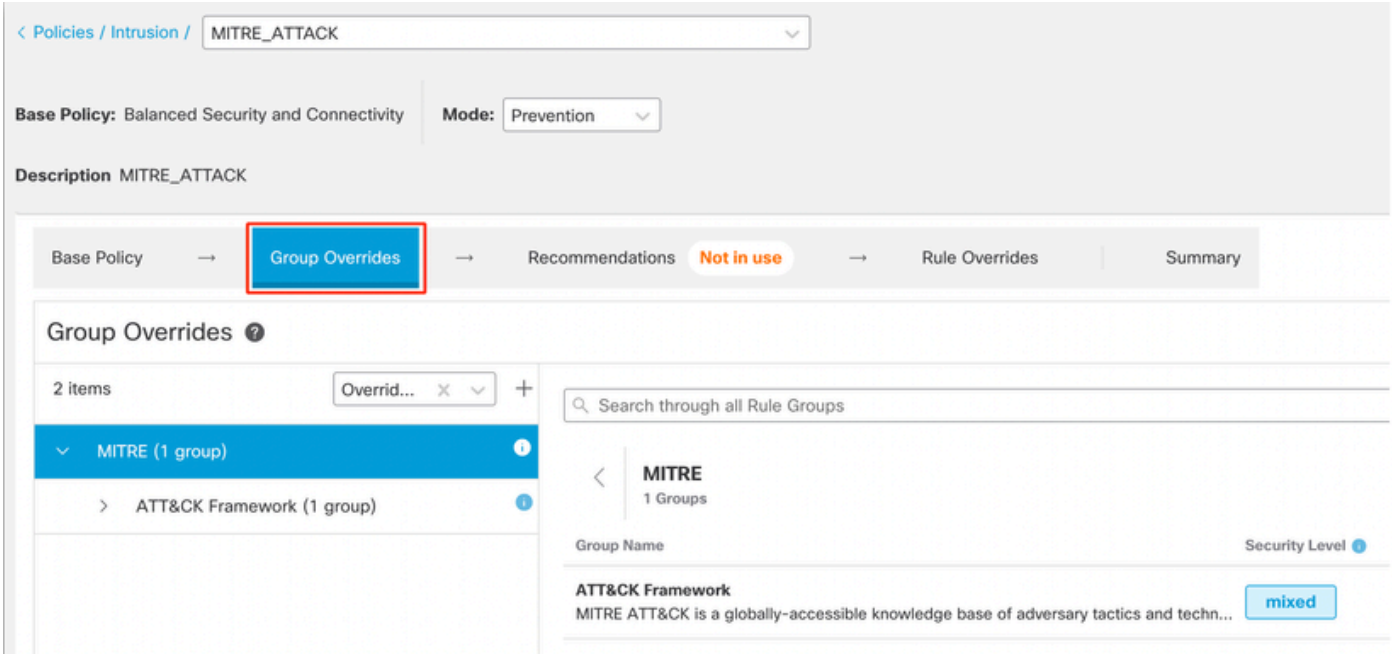
- MITER策略、技術和程式(TTP)被新增到入侵事件中，使管理員能夠根據MITER ATT&CK(Adversary Tractics Technologies and Common Knowledge)框架對流量執行操作。這使管理員能夠更精確地檢視和處理流量，並且他們可以根據漏洞型別、目標系統或威脅類別對規則進行分組。
- 您可以根據MITER ATT&CK框架組織入侵規則。這樣，您就可以根據特定的攻擊者策略和技巧自定義策略。

檢視入侵策略中的MITER框架

使用MITER框架可以在入侵規則中導航。MITER只是規則組的另一類別，並且是Talos規則組的一部分。支援多個級別的規則組的規則導航，從而提供了更多的靈活性和規則的邏輯分組。

1.選擇Policies > Intrusion。
2.確保選擇Intrusion Policies該頁籤。
3.按一下Snort 3 Version要檢視或編輯的入侵策略旁邊。關閉彈出的Snort幫助程式指南。
4.按一下Group Overrides層。

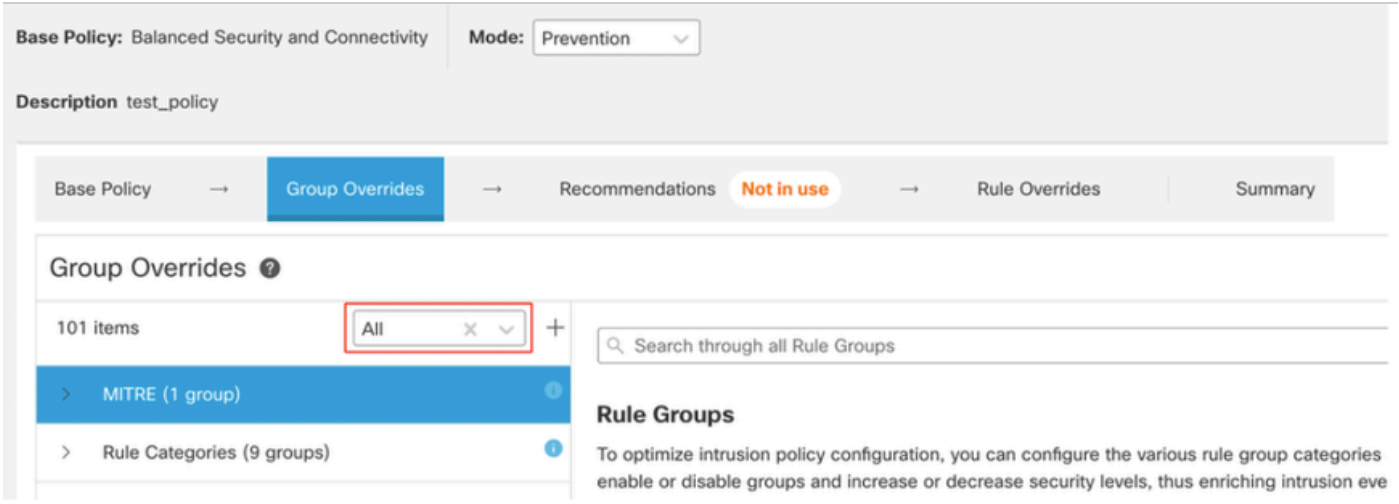
該Group Overrides層以分層結構列出規則組的所有類別。您可以遍歷到每個規則組中的最後一個葉規則組。



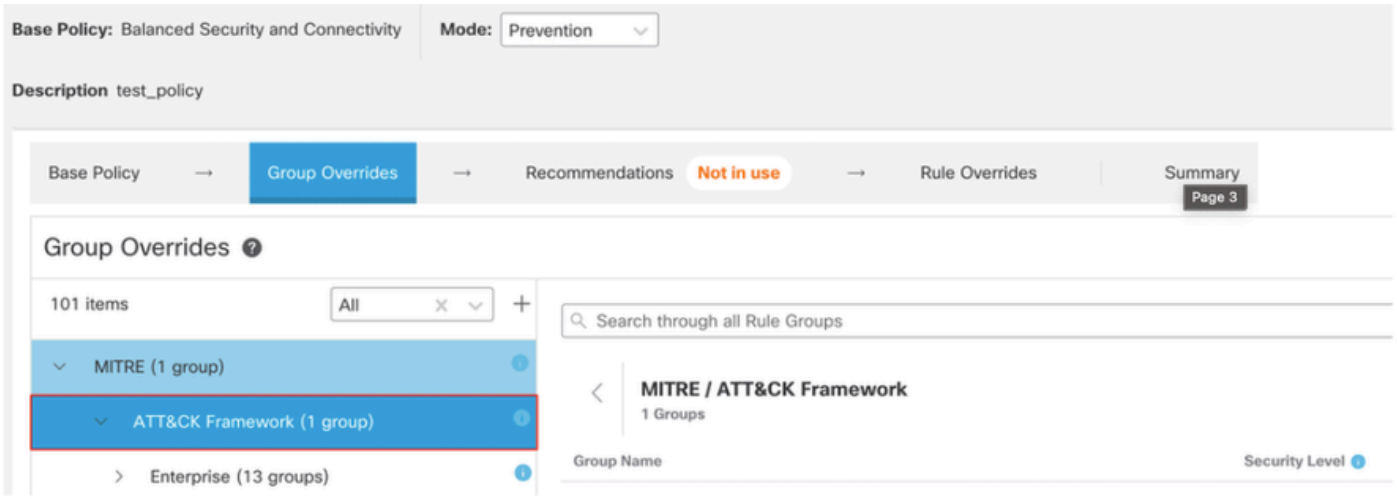
6.在Group Overrides下，確保 All在下拉選單中選擇，以便在左窗格中看到入侵策略的所有規則組。

7.單擊 MITRE在左窗格中。

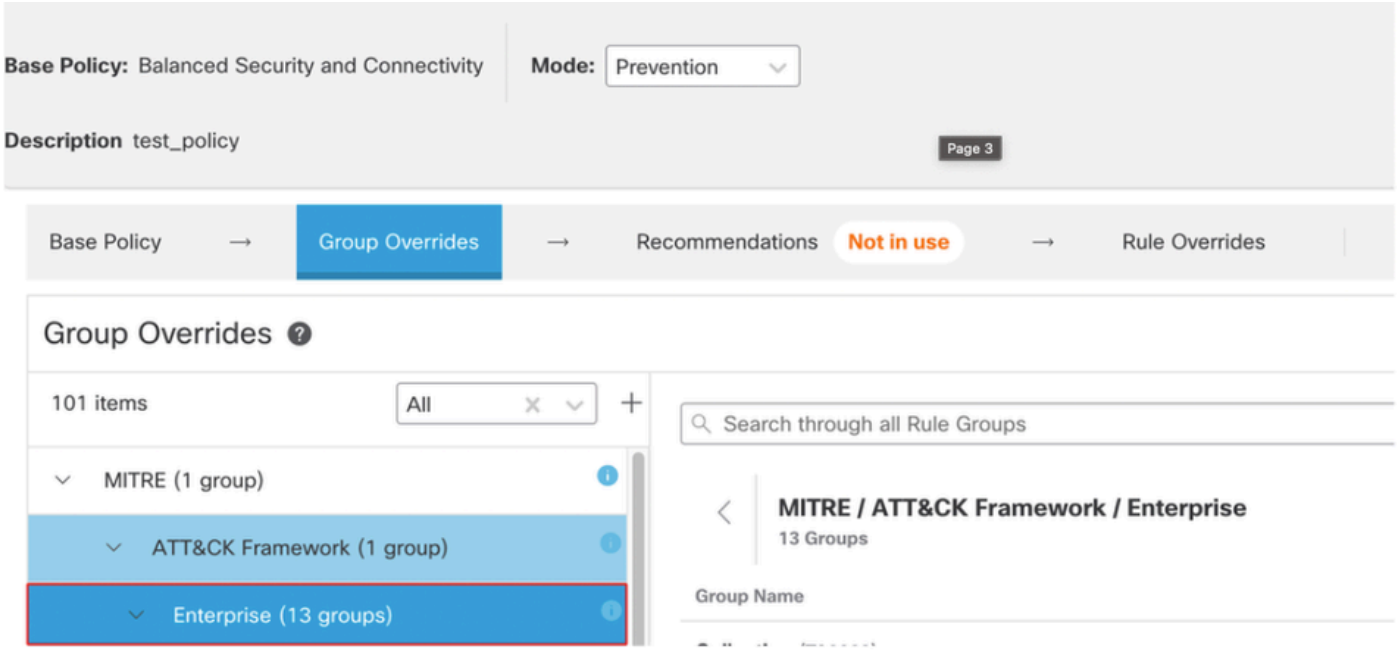
附註：在本例中，選擇了MITER ，但根據您的特定要求，您可以選擇Rule Categories規則組或其下的任何其他規則組和後續規則組。所有規則組都使用MITER框架。



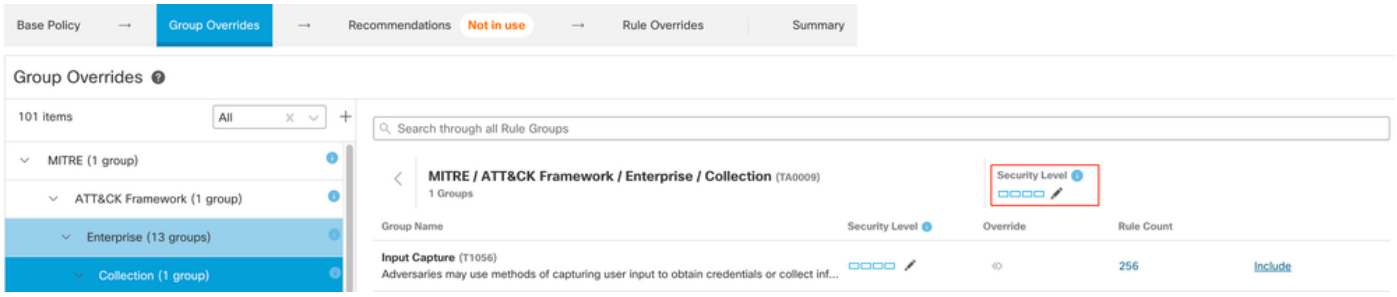
8.在MITRE下，按一下ATT&CK「框架」將其展開。



9.在ATT&CK Framework下，按一下「企業」將其展開。

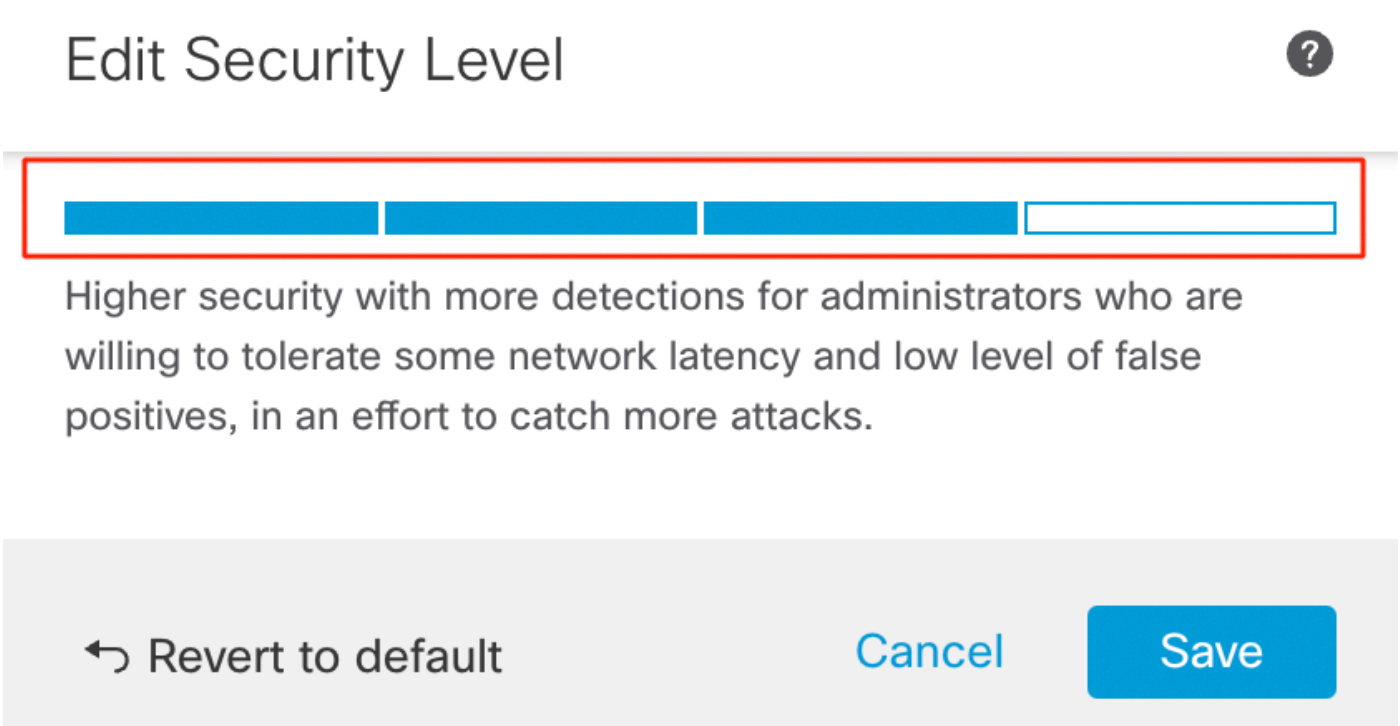


10.單Edit ( ) 擊規則組的「安全級別」旁邊的，對 Enterprise規則組類別。



編輯安全規則組

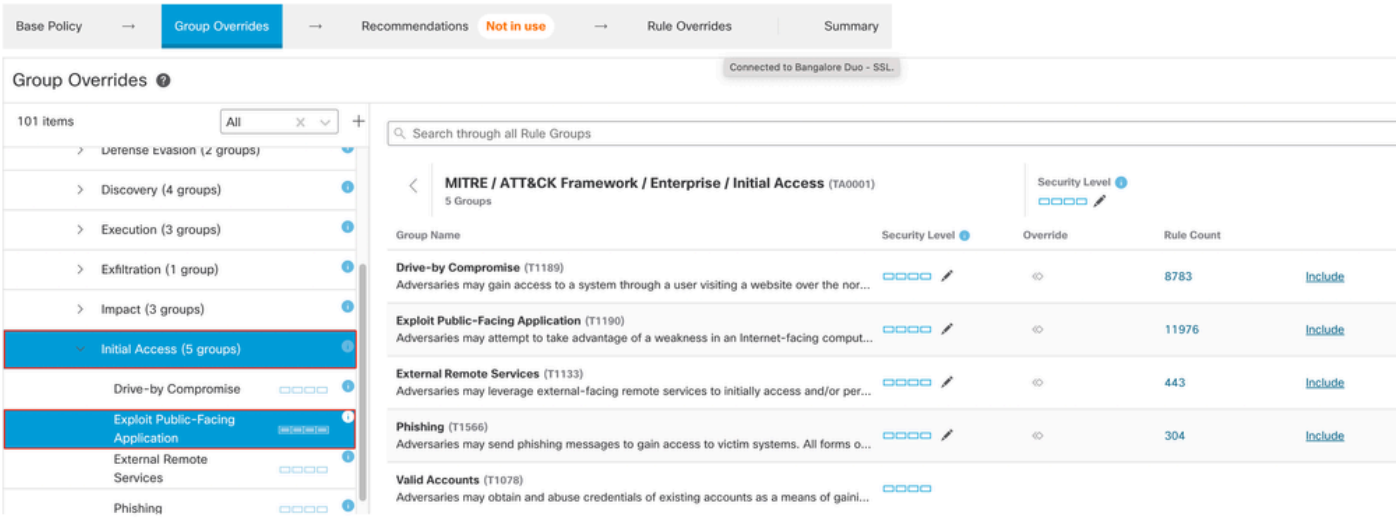
11.例如，在視窗中選擇安全級別3Edit Security Level，然後按一下**Save**。



安全級別

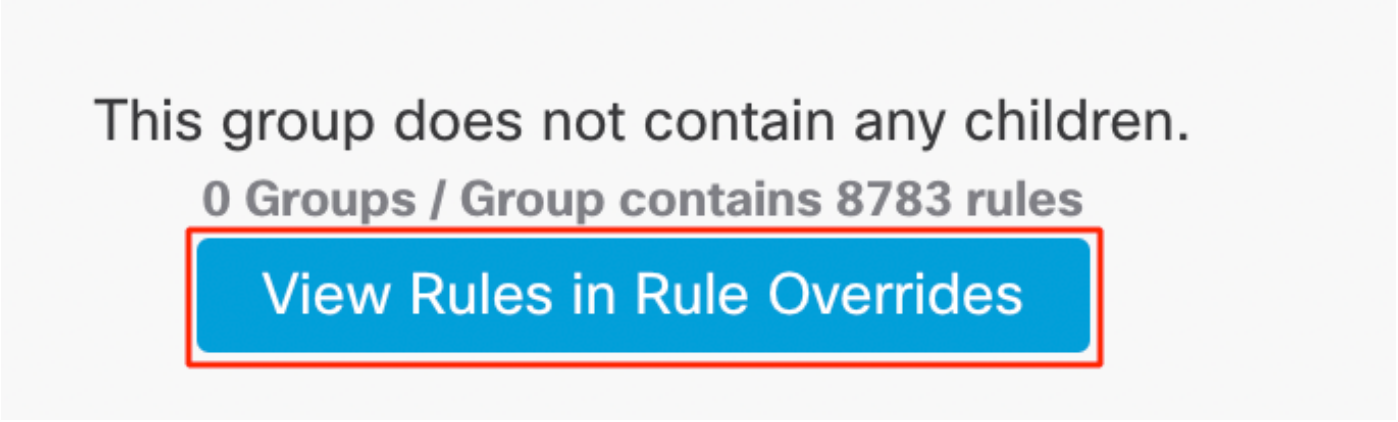
12.在Enterprise下，按一下Initial Access將其展開。

13.在Initial Access下，按一下Exploit Public-Facing Application，這是最後一個葉組。



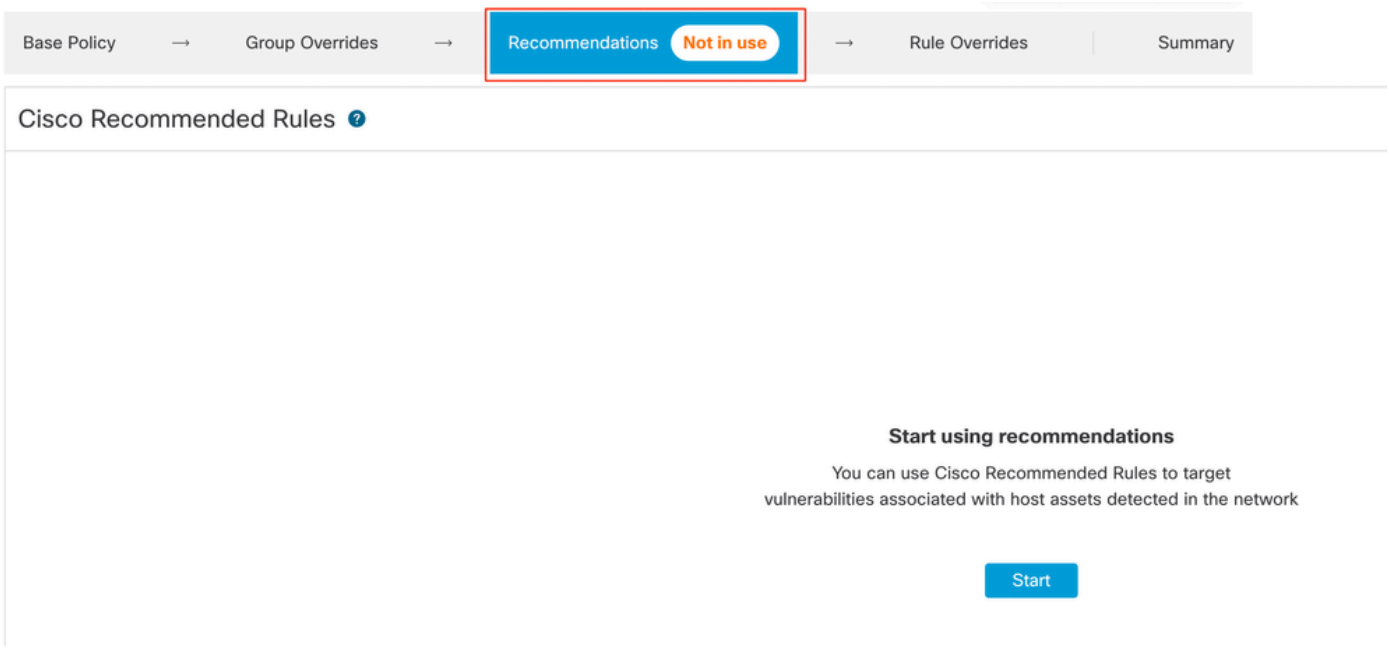
初始訪問組

14.按一下 **View Rules in Rule Overrides**按鈕檢視不同規則的不同規則、規則詳細資訊、規則操作等。

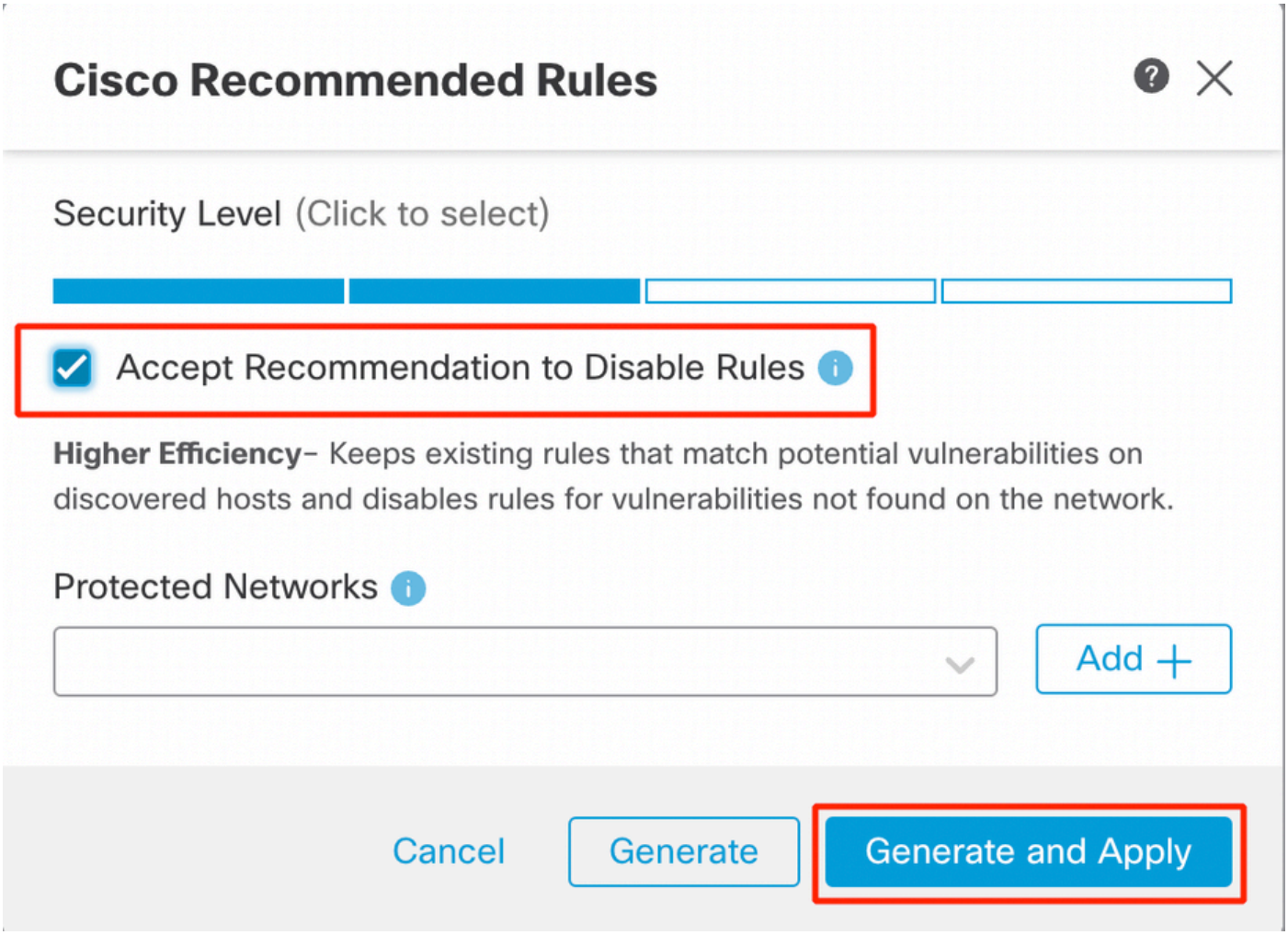


規則覆蓋中的規則

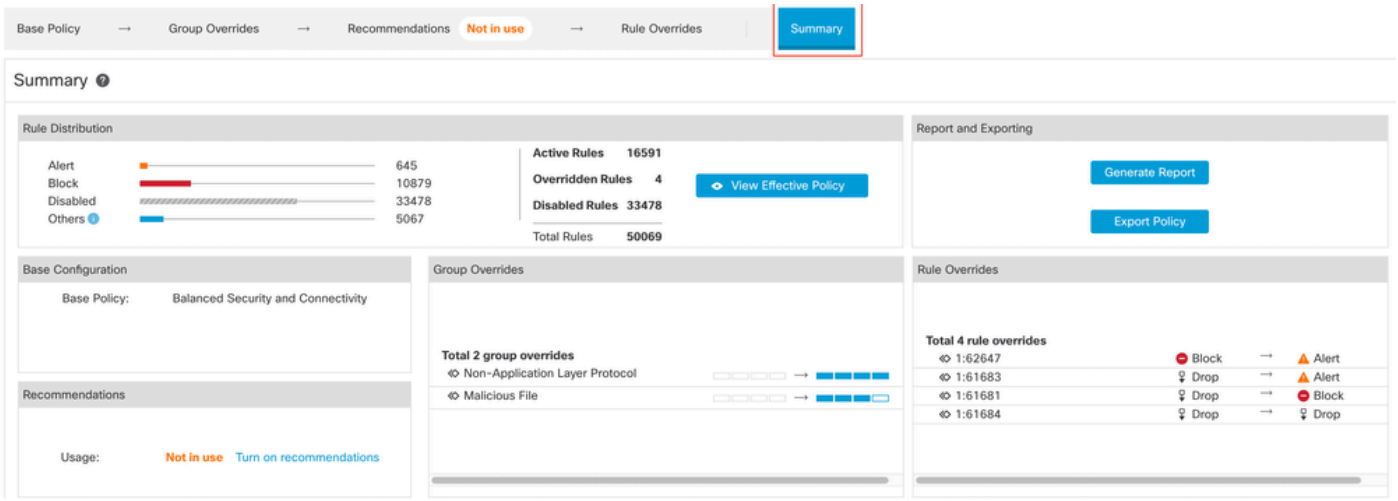
15.按一下 Recommendations層，然後按一下Start，開始使用思科推薦的規則。您可以使用入侵規則建議以與網路中檢測到的主機資產關聯的漏洞為目標。更多資訊.



行動



16.按一下 Summary層，以全面瞭解當前策略更改。您可以檢視策略的規則分佈、組覆蓋、規則覆蓋等。



策略摘要

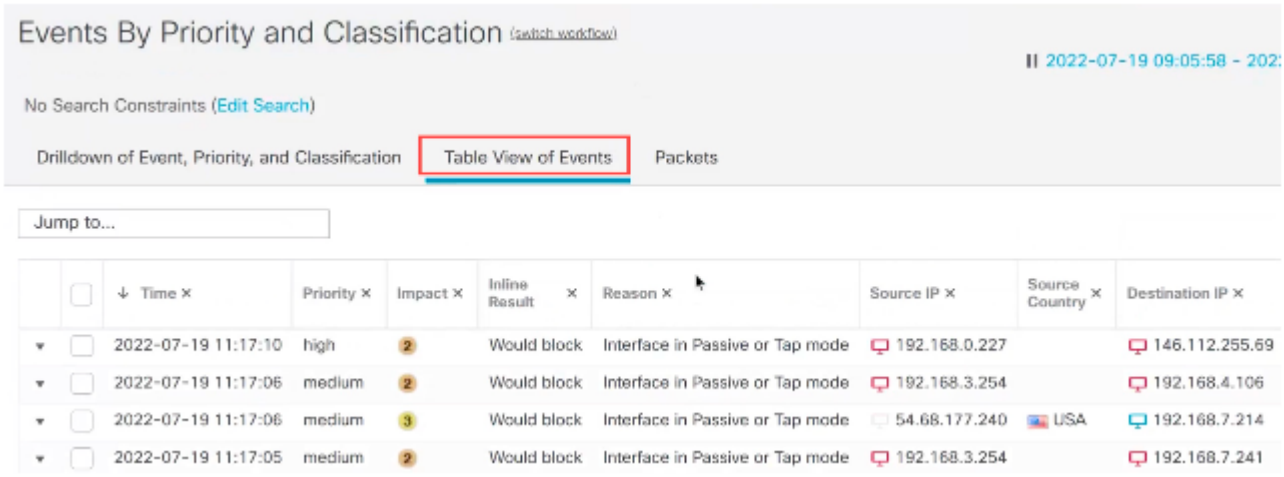
檢視入侵事件

您可以在Classic Event Viewer和Unified Event Viewer中的入侵事件中檢視MITER ATT&CK技術和規則組。Talos提供從Snort規則(GID:SID)到MITER ATT&CK技術和規則組的對映。這些對映將作為輕型安全包(LSP)的一部分安裝。

開始之前，必須部署入侵和訪問控制策略，以檢測和記錄Snort規則觸發的事件。

1.按一下Analysis > Intrusions > Events。

2.按一下 **Table View of Events**頁籤，如圖所示。



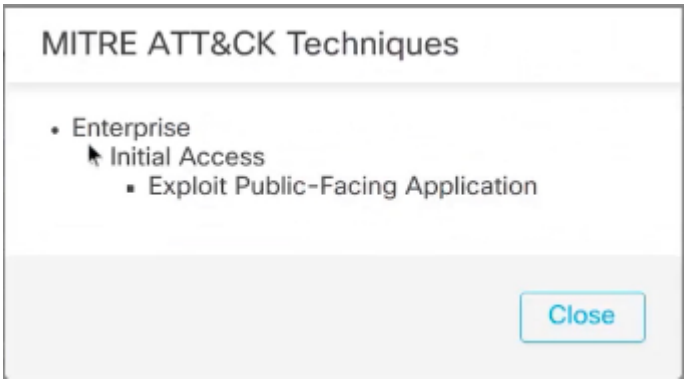
活動

3.在 MITRE ATT&CK列標題中，您可以看到入侵事件的技術。

Access Control Policy	Access Control Rule	Network Analysis Policy	MITRE ATT&CK	Rule Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

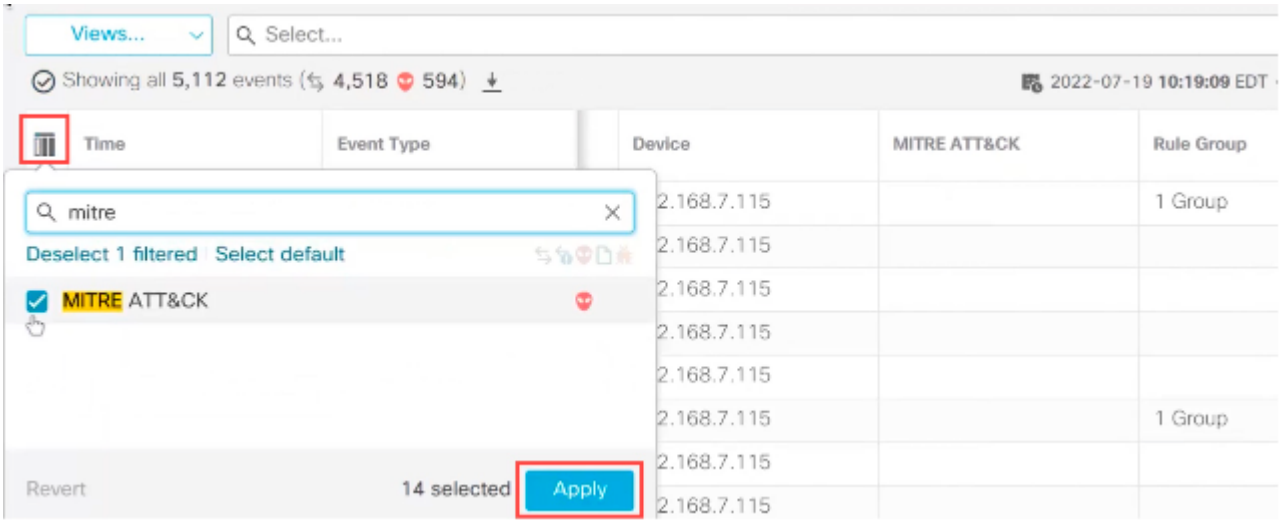
斜接列標題

4.單擊 1 Technique檢視MITER ATT&CK技術，如圖所示。在本例中， Exploit Public-Facing Application就是技術。



MITER ATT&CK技術

5.按一下Close。
6.按一下Analysis > Unified Events。
7.您可以按一下列選擇器圖示以啟用MITRE ATT&CK和Rule Group列。

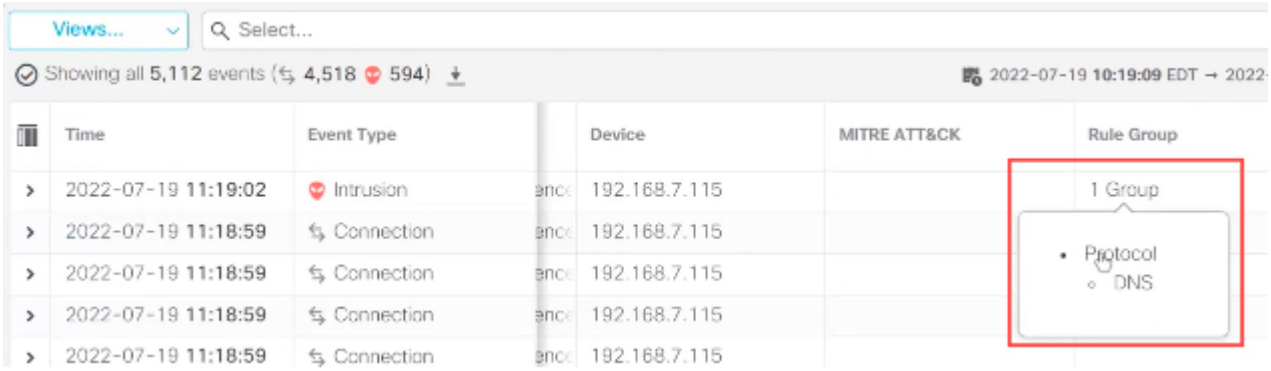


啟用Miter攻擊

8.如以下示例所示，入侵事件由對映到某個規則組的事件觸發。在1 Group 下 Rule Group列。

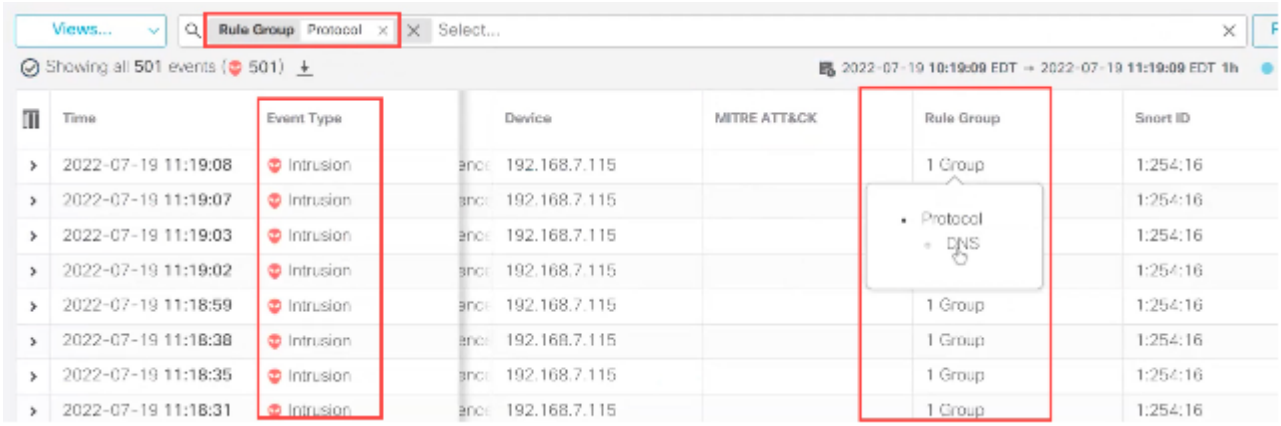
規則組

9.例如，您可以檢視協定（父規則組）及其下的DNS規則組。



檢視協定

10.可以按一下Protocol，搜尋至少具有一個規則組的所有入侵事件，即Protocol > DNS。此時將顯示搜尋結果，如以下示例所示。



規則組協定

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。