在FMC上配置關聯策略

目錄

| <u>簡介</u> | | | | |
|-------------|------------|--|--|--|
| <u>必要條件</u> | | | | |
| <u>需求</u> | | | | |
| <u>採用元件</u> | - | | | |
| <u>背景資訊</u> | | | | |
| <u>設定</u> | | | | |
| 配置關聯 | <u>·規則</u> | | | |
| 設定警示 | 1 | | | |
| 配置關聯 | <u>策略</u> | | | |

簡介

本文檔介紹配置關聯策略以連線事件並檢測網路上異常的過程。

必要條件

需求

思科建議您瞭解以下產品:

- 安全防火牆管理中心(FMC)
- 安全防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• 適用於VMware的Firepower威脅防禦7.6.0版

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。

背景資訊

關聯策略透過配置不同型別的事件來辨識網路上的潛在安全威脅,並用於補救、條件警報和流量策 略。

設定

配置關聯規則

步驟 1.導航到策略>關聯,選擇規則管理。



圖1.導航到關聯策略選單

步驟 2. 選取建立規則來建立新的規則。

| Home | Policy Management | Rule Management | Allow List | Traffic Profiles | | Alerts Remediations Groups |
|-----------------|----------------------------|------------------------------|---------------------|------------------|--|--------------------------------|
| Overview | | | | | | Create Rule Create Group |
| III Analysis | There are no rules current | tly defined. To create a rui | e, click "Create Ru | le". | | |

圖2.規則管理功能表上的規則建立

步驟 3. 選取事件型別和符合規則的條件。

當規則包含多個條件時,必須使用AND或OR運算子將其連結。

| Rule Information | Add Connection Tracker Add User Qualification Add Host Profile Qualification |
|------------------------------|----------------------------------------------------------------------------------------------|
| Rule Name | connection |
| Rule Description | |
| Rule Group | Ungrouped v |
| Select the type of event fo | r this rule |
| If a connection event occurs | at any point of the connection |
| Add condition | Add complex condition |
| Application | Protocol |
| Ac | d condition Add complex condition |
| | Source Country |
| | Source Country |
| | |

圖3.規則建立功能表



設定警示

步驟 1. 導航到策略>操作>警報。

Firewall Management Center Policies / Actions / Alerts / Alerts



圖4.導航到「警報」選單

步驟 2. 選擇Create Alert, 並建立Syslog、SNMP或email alert。

| | | | | Policies intrusion Rules | Allow List Hame Fromes | Alerts Nellieu | | oups I mo | Antor Alerta | |
|-----------------|--------|--------------------|------------------------|------------------------------------|--------------------------|------------------|----------|-----------|--------------|--|
| Home | Alerts | Impact Flag Alerts | Discovery Event Alerts | Advanced Malware Protection Alerts | Intrusion Email | | | | | |
| Overview | | | | | | | | Create | Alert ~ | |
| III Analysis | Name | | | | | Туре | In Use | Enabled | | |
| 2 | email | | | | | Email | Not Used | | 00 | |
| Policies | syslog | | | | | Syslog | Not Used | | 00 | |
| | | | | | | | | | | |

圖5.建立警示

步驟 3. 驗證警報是否已啟用。

配置關聯策略

步驟 1.導航到策略>關聯。



導航到關聯策略選單

圖6.導航到關聯策略選單

步驟 2. 建立新的關聯策略。選擇預設優先順序。使用None可使用特定規則的優先順序。

| cisco Polici | wall Management Center ss / Correlation / Policy Management | Q Search | Deploy 🧳 🐼 🕐 admin 🗸 |
|------------------|-------------------------------------------------------------------------------------|----------|--------------------------------|
| Home | Policy Management Rule Management Allow List Traffic Profiles | | Alerts Remediations Groups |
| Overview | | | Create Policy |
| ⊣IIÌ Analvsis | There are no policies currently defined. To create a policy, click "Create Policy". | | |
| Policies | | | |

圖7.建立新的關聯策略

步驟 3. 透過選擇Add Rules將規則增加到策略。

| Home | | Alerts Remediations Groups |
|-----------------|---------------------------------------------------------------|--------------------------------------|
| | Policy Management Rule Management Allow List Traffic Profiles | |
| Overview | Correlation Policy Information | Cancel Save You have unsaved changes |
| III Analysis | Policy Name Correlation | |
| | Policy Description | |
| Policies | Default Priority None ~ | |
| | Policy Rules | Add Rules |
| Devices | No Rules Currently Active | |
| •_= | | |
| Objects | | |

圖8.增加規則並選擇關聯策略的優先順序

| | Available Rules | Alerts Remediations Groups |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------------------------|
| Policy Management Rule Manager Correlation Policy Informatio Policy Name | Select the rules you wish to add to this policy, then click "Add". ~ Ungrouped Rules _ connection | Cancel |
| Policy Description | Allow List Rules Default Allow List | |
| Policy Rules No Rules Currently Active | | Add Rules |
| | Cancel | |

圖9.選擇要增加到關聯策略的規則

步驟 4. 從您建立的風險通告為規則分配響應,因此每當觸發該響應時,它都會傳送所選風險通告型 別。

| orrelation Policy Informat | tion | Canc | el |
|----------------------------|----------------------------------------|----------|-----|
| Policy Name | Correlation | | |
| Policy Description | | | |
| Default Priority | None ~ | | |
| blicy Rules | | | Add |
| Rule | Responses | Priority | |
| connection | This rule does not have any responses. | Default | |

圖10.「增加響應」按鈕

| Responses for connec | tion | | | | |
|----------------------|---------------|--|--|--|--|
| Assigned Responses | | | | | |
| | | | | | |
| | | | | | |
| email | onses | | | | |
| syslog | | | | | |
| L | | | | | |
| | Cancel Update | | | | |

圖11.將響應分配到關聯規則

步驟 5. 儲存並啟用您的關聯策略。

| Policy Management Rule Manag | gement Allow List Traffic Profiles | S | | |
|--------------------------------|------------------------------------|------------|-------------|--------------------------|
| Correlation Policy Information | tion | | Cancel Save | You have unsaved changes |
| Policy Name | Correlation | | | |
| Policy Description | | | | |
| Default Priority | None ~ | | | |
| Policy Rules | | | | Add Rules |
| Rule | Resp | ponses | Priority | |
| connection | emai | il (Email) | Default | ~ D Ū |
| | | | | |

圖12.響應已正確增加到關聯規則

| Policy Management | Rule Management | Allow List | Traffic Profiles | | |
|-------------------|-----------------|------------|------------------|---------------|---------------|
| | | | | | Create Policy |
| Name | | | | Sort by State | ~ |
| Correlation | | | | | Ū () |

圖13.啟用關聯策略

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)。