配置Firesight管理中心以顯示每個訪問規則的命 中次數

目錄

<u>簡介</u> <u>必要條件</u> <u>需採用定態</u> <u>避難</u> 難解

簡介

本文檔介紹如何配置自定義工作流程/事件檢視器頁面來描述每個訪問規則名稱的連線命中次數。該 配置顯示了與命中計數關聯的規則名稱欄位的基本示例,以及在需要時如何新增其他欄位。

必要條件

需求

思科建議您瞭解以下主題:

- Firepower技術知識
- 瞭解Firesight管理中心內的基本導航

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Firepower管理中心版本6.1.X及更高版本
- 適用於託管威脅防禦/Firepower感測器

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

組態

步驟1.以管理員許可權登入到Firesight管理中心。

成功登入後,導航到Analysis > Custom > Custom Workflows,如下圖所示:

Overview Analysis Policies Devices Objects AMP Intellige	nce					System Help	≠ admin v
Context Explorer Connections • Intrusions • Files • Hosts •	sers • Vulnerabilities •	Correlation •	Custom > Custom Workflows	Lookup 🔻	Search		
						Create Cust	tom Workflow
Custom Workflow			Table				
Events by Impact, Priority, and Host Criticality Summary of Critical Events to Destination Criticality			Intrusion Events with Destination	n Criticality			🔓 🥒 🖯
Events with Destination, Impact, and Host Criticality Current Events by Time, Impact, and Host Criticality			Intrusion Events with Destination	n Criticality			🔓 🥒 🖯
Hosts with Servers Default Workflow Hosts with Servers					🔒 🥜 🗎		
Intrusion Events with Destination Criticality Default Workflow			Intrusion Events with Destination	n Criticality			🔒 🥔 🗎
Intrusion Events with Source Criticality Default Workflow			Intrusion Events with Source Cr	iticality			🕞 🥜 🗐
Server and Host Details Network Server Information with Server OS			Hosts with Servers				🕞 🥜 🖯

步驟2.按一下Create Custom Workflow,然後選取如下圖所示的引數:



步驟3.選擇表欄位作為Connection Events並輸入工作流名稱,然後按一下Save。儲存工作流後,按 一下Add Page,如下圖所示:

Creating	Wo	rkflow							
Name Description	Hi	Access Control Policy Access Control Rule Action							
Table	Cc	Application Protocol Application Protocol Business Relevance Application Protocol Category							
Page 1		Application Protocol Risk Application Protocol Tag							×
Page Name	Hi	Business Relevance							
Sort Type	1	Client Client Business Relevance							
Column 1		Client Category Client Risk		Column 3		Column 4		Column 5	
Sort Priori	ty	Client Tag Client Version	d	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
1 \$		Count DNS Query DNS Record Type DNS Response DNS Sinkhole Name DNS TTL	cess Control 🕏	•	\$	\$	\$	•	\$ Save Cancel

附註:第一列必須為Count,然後在其它列中,您可以從下拉選單的可用欄位中進行選擇。在 這種情況下,第一列是計數,第二列是訪問控制規則。

步驟4.新增工作流程頁面後,按一下儲存。

若要檢視命中次數,請導覽至Analysis > Connections > Events,然後按一下Switch Workflows,如 下圖所示:

Overview Analysis Policies Devices Objects AMP Intelligence							
Context Explorer Connection	s ► Events	Intrusions 🔻	Files 🔻	Hosts 🔻	Users • Vulner	rabilities 🔻	Correlation •
Connection Events *							
Connection Events S > Table View of Connection Events							
Connections by Application							
Connections by Initiator							
Connections by Port							
Connections by Responder	ast Acti	on Reason	Initiator	Initiator	Responder IP	Responder	Ingress
Connections over Time	acket		IP	Country		Country	Security Zone
Hit-Counts	Allow		10.1.1.5		52,39,210,199	USA	
Traffic by Application		•					
Traffic by Initiator	Allow		<u>10.1.1.5</u>		<u>10.76.77.50</u>		
Traffic by Port	Allow		<u>10.1.1.5</u>		<u>10.76.77.50</u>		
Traffic by Responder	Allow	1	<u>10.1.1.5</u>		<u>52.39.210.199</u>	USA	
Unique Initiators by Responder	Allow		<u>10.1.1.5</u>		10.106.38.75		
Unique Responders by Initiator	Allow		<u>10.1.1.5</u>		10.106.38.75		
2017-07-19 08:47:13	Allow		<u>10.1.1.5</u>		<u>10.76.77.50</u>		
2017-07-19 08:47:08	Allow		<u>10.1.1.5</u>		<u>10.76.77.50</u>		
2017-07-19 08:47:08	Allow		<u>10.1.1.5</u>		172.217.7.238	USA	

步驟5.從下拉選單中選擇您建立的自定義工作流(本例中為Hit-Counts),如下圖所示:

Hit-Counts (switch workflow) Hit-Counts Based on Access Control		₩ <u>2017-07-19 07:36:06 - 2017-07-19 08:52:39</u> Expanding
No Search Constraints (Edit Search)		
Jump to 🔻		
Count	Access Control Rule	
4 🗋 66	Default-Allow	
		Dicelouing row 1 of 1 rows 1/ / Page 1 of 1 N

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。