配置Firesight管理中心以显示每个访问规则的命中计数

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 配置 验障排除

简介

本文档介绍如何配置自定义工作流程/事件查看器页面以描述每个访问规则名称的连接命中计数。配 置显示与命中计数关联的规则名称字段的基本示例,以及如果需要,如何添加其他字段。

先决条件

要求

Cisco 建议您了解以下主题:

- Firepower技术知识
- •了解Firesight管理中心内的基本导航

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Firepower管理中心6.1.X及更高版本
- •适用于托管威胁防御/Firepower传感器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

配置

配置

步骤1.以管理员权限登录Firesight管理中心。

Overview Analysis Policies Devices Objects	AMP Intelligence						System Help	≠ admin v
Context Explorer Connections • Intrusions • Files •	Hosts • Users •	Vulnerabilities •	Correlation •	Custom + Custom Workflows	Lookup 🔻	Search		
							Create Cus	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				🕞 🥜 🗊

步骤2.单击"创**建自定义工**作流",然后选择如图所示的参数:



步骤3.选择表字段作为"连接事**件"并**输入工作流名称,然后单击"保**存"**。保存工作流程后,单击"添**加** 页",如图所示:

Creating \	No	rkflow							
Name	Hi	Access Control Policy							
Description		Access Control Rule Action							
Table	Cc	Application Protocol Application Protocol Business Relevance							
Page 1		Application Protocol Category Application Protocol Risk Application Protocol Tag							×
Page Name	Hi	Application Risk Business Relevance							
Sort Type	I	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	cess Control 🖨	•		•		•	\$
		DNS Record Type DNS Response DNS Sinkhole Name DNS TTL							Save Cancel

注意:第一列必须是"计数",然后在其他列中,您可以从下拉列表中选择可用字段。在这种情况下,第一列是Count,第二列是Access Control Rule。

步骤4.添加工作流程页面后,单击"保**存"。**

要查看命中计数,请导航至Analysis > Connections > Events,然后单击Switch Workflows,如图所示:

Overview Analysis Policie	es Devices	Objects /	AMP Intell	igence			
Context Explorer Connection	is ⊧ Events	Intrusions 🔻	Files 🔻	Hosts 🔻	Users • Vulne	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 Act	ion Reason	Initiator	Initiator	Responder IP	Responder	Ingress
Connections over Time	acket		IP	Country		Country	Security Zone
Hit-Counts	Alloy	v	10.1.1.5		52.39.210.199	USA	
Traffic by Application		<u>-</u>					
Traffic by Initiator	Allov	v	<u>10.1.1.5</u>		<u>10.76.77.50</u>		
Traffic by Port	Allow	v	i0.1.1.5 <u>10.1.1.5</u>		10.76.77.50		
Traffic by Responder	Allow	v	<u>10.1.1.5</u>		<u>52.39.210.199</u>	USA	
Traffic over Time •	Allon	M	10 1 1 5		10 106 38 75		
Unique Initiators by Responder	Allow	<u>×</u>	<u>10.1.1.5</u>		10.100.50.75		
Unique Responders by Initiator	Allov	v	<u>10.1.1.5</u>		<u>10.106.38.75</u>		
2017-07-19 08:47:13	Allow	<u>v</u>	<u>10.1.1.5</u>		<u>10.76.77.50</u>		
2017-07-19 08:47:08	Allow	v	<u>il 10.1.1.5</u>		<u>10.76.77.50</u>		
<u>2017-07-19 08:47:08</u>	Allow	v	<u>10.1.1.5</u>		172.217.7.238	USA	

步骤5.从下拉列表中选择您创建的自定义工作流程(在本例中为Hit-Counts),如图所示:

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	
		Displaying row 1 of 1 rows

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。