Configurer Firesight Management Center pour afficher le nombre de visites par règle d'accès

Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Configurations Vérification Dépannage

Introduction

Ce document décrit comment configurer la page d'affichage des flux de travail/événements personnalisée pour représenter le nombre de coups de connexion par nom de règle d'accès. La configuration présente un exemple de base de champ de nom de règle associé au nombre de résultats et indique comment ajouter des champs supplémentaires si nécessaire.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower
- Connaissance de la navigation de base au sein du Firesight Management Center

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Management Center version 6.1.X et ultérieure
- Applicable aux détecteurs de sécurité/Firepower gérés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Configurations

Étape 1. Connectez-vous à Firesight Management Center avec les privilèges d'administrateur.

Une fois la connexion établie, accédez à **Analysis > Custom > Custom Workflows**, comme illustré dans l'image :

	Policios	Davisas Obi	octo A	MD Intolli	00000								Sustam	Help -	admin –
Context Explorer Conn	ections v	Intrusions v	Files v	Hosts v	Users v	Vulnerabilities v	Correlation •	Cust	tom ► Custom Workflows	Lookup 🔻	Search		System	nep v	aunin +
			THES T	10505	00010		conclution			LUURAP	bearen		Crea	te Custom	Workflow
Custom Workflow									Table						
Events by Impact, Priority, and Host Criticality Summary of Critical Events to Destination Criticality Intrusion Events with Destination Criticality									6	2 / 6					
Events with Destination, Impact, and Host Criticality Current Events by Time, Impact, and Host Criticality Intrusion Events with Destination Criticality									6	2 / 6					
Hosts with Servers Default Workflow Hosts with Servers								6	è 🥜 🗎						
Intrusion Events with Destination Criticality Default Workflow Intrusion Events with Destination Criticality								6	🗎 🥔 🗐						
Intrusion Events with Source Criticality Default Workflow Intrusion Events with Source Criticality								6	2 /						
Server and Host Details Network Server Information with Server OS							Hosts with Servers					6	2 / 0		

Étape 2. Cliquez sur **Créer un flux de travail personnalisé** et choisissez les paramètres comme indiqué dans l'image :



Étape 3. Sélectionnez le champ de table **Événements de connexion** et entrez un nom de workflow, puis cliquez sur **Enregistrer**. Une fois le flux de travail enregistré, cliquez sur **Ajouter une page** comme indiqué dans l'image :

Creatin	g Wo	rkflov	N								
Name	Н	Acc	ess Control Policy								
Descriptio	n [Acci	ess Control Rule on								
Table	C	Арр Арр	lication Protocol lication Protocol Business Relevance								
Page 1		App App App	lication Protocol Category lication Protocol Risk lication Protocol Tag								×
Page Nam	еН	App Busi	lication Risk iness Relevance								
Sort Type	C	Clie	nt nt Business Relevance								
Column	1	Clie	nt Category nt Risk		Column 3		Column 4		Column 5		
Sort Pri	ority	Clie	nt Tag	d	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field	
1 \$		✓ Cou DNS	nt S Query	cess Control 🖨	\$	\$	\$		\$		\$
		DNS DNS DNS	S Record Type S Response S Sinkhole Name							Save	Cancel
		DNS	STTL								

Note: La première colonne doit être Count, puis dans la colonne supplémentaire, vous pouvez choisir parmi les champs disponibles dans la liste déroulante. Dans ce cas, la première colonne est un nombre et la deuxième colonne est une règle de contrôle d'accès.

Étape 4. Une fois la page de workflow ajoutée, cliquez sur Enregistrer.

Pour afficher les nombres de résultats, accédez à **Analyse > Connexions > Événements** et cliquez sur **Workflows de commutateur**, comme illustré dans l'image :

Overview Analysis Policies Devices Objects AMP Intelligence										
Context Explorer Connections > Ev	ents Intrusions •	Files • Host	s 🔹 Users 🔹 Vulne	erabilities Correlation						
Connection Events ×										
Connection Events	s > Table View of Connection Events									
Connections by Application										
Connections by Initiator										
Connections by Port										
Connections by Responder	Action Reason	Initiator Init	iator Responder IP	Responder Ingress						
Connections over Time		IP Cou	ntry	Country Security Zone						
Hit-Counts	Allow	10.1.1.5	52.39.210.199	🔤 USA						
Traffic by Application	Allow	10.1.1.5	10 76 77 50							
Traffic by Initiator	Allow	<u>en 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	<u>10.1.1.5</u>	<u>52.39.210.199</u>	USA USA						
Traffic over Time •	Allow	10.1.1.5	10.106.38.75							
Unique Initiators by Responder	Allow	= <u>10 1 1 F</u>	10 106 29 75							
Unique Responders by Initiator	Allow	<u>en 10.1.1.5</u>	<u>10.106.38.75</u>							
2017-07-19 08:47:13	Allow	10.1.1.5	<u>10.76.77.50</u>							
2017-07-19 08:47:08	Allow	10.1.1.5	<u>10.76.77.50</u>							
<u>2017-07-19 08:47:08</u>	Allow	<u>10.1.1.5</u>	172.217.7.238	USA USA						

Étape 5. Dans la liste déroulante, sélectionnez le flux de travail personnalisé que vous avez créé (dans ce cas, nombre d'occurrences), comme indiqué dans l'image :

Hit-Counts (switch workflow) Hit-Counts Based on Access Control		2017-07-19 07:36:06 - 2017-07-19 08:52:39 Expanding
No Search Constraints (Edit Search)		
Jump to 🔻		
Count	Access Control Rule	
4 🗋 66	Default-Allow	
		Displaying row 1 of 1 rows $ \langle \langle Page 1 \rangle \rangle $

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.