Konfigurieren des FireSIGHT Management Center zur Anzeige der Trefferzahlen pro Zugriffsregel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Konfigurationen Überprüfen Fehlerbehebung

Einführung

In diesem Dokument wird beschrieben, wie Sie eine benutzerdefinierte Workflow-/Ereignisanzeige-Seite konfigurieren, um die Verbindungsaufschläge pro Zugriffsregelname anzuzeigen. Die Konfiguration zeigt ein einfaches Beispiel für ein Regelnamenfeld, das Trefferzählungen zugeordnet ist, und wie ggf. zusätzliche Felder hinzugefügt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der FirePOWER-Technologie
- Grundkenntnisse der Navigation im FireSIGHT Management Center

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Firepower Management Center Version 6.1.X und höher
- Gilt für verwaltete Threat Defense-/FirePOWER-Sensoren

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Konfigurationen

Schritt 1: Melden Sie sich mit Administratorrechten beim FireSIGHT Management Center an.

Navigieren Sie nach erfolgreicher Anmeldung zu **Analysis > Custom > Custom Workflows** (Analyse > Benutzerdefiniert > Benutzerdefinierte Workflows), wie im Bild gezeigt:

Overview Analy	ysis Policies	Devices Obj	ects A	MP Intelli	gence						Syste	m Help 🖷	admin 🔻
Context Explorer	Connections •	Intrusions •	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation •	Custom + Custom Workflows	Lookup 🔻	Search			
												reate Custo	m Workflow
Custom Workflow								Table					
Events by Impact, Priority, and Host Criticality Summary of Critical Events to Destination Criticality						Intrusion Events with Destination	Intrusion Events with Destination Criticality						
Events with Destination, Impact, and Host Criticality Intrusion Events with Destinatio Current Events by Time, Impact, and Host Criticality Intrusion Events with Destinatio						n Criticality				🕞 🥒 🗊			
Hosts with Servers Default Workflow Hosts with Servers								🔒 🥒 🗎					
Intrusion Events with Destination Criticality Default Workflow Intrusion Events with Destination Criticality								🔒 🥒 🖯					
Intrusion Events with Source Criticality Default Workflow Intrusion Events with Source Criticality								🕞 🥔 🗐					
Server and Host Details Network Server Information with Server OS Hosts with Servers								🕞 🥜 🖯					

Schritt 2: Klicken Sie auf **Benutzerdefinierten Workflow erstellen** und wählen Sie die im Bild gezeigten Parameter aus:

Overview Ana	Vsis Policies	Devices Obj	ects AM	P Intellio	ence							System	Help 🔻	admin 🔻
Context Explorer	Connections •	Intrusions •	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation •	Custom +	Custom Workflows	Lookup 🔻	Search			
						Creating Workfl Name File-Coi Description Table ✓ Activ Appli Audit Captu Captu Conn Disco File E Heal Host Host Host Host Host Host Host Host	OW Sessions ation Details ations cog Events cod Files co	ise tion Criticality Criticality				Add Page	Add T	able View

Schritt 3: Wählen Sie das Tabellenfeld als **Verbindungsereignisse** aus, geben Sie einen Workflow-Namen ein, und klicken Sie dann auf **Speichern**. Wenn der Workflow gespeichert ist, klicken Sie auf **Seite hinzufügen**, wie im Bild gezeigt:

Name Hi Access Control Policy Description Access Control Rule Action Table Application Protocol Application Protocol Category Application Protocol Risk	
Description Access Control Rule Action Table Cc Application Protocol Application Protocol Business Relevance Application Protocol Category	
Table Cc Application Protocol Application Protocol Business Relevance Application Protocol Category	
Application Protocol Category	
Page 1 Application Protocol Tag	×
Page Name HI Business Relevance	
Sort Type Client Client Business Relevance	
Column 1 Client Category Column 3 Column 4 Column 5	
Sort Priority Client Tag d Sort Priority Field Sort Priority Field Sort Priority Field	
1 ¢ Venue Count DNS Query Cess Control ¢ ¢	\$
DNS Record Type DNS Response DNS Sinkhole Name	cel

Hinweis: Die erste Spalte muss Count (Zähler) sein. In der zusätzlichen Spalte können Sie dann aus dem Dropdown-Menü unter den verfügbaren Feldern auswählen. In diesem Fall ist die erste Spalte eine Count und die zweite Spalte eine Access Control Rule (Zugriffskontrollregel).

Schritt 4: Klicken Sie nach dem Hinzufügen der Workflow-Seite auf Speichern.

Um die Trefferzähler anzuzeigen, navigieren Sie zu **Analysis > Connections > Events** und klicken Sie auf **Switch Workflows**, wie im Bild gezeigt:

Overview Analysis Policie	s Devices	Objects	AMP Intell	igence					
Context Explorer Connection	s ► 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 Actio	n 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	Allow		10115						
Traffic by Initiator	Allow		<u>=</u> 10.1.1.5		<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			
Traffic over Time • Unique Initiators by Responder	Allow		<u>10.1.1.5</u>		<u>10.106.38.75</u>				
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>		10.76.77.50				
2017-07-19 08:47:08	Allow		<u>10.1.1.5</u>		10.76.77.50				
2017-07-19 08:47:08	Allow		<u>10.1.1.5</u>		172.217.7.238	USA			

Workflow (in diesem Fall Hit-Counts), wie im Bild gezeigt:

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 < < Page 1 of 1 >>

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.