# アクセスルールごとのヒットカウントを表示す るためのFiresight Management Centerの設定

### 内容

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>設定</u> <u>設定</u> <u>確認</u> トラブルシュート

#### 概要

このドキュメントでは、カスタムワークフロー/イベントビューアページを設定して、アクセスル ール名ごとの接続ヒットカウントを示す方法について説明します。設定は、ヒットカウントに関 連付けられたルール名フィールドの基本的な例と、必要に応じて追加フィールドを追加する方法 を示します。

## 前提条件

#### 要件

次の項目に関する知識があることが推奨されます。

- FirePOWER の知識
- Firesight Management Center内の基本的なナビゲーションに関する知識

#### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Management Centerバージョン6.1.X以降
- ・マネージド脅威防御/火力センサーに適用可能

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

設定

#### 設定

ステップ1:管理者権限でFiresight Management Centerにログインします。

ログインが正常に完了したら、図に示すように、[Analysis] > [Custom] > [Custom Workflows]に移 動します。

Overview Analysis Policies Devices Objects AMP Intelligence							System	Help 🔻	admin 🔻						
Context Explorer	Connections •	Intrusions •	Files <b>v</b>	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation •	Cust	tom <b>&gt;</b> Custom Workflows	Lookup 🔻	Search				
													O Crea	te Custon	n Workflow
Custom Workflow									Table						
Events by Impact, Priority, and Host Criticality Summary of Critical Events to Destination Criticality								Intrusion Events with Destination Criticality						2 / 6	
Events with Destination, Impact, and Host Criticality Current Events by Time, Impact, and Host Criticality								Intrusion Events with Destination Criticality					2 / 6		
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					2 / 1		
Server and Host Details Network Server Information with Server OS							Hosts with Servers					2 0			

ステップ2:[Create Custom Workflow]をクリックし、図に示すようにパラメータを選択します。



ステップ3:[Connection Events]というテーブルフィールドを選択し、ワークフロー名を入力して、[Save]をクリックします。ワークフローを保存したら、次の図に示すように[Add Page]をクリックします。

Creatin	g Wo	orl	kflow							
Name	Hi		Access Control Policy							
Descriptio	n		Access Control Rule Action							
Table	Co		Application Protocol Application Protocol Business Relevance							
Page 1			Application Protocol Category Application Protocol Risk Application Protocol Tag							×
Page Nam	e Hi		Application Risk Business Relevance							
Sort Type		1	Client Client Business Relevance							
Column	1		Client Category Client Risk		Column 3		Column 4		Column 5	
Sort Pri	ority		Client Tag	d	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
1 \$		~	Count DNS Query	cess Control 🗘	•	\$	<b>•</b>	\$	•	<b>(</b>
			DNS Record Type DNS Response DNS Sinkhole Name						(	Save Cancel
			DNS TTI							

**注**:最初の列は[カウント(Count)]にする必要があり、追加の[列(Column)]では、ドロップダ ウンから使用可能なフィールドから選択できます。この場合、最初の列はカウントで、2番 目の列はアクセスコントロールルールです。

ステップ4:ワークフローページが追加されたら、[保存(Save)]をクリックします。

ヒットカウントを表示するには、図に示すように、[Analysis] > [Connections] > [Events]に移動し、[Switch Workflows]をクリックします。

Overview Analysis Policie	s Devices C	bjects AM	1P Intelli	gence					
Context Explorer Connection	s ► Events I	ntrusions 🔻	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 Action	Reason II	Initiator Initiator		Responder IP	Responder	Ingress		
Connections over Time	acket	<u>I</u>	P	Country		Country	Security Zone		
Hit-Counts	Allow	1	10.1.1.5		52.39.210.199	USA			
Traffic by Application			10115						
Traffic by Initiator	Allow		10.1.1.5		<u>10.76.77.50</u>				
Traffic by Port	Allow		10.1.1.5		10.76.77.50				
Traffic by Responder	Allow		10.1.1.5		<u>52.39.210.199</u>	USA			
Traffic over Time •	Allow		10.1.1.5		10 106 38 75				
Unique Initiators by Responder	<u>riiou</u>				101100100175				
Unique Responders by Initiator	Allow		10.1.1.5		<u>10.106.38.75</u>				
2017-07-19 08:47:13	Allow		10.1.1.5		<u>10.76.77.50</u>				
♣ <u>2017-07-19 08:47:08</u>	Allow		10.1.1.5		<u>10.76.77.50</u>				
2017-07-19 08:47:08	Allow		10.1.1.5		<u>172.217.7.238</u>	USA			

ステップ5:図に示すように、ドロップダウンから、作成したカスタムワークフロー(この場合 はヒットカウント)を選択します。

Hit-Counts (switch workflow) Hit-Counts Based on Access Control		1 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  < < Page 1 of 1 >>

確認

現在、この設定に使用できる確認手順はありません。

## トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。