액세스 규칙당 적중 횟수를 표시하도록 Firesight Management Center 구성

목	차
---	---

소개

이 문서에서는 액세스 규칙 이름별 연결 적중 횟수를 표시하도록 사용자 지정 워크플로/이벤트 뷰 어 페이지를 구성하는 방법에 대해 설명합니다. 컨피그레이션에서는 적중 횟수와 관련된 규칙 이름 필드의 기본 예와 필요한 경우 필드를 추가하는 방법을 보여 줍니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- firepower 기술에 대한 지식
- Firesight Management Center 내의 기본 탐색 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower Management Center 버전 6.1.X 이상
- 관리되는 위협 방어/Firepower 센서에 적용 가능

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설정

1단계. 관리자 권한으로 Firesight Management Center에 로그인합니다.

로그인에 성공하면 이미지에 표시된 대로 Analysis > Custom > Custom Workflows로 이동합니다.

Overview Analysis Policies Devices Objects AMP Intelligence							System	Help 🔻	admin 🔻						
Context Explorer	Connections •	Intrusions •	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities •	Correlation •	Cust	tom + Custom Workflows	Lookup 🔻	Search				
Create Custom W									Workflow						
Custom Workflow									Table						
Events by Impact, Summary of Critical	Priority, and Host Events to Destination	t Criticality on Criticality							Intrusion Events with Destinatio	n 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							2 / 6								
Intrusion Events with Source Criticality Default Workflow Intrusion Events with Source Criticality							2 🥒 🗎								
Server and Host D Network Server Info	etails ermation with Server	OS							Hosts with Servers						2 / 8

2단계. Create Custom Workflow(맞춤형 워크플로 생성)를 클릭하고 이미지에 표시된 대로 매개변 수를 선택합니다.



3단계. 테이블 필드를 Connection Events로 선택하고 워크플로 이름을 입력한 다음 Save를 클릭합니다. 워크플로가 저장되면 이미지에 표시된 대로 Add Page(페이지 추가)를 클릭합니다.

Creating V	Voi	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	ī	Client Client Business Relevance							
Column 1		Client Category Client Risk		Column 3		Column 4		Column 5	
Sort Priorit	y	Client Tag	d	Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
1 \$	1	✓ Count DNS Query	cess Control 🗘	•	(•	(•	(
		DNS Record Type DNS Response DNS Sinkhole Name DNS TTI							Save Cancel

참고: 첫 번째 열은 Count여야 하며, 추가 열에서는 드롭다운에서 사용 가능한 필드 중에서 선 택할 수 있습니다. 이 경우 첫 번째 열은 Count이고 두 번째 열은 Access Control Rule입니다.

4단계. 워크플로 페이지가 추가되면 Save(저장)를 클릭합니다.

적중 횟수를 보려면 그림과 같이 Analysis > Connections > Events로 이동하고 Switch Workflows를 클릭합니다.

Overview Analysis Policies Devices Objects AMP Intelligence								
Context Explorer Connection	ns ► 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	Action Reason	Initiator	Initiator	Responder IP	Responder	Ingress	
Connections over Time	acket		IP Country			Country	Security Zone	
Hit-Counts	A	llow	10.1.1.5		52.39.210.199	USA		
Traffic by Application	_				10 76 77 50			
Traffic by Initiator	A	llow	<u>10.1.1.5</u>		<u>10.76.77.50</u>			
Traffic by Port	A	llow	10.1.1.5		<u>10.76.77.50</u>			
Traffic by Responder	A	llow	<u>10.1.1.5</u>		52.39.210.199	USA		
Traffic over Time •	A	llow	10.1.1.5		10.106.38.75			
Unique Personders by Responder	Δ	llow	10115		10 106 38 75			
			<u>10.1.1.5</u>		<u>10.100.38.75</u>			
2017-07-19 08:47:13	A	llow	10.1.1.5		<u>10.76.77.50</u>			
2017-07-19 08:47:08	A	llow	<u>10.1.1.5</u>		10.76.77.50			
2017-07-19 08:47:08	A	llow	<u>10.1.1.5</u>		<u>172.217.7.238</u>	USA		

5단계. 그림과 같이 드롭다운에서 생성한 맞춤형 워크플로(이 경우 적중 횟수)를 선택합니다.

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

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.