사용자 지정 워크플로

다음 주제에서는 맞춤형 워크플로를 사용하는 방법을 설명합니다.

맞춤형 워크플로 소개

사전 정의된 워크플로와 Cisco에서 제공하는 맞춤형 워크플로가 필요에 부합하지 않을 경우, 맞춤형 워크플로를 생성하고 관리해야 합니다.

맞춤형 워크플로는 조직의 고유한 필요에 맞게 생성하는 워크플로입니다. 맞춤형 워크플로를 생성할 때 워크플로의 기반이 되는 이벤트(또는 데이터베이스 테이블)의 종류를 선택합니다. Firepower Management Center에서 맞춤형 테이블을 맞춤형 워크플로의 기반으로 선택할 수 있습니다. 또한 맞춤형 워크플로에 포함되는 페이지를 선택할 수 있습니다. 맞춤형 워크플로는 드릴다운, 테이블 보기, 호스트 또는 패킷 보기 페이지로 구성될 수 있습니다.

이벤트 평가 프로세스가 변경될 경우 새 필요에 맞게 맞춤형 워크플로를 수정할 수 있습니다. 사전 정의 워크플로는 수정할 수 없습니다.

팁 어떤 이벤트 유형에서도 맞춤형 워크플로를 기본 워크플로로 설정할 수 없습니다.

저장된 맞춤형 워크플로

수정 불가한 사전 정의 워크플로 외에도 Firepower Management Center에는 여러 저장된 맞춤형 워크플로가 있습니다. 이 워크플로 각각은 맞춤형 테이블을 기반으로 하며 수정 가능합니다.

다중 도메인 구축의 경우, 이러한 저장된 워크플로는 Global(전역) 도메인에 속하며 하위 도메인에서는 수정할 수 없습니다.

표 *1:* 저장된 맞춤형 워크플로

워크플로 이름	설명
Events by Impact, Priority, and Host Criticality(영향, 우선순위, 호스트 중요도별 이벤트)	이 워크플로를 사용하여 네트워크에 중요한 호스트, 현재 취약한 호스트, 현재 공격을 받고 있는 호스트를 신속하게 선별하여 집중할 수 있습니다. 이 워크플로는 Intrusion Events with Destination Criticality(대상 중요도가 있는 침입 이벤트) 맞춤형 테이블을 기반으로 합니다.
우선순위 및 분류별 이벤트	이 워크플로는 이벤트와 그 유형을 이벤트 우선순위에 따라 나열하며 각 이벤트의 발생 횟수 카운트도 표시합니다. 이 워크플로는 Intrusion Events(침입 이벤트) 맞춤형 테이블을 기반으로 합니다.
Events with Destination, Impact, and Host Criticality(대상, 영향, 호스트 중요도가 있는 이벤트)	이 워크플로를 사용하여 현재 취약한 상태이며 네트워크에 중요한 호스트에서 발생한 최근의 공격을 확인할 수 있습니다. 이 워크플로는 Intrusion Events with Destination Criticality 사용자 정의 테이블을 기반으로 합니다.
Hosts with Servers Default Workflow(서버 기본 워크플로가 있는 호스트)	이 워크플로를 사용하여 Hosts with Servers(서버가 있는 호스트) 맞춤형 테이블의 기본 정보를 신속하게 볼 수 있습니다. 이 워크플로는 Hosts with Servers(서버가 있는 호스트) 맞춤형 테이블을 기반으로 합니다.
Intrusion Events with Destination Criticality Default Workflow(대상 중요도 기본 워크플로가 있는 침입 이벤트)	이 워크플로를 사용하여 Intrusion Events with Destination Criticality(대상 중요도가 있는 침입 이벤트) 맞춤형 테이블의 기본 정보를 신속하게 볼 수 있습니다. 이 워크플로는 Intrusion Events with Destination Criticality 사용자 정의 테이블을 기반으로 합니다.
Intrusion Events with Source Criticality Default Workflow(소스 중요도 기본 워크플로가 있는 침입 이벤트)	이 워크플로를 사용하여 Intrusion Events with Source Criticality(소스 중요도가 있는 침입 이벤트) 맞춤형 테이블의 기본 정보를 신속하게 볼 수 있습니다. 이 워크플로는 Intrusion Events with Source Criticality(소스 중요도가 있는 침입 이벤트) 맞춤형 테이블을 기반으로 합니다.

워크플로 이름	설명
Server and Host Details(서버 및 호스트 상세정보)	이 워크플로를 사용하여 네트워크에서 어떤 서버가 가장 많이 사용되었는지 그리고 어떤 호스트에서 이 서버를 실행하고 있는지를 확인할 수 있습니다. 이 워크플로는 Hosts with Servers(서버가 있는 호스트) 사용자 지정 테이블을 기반으로 합니다.

맞춤형 워크플로 생성

사전 정의된 워크플로와 Cisco에서 제공하는 맞춤형 워크플로가 필요에 부합하지 않을 경우, 맞춤형 워크플로를 생성해야 합니다.

팁 새 맞춤형 워크플로를 생성하지 않고 다른 어플라이언스에서 맞춤형 워크플로를 내보낸 다음 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 워크플로를 필요에 맞게 수정할 수 있습니다.

맞춤형 워크플로를 생성할 때는 다음을 수행합니다.

- 워크플로의 소스가 될 테이블 선택
- 워크플로 이름 지정
- 워크플로에 드릴다운 페이지 및 테이블 보기 페이지 추가

워크플로의 각 드릴다운 페이지에 대해 다음을 수행할 수 있습니다.

- 웹 인터페이스에서 페이지의 맨 위에 나타날 이름 지정
- 페이지당 최대 5개의 열 포함
- 기본 정렬 순서 지정, 오름차순 또는 내림차순

일련의 워크플로 페이지에서 임의의 위치에 테이블 보기 페이지를 추가할 수 있습니다. 여기에는 페이지 이름, 정렬 순서, 맞춤형 열 위치와 같은 수정 가능한 속성이 없습니다.

참고 하나 이상의 드릴다운 페이지 또는 이벤트 테이블 보기를 맞춤형 워크플로에 추가해야 합니다.

참고 테이블 유형으로 **Vulnerabilities(**취약성**)**를 선택한 경우, **IP Address(IP** 주소**)**를 테이블 열로 추가하면 맞춤형 워크플로에서 취약성을 볼 때 IP Address 열이 나타나지 않습니다. 단, 검색 기능을 사용하여 특정 IP 주소 또는 주소 영역을 표시하도록 워크플로를 제한하는 경우는 제외합니다.

맞춤형 워크플로의 최종 페이지는 다음 표에서 설명하는 것처럼 워크플로의 기반이 되는 테이블에 따라 달라집니다. 이 최종 페이지는 워크플로 생성 시 기본적으로 추가됩니다.

표 *2:* 맞춤형 워크플로의 최종 페이지

이벤트/자산 유형	최종 페이지
검색 이벤트	호스트
취약성	취약성 상세정보
서드파티 취약성	호스트
사용자	사용자
보안 침해 지표	호스트
침입 이벤트	패킷

시스템은 다른 종류의 이벤트(예: 감사 로그, 악성 코드 이벤트)를 기반으로 한 맞춤형 워크플로에는 최종 페이지를 추가하지 않습니다.

연결 데이터를 기반으로 하는 맞춤형 워크플로는 다른 맞춤형 워크플로와 동일하지만, 연결 요약 데이터가 있는 드릴다운 페이지와 연결 데이터 그래프 페이지, 개별 연결 및 테이블 보기 페이지가 있는 드릴다운 페이지를 포함할 수 있습니다.

비 연결 데이터 기반 맞춤형 워크플로 생성

비 연결 데이터를 기반으로 맞춤형 워크플로우를 생성하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**맞춤형 워크플로**)**을(를) 선택합니다.

단계 **2** **Create Custom Workflow(**맞춤형 워크플로 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 워크플로의 이름을 입력합니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** **Table(**테이블**)** 드롭다운 목록에서 추가할 표를 선택합니다.

단계 **6** 워크플로에 드릴다운 페이지를 하나 이상 추가하려는 경우에는 **Add Page(**페이지 추가**)**를 클릭합니다.

단계 **7** **Page Name(**페이지 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **8** Column 1에서 정렬 우선순위와 테이블 열을 선택합니다. 이 열은 페이지의 맨 왼쪽 열로 나타납니다.

예제**:**

예를 들어 대상이 된 대상 포트를 표시하는 페이지를 생성하고 그 페이지를 카운트 순으로 정렬하려면, **Sort Priority(**정렬 우선순위**)** 드롭다운 목록에서 **2**를 선택하고 **Field(**필드**)**드롭다운 목록에서 **Destination Port/ICMP Code(**대상 포트**/ICMP** 코드**)**를 선택합니다.

단계 **9** 페이지에 표시할 필드가 모두 지정될 때까지, 포함할 필드를 선택하고 정렬 우선순위를 설정합니다.

단계 **10** 테이블 보기 페이지 워크플로를 추가 하려는 경우 추가 테이블 보기를 클릭 합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

맞춤형 연결 데이터 워크플로 생성

연결 데이터 기반의 맞춤형 워크플로는 다른 맞춤형 워크플로와 비슷하지만, 드릴다운 페이지 및 테이블 보기 페이지뿐 아니라 연결 데이터 그래프 페이지까지 포함할 수 있습니다. 각 페이지 유형을 원하는 개수와 순서로 워크플로에 포함할 수 있습니다. 각 연결 데이터 그래프 페이지는 단일 그래프를 포함하는데, 이는 선 그래프, 막대 그래프 또는 원도표가 될 수 있습니다. 선 그래프와 막대 그래프는 둘 이상의 데이터 집합을 포함할 수 있습니다.

연결 데이터를 기반으로 맞춤형 워크플로우를 생성하려면 관리자 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**맞춤형 워크플로**)**을(를) 선택합니다.

단계 **2** **Create Custom Workflow(**맞춤형 워크플로 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 워크플로의 이름을 입력합니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** **Table(**표**)** 드롭다운 목록에서 **Connection Events(**연결 이벤트**)**를 선택합니다.

단계 **6** 워크플로에 드릴다운 페이지를 하나 이상 추가하려는 경우에는 두 가지 방법을 사용할 수 있습니다.

- **Add Page(**페이지 추가**)**를 클릭하여 개별 연결의 데이터를 포함하는 드릴다운 페이지를 추가합니다.
- **Add Summary Page(**요약 페이지 추가**)**를 클릭하여 연결 요약 데이터를 포함하는 드릴다운 페이지를 추가합니다.

단계 **7** **Page Name(**페이지 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **8** **Column 1**에서 정렬 우선순위와 테이블 열을 선택합니다. 이 열은 페이지의 맨 왼쪽 열로 나타납니다.

단계 **9** 페이지에 표시할 필드가 모두 지정될 때까지, 포함할 필드를 선택하고 정렬 우선순위를 설정합니다.

예제**:**

예를 들어 모니터링되는 네트워크를 통해 전송된 트래픽의 양을 표시하는 페이지를 생성하고 가장 많은 트래픽을 전송한 응답자의 순으로 페이지를 정렬하려면 **Sort Priority(**정렬 우선순위**)** 드롭다운 목록에서 **1**을 선택하고 **Field(**필드**)** 드롭다운 목록에서 **Responder Bytes(**응답자 바이트**)**를 선택합니다.

단계 **10** 워크플로에 그래프 페이지를 하나 이상 추가하려는 경우에는 **Add Graph(**그래프 추가**)**를 클릭합니다.

단계 **11** **Graph Name(**그래프 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **12** 페이지에 포함하려는 그래프의 유형을 선택합니다.

- 선 그래프(선형 차트())
- 막대 그래프(막대그래프())
- 원도표원도표( ))

단계 **13** 그래프의 X축과 Y축을 선택하여 그래프에 표시할 데이터 종류를 지정합니다.

원도표에서 X축은 독립 변수를, Y축은 종속 변수를 나타냅니다.

단계 **14** 그래프에 포함할 데이터 집합을 선택합니다.

원도표는 하나의 데이터 집합만 포함할 수 있습니다.

단계 **15** 연결 데이터의 테이블 보기를 추가하려는 경우에는 **Add Table View(**테이블 보기 추가**)**를 클릭합니다.

테이블 보기를 구성할 수 없습니다.

단계 **16** **Save(**저장**)**를 클릭합니다.

맞춤형 워크플로 사용 및 관리

워크플로를 표시하는 데 사용하는 방법은 워크플로가 사전 정의 이벤트 테이블 중 하나 또는 맞춤형 테이블을 기반으로 하느냐에 따라 달라집니다.

맞춤형 워크플로가 사전 정의 이벤트 테이블을 기반으로 할 경우 어플라이언스와 함께 제공되는 워크플로에 액세스하는 것과 동일한 방법으로 액세스합니다. 예를 들어 Hosts(호스트) 테이블을 기반으로 하는 맞춤형 워크플로에 액세스하려면 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Hosts(**호스트**)**을(를) 선택합니다. 반대로 맞춤형 워크플로가 맞춤형 테이블을 기반으로 한다면, Custom Tables(맞춤형 테이블) 페이지에서 액세스해야 합니다.

이벤트 평가 프로세스가 변경될 경우 새 필요에 맞게 맞춤형 워크플로를 수정할 수 있습니다. 사전 정의 워크플로는 수정할 수 없습니다.

팁 어떤 이벤트 유형에서도 맞춤형 워크플로를 기본 워크플로로 설정할 수 없습니다.

사전 정의 테이블 기반 맞춤형 워크플로 보기

맞춤형 워크플로우를 보려면 관리자, 유지 보수 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** 워크플로 선택에서 설명한 대로 맞춤형 워크플로의 기반이 되는 테이블에 적합한 메뉴 경로와 옵션을 선택합니다.

단계 **2** 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 현재 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다.

단계 **3** 어떤 이벤트도 발생하지 않으며 워크플로를 시간으로 제한할 수 있다면, 시간 범위 조정이 필요할 수 있습니다. 이벤트 시간 제약 조건 섹션을 참조하십시오.

맞춤형 테이블 기반 맞춤형 워크플로 보기

맞춤형 테이블을 기반으로 하는 맞춤형 워크플로우를 보려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 워크플로를 표시하며 이러한 워크플로는 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 워크플로도 표시되지만, 이러한 워크플로는 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 워크플로를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**맞춤형 테이블**)**를 선택합니다.

단계 **2** 확인할 맞춤형 테이블 옆의 보기 ( )를 클릭하거나 맞춤형 테이블의 이름을 클릭합니다.

단계 **3** 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다.

단계 **4** 어떤 이벤트도 발생하지 않으며 워크플로를 시간으로 제한할 수 있다면, 시간 범위 조정이 필요할 수 있습니다. 이벤트 시간 제약 조건 섹션을 참조하십시오.

맞춤형 워크플로

맞춤형 워크 플로우를 편집하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 워크플로를 표시하며 이러한 워크플로는 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 워크플로도 표시되지만, 이러한 워크플로는 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 워크플로를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**맞춤형 워크플로**)**를 선택합니다.

단계 **2** 편집하려는 워크플로 이름 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 원하는 변경사항을 워크플로에 적용합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.