사용자 지정 표

다음 주제에서는 맞춤형 테이블을 사용하는 방법을 설명합니다.

맞춤형 테이블 소개

Firepower System이 네트워크에 대한 정보를 수집하면 Firepower Management Center은(는) 이를 일련의 데이터베이스 테이블에 저장합니다. 워크플로를 사용하여 결과 정보를 볼 경우 Firepower Management Center은(는) 이러한 테이블 중 하나에서 데이터를 가져옵니다. 예를 들어 Count 워크플로의 각 Network Applications(네트워크 애플리케이션) 페이지에 있는 열은 Applications(애플리케이션) 테이블의 필드에서 옵니다.

서로 다른 테이블의 필드를 조합하여 네트워크에서의 활동 분석을 개선할 수 있다고 생각되는 경우 맞춤형 테이블을 생성할 수 있습니다.

사전 정의 테이블 또는 맞춤형 테이블에 대한 맞춤형 워크플로를 생성할 수 있습니다.

사전 정의 맞춤형 테이블

맞춤형 테이블에는 둘 이상의 사전 정의 테이블에서 오는 필드가 포함됩니다. Firepower System에서는 다수의 시스템 정의 맞춤형 테이블을 제공하지만, 사용자는 특정 요구에 맞는 정보만 포함하는 맞춤형 테이블을 추가로 생성할 수 있습니다.

예를 들어 Firepower System에서는 침입 이벤트 데이터를 호스트 데이터와 상호 연결하는 시스템 정의 맞춤형 테이블을 제공하므로, 중요 시스템에 영향을 미치는 이벤트를 검색하고 하나의 워크플로에서 검색 결과를 볼 수 있습니다.

다중 도메인 구축의 경우, 사전 정의된 맞춤형 테이블은 Global(전역) 도메인에 속하며 하위 도메인에서는 수정할 수 없습니다.

다음 표에서는 시스템에서 제공하는 맞춤형 테이블에 대해 설명합니다.

표 *1:* 시스템 정의 맞춤형 테이블

표	설명
서버가 있는 호스트	Hosts(호스트) 및 Servers(서버) 테이블의 필드를 포함하며, 네트워크에서 실행 중인 탐지된 애플리케이션에 대한 정보는 물론 그러한 애플리케이션을 실행하는 호스트에 대한 기본 운영체제 정보도 제공합니다.
대상 중요도가 있는 침입 이벤트	Intrusion Events(침입 이벤트) 및 Hosts(호스트) 테이블의 필드를 포함하며, 침입 이벤트에 대한 정보는 물론 각 침입 이벤트와 관련된 대상 호스트의 호스트 중요도도 제공합니다. 이 테이블을 사용해 호스트 중요도가 높은 대상 호스트와 관련된 침입 이벤트를 검색할 수 있습니다.
소스 중요도가 있는 침입 이벤트	Intrusion Events(침입 이벤트) 및 Hosts(호스트) 테이블의 필드를 포함하며, 침입 이벤트에 대한 정보 및 각 침입 이벤트와 관련된 소스 호스트의 호스트 중요도를 확인할 수 있습니다. 이 테이블을 사용해 호스트 중요도가 높은 소스 호스트와 관련된 침입 이벤트를 검색할 수 있습니다.

가능한 테이블 조합

맞춤형 테이블을 만들 때에는 관련 데이터가 포함된 사전 정의 테이블의 필드를 조합할 수 있습니다. 다음 표에는 새 맞춤형 테이블 생성을 위해 조합할 수 있는 사전 정의 테이블이 나열되어 있습니다. 둘 이상의 사전 정의된 맞춤형 테이블에서 오는 필드를 조합하는 맞춤형 테이블을 생성할 수 있습니다.

표 *2:* 맞춤형 테이블 조합

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
애플리케이션	• 상관 관계 이벤트 • 침입 이벤트 • 연결 요약 데이터 • 호스트 속성 • 애플리케이션 세부사항 • 검색 이벤트 • 호스트 • 서버 • 화이트 이벤트 나열
Correlation Events	• 애플리케이션 • 호스트 속성 • 호스트
침입 이벤트	• 애플리케이션 • 호스트 속성 • 호스트 • 서버
Connection Summary Data(연결 요약 데이터)	• 애플리케이션 • 호스트 속성 • 호스트 • 서버

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
보안 침해 지표	• 애플리케이션 • 애플리케이션 세부사항 • 캡처된 파일 • Connection Summary Data(연결 요약 데이터) • Correlation Events • 검색 이벤트 • 호스트 속성 • 호스트 • 침입 이벤트 • 보안 인텔리전스 이벤트 • 서버 • 화이트 이벤트 나열
호스트 속성	• 애플리케이션 • Correlation Events • 침입 이벤트 • Connection Summary Data(연결 요약 데이터) • 애플리케이션 세부사항 • 검색 이벤트 • 호스트 • 서버 • 화이트 이벤트 나열
애플리케이션 세부사항	• 애플리케이션 • 호스트 속성 • 호스트
검색 이벤트	• 애플리케이션 • 호스트 속성 • 호스트

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
보안 인텔리전스 이벤트	• 애플리케이션 • 호스트 속성 • 호스트 • 서버
호스트	• 애플리케이션 • Correlation Events • 침입 이벤트 • Connection Summary Data(연결 요약 데이터) • 호스트 속성 • 애플리케이션 세부사항 • 검색 이벤트 • 서버 • 화이트 이벤트 나열
서버	• 애플리케이션 • 침입 이벤트 • Connection Summary Data(연결 요약 데이터) • 호스트 속성 • 호스트
화이트 이벤트 나열	• 애플리케이션 • 호스트 속성 • 호스트

때때로 한 테이블의 한 필드가 또 다른 테이블의 둘 이상의 필드에 매핑됩니다. 예를 들어 사전 정의된 **Intrusion Events with Destination Criticality(**대상 중요도가 있는 침입 이벤트**)** 맞춤형 테이블은 Events(이벤트) 테이블과 Hosts(호스트) 테이블의 필드를 결합합니다. Intrusion Events(침입 이벤트) 테이블의 각 이벤트에는 두 개의 관련 IP 주소(소스 IP 주소 및 목적지 IP 주소)가 있습니다. 그러나 Hosts(호스트) 테이블의 "이벤트"는 각각 단일 호스트 IP 주소를 나타냅니다(호스트에 여러 IP 주소가 있을 수 있음). 따라서 Intrusion Events(침입 이벤트) 테이블과 Hosts(호스트) 테이블을 기반으로 맞춤형 테이블을 생성할 때에는 Hosts(호스트) 테이블에서 표시하는 데이터가 Intrusion Events(침입 이벤

트) 테이블의 호스트 소스 IP 주소 또는 호스트 목적지 IP 주소에 적용되는지 여부를 선택해야 합니다.

새 맞춤형 테이블을 생성하면 테이블의 모든 열을 표시하는 기본 워크플로가 자동으로 생성됩니다. 또한 사전 정의 테이블과 마찬가지로, 네트워크 분석에서 사용할 데이터에 대한 맞춤형 테이블을 검색할 수 있습니다. 사전 정의 테이블과 마찬가지로, 맞춤형 테이블을 기반으로 보고서를 생성할 수 있습니다.

사용자 정의 맞춤형 테이블

팁 새 맞춤형 테이블을 생성하는 대신, 다른 Firepower Management Center에서 맞춤형 테이블을 내보낸 다음 현재 Firepower Management Center로 가져올 수 있습니다.

맞춤형 테이블을 생성하려면, Firepower System과 함께 제공된 사전 정의 테이블 중 어떤 것에 맞춤형 테이블에 포함할 필드가 포함되어 있는지를 확인해야 합니다. 그런 다음, 포함하고자 하는 필드를 선택하고 필요한 경우 공통 필드에 대한 필드 매핑을 구성할 수 있습니다.

팁 Hosts(호스트) 테이블과 관련된 데이터에서는 하나의 특정 IP 주소보다는 한 호스트의 모든 IP 주소와 연결된 데이터를 볼 수 있습니다.

예를 들어 Correlation Events(상관관계 이벤트) 테이블과 Hosts(호스트) 테이블의 필드를 조합하는 맞춤형 테이블이 있다고 가정해보겠습니다. 이 맞춤형 테이블을 사용하면 상관관계 정책의 위반과 관련된 호스트에 대한 자세한 정보를 얻을 수 있습니다. Correlation Events(상관관계 이벤트) 테이블의 소스 IP 주소 또는 목적지 IP 주소와 일치하는 Hosts(호스트) 테이블의 데이터를 표시할지 여부를 결정해야 합니다.

이 맞춤형 테이블에 대한 이벤트를 테이블 보기로 보면 한 행에 하나씩 상관관계 이벤트가 표시됩니다. 다음 정보를 포함하도록 맞춤형 테이블을 설정할 수 있습니다.

- 이벤트가 생성된 날짜 및 시간
- 위반된 상관관계 정책의 이름
- 위반을 트리거한 규칙의 이름
- 상관관계 이벤트와 관련된 소스 또는 시작 호스트와 연결된 IP 주소
- 소스 호스트의 NetBIOS 이름
- 소스 호스트가 실행 중인 운영체제 및 버전
- 소스 호스트 중요도

팁 대상 또는 응답 호스트에 대한 동일한 정보를 표시하는 유사한 맞춤형 테이블을 생성할 수 있습니다.

맞춤형 테이블 생성

프로시저

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

단계 **2** **Create Custom Table(**맞춤형 테이블 생성**)**을 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 맞춤형 테이블의 이름을 입력합니다.

예제**:**

예를 들어 `Correlation Events with Host Information (Src IP)`을 입력할 수 있습니다.

단계 **4** **Tables(**테이블**)** 드롭다운 목록에서 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.

단계 **5** **Fields(**필드**)**에서 **Time(**시간**)**을 선택하고 **Add(**추가**)**를 클릭하여 상관관계 이벤트가 생성된 날짜와 시간을 추가합니다.

단계 **6** 5단계를 반복하여 **Policy(**정책**)** 및 **Rule(**규칙**)** 필드를 추가합니다.

팁 여러 필드를 선택하려면 Ctrl 또는 Shift 키를 누른 상태에서 클릭합니다. 클릭하고 드래그하여 인접한 여러 값을 선택할 수도 있습니다. 그러나 테이블과 연결된 이벤트의 테이블 보기에 필드가 나타나는 순서를 지정하려면, 필드를 한 번에 하나씩 추가해야 합니다.

단계 **7** **Tables(**테이블**)** 드롭다운 목록에서 **Hosts(**호스트**)**를 선택합니다.

단계 **8** 맞춤형 테이블에 **IP Address(IP** 주소**)**, **NetBIOS Name(NetBIOS** 이름**)**, **OS Name(**운영체제 이름**)**, **OS Version(**운영체제 버전**)** 및 **Host Criticality(**호스트 중요도**)** 필드를 추가합니다.

단계 **9** **Common Fields(**공통 필드**)** 아래의 **Correlation Events(**상관관계 이벤트**)** 옆에 있는 **Source IP(**소스 **IP)**를 선택합니다.

상관관계 이벤트와 관련된 소스 또는 시작 호스트에 대해 8단계에서 선택한 호스트 정보를 표시하도록 맞춤형 테이블이 구성됩니다.

팁 이 절차를 수행하되 **Source IP(**소스 **IP)** 대신 **Destination IP(**목적지 **IP)**를 선택하여, 상관관계 이벤트와 관련된 대상 또는 응답 호스트에 대한 자세한 호스트 정보를 표시하는 맞춤형 테이블을 생성할 수 있습니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

맞춤형 테이블 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며 이러한 테이블은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 수정

할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

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

단계 **2** 편집하려는 테이블 옆에 있는 수정( )을 클릭합니다.

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

단계 **3** 선택적으로, 제거하려는 필드 옆에 있는 삭제( )을 클릭하여 테이블에서 필드를 제거합니다.

참고 보고서에 현재 사용되고 있는 필드를 삭제하는 경우, 해당 보고서에서 해당 필드를 사용하는 섹션을 제거할 것인지 묻는 메시지가 표시됩니다.

단계 **4** 필요에 따라 다른 변경사항을 적용합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

맞춤형 테이블 삭제

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며, 이러한 테이블은 삭제할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 삭제할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 삭제하려면 해당 도메인으로 전환하십시오.

프로시저

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

단계 **2** 삭제하고자 하는 맞춤형 테이블 옆에 있는 아이콘(삭제( ))을 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

맞춤형 테이블 기반 워크플로 보기

맞춤형 테이블을 생성하면 시스템은 자동으로 이에 대한 기본 워크플로를 생성합니다. 이 워크플로의 첫 번째 페이지에는 이벤트의 테이블 보기가 표시됩니다. 맞춤형 테이블에 침입 이벤트를 포함하면 워크플로의 두 번째 페이지는 패킷 보기 페이지가 됩니다. 그렇지 않으면 워크플로의 두 번째 페

이지는 호스트 페이지가 됩니다. 맞춤형 테이블을 기반으로 고유한 맞춤형 워크플로를 생성할 수도 있습니다.

팁 맞춤형 테이블을 기반으로 맞춤형 워크플로를 만드는 경우이를 해당 테이블의 기본 워크플로로 지정할 수 있습니다.

사전 정의 테이블을 기반으로 이벤트 보기에 대해 사용하는 맞춤형 테이블에서 이벤트를 보려면 이 방법을 사용할 수 있습니다.

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

프로시저

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

단계 **2** 확인할 워크플로와 관련된 맞춤형 테이블 옆에 있는 보기 ( )을 클릭합니다.

맞춤형 테이블 검색

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

프로시저

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

단계 **2** 검색할 맞춤형 테이블 옆에 있는 보기 ( )을 클릭합니다.

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

단계 **3** **Search(**검색**)**를 클릭합니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트 또는 데이터를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

단계 **4** 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다.

팁 검색 기준으로 개체를 사용하려면 검색 필드 옆에 있는 개체( )을 클릭합니다.

단계 **5** 선택적으로, 검색을 저장하려면 **Private(**비공개**)** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 마십시오.

팁 사용자 지정 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다.

단계 **6** 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save(**저장**)**를 클릭합니다. **Private(**비공개**)** 확인란을 선택해야 검색이 계정에 표시됩니다.
- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New(**신규로 저장**)**를 클릭합니다. **Private(**비공개**)** 확인란을 선택해야 검색이 저장되고 계정에 표시됩니다.

단계 **7** 검색을 시작하려면 **Search(**검색**)**를 클릭합니다.

검색 결과가 현재 시간과 범위로 제한되어(적용 가능한 경우) 맞춤형 테이블에 대한 기본 워크플로에 나타납니다.

맞춤형 테이블 기록

기능	버전	세부 사항
맞춤형 테이블의 연결 이벤트 지원은 삭제되었습니다.	6.6	이제 연결 이벤트가 포함된 맞춤형 테이블을 생성할 수 없습니다. 6.6 버전으로 업그레이드한 경우: 연결 이벤트가 있는 기존 테이블은 사용되지 않음으로 표시되며 데이터가 표시되지 않고 테이블을 내보내거나 편집할 수 없습니다. 기존 보고서, 맞춤형 워크플로, 대시보드가 사용되지 않는 테이블을 포함할 수 있으며 사용자는 이를 검토할 수 있습니다. 수정된 화면: **Analysis(**분석**) > Advanced(**고급**) > Custom Tables(**맞춤형 테이블**)**과 맞춤형 테이블 추가 및 편집 페이지 영향을 받는 플랫폼: FMC