상관관계 및 규정 준수 이벤트

다음 주제에서는 상관관계 및 규정 준수 이벤트를 보는 방법을 설명합니다.

상관관계 이벤트 보기

활성 상관관계 정책 내 상관관계 규칙이 트리거되면 시스템은 상관관계 이벤트를 생성하고 이를 데이터베이스에 로깅합니다.

참고 활성 상관관계 정책 내 규정준수 화이트 목록이 트리거되면 시스템은 화이트 목록 이벤트를 생성합니다.

상관관계 이벤트의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

상관관계 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 상관관계 이벤트의 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > **Correlation Events(**상관관계 이벤트**)** 을(를) 선택합니다.

원하는 경우, 맞춤형 워크플로 등 다른 워크플로를 사용하려면 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.

팁 상관관계 이벤트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.

단계 **2** 원하는 경우, 타임 윈도우 변경에 설명된 대로 시간 범위를 조정합니다.

단계 **3** 다음 작업 중 하나를 수행합니다.

- 표시되는 열에 대한 자세한 내용은 상관관계 이벤트 필드, 3 페이지를 참조하십시오.
- IP 주소의 호스트 프로파일을 보려면 IP 주소 옆에 표시되는 호스트 프로파일을 클릭합니다.
- 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘를 클릭합니다.
- 이벤트를 정렬 및 제한하거나 현재 워크플로 페이지 내에서 이동하려면 워크플로 사용를 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다.
- 워크플로의 다음 페이지로 드릴다운하여 특정 값으로 제한하려면 드릴다운 페이지 사용를 참조하십시오.
- 일부 또는 모든 상관관계 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제하려 한다고 확인합니다.
- 다른 이벤트 보기로 이동해 연결된 이벤트를 보려면 워크플로 간 탐색을 참조하십시오.
- Firepower 시스템 외부에서 이용할 수 있는 소스의 데이터를 보려면 이벤트 값에서 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사 섹션을 참조해 주십시오.
- 이벤트에 대한 인텔리전스를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사를 참고하십시오.

관련 항목

데이터베이스 이벤트 제한 수

워크플로 페이지

상관관계 이벤트 필드

상관관계 규칙이 트리거되면 시스템은 상관관계 이벤트를 생성합니다. 다음 표는 상관관계 테이블에서 보고 검색할 수 있는 필드를 설명합니다.

표 *1:* 상관관계 이벤트 필드

필드	설명
설명	상관관계 이벤트의 설명. 설명의 정보는 규칙이 트리거된 방식에 따라 달라집니다. 예를 들어 규칙이 운영 체제 정보 업데이트 이벤트에 의해 트리거된 경우 새 운영 체제 이름 및 신뢰도 레벨이 나타납니다.
디바이스	정책 위반을 트리거한 이벤트를 생성한 디바이스의 이름.
도메인	모니터링되는 트래픽이 정책 위반을 트리거한 디바이스의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
영향	침입 데이터, 검색 데이터, 취약성 정보 간 상관관계를 기반으로 상관관계 이벤트에 할당되는 영향 레벨. 이 필드를 검색할 때 대소문자를 구분하지 않는 유효한 값은 `Impact 0`, `Impact Level 0`, `Impact 1`, `Impact Level 1`, `Impact 2`, `Impact Level 2`, `Impact 3`, `Impact Level 3`, `Impact 4`, `Impact Level 4`입니다. 영향 아이콘 색 이나 부분 문자열을 사용하지 마십시오(예를 들어 `blue`, `level 1` 또는`0`을 사용하지 마십시오).
Ingress Interface 또는 Egress Interface	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 인터페이스.
Ingress Security Zone 또는 Egress Security Zone	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 보안 영역.

필드	설명
인라인 결과	다음 중 하나에 해당합니다. • 검은색 아래쪽 화살표 - 시스템이 침입 규칙을 트리거한 패킷을 삭제했음을 나타냄 • 회색 아래쪽 화살표 - **Drop when Inline(**인라인 시 삭제**)** 침입 정책 옵션을 활성화했다면 시스템이 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제했을 것임을 나타냄 • 공백 - 트리거된 침입 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)으로 설정되지 않았음을 나타냄 이 필드를 사용하여 침입 이벤트에 의해 트리거되는 정책 위반을 검색할 때는 다음 중 하나를 입력합니다. • `dropped` - 패킷이 인라인, 스위치드 또는 라우티드 구축에서 삭제되었는지 여부를 지정 • `would have dropped` - 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제하도록 침입 정책을 구성했다면 패킷이 삭제되었을 것인지를 지정 침입 정책의 규칙 상태 또는 삭제 동작과 상관없이, 인라인 집합이 탭 모드인 경우를 포함하여 패시브 구축에서는 시스템이 패킷을 삭제하지 않습니다.
정책	위반된 정책의 이름.
Priority(우선순위)	트리거된 규칙 또는 위반된 상관관계 정책의 우선순위에 의해 결정되는 상관관계 이벤트의 우선순위. 이 필드를 검색할 때 우선순위가 없는 경우, `none`을 입력합니다.
규칙	정책 위반을 트리거한 규칙의 이름.
보안 인텔리전스 카테고리	정책 위반을 트리거한 이벤트에서 차단된 IP 주소를 나타내거나 포함하는 개체의 이름. 이 필드를 검색할 때 정책 위반을 트리거한 상관 관계 이벤트에 연결된 보안 인텔리전스 카테고리를 지정합니다. 보안 인텔리전스 카테고리는 보안 인텔리전스 개체의 이름, 전역 차단 목록, 맞춤형 보안 인텔리전스 목록이나 피드 또는 인텔리전스 피드의 카테고리 중 하나일 수 있습니다.
Source Continent 또는 Destination Continent	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트 IP 주소에 연결된 대륙.

필드	설명
Source Country 또는 Destination Country	정책 위반을 트리거한 이벤트에서 소스 또는 대상 IP 주소에 연결된 국가.
Source Host Criticality 또는 Destination Host Criticality	상관관계 이벤트와 관련된 소스 또는 대상 호스트에 사용자가 할당하는 호스트 중요도: `None`, `Low`, `Medium`, `High`. 검색 이벤트, 호스트 입력 이벤트 또는 연결 이벤트 기반의 규칙에 의해 생성된 상관관계 이벤트에만 소스 호스트 중요도가 포함됩니다.
Source IP 또는Destination IP	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트의 IP 주소.
Source Port/ICMP Type 또는 Destination Port/ICMP Code	정책 위반을 트리거한 이벤트에 연결된 소스 트래픽의 소스 포트 또는 ICMP 유형 또는 대상 트래픽의 대상 포트 또는 ICMP 코드.
Source User 또는 Destination User	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트에 로그인한 사용자의 이름.
시간	상관관계 이벤트가 생성된 날짜 및 시간. 이 필드는 검색할 수 없습니다.
Count(개수)	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약조건을 적용한 경우에만 **Count(**개수**)** 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색

컴플라이언스 화이트 목록 워크플로우 사용

Firepower Management Center에서는 네트워크에 대해 생성되는 화이트 목록 이벤트 및 위반의 분석에 사용할 수 있는 워크플로우 집합을 제공합니다. 워크플로는 네트워크 맵 및 대시보드와 더불어 네트워크 자산의 규정 준수에 대한 핵심 정보 소스입니다.

시스템은 화이트 목록 이벤트 및 위반에 대한 사전 정의된 워크플로우를 제공합니다. 사용자 지정 워크플로를 생성할 수도 있습니다. 규정 준수 화이트 목록 워크플로우를 사용하면 여러 일반적인 작업을 수행할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 보안 분석가 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관 관계**)** 메뉴를 사용하여 화이트 목록 워크플로우에 액세스합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 워크플로 전환 - 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 시간 범위 - 시간 범위를 조정합니다. 이벤트가 표시되지 않는 경우에 유용합니다(타임 윈도우 변경 참조).
- 호스트 프로파일 - IP 주소의 호스트 프로파일을 보려면 호스트 프로파일()을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 보안 침해된 호스트를 클릭합니다.
- 사용자 프로파일(이벤트만 해당) - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘를 클릭합니다.
- 제한 - 표시되는 열을 제한하려면 숨기려는 열 머리글의 닫기( )을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 검색 제약 조건을 확장한 다음 Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 드릴다운 - 드릴다운 페이지 사용 참조.
- 정렬 - 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.
- 이 페이지 탐색 - 워크플로 페이지 이동 툴 참조.
- 페이지 간 이동 - 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 이벤트 보기 간 이동 - 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.
- 이벤트 삭제(이벤트만 해당) - 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.

관련 항목

워크플로 페이지

이벤트 보기 구성

화이트리스트 이벤트 보기

최초 평가 후 시스템은 모니터링되는 호스트가 활성 화이트리스트 규정준수에서 벗어날 때마다 화이트리스트 이벤트를 생성합니다. 화이트리스트는 특수한 종류의 상관관계 이벤트이며, FMC 상관관계 이벤트 데이터베이스에 로깅됩니다.

Firepower Management Center를 사용하여 규정준수 화이트리스트 이벤트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

화이트리스트 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로우에 따라 달라집니다. 이벤트의 테이블 보기에서 종료되는 미리 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 보안 분석가 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > 화이트리스트**Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 기본 워크플로 작업을 수행하려면 컴플라이언스 화이트 목록 워크플로우 사용, 5 페이지를 참조하십시오.
- 테이블의 열 내용을 자세히 알아보려면 화이트 목록 이벤트 필드, 7 페이지를 참조하십시오.
- 더 많은 옵션을 보려면 테이블의 값을 마우스 오른쪽 버튼으로 클릭합니다.

화이트 목록 이벤트 필드

워크플로를 사용하여 보고 검색할 수 있는 화이트 목록 이벤트에는 다음 필드가 포함됩니다.

디바이스

화이트 목록 위반을 탐지한 매니지드 디바이스의 이름입니다.

설명

화이트 목록을 어떤 식으로 위반했는지 설명합니다. 예를 들면 다음과 같습니다.

클라이언트 “AOL Instant Messenger”는 허용되지 않습니다.

애플리케이션 프로토콜과 관련된 위반은 애플리케이션 프로토콜 이름과 버전은 물론 애플리케이션 프로토콜이 사용 중인 포트와 프로토콜(TCP 또는 UDP)을 나타냅니다. 금지를 특정 운영 체제로 제한할 경우, 설명에는 해당 운영 체제 이름이 포함됩니다. 예를 들면 다음과 같습니다.

서버 "ssh / 22 TCP (OpenSSH 3.6.1p2)"는 운영 체제 “Linux Linux 2.4 또는 2.6”에서 허용되지 않습니다.

도메인

화이트 목록을 준수하지 않게 된 호스트의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Host Criticality(호스트 심각도**)**

화이트 목록을 준수하지 않는 소스 호스트에 대해 사용자가 할당하는 호스트 중요도(None, Low, Medium, High)입니다.

IP 주소

화이트 목록을 준수하지 않게 된 호스트의 IP 주소.

정책

위반된 상관관계 정책의 이름입니다. 즉, 화이트 목록이 포함된 상관관계 정책입니다.

포트

애플리케이션 프로토콜 화이트 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 검색 이벤트에 연결된 포트. 다른 유형의 화이트 목록 위반의 경우, 이 필드는 비어 있습니다.

Priority(우선순위**)**

정책 또는 정책 위반을 트리거한 화이트 목록에 의해 지정된 우선순위. 상관관계 정책의 화이트 목록 우선 순위 또는 상관관계 정책 자체의 우선 순위에 의해 결정됩니다. 화이트 목록 우선 순위는 해당 정책의 우선 순위를 재정의합니다. 이 필드를 검색할 때 우선 순위가 없는 경우, `none`을 입력합니다.

시간

화이트 목록 이벤트가 생성된 시간 및 날짜입니다. 이 필드는 검색할 수 없습니다.

User

화이트 목록을 준수하지 않게 된 호스트에 로그인한 알려진 사용자의 ID.

화이트 목록

화이트 목록의 이름입니다.

Count(개수)

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

화이트리스트 위반 보기

시스템은 네트워크에서 현재 화이트리스트 위반의 레코드를 유지합니다. 각 위반은 호스트 중 하나에서 허용되지 않는 것이 실행 중임을 나타냅니다. 호스트가 규정을 준수하게 되면 시스템은 이제 수정된 위반을 데이터베이스에서 제거합니다.

Firepower Management Center를 사용하여 모든 활성 화이트리스트에 대한 화이트리스트 위반 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

화이트리스트 위반에 액세스할 때 표시되는 페이지는 사용하는 워크플로우에 따라 달라집니다. 사전 정의 워크플로는 제약 조건을 충족하는 모든 호스트의 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(분석)** > **Correlation(상관관계)** > 화이트리스트**Violations(위반)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 기본 워크플로 작업을 수행하려면 컴플라이언스 화이트 목록 워크플로우 사용, 5 페이지를 참조하십시오.
- 테이블의 열 내용을 자세히 알아보려면 화이트 목록 위반 필드, 9 페이지를 참조하십시오.
- 더 많은 옵션을 보려면 테이블의 값을 마우스 오른쪽 버튼으로 클릭합니다.

화이트 목록 위반 필드

워크플로를 사용하여 보고 검색할 수 있는 화이트 목록 위반에는 다음 필드가 포함됩니다.

도메인

규정을 준수하지 않는 호스트가 있는 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

정보

화이트 목록 위반과 관련하여 제공되는 모든 공급업체, 제품 또는 버전 정보입니다. 화이트 목록을 위반하는 프로토콜의 경우, 이 필드에는 위반이 네트워크 프로토콜로 인한 것인지 전송 프로토콜로 인한 것이지도 표시됩니다.

IP 주소

규정 준수 위반 호스트의 IP 주소입니다.

Port(포트**)**

애플리케이션 프로토콜 화이트 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트에 연결된 포트입니다. 다른 유형의 화이트 목록 위반의 경우, 이 필드는 비어 있습니다.

프로토콜

애플리케이션 프로토콜 화이트 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트에 연결된 프로토콜. 다른 유형의 화이트 목록 위반의 경우, 이 필드는 비어 있습니다.

시간

화이트 목록 위반이 탐지된 시간 및 날짜입니다.

유형

화이트 목록 위반의 유형입니다. 즉, 규정을 준수하지 않아 발생한 위반인지 나타냅니다.

- 운영체체(os) (이 필드를 검색할 때는 **os** 또는 **operating system**을 입력합니다.)
- 애플리케이션 프로토콜(서버)
- 클라이언트
- protocol
- 웹 애플리케이션(웹) (이 필드를 검색할 때는 **web application**을 입력합니다.)

화이트 목록

위반된 화이트 목록의 이름입니다.

Count(개수**)**

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

교정 상태 이벤트

교정이 트리거되면 시스템은 교정 상태 이벤트를 데이터베이스에 로깅합니다. 이러한 이벤트는 Remediation Status(교정 상태) 페이지에서 볼 수 있습니다. 교정 상태 이벤트를 검색하고 보고 삭제할 수 있습니다.

관련 항목

교정 상태 테이블 필드, 12 페이지

교정 상태 이벤트 보기

교정 상태 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 교정 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 테이블 보기에는 각 교정 상태 이벤트의 행이 포함됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > **Status(**상태**)**을(를) 선택합니다.

단계 **2** 원하는 경우, 타임 윈도우 변경에 설명된 대로 시간 범위를 조정합니다.

단계 **3** 원하는 경우, 맞춤형 워크플로 등 다른 워크플로를 사용하려면 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.

팁 교정의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)** 메뉴를 클릭한 다음 **Remediation Status(**교정 상태**)**를 선택하십시오.

단계 **4** 다음 옵션을 이용할 수 있습니다.

- 표시되는 열에 대한 자세한 내용은 교정 상태 테이블 필드, 12 페이지를 참조하십시오.
- 이벤트를 정렬하고 제한하려면 워크플로 사용를 참조하십시오.
- 상관관계 이벤트 보기로 이동해 연결된 이벤트를 보려면 **Correlation Events(**상관관계 이벤트**)**를 클릭합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다. 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.

- 테이블 보기의 데이터를 기반으로 보고서를 생성하려면 이벤트 보기에서 보고서 템플릿 생성의 설명에 따라 **Report Designer(**리포트 디자이너**)**를 클릭합니다.
- 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용 섹션을 참조하십시오.
- 시스템에서 교정 상태 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제하려 한다고 확인합니다.
- 교정 상태 이벤트를 검색하려면 **Search(**검색**)**를 클릭합니다.

관련 항목

워크플로 사용

교정 상태 테이블 필드

다음 표는 교정 상태 테이블에서 보고 검색할 수 있는 필드를 설명합니다.

표 ***2:*** 교정 상태 필드

필드	설명
도메인	모니터링되는 트래픽이 정책 위반을 트리거한 다음 교정을 트리거한 디바이스의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
정책	위반되어 교정을 트리거한 상관관계 정책의 이름.
Remediation Name(리미디에이션 이름)	실행된 교정의 이름.

필드	설명
결과 메시지	교정이 실행되었을 때 발생한 상황을 설명하는 메시지. 상태 메시지는 다음을 포함합니다. • 성공적으로 교정 완료 • 교정 모듈에 제공된 입력에 오류가 있음 • 교정 모듈 구성에 오류가 있음 • 원격 디바이스 또는 서버에 로그인할 때 오류 발생 • 원격 디바이스 또는 서버에 대한 필요한 권한을 얻을 수 없음 • 원격 디바이스 또는 서버에 로그인할 때 시간 초과 • 원격 명령 또는 서버를 실행할 때 시간 초과 • 원격 디바이스 또는 서버에 연결하지 못했음 • 교정을 시도했으나 실패했음 • 리미디에이션 프로그램을 실행하지 못함 • 알 수 없는/예기치 않은 오류 맞춤형 교정 모듈이 설치된 경우 맞춤형 모듈에 의해 구현되는 추가 상태 메시지를 볼 수 있습니다.
규칙	교정을 트리거한 상관관계 규칙의 이름입니다.
시간	Firepower Management Center가 교정을 트리거한 날짜 및 시간
Count(개수)	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색

교정 상태 이벤트 테이블 사용

이벤트 보기의 레이아웃을 변경하거나 보기의 이벤트를 필드 값으로 제한할 수 있습니다.

비활성화한 열은 나중에 다시 추가하지 않는 한 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화하면 Count(카운트) 열이 추가됩니다.

테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 않습니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > **Status(**상태**)**을(를) 선택합니다.

팁 교정의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)** 메뉴를 클릭한 다음 **Remediation Status(**교정 상태**)**를 선택하십시오.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 표시되는 열에 대한 자세한 내용은 교정 상태 테이블 필드, 12 페이지를 참조하십시오.
- 이벤트를 정렬하고 제한하려면 워크플로 사용를 참조하십시오.