워크플로우

다음 주제에서는 워크플로를 사용하는 방법을 설명합니다.

개요: 워크플로

워크플로는 management center 웹 인터페이스에 있는 일련의 맞춤 데이터 페이지이며, 분석가는 시스템에서 생성된 이벤트를 평가하는 데 이를 사용할 수 있습니다.

다음 워크플로 유형은 management center에서 사용할 수 있습니다.

사전 정의 워크플로

시스템으로 전달한 미리 설정된 워크플로입니다. 사전 정의한 워크플로는 편집하거나 삭제할 수 없습니다. 하지만 사전 정의한 워크플로를 복사하고 맞춤형 워크플로의 기반으로 사용하는 것은 가능합니다.

저장된 맞춤형 워크플로

management center(으)로 전달한 저장된 맞춤형 테이블을 기반으로 하는 맞춤형 워크플로입니다. 이러한 워크플로는 편집, 삭제, 복사할 수 있습니다.

사용자 지정 워크플로

생성하고 필요에 맞게 맞춤형한 워크플로 또는 맞춤형 테이블을 생성할 때 시스템이 자동으로 생성한 워크플로입니다. 이러한 워크플로는 편집, 삭제, 복사할 수 있습니다.

많은 경우 워크플로에 표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다.

사전 정의 워크플로

다음 섹션에서 설명하는 사전 정의된 워크플로는 시스템을 통해 전달됩니다. 사전 정의된 워크플로는 편집하거나 삭제할 수 없지만, 사전 정의한 워크플로를 복사하고 맞춤형 워크플로의 기반으로 사용하는 것은 가능합니다.

사전 정의 침입 이벤트 워크플로

다음 표에서는 Firepower System에 포함된 사전 정의 침입 이벤트 워크플로에 대해 설명합니다.

표 ***1:*** 사전 정의 침입 이벤트 워크플로

워크플로 이름	설명
목적지 포트	대상 포트가 대개 애플리케이션과 연결되므로, 이 워크플로는 알림의 양이 비정상적으로 많은 애플리케이션을 탐지하는 데 사용할 수 있습니다. Destination Port(대상 포트) 열은 네트워크에 있어서는 안 될 애플리케이션을 식별하는 데에도 도움이 됩니다.
이벤트 관련	이 워크플로는 두 가지의 유용한 기능을 제공합니다. 자주 발생하는 이벤트는 다음을 의미할 수 있습니다. • 오탐 • 웜 • 잘못 구성된 네트워크 드물게 발생하는 이벤트는 표적 공격의 증거일 가능성이 높으므로 각별한 주의가 필요합니다.
우선순위 및 분류별 이벤트	이 워크플로는 이벤트와 그 유형을 이벤트 우선순위에 따라 나열하며 각 이벤트의 발생 횟수 카운트도 표시합니다.
대상에 대한 이벤트	이 워크플로는 어떤 호스트 IP 주소가 공격받고 있으며 공격의 특성이 어떠한지 총괄적으로 보여줍니다. 가능한 경우 공격 관련 국가에 대한 정보도 볼 수 있습니다.
IP 관련	이 워크플로에서는 어떤 호스트 IP 주소가 가장 많은 알림을 생성하는지를 보여줍니다. 이벤트 수가 가장 많은 호스트는 일반에게 공개되는 수신 웜 유형 트래픽이거나(튜닝을 위한 조사 대상으로 적합), 알림의 원인을 확인하기 위해 추가 조사가 필요한 곳입니다. 카운트가 가장 낮은 호스트 역시 조사가 필요한데, 표적 공격의 주체일 가능성이 있습니다. 카운트가 낮으면 네트워크에 속하지 않는 호스트일 수도 있습니다.
영향 및 우선순위	이 워크플로에서는 영향이 큰 반복적 이벤트를 신속하게 찾을 수 있습니다. 보고된 영향 레벨은 이벤트가 발생한 횟수와 함께 표시됩니다. 이 정보를 사용 하면 가장 자주 재발 하는 영향력이 큰 이벤트를 식별 하 여 네트워크에 대 한 광범위 한 공격의 지표가 될 수 있습니다.

워크플로 이름	설명
영향 및 소스	이 워크플로는 진행 중인 공격의 출처를 파악하는 데 도움이 될 수 있습니다. 보고된 영향 레벨은 이벤트의 소스 IP 주소와 함께 표시됩니다. 예를 들어 영향 레벨이 1인 이벤트가 동일한 IP 주소에서 반복적으로 발생하는 경우, 공격자가 취약한 시스템을 찾아내 표적으로 삼고 있음을 의미할 수 있습니다.
대상에 대한 영향	이 워크플로를 통해 취약한 컴퓨터에서 반복적으로 발생하는 이벤트를 식별할 수 있어 시스템의 취약성을 해결하고 진행 중인 공격이 있을 경우 공격을 중지시킬 수 있습니다.
소스 포트	이 워크플로는 어떤 서버에서 가장 많은 알림을 생성하는지 나타냅니다. 튜닝이 필요한 영역을 식별하고 주의가 필요한 서버를 확인하는 데 이 정보를 사용할 수 있습니다.
소스 및 대상	이 워크플로는 높은 수준의 알림을 공유하는 호스트 IP 주소를 식별합니다. 목록 맨 위의 쌍은 오탐일 가능성이 있으며, 따라서 튜닝이 필요한 영역을 나타내는 것일 수도 있습니다. 목록 맨 아래의 쌍은 표적 공격, 권한이 없는 리소스에 액세스하는 사용자, 네트워크에 속하지 않는 호스트인지의 여부에 대해 조사할 수 있습니다.

사전 정의 악성코드 워크플로

다음 표에서는 management center에 포함된 사전 정의 악성코드 워크플로에 대해 설명합니다. 모든 사전 정의 악성코드 워크플로에서는 악성코드 이벤트의 테이블 보기를 사용합니다.

표 ***2:*** 사전 정의 악성코드 워크플로

워크플로 이름	설명
악성코드 요약	이 워크플로는 네트워크 트래픽에서 또는 엔드포인트 기반 AMP for Endpoints Connector에 의해 탐지된 악성코드를 개별 위협을 기준으로 그룹화한 목록을 제공합니다.
악성코드 이벤트 요약	이 워크플로에서는 다양한 악성 코드 이벤트 유형 및 하위 유형을 신속하게 분석할 수 있습니다.
악성코드를 수신하는 호스트 수	이 워크플로는 악성코드를 수신한 호스트 IP 주소를 악성코드 파일의 관련 성향을 기준으로 그룹화한 목록을 제공합니다.
악성코드를 송신하는 호스트 수	이 워크플로는 악성코드를 전송한 호스트 IP 주소를 악성코드 파일의 관련 성향을 기준으로 그룹화한 목록을 제공합니다.
Applications Introducing Malware	이 워크플로는 파일을 수신한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.

사전 정의 파일 워크플로

다음 표에서는 management center에 포함된 사전 정의 파일 이벤트 워크플로에 대해 설명합니다. 모든 사전 정의 파일 이벤트 워크플로에서는 파일 이벤트의 테이블 보기를 사용합니다.

표 *3:* 사전 정의 파일 워크플로

워크플로 이름	설명
파일 요약	이 워크플로에서는 다양한 파일 이벤트 카테고리와 유형을 신속하게 분석할 수 있으며, 관련 악성코드 성향도 표시합니다.
파일을 수신하는 호스트 수	이 워크플로는 파일을 수신한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.
파일을 송신하는 호스트 수	이 워크플로는 파일을 전송한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.

사전 정의 캡처 파일 워크플로

다음 표에서는 management center에 포함된 사전 정의 캡처 파일 워크플로에 대해 설명합니다. 모든 사전 정의 캡처 파일 워크플로에서는 캡처 파일의 테이블 보기를 사용합니다.

표 *4:* 사전 정의 캡처 파일 워크플로

워크플로 이름	설명
캡처된 파일 요약	이 워크플로에서는 유형, 카테고리, 위협 점수를 기준으로 캡처 파일을 분석할 수 있습니다.
동적 분석 상태	이 워크플로에서는 캡처 파일이 동적 분석을 위해 제출되었는지 여부에 따라 그 카운트를 제공합니다.

사전 정의 연결 데이터 워크플로

다음 표에서는 management center에 포함된 사전 정의 연결 데이터 워크플로에 대해 설명합니다. 모든 사전 정의 연결 데이터 워크플로에서 연결 데이터의 테이블 보기를 사용합니다.

표 *5:* 사전 정의 연결 데이터 워크플로

워크플로 이름	설명
연결 이벤트	이 워크플로에서는 기본 연결 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트 테이블 보기로 드릴다운할 수 있습니다.
애플리케이션별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 탐지된 연결 수를 기준으로 가장 활동적인 10개의 애플리케이션을 그래프로 나타냅니다.
이니시에이터를 이용한 연결	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 호스트가 연결 트랜잭션을 시작한 연결의 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
포트별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 탐지된 연결 수를 기준으로 가장 활동적인 10개의 포트를 그래프로 나타냅니다.

워크플로 이름	설명
응답자별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 호스트 IP 주소가 연결 트랜잭션의 응답자인 연결의 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
시간에 따른 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 시간의 경과에 따른 총 연결 수를 그래프로 나타냅니다.
애플리케이션별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 전송된 킬로바이트 수를 기준으로 가장 활동적인 10개의 애플리케이션을 그래프로 나타냅니다. 애플리케이션 카운트는 애플리케이션 연결과 일치하는 각 탐지기를 반영합니다. 트래픽과 일치하는 것이 애플리케이션 프로토콜, 웹 애플리케이션, 클라이언트 탐지기, 내부 탐지기 중 무엇인지에 따라, 그리고 트래픽이 모바일 디바이스에서 발생했는지 암호화된 세션의 일부인지에 따라 같은 애플리케이션 세션이 목록에서 여러번 나타날 수도 있습니다. 클라이언트 플로우에 애플리케이션이 표시되며 특별한 클라이언트 탐지기가 존재하지 않는다면, 일반 클라이언트가 보고될 수 있습니다. 예를 들어 (YouTube 웹 애플리케이션 탐지기와 일치하기 때문에) **YouTube**로 보고되거나, (내부 YouTube 탐지기가 클라이언트 세션에서 일반적으로 표시되는 특성과 일치하기 때문에) **YouTube** 클라이언트로 보고된 YouTube 트래픽과 같은 세션이 표시될 수 있습니다. 네트워크의 연결 이벤트와 네트워크 맵에 있는 정보를 사용하여 특정 애플리케이션 연결에 대한 추가 정보를 확인합니다.
이니시에이터별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소로부터 전송된 총 킬로바이트 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
포트별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 전송된 킬로바이트 수를 기준으로 가장 활동적인 10개의 포트를 그래프로 나타냅니다.
응답자별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소가 수신한 총 킬로바이트 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
시간에 따른 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 시간의 경과에 따른 총 전송 킬로바이트 수를 그래프로 나타냅니다.
응답자별 고유 이니시에이터	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소에 연결한 고유 initiator 수를 기준으로 가장 활동적인 10개의 응답 호스트 IP 주소를 그래프로 나타냅니다.
이니시에이터별 고유 응답자	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소가 연결한 고유 responder 수를 기준으로 가장 활동적인 10개의 발신 호스트 IP 주소를 그래프로 나타냅니다.

사전 정의 보안 인텔리전스 워크플로

다음 표에서는 management center에 포함된 사전 정의 보안 인텔리전스 워크플로에 대해 설명합니다. 모든 사전 정의 보안 인텔리전스 워크플로에서는 보안 인텔리전스 이벤트의 테이블 보기를 사용합니다.

표 ***6:*** 사전 정의 보안 인텔리전스 워크플로

워크플로 이름	설명
보안 인텔리전스 이벤트	이 워크플로에서는 기본 보안 인텔리전스 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트 테이블 보기로 드릴다운할 수 있습니다.
보안 인텔리전스 요약	이 워크플로는 Security Intelligence Events(보안 인텔리전스 이벤트) 워크플로와 동일하지만 보안 인텔리전스 이벤트를 카테고리 및 카운트별로만 나열하는 Security Intelligence Summary(보안 인텔리전스 요약) 페이지로 시작합니다.
DNS 상세정보가 있는 보안 인텔리전스	이 워크플로는 Security Intelligence Events(보안 인텔리전스 이벤트) 워크플로와 동일하지만 Security Intelligence(보안 인텔리전스) 이벤트를 카테고리 및 DNS 관련 특성별로만 나열하는 Security Intelligence with DNS Details(DNS 상세정보가 있는 보안 인텔리전스) 페이지로 시작합니다.

사전 정의 호스트 워크플로

다음 표에서는 호스트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***7:*** 사전 정의 호스트 워크플로

워크플로 이름	설명
호스트	이 워크플로에서는 호스트의 테이블 보기에 이어 호스트 보기가 표시됩니다. 호스트 테이블 기반의 워크플로 보기에서는 어떤 호스트와 관련된 모든 IP 주소의 데이터를 편리하게 볼 수 있습니다.
운영 체제 요약	이 워크플로를 사용하여 네트워크에서 사용 중인 운영체제를 분석할 수 있습니다.

사전 정의 보안 침해 지표 워크플로

다음 표에서는 IOC 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 *8:* 사전 정의 보안 침해 지표 워크플로

워크플로 이름	설명
Host(호스트) 보안 침해 지표	이 워크플로는 IOC 데이터를 카운트 및 범주별로 그룹화한 요약 보기로 시작하며, 요약 데이터를 이벤트 유형별로 세분화하는 세부사항 보기를 제공합니다. **Analysis(**분석**) > Hosts(**호스트**)** 메뉴를 통해 이 워크플로에 액세스합니다.
호스트별 보안 침해 지표	이 워크플로를 사용하여 네트워크의 어떤 호스트가 공격받을 가능성이 가장 높은지 (IOC 데이터를 기반으로) 평가할 수 있습니다. **Analysis(**분석**) > Hosts(**호스트**)** 메뉴를 통해 이 워크플로에 액세스합니다.
사용자 보안 침해 지표	이 워크플로는 IOC 데이터를 카운트 및 범주별로 그룹화한 요약 보기로 시작하며, 요약 데이터를 이벤트 유형별로 세분화하는 세부사항 보기를 제공합니다. **Analysis(**분석**) > Users(**사용자**)** 메뉴를 통해 이 워크플로에 액세스합니다.
사용자별 보안 침해 지표	이 워크플로를 사용하여 네트워크의 어떤 사용자가 잠재적 침해에 연관될 가능성이 가장 높은지 (IOC 데이터를 기반으로) 평가합니다. **Analysis(**분석**) > Users(**사용자**)** 메뉴를 통해 이 워크플로에 액세스합니다.

사전 정의 애플리케이션 워크플로

다음 표에서는 애플리케이션 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 *9:* 사전 정의 애플리케이션 워크플로

워크플로 이름	설명
애플리케이션 비즈니스 관련성	이 워크플로를 사용하여 네트워크의 예상 비즈니스 타당성 레벨별로 실행 중인 애플리케이션을 분석함으로써 네트워크 리소스가 적절하게 사용되는지 모니터링할 수 있습니다.
애플리케이션 범주	이 워크플로를 사용하여 네트워크에서 카테고리(예: 이메일, 검색 엔진, 소셜 네트워킹)별로 실행 중인 애플리케이션을 분석함으로써 네트워크 리소스가 적절하게 사용되는지 모니터링할 수 있습니다.
애플리케이션 위험성	이 워크플로를 사용하여 네트워크에서 각 예상 보안 위험 레벨의 실행 중인 애플리케이션을 분석함으로써 사용자 활동의 잠재적 리스크를 추정하고 적절한 조치를 취할 수 있습니다.
애플리케이션 요약	이 워크플로를 사용하여 네트워크의 애플리케이션 및 해당 호스트에 대한 세부 정보를 얻어 호스트 애플리케이션 활동을 면밀하게 조사할 수 있습니다.
애플리케이션	이 워크플로를 사용하여 네트워크에서 실행 중인 애플리케이션을 분석함으로써 네트워크가 어떻게 사용되고 있는가를 개괄적으로 파악할 수 있습니다.

사전 정의 애플리케이션 상세정보 워크플로

다음 표에서는 애플리케이션 상세정보 및 클라이언트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***10:*** 사전 정의 애플리케이션 상세정보 워크플로

워크플로 이름	설명
애플리케이션 세부사항	이 워크플로를 사용하여 네트워크의 클라이언트 애플리케이션을 더 자세히 분석할 수 있습니다. 그런 다음 클라이언트 애플리케이션의 테이블 보기와 호스트 보기로 이어집니다.
클라이언트	이 워크플로에서는 클라이언트 애플리케이션의 테이블 보기에 이어 호스트 보기가 표시됩니다.

사전 정의 서버 워크플로

다음 표에서는 서버 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***11:*** 사전 정의 서버 워크플로

워크플로 이름	설명
카운트별 네트워크 애플리케이션	이 워크플로를 사용하여 네트워크에서 가장 자주 사용되는 애플리케이션을 분석할 수 있습니다.
히트별 네트워크 애플리케이션	이 워크플로를 사용하여 네트워크에서 가장 활동적인 애플리케이션을 분석할 수 있습니다.
서버 세부 정보	이 워크플로를 사용하여 탐지된 서버 애플리케이션 프로토콜의 벤더 및 버전을 더 자세히 분석할 수 있습니다.
서버	이 워크플로에서는 애플리케이션의 테이블 보기에 이어 호스트 보기가 표시됩니다.

사전 정의 호스트 속성 워크플로

다음 표에서는 호스트 속성 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***12:*** 사전 정의 호스트 속성 워크플로

워크플로 이름	설명
특성	이 워크플로를 사용하여 네트워크에 있는 호스트의 IP 주소 및 호스트의 상태를 모니터링할 수 있습니다.

사전 정의 검색 이벤트 워크플로

다음 표에서는 검색 및 ID 데이터를 확인하는 데 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***13:*** 사전 정의 검색 이벤트 워크플로

워크플로 이름	설명
검색 이벤트	이 워크플로에서는 검색 이벤트의 세부 목록을 테이블 보기 형태로 제공하고 이어서 호스트 보기를 표시합니다.

사전 정의 사용자 워크플로

다음 표에서는 사용자 검색 및 사용자 ID 데이터를 확인하는 데 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***14:*** 사전 정의 사용자 워크플로

워크플로 이름	설명
활성 세션	이 워크플로는 사용자 ID 소스가 수집한 활성 세션 목록을 제공합니다.
사용자	이 워크플로는 사용자 ID 소스가 수집한 사용자 정보 목록을 제공합니다.

사전 정의 취약성 워크플로

다음 표에서는 management center에 포함된 사전 정의 취약성 워크플로에 대해 설명합니다.

표 ***15:*** 사전 정의 취약성 워크플로

워크플로 이름	설명
취약성	이 워크플로를 이용하면 네트워크에서 탐지된 호스트에 적용되는 활성 취약성만 표시하는 테이블 보기 등을 이용해, 데이터베이스에 있는 취약성을 검토할 수 있습니다. 또한 제약 조건에 부합하는 모든 취약성에 대해 자세히 설명하는 취약성 세부사항 보기도 제공합니다.

사전 정의 서드파티 취약성 워크플로

다음 표에서는 management center에 포함된 사전 정의 서드파티 취약성 워크플로에 대해 설명합니다.

표 ***16:*** 사전 정의 서드파티 취약성 워크플로

워크플로 이름	설명
IP 주소별 취약성	이 워크플로를 사용하여 모니터링되는 네트워크의 호스트 IP 주소별로 탐지된 서드파티 취약성의 수를 신속하게 확인할 수 있습니다.
소스별 취약성	이 워크플로를 사용하여 서드파티 취약성 소스(예: QualysGuard Scanner)별로 탐지된 서드파티 취약성의 수를 신속하게 확인할 수 있습니다.

사전 정의 상관관계 및 허용 목록 워크플로

상관관계 데이터, 허용 목록 이벤트, 허용 목록 위반, 교정 상태 이벤트의 유형별로 사전 정의 워크플로가 있습니다.

표 ***17:*** 사전 정의 상관관계 워크플로

워크플로 이름	설명
상관관계 이벤트	이 워크플로는 상관관계 이벤트의 테이블 보기로 구성됩니다.
허용 이벤트 나열	이 워크플로는 허용 목록 이벤트의 테이블 보기로 구성됩니다.
호스트 위반 카운트	이 워크플로는 하나 이상의 허용 목록을 위반하는 모든 호스트 IP 주소를 나열하는 일련의 페이지로 구성됩니다.
허용 위반 목록	이 워크플로에는 모든 위반을 나열하는 허용 목록 위반의 테이블 보기가 포함되는데, 가장 최근에 탐지된 위반이 맨 위에 옵니다. 테이블의 각 행에는 탐지된 위반 사항이 하나씩 포함되어 있습니다.
상태	이 워크플로는 교정 상태의 테이블 보기로 구성됩니다. 여기에는 위반한 정책의 이름, 적용된 교정의 이름과 상태가 포함됩니다.

사전 정의 시스템 워크플로

Firepower System에서는 몇 가지 추가 워크플로를 제공하는데, 여기에는 감사 이벤트 및 상태 이벤트와 같은 시스템 이벤트 뿐만 아니라 규칙 업데이트 가져오기 및 활성 검사의 결과를 나열하는 워크플로도 포함됩니다.

표 ***18:*** 추가 사전 정의 워크플로

워크플로 이름	설명
감사 로그	이 워크플로는 감사 이벤트를 나열하는 감사 로그의 테이블 보기로 구성됩니다.

워크플로 이름	설명
상태 이벤트	이 워크플로에서는 상태 모니터링 정책에 의해 트리거되는 이벤트를 표시합니다.
규칙 업데이트 가져오기 로그	이 워크플로는 성공한 규칙 업데이트 가져오기 및 실패한 규칙 업데이트 가져오기에 대한 정보를 나열하는 테이블 보기로 구성됩니다.
스캔 결과	이 워크플로는 완료된 각 스캔을 나열하는 테이블 보기로 구성됩니다.

맞춤형 테이블 워크플로

맞춤형 테이블 기능을 사용하여 이벤트 유형 2가지 이상의 데이터를 사용하는 테이블을 생성할 수 있습니다. 이를테면 침입 이벤트 데이터를 검색 데이터와 연계하여 중요 시스템에 영향을 주는 이벤트의 단순 검색을 지원하는 테이블과 워크플로를 만들 때 유용한 기능입니다.

맞춤형 테이블을 생성하는 경우, 시스템은 테이블과 관련된 이벤트를 볼 수 있는 워크플로를 자동으로 생성합니다. 워크플로의 기능은 사용하는 테이블 유형에 따라 달라집니다. 예를 들어 침입 이벤트 테이블을 기반으로 하는 맞춤형 테이블 워크플로는 항상 패킷 보기로 끝납니다. 그러나 검색 이벤트를 기반으로 하는 맞춤형 테이블 워크플로는 호스트 보기로 끝납니다.

사전 정의 이벤트 테이블 기반의 워크플로와 달리 맞춤형 테이블 기반의 워크플로는 다른 워크플로 유형에 대한 링크가 없습니다.

워크플로 사용

프로시저

단계 **1** 워크플로 선택, 13 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택합니다.

단계 **2** 현재 워크플로 내에서 이동:

- 선택한 이벤트 데이터 유형에서 사용 가능한 행을 모두 보려면 테이블 보기 페이지를 사용하십시오(테이블 보기 페이지 사용, 20 페이지 참조).
- 선택한 이벤트 데이터 유형에서 사용 가능한 행의 하위 집합을 보려면 드릴다운 페이지를 사용하십시오(드릴다운 페이지 사용, 19 페이지 참조).
- 워크플로우의 다음 페이지에 해당 행을 표시하려면 **Down-Arrow(**아래쪽 화살표**)** (▼)을 클릭합니다.
- 여러 페이지가 있는 워크플로의 페이지 사이를 이동하려면 각 페이지 하단에 있는 툴을 사용하십시오(워크플로 페이지 이동 툴, 17 페이지 참조).
- 다른 유형의 워크플로에 적용된 같은 제약을 보려는 경우, **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.

단계 **3** 현재 워크플로의 표시 화면을 수정합니다.

- 페이지에서 하나 이상의 열 옆에 있는 체크 박스를 선택해 영향받는 열을 표시하고, 페이지 하단의 버튼 중 하나(예: **View(**보기**)**)를 클릭해 선택한 열 전체에 작업을 수행합니다.
- 열 상단에 있는 체크 박스를 선택해 페이지의 모든 열을 선택하고, 페이지 하단의 버튼 중 하나(예: **View(**보기**)**)를 클릭해 페이지의 열 전체에 작업을 수행합니다.
- 표시하지 않을 컬럼 헤드의 **Close(**닫기**)** (✕)을 클릭하여 화면에 표시되는 열을 제한합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

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

- 선택한 필드의 선택된 값을 이용해 데이터 보기를 제한합니다. 자세한 내용은 이벤트 보기 제약 조건, 35 페이지 및 복합 이벤트 보기 제약, 37 페이지 섹션을 참고하십시오.
- 이벤트 보기의 시간 제약을 변경합니다. 페이지의 오른쪽 위에 있는 날짜 범위는 워크플로에 포함할 이벤트의 시간 범위를 설정합니다. 자세한 내용은 이벤트 시간 제약 조건, 29 페이지 섹션을 참조하십시오.

  참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

- 열을 기준으로 데이터를 정렬하려면 열의 이름을 클릭합니다. 정렬 순서를 반대로 하려면 열 이름을 다시 클릭합니다. 방향 아이콘은 데이터가 정렬되는 열과 정렬이 오름차순인지 내림차순인지를 표시합니다.
- 워크플로 페이지 링크를 클릭하여 활성 제약 조건을 사용해 해당 페이지를 표시합니다. 사전 정의된 워크플로 테이블 보기 및 드릴다운 페이지의 왼쪽 위에서 이벤트 위, 워크플로 이름 아래에 워크플로 페이지 링크가 나타납니다.

단계 **4** 현재 워크플로 내의 추가 데이터를 확인합니다.

- 파일의 경로 맵을 새 창에서 보려면, 파일 이름과 SHA-256 해시 값 열에서 네트워크 파일 경로를 클릭합니다. 아이콘은 파일 상태에 따라 달라집니다(파일 경로 아이콘, 17 페이지 참조).
- IP 주소와 관련된 호스트 프로파일의 팝업 윈도우를 표시하려는 경우, 아무 IP 주소 열의 호스트 프로파일을 클릭합니다. 아이콘은 파일 상태에 따라 달라집니다(호스트 프로파일 아이콘, 18 페이지 참조).
- 파일의 최고 위협 점수에 대한 Dynamic Analysis Summary(동적 분석 요약) 보고서를 보려는 경우, 위협 점수 열에 나타나는 위협 점수를 클릭합니다. 아이콘은 파일의 최고 위협 점수에 따라 달라집니다(위협 점수 아이콘, 18 페이지 참조).

- 사용자 프로파일 정보를 보려는 경우에는 아무 사용자 ID 열의 사용자 또는 보안 침해 지표와 관련된 사용자의 경우에는 빨간색 사용자를 클릭합니다. 해당 사용자가 데이터베이스에 존재할 수 없다면(즉 AMP for Endpoints Connector 사용자려면) 사용자 아이콘은 흐리게 표시됩니다.
- 서드파티 취약성의 취약성 상세정보를 보려는 경우네는 아무 서드파티 취약성 ID 열의 취약성을 클릭합니다.
- 집계된 데이터 포인트를 볼 때 마우스 포인터를 플래그 위에 올리면 국가 이름을 볼 수 있습니다.
- 개별 데이터 포인트를 볼 때 플래그를 클릭하면 지리위치, 22 페이지에서 설명하는 추가 지리위치 상세정보를 볼 수 있습니다.

단계 **5** 다른 워크플로로 이동합니다.

다른 워크플로를 이용하는 같은 이벤트 유형을 보려는 경우, 워크플로 제목 옆에 있는 **(switch workflow)**을 클릭하고 사용할 워크플로를 선택합니다. 스캔 결과에 대해 다른 워크플로를 사용할 수는 없습니다.

사용자 역할별 워크플로 액세스

워크플로에 대한 액세스는 사용자의 역할에 따라 결정됩니다. 자세한 내용은 아래 표를 참고하십시오.

사용자 역할	액세스 가능한 워크플로
관리자	어떤 워크플로에도 액세스할 수 있으며, 감사 로그, 검사 결과, 규칙 업데이트 가져오기 로그에 액세스할 수 있는 유일한 사용자입니다.
유지 보수 사용자	상태 이벤트에 액세스할 수 있습니다.
Security Analyst 및 Security Analyst(읽기 전용)	침입, 악성코드, 파일, 연결, 검색, 취약성, 상관관계, 상태 워크플로에 액세스할 수 있습니다.

워크플로 선택

시스템에서는 다음 테이블에 나열된 데이터 유형에 대해 사전 정의된 워크플로우를 제공합니다.

표 ***19:*** 워크플로를 사용하는 기능

기능	메뉴 경로	옵션
연결 이벤트	분석 > 연결	이벤트
보안 인텔리전스 이벤트	분석 > 연결	보안 인텔리전스 이벤트

기능	메뉴 경로	옵션
상관관계 이벤트	분석 > 상관관계	상관관계 이벤트 허용 이벤트 나열 허용 위반 목록 상태
악성코드 이벤트	분석 > 파일	악성코드 이벤트
파일 이벤트	분석 > 파일	파일 이벤트
캡처된 파일	분석 > 파일	캡처된 파일
호스트 이벤트	분석 > 호스트	네트워크 맵 호스트 보안 침해 지표 애플리케이션 애플리케이션 세부사항 서버 호스트 속성 검색 이벤트
침입 이벤트	분석 > 침입	이벤트 검사된 이벤트
사용자 이벤트	분석 > 사용자	활성 세션 사용자의 활동 사용자 보안 침해 지표
취약성 이벤트	분석 > 호스트	취약성 서드파티 취약성
스캔 결과	정책 > 작업 > 스캐너	—
상태 이벤트	System(시스템) > Health(상태) > Events(이벤트)	—
감사 이벤트	시스템 > 모니터링	감사

기능	메뉴 경로	옵션
규칙 업데이트 가져오기 로그	시스템 > 업데이트 7.2.0~7.2.5 버전: 시스템 > 업데이트 7.4.1 이상 버전: 시스템 > 콘텐츠 업데이트	규칙 업데이트

위 표에 있는 데이터 유형을 표시할 경우 그 데이터의 기본 워크플로 중 첫 페이지에 이벤트가 나타납니다. 이벤트 보기 설정을 구성하여 다른 기본 워크플로를 지정할 수 있습니다. 워크플로 액세스는 사용자 역할에 따라 달라집니다.

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

관련 항목

이벤트 보기 구성

워크플로 페이지

각 워크플로 유형의 데이터는 저마다 다르지만, 모든 워크플로가 공유하는 공통 기능이 있습니다. 워크플로는 페이지의 여러 유형을 포함할 수 있습니다. 워크플로 페이지에서 수행할 수 있는 작업은 페이지 유형에 따라 달라집니다.

워크플로의 드릴다운 및 테이블 보기 페이지를 통해 신속하게 데이터 보기의 범위를 한정하여 분석에 중요한 이벤트에 초점을 맞출 수 있습니다. 테이블 보기 페이지 및 드릴다운 페이지는 표시할 이벤트 집합을 제한하거나 워크플로를 이동하는 데 사용할 수 있는 여러 기능을 지원합니다. 워크플로의 드릴다운 페이지나 테이블 보기에서 데이터를 볼 때, 사용 가능한 아무 열을 기준으로 데이터를 오름차순이나 내림차순으로 정렬할 수 있습니다. 데이터베이스가 단일 워크플로 페이지에 표시할 수 있는 것보다 많은 이벤트를 포함할 경우, 페이지 맨 아래의 링크를 클릭하여 추가 이벤트를 표시할 수 있습니다. 이 링크 중 하나를 클릭할 때 동일한 이벤트가 두 번 표시되지 않도록 시장 창이 자동으로 일시 중지합니다. 언제라도 타임 윈도우의 일시 중지를 취소할 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.

테이블 보기

페이지가 기본적으로 활성화되는 경우, 테이블 보기에는 워크플로가 기반으로 하는 데이터베이스의 각 필드에 대한 열이 포함됩니다.

최상의 성능을 위해 필요한 열만 표시합니다. 열이 많이 표시될수록 데이터를 표시하는 데 더 많은 리소스가 필요합니다.

테이블 보기에서 어떤 열을 비활성화할 경우 그 열을 비활성화함으로써 둘 이상의 동일한 행이 생성되고 6개 미만의 열이 표시된다면(Count 열 제외) Firepower System에서는 이벤트 보기에 Count 열을 추가합니다.

테이블 보기 페이지에서 어떤 값을 클릭하면 그 값으로 제한할 수 있습니다.

맞춤형 워크플로를 생성할 때 **Add Table View(**테이블 보기 추가**)**를 클릭하여 여기에 테이블 보기를 추가합니다.

드릴다운 페이지

일반적으로 드릴다운 페이지는 보기 페이지로 이동하기 전에 조사 범위를 몇몇 이벤트로 한정하는 데 사용하는 중간 단계의 페이지입니다. 드릴다운 페이지는 데이터베이스에서 제공하는 열의 일부를 포함합니다.

예를 들어 검색 이벤트의 드릴다운 페이지에 IP Address, MAC Address, Time 열만 포함될 수 있습니다. 한편 침입 이벤트의 드릴다운 페이지는 Priority, Impact Flag, Inline Result, Message 열이 포함될 수 있습니다.

드릴다운 페이지에서는 표시하는 이벤트의 범위를 좁히고 워크플로에서 다음으로 진행할 수 있습니다. 이를테면 드릴다운 페이지에서 어떤 값을 클릭할 경우 그 값을 기준으로 제한하고 워크플로의 다음 페이지로 이동함으로써, 선택한 값과 매칭하는 이벤트에 더 초점을 맞출 수 있습니다. 드릴다운 페이지에서 어떤 값을 클릭하더라도 그 값이 있는 열이 비활성화되지 않습니다. 진행할 페이지가 테이블 보기인 경우도 마찬가지입니다. 사전 정의 워크플로의 드릴다운 페이지에는 항상 Count 열이 있습니다. 맞춤형 워크플로를 생성할 때 **Add Page(**페이지 추가**)**를 클릭하여 드릴다운 페이지를 추가합니다.

Graphs(그래프**)**

연결 데이터 기반의 워크플로는 연결 그래프라고도 하는 그래프 페이지를 포함할 수 있습니다.

예를 들어 연결 그래프에서 시간의 경과에 따른 탐지된 연결 수를 나타내는 선 그래프가 표시될 수 있습니다. 일반적으로 연결 그래프는 드릴다운 페이지처럼 조사 범위를 한정하는 데 사용하는 중간 단계의 페이지입니다.

최종 페이지

워크플로의 최종 페이지는 워크플로의 기반이 되는 이벤트의 유형에 따라 달라집니다.

- 호스트 보기는 애플리케이션, 애플리케이션 상세정보, 검색 이벤트, 호스트, 보안 침해 지표(IOC), 서버, 허용 목록 위반, 호스트 속성 또는 서드파티 취약성을 기반으로 하는 워크플로의 최종 페이지입니다. 이 페이지에서 호스트 프로파일을 보면서 다중 주소를 갖는 호스트의 모든 IP 주소에 대한 데이터를 편리하게 볼 수 있습니다.
- 사용자 상세정보 보기는 사용자, 사용자 활동, 사용자 보안 침해 지표를 기반으로 하는 워크플로의 최종 페이지입니다.
- 취약성 상세정보 보기는 Cisco 취약성을 기반으로 하는 워크플로의 최종 페이지입니다.
- 패킷 보기는 침입 이벤트를 기반으로 하는 워크플로의 최종 페이지입니다.

다른 종류의 이벤트(예: 감사 로그 이벤트, 악성코드 이벤트)를 기반으로 하는 워크플로는 최종 페이지가 없습니다.

워크플로의 마지막 페이지에서 세부사항 섹션을 확장하여 초점 대상인 집합의 각 개체에 대해 워크플로의 진행에 따른 구체적인 정보를 볼 수 있습니다. 웹 인터페이스에서는 워크플로의 최종 페이지에 제약 조건을 나열하지 않지만, 이미 설정된 제약 조건이 유지되어 데이터 집합에 적용됩니다.

워크플로 페이지 탐색 툴

워크플로 페이지는 각 페이지를 손쉽게 탐색하고 이벤트 분석 동안 표시할 정보를 선택하는 데 도움이 되는 시각적 단서를 제공합니다.

워크플로 페이지 이동 툴

워크플로에 여러 페이지의 데이터가 있는 경우, 각 페이지 하단에 워크플로의 페이지 숫자가 표시되며, 아래 표에 나열된 툴을 이용해 페이지를 이동할 수 있습니다.

표 ***20:*** 워크플로 페이지 이동 툴

페이지 이동 툴	조치
페이지 번호 (다른 페이지를 보려는 경우 확인할 페이지 번호를 입력하고 Enter를 누릅니다.)	다른 페이지 보기
>	다음 페이지 보기
<	이전 페이지 보기
>|	마지막 페이지로 바로 이동
|<	첫 페이지로 바로 이동

파일 경로 아이콘

워크플로 페이지에서 파일의 경로 맵을 새 창에서 볼 수 있다면, 네트워크 경로 아이콘이 표시됩니다. 이 아이콘은 파일 상태에 따라 달라집니다.

표 ***21:*** 파일 경로 아이콘

파일 경로 아이콘	파일 상태
정상	정상
악성코드	악성코드
맞춤형 탐지	맞춤형 탐지
알 수 없음	알 수 없음
사용 불가능	사용 불가능

호스트 프로파일 아이콘

워크플로 페이지에서 IP 주소와 연결된 호스트 프로파일을 팝업 윈도우에서 볼 수 있다면, 호스트 프로파일 아이콘이 표시됩니다. 호스트 프로파일 아이콘이 흐리게 표시될 경우 호스트가 네트워크 맵에 포함될 수 없으므로(예: 0.0.0.0) 호스트 프로파일을 볼 수 없습니다. 이 아이콘은 호스트의 상태에 따라 다르게 표시됩니다.

표 ***22:*** 호스트 프로파일 아이콘

호스트 프로파일 아이콘	**Host Status(**호스트 상태**)**
	호스트가 침해 가능성 있음으로 태그되지 않았습니다.
	호스트가 트리거된 보안 침해 지표(IOC) 규칙에 의해 침해 가능성 있음으로 태그되었습니다.
	차단 목록에 추가됨(보안 인텔리전스 데이터를 바탕으로 트래픽 필터링을 수행하는 경우에만 표시됩니다.)
	차단 목록에 추가됨, 모니터링하도록 설정(보안 인텔리전스 데이터를 바탕으로 트래픽 필터링을 수행하는 경우에만 표시됩니다.)

위협 점수 아이콘

워크플로 페이지를 제공 하는 경우 가장 높은 위협 점수에 대 한 동적 분석 요약 보고서를 볼 수 있는 기회와 연결 파일을 위협 점수 아이콘 위에 표시 됩니다. 아이콘은 파일의 최고 위협 점수에 따라 다릅니다.

표 ***23:*** 위협 점수 아이콘

위협 점수 아이콘	위협 점수 레벨
낮음	낮음
보통	보통
높음	높음
매우 높음	매우 높음

사용자 아이콘

워크플로 페이지에서 사용자 이름과 연결된 사용자 ID를 팝업 윈도우에서 볼 수 있다면, 사용자 아이콘이 표시됩니다.

표 *24:* 사용자 아이콘

사용자 아이콘	사용자 상태
사용자	사용자가 어떠한 보안 침해 지표와도 연결되어 있지 않습니다.
빨간색 사용자	사용자가 하나 이상의 보안 침해 지표와 연결되어 있습니다.

워크플로 툴바

워크플로의 각 페이지에는 관련 기능에 빠르게 액세스할 수 있는 툴바가 있습니다. 다음 표에서는 툴바의 각 링크에 대해 설명합니다.

표 *25:* 워크플로 툴바 링크

기능	설명
이 페이지를 즐겨찾기에 추가	현재 페이지에 북마크를 지정하여 나중에 다시 돌아올 수 있게 합니다. 북마크는 현재 보고 있는 페이지에 적용된 제약 조건을 캡처하므로 나중에 (데이터가 그대로 있을 경우) 동일한 데이터로 돌아올 수 있습니다.
보고서 디자이너	현재 제약 조건이 적용된 워크플로를 선택 기준으로 하는 보고서 디자인 도구를 엽니다.
대시보드	현재 워크플로와 관련된 대시보드를 엽니다. 예를 들어 Connection Events(연결 이벤트) 워크플로는 Connection Summary(연결 요약) 대시보드와 연결됩니다.
즐겨찾기 보기	선택 가능한 저장된 즐겨찾기의 목록을 표시합니다.
검색	워크플로의 데이터에 대한 고급 검색을 수행할 수 있는 Search(검색) 페이지를 표시합니다. 아래쪽 화살표 아이콘을 클릭하여 저장된 검색을 선택하고 사용할 수도 있습니다.

관련 항목

이벤트 보기에서 보고서 템플릿 생성
대시보드 정보
이벤트 검색
북마크, 39 페이지
즐겨찾기 생성, 40 페이지
즐겨찾기 보기, 40 페이지

드릴다운 페이지 사용

프로시저

단계 **1** 워크플로를 사용하는 기능에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 모든 워크플로에는 다음 옵션이 있습니다.

- 특정 값으로 제한하여 다음 워크플로 페이지로 드릴다운하려면 행 내의 값을 클릭합니다. 이 방법은 드릴다운 페이지에만 적용됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한될 뿐이고 다음 페이지로 드릴다운되지 않습니다.
- 일부 이벤트로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 이벤트의 옆에 있는 확인란을 선택하고 **View(**보기**)**를 클릭합니다.
- 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All(**모두 보기**)**을 클릭합니다.

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

테이블 보기 페이지 사용

테이블 보기 페이지는 드릴다운, 호스트 보기, 패킷 보기 또는 취약성 세부사항 페이지에 없는 기능을 제공합니다. 이러한 기능은 아래 설명대로 사용하십시오.

프로시저

단계 **1** 워크플로 선택, 13 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 워크플로 이름 아래에 표시된 워크플로 경로에서 테이블 보기를 선택합니다.

단계 **3** 이벤트 데이터가 원격으로 저장된 경우, 로컬 데이터를 표시할지 아니면 원격 데이터를 표시할지를 선택하는 옵션이 나타날 수 있습니다.

Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Secure Firewall Management Center에서 작업, 21 페이지의 내용을 참조하십시오.

단계 **4** 필요에 따라 아래 나열된 기능을 사용하여 테이블 보기를 정렬하고 내부를 이동합니다.

- 비활성화된 열의 목록을 표시하려면 Search Constraints(검색 제약 조건) **Expand Arrow(**확장 화살표**)**( )를 클릭합니다.
- 비활성화된 열의 목록을 숨기려면 Search Constraints(검색 제약 조건) **Collapse Arrow(**축소 화살표**)**( )를 클릭합니다.
- 비활성화된 열을 이벤트 보기에 다시 추가하려면 Search Constraints(검색 제약 조건) **Expand Arrow(**확장 화살표**)**( )를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 열을 표시하거나 숨기려면(비활성화하려면) 아무 열 이름 옆에 있는 **Clear(**지우기**)** (✕)를 클릭합니다. 표시되는 팝업 윈도우에서 적절한 체크 박스를 선택하거나 선택 취소해 표시할 열을 나타낸 다음, **Apply(**적용**)**를 클릭합니다.

Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Secure Firewall Management Center에서 작업

디바이스가 Security Analytics and Logging(보안 애널리틱스)을(를) 사용하여 Secure Network Analytics 어플라이언스에 연결 이벤트를 전송하는 경우, management center의 이벤트 뷰어 및 상황 탐색기에서 원격으로 저장된 이벤트를 확인하고 작업을 수행하고 보고서를 생성할 때 해당 이벤트를 포함할 수 있습니다. management center의 이벤트에서 교차 실행하여 Secure Network Analytics 어플라이언스의 관련 데이터를 볼 수도 있습니다.

기본적으로 시스템은 사용자가 지정한 시간 범위에 따라 적절한 데이터 소스를 자동으로 선택합니다. 데이터 소스를 재정의하려는 경우 이 절차를 사용합니다.

중요 데이터 소스를 변경하는 경우 로그아웃한 후에도 변경 사항이 있을 때까지 보고서를 포함하여 이벤트 데이터 소스를 사용하는 모든 관련 분석 기능에서 선택 사항이 유지됩니다. 다른 management center 사용자에게는 선택 항목이 적용되지 않습니다.

선택한 데이터 소스는 우선순위가 낮은 연결 이벤트에만 사용됩니다. 기타 모든 이벤트 유형(침입, 파일 및 악성 코드 이벤트, 해당 이벤트와 연결된 연결 이벤트, 보안 인텔리전스 이벤트)은 데이터 소스에 관계 없이 표시됩니다.

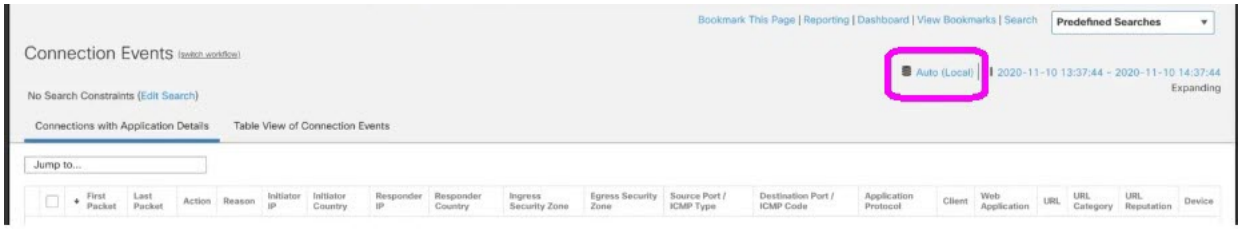
시작하기 전에

마법사를 사용하여 연결 이벤트를 Security Analytics and Logging(보안 애널리틱스)에 보냈습니다.

프로시저

단계 **1** management center 웹 인터페이스에서 **Analysis(**분석**) > Connections(**연결**) > Events(**이벤트**)**와 같은 연결 이벤트 데이터를 표시하는 페이지로 이동합니다.

단계 **2** 여기에 표시된 데이터 소스를 클릭하고 옵션을 선택합니다.



주의 **Local(**로컬**)**을 선택하면 선택한 전체 시간 범위에 대해 로컬 데이터를 사용할 수 없는 경우에도 management center에서 사용 가능한 데이터만 표시됩니다. 이러한 상황이 발생했다는 알림이 표시되지 않습니다.

단계 **3** (선택 사항) Secure Network Analytics 어플라이언스에서 관련 데이터를 직접 보려면 IP 주소 또는 도메인과 같은 값을 마우스 오른쪽 버튼으로 클릭(통합 이벤트 뷰어에서 클릭)하고 교차 실행 옵션을 선택합니다.

지리위치

지리위치 데이터베이스(GeoDB)를 활용하여 국가 및 대륙을 기준으로 트래픽을 보고 필터링할 수 있습니다. 한 국가에서 다른 국가로 이동하는 모바일 디바이스 및 다른 탐지된 호스트의 경우, 시스템은 특정 국가 대신 대륙을 보고하기도 합니다.

시스템은 IP 주소를 국가/대륙에 매핑하는 초기 GeoDB 국가 코드 패키지와 함께 제공되므로 정보를 항상 사용할 수 있습니다. GeoDB를 업데이트하면 시스템은 상황 데이터가 포함된 IP 패키지도 다운로드합니다. 여기에는 다음이 포함될 수 있습니다.

- 지역(주/도 또는 기타 국가 하위 지역), 도시 및 우편번호
- 위도/경도, 표준 시간대 및 클릭 가능한 맵
- ASN(Autonomous System Number) 및 ASN에 대한 추가 정보
- ISP(Internet Service Provider), 연결 유형 및 프록시 유형
- 홈/비즈니스, 조직 및 도메인 이름 정보

이 정보를 보려면 이벤트, 자산 프로파일, Context Explorer, 대시보드 및 기타 분석 툴에 표시되는 작은 국가 플래그 아이콘 및 ISO 국가 코드를 클릭합니다. Connection Summary(연결 요약) 대시보드 등에서는 종합 지리위치 정보에 대한 상세정보를 볼 수 없습니다.

참고 GeoDB에 주기적인 업데이트를 생성합니다. 정확한 지리적 위치 정보를 얻으려면 GeoDB를 정기적으로 업데이트해야 합니다. GeoDB(지리위치 데이터베이스) 업데이트의 내용을 참조하십시오.

관련 항목

네트워크 조건
지리위치
상관관계 정책 및 규칙 소개
트래픽 프로파일 조건
GeoDB(지리위치 데이터베이스) 업데이트

연결 이벤트 그래프

표 드릴다운 페이지와 이벤트의 최종 테이블 보기를 사용하는 워크플로 외에도, 시스템은 5분 간격으로 집계한 데이터를 이용해 특정 연결 데이터를 그래픽으로 표시할 수 있습니다. 데이터를 집계하는 데 사용한 정보, 즉 소스 및 목적지 IP 주소(및 해당 호스트와 연결된 사용자), 대상 포트, 전송 프로토콜, 애플리케이션 프로토콜만 그래프로 표시할 수 있습니다.

팁 Security Intelligence(보안 인텔리전스) 이벤트를 관련된 연결 이벤트와 별도로 그래프로 표시할 수는 없습니다. Security Intelligence(보안 인텔리전스) 필터링 활동에 대한 그래픽 개요를 보려면 대시보드와 Context Explorer(맥락 탐색기)를 사용하십시오.

연결 그래프는 세 가지 유형이 있습니다.

- 원도표는 불연속 카테고리로 그룹화한 단일 데이터 집합의 데이터를 표시합니다.
- 막대 그래프는 불연속 카테고리로 그룹화한 하나 이상의 데이터 집합의 데이터를 표시합니다.
- 선 그래프는 표준 또는 속도(변경 속도) 보기 중 하나를 사용하여, 하나 이상의 데이터 집합에서 얻은 데이터의 시간에 따른 변화를 표시합니다.

참고 시스템은 트래픽 프로파일을 선 그래프로 표시하며, 이 그래프는 몇 가지 제한 사항은 있지만 다른 연결 그래프와 같은 방식으로 조작할 수 있습니다. 트래픽 프로파일을 보려면 관리자 액세스 권한이 있어야 합니다.

워크플로 테이블처럼, 워크플로 그래프도 분석에 집중할 수 있도록 드릴다운하고 제한할 수 있습니다.

막대 그래프와 선 그래프는 모두 여러 데이터 집합을 표시할 수 있습니다. 즉, 각 x축 데이터 포인트의 y축에 여러 값을 표시할 수 있습니다. 예를 들어 고유한 이니시에이터 및 응답자의 총 수를 표시할 수 있습니다. 원도표는 데이터 집합을 하나만 표시할 수 있습니다.

x축, y축 또는 두 축을 모두 변경하여 연결 그래프에 다른 데이터와 데이터 집합을 표시할 수 있습니다. 원도표의 경우, x축을 변경하면 독립 변수가 변경되고 y축을 변경하면 종속 변수가 변경됩니다.

관련 항목

연결 요약(그래프에 대한 집계된 데이터)

연결 이벤트 그래프 사용

management center에서는 연결 이벤트 그래프를 보고, 찾는 정보에 맞게 그래프를 조작할 수 있습니다.

연결 그래프에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 연결 이벤트의 테이블 보기에서 종료되는 사전 정의된 워크플로를 사용할 수 있습니다. 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**)** > **Connections(**연결**)** > **Events(**이벤트**)**을(를) 선택합니다.

참고 그래프 대신 연결 이벤트 테이블이 표시되거나 다른 그래프를 보려는 경우, 워크플로 제목별로 **(switch workflow)**을 클릭하고 그래프를 포함하는 사전 정의된 워크플로 또는 맞춤형 워크플로를 선택합니다. 미리 정의된 연결 이벤트 워크플로(연결 그래프 포함)는 연결의 테이블 보기에서 종료됩니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- Time Range(시간 범위) - 시간 범위를 조정합니다. 그래프에 아무것도 표시되지 않는 경우에 유용합니다(타임 윈도우 변경, 32 페이지 참조).
- Field Names(필드 이름) - 그래프로 표시할 수 있는 데이터에 관한 자세한 정보는 연결 및 보안 관련 연결 이벤트 필드 섹션을 참조하십시오.
- Host Profile(호스트 프로파일) - IP 주소에 대한 호스트 프로파일을 보려면, 연결 데이터를 이니시에이터 또는 응답자별로 표시하는 그래프에서 막대 그래프의 막대나 원도표의 쐐기를 클릭하고 **View Host Profile(**호스트 프로파일 보기**)**을 선택합니다.
- User Profile(사용자 프로파일) - 사용자 프로파일 정보를 보려면, 연결 데이터를 이니시에이터 사용자별로 표시하는 그래프에서 막대 그래프의 막대나 원도표의 쐐기를 클릭하고 **View User Profile(**사용자 프로파일 보기**)**을 선택합니다.
- Other Information(기타 정보) - 그래프로 표시한 데이터에 관해 자세히 알고 싶다면, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기에 마우스 포인터를 올립니다.
- Constrain(제한) - 워크플로우를 다음 페이지로 진행하지 않고 아무 X축(독립 변수) 기준을 이용하여 연결 그래프를 제한하려는 경우, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기를 클릭하고 **View by...(**보기 기준**)** 옵션을 선택합니다.
- Data Selection(데이터 선택) - 그래프에 표시되는 데이터를 변경하려면 **X-Axis(X**축**)** 또는 **Y-Axis(Y**축**)**를 클릭하고 그래프로 표시한 새 데이터를 선택합니다. X축을 **Time(**시간**)**으로 변경하거나 시간에서 다른 항목으로 변경하면 그래프 유형도 변경됩니다. Y축을 변경하면 표시되는 데이터 집합도 영향을 받습니다.
- Datasets(데이터 집합) - 그래프의 데이터 집합을 변경하는 경우, **Datasets(**데이터 집합**)**를 클릭하고 새 데이터 집합을 선택합니다.
- Detach(분리) - 기본 시간 범위에 영향을 주지 않고 추가 분석을 수행할 수 있도록 연결 그래프를 분리하려면 **Detach(**분리**)**를 클릭합니다.

  팁 분리된 그래프에서 **New Window(**새 창**)**를 클릭하여 복사본을 만듭니다. 그러면 각각의 분리된 그래프에 서로 다른 분석을 수행할 수 있습니다. 트래픽 프로파일은 분리된 그래프라는 점을 유의하십시오.

- Drill Down(드릴다운) - 워크플로의 다음 페이지로 드릴다운하려면, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기를 클릭하고 **Drill-down(**드릴다운**)**을 선택합니다. 선 그래프의 특정 지점을 클릭하면 이 클릭한 지점을 중심으로 다음 페이지의 시간 범위가 10분 간격으로 제한됩니다. 막대 그래프의 막대를 클릭하거나 원도표의 쐐기 모양을 클릭하면 막대 또는 쐐기 모양에 따라 표시된 기준에 의해 다음 페이지가 제한됩니다.
- Export(내보내기) - 그래프에 대한 연결 데이터를 CSV(쉼표로 구분된 값) 파일로 내보내려면 **Export Data(**데이터 내보내기**)**를 클릭합니다. 그런 다음 **Download CSV File(CSV** 파일 다운로드**)**을 클릭하고 파일을 저장합니다.
- Graph Type(그래프 유형): 선 - 표준 또는 속도(변경 속도) 그래프로 전환하려면 **Velocity(**속도**)**를 클릭하고 **Standard(**표준**)** 또는 **Velocity(**속도**)**를 선택합니다.
- Graph Type(그래프 유형): 막대 및 원 - 막대 그래프 또는 원도표로 전환하려면 **Switch to Bar(**막대 그래프로 전환**)** 또는 **Switch to Pie(**원도표로 전환**)**를 클릭합니다. 원도표에는 여러 데이터 집합을 표시할 수 없으며, 따라서 여러 데이터 집합이 있는 막대 그래프에서 원도표로 전환하면 원도표에는 자동으로 선택되는 데이터 집합 하나만 표시됩니다. 표시할 데이터세트를 선택할 경우, management center은(는) 이니시에이터 및 응답자 통계보다 전체 통계를 우선시하고, 응답자 통계보다는 이니시에이터 통계를 우선시합니다.
- 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.
- Recenter(중앙으로 지정) - 시간 범위를 변경하지 않고 특정 시간 지점을 선 그래프의 중앙으로 지정하려면, 해당 지점을 클릭하고 **Recenter(**중앙으로 지정**)**를 선택합니다.
- Zoom(확대/축소) - 확대 또는 축소하지 않고 특정 시간 지점을 선 그래프의 중앙으로 지정하려면, 해당 지점을 클릭하고 **Zoom(**확대/축소**)**을 선택한 다음 새 기간을 선택합니다.

참고 제한, 중앙으로 지정, 확대/축소 작업은 management center의 기본 시간 범위를 변경합니다. 단 분리된 그래프를 이용해 작업하는 경우는 예외입니다.

예

예**:** 연결 그래프 제한

시간 추이에 따른 연결 그래프를 고려해 보십시오. 포트에 따라 그래프의 포인트를 제한할 경우, 탐지된 연결 이벤트 수를 기준으로 가장 활성화된 포트 10개가 제시되지만, 사용자가 클릭한 포인트를 중심으로 한 10분 간격으로 제한된 막대 그래프가 표시됩니다.

막대 중 하나를 클릭하고 **View by Initiator IP(**이니시에이터 **IP**별로 보기**)**를 선택하여 그래프를 추가로 제한할 경우, 이전과 동일한 10분 간격뿐만 아니라 클릭한 막대에 따라 표시되는 포트를 기준으로 제한된 새로운 막대 그래프가 표시됩니다.

예**:** 원도표의 **X**축과 **Y**축 변경

포트당 킬로바이트 단위로 그래프를 작성하는 원도표를 고려해보십시오. 이 경우 x축은 **Responder Port**이고 y축은 **KBytes**입니다. 이러한 원도표는 특정 간격 동안 모니터링되는 네트워크를 통해 전송된 데이터의 총 킬로바이트를 나타냅니다. 원의 쐐기 모양은 각 포트에서 탐지된 데이터의 비율을 나타냅니다.

- **Application Protocol(**애플리케이션 프로토콜**)**에 대한 차트의 x축을 변경할 경우 원도표에는 전송된 총 킬로바이트가 계속 표시되지만, 원형의 쐐기 모양은 각 탐지된 애플리케이션 프로토콜에 전송된 데이터의 비율을 나타냅니다.
- 도표의 y축을 **Packets**로 변경할 경우 원도표는 특정 간격 동안 모니터링되는 네트워크를 통해 전송된 총 패킷 수를 나타내며, 원의 쐐기 모양은 각 포트에서 탐지된 총 패킷 수의 비율을 나타냅니다.

관련 항목

워크플로 사용, 11 페이지
이벤트 보기 구성

연결 그래프 데이터 옵션

x축, y축 또는 두 축을 모두 변경하여 연결 그래프에 다른 데이터를 표시할 수 있습니다. 원도표의 경우, x축을 변경하면 독립 변수가 변경되고 y축을 변경하면 종속 변수가 변경됩니다.

표 *26: X*축 옵션

X축 옵션	그래프 유형	이 데이터를 그래프로 표시
애플리케이션 프로토콜	막대 또는 원	가장 활성화된 10가지 애플리케이션 프로토콜별
디바이스	막대 또는 원	가장 활성화된 10가지 매니지드 디바이스별
초기자 IP	막대 또는 원	가장 활성화된 10가지 이니시에이터 호스트 IP 주소별
이니시에이터 사용자	막대 또는 원	가장 활성화된 10가지 이니시에이터 사용자별
응답기 IP	막대 또는 원	가장 활성화된 10가지 응답자 호스트 IP 주소별
응답자 포트	막대 또는 원	가장 활성화된 10가지 응답자 포트별
소스 디바이스	막대 또는 원	가장 활성화된 10가지 NetFlow 데이터 엑스포터, 그리고 Firepower System 매니지드 디바이스가 탐지한 모든 연결에 대한 `Firepower` 라는 이름의 소스 디바이스별

X축 옵션	그래프 유형	이 데이터를 그래프로 표시
시간	라인	시간 추이 y축을 **Time(**시간**)**으로 변경하거나 시간에서 다른 항목으로 변경하면 그래프 유형도 변경되며, 데이터 집합이 변경될 수도 있습니다.

표 ***27: Y***축 옵션

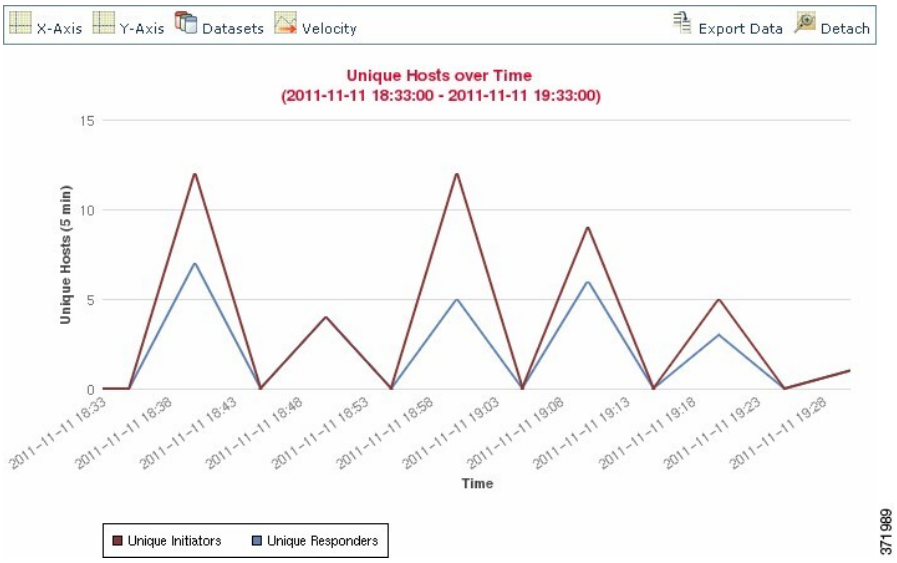
Y축 옵션	**X**축 기준을 사용하여 이 데이터를 그래프로 표시
바이트	전송된 바이트
연결	연결 수
KB	전송된 킬로바이트
초당 KB	초당 킬로바이트
패킷	전송된 패킷 수
고유 호스트	탐지한 고유 호스트 수
고유한 애플리케이션 프로토콜	고유 애플리케이션 프로토콜 수
고유한 사용자	고유한 사용자 수

여러 데이터 집합이 포함된 연결 그래프

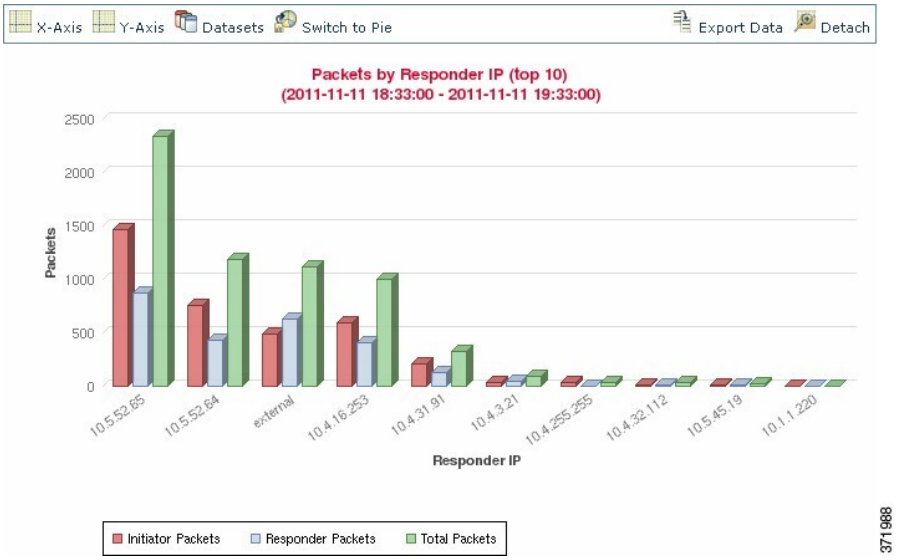
막대 그래프와 선 그래프는 모두 여러 데이터 집합을 표시할 수 있습니다. 즉, 각 x축 데이터 포인트의 y축에 여러 값을 표시할 수 있습니다. 예를 들어 고유한 이니시에이터 및 응답자의 총 수를 표시할 수 있습니다.

참고 원도표에서는 여러 데이터세트를 표시할 수 없습니다. 여러 데이터세트가 있는 막대 그래프에서 원도표로 전환할 경우, 원도표에는 자동으로 선택된 하나의 데이터세트만 표시됩니다. 표시할 데이터세트를 선택할 경우, management center은(는) 이니시에이터 및 응답자 통계보다 전체 통계를 우선시하고, 응답자 통계보다는 이니시에이터 통계를 우선시합니다.

선 그래프에서 여러 데이터세트는 각기 다른 색상의 여러 선으로 표시됩니다. 예를 들어 다음 그래픽에는 1시간 간격 동안 모니터링된 네트워크에서 탐지된 고유한 개시자의 총수 및 고유한 응답자의 총수가 표시됩니다.



막대 그래프에서 여러 데이터세트는 각 x축 데이터 포인트의 색상 막대로 표시됩니다. 예를 들어 다음 막대 그래프에는 모니터링된 네트워크에서 전송된 총 패킷, 이니시에이터가 전송한 패킷, 응답자가 전송한 패킷이 표시됩니다.



연결 그래프 데이터 집합 옵션

다음 표에서는 연결 그래프의 x축에 표시할 수 있는 데이터세트를 설명합니다.

표 ***28:*** 데이터 집합 옵션

y축에 표시되는 내용	선택 가능한 데이터 집합
연결	기본값 전용 - 모니터링되는 네트워크에서 탐지된 연결의 수(**Connections**) 이는 트래픽 프로파일 그래프의 유일한 옵션입니다.

y축에 표시되는 내용	선택 가능한 데이터 집합
KB	다음을 조합하여 선택 • 모니터링되는 네트워크에서 전송된 총 킬로바이트(**Total KBytes**) • 모니터링되는 네트워크의 호스트 IP 주소에서 전송한 킬로바이트 수(**Initiator KBytes**) • 모니터링되는 네트워크의 호스트 IP 주소가 수신한 킬로바이트 수(**Responder KBytes**)
초당 KB	기본값 전용 - 모니터링되는 네트워크에서 전송된 초당 총 킬로바이트(**Total KBytes Per Second**)
패킷	다음을 조합하여 선택 • 모니터링되는 네트워크에서 전송된 총 패킷(**Total Packets**) • 모니터링되는 네트워크의 호스트 IP 주소에서 전송한 패킷 수(**Initiator Packets**) • 모니터링되는 네트워크의 호스트 IP 주소가 수신한 패킷 수(**Responder Packets**)
고유 호스트	다음을 조합하여 선택 • 모니터링되는 네트워크의 고유한 세션 개시자 수(**Unique Initiators**) • 모니터링되는 네트워크의 고유한 세션 응답자 수(**Unique Responders**)
고유한 애플리케이션 프로토콜	기본값 전용 - 모니터링되는 네트워크의 고유한 애플리케이션 프로토콜 수(**Unique Application Protocols**)
고유한 사용자	기본값 전용 - 모니터링되는 네트워크의 세션 개시자에 로깅된 고유한 사용자 수(**Unique Initiator Users**)

이벤트 시간 제약 조건

각 이벤트에는 이벤트가 발생한 시점을 나타내는 타임스탬프가 있습니다. 시간 범위라고도 하는 타임 윈도우를 설정하여 일부 워크플로에 나타나는 정보를 제한할 수 있습니다.

시간을 기준으로 제한할 수 있는 이벤트를 기반으로 하는 워크플로는 페이지 상단에 시간 범위 줄이 나타납니다.

기본적으로 워크플로는 지난 시간으로 설정된 확장 타임 윈도우를 사용합니다. 예를 들어 오전 11:30분에 로그인할 경우 오전 10:30분부터 오전 11:30분까지의 이벤트를 볼 수 있습니다. 시간이 경과하면서 타임 윈도우가 확장됩니다. 오후 12:30분에는 오전 10:30분부터 오후 12:30분까지의 이벤트를 볼 수 있습니다.

이 동작은 이벤트 보기 설정에서 자체 기본 타임 윈도우를 설정해 변경할 수 있습니다. 이것은 세 가지 속성을 제어합니다.

- 타임 윈도우 유형(고정, 확장, 슬라이딩)
- 타임 윈도우 길이
- 타임 윈도우 개수(다중 타임 윈도우 또는 단일 글로벌 타임 윈도우)

기본 타임 윈도우 설정과 무관하게 이벤트 분석 과정에서 페이지 맨 위의 시간 범위를 클릭하면 표시되는 Date/Time(시간/날짜) 팝업 창에서 수동으로 타임 윈도우를 변경할 수 있습니다. 구성한 타임 윈도우의 개수 및 사용 중인 어플라이언스의 유형에 따라 Date/Time(시간/날짜) 창을 사용하여 현재 보고 있는 이벤트 유형의 기본 타임 윈도우를 변경할 수도 있습니다.

마지막으로, 슬라이딩 또는 확장 워크플로를 보는 도중 타임 윈도우를 일시 중지할 수 있습니다. 타임 윈도우 일시 중지로 데이터 집합 임시 중지, 33 페이지의 내용을 참조하십시오.

관련 항목

이벤트 보기 구성

연결 및 보안 관련 연결 이벤트 테이블 사용

이벤트에 대한 세션별 타임 윈도우 맞춤 설정

기본 타임 윈도우과 무관하게 이벤트 분석 과정에서 타임 윈도우를 수동으로 변경할 수 있습니다.

참고 수동 타임 윈도우 설정은 현재 세션에만 유효합니다. 로그아웃하고 다시 로그인하면 타임 윈도우는 기본값으로 돌아갑니다.

구성된 타임 윈도우의 수에 따라 어떤 워크플로의 타임 윈도우를 변경하면 어플라이언스의 다른 워크플로에 영향을 줄 수 있습니다. 예를 들어 단일 글로벌 타임 윈도우가 있을 경우 한 워크플로의 타임 윈도우를 변경하면 어플라이언스의 다른 워크플로에서도 변경됩니다. 이와 달리 다중 타임 윈도우를 사용하는 경우 감사 로그 또는 상태 이벤트 워크플로의 타임 윈도우를 변경하더라도 다른 타임 윈도우에 영향을 주지 않습니다. 반면에 다른 이벤트 종류의 타임 윈도우를 변경하면 (감사 이벤트 및 상태 이벤트를 제외하고) 시간의 제한을 받을 수 있는 모든 이벤트에 적용됩니다.

일부 워크플로는 시간의 제한을 받지 않을 수 있으므로 타임 윈도우 설정은 호스트, 호스트 속성, 애플리케이션, 애플리케이션 세부사항, 취약성, 사용자 또는 허용 목록 위반을 기반으로 한 워크플로에는 적용되지 않습니다.

Date/Time(시간/날짜) 창의 Time Window(타임 윈도우) 탭을 사용하여 수동으로 타임 윈도우를 구성합니다. 기본 타임 윈도우 설정에서 구성한 타임 윈도우의 수에 따라 탭의 제목은 다음 중 하나가 됩니다.

- **Events Time Window(**이벤트 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 감사 로그 또는 상태 이벤트 워크플로가 아닌 워크플로의 타임 윈도우를 설정하는 경우
- **Health Monitoring Time Window(**상태 모니터링 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 상태 이벤트 워크플로의 타임 윈도우를 설정하는 경우

- **Audit Log Time Window(**감사 로그 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 감사 로그에 대한 타임 윈도우를 설정하는 경우
- **Global Time Window(**전역 타임 윈도우**)** - 단일 타임 윈도우를 구성한 경우

타임 윈도우를 구성할 때는 사용할 타임 윈도우 유형을 가장 먼저 결정해야 합니다.

- 고정(*static*) 타임 윈도우는 특정 시작 시간부터 종료 시간까지의 모든 이벤트를 표시합니다.
- 확장(*expanding*) 타임 윈도우는 특정 시작 시간부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 타임 윈도우가 확장되고 새 이벤트가 이벤트 보기에 추가됩니다.
- 슬라이딩(*sliding*) 타임 윈도우는 특정 시작 시간(예: 1주일 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 페이지를 새로고침하면 타임 윈도우가 "슬라이딩"하므로 구성된 범위(이 예에서는 지난주)의 이벤트만 볼 수 있습니다. 검사하는 동안 데이터 집합의 업데이트를 일시 중단하는 방법은 타임 윈도우 일시 중지로 데이터 집합 임시 중지, 33 페이지 섹션을 참조하십시오.

선택하는 유형에 따라 Date/Time(시간/날짜) 창이 바뀌어 각기 다른 설정 옵션을 제공합니다.

참고 Firepower System에서는 시간대 환경설정에서 지정한 시간에 따라 24시간 시계를 사용합니다.

타임 윈도우 설정

다음 표에서는 Time Window 탭에서 구성할 수 있는 다양한 설정에 대해 설명합니다.

표 ***29:*** 타임 윈도우 설정

설정	타임 윈도우 유형	설명
타임 윈도우 유형 드롭다운 목록	해당 없음	사용할 타임 윈도우의 유형을 고정, 확장, 슬라이딩 중에서 선택합니다. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
타임 캘린더 시작	고정, 확장	타임 윈도우의 시작 날짜와 시간을 지정합니다. 모든 타임 윈도우의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다. 달력 대신 아래에서 설명하는 미리 설정 옵션을 사용할 수 있습니다.

설정	타임 윈도우 유형	설명
타임 캘린더 종료	고정	타임 윈도우의 종료 날짜와 시간을 지정합니다. 모든 타임 윈도우의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다. 확장 타임 윈도우를 사용하는 경우 End Time 달력이 회색으로 표시되어 종료 시간이 "현재"임을 나타냅니다. 달력 대신 아래에서 설명하는 미리 설정 옵션을 사용할 수 있습니다.
최종 필드 및 드롭다운 목록 보기	슬라이딩	슬라이딩 타임 윈도우의 길이를 구성합니다.
미리 설정: 모두	모두	목록에 있는 시간 범위 중 하나를 클릭하여 어플라이언스의 로컬 시간에 따라 타임 윈도우를 변경합니다. 예를 들어 **1 week(1** 주**)**클릭하면 지난주를 나타내도록 타임 윈도우가 변경됩니다. 미리 설정된 값을 클릭하면 선택한 설정을 반영하여 달력이 변경됩니다.
미리 설정: 현재	고정, 확장	목록에 있는 시간 범위 중 하나를 클릭하여 어플라이언스의 로컬 시간 및 날짜에 따라 타임 윈도우를 변경합니다. 미리 설정된 값을 클릭하면 선택한 설정을 반영하여 달력이 변경됩니다. 다음을 참고하십시오. • 현재 요일은 자정에 시작합니다. • 현재 주는 일요일 자정에 시작합니다. • 현재 월은 월의 첫날 자정에 시작합니다.
미리 설정: 동기화	모두(글로벌 타임 윈도우를 사용하는 경우에는 사용 불가)	다음 중 하나를 클릭합니다. • **Events Time Window(**이벤트 타임 윈도우**)** - 현재 타임 윈도우를 이벤트 타임 윈도우dhk 동기화합니다. • **Health Monitoring Time Window(**상태 모니터링 타임 윈도우**)** - 현재 타임 윈도우를 상태 모니터링 타임 윈도우와 동기화합니다. • **Audit Log Time Window(**감사 로그 타임 윈도우**)** - 현재 타임 윈도우를 감사 로그 타임 윈도우와 동기화합니다.

타임 윈도우 변경

프로시저

단계 **1** 시간으로 제한된 워크플로에서 **Time Range(**시간 범위**)** ( )를 클릭하여 Date/Time(날짜/시간) 창으로 이동합니다.

단계 **2** **Events Time Window(**이벤트 타임 윈도우**)**에서 타임 윈도우 설정, 31 페이지에 설명된 대로 타임 윈도우를 설정합니다.

팁 **Reset**을 클릭하여 타임 윈도우를 기본 설정으로 변경합니다.

단계 **3** **Apply(**적용**)**를 클릭합니다.

타임 윈도우 일시 중지로 데이터 집합 임시 중지

슬라이딩 또는 확장 타임 윈도우를 사용하는 경우, 타임 윈도우를 일시 중지해 워크플로가 제공하는 데이터의 스냅샷을 조사할 수 있습니다. 중지하지 않은 워크플로가 업데이트되면 조사할 이벤트가 제거되거나 조사 대상이 아닌 이벤트가 추가될 수 있습니다. 이 기능은 이런 경우에 유용합니다.

페이지 하단의 링크를 클릭해 다른 이벤트 페이지를 표시하면 타임 윈도우는 자동으로 일시 중지됩니다. 준비가 끝나면 타임 윈도우의 일시 중지를 취소하면 됩니다.

분석을 마치면 타임 윈도우의 일시 중지를 취소할 수 있습니다. 타임 윈도우 일시 중지를 취소하면 환경설정에 따라 업데이트되며, 이벤트 보기도 업데이트되어 일시 중지 취소된 타임 윈도우가 반영됩니다.

이벤트 타임 윈도우를 일시 중지하더라도 대시보드에 아무런 영향이 없으며, 또한 대시보드를 일시 중지하더라도 이벤트 타임 윈도우 일시 중지는 영향받지 않습니다.

프로시저

시간 기준으로 제한되는 워크플로에서, 원하는 시간 범위 제어를 선택합니다.

- 시간 창을 일시 중지하려면 시간 범위 제어 아이콘**(Pause(**일시 중지**)** (⏸))을 클릭합니다.
- 시간 창 일시 중지를 취소하려면 시간 범위 제어 아이콘**(Play(**재생**)** (▶))을 클릭합니다.

이벤트에 대한 기본 타임 윈도우

이벤트 분석 과정에서 Date/Time(날짜/시간) 창의 Preferences(환경설정) 탭을 사용하면 이벤트 보기 설정을 사용하지 않고도 현재 표시하는 이벤트 유형의 기본 타임 윈도우를 변경할 수 있습니다.

이렇게 기본 타임 윈도우를 변경하면 현재 보고 있는 이벤트 유형의 기본 타임 윈도우만 바뀝니다. 예를 들어 다중 타임 윈도우를 구성한 경우 Preferences(환경설정) 탭에서 기본 타임 윈도우를 변경하면 이벤트, 상태 모니터링 또는 감사 로그 창, 즉 첫 번째 탭에 표시된 타임 윈도우의 설정이 바뀝니다. 단일 타임 윈도우를 구성한 경우 Preferences(환경설정) 탭에서 기본 타임 윈도우를 변경하면 모든 이벤트 유형의 기본 타임 윈도우가 바뀝니다.

관련 항목

기본 시간대

이벤트 유형에 대한 기본 타임 윈도우 옵션

다음 표에서는 Preferences(환경설정) 탭에서 구성할 수 있는 다양한 설정에 대해 설명합니다.

표 ***30:*** 타임 윈도우 환경설정

기본 설정	설명
간격 새로고침	이벤트 보기의 새로 고침 간격을 분 단위로 설정합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다.
타임 윈도우 수	사용할 타임 윈도우의 개수를 지정합니다. • 감사 로그, 상태 이벤트, 시간의 제한이 가능한 이벤트 기반 워크플로에 각각 기본 타임 윈도우를 구성하려면 **Multiple**을 선택합니다. • 모든 이벤트에 적용되는 글로벌 타임 윈도우를 사용하려면 **Single**을 선택합니다.
Default Time Window: Show the Last - Sliding	이 설정에서는 지정하는 길이의 슬라이딩 기본 타임 윈도우를 구성할 수 있습니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하면 시간대가 "슬라이딩"하므로 항상 지난 1시간의 이벤트가 표시됩니다.
Default Time Window: Show the Last - Static/Expanding	이 설정에서는 지정하는 길이의 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대 현재 시간으로 확장됩니다.
Default Time Window: Current Day - Static/Expanding	이 설정에서는 현재 일에 대해 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 현재 날짜는 현재 세션의 표준 시간대 설정에 따라 자정에 시작합니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 자정부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 자정부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대가 현재 시간으로 확장됩니다. 로그아웃하기 전 24시간 이상 분석이 계속될 경우 이 시간대가 24시간을 초과할 수 있습니다.

기본 설정	설명
Default Time Window: Current Week - Static/Expanding	이 설정에서는 현재 주에 대해 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 현재 주는 현재 세션의 표준 시간대 설정에 따라 이전 일요일 자정에 시작합니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 자정부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 일요일 자정부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대는 현재 시간으로 확장됩니다. 로그아웃하기 전 1주일 이상 분석이 계속될 경우, 시간대는 1주를 초과할 수 있습니다.

이벤트 유형에 대한 기본 타임 윈도우 변경

프로시저

단계 **1** 시간으로 제한된 워크플로우에서 **Time Range(**시간 범위**)** ( )를 클릭하여 Date/Time(날짜/시간) 창으로 이동합니다.

단계 **2** **Preferences(**환경설정**)**를 클릭하고 이벤트 유형에 대한 기본 타임 윈도우 옵션, 34 페이지에 설명된 대로 환경설정을 변경합니다.

단계 **3** **Save Preferences(**환경설정 저장**)**를 클릭합니다.

단계 **4** 다음 2가지 옵션을 사용할 수 있습니다.

- 보고 있는 이벤트 보기에 새 기본 타임 윈도우 설정을 적용하려면 **Apply(**적용**)**를 클릭하여 Date/Time(날짜/시간) 창을 닫고 이벤트 보기를 새로 고칩니다.
- 기본 타임 윈도우 설정을 적용하지 않고 분석을 계속하려면 **Apply(**적용**)**를 클릭하지 않고 Date/Time(날짜/시간) 창을 닫습니다.

이벤트 보기 제약 조건

워크플로 페이지에 표시되는 정보는 지정된 제약 조건에 따라 결정됩니다. 예를 들어 초기에 이벤트 워크플로를 열 때 그 정보는 이전 시간 동안 생성된 이벤트로 제한됩니다.

워크플로의 다음 페이지로 이동하고 표시되는 데이터를 특정 값으로 제한하려면 페이지에서 해당 값의 행을 선택하고 **View(**보기**)**를 클릭합니다. 워크플로에서 다음 페이지로 이동하되 현재 제약 조건을 유지하고 모든 이벤트를 이월하려면 **View All(**모두 보기**)**을 선택합니다.

참고 카운트가 아닌 다중 값을 포함한 행을 선택하고 **View(**보기**)**를 클릭하면 복합 제약 조건이 생성됩니다.

워크플로에서 데이터를 제한하는 3번째 방법이 있습니다. 선택한 값의 행으로 페이지를 제한하고 선택한 값을 페이지 맨 위의 제약 조건 목록에 추가하려면 페이지에서 특정 행의 값을 클릭합니다. 예를 들어 로깅된 연결의 목록을 보는 중에 액세스 컨트롤을 통해 허용된 연결로 목록을 제한하려면 **Action(**작업**)** 열에서 **Allow(**허용**)**를 클릭합니다. 또 다른 예로 침입 이벤트를 보는 중에 목적지 포트가 80인 이벤트로 제한하려는 목록을 제한하려는 경우 **Destination Port/ICMP Code(**대상 포트**/ICMP** 코드**)** 열에서 **80 (http)/tcp**를 클릭합니다.

팁 모니터 규칙 기준에 따라 연결 이벤트를 제한하는 절차는 약간 다르며 추가 단계가 필요할 수 있습니다. 또한 관련된 파일 또는 침입 정보를 기준으로 연결 이벤트를 제한할 수는 없습니다.

검색을 사용하여 워크플로의 정보를 제한할 수도 있습니다. 단일 열에서 다중 값을 대상으로 제한하려면 이 기능을 사용합니다. 예를 들어 두 IP 주소와 관련된 이벤트를 보려는 경우 **Edit Search(**검색 편집**)**를 클릭하고 Search(검색) 페이지에서 해당 IP 주소 필드를 수정하여 두 주소를 모두 포함하게 한 다음 **Search(**검색**)**를 클릭합니다.

검색 페이지에 입력하는 검색 기준은 페이지 맨 위에 제약 조건으로 나열되며, 그에 따라 결과 이벤트가 제한됩니다. management center에서는 현재 제약 조건이 다른 워크플로로 이동할 때에도 적용됩니다. 단, 복합 제약 조건인 경우는 제외합니다.

검색할 때 검색 제약 조건이 검색 중인 테이블에 적용될 것인지를 각별히 주의해야 합니다. 예를 들어 클라이언트 데이터는 연결 요약에서 사용할 수 없습니다. 연결에서 탐지된 클라이언트를 기반으로 연결 이벤트를 검색한 다음 그 결과를 연결 요약 이벤트 보기에 표시할 경우 management center에서는 아무런 제한을 받지 않은 것처럼 연결 데이터를 표시합니다. 잘못된 제약 조건은 N/A(not applicable) 레이블이 지정되고 취소선으로 표시됩니다.

이벤트 제약

프로시저

단계 **1** 워크플로 선택, 13 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 모든 워크플로에는 다음 옵션이 있습니다.

- 단일 값과 일치하는 이벤트만 보도록 제한하려면, 페이지의 행에서 원하는 값을 클릭합니다.
- 여러 값과 일치하는 이벤트만 보도록 제한하려면, 해당 값이 있는 이벤트의 확인란을 선택하고 **View(**보기**)**를 클릭합니다.

  참고 행에 카운트가 아닌 다중 값이 있을 경우 복합 제약 조건이 추가됩니다.

- 제약 조건을 제거하려면 Search Constraints(검색 제약 조건) **Expand Arrow(**확장 화살표**)(**)를 클릭하고 확장된 Search Constraints(검색 제약 조건) 목록에서 제약 조건 이름을 클릭합니다.
- Search(검색) 페이지를 사용하여 제약 조건을 편집하려면 **Edit Search(**검색 편집**)**를 클릭합니다.
- 제약 조건을 저장된 검색으로 저장하려면 **Save Search(**저장 검색**)**를 클릭하고 쿼리에 이름을 지정합니다.

  참고 복합 제약 조건을 포함한 쿼리는 저장할 수 없습니다.

- 동일한 제약 조건을 다른 이벤트 보기와 함께 사용하려면 **Jump to(**이동**)**를 클릭하고 이벤트 보기를 선택합니다.

  참고 다른 워크플로로 전환하는 경우 복합 제약 조건은 유지되지 않습니다.

- 제약 조건 표시를 전환하려면 Search Constraints(검색 제한 조건) **Expand Arrow(**확장 화살표**)(**) 또는 Search Constraints(검색 제약 조건) **Collapse Arrow(**축소 화살표**)(**)를 클릭합니다. 제약 조건의 목록이 커서 화면의 대부분을 차지할 때 유용한 기능입니다.

복합 이벤트 보기 제약

복합 제약 조건은 특정 이벤트에 대해 카운트가 아닌 모든 값을 기반으로 합니다. 카운트가 아닌 다중 값이 있는 행을 선택할 때 해당 페이지에서 그 행의 카운트가 아닌 모든 값과 매칭하는 이벤트만 가져오는 복합 제약 조건이 설정됩니다. 예를 들어 소스 IP 주소 `10.10.31.17`, 목적지 IP 주소 `10.10.31.15`를 포함하는 행 및 소스 IP 주소가 `172.10.10.17`, 목적지 IP 주소가 `172.10.10.15`인 행을 선택할 경우 다음 사항이 모두 검색됩니다.

- 소스 IP 주소가 10.10.31.17이고 목적지 IP 주소가 10.10.31.15인 이벤트

  또는

- 소스 IP 주소가 172.10.31.17이고 목적지 IP 주소가 172.10.31.15인 이벤트

복합 제약 조건을 단순 제약 조건과 결합할 경우 단순 제약 조건은 복합 제약 조건의 전 범위에 배포됩니다. 예를 들어 프로토콜 값이 `tcp`인 단순 제약 조건을 위에 소개된 복합 제약 조건에 추가한 경우 다음 사항이 모두 검색됩니다.

- 소스 IP 주소가 10.10.31.17이고 목적지 IP 주소가 10.10.31.15이며 프로토콜이 tcp인 이벤트

  또는

- 소스 IP 주소가 172.10.31.17이고 목적지 IP 주소가 172.10.31.15이며 프로토콜이 tcp인 이벤트

복합 제약 조건에 대해서는 검색을 수행하거나 검색을 저장할 수 없습니다. 또한 이벤트 보기 링크를 사용하거나 **(switch workflow)**을 클릭하여 다른 워크플로로 전환할 때 복합 제약 조건을 유지할 수 없습니다. 복합 제약 조건이 적용된 이벤트 보기에 즐겨찾기를 지정할 경우 제약 조건은 즐겨찾기와 함께 저장되지 않습니다.

복합 이벤트 보기 제약 사용

프로시저

단계 **1** 워크플로 선택, 13 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 복합 제약 조건은 다음 방법으로 관리할 수 있습니다.

- 복합 제약 조건을 생성하려면 카운트가 아닌 다중 값을 포함한 행을 하나 이상 선택하고 **View(**보기**)**를 클릭합니다.
- 복합 제약 조건을 지우려면 Search Constraints(검색 제약 조건) **Expand Arrow(**확장 화살표**)**( ) 를 클릭하고 **Compound Constraints(**복합 제약 조건**)**를 클릭합니다.

워크플로 간 탐색

워크플로 페이지에서 **Jump to...(**이동**...)** 드롭다운 목록의 링크를 사용하여 다른 워크플로로 이동할 수 있습니다. 드롭다운 목록을 선택하여 추가 워크플로를 표시하고 선택합니다.

새 워크플로를 선택하면 선택한 행에서 공유하는 속성 및 설정된 제약 조건이 새 워크플로에서 사용됩니다(적용 가능한 경우). 구성된 제약 조건 또는 이벤트 속성이 새 워크플로의 필드에 매핑되지 않을 경우 삭제됩니다. 또한 복합 제약 조건은 다른 워크플로로 전환할 때 유지되지 않습니다. 캡처 파일 워크플로의 제약 조건은 파일 및 악성코드 이벤트 워크플로로만 전송됩니다.

참고 어떤 시간 범위의 이벤트 수를 볼 때 총 이벤트 수가 세부사항 데이터가 있는 이벤트의 수를 반영하지 않을 수 있습니다. 이는 디스크 공간 사용량을 관리하기 위해 때때로 오래된 이벤트의 세부사항을 삭제하기 때문입니다. 이벤트 세부사항이 삭제되는 경우를 최소화하기 위해 이벤트 로깅을 세밀하게 조정하여 구축에 가장 중요한 이벤트만 로깅하게 할 수 있습니다.

타임 윈도우를 일시 중지하거나 고정 타임 윈도우를 구성한 경우를 제외하고 타임 윈도우는 워크플로를 변경할 때 바뀝니다.

이 기능으로 의심스러운 활동을 더 효과적으로 조사할 수 있습니다. 예를 들어 연결 데이터를 보는 중에 내부 호스트가 비정상적으로 많은 양의 데이터를 외부 사이트에 보내는 것이 확인될 경우 responder IP 주소와 포트를 제약 조건으로 선택한 다음 **Applications(**애플리케이션**)** 워크플로로 바로 이동할 수 있습니다. 애플리케이션 워크플로는 responder IP 주소와 포트를 IP Address 및 Port 제약 조건으로 사용하면서 애플리케이션에 대한 추가 정보, 이를테면 어떤 종류의 애플리케이션인가를 표시합니다. 페이지 맨 위의 **Hosts(**호스트**)**를 클릭하여 원격 호스트의 호스트 프로파일을 볼 수도 있습니다.

애플리케이션에 대한 추가 정보를 얻은 다음 **Correlation Events(**상관관계 이벤트**)**를 클릭하여 연결 데이터 워크플로로 돌아가거나 제약 조건에서 Responder IP를 제거하거나 제약 조건에 Initiator IP를

추가하거나 **Application Details(**애플리케이션 세부사항**)**를 선택하여 시작 호스트의 사용자가 원격 호스트에 데이터를 전송할 때 사용한 클라이언트를 확인할 수 있습니다. Port 제약 조건은 Application Details 페이지에 전송되지 않습니다. 로컬 호스트를 제약 조건으로 유지하지만 다른 탐색 버튼을 사용하여 추가 정보를 찾을 수도 있습니다.

- 로컬 호스트가 어떤 정책을 위반했는지 알아보려면 IP 주소를 제약 조건으로 유지하고 **Jump to(**이동**)** 드롭다운 목록에서 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.
- 호스트에 대해 침입 규칙이 트리거되었는지(공격 지표) 확인하려면 **Jump to(**이동**)** 드롭다운 목록에서 **Intrusion Events(**침입 이벤트**)**를 선택합니다.
- 로컬 호스트에 대한 호스트 프로파일을 보고 호스트가 만일의 익스플로잇 취약성을 갖고 있는지 확인하려면 **Jump to(**이동**)** 드롭다운 목록에서 **Hosts(**호스트**)**를 선택합니다.

통합 이벤트 보기로 작업

통합 이벤트는 여러 유형의 방화벽 이벤트(연결, 침입, 파일, 악성코드 및 일부 보안 관련 연결 이벤트)를 단일 화면 보기로 제공합니다. 통합 이벤트 테이블은 수준 높은 사용자 맞춤화가 가능합니다. 이벤트 보기에 표시되는 정보를 세부적으로 조정할 수 있도록 사용자 지정 필터를 생성하고 적용할 수 있습니다. 통합 이벤트 테이블의 **Live View(**라이브 보기**)** 옵션을 사용하면 방화벽 이벤트를 실시간으로 확인하고 네트워크 활동을 모니터링할 수 있습니다.

통합 이벤트 보기를 사용하는 경우에는 다음을 수행할 수 있습니다.

- 다양한 유형의 이벤트 간 관계 찾기
- 실시간으로 정책 변경의 영향 확인

프로시저

단계 **1** 분석 > 통합 이벤트을 선택합니다.

단계 **2** 특정 기간의 방화벽 이벤트를 보려면 시간 범위(고정 또는 슬라이딩)를 선택합니다. 기본적으로 통합 이벤트 보기 테이블에는 이전 시간의 이벤트가 표시됩니다. 보안 이벤트의 더욱 세부적인 컨텍스트를 가져오거나, 테이블 열을 사용자 지정하거나, 라이브 보기를 활성화하고 이벤트의 업데이트를 실시간으로 확인하기 위해 테이블을 필터링할 수 있습니다.

통합 이벤트에 대한 자세한 내용은 통합 이벤트를 참고하십시오.

북마크

이벤트 분석의 특정 위치 및 시점으로 신속하게 돌아갈 수 있게 하려면 즐겨찾기를 생성합니다. 즐겨찾기는 다음 사항에 대한 정보를 유지합니다.

- 사용 중인 워크플로
- 워크플로에서 표시 중인 부분
- 워크플로 내의 페이지 번호
- 모든 검색 제약 조건
- 모든 비활성 열
- 사용 중인 시간 범위

생성하는 즐겨찾기는 즐겨찾기 액세스 권한이 있는 모든 사용자 계정에서 사용할 수 있습니다. 즉 심층 분석이 필요한 이벤트 모음을 발견할 경우 편리하게 즐겨찾기를 생성한 다음 알맞은 권한을 가진 다른 사용자에게 조사를 맡길 수 있습니다.

참고 즐겨찾기에 나타난 이벤트가 삭제될 경우(사용자 직접 삭제 또는 자동 데이터베이스 정리에 의해 삭제) 즐겨찾기는 더 이상 원래의 이벤트 집합을 표시하지 않습니다.

즐겨찾기 생성

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 즐겨찾기만 볼 수 있습니다.

프로시저

단계 **1** 이벤트를 분석할 때 관심 이벤트가 표시된 상태에서 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다.

단계 **2** **Bookmark Name(**즐겨찾기 이름**)** 필드에 이름을 입력합니다.

단계 **3** **Save Bookmark(**즐겨찾기 저장**)**를 클릭합니다.

즐겨찾기 보기

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 즐겨찾기만 볼 수 있습니다.

프로시저

모든 이벤트 보기는 두 가지 옵션을 제공합니다.

- **View Bookmarks(**즐겨찾기 보기**)**에 마우스 포인터를 올리고, 드롭다운 메뉴에서 원하는 즐겨찾기를 클릭합니다.

- View Bookmarks(즐겨찾기 보기) 페이지에서 **View Bookmarks(**즐겨찾기 보기**)**를 클릭하고, 원하는 즐겨찾기 이름이나 옆에 있는 **View(**보기**)** ( )을 클릭합니다.

  참고 원래 즐겨찾기에 나타난 이벤트가 삭제될 경우(사용자 직접 삭제 또는 자동 데이터베이스 정리에 의해 삭제) 즐겨찾기는 더 이상 원래의 이벤트 집합을 표시하지 않습니다.

워크플로우 히스토리

기능	버전	세부 사항
IPS 이벤트 데이터스토어 교체	7.2.0	침입 이벤트 및 이벤트 클립보드 페이지는 더 이상 사용되지 않습니다. 사용되지 않는 페이지: • **Analysis(**분석**) > Intrusions(**침입**) > Clipboard(**클립보드**)** • **Analysis(**분석**) > Intrusions(**침입**) > Incidents(**인시던트**)** 지원되는 플랫폼: management center
통합 이벤트 뷰어	7.0.0	연결(보안 인텔리전스 포함), 침입, 파일 및 악성 코드 등 여러 이벤트 유형이 포함된 단일 테이블을 보고 작업합니다. 새 페이지/수정 페이지: 분석 > 통합 이벤트 아래 새 페이지 지원되는 플랫폼: management center
원격으로 저장된 이벤트 작업	7.0.0	Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 management center에서 작업할 수 있습니다. 시스템은 가장 적합한 데이터 소스를 자동으로 사용합니다. 또는 소스를 명시적으로 선택할 수 있습니다. 이 옵션은 Security Analytics and Logging(보안 애널리틱스) 마법사를 완료한 경우에만 나타납니다. 신규/수정 페이지: 연결 이벤트를 표시하는 경우, 즉 Analysis(분석) 메뉴 아래의 Workflow table(워크플로우 테이블), 대시 보드, 상황 탐색기 및 보고서. 지원되는 플랫폼: management center
특정 경우에 워크플로우 테이블의 개선된 로딩 속도	6.6.0	워크플로우 페이지의 테이블에는 열이 6개 이하로 표시되는 경우에만 동일한 행에 대한 개수 열이 표시됩니다. 이렇게 하면 필요한 계산량이 최소화되므로 테이블 로드 속도가 향상됩니다. 신규/수정 페이지: Analysis(분석) 메뉴 아래의 모든 페이지에서 워크플로우 테이블을 표시합니다. 지원되는 플랫폼: management center