다음 단계

다음 단계

Security Analytics and Logging(온프레미스)의 일부로 Secure Network Analytics 어플라이언스에 이벤트 데이터를 전송하도록 방화벽 디바이스를 구성한 후 다음 단계를 수행할 수 있습니다.

- management center 온라인 도움말을 검토합니다.
- 관리자웹 애플리케이션 온라인 도움말Secure Network Analytics에서 자세한 내용을 참고하십시오.

Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Management Center에서 작업

디바이스가 Security Analytics and Logging(온프레미스)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.

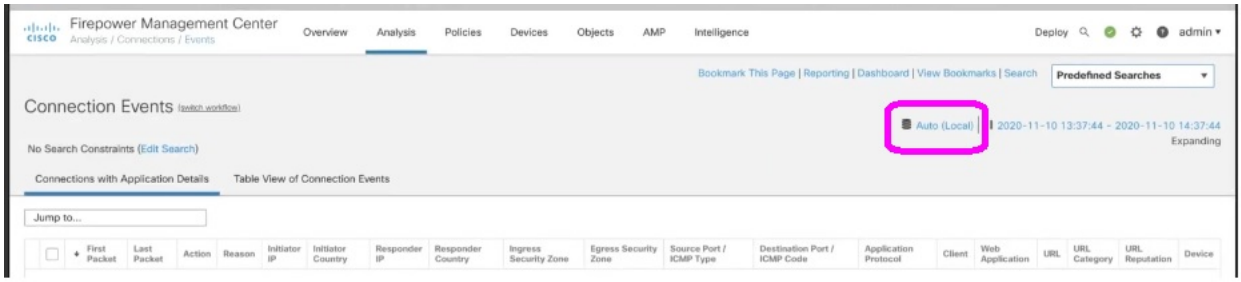
선택한 데이터 소스는 우선순위가 낮은 연결 이벤트에만 사용됩니다. 기타 모든 이벤트 유형(침입, 파일 및 악성 코드 이벤트, 해당 이벤트와 연결된 연결 이벤트, 보안 인텔리전스 이벤트)은 데이터 소스에 관계 없이 표시됩니다.

시작하기 전에

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

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.

교차 실행을 이용한 이벤트 조사

management center에서 이벤트를 볼 때 특정 이벤트 데이터(예: IP 주소)를 마우스 오른쪽 버튼으로 클릭하고 관리자에서 관련 데이터를 볼 수 있습니다.

단계 **1** 이벤트를 표시하는 management center의 다음 페이지 중 하나로 이동합니다.

- 대시보드(**Overview(개요) > Dashboards(대시보드)**) 또는
- 이벤트 뷰어 페이지(이벤트의 테이블을 포함하는 분석 메뉴에서 아무 메뉴 옵션).

단계 **2** 관심 있는 이벤트를 오른쪽으로 클릭하고 사용할 Security Analytics and Logging(온프레미스) 교차 실행 리소스를 선택합니다. 별도의 브라우저 창에 관리자이(가) 열립니다. 아직 로그인하지 않은 경우 사용자 이름과 암호를 입력하라는 메시지가 표시될 수 있습니다. 쿼리하는 데이터의 양, 관리자의 속도 및 요구 등의 요소에 따라 쿼리 처리에 시간이 오래 걸릴 수도 있습니다.

단계 **3** 관리자에 로그인합니다.