연관분석 과정

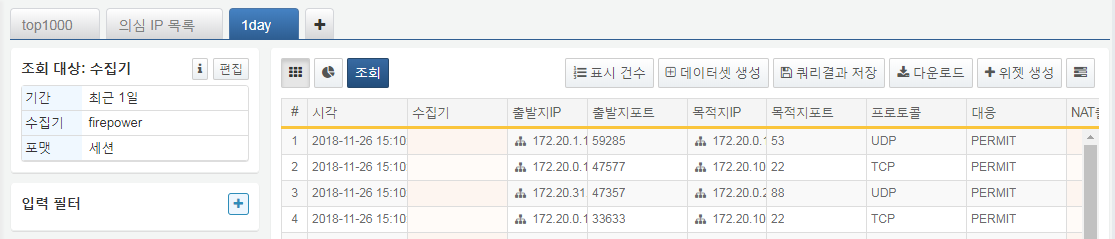
단계 1

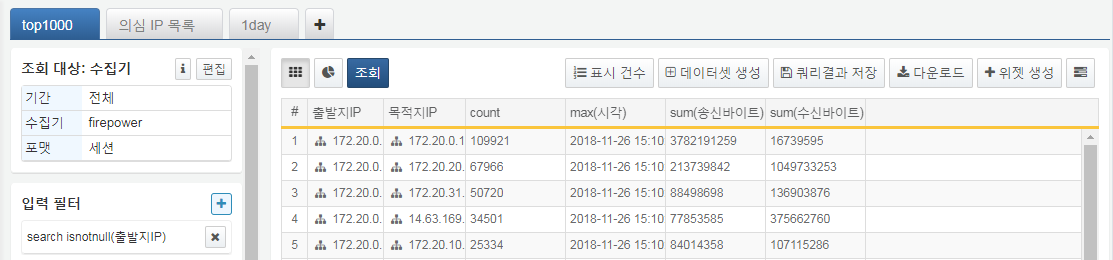
데이터 준비

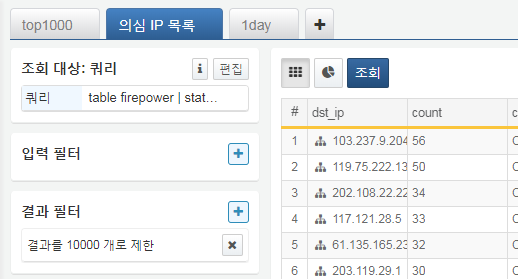
연관분석을 하기 위해선 피벗 화면에서 탭을 최소한 2개 이상 열고, 각각 탭에 분석할 데이터를 준비합니다. 필요시 탭 우측 버튼을 눌러 탭 이름을 변경하거나 탭을 삭제합니다.

아래 예시에서는 3개의 탭을 준비했습니다.

* 1day 탭: 최근 1일 동안 입력된 방화벽 데이터 (분석대상 데이터)
* top1000 탭: 네트워크 트래픽이 가장 많은 출발지IP-목적지IP 페어 1000개 (비교대상 데이터1)
* 의심 IP 목록 탭: 의심되는 IP 목록 (비교대상 데이터2)





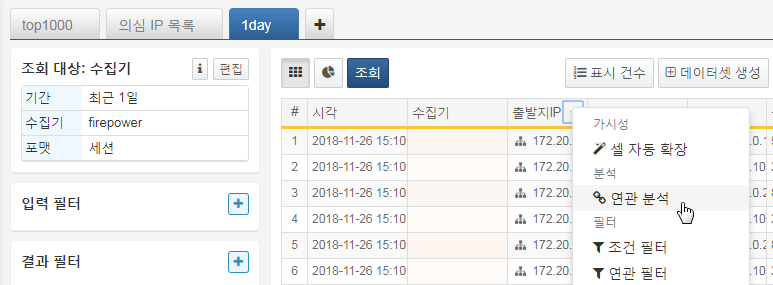


단계 2

연관분석 추가

연관 분석을 진행하기 위해서는 데이터 결과 창에서 열 제목 클릭 후 연관 분석 메뉴를 선택합니다.

예시에서는 1day 탭에서 출발지IP에 대한 연관 분석을 진행합니다.

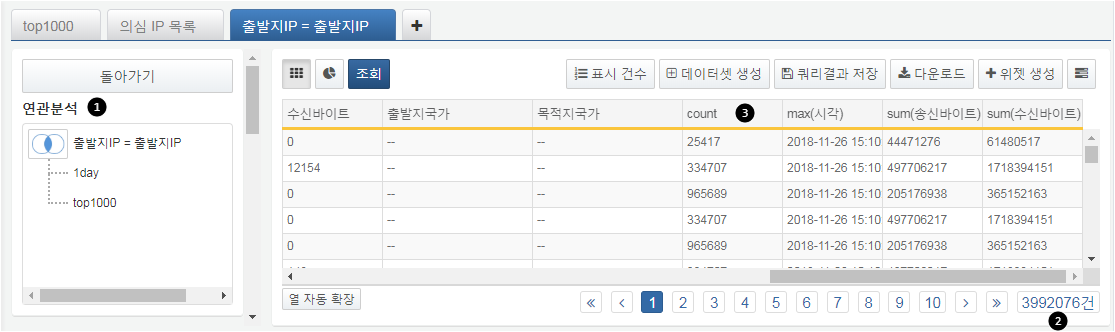


연관 분석 메뉴에서 연관 분석 설정을 입력할 수 있습니다.

예시에서는 top1000탭의 출발지IP 필드와 Inner 조인 유형의 연관분석을 추가합니다.



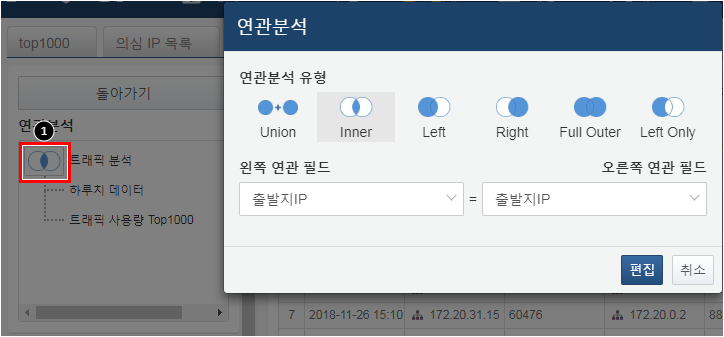
위와 같은 조건으로 연관분석 추가 시 화면이 다음과 같이 변경됩니다. 먼저, 왼쪽 위에 조회 대상 메뉴가 연관분석 메뉴(1)로 바뀌었으며 현재 연관분석 정보가 표시됩니다. 그리고 Inner 조인을 했기 때문에 매핑된 데이터만 출력되므로 출력 건수(2)가 줄었습니다. 또한 기존에 존재하지 않았던 count, sum(송신바이트), sum(수신바이트) 컬럼(3)이 추가되었습니다.



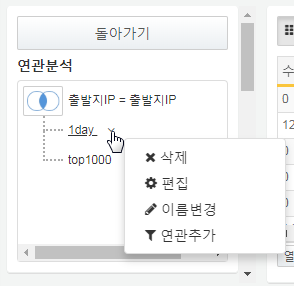
단계 3

연관분석 수정

연관분석 메뉴에서 연관분석 유형(벤 다이어그램 아이콘 1)을 클릭하면 연관분석 유형과 연관 필드를 변경할 수 있습니다.



연관분석 메뉴에서 연관분석이나 탭을 클릭하면 컨텍스트 메뉴가 표시됩니다. 각 탭을 클릭할 경우 삭제, 편집, 이름변경, 연관추가 메뉴가 뜨고, 연관분석 이름을 클릭할 경우 삭제, 이름변경, 연관추가 메뉴가 뜹니다.



**삭제**

해당 탭이나 연관분석을 삭제합니다. 삭제시 연관분석 적용 이전 상태로 돌아갑니다.

**편집**

해당 탭 데이터를 편집합니다. 데이터 원본, 필터, 집계 등을 수정할 수 있습니다.

**이름변경**

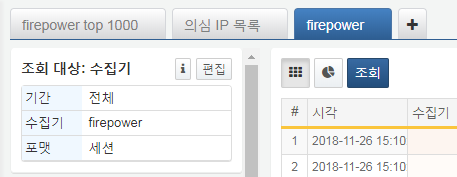
연관분석 메뉴에서 표시되는 이름을 변경합니다.

**연관추가**

새로운 연관분석을 추가합니다.

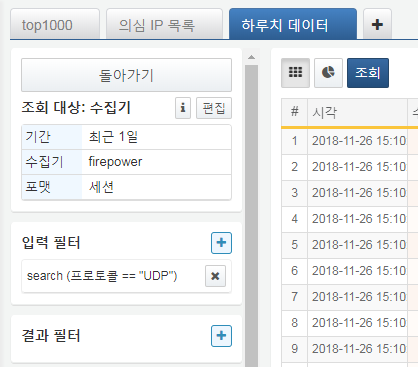
**삭제**

연관분석 삭제 시 해당 연관분석이 삭제됩니다. 탭 삭제 시 해당 탭을 사용한 연관분석이 삭제됩니다.



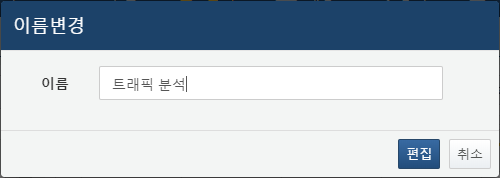
**편집**

편집을 선택하면 해당 데이터 탭으로 들어가서 설정을 수정할 수 있습니다. 데이터 유형과 조회 기간을 변경하거나, 필터 설정을 변경하거나, 집계 필드들을 바꾸고 설정을 변경할 수 있습니다. 편집 작업이 완료되면 돌아가기 버튼을 눌러 다시 연관분석 화면으로 돌아갑니다.



**이름변경**

연관분석과 데이터 탭의 이름을 변경하여 좀 더 편하게 데이터 분석 작업을 진행할 수 있습니다. 이름변경을 클릭하면 아래와 같이 이름변경 창이 뜹니다.



변경할 이름을 입력하고 편집 버튼을 누르면 연관분석 화면에 이름이 적용됩니다.



**연관추가**

연관분석을 추가할 수 있습니다. 연관분석 추가 창에서 사용할 탭, 연관분석 유형, 연관필드를 설정합니다. 자세한 내용은 다음 단계인 **추가 연관분석 적용** 단계를 확인하시면 됩니다.



단계 4

추가 연관분석 적용

연관분석은 계속해서 적용할 수 있습니다. 연관분석이 적용된 다음에도 다른 연관분석을 적용하려면 2단계처럼 열 제목을 클릭해서 컨텍스트 메뉴에서 연관분석을 추가하거나, 3단계에서 연관분석 컨텍스트 메뉴에서 연관추가를 할 수 있습니다.

아래 예시에서는 1day 탭의 목적지IP 필드에 연관추가를 하여 의심 IP 목록 탭의 dst\_ip 필드와 매핑하는 과정입니다.



연관분석을 추가하면 다음과 같이 연관분석 화면에 추가된 연관분석이 표시됩니다.

