### alert

입력 레코드를 이용하여 소나 이벤트를 생성합니다.

#### 문법

alert

#### 설명

alert는 컨트롤 노드에서만 사용 가능하고, 클러스터 관리자만 사용할 수 있습니다. 기본적으로 각 데이터 노드에서 실시간 룰 탐지 후 컨트롤 노드로 전송되는 이벤트를 수신하는 스트림 쿼리에 alert 명령을 설정해서 사용합니다.

중복된 이벤트가 수신된 경우 실시간 시나리오의 이벤트 축약 설정에 의해 제거될 수 있습니다. 또한, 실시간 시나리오 설정에 따라 티켓이 생성되거나 기존 티켓에 병합될 수 있습니다. 생성된 이벤트는 이벤트 메뉴에서 조회할 수 있습니다.

입력 레코드는 아래 규격을 만족해야 합니다.

입력 레코드는 다음과 같은 필드로 구성되어야 합니다:

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 이름 | 유형 | 타입 | 설명 |
| \_logger | 필수 | 32비트 정수 | 수집기 ID 식별자 |
| \_rule | 필수 | 32비트 정수 | 실시간 시나리오 ID 식별자 |
| \_time | 선택 | 날짜/시각 | 원본 이벤트 발생 시각. 값이 없거나 타입이 일치하지 않으면 입력 시점 시각으로 처리됩니다. |
| emp\_key | 선택 | 문자열 | 임직원 사번 |
| emp\_name | 선택 | 문자열 | 임직원 성명 |
| host\_ip | 선택 | IP 주소 | 사내 호스트 IP |
| src\_ip | 선택 | IP 주소 | 출발지 IP |
| src\_country | 선택 | 문자열 | 출발지 ISO 국가코드 |
| src\_port | 선택 | 32비트 정수 | 출발지 포트 |
| dst\_ip | 선택 | IP 주소 | 목적지 IP |
| dst\_country | 선택 | 문자열 | 목적지 ISO 국가코드 |
| dst\_port | 선택 | 32비트 정수 | 목적지 포트 |
| protocol | 선택 | 문자열 | 프로토콜 |
| action | 선택 | 문자열 | 대응 방식 |