#### 배치 탐지 시나리오 추가

목록에서 새 시나리오 추가 버튼을 클릭하면 시나리오 설정 화면으로 전환됩니다.



배치 탐지 시나리오 설정은 아래의 단계로 이루어집니다:

이름 입력: 배치 탐지 시나리오 이름을 입력합니다.

분류: sonar\_rule\_categories 테이블에 입력되어 관리되는 룰 그룹의 목록을 선택합니다.

메시지 입력: 이벤트 메시지 텍스트를 입력합니다. **$필드이름** 형식으로 매크로를 사용할 수 있습니다. 매크로는 로그의 지정된 필드 값으로 대체됩니다. 메시지는 티켓의 제목으로도 사용됩니다. 별도로 중복 기준 키를 설정하지 않으면, 매크로가 대체된 최종 메시지 텍스트가 중복 기준 키로 사용됩니다.

중요도 선택: 상, 중, 하 3단계 중 하나의 중요도를 지정합니다.

분석대상 기간 입력: 배치 대상 기간을 선택합니다. 쿼리문에서 $("from"), $("to") 매크로를 사용하여 대상 기간을 지정할 수 있습니다. 예를 들어 10분 선택시 쿼리문에 table $("from") to=$("to") firepower 쿼리를 입력하여 최근 10분 동안 firepower 테이블에 입력된 데이터에 대해 배치를 실행하게 할 수 있습니다.

시간 절사 단위 선택: 대상기간 선택 시 기준시간 단위를 절사할 단위를 선택합니다.

티켓 인수자 선택: 티켓 생성 시 할당받을 담당자를 선택합니다.

실행 주기 입력: CRON 문법으로 쿼리 실행 일정을 입력합니다.

알람 그룹: 알람 그룹을 지정하면, 탐지 시 알람 그룹에 지정된 계정 및 매체(SMS, 메일, 메신저)에 따라 메시지 전송을 합니다.

분석 방식 선택: 쿼리 혹은 데이터셋을 선택합니다. 쿼리 선택 시 쿼리를 직접 입력하며, 데이터셋 선택시 기존에 생성된 데이터셋 쿼리를 사용합니다.

쿼리 입력: 쿼리 분석 방식을 선택한 경우 탐지 쿼리를 입력합니다. 배치 시나리오는 메시지 혹은 중복 기준 키에 입력된 필드를 쿼리 결과의 그룹 키로 사용합니다. 쿼리 결과는 키 필드를 기준으로 정렬된 후 그룹화됩니다. 하나의 그룹은 하나의 이벤트 및 티켓을 생성하는데 사용됩니다. 메시지의 필드이름 매크로는 키 필드 값으로 대체되어 사용되고, 동일한 키 필드 값을 가진 다수의 레코드들은 티켓의 근거 자료로 취합됩니다.

설명: 배치 탐지 시나리오에 대한 설명을 입력합니다.

소명 요청 설정: 탐지시 자동으로 소명 요청 할 지를 설정합니다. 소명 시 필요한 소명대상 필드, 분류, 소명확인 계정, 마감시한 등을 설정해야 합니다.

소명대상 필드: 소명할 계정 정보가 존재하는 대상 필드를 선택합니다. 탐지가 발생될 경우 탐지된 계정으로 자동 소명 요청이 생성됩니다. 기본 값은 emp\_key입니다.

분류: 소명 분류를 설정합니다.

소명확인 계정: 소명의 2차 검토자를 설정합니다. 미설정 시, 기본 값은 "부서장 전결"이고, 이는 2차 검토자를 지정하지 않고 1차 검토자가 최종 검토자가 되는 것을 의미합니다. 1차 검토자의 경우 소명대상 필드에서 탐지된 계정의 부서장이 자동으로 지정됩니다. 만약 부서장이 존재하지 않을 경우, 상위 부서의 부서장이 자동 지정됩니다.

마감시한: 소명 처리 시한을 설정합니다. 기본 값은 7일입니다. CLI에서 'sonar.setGlobalOption explanation\_period 마감시한 (일)' 을 설정하면 해당 값이 기본 값이 됩니다.

고급 설정: 필요시 고급 설정 메뉴를 열어 티켓 분류 선택 및 중복 이벤트 제거 설정을 합니다.

티켓 분류 선택: 선택 안함 상태로 두면 티켓을 생성하지 않습니다.

중복 기준 필드 입력: 필드이름 매크로를 이용하여 중복 기준 키 문자열을 입력합니다. 매크로가 대체된 최종 중복 기준 키 문자열은 이벤트나 티켓 중복을 판정하는 기준으로 사용됩니다. 중복 기준 키를 입력하지 않으면, 매크로가 대체된 최종 메시지 텍스트가 중복 기준 키로 사용됩니다. 즉, 중복 기준 키는 메시지와 다르게 중복 기준을 설정하려고 할 때 유용합니다. 예를 들어, 메시지는 "호스트 스캔: $src\_ip에서 $count대 스캔" 으로 설정했지만, 동일 호스트에서 스캔 호스트 수($count)만 바뀌면서 이벤트나 티켓이 불필요하게 다수 발생하지 않도록 억제한다면, 중복 기준 키를 "$src\_ip" 로 설정할 수 있습니다.

중복 이벤트 제거 설정: 첫 이벤트가 발생한 후 지정된 시간 동안 동일한 이벤트가 발생하면 무시됩니다. 시간을 0으로 설정하면 비활성화됩니다.

중복 티켓 축약 설정: 첫 티켓이 생성된 후 지정된 시간 동안 동일한 티켓이 발생하면 건수만 증가시키고 무시합니다. 시간을 0으로 설정하면 비활성화됩니다.

출력 필드 순서: 쉼표로 구분된 필드 이름 목록을 지정하면 티켓 근거자료의 출력 필드에 우선 순위로 지정되어 출력됩니다.

티켓 완료 처리 방식: 중복 티켓 축약이 설정되어 있는 상태의 티켓이 완료된 경우, 축약기간 내에 발생하는 이벤트에 대한 티켓을 신규 생성할지, 완료된 티켓으로 축약할지 설정합니다. 기본 값은 축약 타이머 초기화 입니다.

쿼리 테스트: 쿼리 결과를 시뮬레이션 해볼 수 있습니다. 분석 방식 및 쿼리 입력 후 가상 실행 시간을 설정하면 시뮬레이션 쿼리가 생성되며, 쿼리를 실행하여 시나리오 결과를 시뮬레이션 해볼 수 있습니다.

예를 들어, 아래의 배치 시나리오 탐지 쿼리는 분석대상 기간 내에 동일 호스트에서 100대 이상 내부망 스캔이 발생한 경우 티켓을 발생시키고, 상세 호스트 스캔 내역을 근거자료로 생성합니다.

table from=$("from") to=$("to") firewall | fields \_time, src\_ip, dst\_ip, dst\_port, protocol| join src\_ip, dst\_port, protocol [ table from=$from$ to=$to$ firewall | search network(src\_ip, 16) == "172.20.0.0" and network(dst\_ip, 16) == "172.20.0.0" | stats dc(dst\_ip) as count by src\_ip, dst\_port, protocol | search count >= 100]