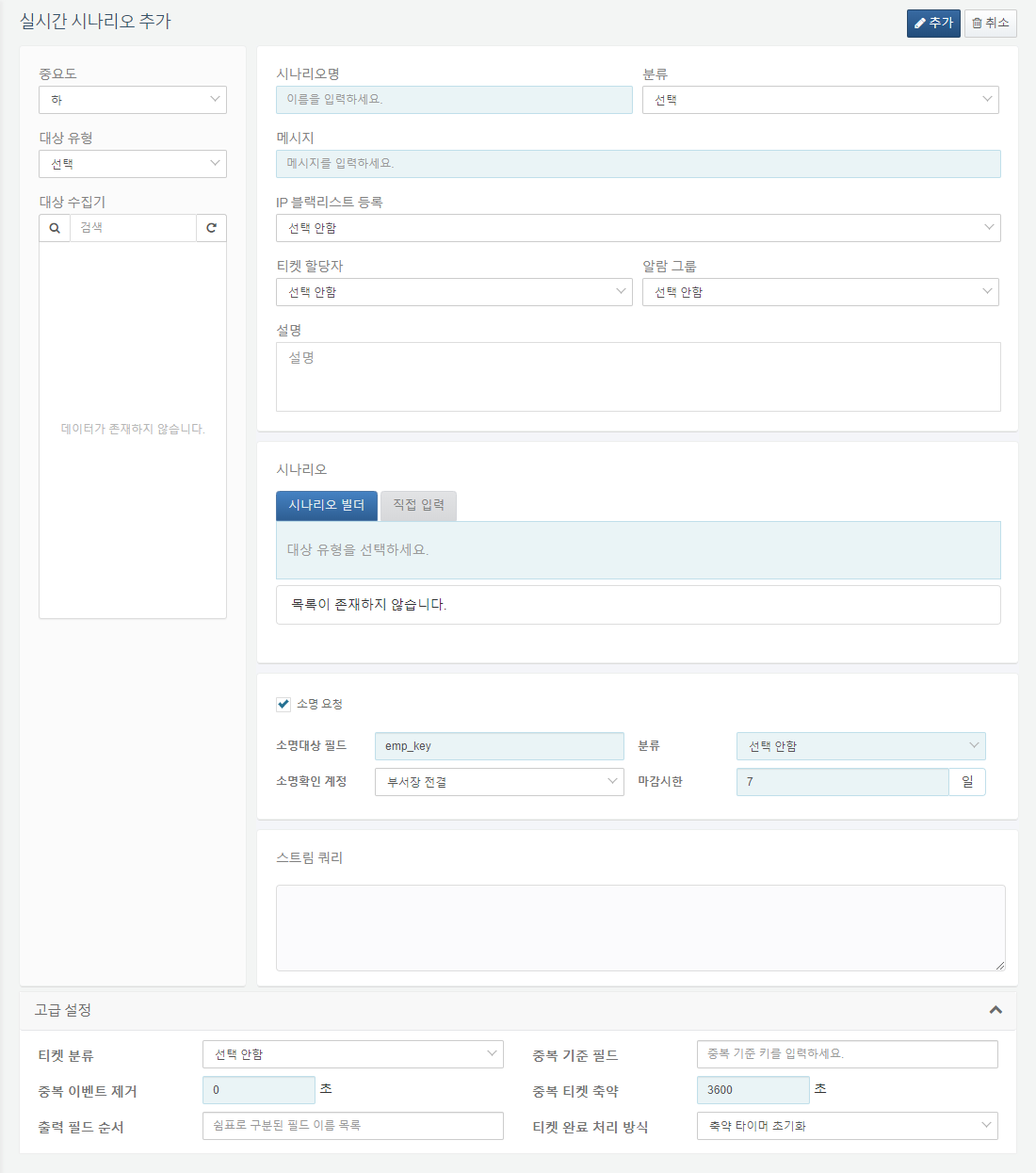
#### 실시간 탐지 시나리오 추가

목록에서 새 시나리오 추가 버튼을 클릭하면 시나리오 설정 화면으로 전환됩니다.



실시간 탐지 시나리오 설정은 아래의 단계로 이루어집니다:

중요도 선택: 상, 중, 하 3단계 중 하나의 중요도를 지정합니다.

대상 유형 선택: 선택하는 정규화 스키마에 따라, 그에 맞는 수집기 목록이 표시됩니다.

수집기 목록 선택: 실시간 탐지 시나리오를 적용할 수집기 목록을 선택합니다.

시나리오명 입력: 화면에 표시할 시나리오 이름을 입력합니다. 시나리오 이름은 향후 진단 시 참고할 수 있도록 스트림 쿼리의 설명 항목에 설정됩니다.

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.

주소 그룹 선택: 이벤트 탐지 시 출발지 IP 필드(src\_ip)를 자동으로 주소 그룹에 등록하려면, 목록에서 주소 그룹을 선택합니다. 선택 안함 상태로 두면 무시됩니다.

티켓 할당자: 티켓 할당자를 지정하면, 탐지 시 지정한 계정으로 티켓이 자동 할당됩니다.

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

설명: 실시간 탐지 시나리오에 대한 설명을 입력합니다.

시나리오 구성: 시나리오 빌더를 사용하거나 스트림 쿼리를 직접 입력하여 탐지 규칙을 설정합니다. 최상단 필터부터 아래로 내려가면서 필터링을 수행합니다. 상단의 필터를 만족시키지 못하면 하단 필터는 실행되지 않습니다. 각 필터의 실행 순서는 단위 시간당 처리량 성능에 영향을 미칠 수 있습니다. 가장 빠르고 단순한 조건을 이용하여 상단에서 관련없는 로그를 최대한 걸러내는 것이 중요합니다.

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

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 "C&C 서버 접속: $src\_ip -> $dst\_ip" 으로 설정했지만, 동일 호스트에서 다른 C&C 서버로 접속한 이벤트나 티켓이 불필요하게 다수 발생하지 않도록 억제한다면, 중복 기준 키를 "$src\_ip" 로 설정할 수 있습니다.

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.

저장: 마지막으로 저장 버튼을 클릭하여 시나리오 생성을 완료합니다.

시나리오 빌더는 GUI 방식으로 필터를 설정할 수 있도록 지원합니다. 대상 유형으로 지정된 정규화 스키마에 따라 시나리오 빌더에서 선택 가능한 필드 목록이 전환됩니다. 시나리오 빌더에서 필드를 선택하면, 선택된 필드의 타입에 따라 사용 가능한 룰 목록이 표시됩니다. 아래의 표는 필드 타입별로 사용할 수 있는 룰과 상대적인 수행 성능에 대한 설명입니다:

|  |  |  |  |
| --- | --- | --- | --- |
| 타입 | 룰 이름 | 매개변수 | 실행 부하 |
| IP | IP 주소 일치 | IP 주소 | 하 |
| IP | IP 주소가 네트워크 대역에 포함 | 네트워크 대역 | 하 |
| IP | IP 주소가 블랙리스트에 포함 | 블랙리스트 | 하 |
| IP | IP 주소가 IP 평판 DB에 포함 | 위협 인텔리전스 피드 | 중 |
| IP | IP 주소로 이벤트 연관 대기 | 이벤트 이름, 타임아웃 시간 | 상 |
| IP | IP 주소로 이벤트 연관 탐지 | 이벤트 이름 | 상 |
| IP | IP 주소로 이벤트 발생 임계치 초과 | 이벤트 이름, 임계치 | 상 |
| PORT | 포트 번호 일치 | 포트 번호 | 하 |
| PORT | 포트 범위 일치 | 시작 포트 번호, 끝 포트 번호 | 하 |
| PORT | 포트 그룹에 포함 | 포트 그룹 | 하 |
| STRING | 대상 문자열과 일치 | 비교 문자열 | 하 |
| STRING | 대상 문자열을 포함 | 포함 문자열 | 하 |
| STRING | 시그니처 패턴탐지 | 패턴 그룹 | 중 |
| COUNTRY | 국가 코드 일치 | ISO 국가 코드명 | 하 |
| DATE | 요일 매칭 | 요일 | 하 |
| DATE | 주중 매칭 |  | 하 |
| DATE | 주말 매칭 |  | 하 |
| DATE | 시간 범위 | 시작 시각, 끝 시각 | 하 |