## 대응

티켓과 소명 기능은 로그프레소 소나에서 탐지한 위협에 대해 대응하는 기능들입니다. 실시간/배치 탐지 시나리오를 통해 관제 대상 시스템에 보안위협이 의심되는 이벤트가 발생할 경우 티켓/소명을 생성할 수 있습니다. 티켓 발생 시 할당된 담당자는 보안위협에 대한 대응을 한 후 결재자에게 결재를 받아 티켓을 완료합니다. 소명 발생 시 할당된 담당자는 보안위협으로 의심되는 이벤트가 발생한 이유에 대해 소명을 한 후, 결재자는 해당 이벤트가 정상인지 보안 위반인지 판단하여 소명을 완료합니다.

티켓과 소명의 차이 중 하나는 담당자의 차이입니다. 티켓의 경우, 로그프레소 소나에 로그인할 수 있는 계정을 가지고있으며, 보안위협에 대응할 수 있는 IT 담당자가 처리합니다. 소명의 경우, 보안위협 의심 행위를 한 임직원이 소명을 작성합니다. 임직원 정보가 등록된 직원이라면 소나 로그인 계정 없이 이메일로 소명 요청을 할당받아 처리할 수 있습니다. 반대로 임직원 정보가 등록되지 않으면 소나 계정이 존재해도 소명을 할당받을 수 없습니다.

티켓은 보안팀의 대응을 요구하기 때문에, 탐지 시나리오를 조정하여 매일 처리 가능한 수준으로 티켓 생성 수량을 관리하는 것이 좋습니다.

소명 프로세스가 제대로 동작하기 위해서는 소명 템플릿이 설정되어있어야 하며 임직원 이메일 정보가 포함된 임직원 DB 정보가 입력되어야 합니다.