

단계	현업부서	보안관제	침해대응	보안진단	고객사
탐지	이상징후 신고, 내부 담당자 알림	이벤트 모니 터링, 티켓 생성, 정/오 탐 판별, 기 관 보고	로그·패킷 확보, 초동 분석 지원	취약점 점검, 유사 공격 분 석	탐지 결과 통보 확인, 협조
대응	상황 전 파, 정책 반영 승인	공격자 IP 차단, 대응 보고서 작 성, 이력관 리	상세분석·대 응방안 수 립, 대응지 원	보안정책 변 경 검토, 예외 처리 확인	최종 승인, 결 과 확인 및 재 발방지 조치