공격의 근거를 찾고,
수정의 기준을 만듭니다.

웹·API 모의해킹 · AI 서비스 보안 진단 · 외부 자산 관리

센트릭스는 시스템의 취약점을 업무 흐름과 함께 검증합니다.
보안팀이 판단할 근거와 개발팀이 실행할 조치 방향을 함께 전달합니다.

검토할 상황

출시 전 검증 / 계정·권한 구조 변경 / AI 기능 도입
외부 노출 자산과 후속 조치 관리

01

웹·API 모의해킹

사용자·조직 간 접근 권한, 인증·세션, 결제·정산 등
합의한 업무 흐름의 악용 가능성을 검증합니다.

02

AI 심화 취약점 진단

일반 웹·API 또는 LLM·AI 서비스의 범위를 선택합니다.
자동 분석과 전문가 검증으로 근거와 영향을 확인합니다.

03

SENTRIX ASM

외부 자산 발견·소유 확인부터 담당자 지정, 조치와
재확인 이력까지 관리합니다. 도입 상담 후 견적.

구성원 경력·수상·제보

보안 실무 10년 · 2025 식약처 주최 AI 레드팀 챌린지 최우수상(구성원)
국가 취약점(KVE) 제보 · 자체 보안 점검 서비스 CodeScan 운영

언급된 기관과의 제휴·후원·고객 관계를 의미하지 않습니다.

담당자가 설명하고,
개발자가 수정할 수 있도록.

확인된 결과, 추가 확인이 필요한 항목, 남은 위험을 구분합니다.

예시 F-01 / 접근 통제 / 합성 예시

다른 조직의 보고서에 접근할 수 있는 경우

재현 조건	조직 A 테스트 계정으로 로그인한 뒤, 조직 B의 보고서 식별자를 요청합니다.
확인 근거	서버의 소유권 검증 여부, 요청·응답, 역할과 영향 범위를 기록합니다. 원문 증적의 민감정보는 가립니다.
수정 방향	서버에서 사용자 조직과 리소스 소유권을 함께 검증하고, 목록·상세·다운로드 경로에 동일한 정책을 적용합니다.
재점검 기준	다른 조직의 요청은 차단되고 정상 업무는 유지되는지 합의한 계정과 경로로 확인합니다.

보고서 구성 설명용 합성 예시이며 실제 고객의 발견 사항이나 개선 성과가 아닙니다.

보안·의사결정 담당자

영향을 받는 업무와 우선순위
확인된 범위·미확인 사항·잔여 위험
조치 순서와 후속 검토 항목

개발·운영 담당자

재현 조건과 절차·요청/응답 증적
원인과 수정 방향
합의한 재점검 결과와 상태

서비스별 산출물 예시 → sentrix.co.kr/services/compare/

착수 전 합의부터
조치 후 확인까지.

대상·권한·운영 영향을 확인한 뒤 승인된 범위에서 수행합니다.

01 **대상·범위 상담**

서비스, 계정 역할, 점검할 업무 흐름과 희망 일정을 확인합니다.

02 **NDA·서면 승인**

대상·제외 범위, 허용 시간, 접근 방법과 중단 연락 체계를 합의합니다.

03 **진단·결과 검토**

합의한 시나리오로 검증하고 근거·영향·조치 방향을 설명합니다.

04 **조치·재점검**

계약에서 정한 기간·횟수에 따라 조치 결과와 잔여 위험을 확인합니다.

자료 취급

접근 담당자, 보관·삭제, 외부 AI/API 처리 여부와 데이터 전달 범위를 계약 전에 확인합니다.

비용·일정

시스템 수, 역할, API·업무 흐름, 결과 형식과 재점검 범위를 확인한 뒤 제안합니다. ASM은 도입 상담 후 견적입니다.

검토할 서비스와 희망 일정을 알려주세요.

support@sentrix.co.kr

010-8179-0854

진단 문의하기 ↗

영업일 기준 24시간 내 회신합니다. 최초 문의에는 비밀정보 없이 대상과 목적만 보내주세요.

센트릭스 · 대표 김소하 · 사업자등록번호 673-54-01057 · 통신판매업 2026-용인수지-1588