AUTONOMOUS RED TEAM PLATFORM

GILDAL

거버넌스 기반 자율 공격 보안

무엇이 악용 가능한지 증명하는 자율 모의해킹

거버넌스가 적용된 공격 보안 플랫폼입니다. 보안 특화 AI 레드팀이 **공격 전략을 스스로 수립·실행**하고, 완전한 자체 호스팅 환경에서도 계속 동작하며, **전문 모의해킹 리포트를 자동으로 생성**합니다 — 모든 위험 행위는 합의된 범위 안에 머물고 격리된 환경에 봉인됩니다.

- 자율 킬체인
- 보안 특화 AI 모델
- 범위 가드레일
- 완전 격리
- 축적되는 경험
- 리포트 자동화

GILDAL의 보장

오탐 제로

GILDAL이 보고하는 모든 취약점에는 재현 가능한 실제 악용 증거가 함께 제공됩니다. **악용할 수 없으면 보고하지 않습니다** — 그래서 팀이 오탐을 쫓을 일이 없습니다.

모의해킹은 느리고 비쌉니다.
자동화는 통제를 잃습니다.

조직은 더 넓은 공격 표면을 더 자주 점검해야 하지만, 숙련된 모의해킹 인력은 드물고 비쌉니다.
단순 스캐너는 빠르지만 **맥락 없는 오탐**을 쏟아내고, 자율 AI 공격은 **통제하기 어렵습니다**.
GILDAL은 바로 그 간극을 메웁니다.

01 — 비용

인력 의존

모의해킹은 인력과 일정에 묶여 잘해야 분기 1회. 계속 변하는 공격 표면을 따라가지 못합니다.

02 — 노이즈

맥락 없는 오탐

기존 스캐너는 시그니처만 맞출 뿐, 실제로 **악용 가능한지**는 증명하지 못합니다. 검증은 결국 사람 몫입니다.

03 — 통제

통제 불능의 자율성

자율 AI 공격은 범위를 벗어나거나 외부로 새어나갈 위험이 있고, 책임 추적과 감사가 어렵습니다.

04 — 종속

클라우드 종속

프론티어 클라우드 LLM에만 의존하면 비용·데이터 주권·격리 환경 측면의 제약이 따릅니다.

GILDAL의 해법

거버넌스가 적용된 AI 레드팀이 직접 공격을 수행하되, 모든 위험 행위는 **범위 게이트**를 통과하고 **봉인된 환경** 안에 머뭅니다. GILDAL은 **검증된 취약점**만 — 오탐 없이 — 보고하며, 각 항목에 완전한 감사 로그가 따라붙습니다.

정찰에서 증명까지, 전 과정 자율로.

01 · 정찰

공격 표면을 지도화

실제 공격자처럼 대상을 탐색 — 노출된 서비스·엔드포인트·취약 지점을 찾습니다.

02 · 공격

실제 공격을 연결

취약점을 실제 악용으로 자율 연결 — 봉인된 환경, 허가된 범위 내에서만.

03 · 재현

모든 발견을 검증

각 발견을 독립 재검증해 악용 가능함을 증명합니다. 오탐 없음.

04 · 리포트

리포트까지 자동

증거·영향·조치를 담은 규제 대응 리포트 — OWASP·CWE·CVE 매핑.

점검할수록 더 날카로워집니다

발견과 증거가 자동으로 축적되어, 지금까지 본 모든 것을 바탕으로 추론합니다 — 시간이 갈수록 더 빠르고 정교해지며, 완전한 **자체 호스팅 환경**에서도 마찬가지입니다.

클라우드

최고 탐지력

최고 수준의 탐지력으로 완전 자율 점검 — 높은 보증 수준이 필요한 공식 진단에 적합합니다.

자체 호스팅

완전한 데이터 주권

환경 내부에서만 동작하며 데이터가 외부로 나가지 않습니다. 규제 대상·망분리(에어갭) 환경을 위해 설계됐습니다.

보안 특화 자체 AI 모델

공격 보안에 특화된 GILDAL 자체 모델 — MITRE ATT&CK, CVE·CWE 카탈로그, 방대한 실제 공격 지식으로 학습되어 범용 AI가 놓치는 패턴을 인식합니다.

- MITRE ATT&CK
- CVE
- CWE
- EXPLOIT-DB

자율성과 거버넌스, 동시에.

범위 가드레일

허용 대상·도구·시간대·점검 제외일을 사전에 정의합니다. 그 밖의 행위는 시도 즉시 차단됩니다 — GILDAL은 **기본이 차단(fail-closed)**이며 절대 열린 채로 두지 않습니다.

완전 격리 (제로 이스케이프)

모든 점검은 봉인된 환경에서 실행됩니다. 트래픽은 허가된 대상에만 도달하고 그 외에는 **나가는 길도, 범위를 넘는 이동(피벗)도 없습니다**. 경계 밖은 모두 차단됩니다.

리포트 자동 생성

설명·조치 가이드·공격 표면 분석·경영진용 요약이 하나로 묶여 **규제 대응 수준의 전문 리포트**로 자동 생성됩니다.

위협 인텔 보강

실제 NVD CVE · MITRE ATT&CK · CWE 매핑과 자동 **OWASP/CWE 분류**로, 모든 발견이 경영진과 엔지니어 모두에게 익숙한 표준 프레임워크에 정렬됩니다.

멀티 타겟 캠페인

여러 대상을 순차 또는 병렬로 점검하고 캠페인 단위 리포트를 생성합니다. 한 대상이 실패해도 **나머지는 보존**되고, 실패는 별도로 보고됩니다.

콘솔 & 고객 포털

보안팀을 위한 실시간 **운영 콘솔**(세션·발견·공격 경로·실시간 활동)과 결과 전달용 **고객 포털**, 그리고 자동화가 필요할 때 쓰는 API를 제공합니다.

역량은 결국 산출물로 증명됩니다.

레드팀 진단 리포트

GILDAL 자동 생성
OWASP · CWE · CVE 매핑

2	3	5	4
심각	높음	중간	낮음

F-001	원격 코드 실행(RCE) — Tomcat manager (uid=0 root)	확인됨
F-002	횡적 이동 — 호스트 간 SSH 피벗 (deploy 계정)	확인됨
F-003	SQL 인젝션 — 인증 필요 엔드포인트	검증됨

다양한 포맷 출력

HTML · PDF · DOCX 버튼 한 번으로.

KISA 28개 항목 체크리스트

한국 진단 기준에 맞춰 자동 채점.

완전한 감사 로그

모든 행위를 기록 — 완전한 감사 추적.

이제 지휘소에 불을 켤 시간입니다.

GILDAL — 거버넌스 기반 자율 공격 보안

문의 — 준비 중