AhnLab

Data Sheet

AI 기반 공격을 방어하는 AI-Native 보안 플랫폼

공격자와 방어자 관점의 체계적인 AI 통합 보안

금융권을 시작으로 여러 산업군에서 AI발 침해 사고가 발생하고 있다. 특히, ARTEX 등 AI 에이전트가 공격에 쓰이는 것으로 나타났다. 공격자는 AI를 활용해 취약점을 빠르게 찾고 공격을 반복적으로 수행한다. AI 기반 공격의 본질은 새로운 기법이 아니라 기존 공격의 자동화와 고속화다.

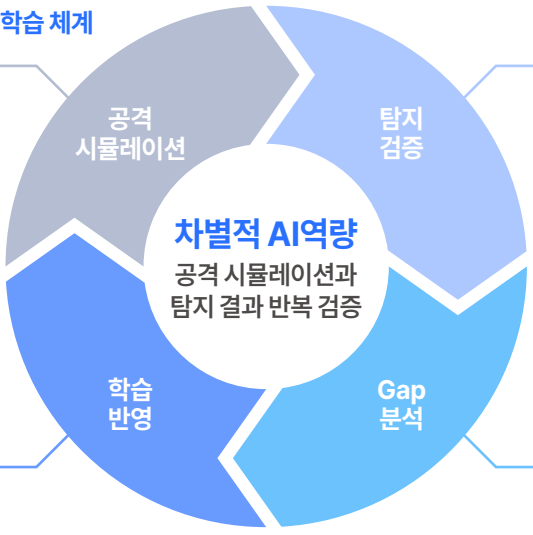
반면, 방어자의 공격 표면 식별과 탐지/차단 속도는 공격자를 따라가지 못하고 있다. 현 보안 체계에 더 많은 솔루션을 추가하는 것이 아니라, 공격 표면 발견부터 탐지, 조치 및 검증까지 운영 사이클 전체를 AI 네이티브 보안 플랫폼을 기반으로 재설계 하는데 초점을 맞춰야 한다.

Dual AI Operations – Offensive and Defensive AI

AI 위협 방어는 AI를 활용하여 공격 전 리스크 관리와 공격 후 탐지·대응이 하나의 운영 체계로 연결될 때 완성된다. 쉽게 설명하면, 공격 측면의 'Offensive AI'는 공격자의 관점으로 약점을 먼저 찾아낸다. 방어 측면의 'Defensive AI'는 방어자의 관점에서 빠르게 탐지·조사·대응하는 것이다.

안랩은 AI 네이티브 보안 플랫폼 'AhnLab AI PLUS'를 중심으로 Offensive와 Defensive AI를 결합한 '듀얼 AI 운영'을 제공한다. 여러 AI 에이전트가 협업해 모의 침투, 방어, 검증을 수행한다. AI가 위험을 이해하고 우선순위를 제시해 사람이 빠르고 정확하게 판단할 수 있도록 한다.

안랩의 AI 탐지 · 검증 · 학습 체계



01 Offensive AI
공격 수행

02 Defensive AI
보안 솔루션

03 미탐 · 개선사항 도출

04 강화 학습 · 파인 튜닝

Why AhnLab against AI-Driven Attack

- **SOC Efficiency:** AI로 분석 평균 소요 시간 60% 단축
- **Data:** 30년 이상 축적된 데이터를 학습한 자체 AI 모델과 에이전트
- **Expertise:** 오랜 기간 침해 대응과 관제를 수행해온 노하우
- **Coverage:** 공격과 방어 관점의 폭넓은 에이전트 협업 체계
- **HITL:** AI가 작업하고 사람이 결정하는 구조로 효율성과 안정성 확보
- **기술력:** 마이터 등 글로벌 평가와 다양한 고객 사례로 기술력 검증

About AhnLab AI PLUS

- 안랩의 AI 네이티브 보안 플랫폼이자 모든 AI 기술의 허브
- Offensive와 Defensive AI에 적용되어, 공격 표면 탐색, 침투 가능성 검증, 탐지·조사·대응 및 검증 연계
- 탐지·검증·학습 체계를 통해 탐지와 대응 품질을 강화하는 AI 네이티브 보안

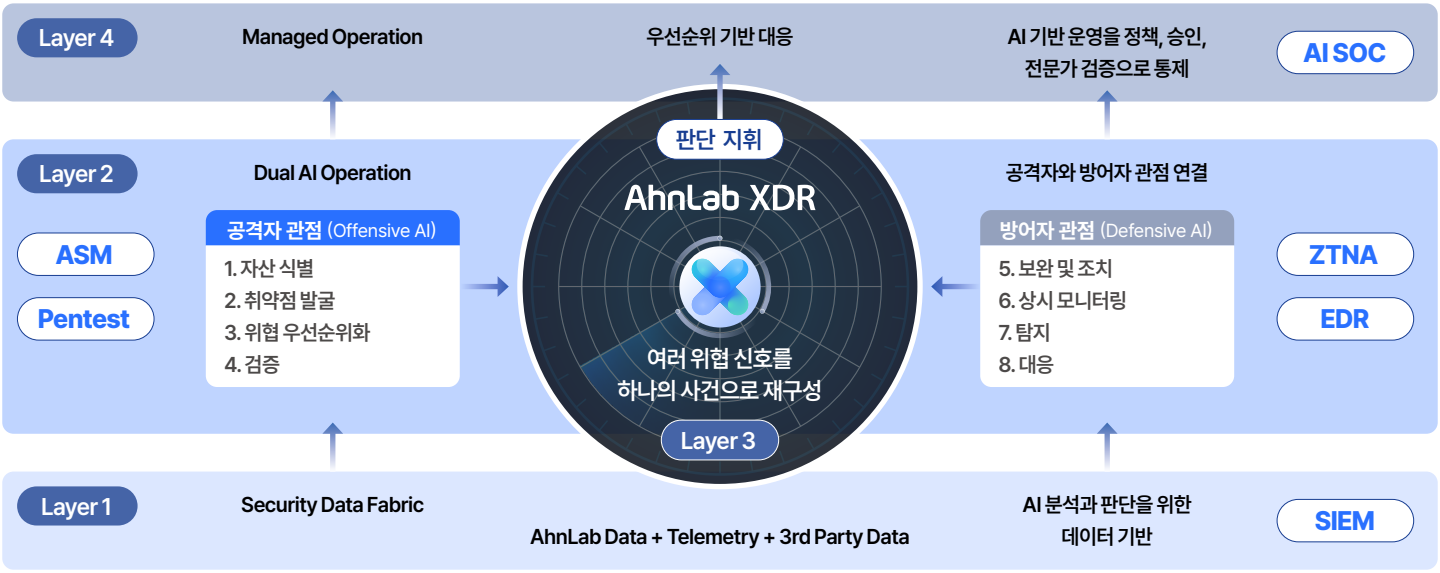
안랩의 4-Layer AI 네이티브 보안 오퍼링

ASM/AI Pentest (Offensive AI)
리스크 선제 식별 및 검증

EDR/ZTNA (Defensive AI)
공격 경로 최소화 및 탐지/대응

XDR
위협 재구성 및 우선순위 설정

AI SOC
AI 보안 운영 - 전문가 검증



Offensive AI

AhnLab AI PLUS SecOps | ASM

내·외부 공격 표면 데이터를 결합한 모니터링으로 공격자가 발견할 수 있는 노출 자산과 취약점을 식별해 분석하고 대응 우선순위를 도출한다.

내부 공격 표면 (단말 관점)

- **CVE 취약점 매핑**
  단말에 설치된 SW 중 CVE가 있는 단말 식별 및 관리
- **오픈 포트 현황**
  비정상적으로 오픈되어 있는 포트 상시 모니터링
- **EOS OS 현황**
  EOS된 OS 사용 단말을 식별해 관리하여 침해 사고 사전 예방

외부 공격 표면 (공격자 관점)

- **취약점 스캔**
  외부 노출 서버의 취약 서비스, 인증서 만료 등 점검
- **계정 유출 모니터링**
  다크웹, 텔레그램 등을 통해 유출된 조직 계정 정보 모니터링 및 관리
- **유사 도메인 모니터링**
  유사 도메인 활용 피싱 사이트 활성화 여부 등 모니터링

AI Pentest

AI 에이전트가 취약점의 실제 침투 가능성을 확인하고 조치 후 재공격해 방어 여부를 확인한다. 그리고, 보안 우선순위와 대응 방안을 제시한다.

Red Teaming
AI 에이전트가 해커 관점에서 최신 공격 기법으로 보안 사각지대 선제 식별

전방위 검증
ASM으로 미관리 자산을 전수 파악하고, 웹, 앱, 내부망, CVE 등을 전방위 검증

전문가 분석
AI 기반 자동 탐지에 안랩 전문가 분석을 더해 신뢰도 높은 맞춤형 조치 방안 제공

Defensive AI

AhnLab AI PLUS Endpoint | EDR

엔드포인트 행위 데이터를 상시 수집하고 AI가 위협 분류, 분석, 대응 권고 및 의사결정을 지원해 보안 운영의 속도와 정확도를 높인다.



AI Triage
이벤트 위험도 자동 분류 – 정·오탐 판단과 근거 제공



AI Investigation
이벤트 중 위협에 대한 심층 조사 자동 수행



AI Insight
대량의 데이터를 자동 분석해 요약 정보 제공



AI Response
AI의 대응 방안 추천 - 관리자 승인 후 원클릭 실행

AhnLab XTG | ZTNA

사용자와 단말 신뢰도 기반 세밀한 접근 통제와 정책 기반 네트워크 제어를 지원한다. 비인가 접근을 차단하고 내부 침해 확산을 최소화한다.

이상 변화 탐지
정상 패턴을 벗어난 사용자, 단말 등 식별

접근 정책 조정
접속 맥락과 위험 변화 기반 접근 권한 조정

위협 대응 연계
위협을 접근 정책과 연결해 세션 중 대응

AI-Native Operations

AhnLab AI PLUS SecOps | XDR

공격 표면 리스크와 위협 신호를 단일 사건으로 재구성하고, AI를 중심으로 우선순위 설정, 조사, 대응, 검증 등을 조율해 보안 운영을 확장한다.

우선순위 설정
AI가 여러 도메인의 이벤트의 정/오탐을 분류하고 대응이 필요한 위협 선별

확장 조사
의심 행위의 연관 리스크를 하나의 케이스로 도출해 심층 조사 및 지속 추적

대응 최적화
AI가 최적의 대응 방안을 추천하고 승인 또는 사전 정의 정책에 따라 자동 실행

AI SOC

AI의 속도와 보안 전문가의 판단력 결합이 핵심이다. 전문가 검증, 고위험 이벤트 승인 체계 개선을 통해 AI 기반 보안 운영의 신뢰도를 높인다.

MSS
시그니처 기반 신속 정확한 대응

MDR
EDR과 위협 인텔리전스 결합 및 위협 헌팅

MXDR
XDR 리스크 점수 기반 통합 맥락 분석 및 대응

Pentest-as-a-Service
웹, 모바일, 시스템, CVE, 크리덴셜 스터핑 등 포괄적인 침투 테스트 서비스

AhnLab AI PLUS Endpoint
엔드포인트 통합 보안을 제공하는 SaaS형 보안 플랫폼

AhnLab AI PLUS SecOps
AI 기반 통합 탐지-보호-대응을 수행하는 보안 운영 플랫폼

What to do: AI 공격 예방 및 대응

다음은 AI 공격에 대한 예방 방안이다. 핵심은 무엇이 노출됐는지 아는 것이다.

영역	점검 항목
노출 자산 관리	• 인터넷 노출 웹, API, 관리 페이지, 원격 접속 지점 목록화 • 쓰지 않는 서비스와 테스트 서버 외부 접근 차단 • 자산 관리 작업 담당자 지정
앱 백엔드 API	• 모든 API 요청에서 서버 측 인증과 객체 단위 인가 검증 • 앱 안에 API 키나 인증 정보를 넣지 않을 것 • 사용자당 조회 건수 제한, 비정상 반복 조회 탐지 적용
관리/업무 도구	• 관리 페이지, BI 도구, 영업지원시스템 외부 직접 접근 통제 • (불가피할 경우) 접근 IP 제한 및 다중 인증 적용 • 해당 도구가 업무 DB를 읽을 수 있는 권한 최소화
위탁 SaaS 및 공급망	• 위탁 업체가 보유한 데이터와 연결 권한 목록화 • 위탁 앱에 부여한 클라우드 권한(OAUTH 동의 등) 정기 검토 • 위탁 업체의 침해 통보 절차 계약서에 명시
계정/인증	• VPN, 원격 접속, 업무용 클라우드 계정에 MFA 적용 • 로그인 실패 반복 및 비정상 위치 접속 탐지
패치	• 인터넷 노출 요소(PHP, GITLAB, NODE.JS 등)는 취약점 공개 당일 대응 • 기술지원이 끝난 시스템 교체 계획 수립 및 외부 노출 최소화
데이터	• 보존 기간 만료된 회원, 퇴직자 정보, 개발용 임시 파일 정리
탐지/관제	• 외곽 접점 로그를 핵심 시스템처럼 수집하고 24시간 관제 • 웹 서버가 셸을 실행하는 행위 등 침해 후 활동 탐지 규칙 운영

침해가 발생했다면 다음과 같이 대응한다. 초기 대응에 따라 피해 규모가 달라진다.

단계	대응
초동 조치	• 공격 IP와 악용된 경로 차단 및 해당 서비스 격리 • 서버를 초기화하지 않고 로그, 메모리, 디스크 이미지 확보
범위 확인	• 침해 지점에 연결 DB, 내부 시스템, 위탁 업체 시스템 등 접근 흔적 추적 • 취약점 정보 공개일 이전까지의 로그를 역추적 및 점검
자격증명 조치	• 침해 경로 관련 계정, API 키, 접근 토큰 폐기 및 재발급 • 웹셸 등 지속성 확보 수단이 남아 있는지 확인
신고	• (국내) 정보통신망법에 따라 침해사고를 인지하면 24시간 이내에 과학기술정보통신부 또는 한국인터넷진흥원(KISA, 국번 없이 118)에 신고. • 개인정보 유출 시 개인정보보호법에 따라 원칙적으로 인지 후 72시간 이내에 정보주체에게 통지하고 개인정보보호위원회 또는 KISA에 신고 • 금융회사는 금융감독원 보고, 범죄 피해는 경찰청 사이버수사 부서 신고
2차 피해 방지	• 유출된 정보를 이용한 피싱, 스미싱, 계정 대입 공격이 이어질 수 있으므로 이용자에게 비밀번호 변경과 사칭 연락 주의 안내 • 공격자의 금전 요구에는 응하지 않고 수사기관과 협의

도입 효과

보안 운영 생산성 강화

3x
연간 이벤트 처리 규모

60%
분석 평균 소요 시간 단축 (MTTR 단축)

2.5x
보안 관제 효율성

원스톱 AI 네이티브 보안 구현

공격과 방어 관점 AI 운영으로
AI 보안 도전과제 원스톱 해결

업계에서 신뢰받는 기술력

MITRE | ATT&CK Evaluations
국내 유일 6회 연속 참가
Round 7 차단율 100%

SE LABS
SE Labs Advanced Security Test 최고 등급 'AAA' 획득

Gartner Peer Insights
"AhnLab XDR과 EDR은 안랩의 방대한 데이터를 기반으로 탁월한 기술력과 적응력을 제공했다."

FROST & SULLIVAN
2026년 APAC 엔드포인트 보안경쟁전략 리더십 어워드 수상

AI 사이버 위협 보안 솔루션

도입 문의 →

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901
© 2026 AhnLab, Inc. All rights reserved.

AhnLab