AI with Security, Security with AI

RAON Agentic AI Platform

라온시큐어 Agentic AI 플랫폼 라인업

make AI fun and secure

RAON

01

ONESOAR | AI 자율보안 컨트롤 타워

자연어 명령 기반 보안 운영 자동화

AI 기반 보안 운영 자동화 및 지능형 위협 대응을 위한

Agentic AI 자율보안 컨트롤 타워

자연어 보안 운영 자동화

복잡한 콘솔 설정 없이 자연어 명령만으로
최적의 보안 정책 생성 및 인프라 즉시 반영

계정 라이프사이클 자동화

임직원의 인사 생애주기(입사·퇴사) 및 조직
변경에 맞춰 시스템 접근 계정 자동 조정

이상행위 AI 탐지 및 자율 관제

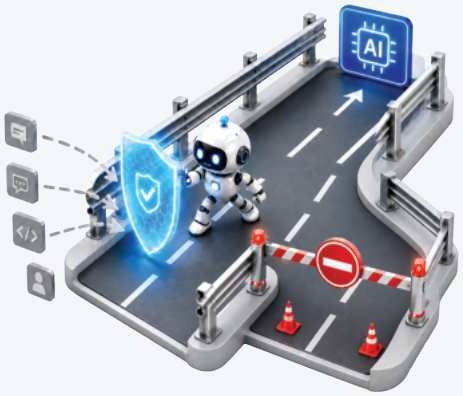
로그 분석 및 이상행위 탐지 기반으로
계정 잠금·MFA 강화·관리자 알림 등
자율 방어 체계 즉각 실행

보안 운영 최적화

전문가의 수동 개입과 반복 관제 최소화로
인프라 운영 비용 절감 및 보안 회복탄력성 강화

02

ONEShield | AI 세이프 가드레일



악성프롬프트, Jailbreak 공격 탐지

AI 에이전트의 행위·정책·신뢰 검증을 통해 기업 데이터와
업무 환경을 보호하는 **Agentic AI 세이프 가드레일**

악성 프롬프트·Jailbreak 차단

시스템 권한 탈취를 노리는 Jailbreak 시도와
악성 프롬프트 인젝션 공격 실시간 감시·차단

개인정보 식별 및 마스킹

데이터 입출력 과정에서 주민등록번호 등
개인정보(PII)와 기업 기밀 데이터를
자동 식별·마스킹 처리해 외부 유출 방지

유해 콘텐츠·정책 위반 탐지

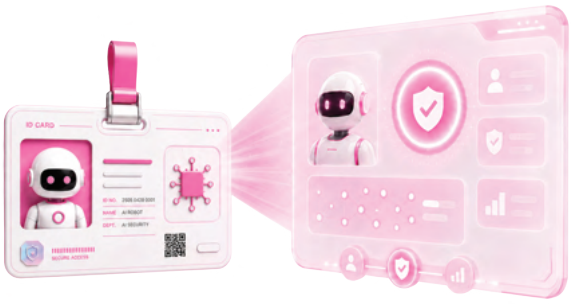
LLM 사용 시 폭력성, 선정성, 범죄 등
유해 콘텐츠 원천 봉쇄와 AI 기본법·
개인정보보호법 등 보안 정책 위반 행위 탐지

SEB 보안 브라우저 통제

복잡한 보안 프로그램 설치 없이 SEB 보안
브라우저 하나로 정보유출과 외부 위협,
화면 캡처 및 웹 유출 시도 차단

03

ONE Access | AI 신분증



AI 에이전트·로봇 권한 관리(AAM)

AI 에이전트에 고유 ID를 부여하고

권한·위임·이력을 통합 관리하는 **Agentic AI 신분증**

AI 에이전트·로봇 신분증 발급

위·변조가 불가능한 고유 ID를 부여해 생성부터 소멸까지 에이전트 신원 생애주기 관리

AI 에이전트 간 상호 인증

협업 시 상대방의 신원을 실시간 상호 인증하고 보안 채널을 형성해 인가되지 않은 비정상 에이전트의 개입 원천 차단

권한 기반 활동 범위 제어

업무 및 상황에 맞춰 필요한 최소 권한을 부여·위임하고 위협 감지 시 권한을 즉각 회수해 데이터 유출 방지

감사 추적 및 책임 귀속

모든 활동 이력을 블록체인에 영구 기록해 책임 소재를 명확히 하고 AI 기본법·금융권 감사 요구에 완벽하게 대응

04

ONE Tag | AI 데이터 라벨러

AI 학습 데이터 민감도 자동 분류

AI가 데이터의 맥락을 이해해 문서를 분류하고

보안 레이블을 자동 부여하는 **Agentic AI 데이터 라벨러**

문서 맥락 자동 분류

AI 에이전트가 데이터 맥락을 이해해 문서 등급을 정밀 자동 분류하고, 한국 국가 망 보안체계(N2SF)의 C·S·O 등급 분류 완벽 지원

지능형 자동 레이블링

대규모 데이터셋에 일관된 기준의 메타데이터와 레이블을 실시간 부여해 데이터 자산화 및 AI 학습 준비 시간을 획기적으로 단축

데이터 보호 정책 적용

자동 라벨링된 데이터 등급에 맞춰 사내 접근 권한 및 제어 정책 실시간 자동 연동

보안 거버넌스 연동(향후)

분류된 데이터 등급 기반의 접근 권한·암호화 정책 자동 매칭으로 데이터 유출 방지(DLP) 및 컴플라이언스 대응, 글로벌 표준(NIST) 기반 차등 적용

05

ONEHacker | AI 모의해커

완전 자율 AI 모의침투 수행

AI 에이전트가 공격자 관점에서 취약점을
탐지하고 검증하는 **Agentic AI 모의해커**

PTG 기반 실전 모의침투 시나리오

DEFCON 3회 우승 화이트해커팀이 설계한
PTG 기반 시나리오로 단순 스캔을 넘어
실제 업무 프로세스까지 종합 보안 점검

24시간 상시·반복 모의해킹

일회성 점검을 넘어 변화하는 환경에 맞춰
합리적인 비용으로 연간 24시간 중단 없는
상시·반복 모의침투 체계 제공

로컬·클라우드 모델 검증

국산 범용 SLM(Upstage)과 보안 특화 멀티모델
기반으로 공공·금융 로컬 모델의 제어권 탈취
위험과 민간 클라우드 모델의 보안 사각지대 검증

하이브리드 모의해킹

AI 기반 신속 자동화 점검과 글로벌 최고 수준
화이트해커의 정밀 검증을 결합해 효율성과
신뢰성을 갖춘 보안 무결성 확보

Agentic AI 자율 방어 연계 시나리오

하나로 연결되는 보안, 더 정교해지는 대응
Agentic AI 제품군의 유기적 연계를 통해 고객 환경에 맞는 자율 대응 체계를 단계적으로 확장합니다.

ONESOAR
사용자 접속 및 통제 확립
사용자 계정 상태, 접속 IP·기기 환경, MFA 인증 정보 등을 기반으로 **실시간 검증 및 통제**

ONEAccess
업무 수행 및 에이전트 신뢰 인프라 가동
분산신원증명(DID)과 검증 가능한 자격증명(VC) 기술을 기반으로 **호출된 AI 에이전트의 신원과 배정된 권한 범위를 상호 검증**

ONEShield
실시간 프롬프트 가드레일 실현
AI 에이전트와 LLM 사이의 모든 입출력 **길목을 완전히 통제**

ONEHacker
상시 방어력 검증 및 취약점 선제 대응
이상 행위의 유입 경로와 업무·서비스 등 연계 시스템 내 사각지대를 분석하여 **실시간으로 자동 모의 침투 테스트를 수행하고 추가적인 보안 조치 권고**

사용자

1. **사내 업무 시스템 · AI 기반 서비스 접근 시도**
   사용자 인증 및 MFA 등 사용자 접속 인증 & 컨텍스트 감시 시작
2. **업무·서비스 처리를 위한 각종 명령 및 AI 에이전트 호출**
   AI 에이전트 호출 시 DID·VC 기반 신뢰 검증 및 세션 권한 부여
3. **사용자 질의·명령, 비즈니스 로직 기반 AI 에이전트 실행**
   AI 에이전트 업무 처리 시 입출력 데이터에 대한 가드레일 실시간 필터링, 각종 AI 에이전트·API 등 연계 처리
4. **다양한 위협 대응 조치 후 위험 공격·취약점 분석 실행**
   위협 방식, 공격 경로, 인프라 취약점 대상 상시 모의 침투 및 검증 데이터 수집

이상 행위 및 위협 감지

ONESOAR → ONEShield + ONEAccess 연계 차단 처리
위협 탐지 시 동적 동시 차단 및 자격·권한 회수

위협·위험 징후를 실시간 탐지한 OneSOAR가
즉시 해당 사용자 세션을 강제 종료하고 계정을 잠금 처리
- OneShield에 긴급 차단 명령 전송
- OneAccess는 해당 AI 에이전트 자격증명 즉시 무효화

ONESOAR + ONETag
보안 데이터 피드백 및 자율 학습 선순환 체계 완성

- 수집된 데이터의 정제를 통해 RAG 지식베이스를 최신화하고 **AI 보안 탐지 모델과 SLM을 고도화**
- 고도화된 모델의 지속적인 재투입으로 방어 엔진이 더 높은 정확도로 위협을 탐지할 수 있도록 **스스로 진화하는 자율 선순환**

5. **다양한 위협과 이상행위 로그, 보안 가드레일 처리, 모의침투 등 데이터 학습**
   위협·방어 데이터 자동 정제 및 레이블링

라온시큐어(주)
본사 서울특별시 영등포구 여의대로 108, 파크원타워2 47-48층 (여의도동)
대표전화 02-561-4545 | **Fax** 02-565-5350 | **문의** salesplan@raon.com
홈페이지 www.raon.com

Scan QR code