SECURE AIR

보안 분석을 넘어,
보안 운영의 새로운 기준

Secure AIR는 XAI(eXplainable AI) 기반 AI CERT와 생성형 AI(LLM) 기술을 결합하여 보안 이벤트 정·오탐 분석부터 보안 운영 자동화까지 지원하는 **차세대 통합 보안 플랫폼**입니다.
MSA(Microservice Architecture) 기반 설계로 독립 운영이 가능한 단독형과 기존 Secure Orchestra 플랫폼에 연동하는 확장형을 모두 지원하여 고객 환경과 운영 전략에 따라 유연하게 도입할 수 있습니다.

핵심가치

XAI 보안 분석으로 신뢰성 확보

설명 가능한 AI (XAI) 기반
보안 분석

정·오탐 최소화 및 운영 효율성 향상

반복적인 분석 업무를 자동화하여
운영 부담 감소

직관적인 대화형 보안 운영 환경

생성형 AI 기반으로
보안 데이터를 직관적으로 활용

XAI 기반 AI CERT

Secure AIR는 인공지능 정오탐 분석 모델러 R을 통해 AI의 판단 근거를 명확히 제시하는 설명 가능한 AI (XAI) 기반의 보안 분석으로 보안 운영의 정확도와 신뢰성을 향상시킵니다.

R1
웹공격 정·오탐 분석모델

- 웹 공격 탐지 이벤트에 대한 정·오탐 자동 분석
- 요청 패턴, 공격 특성, 탐지 근거에 대해 XAI 기반 분석
- 웹 보안 운영의 정확도 및 신뢰도 향상

R2
멀웨어 페이로드 정·오탐 분석모델

- 멀웨어 페이로드 기반 탐지 이벤트 분석
- 정상 / 악성 판단 근거의 명확한 시각화
- 지능형 분석으로 룰 기반 탐지의 한계 해결

R3
네트워크 패킷 정·오탐 분석모델

- 네트워크 패킷 흐름 및 행위 기반 정·오탐 분석
- 이상 행위 발생 원인을 맥락적으로 해석
- 네트워크 보안 이벤트 대응 속도 향상

생성형 AI(LLM) 기반 Agentic SOAR

Secure AIR는 생성형 AI를 기반으로 하는 **Agentic SOAR**를 통해 보안 운영의 자동화 수준을 한 단계 더 끌어 올립니다. 보안 담당자의 지시를 기다리는 단순 자동화를 넘어 **AI 에이전트가 상황을 이해하고 판단하여 능동적으로 대응**합니다.

*SOAR: Security Orchestration, Automation and Response

대화형 보안 제어
자연어 대화로 실시간 보안 현황 파악 및 대응 작업 즉시 지시

자율 대응 에이전트
이벤트 분석 결과에 따라 최적의 대응 시나리오 자동 실행

지능형 운영 가이드
운영에 필요한 매뉴얼과 설정 정보 실시간 탐색

자연어 로그 분석
복잡한 쿼리 없이 자연어로 로그 검색 및 분석 결과 요약

데이터 기반 인사이트
로그와 인시던트 종합 분석으로 조치가 시급한 대응 우선순위 제시

정책 관리 자동화
악성 IP 등록 및 방화벽 정책 변경·적용 전 과정의 자동화

고급 인시던트 분석 기능

Incident 통합 및 연관분석
산재된 다수의 보안 이벤트를 단일 Incident로 통합해 공격 흐름과 위협 시나리오를 한눈에 파악

시맨틱 기반 맥락 분석
이벤트의 의미와 관계를 이해하여 공격원인, 영향 범위, 위협 수준을 직관적으로 도출

지능형 대응 판단지원 보안
담당자의 상황 인식을 돕고 최적의 대응 판단을 지원하는 고도화된 기능 단계적 제공

Secure AIR 도입 효과

SPEED — 대응 시간 극대화
- MTTR 단축 : 위협 탐지 즉시 분석 에이전트 가동으로 신속한 조치
- 실시간 리포팅 : LLM 기반의 즉각적인 공격 의도 파악 및 보고서 생성
- 원-클릭 대응 : 자연어 명령을 통한 복잡한 보안 워크플로우 즉시 시행

Efficiency — 운영 효율성 최적화
- 오탐(False Positive)제거 : 알람 필터링 및 실제 위협에 집중
- 리소스 재배치 : 단순 반복 업무 AI, 전문가는 핵심 전략 업무에 집중
- 알람 피로도 해소 : 무분별한 보안 알람 문제를 근본적으로 해결

Intelligence — 지능형 자율 운영
- 자율형 보안 : 상황별 스스로 판단하고 대응하는 능동형 체계로 전환
- 최적 플레이북 : 인시던트 심각도를 판단, 최적의 대응 시나리오 제안
- 실시간 학습 : 제품 매뉴얼 및 최신 위협 정보를 학습, 유연한 대응 환경 구축

Visibility — 의사결정 및 가시성
- 공격 흐름 통합 : 개별 이벤트를 하나의 공격 스토리라인으로 시각화
- 데이터 기반 판단 : 객관적 분석 데이터를 통한 신속하고 정확한 의사결정 지원
- 자연어 인사이트 : 로그 통계 및 분석 결과의 요약으로 명확한 보고 근거 마련

서울특별시 강동구 고덕비즈밸리로 2가길 67(고덕동 휴네시온 타워) 7층
Tel. 1833-9195 | **E-mail.** support@securesystems.co.kr | www.securesystems.co.kr

SECURE SYSTEMS