SOMANSA

바이러스 불러틴 VB100 인증 A+ Microsoft MVI 보안 파트너

Privacy-i AIDR NEW

AI 에이전트 위협 대응 · 데이터 유출통제 솔루션

소만사의 Privacy-i AIDR은 **AI 에이전트에서 발생하는 차세대 공격에 대응**하기 위한 솔루션입니다.
기존 EDR의 엔드포인트 위협 탐지·대응 역량에, DLP와 AI 에이전트 상호작용을 보호하는 AIDR을 결합하여
임직원 PC부터 생성형 AI까지 **새로운 비즈니스 환경의 보안 가시성과 대응 체계**를 제공합니다.
Privacy-i AIDR은 최신 보안 신기술을 선제적으로 적용한 **국내 최초 AI 에이전트 보안 솔루션**입니다.

1 AI 에이전트 오남용과 자율 실행 위협 통제

- 프롬프트 인젝션, 비인가 명령, 개인·기밀정보 노출 등 AI 에이전트의 자율 실행 과정에서 발생하는 위협을 탐지하고 차단. 대화는 메신저 형태로 저장되어 전후 맥락을 직관적으로 파악
- AI 에이전트의 데이터 접근, API 호출, 인증 이벤트 등 작업 내역을 추적하고 정상 범위를 벗어난 행위를 탐지 및 차단. 모든 행위에 대해 감사 로그 저장

2 AI 업무 환경의 데이터 유출 통제

- 조직 내 비인가 AI 에이전트, AI 서비스, MCP서버 등을 자동 식별하고 (Shadow AI) 사용자·부서별 인가된 AI 자산과 사용 현황을 관리
- 시장 1위 자사 DLP 기술력을 적용하여 프롬프트에 포함된 개인정보, 민감정보, 소스코드 등을 탐지하고 정책에 따라 차단하거나 비식별화하여 데이터 유출을 방지

국내 최대 AI 커버리지

3대 AI 활용 영역을 통제하는 통합 AI 보안 체계

AI 에이전트 자율행위 모니터링 및 차단

AI 에이전트의 데이터 접근과 내부망/외부망에서의 API 호출 등 모든 수행 작업을 추적하고 정상 범위를 벗어난 행동을 차단

임직원 생성형AI 사용 모니터링 및 차단

사진·문서 등 전송유형별 통제 및 내용 기반 DLP를 활용한 프롬프트 내 개인정보, 민감정보 탐지 및 차단하고 비식별화

개발자 AI에이전트 사용 모니터링 및 차단

코드 편집기에 내장·연동된 AI 플러그인과 터미널 환경에서 전송되는 소스코드, 자동완성 등 AI 개발 행위와 취약점을 통제

기능

에이전트 실행 현황 및 프롬프트 내역 실시간 모니터링

- 임직원이 사용하는 AI 에이전트, AI 서비스에 대한 사용 현황을 실시간으로 통계
- 생성형 AI 서비스와의 모든 대화기록을 저장하고, 사용자 질의와 AI 응답에 포함된 민감정보는 대체하여 비식별화
- 파일 접근, 네트워크 통신 모니터링을 통한 비정상 명령 실행을 감지하고 선제적 차단

프롬프트 공격 및 비정상 행위 실시간 차단

- 프롬프트 인젝션, 탈옥, 하이재킹, 비인가 명령, 개인정보·민감정보 입력 및 전송여부 탐지 및 차단
- 프롬프트 인젝션 : AI에게 악의적인 지시를 입력해, AI가 공격자의 명령을 따라 정보를 유출하도록 하는 공격
- 탈옥 : 역할극, 반복 명령 등으로 AI에 설정된 보안 정책을 우회하여 금지된 답변이나 행동을 이끌어내는 공격
- 탐지 저장된 개인정보내역은 마스킹 처리되어 2차 유출 방지

조직 내 비인가 AI(Shadow AI) 탐지 & 사용자별 AI 자산 식별

- 조직에서 허용하지 않은 AI 에이전트, 서비스, MCP서버 등을 식별 (모델별 세부 통제 가능)
- 매일 수십 개씩 새롭게 등장하는 생성형 AI 서비스를 식별하고 선제적 접근 차단
- 부서, 사용자, 에이전트별 사용 중인 AI 자산과 인가 여부를 가시화하여 오남용 현황 실시간 관리

권한별 접속 통제 정책으로 임직원 오남용 최소화

- 허가받은 임직원은 AI 에이전트 및 AI 서비스 사용 가능
- 승인된 AI 에이전트에 한정하여 특정 부서, PC에서의 실행을 허용
- 비인가 또는 미분류 AI를 사용할 경우 실행 차단 및 관리자 알림