정보관리기술사 데일리 다이제스트

2026-10-05 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE AI 정보보안	**금융권 해킹서 AI 공격도구 'ARTEX' 정황 포착** **근거** MITRE ATLAS (AI 위협 전술 프레임워크) · AI 공격자동화 실증 사례 · dailysecu.com/news/articleView.html?idxno=208724	ARTEX · AI 공격자동화 · 금융권해킹 · 위협인텔리전스
국제	AI SE 인공지능	**AI 보안엔진 OpenAPPA, 유출 공격 0% 차단** **근거** OWASP LLM Top 10 (LLM01: Prompt Injection) · 에이전트 보안 벤치마크 신기록 · infoq.com/news/2026/10/open-APPA-zero-security-breach/	OpenAPPA · 프롬프트인젝션 · 데이터유출 · AI TRiSM
공공·정책	LAW AI 법·규제	**개인정보위, AI시대 개인정보 활용방안 의견수렴** **근거** 「개인정보 보호법」 · AI시대 개인정보 정책 방향 공론화 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttId=12550	개인정보위 · AI데이터활용 · 공론화 · 개인정보보호법

2. 오늘의 토픽 — 공격형 AI 에이전트(Offensive AI Agent) 기반 자동화 사이버공격

AI SE LAW | 출제 예상: **2교시** | 근거: **MITRE ATLAS (AI 시스템 위협 전술 프레임워크)**

2-1. 개념 및 정의

정찰·침투·전파 등 공격 체인을 자율 수행하는 AI 기반 공격 자동화 도구. 공격자의 생산성과 확산 속도를 높여 탐지·대응 시간을 단축시키는 기술.

2-2. 등장 배경

국내 금융권 연쇄 해킹 공격 인프라에서 AI 기반 침투테스트 도구 'ARTEX' 흔적이 다수 포착된 사건. 14개국 359개 고유 IP에서 동일 도구 관련 정황이 확인되며 공격 자동화의 전 지구적 확산 우려 고조.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
공격 자동화 요소	자율 정찰, 익스플로잇 체이닝, C2 자동화	공격 체인 단계별 AI 자율 수행 메커니즘
탐지·방어 기술	이상행위 탐지(UEBA), 위협 인텔리전스, AI TRiSM	AI 공격 패턴 식별 및 리스크 관리 체계
거버넌스·법제	비인간 신원관리(NHI), 망분리, 사고 보고 의무	AI 공격 주체에 대한 책임·통제 체계

2-4. 시험·실무 관점

- [SE 연계] AI 공격자동화 대응 EDR·NDR 탐지체계 설계
- [LAW 연계] AI 공격 주체 특정과 사고보고·책임귀속 쟁점
- [AI 연계] 공격·방어 양면의 Agentic AI 이중용도 리스크

답안 필수 키워드 — Offensive AI Agent / ARTEX / 공격 자동화 / AI TRiSM / MITRE ATLAS