정보관리기술사 데일리 다이제스트

2026-11-22 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	LAW SE 법·규제	**전자금융기반시설 취약점 점검 반기 1회 강화** **근거** 「전자금융감독규정」 일부 개정안 · 점검 주기·범위 확대 규제 변화 · dailysecu.com/news/articleView.html?idxno=209648	전자금융기반시설 · 취약점 평가 · 업무지원 시스템 · 중계 서버
국제	SE AI 정보보안	**AI 에이전트 기반 제로데이 자율 탐지·루트 탈취** **근거** OWASP Top 10 for LLM Applications · 공격 자동화 시대 방어 패러다임 전환 · bleepingcomputer.com/news/security/hackers-use-autonomous-ai-tool-cairn-to-find-zero-day-take-over-server/	자율 AI 에이전트 · 제로데이 · 침투테스트 프레임워크 · MONAI Label
공공·정책	LAW IM 법·규제	**아동·청소년 의견 반영 개인정보 보호정책** 이해관계자 참여형 개인정보 거버넌스 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttId=12654	아동·청소년 개인정보 · 정책 참여 · 개인정보위

2. 오늘의 토픽 — 자율 AI 에이전트 기반 공격(Agentic Offensive AI)

SE AI SW LAW | 출제 예상: **2교시** | 근거: **OWASP Top 10 for LLM Applications**

2-1. 개념 및 정의

자율 AI 에이전트가 취약점 탐색·악용·권한상승을 사람 개입 없이 반복 수행하는 공격 방식. 공격 속도·규모 확대와 탐지 윈도 단축 유발.

2-2. 등장 배경

AI 침투테스트 프레임워크를 이용한 의료영상 서버 제로데이 탐지 및 루트 탈취 사례 확인. Bell Canada 침해에서 에이전틱 위협 행위자 공식 언급.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
공격 자동화	자율 정찰, 취약점 발굴, 익스플로잇 생성	사람 없이 약 하루간 적응형 반복 공격
방어 체계	AI SecOps, 자동 패치, 이상행위 탐지	머신 속도 대응을 위한 탐지·대응 자동화
통제 원칙	제로트러스트, 최소권한, 에이전트 감사로그	에이전트를 비신뢰 실행주체로 간주하는 통제

2-4. 시험·실무 관점

- [AI 연계] 에이전트 자율성 수준별 위험 분류와 감독 체계
- [SW 연계] 오픈소스 취약점 선제 발굴·패치 파이프라인 단축
- [LAW 연계] 침해사고 신고·책임 체계의 자동화 공격 대응

답안 필수 키워드 — Agentic AI / 자율 침투테스트 / 제로데이 / 머신 속도 방어 / 제로트러스트