정보관리기술사 데일리 다이제스트

2026-11-04 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	AI SE IM 인공지능	**핵심 R&D 조직의 외부 생성형 AI 사용 일시 중단** 외부 AI 경유 핵심기술 유출 통제 사례 · etnews.com/20261103000455	섀도 AI · 기술 유출 · DLP · AI 사용통제
국제	SE AI DS 정보보안	**LLM 접근권한 탈취(LLMjacking)와 클라우드 과금 피해** **근거** OWASP Top 10 for LLM Applications (Unbounded Consumption) · AI 자원 탈취의 신규 공격 유형 · bleepingcomputer.com/news/security/google-llmjacking-attacks-rack-up-1-million-in-cloud-ai-charges/	LLMjacking · API 키 탈취 · 비용 폭증 · FinOps
공공·정책	LAW SE AI 법·규제	**사전예방 중심 개인정보 보호체계와 AI 보안 대응** **근거** 「개인정보 보호법」 · 사후 제재에서 사전 예방으로의 정책 전환 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttId=12607	사전예방 · AI 보안 · 개인정보 보호체계 · 책임성

2. 오늘의 토픽 — LLMjacking (LLM 접근권한 탈취)

SE AI DS | 출제 예상: **1교시** | 근거: **OWASP Top 10 for LLM Applications (Unbounded Consumption)**

2-1. 개념 및 정의

탈취한 API 키·클라우드 자격증명으로 LLM 자원을 무단 사용하는 공격 기법. 피해 조직에 연산 비용을 전가하고 모델 접근권을 재판매하는 수익화 구조.

2-2. 등장 배경

고가 GPU 추론 자원의 공격 수익성 증대와 AI 서비스 도입 확산. 일 10만 달러 초과 과금 사례 보고에 따른 비용 기반 보안 위협 부상.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
침투 단계	API 키 노출, 자격증명 탈취, 역프록시	소스·설정 유출 키의 모델 호출 권한 획득
악용 단계	모델 접근권 재판매, 고비용 모델 호출	피해 조직 과금 전가와 불법 수익화
방어 단계	키 단기수명화, 쿼터·예산 경보, 호출 이상탐지	최소권한과 사용량 기반 조기 차단

2-4. 시험·실무 관점

- [SE 연계] 비인가 호출에 대한 최소권한·키 수명주기 관리
- [AI 연계] 모델 호출 로그 기반 이상 사용량 탐지
- [DS 연계] 클라우드 과금 가시성(FinOps)과 쿼터 통제

답안 필수 키워드 — LLMjacking / API 키 탈취 / Unbounded Consumption / 쿼터 통제 / FinOps