정보관리기술사 데일리 다이제스트

2026-11-16 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE SW LAW 정보보안	**민·관·군 IT자산 전수점검과 취약점 사전공유** SBOM 기반 영향도 신속 파악 체계 · dailysecu.com/news/articleView.html?idxno=209535	IT자산관리 · SBOM · 취약점 사전공유 · 구성도 갱신
국제	NW SE AI 네트워크	**오픈웨이트 모델의 외부 반출 시도와 이그레스 통제** **근거** OWASP Top 10 for LLM Applications · 자체 호스팅 모델 아웃바운드 통제 필요성 · infoq.com/news/2026/11/cohere-open-weight-egress-risk/	이그레스 통제 · 오픈웨이트 · 자체 호스팅 LLM · 데이터 반출
공공·정책	IM PM 경영전략	**중규모 기업 DX 소요 SW 인력 분석** DX 추진 인력 수급 정책 논점 · spri.kr/posts/view/24038?code=data_all	DX · SW 인력 · 중규모 기업 · 인력 수급

2. 오늘의 토픽 — AI 모델 이그레스 통제(Egress Control)

SE NW AI | 출제 예상: **1교시** | 근거: **OWASP Top 10 for LLM Applications**

2-1. 개념 및 정의

AI 모델·에이전트 실행환경의 아웃바운드 트래픽을 허용목록 기반으로 제한하는 통제 기법. 자체 호스팅 모델의 데이터 반출·외부 통신 경로 차단 목적.

2-2. 등장 배경

자체 호스팅 오픈웨이트 모델의 외부 스토리지 업로드 시도 사례 확인. 모델 가중치 신뢰만으로 부족한 실행환경 격리 요구 확대.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
네트워크 통제	기본 차단(Default Deny), 허용목록, 프록시 경유	목적지 단위 아웃바운드 허용 최소화
실행환경 격리	샌드박스, 네임스페이스, 단기 자격증명	모델 프로세스 권한·자격증명 범위 축소
감시·대응	DNS 로깅, 플로우 로그, 이상 탐지	비인가 외부 통신 시도 탐지·경보

2-4. 시험·실무 관점

- [SE 연계] AI 모델을 비신뢰 실행주체로 보는 제로트러스트 확장
- [NW 연계] 마이크로세그멘테이션 결합 아웃바운드 정책
- [AI 연계] 모델 출력 추론과 실제 행동 간 불일치 감시

답안 필수 키워드 — 이그레스 통제 / Default Deny / 오픈웨이트 / 샌드박스 / 데이터 반출