정보관리기술사 데일리 다이제스트

2026-10-03 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE AI 정보보안	**AI 자율침투 공격, 금융권 연쇄 개인정보 유출 사고** **근거** OWASP API Security Top 10 · AI 공격의 API 인증허점 악용 확산 · dailysecu.com/news/articleView.html?idxno=208718	API 권한검증 · 자율침투 · 제로트러스트 · 금융권해킹
국제	DS SE 디지털서비스	**AI 에이전트 권한을 OCI 이미지로 표준화** **근거** OCI(Open Container Initiative) 이미지 규격 · AI 에이전트 권한 체계의 컨테이너 표준화 시도 · infoq.com/news/2026/10/docker-sandbox-ai-agent/	OCI 이미지 · 에이전트 샌드박스 · CNCF · 컨테이너 격리
공공·정책	IM LAW 경영전략	**공공기관 사이버보안 징계, 기관장 책임 강화** 공공기관 보안사고 책임을 경영진 차원 격상 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttId=12548	기관장 책임 · 징계기준 · 거버넌스 · 공공보안

2. 오늘의 토픽 — AI 에이전트 샌드박싱(Agent Sandboxing)

DS SE OS | 출제 예상: **2교시** | 근거: **NIST SP 800-207 (Zero Trust Architecture)**

2-1. 개념 및 정의

AI 에이전트의 실행 권한·자원 접근범위를 OCI 이미지로 패키징해 격리 구동하는 경량 샌드박싱 기법. 에이전트별 권한을 이식 가능한 표준 포맷으로 고정해 과다권한·기능충돌을 차단하는 목적.

2-2. 등장 배경

에이전틱 AI 확산으로 과다권한·프롬프트 인젝션발 권한남용 위험 부상. Docker가 샌드박스 명세를 CNCF에 기부하며 에이전트 권한의 업계 표준화 논의 본격화.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
격리 기술	OCI 이미지, microVM, 컨테이너 런타임	에이전트 실행환경을 표준 이미지로 격리 구동
권한 통제	최소권한, 권한 매니페스트, 정책엔진	접근 가능 자원·API 범위를 선언적으로 제한
거버넌스 표준	CNCF, OCI 스펙, Non-Human Identity	비인간 신원 기반 에이전트 통제 체계 표준화

2-4. 시험·실무 관점

- [SE 연계] 제로트러스트 비신뢰 실행주체로서 에이전트 접근통제 설계
- [OS 연계] microVM·컨테이너 런타임 격리수준과 성능 트레이드오프

답안 필수 키워드 — 에이전트 샌드박싱 / OCI 이미지 / 제로트러스트 / Non-Human Identity / CNCF