

정보관리기술사 데일리 다이제스트

2026-09-22 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	AI SE 인공지능	테니엄·엔트로픽, AI 코드취약점 선제탐지 근거 NIST SP 800-218 (SSDF) · 프론티어 AI 보안 실증 사례 · dailysecu.com/news/articleView.htm l?idxno=208566	AI취약점탐지 · Agentic AI · DevSecOps · 프론티어모델
국제	LAW DS 법·규제	구글, 위치정보 GDPR 위반 4.03억유로 과징금 근거 GDPR(EU 일반개인정보보호규정) · 위치정보 규제 위반 대형 제재 · thehackernews.com/2026/0 9/google-fined-403-million-over-gdpr.html	GDPR · 위치정보 · 개인정보보호 · 과징금
공공·정책	LAW DS AI 법·규제	개인정보위, AI 데이터혁신 거점 추가지정 근거 개인정보위 규제 샌드박스(개인정보 이노베이션 존) 제도 · AI 데이터 활용 규제특례 확대 · pipc.go.kr/ np/cop/bbs/selectBoardArticle.do?bbsId=BS07 4&mCode=D010030000&nttId=12520	개인정보이노베이션존 · 규제샌드박스 · AI데이터활용 · 가명정보

2. 오늘의 토픽 — AI 에이전트 기반 자동 취약점 탐지(Autonomous Vulnerability Research)

AI SE SW | 출제 예상: 2교시 | 근거: NIST SP 800-218 (SSDF), OWASP Top 10 for LLM Applications

2-1. 개념 및 정의

프론티어 AI 모델이 소스코드를 자동 분석해 취약점을 선제 발굴하는 보안 기법. 수동 코드리뷰의 속도 한계를 보완해 패치 대응시간을 단축시키는 목적.

2-2. 등장 배경

구글·엔트로픽 등 빅테크가 프론티어 모델을 실전 보안업무에 투입하는 사례 확산. AI 에이전트의 자율 실행권한 확대에 따른 오탐·오남용 통제 필요성 대두.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
핵심 기술요소	LLM 코드분석, 자동퍼징, 정적/동적분석 통합	소스코드 취약점 자동 스캐닝·패치안 생성
대표 프로젝트	Project Glasswing, Big Sleep, Aardvark	프론티어 모델 기반 실전 취약점 발굴 사례
리스크 통제요소	휴먼인더루프, 승인경계, 오탐검증	AI 탐지결과 신뢰성 검증 및 오남용 방지

2-4. 시험·실무 관점

- [SE 연계] AI 탐지결과 오탐 검증과 책임소재 규명 체계 설계
- [SW 연계] CI/CD 파이프라인 내 AI 정적분석 자동화 통합방안
- [AI 연계] 에이전트 AI 자율실행권한과 승인경계 설계 원칙

답안 필수 키워드 — AI 취약점탐지 / Agentic AI Security / DevSecOps / Human-in-the-loop / 프론티어 모델