이현재 Hyunjae Lee

정보보안 엔지니어 · AI 보안

hyunjae@kaist.ac.kr
hyunjae-lee.github.io
github.com/hyunjae-lee · linkedin.com/in/hyunjaedev
대전

AI 보안과 현장 보안 운영이 만나는 지점에서 일합니다. 국가정보원 N2SF 구성도에 대응하는 **LLM 가드레일 게이트웨이**를 연구 프로젝트의 책임자로 구현·실증했고, 교내 웹사이트의 **취약점 정기 점검**과 **인증서 자동화**를 운영합니다. 그전에는 국정원·과기정통부와 함께 **연 100건 이상의 보안성 검토**를 이끌었고, 약 USD 130M 규모 차세대 정보시스템 구축의 핵심 실무를 맡았습니다.

경력

KAIST 기술원 — 2020 — 현재

정보보안팀 · 웹 보안 / AI 보안 — 2026.07 — 현재

- **생성형 AI 가드레일 실증 연구 연구책임자**(3인, 연구 프로젝트 완료·기관 운영 미적용) — 송신 8·수신 6단계 검사, RAG 권한 통제, 카나리아 토큰. 평가셋 205문항과 배포 게이트로 공격 미탐 30%→0%, 정상 오차단 2.6%→0%, 검사당 6ms(GPU 없음). OWASP LLM Top 10 대응.
- **교내 웹 취약점 정기 점검** 운영 — 계획 대상 100% 점검, 상용 스캐너 공백은 nuclei 자체점검으로 해소, 취약 사이트 담당자 개별 조치 안내·재점검.
- **인증서 자동화 체계** 설계·구축·운영 — 명령 한 줄 ACME 설치, 자가 업데이트 에이전트, 실제 서비스 중인 인증서 검증, 80번 포트를 열 수 없는 서버용 DNS-01 인증. 인증서 만료 0건.
- 셀프서비스 보안포털 설계, 악성 URL IoC 판정 기준 수립, KISA 가이드 기반 서버 보안 기준 47항목 자동 판정 설계, WAF 운영.

정보보안팀 · 거버넌스 — 2025.07 — 2026.07

- AI·클라우드 서비스 포함 주요 정보화사업 **보안성 검토 연 100건 이상**(국정원·과기정통부 협력, 국가정보원 사이버보안 기본지침 기반).
- 과기정통부 정보보안·개인정보 감사 대응 주도 — 원인 분석·이의신청·보완자료로 **기관 평가 등급 상향**. 전 부서 실태점검·불시감찰, 매체 보안, 실무자 교육.

정보개발팀 · 학사 시스템 — 2020 — 2025.07

- 약 USD 130M·3년 **차세대 통합정보시스템** 학사 모듈 핵심 실무 — 졸업요건 1,400건 이상 현행화, 전환기 졸업 2,000명 이상 무중단 처리 (KAIST 특별표창).
- 학사 모듈 **보안·개인정보 보호** — 역할별 권한·접근통제 설계, 개인정보 암호화·마스킹, 개인정보 영향평가·접속기록 반영, 오픈 전 취약점 조치·시큐어코딩.

TmaxSoft 연구원 — 2020.01 — 06

- Spring 기반 엔터프라이즈 제품 개발, Docker·Kubernetes 클라우드 네이티브 전환.

Head Start (미국 새너제이) 데이터 사이언티스트 인턴 — 2019.07 — 08

- 머신러닝 모델 구축·평가.

중앙대 분산플랫폼·보안 연구실 학부 연구원 — 2018 — 2019

- 블록체인 이중지불 방지 연구 — IEEE 논문, 특허.

기술

AI 보안	LLM 가드레일 · 프롬프트 인젝션 방어 · RAG 권한 통제 · AI 레드팀 평가(promptfoo, garak) · OWASP LLM Top 10 · MITRE ATLAS · N2SF
보안	웹 취약점 점검(nuclei, AppScan) · TLS/PKI/ACME · WAF · 위협 인텔리전스 · 악성코드 분석 · ATT&CK · 보안성검토 · 감사
개발 · 인프라	Python · FastAPI · Java/Spring · Docker · Kubernetes · CI/CD · Linux/Windows Server · DNS · ONNX(한국어 NER)

학력

중앙대학교 컴퓨터공학 학사 — 2013 — 2020

ECE Paris 정보시스템 교환학생 — 2018 — 2019

자격 · 어학

정보처리기사 (2024)

OPIc 영어 AL — 최고 등급 (2025)

영어 업무 능숙 · 스페인어·프랑스어 초급

교육 이수

로컬 LLM 구축 및 실무 적용 — 사이버안보훈련센터, 21시간 (2026)

정보화사업 보안성 검토 — 사이버안보훈련센터, 7시간 (2026)

논문 · 특허

Recipient-Oriented Transaction for Preventing Double Spending Attacks in Private Blockchain — IEEE SECON 2018

특허 KR 10-2018-0089040 — 이중지불 방지를 위한 수신자 중심 트랜잭션 검증 방법 및 장치

수상

KAIST 특별표창 — 차세대 통합정보시스템 (2025)

SW 챌린지 동상 — 한국소프트웨어산업협회 (2019)

다빈치 SW TECH-FAIR 우수상 — 중앙대 (2019)