정연승 (Yeonseung Jeong)

2027.02 졸업 예정, 현재 Full-Time 근무 가능

(+82) 10-7288-2683 | yeonseung607@gmail.com | www.jysdev.com | itcase.tistory.com | jys705



요약

악성코드와 웹 취약점을 진단하며 네트워크와 시스템 단에서 위협의 동작 과정을 분석하고, 위협의 활동 반경이 클라우드와 AI로 넓어진 만큼 다루는 범위도 함께 넓혀왔습니다. 진행해온 활동과 프로젝트를 기술 트렌드와 함께 2023년 10월부터 최근까지 블로그 390여 편으로 기록하고, 공유했습니다.

AWS 인프라를 Terraform으로 코드화해 배포 전 검사에서 취약한 설정을 차단, 운영 중 위협은 탐지부터 차단까지 자동화하고, Datadog으로 통합 관제하는 구성을 구축했습니다. AI는 클라우드 환경에서 AWS 서버리스 중심 Bedrock RAG 서비스를 4인 팀 팀장으로 설계 및 운영하고, 별도의 개인 생산성 향상을 위해 반복되는 조사와 검증을 자동화하는 Agent를 구현했습니다.

주요 활동

AI Agent, LLMOps 멘토링 1기

AI 스쿨 & Lab
2026.03 - 2026. 06

역할 | 개인, 프롬프트 엔지니어링과 RAG 파이프라인, 자율형 에이전트 설계, 구현
과정 | 약 4개월 간 실습 중심 교육 참여, 주차별 PR 제출과 온라인 발표

- RAG 정답률 저하 원인을 검색 실패와 생성 실패로 판단하고 Ragas로 두 구간을 각각 평가. BM25와 벡터 검색을 결합하고 메타데이터 필터를 적용해 골든 데이터셋 기준 정답률을 70%에서 90%로, 검색 정확도를 약 45%에서 100%로 개선.
- 최신 IT 트렌드와 여러 정보를 수집하고 대조하는 데에서 불편함을 느껴, 정보 수집의 결과에 따라 AI의 재탐색과 생성을 반복하는 ReAct 에이전트를 구현, 고정 Workflow 구간과 자율 판단 구간, 사람의 최종 선택 구간을 분리. 운영 중 병목을 LangSmith 추적으로 식별해 동작의 변화 없이 토큰 8.4%와 비용 8.0% 절감.
- OWASP Top 10 for LLM의 직접 인젝션과 간접 인젝션을 기준으로 방어 단계를 적용. 사용자 입력은 정규식 가드레일로 LLM 도달 전 차단해 호출 비용이 발생하지 않게 하고, 외부 API 소스 5개에서 수집되는 데이터는 의심 항목을 드롭하되 과다 감지 시 전체 수집을 중단하는 조건을 설정해 에이전트에 대한 위협 통제.

국민대학교 x AWS Korea 글로벌 인재양성 프로그램 캡스톤디자인, 금상

국민대학교 *x AWS Korea*
2026.02 - 2026. 05

역할 | 4인 팀 팀장, 기획 주도, AI 개발, AWS 인프라 설계, 구축, 운영
과정 | 약 4개월 간 교육 참여도와 개발, 전시, 발표 전 구간 평가(AWS Support 팀 기술 교육, 개발 단계 AWS ProServe 멘토링)

- 밀리초 단위로 끝나는 일반 API와 최대 111초가 소요되는 AI 호출을 Lambda 2개로 분리해 타임아웃과 메모리를 개별 설정. Bedrock 호출 권한은 AI 담당 Lambda 실행 역할에만 부여해 권한을 분리하고, 무거운 AI 호출의 지연이 일반 API 응답에 영향을 주지 않는 구조로 운영.
- 응답을 버퍼링하던 Mangum을 Lambda Web Adapter로 교체하고 API Gateway 응답 스트리밍을 적용해 Bedrock 토큰을 SSE로 실시간 전달. 통합 제한 시간 29초를 초과하는 문서 생성 작업은 비동기 Job과 폴링으로 분리해, 응답 시간이 다른 두 가지 기능을 하나의 API 진입점에서 모두 제공.
- 단일 API Gateway에서 AI 경로만 명시 라우팅하고 나머지는 캐치올로 위임해, 백엔드가 API를 추가해도 인프라를 변경하지 않고 확장 가능한 구조로 설계.
- 기획부터 개발과 전시, 발표까지 팀장으로 주도하고 모든 작업을 Issue와 이슈 번호를 표기한 PR로 관리해 master를 항상 빌드 가능한 상태로 유지. 팀 Slack 채널을 활용해 진행 상황과 결정 사항을 지속적으로 공유. 실제 사용자가 접속하는 서비스로 배포, 운영해 전 구간 평가에서 금상 수상.

클라우드 시큐리티 멘토링 8기

AI 스쿨 & Lab
2025.11 - 2026. 02

역할 | 개인, 클라우드(AWS) 보안 체계 설계, Zero Trust, IaC와 컴플라이언스, 위협 탐지와 대응 자동화, 통합 관제 구축
과정 | 약 4개월 간 실습 중심 교육 참여, 주차별 수행 보고서 제출과 온라인 발표

- 인프라를 Terraform으로 코드화하고, 배포 권한은 Access Key 발급 없이 IAM Identity Center 단기 자격 증명으로 부여. IaC와 매니페스트는 Checkov, 앱 코드와 의존성은 CodeQL과 Dependabot, 이미지는 Trivy로 GitHub Actions에서 자동 검사하고 실패 시 머지가 차단되도록 설정, push 후 60초 내에 코드 결함 10건이 확인되어 취약한 설정이 배포에 반영되기 전에 차단.
- Zero Trust Identity 관점에서 네트워크 위치가 아닌 인증된 신원으로 접근을 판단하도록, 서비스 진입 경로에 Auth0를 IdP로 연동해 OIDC 인증을 통과한 요청만 내부에 도달하게 제어. 인증 로그는 Datadog으로 스트리밍해, AWS 로그만으로는 확인되지 않는 외부 로그인 시도까지 탐지 대상으로 확보.
- EKS 워커 노드를 Private Subnet에 배치하고, SSH 22번 포트 개방 대신, 키 관리 없이 SSM Session Manager로 장애 대응 접속 경로를 구성해 IAM으로 인가. 접속 이력과 셸 세션 로그는 노드가 교체되어도 보관돼 사후 감사 근거를 확보.
- GuardDuty 탐지를 EventBridge로 필터링하고 Lambda가 공격 IP를 파싱해 WAF IP Set에 등록하는 자동 대응을 구현, 사람이 수동으로 확인하고 콘솔에서 차단하던 과정 없이 자동으로 약 1.2초에 탐지와 차단이 완료. 별도로 차단 발생 시 IP와 탐지 유형, 심각도를 보안 담당자 Slack 채널로 전송해 해제 여부를 즉시 판단할 수 있는 경로까지 함께 구성.
- 실시간 위협 탐지 서비스가 다루지 않는 AWS 계정의 설정 결함은 Prowler(CSPM)로 CIS 벤치마크 기준 진단해 26건을 식별. 출력 형식이 서로 다른 결과들을 Security Hub로 집계한 뒤 Datadog(SIEM)으로 스트리밍해, 자동 차단 대상에서 제외한 결함의 심각도 분포와 발생 빈도 등을 한 화면에서 지속 모니터링.

웹 서비스 개발, 코딩 테스트 멘토링

AI 스쿨 & Lab
2025.02 - 2025. 10

역할 | 개인, React 중심 프론트엔드와 백엔드, 배포와 운영, Python과 Java 기초 코딩, Zero Trust 기반 관리자 경로 제어
과정 | 약 9개월 간 실습 중심 교육 참여, 주차별 수행 기록 제출과 온라인 발표

- OpenAI Assistants API 기반 챗봇을 React 웹사이트(www.jysdev.com)로 개발하고 Flask 백엔드를 Amazon EC2에 배포. Nginx 리버스 프록시와 Let's Encrypt 인증서로 HTTPS를 구성, 모든 요청이 프록시를 경유하도록 인바운드는 443만 개방하고 애플리케이션 포트는 폐쇄해 외부에서 애플리케이션에 직접 도달할 수 있는 가능성을 제거.
- Vercel 서버리스(Next.js)로 백엔드를 마이그레이션해 EC2 과금을 제거하고, MongoDB Atlas를 연동해 AI 응답과 추천 질문을 저장하며 현재까지 운영 중.
- 이후 관리자 경로(/admin)에 Cloudflare Zero Trust와 Auth0 인증으로 조건부 액세스를 구성해, 인증되지 않은 요청이 서버에 도달하기 전 Edge에서 차단.

정보보안 전문가 멘토링 — *AI 스쿨 & Lab*, *2023.10 - 2025. 01*

역할 | 개인, 악성코드 분석과 탐지 룰 작성, 웹 모의해킹
과정 | 약 16개월 간 실습 중심 교육 참여, 상급자 제출 형식 보고서 작성, 주차별 PowerPoint 제출과 온라인 발표

- VMware에 격리된 분석 환경을 구성하고 악성코드 샘플 3종의 동작을 정적 분석(패킹 여부, PE 구조), 동적 분석(프로세스 생성, 레지스트리 변조, 네트워크)으로 추적. 이어서 Wireshark로 패킷 단위까지 분석해 샘플이 통신을 시도한 C2 서버 IP와 포트를 식별, 현재는 응답하지 않으나 앞선 분석 결과들과 함께 활동이 재개될 가능성을 열어 두고 악성 IP와 다운로드 시도 파일명을 자동으로 탐지하는 Snort IDS 룰 8건을 작성, 위협 재개 시 네트워크 단에서 탐지, 기록되도록 구성.
- 분석부터 예방과 대응 방안까지 포함한 상급자 제출 형식의 보고서 2건(22쪽, 32쪽)으로 정리. 수집 환경과 악성코드 유형의 추정 근거, 대응 절차를 전문용어 주석과 함께 명시하고, 변조된 Windows 시스템 파일 복구와 통신을 시도한 IP를 내장 방화벽으로 차단하는 조치를 직접 수행해 대응 예시로 수록.
- Kali Linux에 DVWA와 Burp Suite로 모의해킹 환경을 구성하고, XSS, SQL Injection, File Upload 등의 주요 웹 취약점을 재현. 애플리케이션 소스코드 수준에서 불완전한 입력 검증 등을 우회하고, 서버 측 재검증이 적용된 방어 수준부터 우회가 성립하지 않는 것을 확인 및 취약점별로 방어 방안을 정리.

자격증

2026.09	**AWS Certified Security - Specialty (SCS-C03),** d8d9d95d63dd4530ac436aadf5797368	*Amazon Web Services*
2026.06	**정보처리기사,** 26201011206H	한국산업인력공단
2026.02	**Certified Kubernetes Administrator (CKA),** LF-rz36pbnwxy	*The Linux Foundation*
2026.01	**AWS Certified Solutions Architect - Associate (SAA-C03),** 0f9fcbbce81648a3a8079226d99db088	*Amazon Web Services*
2026.09	**OPIc 영어 - IM1,** 2A2556821642	*ACTFL*

학력

국민대학교 (Kookmin University) — 서울, 대한민국
소프트웨어전공 학사 (B.E. in School of Software) — *2021.03 - 2027.02 (졸업 예정)*

- 취득 학점 136/136, 전공 4.01/4.5, 전체 3.8/4.5

프로젝트

IdP 인증 제어와 AWS 기반 클라우드 보안 운영 체계 구축 - https://itcase.tistory.com/entry/cloud-security-roadmap-00

클라우드 환경의 위협 '탐지'와 '대응'에 집중한 프로젝트. 시나리오를 여러 지역에 흩어진 구성원만 사용하는 사내 플랫폼을 대상으로, 네트워크 위치 대신 인증으로 접근을 판단하는 환경으로 가정. 이메일 화이트리스트와 MFA로 인증된 계정만 통과하는 진입 통제, 오픈소스 CSPM 기반 계정 설정 진단부터 컨테이너 이미지와 런타임 위협의 상시 탐지, 심각도 조건에 따른 자동 차단 파이프라인과 Critical/High 경보 규칙을 포함하는 대시보드까지 하나의 운영 체계로 구축.

- **역할** | 개인, CloudFront 커스텀 헤더를 검증하는 리스너 규칙으로 진입 경로 한정, Auth0 OIDC 인증 연동과 인증 로그 스트리밍, GuardDuty finding을 파싱해 WAF IP Set에 등록하는 Lambda 구현, 화이트리스트 우선 평가와 Lambda 권한 범위 한정으로 오탐 차단 방지, Datadog 대시보드와 탐지 규칙 작성
- **스택** | WAF, ALB, CloudFront, Auth0 by Okta(OIDC), GuardDuty, EventBridge, Lambda(Python, Boto3), Security Hub, Inspector, Prowler(CSPM), Datadog(SIEM), Slack
- 리소스를 나열해 연결하기보다 탐지와 대응 범위에 따라 각 리소스를 어느 위치에 두고 어떤 역할을 맡길지 고민해본 경험, 복구 비용이 낮은 IP 차단만 자동으로 실행하고, 영향 검토가 필요한 결함은 관제와 경보로 분리하는 기준을 정함.

EKS 보안 구성과 DevSecOps 파이프라인 구축 - https://itcase.tistory.com/entry/devsecops-00, https://github.com/jys705/devsecops-eks-pipeline

클라우드 환경의 위협 '예방'에 집중한 프로젝트. 시나리오를 비공개 클러스터를 대상으로 소수의 운영자가 인프라와 워크로드, 앱 코드를 하나의 저장소에서 관리하는 환경으로 가정. 배포 전 코드 자동 검사와 차단, 장기 키 없는 배포 권한, 컨테이너가 탈취되어도 권한이 확산되지 않는 워크로드 구성.

- **역할** | 개인, Terraform을 통한 VPC, EKS, IAM 등의 인프라 코드화, GitHub Actions 병렬 Job 구성과 검사 통과, 리뷰 승인을 머지 조건으로 지정, IAM Identity Center와 OIDC로 사람과 파이프라인의 배포 권한 관리, tfstate S3, KMS 원격 관리와 시크릿 write-only 주입, IMDS 제한과 Pod Security Context, PSA를 통한 워크로드 권한 축소, CloudTrail, VPC Flow Logs, EKS audit 로그 활성화
- **스택** | Terraform, Docker, Kubernetes, GitHub Actions, Checkov, Trivy, GHAS(CodeQL, Dependabot), EKS, ECR, S3, IAM Identity Center, OIDC, SSM Session Manager, KMS, Secrets Manager, CloudTrail, VPC Flow Logs
- DevSecOps 모델의 시프트 레프트 원칙을 중심으로 개발 주기를 시작할 때부터 보안을 고려해본 경험, 취약한 설정이 배포에 반영되기 전에 코드 단계에서 드러나고, 같은 기준이 배포마다 일관되게 적용됨.

AWS 서버리스 중심 Bedrock RAG 서비스 개발과 운영 - https://github.com/kookmin-sw/2026-capstone-59, https://www.jysdev.com/archive/award

소프트웨어 개발 방법론(SDLC) 문서를 AI가 실시간 참조해 다음 단계를 제안하는 서비스로, 인프라를 설계하고 실제 사용자 서비스로 배포, 운영.

- **역할** | 4인 팀 팀장, 기획, 방법론과 소프트웨어공학 문서 수집 및 재구성, AI 개발, API Gateway와 Lambda, 데이터 저장소 등 AWS 서버리스 중심 인프라 설계와 구축, 배포, 운영 전 과정 주도
- **스택** | API Gateway(REST API, STREAM 모드), Lambda, Lambda Web Adapter, Bedrock(Claude Haiku 4.5), Bedrock Knowledge Bases, S3 Vectors, RDS PostgreSQL, S3, CloudWatch, IAM
- 클라우드 환경에서 AI 서비스를 설계하고 운영해본 경험, 담당이 나뉜 4인 팀에서 팀원들과 함께 모든 작업을 Issue와 PR, 주차별 대면 회의로 관리하고 리뷰.

악성코드 분석, 취약점 진단, 웹 모의해킹 - https://itcase.tistory.com/entry/security-roadmap-00, https://itcase.tistory.com/entry/22-malware-reports

로컬과 격리된 가상 환경을 구성해 실제 악성코드 샘플을 실행하고 분석, Google 검색 엔진과 Shodan으로 인터넷에 노출된 자산을 식별, 웹 취약점은 의도적으로 취약하게 만들어진 실습 환경에서 재현.

- **역할** | 개인, 격리된 분석용 VMware 가상 환경 구성과 악성코드 샘플 3종의 정적, 동적 분석, IDS 룰 작성, 보고서 작성, Google Hacking과 Shodan을 통해 인터넷에 노출된 자산과 IoT 장치의 취약점 식별, Kali Linux와 DVWA 모의해킹 환경 구성과 주요 웹 취약점 재현 및 방어 방안 도출
- **스택** | VMware(Windows), VirusTotal, PEview, Exeinfo PE, PEiD, bintext, Process Explorer, Process Monitor, Autoruns, CurrPorts, SmartSniff, Wireshark, Snort, Google Hacking, Shodan, Kali Linux, DVWA, Burp Suite, SQLMap
- 네트워크와 엔드포인트, 애플리케이션에서 발생하는 위협의 동작을 다룬 경험, 이를 상급자 제출 형식 보고서, 취약점별 방어 방안 등 예방과 대응의 형태로 도출.