

# 이재철

인프라·보안 엔지니어

## 연락처

- 전화: 010-5757-9592
  - 이메일: qws941@kakao.com
  - 주소: 경기도 시흥시 장현천로61, 307동 1301호
  - GitHub: github.com/qws941
- 

## 학력

- 한양사이버대학교 컴퓨터공학과 (2024.03 ~ 재학중)
  - 용남고등학교 졸업 (2013)
- 

## 경력 요약

총 경력: 8년 8개월 (2017.02 ~ 현재)

## 보유 기술

- 보안: FortiGate 방화벽, DDoS, IPS, WAF, NAC, DLP, EDR, APT, Splunk SIEM (15종 운영 경험)
- 클라우드: AWS (EC2, VPC, IAM, S3), Docker, Kubernetes, Cloudflare Workers (Edge Computing)
- 자동화: Python, Shell, Ansible, Terraform, n8n (워크플로우 오케스트레이션)
- 모니터링: Grafana, Prometheus, Loki, Sentry (통합 관제 플랫폼)
- DevOps: GitLab EE, CI/CD, Container Registry, Docker Compose
- AI/ML: Claude AI (자동화 파이프라인), ML 기반 위협 예측 및 자동 라우팅 시스템 (22 MCP 서버 통합)
- 금융 규제: 금융감독원 감사 대응, ISMS-P, ISO27001, FSC 본인가

## 자격증 및 교육

- 진행 중: CISSP (Certified Information Systems Security Professional) 준비
- 계획: CISM (Certified Information Security Manager) 취득 예정 (2026년 상반기)
- AWS Certified Solutions Architect 준비 중
- 한양사이버대학교 컴퓨터공학과 재학 (2024.03 ~ )

## 금융 보안 전문성

- 금융감독원 감사: 4회 연속 지적사항 0건 (2024년 Q1/Q2/Q3/Q4)
  - FSC 본인가: 금융위원회 본인가 사전 심사 보안 분야 지적사항 0건
  - 망분리 설계: 5계층 망분리 (외부/거래/내부/개발/관리) 및 Air-Gap 구축
  - 재해복구: RTO 4시간, RPO 15분 기준 DR 운영 및 분기별 테스트
  - 규제 준수: ISMS-P 90%, ISO27001 85% 이행
  - 운영 규모: 일 10만+ 거래, 10TB+ 데이터 처리
-

## 경력사항

### (주)아이티센 CTS | 정보보안 운영 엔지니어

2025.03 ~ 현재 (9개월) | Nextrade 대체거래소 운영SM (정보보안팀)

**프로젝트 규모** - 운영 인프라: 단말 300대, 서버 150대, 네트워크 장비 80대 - 일일 거래량: 10만+ 주문, 10TB+ 데이터 처리 - 사용자: 직원 200명

**주요 업무** - **SOC 운영**: 3교대 24/7 보안관제 (월 6천건 이벤트 처리) - **보안 솔루션 관제**: 15종 솔루션 통합 관제 (시스템/네트워크/엔드포인트) - **인시던트 대응**: P0~P3 등급별 SLA 기반 대응 (P1: 30분 이내) - **재해복구 운영**: DR 사이트 관리 및 분기별 테스트 (RTO 4시간, RPO 15분) - **취약점 관리**: 주간/월간 스캔 및 SLA 기반 패치 (Critical 7일, High 14일) - **규제 준수**: FSC 분기별 감사, ISMS-P 90%, ISO27001 85% 이행 - **협업**: 개발팀·거래팀·운영팀 간 보안 요구사항 조율 - **인시던트 분석**: 긴급 보안 사고 시 TF 구성 및 72시간 내 근본 원인 분석

**주요 성과** - 20개월 연속 보안 침해사고 0건 (2023.11 ~ 2025.07) - 금융감독원 감사 4회 연속 지적사항 0건 (2024년 Q1/Q2/Q3/Q4) - 거래 플랫폼 가용성 99.98% 유지 (연간 다운타임 1.75시간) - Splunk-FortiNet 통합: 80개 방화벽 중앙 관리, 정책 배포 시간 단축, 일 100만+ 이벤트 처리 - Grafana 모니터링: 5개 대시보드 구축, 평균 복구 시간 단축 - Claude AI 위협 정보 자동화: 수동 분석 작업 자동화, 처리 속도 개선 - n8n 워크플로우 자동화: 541개 노드 활용, API 처리 성능 개선, 반복 작업 자동화 - 보안 오탐 감소 - 취약점 893건 처리 (SLA 준수율 98.5%) - DR 복구 시간 단축

---

### (주)가온누리정보시스템 | 프리랜서 인프라 엔지니어

2024.03 ~ 2025.02 (11개월) | Nextrade 대체거래소(다자간매매체결회사) 구축 프로젝트

**프로젝트 규모** - 신규 구축 인프라: 서버 150대, 단말 300대, 네트워크 장비 80대 - 금융시스템: 거래 플랫폼, 청산 시스템, 감시 시스템, 백오피스 - 사용자 목표: 직원 200명

**주요 업무** - **보안 아키텍처 설계**: 5계층 망분리 (외부/거래/내부/개발/관리) 및 Air-Gap 구축 - **보안 솔루션 구축**: 시스템보안, 네트워크보안, 엔드포인트보안 - **자동화 개발**: Python 기반 방화벽/NAC/DLP 정책 자동화 시스템 - **FSC 본인가**: 금융위원회 본인가 사전 심사 대응 및 보안 체크리스트 이행 - **DR 인프라 구축**: DR 사이트 설계 및 구축 (RTO 4시간, RPO 15분) - **컴플라이언스**: ISMS-P, ISO 27001 인증 준비 및 Gap Analysis

**주요 성과** - 방화벽 정책 500건 자동화 (Python, 오류율 0%) - EPP/DLP 최적화로 단말 CPU 사용을 개선 - 11개월 보안 침해사고 0건 - FSC 본인가 사전 심사 보안 분야 지적사항 0건 - 5계층 망분리 (외부/거래/내부/개발/관리) - NAC 정책 배포 시간 단축 - ISMS-P 90%, ISO27001 85% - DR 복구 절차 자동화

---

### (주)관텍투자일임 | 인프라·정보보호팀 인프라 엔지니어

2022.08 ~ 2024.03 (1년 7개월) | AI 기반 주식투자 서비스

**주요 업무** - 금융보안데이터센터(FSDC) 운영 - 150대 이상 서버 및 스토리지 형상관리 - 망분리 환경 내 DLP, DB 접근제어, VPN 정책 관리 - AWS 클라우드 보안(VPC, IAM, CloudTrail, GuardDuty) 구성

**주요 성과** - Python 자동화로 월간 시스템 장애 감소 - 19개월 연속 개인정보 유출사고 0건 - DB 접근제어 쿼리 튜닝으로 CPU 사용을 개선 - PB 플랫폼 POC 성능 검증

---

### (주)편엔씨 | DevOps 엔지니어

2022.05 ~ 2022.07 (3개월) | 클라우드 인프라

주요 업무 - AWS 클라우드 아키텍처 구축 (EC2, Auto Scaling, VPC, Route 53, S3) - Kubernetes 마이그레이션  
사전 검토 - Python/Shell 기반 백업·복구 자동화

주요 성과 - 백업/복구 자동화로 MTTR 단축 - CI/CD 파이프라인에 보안 스캔 통합 - 컨테이너 보안 정책 수립

---

### ㈜조인트리 | 인프라·시스템 엔지니어

2021.09 ~ 2022.04 (8개월) | 국민대학교 차세대 정보시스템

주요 업무 - UTM, VMware NSX-T 기반 네트워크 세분화 - NAC, DLP, APT 등 보안 솔루션 통합 운영 - OSS 기반 보안 모니터링 구축

주요 성과 - 네트워크 세분화로 월간 장애 감소 - APT·NAC·DLP 통합으로 침해 시도 월 200건 차단 - DLP 룰 최적화로 오탐 감소 - 이중화 구성으로 서비스 가용률 99.9%

---

### ㈜메타넷애플랫폼 | 인프라·시스템 엔지니어

2019.12 ~ 2021.08 (1년 9개월) | 대규모 콜센터 인프라

주요 업무 - 1,000명 규모 재택근무 환경 구축 - SSL VPN, NAC 솔루션 통합 - Ansible 기반 정책 자동 배포 - Python 기반 네트워크 스위치 자동 점검 시스템 개발

주요 성과 - Python으로 네트워크 점검 자동화 - 백신·VPN 충돌 원인 분석 및 해결 - Ansible로 NAC 정책 배포 자동화 - 신규 사이트 3개소 네트워크 설계 및 구축

---

### ㈜엠티데이터 | 서버·시스템 엔지니어

2017.02 ~ 2018.10 (1년 9개월) | 한국항공우주산업(KAI)

주요 업무 - Linux 서버 50대 이상 운영 및 보안 패치 - 방화벽, IDS 정책 관리 및 로그 분석 - DB 접근제어 솔루션 초기 구성

주요 성과 - 방화벽 정책 분석 및 최적화 - 제조망·개발망 물리적 분리로 21개월 연속 유출사고 0건 - 월간 취약점 점검 체계 구축

---

## 주요 프로젝트

### ☑ 실전 보안 운영 자동화 플랫폼 (2024 ~ 현재)

#### 개인 프로젝트 | Production-Ready Security Operations Platform

GitHub: [github.com/qws941](https://github.com/qws941)

#### 보안 통합 관리 플랫폼

- 목적: 80대 방화벽 실시간 중앙관리 플랫폼
- 기술스택: Node.js, Cloudflare Workers, JavaScript, REST API, Webhook
- 아키텍처: 도메인 기반 아키텍처 설계, 방화벽 중앙관리 API 연동
- 핵심기능:
  - 중앙 집중식 로그 분석 및 정책 검증
  - 방화벽 실시간 데이터 수집 및 정책 위반 자동 탐지
  - 대용량 이벤트 처리 시스템

- **운영성과:**
  - 80대 방화벽 중앙 관리
  - 정책 검증 자동화
  - 위협 분석 및 알림 시스템

### SafeWork Industrial Health Platform

- **목적:** 산업보건 설문조사 SaaS 플랫폼
- **기술스택:** Flask 3.0, PostgreSQL 15, Redis 7, Cloudflare Workers
- **아키텍처:** Cloudflare Workers Edge API 기반 전국 동시 접속 처리, Flask 3.0 하이브리드 아키텍처
- **핵심기능:**
  - 종이 설문 디지털 전환 및 집계 자동화
  - 실시간 데이터 분석 및 리포팅
  - Edge API를 통한 고성능 및 저지연 서비스 제공
- **운영성과:**
  - 종이 설문 대비 집계 오류 제거
  - 전국 동시 접속 처리
  - 중소기업 10곳 이상 운영

### Public Grafana Dashboard (퍼블릭 대시보드)

- **목적:** 실시간 인프라 모니터링 및 관찰성 플랫폼 공개
- **기술스택:** Grafana, Prometheus, Loki, Tempo, Synology NAS
- **접근:** <https://grafana.jclee.me>
- **핵심기능:**
  - 13개 프로덕션 서비스 실시간 모니터링
  - 메트릭, 로그, 트레이스 통합 대시보드
  - 99.9% 가용성 달성 및 실시간 알림 시스템
  - 30일 데이터 보관 및 히스토리 분석
- **운영성과:**
  - 퍼블릭 대시보드 운영: <https://grafana.jclee.me>
  - 실시간 성능 지표 공개
  - 13개 서비스 라이브 메트릭
  - 99.9% 가용성

### Nextrade 대체거래소 인프라 구축 및 운영

가온누리정보시스템 + 아이티센 CTS | 2024.03 ~ 현재 (19개월)

**프로젝트 개요 - 프로젝트 성격:** 대한민국 20년 만에 신규 대체거래소 구축 (다자간매매체결회사) - **인프라 규모:** 서버 150대, 단말 300대, 네트워크 장비 80대, 일일 10만+ 주문 처리 - **사용자:** 직원 200명 - **핵심 시스템:** 거래 플랫폼, 청산 시스템, 감시 시스템, 백오피스

**구축 단계 (2024.03 ~ 2025.02, 11개월) - 역할:** 보안 인프라 설계 및 구축 총괄 (가온누리정보시스템) - **핵심 아키텍처:** - Zero Trust 보안 모델 기반 5계층 망분리 (외부망/거래망/내부망/개발망/관리망) - 보안 솔루션 통합 (시스템보안 / 네트워크보안 / 엔드포인트보안) - Python 기반 보안 자동화 프레임워크 (방화벽, NAC, DLP 정책 자동화) - **주요 성과:** - 금융위원회 본인가 사전 심사 보안 분야 지적사항 0건 - 방화벽 정책 자동화 (500+ 정책, 0% 오류율) - EPP/DLP 최적화로 단말 CPU 사용률 개선 - 11개월 구축 기간 동안 보안 침해사고 0건

**운영 단계 (2025.03 ~ 현재, 8개월) - 역할:** 정보보안팀 운영 엔지니어 (아이티센 CTS) - **핵심 업무:** - SOC 24/7 운영 총괄 (3교대 체계, 월 6천건 보안 이벤트 처리) - 15종 보안 솔루션 통합 관제 및 인시던트 대응 (P0~P3 등급별 SLA) - 재해복구 계획 운영 (RTO 4시간, RPO 15분, 분기별 DR 테스트) - 금융규제 준수 (FSC 분기별 감사, ISMS-P 90%, ISO27001 85%) - **주요 성과:** - 19개월 연속 보안 침해사고 0건 - 금융감독원 감사 지적사항 0건 (3회 연속) - 거래 플랫폼 가용성 99.98% (목표 99.95%) - MTTD 3.2분, MTTR 27분 - 보안 오탐 감소 - DR 복구 시간 단축

**기술적 하이라이트:** - **자동화:** Python 기반 프레임워크로 연간 461시간 수작업 자동화 (\$188K 비용 절감) - **컴플라이언스:** ISMS-P 90% 준수, ISO 27001 85% 준비, FSC 요구사항 100% 충족 - **가용성:** 99.98% 거래 플랫폼 가용성, DR 복구 시간 단축 - **보안 성과:** 19개월 무사고 운영, 취약점 SLA 준수율 98% (797/847건)

## 대규모 콜센터 원격근무 전환

메타넷애플랫폼 | 2020

역할: 보안 인프라 구축 리드 규모: 1,000명 동시 접속 기술: SSL VPN, NAC, Ansible, Python 성과: COVID-19 대응 2주 내 구축 완료, 운영 인력 3명에서 1명으로 축소

## 금융 클라우드 보안 아키텍처

관텍투자일임 | 2023

역할: AWS 보안 설계 및 구현 기술: AWS (VPC, IAM, GuardDuty), Python, Terraform 성과: 실시간 이상징후 탐지 시스템 구축, 인프라 비용 20% 절감

## ☑ AI 기반 인프라 자동화 플랫폼 (2024.09 ~ 현재)

### 개인 프로젝트 | AI-Powered Infrastructure Automation & Observability Platform

GitHub: [github.com/qws941](https://github.com/qws941) | Live: <https://resume.jclee.me>

**시스템 규모 & 아키텍처:** - **인프라:** Rocky Linux 9.6, Hyper-V, 40GB RAM, 8 CPU cores - **프로젝트:** 12개 프로덕션 애플리케이션 (blacklist, mcp, resume, safework, grafana, n8n 등) - **컨테이너:** Docker 28.5.1, 14개 운영 컨테이너 (Prometheus, Loki, Promtail, cAdvisor, Node Exporter) - **모니터링:** 중앙 집중식 Grafana Stack (Synology NAS), 15개 리스닝 포트, 99.9% 가용성

**기술스택 & 도구:** - **AI/ML:** Claude Code (Sonnet 4.5), MCP Protocol (22 servers, 145+ tools), GitHub Copilot - **컨테이너:** Docker, Docker Compose, Watchtower (자동 업데이트), Portainer API - **모니터링:** Grafana, Prometheus, Loki, Tempo, Splunk, cAdvisor, Node Exporter - **언어:** Python 3.9, Node.js 22, JavaScript/TypeScript, Shell Script - **CI/CD:** GitHub Actions, Cloudflare Workers, Git-based automation - **네트워크:** Traefik (Reverse Proxy), NFS v3/v4 (Synology integration), Multi-host Docker

### 세부 프로젝트 컴포넌트:

**1. ML Agent Selection System** - 목적: ML 기반 자동 에이전트 라우팅 시스템 - **기술스택:** Python, Flask, Scikit-learn, PostgreSQL, 22 MCP Servers - **규모:** 145+ 스크립트 관리, Constitutional Framework v12.0 - **성과:** AI 작업 효율 향상, 자동 에이전트 라우팅으로 의사결정 시간 단축 - **Live:** <http://127.0.0.1:5001> - **GitHub:** [github.com/qws941/claude](https://github.com/qws941/claude)

**2. n8n Workflow Automation** - 목적: Self-hosted 워크플로우 자동화 플랫폼 - **기술스택:** n8n, PostgreSQL, Redis, Docker, 541 Nodes - **규모:** 2709+ 템플릿, API 오케스트레이션 - **성과:** 반복 작업 자동화로 월 100+ 시간 절감, 워크플로우 재사용성 향상 - **Live:** <https://n8n.jclee.me> - **GitHub:** [github.com/qws941/n8n](https://github.com/qws941/n8n)

**3. GitLab Enterprise Edition** - 목적: Self-hosted DevOps 플랫폼 및 Container Registry - **기술스택:** GitLab EE 17.5.3, PostgreSQL 16.1, Redis 7.2, Traefik - **규모:** CI/CD pipelines, Container Registry, 7일 자동 백업 - **성과:** Private 코드 호스팅, 자동화된 CI/CD, 컨테이너 이미지 관리 - **Live:** <https://gitlab.jclee.me> - **GitHub:** [github.com/qws941/claude/tree/main/app/gitlab](https://github.com/qws941/claude/tree/main/app/gitlab)

**4. Nginx Airgap Configuration** - 목적: 폐쇄망 환경용 Nginx 설정 및 보안 강화 - **기술스택:** Nginx 1.24+, Airgap Deployment, Security Hardening - **특징:** 패키지 사전 준비, 오프라인 설치 지원 - **성과:** 폐쇄망 환경에서 100% 자급 배포 가능, 보안 설정 표준화 - **GitHub:** [github.com/qws941/nginx](https://github.com/qws941/nginx)

**5. Python Automation Framework** - 목적: 인프라 자동화 프레임워크 - **기술스택:** Python, Ansible, Bash, Git Hooks, 145+ Scripts - **특징:** 파일 거버넌스, AI 보상 시스템, 세션 연속성 - **성과:** 인프라 운영 시간 단축, 스크립트 재사용성 향상 - **GitHub:** [github.com/qws941/claude](https://github.com/qws941/claude)

**6. Constitutional Governance System v12.0** - 목적: 파일 생성 쿼터 관리 및 구조 거버넌스 - 기술스택: Bash, Python, JSONL, Git Hooks - 규모: 파일 생성 쿼터 (3 scripts, 2 docs), 70% 유사도 감지, 자동 로깅 - 성과: 파일 중복 감소, 프로젝트 구조 일관성 유지 - GitHub: [github.com/qws941/claude/blob/main/scripts/master-prevention-system.sh](https://github.com/qws941/claude/blob/main/scripts/master-prevention-system.sh)

**7. AI Compensation Core** - 목적: AI 한계 보상 시스템 (8가지 보상 메커니즘) - 기술스택: Python, Pattern Detection, Multi-Model Validation - 보상 영역: Context window, Hallucination 감지, Real-time data, Domain routing - 성과: AI 오답률 감소, 작업 신뢰도 향상 - GitHub: [github.com/qws941/claude/blob/main/scripts/ai-compensation-core.py](https://github.com/qws941/claude/blob/main/scripts/ai-compensation-core.py)

**8. Ansible FortiManager Automation** - 목적: FortiManager 방화벽 정책 자동화 (Infrastructure as Code) - 기술스택: Ansible, FortiManager API, Ansible Vault, Docker - 규모: 3개 플레이북 (584 lines), fortinet.fortimanager collection - 기능: 정책 조회/생성/수정, 백업/복원, 오브젝트 관리, Docker 배포 자동화 - 성과: 정책 배포 시간 단축, 수동 오류 제거 - GitHub: [github.com/qws941/policy](https://github.com/qws941/policy)

**9. NAS Infrastructure Deployment** - 목적: Synology NAS 인프라 자동 배포 시스템 - 기술스택: Bash, rsync, SSH, Docker Compose, Synology DSM - 규모: 9개 서비스 (Grafana, Prometheus, Loki, Alert-Manager, GitLab, Traefik, Splunk, Promtail, Node Exporter) - 기능: 원격 Docker 관리, 자동 rsync 동기화, 멀티 서비스 오케스트레이션 - 성과: 배포 자동화로 수동 작업 제거, 인프라 동기화 시간 단축 - GitHub: [github.com/qws941/claude/tree/main/infra](https://github.com/qws941/claude/tree/main/infra)

#### 핵심 아키텍처 설계:

##### 1. Universal Observability Architecture

- 중앙 집중식 모니터링 (Synology NAS: [grafana.jclee.me](https://grafana.jclee.me))
- 메트릭 수집: Prometheus, Synology 통합
- 로그 수집: Promtail, Loki, Grafana 실시간 스트리밍
- 컨테이너 메트릭: cAdvisor (8081) + Node Exporter (9101)
- 헬스체크: 모든 서비스 /health 엔드포인트 표준화

##### 2. Multi-Host Docker Context System

- 로컬 Docker (localhost): blacklist, mcp, local-exporters
- Synology Docker (192.168.50.215): grafana, n8n, xwiki, file
- NFS 마운트: /home/jclee/app/{grafana,n8n,xwiki}, Synology 동기화
- .docker-context 파일 기반 자동 라우팅

##### 3. AI-Driven Automation Framework

- 150+ SlashCommand 시스템
- MCP 도구 생태계: filesystem, github, slack, tmux, n8n, sqlite, puppeteer
- Constitutional AI 거버넌스 (CLAUDE.md): 자율 실행, 검증, 메타 학습
- 자동화 스크립트: 57개 Bash scripts (보안, 모니터링, 배포, 테스트)

##### 4. Production-Ready CI/CD Pipeline

- GitHub Actions: resume (Cloudflare Workers), blacklist (Docker)
- Watchtower: 자동 이미지 업데이트 및 무중단 재배포
- Git-based: 모든 변경사항 추적 가능, 자동 롤백 지원
- 테스트 자동화: Jest 30 (유닛), Playwright 1.56 (E2E)

#### 프로젝트별 상세:

**Resume Portfolio (Cloudflare Workers + Observability)** - 배포: <https://resume.jclee.me> (< 50ms 응답, 글로벌 CDN) - 기술스택: Cloudflare Workers (152 KB), HTML/CSS, JSON-LD SEO, Grafana Loki 통합 - 인프라: GitLab (Primary, 192.168.50.215:2222) + GitHub (Mirror, CI/CD) - CI/CD: GitHub Actions 자동 배포, 배포 타임스탬프 주입 - 모니터링: - Grafana Loki 실시간 로깅 (<https://grafana.jclee.me/loki>) - Prometheus 메트릭 수집 (/metrics 엔드포인트) - Web Vitals 추적 (LCP, FID, CLS, FCP, TTFB) - Health Check (/health): 배포 시각, 가동 시간, 요청 통계 - 보안: CSP SHA-256 해시 (unsafe-inline 제거), HSTS, X-Frame-Options - 테스트: 23/23 유닛 테스트, 10/10 E2E 테스트 (Playwright) - 성과: Lighthouse 100점, 접근성 95%+, Open Graph 소셜 미리보기 - 최신 배포: 2025-11-12T01:04:49Z (Account: a8d9c67f586acdd15eebcc65ca3aa5bb)

**Blacklist (IP 블랙리스트 관리 시스템)** - 아키텍처: PostgreSQL 15, Redis 7, Flask 3.0, React (Frontend) -

스케일: 10,000+ IP 주소 실시간 관리 - 모니터링: Prometheus metrics (/metrics), Health check (/health) - 배포: Multi-port (2542), Docker Compose, Traefik integration

**MCP Platform (AI 도구 통합)** - 역할: Model Context Protocol 서버 통합 플랫폼 - 규모: 14개 MCP 서버, 70개 도구 (filesystem, github, slack, tmux, n8n) - WebUI: Node.js 22 (3001), Nginx reverse proxy (3002) - 성과: AI 작업 효율 향상, 도구 통합 복잡성 감소

**Local Exporters (모니터링 스택)** - 구성: Prometheus, Node Exporter, cAdvisor, Promtail - 메트릭: 시스템 (CPU, RAM, Disk), 컨테이너 (Docker stats), 로그 (Loki) - 중앙 통합: Synology Grafana (192.168.50.215)

**Splunk Demo (로그 분석)** - 규모: 초당 10만 이벤트 처리 가능 - 포트: 8000 (WebUI), 8088-9 (HEC), 9997 (Forwarder) - 용도: 보안 이벤트 중앙 집중 분석, FortiNet 통합

**운영 성과 (2024.09 ~ 현재):** - **자동화:** 반복 작업 시간 단축 - **안정성:** MTTR 개선 - **가시성:** 통합 대시보드 구축, 모든 서비스 실시간 모니터링 - **테스트:** Jest + Playwright 통합, 100% 커버리지 달성 - **보안:** SELinux + Firewall 구성 - **비용:** 로컬 + Synology 하이브리드로 클라우드 비용 제로

**기술적 하이라이트:** - Worker 생성 자동화 - ROUTES 객체 패턴 - Integration 테스트 - Constitutional AI - Docker Context Auto-routing

---

## 기술 스택

### 보안 솔루션

- 네트워크 보안: 방화벽, DDoS, IPS/IDS, WAF
- 엔드포인트: NAC, DLP, EDR/EPP, MDM, APT
- 접근제어: 서버/DB 접근제어, SSL VPN, IPSec, SSL 복호화
- 모니터링: SIEM, SOAR

### 클라우드 및 가상화

- AWS: EC2, VPC, IAM, S3, CloudTrail, GuardDuty, Route53
- 가상화: VMware vSphere, NSX-T, Hyper-V
- 컨테이너: Docker, Kubernetes, Helm

### 자동화 및 개발

- Languages: Python, Shell Script, PowerShell, Node.js, TypeScript, JavaScript
- IaC: Ansible, Terraform, CloudFormation
- CI/CD: Jenkins, GitLab CI, GitHub Actions, Watchtower
- 모니터링: Prometheus, Grafana, Loki, ELK Stack, Tempo, Splunk

### AI/ML 및 자동화

- AI 도구: Claude Code, GitHub Copilot, ChatGPT API
- MCP 프로토콜: 14개 서버 통합 (filesystem, github, brave-search, memory, tmux 등)
- 자동화 프레임워크: Custom SlashCommand 시스템 (150+ 명령어)
- 관찰성: Universal Observability 아키텍처 (Grafana 중심)

### 컨테이너 및 오케스트레이션

- 컨테이너 플랫폼: Docker, Portainer API, Docker Compose
- 레지스트리: Private Docker Registry (registry.jclee.me)
- 배포 전략: Multi-Port Deployment, Blue-Green, Canary
- 자동화: Watchtower 기반 자동 업데이트, 무중단 배포

## 네트워크

- Routing/Switching: OSPF, BGP, VLAN, VxLAN
  - Load Balancing: F5, HAProxy, Nginx
  - SDN: VMware NSX-T, OpenFlow
- 

## 자격증

자격증명	발급기관	취득일
CCNP	Cisco Systems	2020.08
RHCSA	Red Hat	2019.01
CompTIA Linux+	CompTIA	2019.02
LPIC Level 1	Linux Professional Institute	2019.02
사무자동화산업기사	한국산업인력공단	2019.12
리눅스마스터 2급	한국정보통신진흥협회	2019.01

---

최종 업데이트: 2025년 11월 21일