이재철 이력서

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)

핵심 역량 (Technical & Domain Expertise)

- **보안 솔루션 통합 운영**: DDoS, IPS, WAF, NAC, DLP, EDR, APT 등 15종 이상 보안 솔루션 설계, 구축 및 통합 관제
- **클라우드 & 컨테이너 인프라**: AWS 기반 클라우드 환경 설계 및 운영, Docker, Kubernetes, Portainer API를 활용한 컨테이너 오케스트레이션 및 Private Registry 관리

- **금융권 보안 규제 준수**: 금융감독원 감사 0건 지적, ISMS-P, ISO27001 등 국내외 정보보호 인증 및 규제 준수 체계 구축 및 운영
- **대규모 시스템 운영**: 단말 1,000대 이상, 서버 150대 이상 규모의 대규모 인프라 운영 및 안정화 경험
- **운영 자동화 및 효율화**: Python/Shell 스크립트 기반 업무 자동화 시스템 개발, 반복 업무 시간 50~95% 단축, 평균 장애 복구 시간(MTTR) 70% 개선
- **무중단 프로덕션 배포**: CI/CD 파이프라인 구축 및 운영, 무중단 배포, 자동 롤백 시스템을 통한 99.9% 서비스 가용성 달성

경력사항

㈜아이티센 CTS | 정보보안 운영 엔지니어

2025.03 ~ 현재 (8개월) | Nextrade 증권거래소 운영SM (정보보안팀)

프로젝트 규모 - 운영 인프라: 단말 300대, 서버 150대, 네트워크 장비 80대 - 일일 거래량: 10만+ 주문, 10TB+ 데이터 처리 - 사용자: 직원 200명, 등록 트레이더 5만명

주요 업무 - **SOC 24/7 운영 총괄**: 3교대 보안관제 체계 구축 및 운영 (보안 이벤트 월 6천건 처리) - **보안 솔루션 통합 관제**: 시스템보안 / 네트워크보안 / 엔드포인트 보안 - **보안 인시던트 대응**: P0~P3 등급별 SLA 기반 대응 체계 운영 (P1: 30분 이내 대응) - **재해복구 계획 운영**: DR 사이트 관리 및 분기별 DR 테스트 수행 (RTO 4시간, RPO 15분) - **취약점 관리**: 주간/월간 취약점 스캔 및 SLA 기반 패치 관리 (Critical 7일, High 14일) - **금융규제 준수**: FSC 분기별 감사 대응, ISMS-P 90% 준수, ISO27001 85% 준비

주요 성과 - **보안사고 제로**: 19개월 연속 보안 침해사고 0건, 데이터 유출 0건 달성 - **규제 완벽 대응**: 금융감독원 정기 감사 지적사항 0건 달성 (3회 연속 무결점) - **시스템 가용성**: 거래 플랫폼 99.98% 가용성 달성 (목표 99.95% 초과 달성) - **대응 시간 단축**: MTTD 3.2분, MTTR 27분 달성 (업계 평균 대비 50% 우수) - **오탐 대폭 감소**: 보안 알림 False Positive 60% → 33% 개선 (일 200건 → 100건) - **취약점 관리**: Critical/High 취약점 SLA 준수율 98% 달성 (797/847건 처리) - **DR 테스트 성공**: 전체 DR 훈련 목표 4시간 대비 2.5시간 만에 복구 완료 (37% 초과 달성) - **비용 절감**: 자동화를 통한 연간 $188K 비용 절감 (수작업 461시간 자동화)

㈜가온누리정보시스템 | 프리랜서 인프라 엔지니어

2024.03 ~ 2025.02 (11개월) | Nextrade 증권거래소(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, 등록 트레이더 5만명

주요 업무 - **Zero Trust 보안 아키텍처 설계**: 5계층 망분리 (외부망/거래망/내부망/개발망/관리망) 및 Air-Gap 구축 - **보안 솔루션 도입 총괄**: 시스템보안 / 네트워크 보안 / 엔드포인트보안 - **보안 자동화 프레임워크 개발**: Python 기반 방화벽/NAC/DLP 정책 자동화 시스템 구축 - **FSC 본인가 준비**: 금융위원회 본인가 사전 심사 대응 및 보안 체크리스트 100% 이행 - **재해복구 인프라 구축**: DR 사이트 설계 및 구축 (RTO 4시간, RPO 15분 목표) - **컴플라이언스 체계 수립**: ISMS-P, ISO 27001 인증 준비 및 Gap Analysis

주요 성과 - **자동화 프레임워크 구축**: Python으로 방화벽 정책 자동화 (500+ 정책, 0% 오류율, 50% 시간 단축) - **에이전트 최적화 성공**: EPP/DLP 충돌 근본 원인 분석 및 해결, 단말 CPU 사용률 30% 개선 (60% → 42%) - **보안 사고 예방**: 11개월 구축 기간 동안 보안 침해사고 0건, 정보 유출사고 0건 - **FSC 사전 심사 통과**: 금융위원회 본인가 사전 점검 보안 분야 지적사항 0건 달성 - **망분리 완벽 구현**: 5계층 물리적 망분리 및 Air-Gap 구축 완료 (FSC 요구사항 100% 충족) - **NAC 자동화**: Python 스크립트로 단말 등록/정책 배포 자동화 (처리 시간 70% 단축, 800대 → 240대 기준) - **컴플라이언스 준비**: ISMS-P 90% 준비 완료, ISO 27001 85% 준비 완료 (본인가 전 달성) - **DR 테스트 프레임워크**: 재해복구 절차 문서화 및 자동화 스크립트 개발 (90% 자동화율)

㈜콴텍투자일임 | 인프라·정보보호팀 인프라 엔지니어

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

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

주요 성과 - **자동화 효과**: Python 스크립트로 반복 작업 자동화, 장애율 40% 감소 (월 10건 → 6건) - **컴플라이언스**: 금융감독원 정기 감사 통과, 개인정보 유출사고 0건 (19개월) - **성능 최적화**: DB 접근제어 쿼리 튜닝으로 CPU 사용률 30% 개선 (75% → 52%) - **POC 성공**: PB 플랫폼 구축 프로젝트 성능 검증 완료, 목표 대비 120% 달성

㈜펀엔씨 | 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 - **복구 시간 개선**: 백업/복구 자동화로 MTTR 50% 단축 (평균 2시간 → 1시간) - **보안 강화**: CI/CD 파이프라인에 보안 스캔 단계 추가, 취약점 조기 발견율 80%↑ - **정책 수립**: 컨테이너 보안 정책 초안 작성 및 Kubernetes 마이그레이션 준비 완료

㈜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 - **안정성 향상**: 네트워크 세분화 및 모니터링 강화로 장애율 25% 감소 (월 12건 → 9건) - **보안 강화**: APT·NAC·DLP 통합으로 침해사고 예방률 80% 달성 (차단 200건/월) - **정책 최적화**: DLP 룰 재설계로 민감정보 탐지율 20% 향상 (탐지 누락 50건 → 10건/월) - **고가용성**: 이중화 아키텍처로 서비스 가용률 99.9% 유지 (연간 다운타임 8.7시간 이하)

㈜메타넷엠플랫폼 | 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 - **자동화 구현**: Python으로 네트워크 스위치 점검 자동화, 주당 소요시간 75% 단축 (8시간 → 2시간) - **안정성 개선**: 백신-VPN 충돌 근본 원인 분석 및 해결, 장애 문의 40% 감소 (주 20건 → 12건) - **정책 자동화**: Ansible로 NAC 예외정책 자동 배포, 처리시간 90% 단축 (건당 30분 → 3분) - **아키텍처 설계**: 신규 사이트 3개소 네트워크 설계 및 구축 완료 (동시 500명 규모)

㈜엠티데이타 | 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 - **정책 최적화**: 방화벽 정책 분석 및 재설계, 중복 룰 30% 제거 (3,000개 → 2,100개) - **망분리 구축**: 제조망-개발망 물리적 분리 완료, 내부정보 유출사고 0건 (21개월) - **취약점 관리**: 월간 취약점 점검 체계 구축, 치명적(Critical) 취약점 2주 내 100% 조치

주요 프로젝트

🔧 실전 보안 운영 자동화 플랫폼 (2024 ~ 현재)

개인 프로젝트 | Production-Ready Security Operations Platform

GitHub: 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 정책 실시간 중앙 관리 및 모니터링
  - 정책 검증 자동화
  - 위협 분석 및 자동 알림 시스템 구축

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 100% 제거
  - 전국 동시 접속 환경에서 안정적인 서비스 제공
  - 다수 중소기업에 성공적으로 도입 및 운영 중

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 (퍼블릭 접근 가능)
- **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 대시보드로 투명한 인프라 운영 공개
  - 실시간 성능 지표 및 장애 대응 현황 공유
  - 포트폴리오 프로젝트의 라이브 메트릭 제공
  - 모니터링 베스트 프랙티스 시연

Nextrade 증권거래소 인프라 구축 및 운영

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

프로젝트 개요 - **프로젝트 성격**: 대한민국 20년 만에 신규 증권거래소 구축 (다자간 매매체결회사) - **인프라 규모**: 서버 150대, 단말 300대, 네트워크 장비 80대, 일일 10만+ 주문 처리 - **사용자**: 직원 200명, 등록 트레이더 5만명 목표 - **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 / 네트워크 보안 / 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, 50% 시간 단축) - EPP/DLP 최적화로 단말 CPU 사용률 30% 개선 (60% → 42%) - 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, 데이터 유출 0건 - 금융감독원 정기 감사 지적사항 0건 (3회 연속 무결점) - 거래 플랫폼 99.98% 가용성 달성 (목표 99.95% 초과) - MTTD 3.2분, MTTR 27분 달성 (업계 평균 대비 50% 우수) - 보안 알림 False Positive 60% → 33% 개선 (일 200건 → 100건) - DR 테스트 2.5시간 완료 (목표 4시간 대비 37% 초과 달성)

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 37% 단축 - **보안 성과**: 19개월 무사고 운영, 취약점 SLA 준수율 98% (797/847건)

대규모 콜센터 원격근무 전환

메타넷엠플랫폼 | 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

콴텍투자일임 | 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 Platform

GitHub: github.com/qws941

- **목적**: AI 기반의 지능형 인프라 운영 자동화 및 관측성(Observability) 플랫폼 구축
- **기술스택**: Claude Code, MCP Protocol, Node.js, Python, Docker, Grafana Stack (Prometheus, Loki, Tempo), Traefik, Watchtower
- **아키텍처**: Docker Compose 기반 마이크로서비스 오케스트레이션, Git 기반 CI/CD 파이프라인
- **핵심기능**:
  - 150개 이상의 자동화 명령어 체계(SlashCommand 시스템) 구축 및 통합
  - Universal Observability 아키텍처 구현 (메트릭, 로그, 트레이스 통합 모니터링)
  - MCP(Model Context Protocol) 도구 생태계 구축 (14개 서버, 70개 이상 도구 연동)
  - AI 어시스턴트(Claude Code, GitHub Copilot, ChatGPT API) 통합을 통한 운영 효율 극대화
  - 실시간 로그 스트리밍 파이프라인(Promtail → Loki → Grafana) 구축
  - Watchtower 기반 Docker 컨테이너 자동 업데이트 및 무중단 배포
- **운영성과**:
  - AI 기반 자동화로 인프라 운영 효율 80% 향상 및 수동 작업 시간 대폭 단축
  - 통합 관측성 확보로 장애 발생 시 평균 복구 시간(MTTR) 70% 감소
  - Git 기반 완전 자동화 CI/CD 파이프라인 구축으로 배포 안정성 및 속도 향상
  - 14개 서버에 걸친 70개 이상의 도구를 통합 관리하여 복잡성 감소 및 가시성 증대

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

자격증명	발급기관	취득일
리눅스마스터 2급	한국정보통신진흥협회	2019.01

핵심 강점 (Soft Skills & Work Ethic)

종합적인 보안 및 인프라 전문성

- 7년간 금융, 교육, 제조, IT 서비스 등 다양한 산업군에서 보안 및 인프라 운영 경험
- 15종 이상 보안 솔루션 도입, 운영 및 최적화 경험을 통한 폭넓은 전문성
- Zero Trust 보안 모델 및 최신 보안 트렌드에 대한 깊은 이해와 적용 능력

검증된 문제 해결 및 위기 대응 능력

- Root Cause Analysis(RCA) 기반의 체계적인 문제 분석 및 해결 접근 방식
- 평균 장애 해결 시간(MTTR) 40~50% 단축을 통한 신속한 위기 대응 능력
- 예방적 보안 체계 구축 및 선제적 대응을 통한 침해 사고 발생률 최소화

자동화 주도 혁신 및 효율성 추구

- Python/Shell 스크립팅을 활용한 반복 업무 자동화 및 운영 프로세스 개선
- 자동화를 통한 운영 효율 50~70% 개선 실적 및 비용 절감 기여
- Infrastructure as Code(IaC) 기반의 인프라 표준화 및 관리 효율 증대

강력한 규제 준수 및 컴플라이언스 역량

- 금융감독원, 금융보안원 등 엄격한 국내외 정보보호 규제 및 감사 대응 경험
- ISMS-P, ISO27001 등 주요 정보보호 인증 획득 및 유지 관리 경험
- 컴플라이언스 문서화 및 내부 감사 대응을 통한 조직의 정보보호 수준 향상 기여

최종 업데이트: 2025년 10월 16일