**이력서 / 경력기술서**

**이름**: 이재철  
**연락처**: 010-5757-9592  
**이메일**: qws941@kakao.com  
**주소**: 경기도 부천시 원미구 원미동 32-1, 404호

**학력사항**

* 용남고등학교 졸업 (2013)
* 한양사이버대학교 컴퓨터공학과 재학 (2024.03 ~ )

**경력사항**

**1) ㈜엠티데이타 | 서버·시스템 엔지니어**

*(2017.02 ~ 2018.10)*

* **서버 및 보안장비 유지보수 (Linux, 방화벽, IDS 등)**
  + 한국항공우주산업(KAI) 내 Linux 서버 약 50대를 운영하며, 보안 패치와 계정·권한 관리 작업 수행
  + 방화벽·IDS 로그를 분석해 **취약점 스캐닝**을 실시하고, 취약점 개선 권고안 작성
* **문제해결 사례**
  + 방화벽 룰 중복 및 잘못된 ACL(Access Control List)로 인해 일정 네트워크 구간에서 패킷 드롭 발생
  + **Root Cause**: 정책이 수작업으로 관리되다 보니 특정 포트가 여러 룰에 겹쳐서 적용됨
  + **해결**: 룰 정리와 버전 관리 스크립트(Shell)로 자동화 → 중복 정책 30% 제거, 트래픽 흐름 안정화

**2) ㈜메타넷엠플랫폼 | 인프라·시스템 엔지니어**

*(2019.12 ~ 2021.08)*

* **대규모 콜센터 재택근무(약 1,000명 규모) 환경 구축**
  + Fortigate SSL VPN, Ansible 등을 활용해 임직원 PC에 자동으로 VPN 에이전트를 배포, 접근 정책을 중앙에서 일괄 적용
  + NAC(Network Access Control) 솔루션과 연동해 사용자 단말 상태를 지속 모니터링, 위험 단말은 격리
* **엔드포인트 보안·장애 대응**
  + SSL VPN 클라이언트가 오래된 백신(V3, TrendMicro 등)과 충돌을 일으키는 이슈 다수 발생
  + **Root Cause**: 백신 엔진 업데이트 시 VPN 터널링이 일시적으로 차단되는 충돌
  + **해결**: VPN·백신 간 예외 정책을 재설정, 관련 설정값을 Ansible 플레이북으로 자동화 배포 → 장애 문의 건수 월 40% 감소
* **네트워크 자동화**
  + Python 기반 Cisco 스위치 자동 점검 스크립트 작성: VLAN·포트 상태·Ping 테스트 등을 주기적으로 실행, 결과를 Slack으로 알림
  + 점검 시간 주당 8시간 → 2시간 이하로 단축

**3) ㈜조인트리 | 인프라·시스템 엔지니어**

*(2021.09 ~ 2022.04)*

* **국민대학교 차세대 정보시스템 인프라 구축**
  + Fortigate UTM, VMware NSX-T 등 보안·가상화 솔루션으로 **세분화된 네트워크**와 **보안 정책** 구현
  + 물리 서버·스토리지 약 100대, 가상머신 약 200대를 통합 모니터링 및 성능 최적화
* **보안 정책 유지보수**
  + 주기적으로 UTM 로그를 분석해 악성 IP 차단 리스트를 업데이트하고, NSX-T 미세분할(Micro-segmentation) 정책을 개선

**4) ㈜펀엔씨 | DevOps 엔지니어**

*(2022.05 ~ 2022.07)*

* **AWS 기반 클라우드 운영**
  + EC2, Auto Scaling, Route 53, S3 등을 활용, 서버 배포·확장 자동화
  + Kubernetes 마이그레이션 사전 검토: 컨테이너 보안 정책 및 Pod 보안 컨텍스트 설정 준비
* **백업·복구 자동화**
  + Shell/Python 스크립트로 주기적인 스냅샷·백업 실시, 특정 이벤트 발생 시 Slack 알람 전송

**5) ㈜콴텍투자일임 | 인프라·정보보호팀 인프라 엔지니어**

*(2022.08 ~ 2024.03)*

* **금융 인프라 운영 & 보안 규제 준수**
  + 금융보안데이터센터(FSDC) 내 서버·네트워크 약 150대를 형상관리, AI 기반 투자 앱 장애 모니터링
  + 금융감독원 감사 대비를 위해 개인정보 DB 접근로그, DLP 정책, 망분리 상태 등을 정기 점검
* **PB 플랫폼 구축**
  + 보안성과 가용성을 모두 충족하는 인프라 설계: POC를 통해 Kubernetes·API Gateway·WAF 등 성능·호환성 검사 후 적용
* **문제해결 사례**
  + DB 접근제어 솔루션이 대량 거래 트래픽이 몰릴 때 성능 이슈 유발
  + **Root Cause**: 실시간 모니터링 시 쿼리 로깅이 과도하게 발생
  + **해결**: 모니터링 간격 및 필드 범위 재조정, 우선순위 정책 분리 → CPU 사용률 30% 감소, 처리 지연 개선

**6) ㈜가온누리정보시스템 | 인프라 엔지니어(프리랜서)**

*(2024.03 ~ 현재)*

* **ATS(다자간매매체결회사) 보안 인프라 운영**
  + 금융위원회 본인가 사전 준비: 시스템 이중화, 망연계, NAC 등을 통한 철저한 망분리/보안 체계 구축
  + DDoS, IPS, WAF, VPN 등 보안 솔루션을 통합 모니터링하여 **실시간 위협**에 대응
* **거래소 증권망 방화벽 자동화**
  + **Python 스크립트**로 100개 이상의 방화벽 정책(ACL, NAT 룰 등)을 자동 등록
  + CSV 형식으로 룰 정보를 입력하면 REST API 또는 CLI를 통해 일괄 반영 → **정책 반영 시간 50% 단축**, 인적 오류 최소화
* **엔드포인트 보안 체계 강화(EPP/CPP, DLP, APT, SSL Inspection, NAC)**
  + EPP/CPP, DLP 에이전트 배포 시 일부 단말 성능 저하와 충돌 발생
  + **Root Cause**: 기존 악성 코드 검사 프로세스와 DLP 실시간 스캔이 중복 작동
  + **해결**: 벤더 기술지원 및 내부 테스트를 통해 스캔 시점 분리, NAC 로그 기반 실시간 모니터링 및 알림 시스템 구축 → 사용자 불편도 크게 감소

**주요 역량 요약**

1. **엔드포인트 보안솔루션 운영 (EDR, DLP, NAC 등)**
   * 대규모(1,000명 이상) 단말 환경에서 **설치·업데이트·정책 적용** 및 **장애 대응** 경험 풍부
   * 백신/EDR과 VPN, NAC, DLP 간 충돌 사례를 **벤더 협업** 및 **스크립트 자동화**로 개선
2. **보안시스템 자동화 & API 활용**
   * Python, Shell Script로 **방화벽 정책, NAC 설정** 자동화
   * 보안 솔루션(예: Fortinet, Palo Alto) API 연동으로 중복 업무 감소, 배포 속도 단축
3. **금융권 망분리·컴플라이언스**
   * FSDC, ATS 등 금융망에서 **망연계, DLP, AD 접근제어**를 실무 운영
   * 금융감독원·내부 감사 대응 자료 작성, 규제 사항 충족 절차 수립
4. **대규모 인프라 및 문제해결 프로세스**
   * 콜센터·금융투자사·교육기관 등 50수천 단말 관리
   * **루트 원인 분석(Root Cause Analysis)** → **단계별 해결(정책 조정, 벤더 협업, 스크립트 배포)** → **재발 방지** 프로세스 확립
5. **클라우드/DevOps & 하이브리드 환경**
   * AWS 기반 서버 자동화, Kubernetes, Docker 등 컨테이너 환경 기초 운영
   * Ansible, Jenkins 등 CI/CD 파이프라인 일부 구성 경험

**토스증권 지원동기 및 포부**

저는 금융업계에서 엔드포인트 보안솔루션(AV, EDR, DLP, NAC) **망분리**를 중심으로 폭넓은 실무 경험을 쌓으며, **자동화**와 **효율**에 대한 고민을 끊임없이 해 왔습니다. 토스증권이 지향하는 **국제수준 정보보호**와 **SOAR, ZTNA, Cloud/Container 보안** 강화 기조는 저의 기술 역량과 지향점과도 완벽히 부합한다고 생각합니다.

* **확장 가능한 엔드포인트 보안**: 대규모 단말 운영 경험 및 문제 해결 프로세스로 안정적인 솔루션 운영 체계를 마련하겠습니다.
* **자동화로 인한 효율 혁신**: Python, Script, API 연동 등을 통해 보안솔루션 정책 변경 및 오류 조치 과정을 대폭 단축하여, 팀 전체의 운영 효율과 정확도를 높이겠습니다.
* **금융 컴플라이언스 + 사용자 편의성**: 망연계·DLP 등을 통해 엄격한 규제를 준수하면서도, 임직원·고객이 불편 없이 금융 서비스를 이용하도록 균형 잡힌 보안 아키텍처를 설계하겠습니다.

앞으로 토스증권 보안팀에서 **안전하고 혁신적인 금융 서비스를 제공**하기 위한 여정에 함께하며, 끊임없이 성장하고 기여하겠습니다. 감사합니다.