

1. 자기소개 및 지원동기

안녕하세요. **인프라·보안 엔지니어**로 4년 이상 다양한 환경에서 ****보안 솔루션(서버·DB 접근제어, NAC, DLP, SIEM 등)****과 ****클라우드(AWS)****를 운영해온 **이재철**입니다. 저는 금융·교육·IT기업 등에서 **망분리, 취약점 점검, 침해위협 탐지·대응** 등 전방위적인 보안 업무를 맡아 **안정적인 서비스 환경**을 구현해 왔습니다. 특히 **POC/BMT**를 통해 새 솔루션을 검증·도입하고, **클라우드 보안** 아키텍처 설계에도 참여해왔습니다.

11번가는 대규모 이커머스 서비스로서 보안이 필수 역량이라 생각합니다. 고객 정보와 거래 데이터를 안전하게 보호하는 것은 곧 서비스 신뢰도와 직결되기 때문입니다. 그동안 쌓아온 **인프라 보안 경험**과 **클라우드 보안 지식**을 바탕으로, 11번가 정보보안팀에서 **안전한 IT인프라**를 함께 구축·운영해 보고 싶습니다.

2. 보유 역량 요약

- **서버·DB 접근제어 운영 경험**
 - 내부정보 유출 방지를 위해 **DB 계정권한 분리**, 감사로그 모니터링 체계화
- **NAC·DLP·SIEM 등 보안 솔루션 도입·운영**
 - NAC(네트워크 접근제어)로 단말 인증·상태 검사, DLP로 민감정보 유출 사전 차단, SIEM 연동으로 로그 통합 분석
- **AWS 기반 보안 아키텍처**
 - AWS VPC, Security Group, IAM, CloudTrail, GuardDuty 등 클라우드 네이티브 보안 구성
- **POC/BMT 및 침해위협 대응**
 - 신규 솔루션(접근제어, APT 등) 도입 전 시나리오별 성능·호환성 검증, 실제 운영 중 이슈 해결
 - IDS/IPS, APT 솔루션, Syslog·SIEM 연계로 **실시간 침해 징후 탐지** 및 신속 대응

3. 경력사항

(주)가온누리정보시스템 | 프리랜서 인프라 엔지니어

(2024.03 ~ 현재)

- **ATS(다자간매매채결회사) 인프라 구축·운영**

- 금융위원회 본인가 사전 준비를 위해 망분리, 서버·DB 접근제어, NAC, DLP 등 보안솔루션 설계
- Python 스크립트를 활용한 방화벽 100+ 룰 자동화, 기존 대비 정책 반영 시간 50% 절감
- APT 솔루션 도입으로 공격 패턴 사전 탐지, **거래 데이터 보호 및 침해사고 예방**

주요 성과

- 망분리 구축 후 내부정보 유출사고 0건 달성
- 금융규제 요건 충족 문서화 작업 주도, 본인가 심사 시 보안 측면 이슈 '무' 판정

(주)관텍투자일임 | **인프라·정보보호팀 인프라 엔지니어**

- **금융보안데이터센터(FSDC) 망분리** 환경 운영, DB 접근제어·DLP·VPN 정책 관리
- **AWS 환경**(EC2, S3, CloudTrail)에 대한 보안 검토, EC2 인스턴스 및 VPC 설정을 통해 안전한 내부망 구성
- **NAC** 솔루션 운영으로 단말 상태 실시간 검사, 백신·EDR 충돌 이슈 발견 시 예외 정책 적용

주요 성과

- 금융감독원 감사 대비 문서화·실무 운영, 개인정보 DB Audit 로깅 → 내부정보 유출사고 0건 유지
- Python 기반 자동화 스크립트로 장애발생률 40% 감소, 운영 효율 30% 이상 개선

(주)편엔씨 | **DevOps 엔지니어**

- **AWS 클라우드 운영**: EC2, VPC, Auto Scaling, Route 53 등 구성 및 모니터링
- 백업·복구 자동화(Shell/Python)로 장애 복구 시간 기존 2시간 → 1시간 내 단축

- Kubernetes 마이그레이션 초기 검토, 컨테이너 보안정책 수립 초안 작성

주요 성과

- 애플리케이션 장애 대비 복구 프로세스 확립, **MTTR(Mean Time To Repair) 50% 단축**
- DevOps-보안팀 협업해 CI/CD 파이프라인 일부 보안 점검 항목 추가

(주)조인트리 | 인프라·시스템 엔지니어

- **차세대 정보시스템(국민대학교)** 인프라 구축: Fortigate UTM, NAC, DLP, APT 등 통합 운영
- VMware NSX-T 기반 가상 네트워크 세분화, **안정적 서비스** 가용률 99.9% 유지
- OSS 모니터링 툴(Wazuh, Kibana) 도입으로 침해사고 발생 전 이상징후 80% 사전 탐지

주요 성과

- 장애 발생률 25% 감소, 전산팀 대응 속도 향상
- DLP 정책 최적화로 **민감정보 탐지율 20% ↑**, 업무 편의성도 함께 확보

(주)메타넷애플랫폼 | 인프라·시스템 엔지니어

- **대규모 콜센터(1,000명 규모) 재택근무 환경** 구축: Fortigate SSL VPN, NAC 연동, 백신 정책 적용
- Python으로 Cisco 스위치 점검 자동화, 점검시간 70% 단축
- 백신·EDR 충돌 시 Ansible 예외정책 적용, 장애 문의 월평균 40% 감소

주요 성과

- 재택근무 원격접속 안전성 향상, 문의 폭주 방지
- 내부 기획팀 협업으로 Fortigate VPN 계정정책 정비 → 계정 분실 이슈 50%↓ 개선

(주)엠티데이터 | 서버·시스템 엔지니어

(2017.02 ~ 2018.10)

- **한국항공우주산업(KAI)** 서버(50+대), 방화벽·IDS 운영, 주기적 취약점 분석 및 패치
- DB 접근제어 솔루션 초기 설정, 민감 데이터 감시 프로세스 확립

주요 성과

- 치명적 취약점 발견 후 2주 내 패치·보안정책 반영, 시스템 안정화
- 보안팀과 협업해 Audit 로그 분석 절차 수립 → 내부 감사 시 신속 자료 제출

4. 자격사항

- **CCNP** (Cisco Systems, 2020.08)
- **Red Hat Certified System Administrator (RHCSA)** (2019.01)
- **CompTIA Linux+, LPIC Level 1, 사무자동화산업기사, 리눅스마스터 2급** 등 보안·시스템 관련 자격

5. 입사 후 포부

1. 인프라보안 솔루션 최적화

- 11번가 서비스 특성에 맞춰 NAC, DLP, SIEM, 서버·DB 접근제어 등 **보안솔루션**을 고도화하고, **망분리나 클라우드 보안** 요구사항을 철저히 이행해 **안전한 이커머스** 환경을 구축하겠습니다.

2. 클라우드 보안 아키텍처 강화

- AWS 상에서 VPC·Security Group·IAM·CloudTrail·KMS 등 **보안 서비스**를 활용해, **데이터 보호** 및 **침해사고 예방**을 한층 더 강화하고자 합니다.

3. 취약점 점검·침해대응 프로세스 고도화

- 주기적인 서버·웹 취약점 점검, 실시간 위협 탐지 체계를 구축해 **즉각적인 대응** 프로세스를 마련하겠습니다. DevSecOps 문화를 정착해 개발·보안이 긴밀하게 협업하도록 노력하겠습니다.

이러한 역량과 의지를 바탕으로, 11번가가 **고객에게 안전한 서비스**를 제공하고, **글로벌 경쟁력**을 갖춘 이커머스 플랫폼으로 자리잡는 데 기여하겠습니다. 감사합니다.

