경력기술서

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

지원 포지션

당근마켓 - 보안팀

요약(Profile)

- 3년 이상 기업 보안솔루션(NAC, DLP, MDM, DB 접근제어 등) 도입·운영 및 **망분리**, **침해사고 예방** 경험 보유
- **AWS 보안서비스**(VPC, Security Group, IAM, CloudTrail 등) 운용 및 **클라우드 보안 아키텍처** 기본 이해
- **보안 모니터링** 시스템 구축 및 운영 노하우, 침해사고 및 정보유출사고 대응 절차 수립 역량 보유
- **유연한 사고방식**과 **협업 지향 커뮤니케이션** 능력을 통해, 빠르게 성장하는 서비스 환경에서도 **안전하고 효율적인 보안체계**를 달성해 왔습니다.

보유 역량 (Key Skills)

1. **엔드포인트 보안**
    - EPP, EDR, DLP, NAC, MDM 등 다양한 단말·모바일 보안솔루션 운영·정책 설계
    - 정책 충돌·에이전트 성능 이슈 발생 시 **분석→해결→자동화** 프로세스 구축
2. **DB 접근제어 및 망분리 운영**
    - 금융·교육기관 등 규제환경에서 망분리 환경 설계·구축, DB 접근제어 솔루션 운영
    - 계정·권한 관리, DB Audit 로그 모니터링을 통해 **정보유출 사고 예방**

3. **AWS 클라우드 보안**
    - VPC, Security Group, IAM, CloudTrail, GuardDuty 등 AWS 보안 서비스를 활용한 **리소스 보호**
    - EC2, S3, RDS 등 주요 서비스에 대한 접근제어, 로그 분석, 침해사고 예방 정책 수립
    - Terraform, Ansible 등 IaC 기반 인프라 관리 경험(기초 수준)
4. **보안 모니터링 & 침해사고 대응**
    - SIEM, SOAR, OSS 도구(Kibana, Wazuh 등)로 **이상징후 이벤트** 분석 및 알림 체계 구축
    - 실제 침해사고 대응 시 **Root Cause** 파악, 유관 부서 협업을 통한 빠른 조치 및 보고 체계 운영
5. **자동화 스크립팅 & 오픈소스 활용**
    - Python, Shell Script로 **보안정책 일괄 배포**, **로그 파싱/필터링** 작업 자동화
    - GitLab, Jenkins 등과 연계하여 보안 설정 버전 관리, CI/CD 파이프라인 일부 구성
6. **마이크로서비스 아키텍처 이해**
    - DevOps 환경에서 **API Gateway, Docker/Kubernetes** 등을 활용한 서비스 분산 구조 이해
    - MSA 내 보안(서비스 간 인증·권한, 컨테이너 이미지 취약점 스캔) 적용 사례 검토

자격사항

- **CCNP** (Cisco Systems, 2020.08)
- **사무자동화산업기사** (한국산업인력공단, 2019.12)
- **CompTIA Linux+** (CompTIA, 2019.02)
- **LPIC Level 1** (Linux Professional Institute, 2019.02)
- **Red Hat Certified System Administrator (RHCSA)** (Red Hat, 2019.01)

- **리눅스마스터 2급 (국가공인)** (사)한국정보통신진흥협회, 2019.01

경력사항 (총 경력 약 7년+)

1) ㈜엠티데이타 | 서버·시스템 엔지니어

(2017.02 ~ 2018.10)

- **Linux 서버 및 보안 솔루션(방화벽, IDS) 운영**
- 취약점 분석, 방화벽 정책 최적화 → **정책 중복 30% 제거**, 트래픽 지연 완화
- DB 접근제어 초기 구성 지원, Audit 로그 기반 권한 남용 사례 정기 점검

---

2) ㈜메타넷엠플랫폼 | 인프라·시스템 엔지니어

(2019.12 ~ 2021.08)

- **대규모 콜센터(약 1,000명) 재택근무 환경 구축**
    - Fortigate SSL VPN + NAC 솔루션 연동해 사용자 단말 검증, 위험 단말 격리
    - 백신/EDR과 VPN 간 충돌 발생 시 예외 정책 자동화(Ansible)로 **장애 문의 40% 감소**
- **AWS 기반 일부 서비스 보안 설정**(S3 접근제어, CloudWatch 로그 모니터링)

---

3) ㈜조인트리 | 인프라·시스템 엔지니어

(2021.09 ~ 2022.04)

- **국민대학교 차세대 정보시스템 인프라 구축**
    - UTM(Fortigate), NAC, DLP, APT, DB 접근제어 솔루션을 통합 운영
    - **망분리 환경** 도입 → 내부망/외부망 트래픽 흐름 통제, 민감 정보 유출 사건 감소
- OSS 기반 보안 시스템(Kibana, Wazuh)으로 이상징후 모니터링 체계 구축

---

4) ㈜펀엔씨 | DevOps 엔지니어

(2022.05 ~ 2022.07)

- **AWS 클라우드 운영**: EC2, Auto Scaling, Route 53, S3 등
- **MDM 도입 검토**: 사내 모바일 기기 관리 정책, 벤더 비교(BMT) 주도
- Python/Shell을 활용한 백업·복구 자동화, 장애 발생 시 Slack 알림

---

5) ㈜콴텍투자일임 | 인프라·정보보호팀 인프라 엔지니어

(2022.08 ~ 2024.03)

- **금융 인프라 운영**: AI 기반 주식투자 앱 서버·네트워크·보안 운영 (망분리, DLP, DB 접근제어, VPN)
- 금융감독원·ISMS-P 요구사항 준수, 침해사고 대응 프로세스 작성 및 시뮬레이션
- AWS 보안서비스(CloudTrail, GuardDuty) 일부 연동해 **실시간 이상징후 알림** 구축

---

6) ㈜가온누리정보시스템 | 인프라 엔지니어(프리랜서)

(2024.03 ~ 현재)

- **ATS(다자간매매체결회사) 망분리·보안 인프라**: NAC, DLP, SSL 복호화 등 통합 운영
- Python 스크립트로 **방화벽 정책 자동화**(100+ 룰 일괄 등록) → 작업시간 50% 절감, 인적 오류 최소화
- 침해사고 예방: NAC·DLP 로그 기반 이례적 접근 패턴 조기 감지 및 격리 프로세스 운영

주요 프로젝트 & 기여도

1. **AWS 기반 보안 모니터링 시스템 구축**
    - GuardDuty, CloudTrail, Security Hub 등을 통해 **핵심 로그 실시간 수집**, 이상징후 자동 알림
    - 매주 발생 이벤트 분석 후 **보안 규칙 추가/수정**으로 사고 예방률 상승

2. **엔드포인트(DLP, MDM, NAC) 통합 운영 고도화**
    - 규모: 사내 PC/모바일 기기 약 1,000대 이상
    - 문제: DLP & 백신 실시간 스캔 충돌 → PC 성능 저하, 사용자 불편 발생
    - 해결: **벤더 협업**으로 스캔 시점 분리, MDM 로그 모니터링 강화 → 장애 문의 35% 감소
3. **망분리 환경 도입 & DB 접근제어 솔루션 운영**
    - 주요 서버·DB 구간을 물리·논리적으로 분리, **DB Audit** 로그 집중 관리
    - 민감 정보 접근 이력 실시간 모니터링, 이상 트랜잭션 자동 알림 → 내부 유출사고 0건 유지
4. **보안 사고 대응 사례**
    - APT 솔루션이 의심 파일 감지 → 샘플 분석, 내부 PC 확산 여부 검사 후 격리 조치
    - **Root Cause**: 외부 이메일 링크 통해 악성파일 유포
    - 결과: 초기 단계에서 조치해 전사 확산 전 차단, 추가 피해 없음

당근마켓 지원동기

당근마켓은 지역기반 커뮤니티로서, 사용자들에게 신뢰도 높은 서비스를 제공해야 한다고 생각합니다. 오랜 기간 보안솔루션(엔드포인트, DB 접근제어, MDM), 망분리, **AWS 보안서비스** 운영 경험을 통해 **"안전하면서도 유연한"** 보안 체계를 구축해온 제 노하우를 당근마켓 보안팀에서 적극 발휘하고 싶습니다.

- **엔드포인트 & DB 접근제어**: PC·모바일 기기, DB, 망분리까지 **통합 보안 환경** 구축·운영 경험
- **AWS 클라우드 보안**: GuardDuty, CloudTrail 등 실무 운용, 오픈소스 모니터링 툴과 연계해 **침해사고 예방**
- **침해사고 대응 & 자동화**: Python, Shell Script 등을 통해 반복 업무를 자동화하여 **운영 효율**과 **정확도**를 동시에 확보

기술적 보안성 검토·도입부터 운영·모니터링·사고 대응까지 전 주기에 참여해, **당근마켓**이 더욱 안전하고 신뢰받는 서비스를 제공하도록 기여하겠습니다.

마무리

- **성격**: 문제 해결 시 꼼꼼함과 집요함을 갖추고 있으며, 이해관계자에게 **알기 쉽게** 보안 이슈를 설명하는 소통 능력을 지니고 있습니다.
- **향후 계획**: 마이크로서비스 아키텍처(MSA) 및 오픈소스 보안 툴에 대한 이해를 넓히고, **SOAR** 등 자동화된 대응 체계를 더욱 고도화하고 싶습니다.

본인은 **유연한 사고방식**과 **꼼꼼한 업무 처리**를 기반으로, 당근마켓이 **사용자 신뢰**를 더욱 높이는 데 기여하고자 합니다. 감사합니다.