# 최승우

**지원 직무 :** 보안엔지니어

**지원 회사 :** 안랩

경기도 성남시 분당구 판교역로 231, 13486

(+82) 10-5544-2211

sw_choi.security@vmail.com

## 경력

### 경력 한국인터넷진흥원(KISA), 서울 — 인턴

2023 년 7 월 - 2023 년 8 월

공공기관 보안 관제 시스템 모니터링 보조 및 일일 위협 분석 보고서 작성 지원 업무를 수행하였습니다. 보안 취약점 점검 스크립트의 기초 설계를 도우며 실무적인 방어 기제를 학습했습니다.

## 학력

### 학력 세종대학교 — 정보보호학 학사

2019 년 3 월 - 2025 년 2 월

### 중앙고등학교 — 인문계

2016.03 - 2019.02

## 프로젝트

### 오픈소스 기반 침입 탐지 시스템(IDS) 구축 프로젝트

2024.03 – 2024.06 (한 학기)

본 프로젝트는 학내 가상 네트워크망의 보안 강화를 위해 추진되었으며, 저는 팀장으로서 환경 구축 및 탐지 규칙 설계를 주도했습니다. Snort 를 활용하여 실시간 패킷 수집 환경을 조성하고, SQL 인젝션 및 DDoS 공격 시도를 90% 이상 식별해내는 성과를 거두었습니다. 특히 기존 시스템의 한계인 가시성 문제를 해결하고자 로그 분석 자동화 툴과 시각화 대시보드를 직접 연동하여 위협 수준을 직관적으로 파악하게 설계했습니다. 이를 통해 인프라 보안의 실무적 기초를 다졌으며 프로젝트 전반에 100% 기여하여 기술적 문제 해결 역량을 증명했습니다.

## 수상 경력

교내 정보보안 경진대회 장려상 | 2024.06

교내 캡스톤 디자인 프로젝트 우수상 | 2024.11

## 자격증

정보보안기사 | 2024.05 취득

리눅스마스터 2 급 | 2023.11 취득

네트워크관리사 2 급 | 2023.09 취득

## 언어능력

TOEIC 850 점 | 2024.07 취득

JLPT N2 | 2023.12 취득

# 자기소개서

**해당 회사 및 직무를 지원한 이유를 설명하고, 입사 후 직무전문성을 확보하기 위한 구체적인 성장계획을 기술해 주십시오.**

안랩은 대한민국 보안의 자부심이며, 제가 가진 보안 전문가로서의 윤리 의식과 사명감을 가장 잘 실천할 수 있는 터전입니다. 중학생 시절 지인의 개인정보 유출 피해를 목격하며 느꼈던 보안의 중요성을 바탕으로, 정보보호학을 전공하며 전문성을 쌓아왔습니다. 수많은 자산을 지켜내는 안랩의 통합 보안 솔루션에 저의 기술적 열정을 더해 사회 안전망 구축에 기여하고자 지원했습니다. 입사 초기에는 안랩 고유의 위협 분석 시스템을 완벽히 숙달하여 실시간 모니터링 업무에서 단 하나의 이상 징후도 놓치지 않는 무결점 탐지율을 유지하겠습니다. 이후 3 년 내에는 머신러닝 기술을 보안 실무에 접목하여 지능형 위험 탐지 및 자동 탐지 알고리즘 최적화 프로젝트를 주도적으로 수행하겠습니다. 최종적으로는 급변하는 글로벌 위협 트렌드를 선제적으로 분석하고 대응할 수 있는 보안 아키텍처 전문가로 성장하여, 안랩이 글로벌 보안 시장의 초격차를 유지하는 데 핵심적인 역할을 수행하겠습니다.

**지원 분야와 연관된 협업 경험 1 건을 선택하여, 본인의 역할/기여/의사결정과정/결과를 설명하고, 이를 통해 얻은 구체적인 배움이나 변화를 기술해 주십시오.**

KISA 인턴 당시 공공기관 보안 관제 시스템을 모니터링하며 일일 위협 분석 보고서 작성을 지원했습니다. 당시 방대한 로그 데이터 중 유의미한 위협을 선별하는 과정에서 분석 기준에 대한 팀원 간 의견 차이가 발생했습니다. 저는 꼼꼼한 성격을 발휘해 과거 사고 사례와 대조 분석한 기초 자료를 팀에 제시하며 객관적인 판단 근거를 마련했습니다. 특히 분석 효율을 높이기 위해 반복되는 패턴을 식별하고 이를 자동화할 수 있는 보안 취약점 점검 스크립트의 기초 설계를 제안하는 의사결정을 내렸습니다. 팀원들과의 긴밀한 소통 끝에 스크립트를 적용한 결과, 보고서 작성 시간을 단축하고 분석의 정확도를 높이는 성과를 거두었습니다. 이 과정을 통해 보안 업무는 개인의 기술력 못지않게 팀원 간의 투명한 정보 공유와 협력이 필수적임을 깨달았습니다. 이러한 소통 중심의 태도를 안랩의 협업 프로세스에도 녹여내어 조직의 시너지를 극대화하겠습니다.

**지원 분야와 가장 밀접한 연구 또는 프로젝트 1 건을 선정하여, 문제 정의/접근 방법/성과/한계 및 배운 점을 중심으로 구체적으로 기술해 주십시오.**

학내 가상 네트워크망을 대상으로 한 '오픈소스 기반 IDS 구축 프로젝트'를 수행했습니다. 당시 문제는 기존의 단순 로그 적재 방식으로는 실시간으로 고도화되는 웹 공격에 신속히 대응하기 어렵다는 점이었습니다. 이를 해결하기 위해 리눅스 환경에서 Snort 를 활용해 패킷 수집 환경을 구축하고, SQL 인젝션 및 DDoS 공격 유형에 맞춘 정교한 규칙 기반 탐지 정책을 설계했습니다. 그 결과 시뮬레이션된 공격 시도의 90% 이상을 식별해냈으며, 탐지된 위협을 대시보드와 연동해 관리자가 즉각 인지할 수 있도록 가시성을 확보했습니다. 다만, 규칙에 정의되지 않은 변칙적인 제로데이 공격에 대한 대응에는 한계가 있음을 확인했습니다. 이를 통해 규칙 기반 보안의 기초를 탄탄히 다지는 동시에, 향후 행위 기반 분석 및 AI 를 활용한 보완의 필요성을 절감했습니다. 이 경험은 인프라 보안의 실무적 메커니즘을 이해하고, 문제 해결을 위해 기술적 한계를 분석하는 능동적인 태도를 갖추게 해주었습니다.

**급변하는 업무 환경에 대응하기 위해 본인이 보유한 기술적 기초와 이를 새로운 도구(AI/자동화 등)에 접목하기 위한 본인만의 학습 노하우를 기술해 주십시오.**

저는 네트워크 패킷 분석(Wireshark), 리눅스 시스템 관리, 방화벽 설정 및 운영이라는 보안 엔지니어링의 핵심 기초 역량을 보유하고 있습니다. 이러한 기초는 새로운 도구나 기술을 도입할 때 데이터의 본질적인 흐름을 빠르게 파악하고 적재적소에 기술을 적용할 수 있는 강력한 무기가 됩니다. 저의 학습 노하우는 '실무 중심의 점진적 내재화'입니다. 새로운 기술이 등장하면 이론 공부에 그치지 않고, 이를 기존의 분석 환경에 직접 시뮬레이션해 봅니다. 최근에는 침입 탐지 로그의 효율적 처리를 위해 머신러닝 알고리즘을 공부하며 탐지 모델을 개인 프로젝트에 테스트하고 있습니다. 이러한 능동적 학습 습관은 안랩의 최첨단 위협 탐지 시스템에 새로운 기술이 도입될 때 누구보다 빠르게 적응하고 성과를 내는 원동력이 될 것입니다. 급변하는 보안 시장에서 기초가 튼튼한 기술력을 바탕으로 AI 및 자동화 툴을 능숙하게 다루어 안랩의 기술 경쟁력을 한 단계 더 끌어올리겠습니다.