입 사 지 원 서(예시)

지원부문	정보보안	희망연봉	2300만원	사진

1. 인적사항

성명	(한글)이혜원 /(영문)Lee Hye Won	생년월일	2003.10.29
E-MAIL	wonq1029@gmail.com	전화번호	010-8672-1958
주소			

2. 학력 및 교육사항

기간	학교	학과(학점)	졸업구분
2022.03~2026.02	대구대학교	컴퓨터소프트웨어(3.5/4.5)	졸업예정
2019.02~2021.12	거제고등학교	인문계	졸업

교육사항				
	교육기간(총)	2025.07.16~2026.01.05	**교육시간**	09:00~18:00(주 5 일)
	교육기관	코리아 IT 아카데미대구	**교육과정명**	정보보안
	교육내용			
	보안 전문가 양성을 위한 프로젝트 기반 교육과정			

3. 병역 및 기타사항

병역	해당사항 없음	**군별**		**계급**		**기간**		**병과**	

4. 포트폴리오 주소

깃허브	kk-wonq.github.io

자 기 소 개 서

1)지원동기	소제목

시스템의 구조를 이해하고 보안을 강화하는 일에 매력을 느껴 정보보안 분야를 선택했습니다.

대학교에서 컴퓨터소프트웨어개발을 전공하며 개발 지식을 쌓는 과정에서, 시스템이 작동하는 원리와 구조를 이해하는 일에 자연스럽게 흥미를 느꼈습니다. 이후 진로를 탐색하며 정보보안 관련 직업훈련 과정을 수강했고, 그 과정에서 이 분야가 저의 적성과 흥미에 잘 맞는다는 것을 깨달았습니다.

특히 네트워크 보안의 기반이 되는 리눅스 명령어와 네트워크 체계를 이해하며 시스템을 직접 다루는 과정에서 확실한 자신감을 얻었습니다. 이 경험을 통해 시스템과 네트워크를 보호하고 관리하는 일의 중요성을 체감했으며, 이제는 이론을 넘어 실무 환경에서 로그 분석과 위협 탐지 역량을 강화하고자 합니다.

입사 후에는 이러한 경험을 바탕으로 보안 시스템을 운영·분석하며 실무 역량을 꾸준히 강화하고, 안정적인 네트워크 환경을 구축하는 보안 전문가로 성장하겠습니다.

2)성장과정	소제목

저는 주어진 일에 최선을 다하고, 신뢰를 바탕으로 협력하는 과정을 통해 성장해왔습니다.

본래 저는 팀을 이끄는 역할보다 묵묵히 맡은 일을 수행하는 것을 선호하는 성향이었습니다. 하지만 대학교 첫 팀 프로젝트에서 우연히 팀장을 맡으며 리더십의 책임감과 즐거움을 처음으로 느꼈고, '환경 보호' 캠페인 프로젝트를 성공적으로 이끌며 팀원들의 의견을 조율하고 공동의 목표를 달성하는 보람을 경험했습니다.

이후 직업훈련 과정에서도 팀장을 맡아 팀워크 중심의 리더십을 발휘하고자 노력했습니다. 특히 그 중요성은 웹 CTF 문제 해결 과정에서 빛을 발했습니다. 문제의 단서를 찾지 못해 모두가 막막하던 상황에서, 저는 해결책을 지시하기보다 각자의 생각을 공유하는 브레인스토밍을 제안했습니다. 그 결과 한 팀원은 웹페이지 소스코드의 주석 처리된 경로를, 다른 팀원은 네트워크 탭에서 실패하는 API 요청을 발견했습니다. 저는 이 두 단서를 연결해 '주석 처리된 경로가 숨겨진 엔드포인트일 것'이라는 가설을 세우고 분석을 진행, 파라미터 검증이 미흡한 SQL 인젝션 취약점을 찾아내 문제를 해결할 수 있었습니다.

이 경험을 통해 리더란 모든 해답을 아는 사람이 아니라, 구성원의 잠재력과 다양한 관점을 하나로 모아 시너지를 만드는 사람임을 깨달았습니다. 팀의 협력을 통해 개인의 한계를 넘어서는 성과를 경험했고, 이러한 경험은 조직 내에서도 원활한 소통과 협업으로 시너지를 만드는 기반이 될 것입니다.

입사 후에도 주어진 역할에 충실하면서 팀원들과 적극적으로 협력해, 함께 성장하고 문제를 해결하는 구성원이 되겠습니다.

3)성격의 장단점	소제목

저의 가장 큰 강점은 어떤 일이든 끝까지 책임지고 완성도를 높이는 꼼꼼함입니다.

최근 진행한 '네트워크 침입 탐지 시스템 구축' 팀 프로젝트에서 이러한 강점이 빛을 발했습니다. 프로젝트 진행 시 Snort 를 이용해 특정 패턴의 패킷을 탐지하는 규칙을 설정했지만, 테스트 과정에서 일부 패킷이 간헐적으로 유실되는 문제가 발생했습니다. 팀원들은 큰 문제가 아니라고 여겼지만, 저는 로그 파일의 작은 불일치가 마음에 걸려 원인 분석을 시작했습니다. 가상 환경 설정부터 방화벽 정책, Snort 규칙까지 단계별로 점검한 결과, 특정 프로토콜 옵션의 미세한 설정 오류가 원인임을 찾아냈고, 이를 수정한 뒤 시스템은 100% 탐지율을 기록하며 프로젝트를 성공적으로 마무리했습니다.

반면, 이러한 꼼꼼함이 때로는 하나의 문제에 지나치게 몰두하게 만들어 전체적인 흐름을 놓치는 단점으로 작용하기도 했습니다. 수업 중 실습 과제를 수행할 때, 강사님께서 "이 부분은 넘어가도 좋습니다"라고 하신 사소한 설정 오류에도 집착해, 다음 진도를 놓친 경험이 있었습니다.

이후 이러한 단점을 보완하기 위해 '타임박싱(Time-boxing)' 기법을 도입해 업무 우선순위를 관리하고 있습니다.문제에 직면하면 중요도를 판단하고 '최대 30 분만 투자하자'와 같은 제한을 두며, 해결되지 않으면 진행 상황을 기록하고 다음 업무로 넘어갑니다.

이 과정을 통해 꼼꼼함이라는 장점은 유지하면서도, 제한된 시간 안에 효율적으로 목표를 달성하는 균형 잡힌 태도를 익혔습니다. 입사 후에도 이러한 자세로 맡은 업무를 정확하고 신속하게 수행하며, 팀의 신뢰를 얻는 구성원이 되겠습니다.

4)입사 후 포부	소제목

보안을 단순한 시스템 관리가 아닌, 조직의 신뢰를 지키는 핵심 업무로 여기며 실무형 보안 전문가로 성장하겠습니다.

입사 초기에는 회사의 보안 시스템 구조와 네트워크 환경을 빠르게 파악하고, 보안 장비 운영 및 로그 분석 등 기본 업무를 정확하게 수행하겠습니다. 또한 사내 보안 정책과 대응 절차를 적극적으로 익혀 실무 적응력을 높이겠습니다.

중기에는 Suricata 와 SIEM 등 보안 솔루션을 활용해 침입 탐지와 이상 트래픽 분석 역량을 강화하고, 실제 공격 사례를 분석하여 내부 보안 취약점을 사전에 파악하고 개선 방안을 제시할 수 있는 인재로 성장하겠습니다.

장기적으로는 축적된 경험을 바탕으로 보안 정책 수립과 시스템 개선에 참여해 회사의 보안 체계를 한층 고도화하며, 안전한 서비스 환경을 구축하는 데 기여하겠습니다.

꾸준한 학습과 책임감 있는 자세로 조직의 신뢰를 지키는 보안 전문가로 자리매김하겠습니다.

5) 직무관련 경험	소제목

직무관련 경험으로 직업훈련과정에서의 프로젝트 내용으론 JAVA,Spring,Linux,Burpsuite,Suricata 등의 기술을 기반으로 보안 실습과 팀 프로젝트를 수행하며 직무 핵심 기술을 다뤄보았습니다. 특히 IDS 와 IPS 를 활용한 침입 탐지 실습, Log Analyzer 를 통한 로그 분석, 그리고 웹서버 구축 및 모의해킹 훈련을 경험하며 보안 환경 전반에 대한 이해를 넓혔습니다. 해당 직업 훈련과정 중, 첫 팀 프로젝트에서는 소통 부족으로 어려움이 있었지만, 빠른 결과 도출 후 부족한 부분을 토론하며 완성도를 높였습니다. 이후에는 사전계획과 지속적인 의견 교환을 통해 더 효율적이고 완성도 높은 결과를 얻을 수 있었습니다.

이러한 경험을 통해 보안 직무에 필요한 기술력과 문제 해결력, 그리고 협업 능력을 실제로 갖추게 되었고, 입사 후에도 빠르게 업무에 적응하며 조직에 기여할 수 있을 것이라 확신합니다. 꼼꼼함과 책임감을 바탕으로 보안 전문가로 성장해 나가겠습니다.

프로젝트 소개서

수행프로젝트	항목	주요내용
	프로젝트 명	가상 전자상거래 서비스 '장보고마켓' 웹/모바일 모의해킹 및 대응 분석
	수행기간	2025.11.24-2025.01.05
	목표	웹, 모바일 서비스 대상 주요 보안 취약점을 식별하고, 실제 공격 시나리오 기반 취약점을 검증함. 대응 조치 적용 후 공격 차단 여부 확인 과 로그 및 경보를 통한 보안관제 동작 검증함.
	내용	실무 운영 환경과 동일한 고가용성 전자상거래 서비스(Web/App)를 구축하여, 공격자(Red Team)와 방어자(Blue Team)의 시각을 아우르는 입체적인 모의해킹 프로젝트를 수행했습니다. 본 프로젝트의 핵심 목표는 단순한 취약점 제거를 넘어, 보이지 않는 위협을 데이터로 시각화하여 능동적인 대응 체계를 수립하는 것이었습니다. 이를 위해 **심층 방어(Defense in Depth) 전략**을 기반으로 인프라를 설계했습니다. 네트워크 경계에는 **PfSense** 와 Suricata(IDS/IPS)를 배치하여 내부망(Private Network)을 격리하고 비정상 트래픽을 1 차 소거했으며, 애플리케이션 앞단에는 ModSecurity(WAF)를 적용하여 SQL Injection, XSS 등 OWASP Top 10 공격을 정밀 차단하는 이중 방어막을 형성했습니다. 나아가 파편화된 보안 로그를 하나의 인텔리전스로 통합하는 **관제 데이터 파이프라인**을 완성했습니다. 서버, 방화벽, WAF, 모바일 앱에서 발생하는 이기종 로그를 **rSyslog** 로 중앙 집중화한 후, 성격에 따라 Wazuh(위협 탐지), ELK(앱 사용성 분석), Splunk(웹 공격 시각화)로 분산 처리하여 실시간 모니터링 환경을 구축했습니다. 이를 통해 고위험 취약점을 완벽히 조치함은 물론, 공격 시도 시 탐지-분석-대응에 이르는 소요 시간(MTTR)을 단축하고 데이터 기반의 보안 의사결정 프로세스를 입증했습니다.
	설계/프로세스	웹서버 frontend&backend : React,Tailwind CSS 기반의 웹 프론트 엔드와 Node.js 백엔드, MairaDB 로 구성된 3-Tier 아키텍처를 구축했습니다. Mobile : Android Studio 를 활용하여 웹과 연동되는 하이브리드 모바일 앱 환경을 구성했습니다. 보안관제 : 방어계층으로 pfsense 와 suricata 를 구축하여 웹서버를 pfsense 내부망으로 옮기고 악성트래픽을 1 차로 필터링 하고 WAF 를 배치하여 트래픽을 검사하여 차단합니다. 관제계층으로 rSyslog 로 이벤트 로그들을 수집하여 Wazuh 로 전달하여, 서버 및 모바일 앱 로그를 중앙 집중화하여 시스템 이상징후를 통합 모니터링 합니다. 수행 프로세스: Burpsuite, SQLMAP 등을 사용하여 공격수행. WAF 룰 셋으로 대응하고 검증합니다.
	담당 역할	팀장 및 PM 수행을 위해 전체 프로젝트 일정관리 및 취약점이 있는 웹서버, 모바일을 개발했습니다. 또한 웹/모바일 취약점들을 직접 구현하고 정밀 분석하여 공격하고 보고서로 정리하여, 대응방안을 구축하였습니다. WAF 룰을 작성하여 취약점 공격 시 대응할 수 있도록 방어체계를 구축하였습니다. 또한 공격시도가 들어올 경우 적재되는 WAF 로그를 보다 효율적으로 관리하기 위해 Splunk 관제 도구를 연동하여 공격별 탐지 대시보드를 구축하고 실시간 위협 모니터링을 수행하였습니다..
	느낀점/성장점	공격의 원리를 알아야 완벽한 방어가 가능하다는 것을 체득했습니다. 직접 취약점을 찾아내고 코드를 수정하며 방어하는 과정을 통해, 개발 단계의 보안(Security by Design)이 얼마나 중요한지 깨달았습니다. 또한, Splunk 를 활용해 보이지 않던 위협을 시각화하면서 데이터 기반의 의사결정 역량을 기를 수 있었으며, 이를 통해 실무형 보안 전문가로서의 자신감을 얻었습니다.