김윤성

kys980819@gmail.com · 경기도 부천시
kysportfolio.site · velog.io/@kys980819 · github.com/kys980819

kysportfolio.site에서 더 자세한 포트폴리오를 보실 수 있습니다. 프로젝트 전 과정과 보고서 원문, 질문에 답하는 챗봇을 준비해 두었으니 방문해 주세요.

소개

모르는 문제를 조사하여 직접 풀어 나가며, **IDS 탐지 환경을 직접 구축**하고 악성코드를 정적·동적·네트워크로 **분석해 IOC를 도출**하고 **탐지 룰로 검증**하는 흐름을 단독으로 끝까지 수행했습니다.
3교대 보안 근무 1년 무결근으로, 관제 현장의 지속 근무에도 준비 되어 있습니다

보유 기술

보안 / 관제	**탐지:** Snort(IDS 룰 작성·검증), BASE(탐지 대시보드) **악성코드 분석:** 기초(ExeinfoPE·DIE), 언패킹(mal_unpack·de4dot), 정적(PEview·BinText), 동적(ProcMon·Process Explorer·Autoruns) **네트워크 분석:** Wireshark(패킷 분석), CurrPorts(연결 확인)
네트워크	OSI 7계층, TCP/IP·UDP·HTTP/HTTPS·SSH·DNS
OS / 가상화 / 클라우드	Linux, Windows, VMware, AWS EC2, Vercel
개발(바이브코딩)	Node.js, React, Next.js, Python/Flask, MongoDB, Supabase
형상관리	Git / GitHub
문서화	분석 보고서·분석 노트 작성, MS Word·PowerPoint

프로젝트 & 성과

Snort IDS 탐지 환경 구축 + 악성코드 분석 (CEaN.exe / 정보탈취형)

기간 2026.05.11 ~ 2026.06.05 · 메인 프로젝트 · 단독 수행

- **IDS 환경 구축** - VMware 격리 환경에 Snort 2.9.2.3 + BASE + MySQL 기반 실시간 IDS 직접 구축 (Windows 미러링 제약을 단일 VM 으로 재설계, 버전 호환성은 다운그레이드로 해결)
- **탐지 룰 작성·검증** - IOC 기반 Snort 룰을 작성·BASE 로 검증하고, 탐지 누락 발생 시 원인(체크섬 오프로드)을 트래픽→인터페이스→룰 문법→패킷 처리 순으로 좁혀 -k none 으로 해결
- **검체 선별** - "C2 통신·평문 통신" 두 기준을 세워 MalwareBazaar 에서 반복 검증으로 검체 선별
- **분석·IOC 도출, 보고서 작성** - 기초·정적·동적·네트워크 분석으로 자격증명 수집→평문 SMTP 유출→Run 키 지속성을 실증하고, 파일·레지스트리·네트워크 IOC 도출 및 분석 보고서로 정리 (수동 언패킹 등 심화 코드 분석은 제외하고, 자동화 도구를 이용한 메모리 추출까지만 수행

악성코드 분석 실습 (bton02 / dgrep.exe)

기간 2026.03 ~ 2026.04 보조 프로젝트 · 단독 수행

- **분석 절차 표준화** — VM 격리 환경에서 기초·정적·동적·네트워크 분석 절차를 직접 정립하고, 도구별 분석 노트 양식을 설계해 두 검체에 동일 적용
- **bton02** — 트로이목마·다운로더 유형(VirusTotal 기준) 분석, 분석 노트로 기록
- **dgrep.exe** — 트로이목마·백도어 유형(VirusTotal 기준) 분석. 자기복제·페이로드 로드·Run 키 지속성을 규명하고 C2 통신이 전송 시도 단계임을 판별, 네트워크 IOC 기반 보고서 작성

포트폴리오 사이트 (kysportfolio.site)

기간 2025.09 ~ 지속 개선 중 · 단독 기획·구현·배포

- **취약점 대응** — React Server Components 원격 코드 실행 취약점(CVE-2025-55182) 공개 시, 영향 버전 확인해 패치 버전(Next.js 15.5.7)으로 즉시 재배포
- **공급망 사고 대응** — Vercel 공급망 침해(서드파티 AI 도구 OAuth 토큰 탈취로 고객 환경변수 노출) 시, 영향 가능성 판단해 환경변수·API 키(OpenAI·MongoDB 등) 전수 교체
- **보안 점검** — Claude Code 기반 점검 수행: /api/sendMessage 에 요청 속도 제한(rate limit) 적용, 의존성 취약점 정리, /api/health 정보 노출 축소
- **사이트 구현·배포** — Next.js·React·Node.js 와 MongoDB 로 OpenAI API 챗봇 포함 개인 사이트 구현, Vercel·AWS EC2 배포부터 도메인·DNS·HTTPS·CI/CD·SEO 까지 수행하며 프론트·백엔드·네트워크를 아우르는 IT 전체 흐름 체득

관련 자료 (포트폴리오 사이트에서 다운로드 가능)

- Snort IDS 탐지 프로젝트 보고서
- 악성코드 분석 보고서 [CEaN.exe(AgentTesla)]
- 악성코드 분석 보고서 [dgrep.exe]

경력

회사 / 기간	휴먼TSS (삼성전자 사업장 시설보안) · 2023.11 ~ 2024.11 (1년) - 졸업 유예 기간 중 근무 시작
담당 업무	출입증 발급·출입객 관리, 보안검색(금속탐지·문서감응·엑스레이), 반입·반출 통제, 사업장 순찰, 모의훈련(무단반출·침입·화재) 대응
주요 성과	• 다수 게이트에서 대규모 인원 출입을 통제하며, 주주야야비비 3교대 근무를 1년간 지각·결근 없이 수행 • 단독 근무가 많은 초기 환경에서 표준업무절차를 자기 언어로 재구성한 절차서를 비번에 직접 제작해 빠르게 적응, 동기·선배보다 이른 적응으로 신뢰도 있는 평가 받음 • 다양한 매뉴얼과 지속적으로 올라오는 공지를 빠르게 숙지해 이후 선배들이 먼저 업무를 확인하는 위치가 됨

보조 경험 — 네트워크 구성

- 기가 지원 스위치 교체로 기가인터넷 구간을 확대하고, 이후 통신사 공유기가 방마다 분할하던 분절 구조를 거실 무선 공유기 중심의 단일 서브넷(하나의 로컬 네트워크)으로 통합해 홈네트워크를 단계적으로 재구성

자격증 · 교육 · 학력

자격증 리눅스마스터 2급 (2025.12) · 정보처리기사 필기 합격 (2026.03, 실기 응시 예정)

교육 현직 실무자가 부여한 과제를 매주 직접 해결하며 학습 (2025.08 ~ 현재) - IT 전반의 이해를 다진 뒤 보안·네트워크와 보안관제로 심화, 상기 프로젝트를 직접 수행

학력 호서대학교 법경찰행정학과 (비전공) · 2024.08 졸업

병역 육군(의무경찰) 병장(수경) 만기전역

근무 조건 24시간(3교대) 교대근무 가능 · 해외여행 결격사유 없음