홍승표

Offensive Security Researcher · 경력기술서

newbiepwner@kakao.com 서울특별시 phantomn.github.io phantomn ph4nt0m

요약

금융권 Web/App 모의해킹부터 OT/ICS(IEC 62443)·IoT·의료기기(FDA) 보안, 사이버 공방 훈련 개발까지 24건 이상의 프로젝트를 수행한 Offensive Security Researcher. LS ELECTRIC 자동화기기 Achilles Communication Certificate Level 2 인증 취득, NATO CCDCOE Locked Shields 2025 DFIR CTF 1위, Linux Kernel CVE 16건 + IoT CVE 5건 + FVE 3건 보유.

핵심 역량

- 금융·공공 전자금융기반시설 Web/App 모의해킹 — 저축은행·캐피탈·증권·보험·제조 등 12개 사이트 수행 (A3 Security)
- OT/ICS 보안 — IEC 62443-4-2 Threat Modeling·모의해킹, LS ELECTRIC Achilles Communication Certificate Level 2 인증 취득
- IoT 취약점 분석·보안 도구 개발 — 스마트빌딩 IoT 탐지, IoT/CCTV 침해사고 조사 도구, Linux Kernel File System Fuzzer로 CVE 16건 도출
- 의료기기 보안 — FDA eSTAR 컨설팅 및 Web/App·의료기기 모의해킹, 보안인증(Cybersecurity Controls) 취득 지원
- 사이버 공방 훈련 개발·운영 — 한국전력 ELECCON, NATO CCDCOE Locked Shields 2025 DFIR CTF 1위, APEX CTF 2025 문제 개발

경력

코어시큐리티 (CoreSecurity), ICS 보안연구팀 주임 연구원 — 서울, 6월 2021 – 현재

- OT/ICS 보안 — IEC 62443-4-2 Threat Modeling·모의해킹, LS ELECTRIC Achilles Level 2 인증 취득, 자동화 점검 도구 개발
- IoT 보안 — 스마트빌딩 IoT 취약점 탐지 기술 개발·실증, IoT/CCTV 침해사고 조사 도구 개발
- 의료기기 보안 — FDA eSTAR 컨설팅 및 Web/App·의료기기 모의해킹
- 사이버 공방 훈련 — 한국전력 ELECCON 운영·문제 개발, Locked Shields 2025 DFIR CTF 1위, APEX CTF 2025 문제 개발

A3 Security, 보안기술팀 사원 — 서울, 6월 2020 – 6월 2021

- 금융권·공공기관 전자금융기반시설 모의해킹 12개 사이트 — 고위험 취약점 평균 1~2건/사이트 식별
- KT 기가지니 AI 스피커, 농협중앙회 RPA, DB손해보험 클레임콜 등 비정형 시스템 보안성 검토
- ISMS/ISO 27001 인증 취득 지원 컨설팅 (코웨이)

OT/ICS 보안 (IEC 62443)

LS ELECTRIC 자동화기기 Achilles Communication Certificate Level 2 인증 취득 — 2024.07 – 2025.03 · 기여도 100%

LS ELECTRIC PLC 제품군의 국제 통신 견고성 인증(Achilles Level 2) 취득을 위한 사전 점검·시험·보완. DoS·스톰·비정상 트래픽 환경에서도 제어 기능을 유지해야 하는 통과 기준 충족 필요.

- PLC 제품군 대상 Achilles Communication Certificate Level 2 전 시험 항목 통신 견고성 점검
- XGT Protocol 등 통신 스택 대상 스톰/퍼징/비정상 패킷 내성 검증 및 결함 재현
- [성과] LS ELECTRIC PLC 제품군 Achilles Level 2 인증 취득 달성, 통신 견고성 결함 펌웨어 보완 반영
- 기술: Achilles Test Platform · XGT Protocol · PLC · Wireshark · Python

LS ELECTRIC IEC 62443-4-2 자동화 점검 도구 개발 2025.03 – 2025.11 · 기여도 90%

PLC 제품군의 IEC 62443-4-2 인증 준비 과정에서 컴포넌트 보안 요구사항(CR) 점검이 대부분 수작업이었음. 통신으로 자동 점검이 가능한 요구사항을 도구화해 반복 점검 비용 절감 필요.

- IEC 62443-4-2 SL1 요구사항 중 통신 기반 자동화가 가능한 항목 선별·도구화
- FR2(사용 제어)·FR3(시스템 무결성)·FR4(데이터 기밀성)·FR7(자원 가용성) 영역 점검 자동화
- 점검 대상·결과 관리 웹 UI 및 결과 저장 파이프라인 구축
- [성과] PLC 제품군 IEC 62443-4-2 통신 기반 요구사항 자동 점검 도구 개발, 수작업 대비 점검 시간 단축
- 기술: Python · FastAPI · TypeScript · React · TailwindCSS · SQLite3

LS ELECTRIC 자동화기기 Threat Modeling 컨설팅 2023.03 – 2023.11 · 기여도 40%

자동화기기(XGI-CPUZ)의 IEC 62443-4-2 인증을 위한 체계적 위협 모델링과 이를 검증할 모의해킹 필요.

- System Definition → Function Point Definition → Data Flow Analysis 순 분석, DFD 작성
- STRIDE + DREAD 기반 Threat & Risk Assessment 수행
- 주요정보통신기반시설 취약점 분석평가 방법론 기반 모의해킹으로 위협 검증
- [성과] XGI-CPUZ Threat Modeling 보고서 및 모의해킹 보고서 산출
- 기술: STRIDE · DREAD · DFD · IEC 62443-4-2

스마트쉽 인프라 취약점 분석·검증 도구 및 보안 기술 개발 2024.07 – 2024.11 · 기여도 25%

스마트선박 내부 CBS는 Windows/Linux PC와 Embedded IoT/IIoT가 혼재해 일반 스캔으로 자산·취약점 식별이 어려움. 주요정보통신기반시설 가이드 기반 점검 도구 필요.

- 주요정보통신기반시설 취약점 분석 가이드 기반 Windows/Linux 점검 체크리스트 개발
- SSDP Discovery 기반 IoT/IIoT 센싱으로 OS·호스트·디바이스 정보 수집
- NVD/MITRE CVE·CWE를 CPE 기반으로 CBS에 매핑, PoC 코드로 명령·코드 실행 취약점 검증
- [성과] Shell/Powershell 자동화 모듈 및 5개 엔티티 취약점 DB 구축, 결과 CSV 등 포맷 제공
- 기술: Python · SSDP · CVE/CWE · CPE · SQLite · Shell/Powershell

IoT 취약점·도구 개발

IoT/CCTV 침해사고 조사 도구 개발 2022.08 – 2022.12 · 기여도 45%

CCTV 등 IoT 장비는 침해사고 시 증거 수집 절차·도구가 표준화되어 있지 않음. 펌웨어 내부 설정 파일·로그를 신속 확보하는 자동화 조사 도구 필요.

- 국내·외 CCTV 40종 대상 침해사고 증거 수집 자동화 도구 설계·구현
- UART 접근·플래시 덤프·binwalk 기반 펌웨어 추출 및 설정 파일·로그 전수 수집
- [성과] 공공기관 현장 실증 — 40종 장비 침해 흔적 수집 및 분석
- 기술: Python · C/C++ · UART · binwalk · Firmware Dump · Linux

스마트빌딩 내 IoT 기기 취약점 탐지 기술 개발 및 실증 (1차년도) 2021.08 – 2021.12 · 기여도 40%

스마트빌딩 내 IoT 기기는 임베디드 리눅스 기반으로 일반 스캔이 어렵고 표준 프로토콜이 혼재. 스캐닝~취약점 매핑 자동화 탐지 기술과 검증 테스트베드 필요.

- 유선(BACNet·KNXNet·Modbus)·무선(Wi-Fi·BLE) 프로토콜 디스커버리 기반 IoT 스캐닝 기술 검증
- 수집 정보(OS·프로토콜·펌웨어·모델)와 NVD CVE/CWE 매핑 및 PoC 검증 시나리오 개발
- [성과] 실제 스마트빌딩 기능 테스트베드 구축 및 탐지 도구 완성도 검증
- 기술: BACNet · KNXNet · Modbus · BLE · CVE/CWE · SQLite

스마트빌딩 내 IoT 기기 취약점 탐지 기술 개발 및 실증 (2차년도) 2022.01 – 2022.10 · 기여도 40%

1차년도 탐지 기술을 실제 운영 중인 스마트빌딩에 적용해 탐지 정확도를 검증·개선.

- 실제 스마트빌딩 대상 실증 — 기기·센서·프로토콜 정보 수집 및 취약점 탐지
- 취약점 정탐/오탐/미탐 식별 및 탐지 식별률 도출, 취약점 DB 최신화
- [성과] 실증 기반 탐지 정확도 개선 조치 도출
- 기술: IoT Scanning · CVE/CWE · PoC Validation · CSV/Excel Report

KT 기가지니 AI 스피커 단말 모의해킹 2020.10 · 기여도 100%

- 기가지니 AI 스피커 단말 대상 UART 디버그 인터페이스 분석
- 블루투스 통신 및 Android APK 분석을 통한 공격 표면 점검
- 기술: UART · Bluetooth · APK · Android

의료기기 보안 (FDA/eSTAR)

의료기기 FDA 보안 컨설팅 2024.03 – 2024.12 · 기여도 30%

FDA 시판 전 인증 준비 의료기기 제조사의 사이버보안 요구사항 충족을 위해 인프라 위협 모델링~의료기기·연동 시스템 모의해킹, eSTAR 제출 문서화 지원.

- FDA 인증 대상 인프라 Threat Modeling 및 위협·완화 방안 도출
- 의료기기 본체 및 연동 Web/App 모의해킹으로 취약점 검증
- FDA Premarket Cybersecurity 요구사항 기반 eSTAR 제출 문서화 컨설팅
- 기술: FDA Premarket Cybersecurity · eSTAR · Threat Modeling

의료기기 보안인증 컨설팅 (Cybersecurity Controls) 2024.06 – 2025.03 · 기여도 45%

전자약(ADHD 치료용 경피전기신경자극기) 의료기기의 보안인증 취득을 위해 기기·베이스스테이션·모바일앱·서버 시스템 전반의 사이버보안 통제 설계·문서화.

- 기기-앱(BLE)·앱-서버(LTE/5G)·웹(HTTPS)·베이스스테이션(Wi-Fi) 통신 경로 및 데이터 흐름 분석
- JWT(HS256)·RTR, OTP 가입 인증, 비밀번호 정책, 대시보드 RBAC 등 보안 통제 설계·검증
- [성과] 다중 연결 제한·세션 관리·역할 분리 등 Cybersecurity Controls 인증 제출 문서 작성
- 기술: BLE · JWT/HS256 · OTP · RBAC · HTTPS

연합학습 기반 신약개발 가속화 프로젝트 (K-MELLODDY) 2024.07 – 2024.12 · 기여도 30%

신약개발 연합학습(FDD) 플랫폼은 다기관 데이터·모델을 다루므로 개발 생명주기 전반의 보안 내재화와 실제 위협 통제 필요.

- NIST SSDF 기반 FDD 플랫폼 안전한 개발 프로세스 분석·정의 (IEC 62443·FDA·ISO 27001·EU CRA 검토)
- FDD 위협 모델링 기반 실제 위협 식별 및 소스코드 레벨 보안 통제(API 보안) 적용
- 공급망 보안 관리 체계(SBOM+VEX+EoS) 수립 및 실 운영 환경 모의해킹 2회
- 기술: NIST SSDF · Threat Modeling · SBOM/VEX · IEC 62443 · FDA Cybersecurity

사이버훈련장·CTF 개발

NATO CCDCOE Locked Shields 2025 — 한국-캐나다 연합 DFIR 블루팀 2025.01 – 2025.04 · 기여도 45%

세계 최대 규모 국제 사이버 방어 훈련 Locked Shields에 한국-캐나다 연합 DFIR 블루팀 참가. 실시간 공격 환경에서 침해 흔적 분석·대응 보고.

- 실시간 공격 시나리오 하 침해사고 포렌식 분석 및 타임라인 재구성
- DFIR CTF 과제 수행 — 아티팩트 분석·악성코드 트리아지
- [성과] Locked Shields 2025 훈련 종합 6위 / DFIR CTF 부문 1위
- [성과] Locked Shields 2026 한국-헝가리 연합 Special System 블루팀, 종합 9위
- 기술: DFIR · Volatility · Wireshark · Sysmon · YARA

APEX CTF 2025 — DFIR Network Forensics 문제 개발 2025.06 – 2025.09 · 기여도 45%

- DFIR Network Forensics 카테고리 문제 개발 — 실제 침해사고 기반 포렌식 시나리오
- 기술: DFIR · Network Forensics · Wireshark

한국전력 실전형 사이버 보안 훈련 시스템 보강 (ELECCON) 2023.06 – 2023.12 · 기여도 30%

- ELECCON 예선 CTF 문제 개발
- 전력망(OT/ICS) 환경 기반 본선 공방 시나리오 설계·개발
- 기술: OT/ICS · SCADA · CTF

실전형 사이버보안 훈련시스템 고도화 2022.07 – 2022.09 · 기여도 40%

- 실전형 사이버 공방 훈련 예선 문제 개발
- 전력망(OT/ICS) 환경 기반 본선 공방 시나리오 개발
- 기술: OT/ICS · SCADA · CTF

실전형 사이버 보안 훈련시스템 보강 (2024) 2024.09 – 2025.02 · 기여도 30%
- 전력망(OT/ICS) 환경 기반 본선 공방 시나리오 개발
- 기술: OT/ICS · SCADA

24년 실전형 사이버훈련장 훈련과정 운영 (스마트선박 항만) 2024.07 – 2024.12 · 기여도 20%
- 스마트선박 환경 대상 사이버 훈련 컨텐츠 개발

해킹 시나리오 기반 해킹체험 운영 2024.11 · 기여도 45%
- IoT 기기 대상 해킹 체험 부스 운영

C2021 행사 (ELECCON 대회 운영) 2021.05 – 2021.12 · 기여도 30%
- ELECCON 사이버 공방 대회 운영 보조

금융·공공 Web/App 모의해킹

금융·공공 전자금융기반시설 모의해킹 (12개 사이트, A3 Security) 2020.06 – 2021.06

A3 Security 재직 중 금융권·공공기관 전자금융기반시설 대상 다수 Web/App 모의해킹 및 취약점 분석평가. 정보 유출·2차 공격 가능성 점검 및 개선 방안 제시.
- 전자금융기반시설 취약점 분석평가 — 참저축은행, 애큐온캐피탈, 금융투자협회 등 금융권 Web/App 모의해킹
- 금융·보험·제조 시스템 보안성 검토 — SBI저축은행(오픈뱅킹·디지털창구), 현대자동차 HKMC, DB손해보험 클레임콜
- 농협중앙회 RPA 소스코드 진단, 대교 통합교육 플랫폼·오토핸즈·UNTAC 등 모의해킹
- [성과] 12개 사이트 모의해킹 수행, 사이트당 고위험 취약점 평균 1~2건 식별 및 개선 방안 제시
- 기술: Burp Suite · OWASP Top 10 · Web/App Pentest · Source Code Review

보안 컨설팅·인증

INFINITT DPS 의료영상 플랫폼 모의해킹 2024.07 – 2024.09 · 기여도 70%

의료영상 플랫폼(DPS)의 Web·모바일(Android/iOS) 서비스 대상 체크리스트 기반 취약점 진단 및 침투 시도로 정보 유출·2차 공격 가능성 점검.
- 주요정보통신기반시설 취약점 분석 가이드 + OWASP Top 10 2021 기반 Web/Mobile 수동 진단
- Burp Suite·Wireshark·APKTool 등으로 인증·접근통제·입력검증 취약점 점검
- [성과] 총 14건 취약점 식별(중위험 3·저위험 11), 재점검 전건 조치 완료, 영문 결과 보고서 주저자
- 기술: Burp Suite · Wireshark · APKTool · OWASP Top 10 · Android/iOS

코웨이 인증심사 취득지원 (ISMS, ISO27001) 컨설팅 2020.11 · 기여도 40%
- ISMS·ISO27001 인증심사 취득지원 컨설팅 수행

정보보안 컨설팅 용역 2024.10 – 2025.01 · 기여도 25%
- 정보보안 컨설팅 용역 수행

취약점 연구

OS Kernel CVE 16건 — Best of the Best 8기: 커스텀 File System Fuzzer 설계·구현으로 Linux Kernel CVE 16건(0-day 포함) 도출. CodeBlue 2019(도쿄)·Hack In The Box 2019(암스테르담) 발표.

IoT CVE 5건 — 개인 연구: 임베디드/IoT 장비 취약점 분석. CVE-2024-33788/33789/33791/33792/33793 (CVSS 최대 9.8 CRITICAL).

FVE 3건 — Findthegap 버그바운티: 버그바운티 플랫폼 대상 웹 취약점 보고 3건 (상세 비공개).

자격증 · 교육

- 리눅스 마스터 2급 (KAIT, 2021.07)
- 네트워크 관리사 2급 (KAIT, 2024.07)
- 공주대학교 컴퓨터공학부 학사 (2012.02 – 2020.02)
- 천안상업고등학교 정보처리과 (2009.03 – 2012.02)