

XIoT Security Convergence Company



Z-IoT

XIoT Firmware SECaaS



제품 보안성 향상



점검 시간 및 비용 절감



보안 점검 활용도 향상

Core Technology

Z-PLOIT

(Automatic Binary Security Analysis)

Concolic 분석을 활용하여 펌웨어 내 알려지지 않은 잠재적인 취약점 자동 분석

*특허 기술 보유

Z-BOM

(SBOM Security Management)

바이너리 오픈 소프트웨어의 버전 식별과 별도의 알려진 취약점(CVE) 데이터베이스 보유로 빠르고 정확한 오픈 소프트웨어 관리 및 취약점 대응

점검 펌웨어 암호화

점검 대상 펌웨어에 대한 양자 내성 암호 알고리즘을 통해 암호화하여 저장되는 펌웨어에 대한 보호 가능

운영 데이터 분석

다양한 아키텍처에서 실행 가능한 정보 수집 모듈을 통해 IoT 장치 내 운영 데이터를 수집하고, 이를 기반으로 더 넓은 범위의 보안 취약점 식별

*특허 기술 보유

Solution Architecture



취약점 분석 진행 시간 감축



Key Features

패스워드 보안

펌웨어 내 패스워드 파일을 추출하여 취약한 패스워드, 디폴트 및 하드코딩 패스워드 식별을 통해 Brute Force, Dictionary Attack과 같은 패스워드 대입 공격을 통해 안정성 점검

암호화 보안

펌웨어 내 인증서 파일을 추출하여 인증서 암호화 알고리즘 및 설정을 분석하며, 국내외 권고 암호 알고리즘 적용 여부 진단

실행파일 보안

펌웨어 내 실행파일을 컴파일(사람이 이해하는 언어를 컴퓨터가 이해할 수 있는 언어로 바꿔주는 과정)하여 취약 유무 점검

오픈소프트웨어 보안

펌웨어 내 커널 및 오픈 소프트웨어 파일을 추출해 버전 정보 분석을 하고, 추출 된 버전 정보에 해당하는 알려진 취약점을 제공하며, SBOM 관리 기능 제공

제로데이(Zero-Day) 분석

펌웨어 내 알려지지 않은 잠재된 취약점을 지엔의 바이너리 분석 기술(Taint Analysis & Symbolic Execution)을 사용해 자동으로 발생 가능성 포인트 분석

Z-IoT 발견 취약점



스마트홈
28건



스마트팩토리
4건



스마트 모빌리티
29건



전기차 충전기
2건

Connect the Dots, Secure Confidently.

Core Values

효율성

자동화 정보 수집 모듈과 올인원 보안 취약점
자동 분석을 통한 점검 시간 및 비용 절감



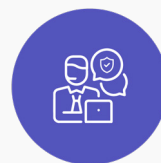
맞춤화

다양한 점검 커버리지 지원 및 기업별 맞춤화된
컴플라이언스 솔루션 제공



전문성

스마트홈(IoT) 해킹대회, '사이버 보안 챌린지'
우승 등 다수 대회 수상 및 특허 보유



Contact

Telephone: +82-70-4571-9851

Email: support@zi-en.io

Website: zi-en.io