디지털 전환 시대, DX 융합보안 전문기업

COONTEC

COrporation **ON** by **TEC**hnology

CONTENTS

COrporation **ON** by **TEC**hnology

모든 산업 분야에 디지털 대전환이 일어나고 있습니다.
우리가 50년 후에 뒤돌아 본다면, 지금이 거대한 새로운 물결의 시작점이었음을 알 것입니다.
쿤텍은 디지털 전환에서 필요한 **융합 산업의 보안**을 중심으로 고객이 디지털 연결을 가속화 하도록 돕고,
더 나아가 쿤텍의 사람과 기술, 기업문화를 통해 시대 전환을 이끄는 기업이 되겠습니다.

쿤텍 CEO 방혁준

현 시대를 사는 우리는 세계를 탐험하며 신대륙을 발견하기엔 너무 늦게, 우주 여행을 하기엔 너무 일찍 태어난 사람들입니다. 쿤텍은 4차 산업혁명이라는 새로운 물결을 항해하는 과정에서 어디로, 어떻게 나아가야 하는지를 함께 고민하고 이에 대한 올바르고 성장 지향적인 방향성을 제시하고자 합니다.

01 COMPANY

1. 회사개요
2. 주요 연혁 및 실적
3. 조직도 및 인력 현황
4. 지적재산권 현황
5. 매출 및 임직원수 추이
6. 핵심 경쟁력
7. 고객사

COrporation **ON** by **TEC**hnology

회사명	**쿤텍**(주) COONTEC Co., Ltd.	대표자	**방혁준**
설립연도	2016. 01. 22	임직원수	88명 ('26.02 기준)
사업영역	**디지털 전환 시대, DX 보안 전문 기업 COONTEC** 공급망 보안 / 인프라 보안 / 임베디드 가상화 및 보안 / AI 공급망 보안 / 5G 특화망 / 교육 및 컨설팅 서비스 제공		
운영	본사 / 연구소 / 아카데미		

2016~2018 | 설립 및 성장

- 2016 쿤텍(주) 설립
- 기업부설연구소 설립
- 벤처기업인증
- IoT 보안테스트베드 구축

2018~2020 | 솔루션 포트폴리오 구축기

- 이기종 리눅스 악성코드 행위기반 탐지/예방 솔루션 개발
- 스마트 팩토리 IoT 지능형 악성코드 분석 및 탐지 프레임워크 개발
- 샌드박스 기반 IoT기기 악성코드 탐지 및 대응 솔루션 개발
- T사(첨단 차량IT기술 전문 상장사) 오픈소스 점검 솔루션 공급

2020~2022 | 솔루션 사업체계 구축기

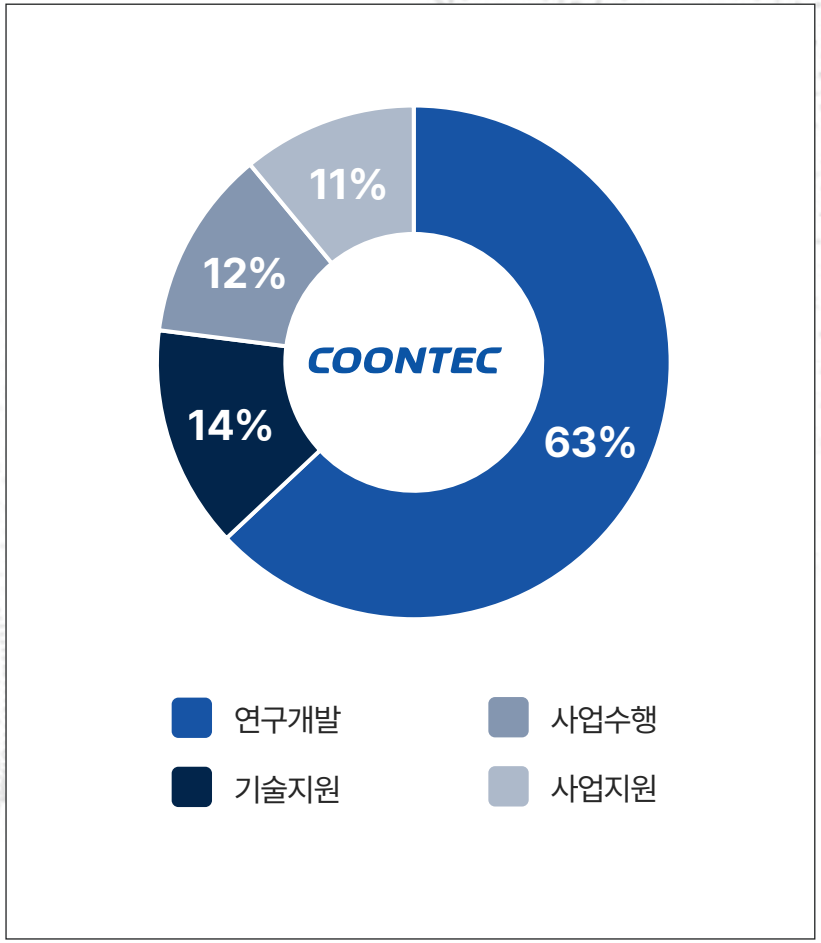
- 발전소 네트워크기반 차세대 해커유인시스템 공급
- T사 애플리케이션 내 화이트박스 암호 라이브러리 공급
- OT 네트워크 융합보안 컨설팅
- 함정 사이버보안 프레임워크 개발
- S은행 오픈소스 보안 취약점 점검 시스템 구축

2022~2024 | 사업 확대

- 쿤텍 아카데미 개원
- K은행 바이너리 취약점 분석 도구 공급
- H사(대기업 계열 금융사) 오픈소스 거버넌스 구축
- N은행 오픈소스 관리시스템 구축
- C사 OT 보안시스템 구축
- 온라인 부정수입물품 유통 모니터링

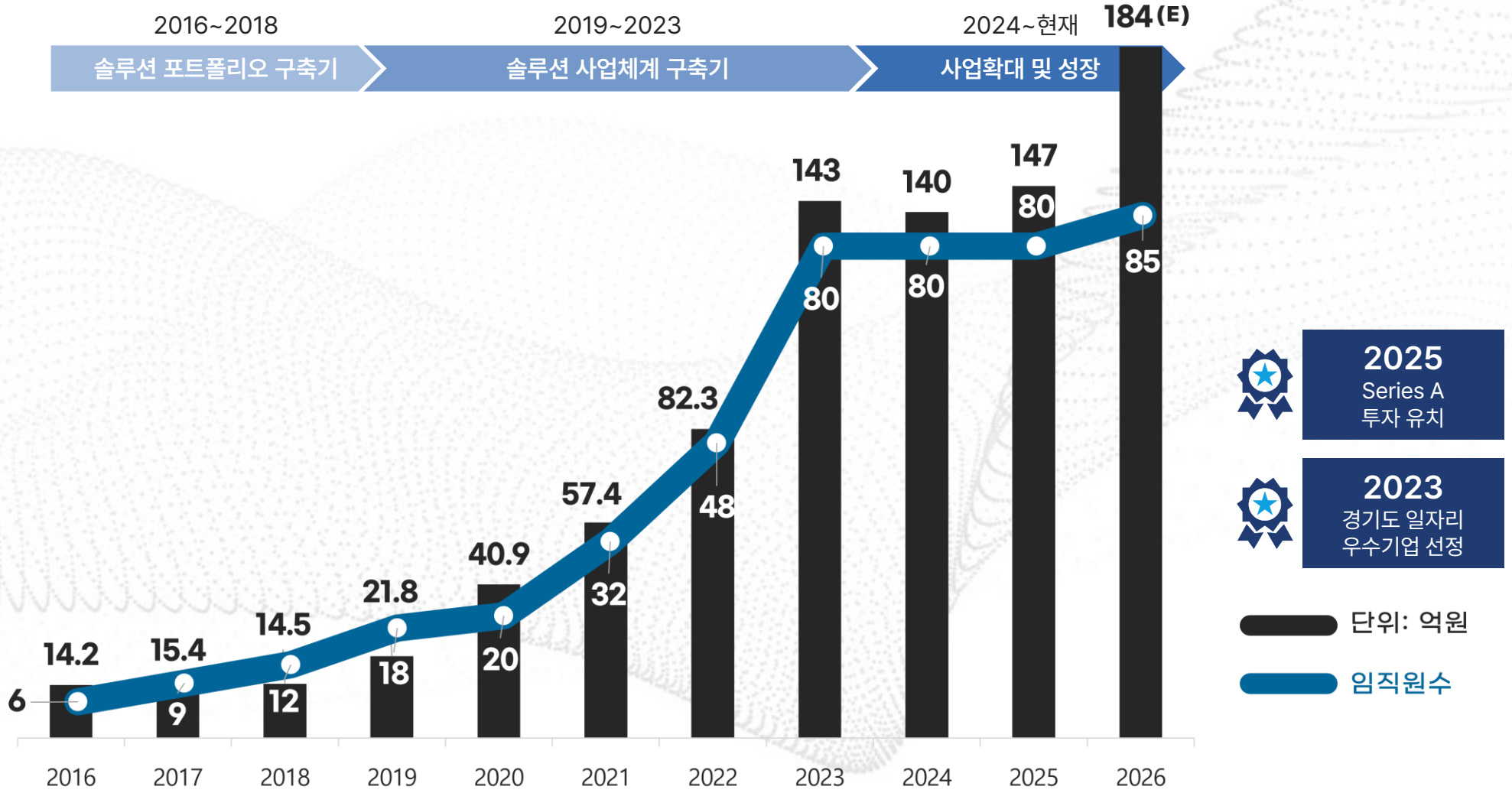
2024~현재 | 새로운 도약기

- L 생명사 오픈소스 관리 시스템 구축
- S 은행 오픈 소스 관리시스템 구축
- M 증권사 오픈소스 관리 시스템 구축
- SBOM 기반 SW 공급망 보안 실증 용역
- W 카드사 오픈소스 관리 시스템 구축
- Series A 투자 유치 (H벤처스, N벤처)



전체 임직원 중 **77%가 연구개발 및 기술지원** 인력으로 구성되어 있으며, 임베디드 가상화 및 공급망 보안 분야의 경력이 **15년 이상인 경력자** 위주로 구성되어 있어 뛰어난 프로젝트 수행 능력을 갖추고 있습니다.
연구개발, 기술지원 부서 외 사업수행, 사업지원 부서 역시 다수의 관련 분야 프로젝트 수행 경험을 보유한 고급 인력으로 구성되어 있어 안정적이고 완성도 높은 프로젝트 수행을 지원합니다.

- 하드웨어·소프트웨어·시스템을 아우르는 **종합 보안 IP 포트폴리오**
- **차세대 보안 기술**(부채널, 화이트박스 암호, 허니팟, 블록체인) 선도
- 기술 보호 및 사업 확장을 위한 **지식재산권 기반** 확보


2016~2018
솔루션 포트폴리오 구축기
2019~2023
솔루션 사업체계 구축기
2024~현재
사업확대 및 성장
184(E)
14.2
15.4
14.5
21.8
40.9
57.4
82.3
143
140
147
184
6
9
12
18
20
32
48
80
80
80
85
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2025
Series A
투자 유치
2023
경기도 일자리
우수기업 선정
단위: 억원
임직원수

다양한 보안 포트폴리오

공급망 보안부터
임베디드 가상화까지
유기적으로 관리할 수 있는
보안 솔루션 포트폴리오 보유

전문분야 실적 및 경험 보유

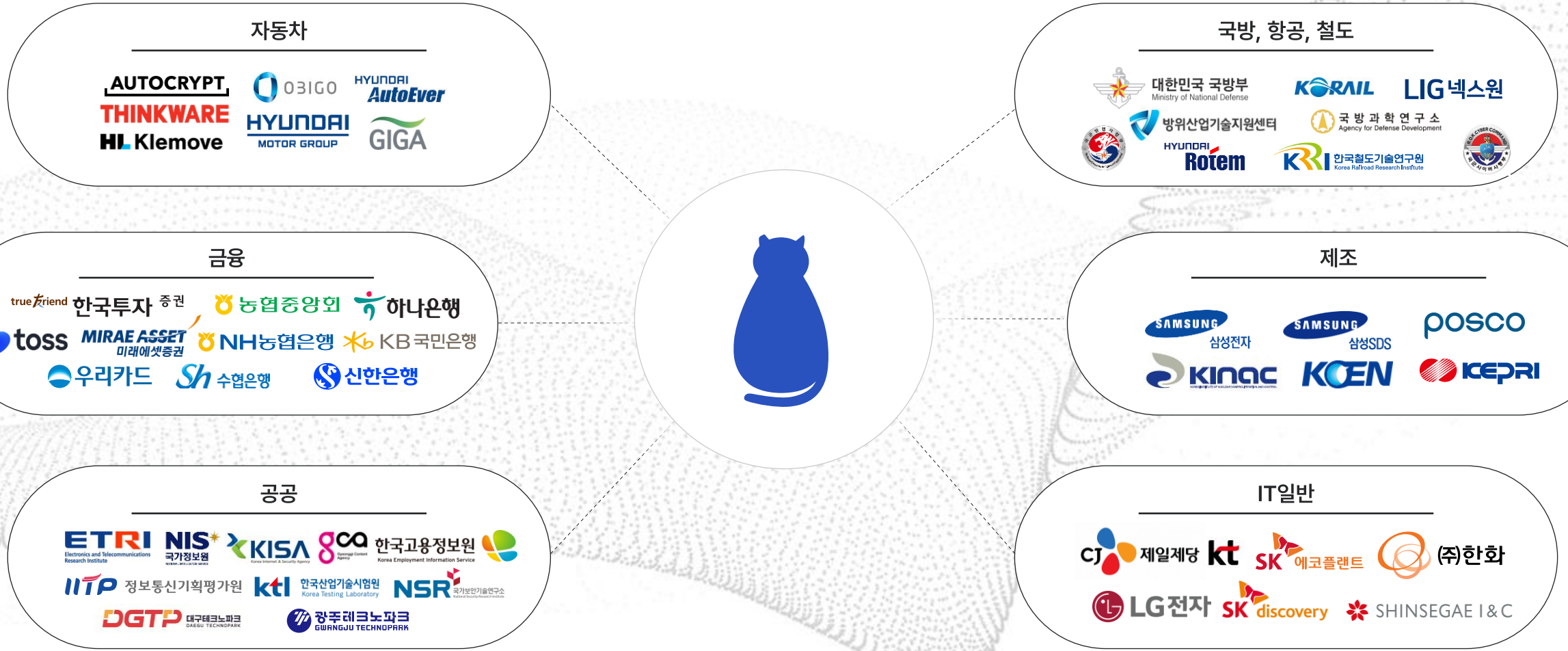
국방, 금융, 공공 등
솔루션이 필요한
전문 분야에 대한
다수의 실적과 수행 경험 보유

솔루션 개발 역량

경력 10년 이상의 개발자 위주로
구성된 기업부설연구소 운영,
신규 솔루션 개발 진행

다수의 정부 과제 수행

’23년~’25년 예산 174억,
39개 정부 과제 수행
’26년~’28년 진행 예정 정부 과제
25개 및 예산 107억 확보


자동차
AUTOCRYPT
O3IGO
HYUNDAI AutoEver
THINKWARE
HYUNDAI MOTOR GROUP
HL Klemove
GIGA
국방, 항공, 철도
대한민국 국방부 Ministry of National Defense
KORAIL
LIG넥스원
방위산업기술지원센터
국방과학연구소 Agency for Defense Development
HYUNDAI Rotem
한국철도기술연구원 Korea Railroad Research Institute
금융
truefriend 한국투자증권
농협중앙회
하나은행
toss
MIRAE ASSET 미래에셋증권
NH농협은행
KB국민은행
우리카드
Sh 수협은행
신한은행
제조
SAMSUNG 삼성전자
SAMSUNG 삼성SDS
posco
KINAC
KOEN
KEPRI
공공
ETRI Electronics and Telecommunications Research Institute
NIS 국가정보원
KISA
gca
한국고용정보원 Korea Employment Information Service
IITP 정보통신기획평가원
ktl 한국산업기술시험원 Korea Testing Laboratory
NSR 국가보안기술연구소
DGTP 대구테크노파크 DAEGU TECHNOPARK
광주테크노파크 GWANGJU TECHNOPARK
IT일반
CJ 제일제당
kt
SK 에코플랜트
㈜한화
LG전자
SK discovery
SHINSEGAE I&C

02 Solutions

1. 공급망 보안
2. 인프라 보안
3. AI 공급망 보안
4. 조선/해양
5. 공격표면 보안
6. 임베디드 보안
7. 임베디드 가상화
8. 5G 특화망

COrporation **ON** by **TEC**hnology

공급망 보안

AEZIZ
AEZIZ Binary
mend.io
sonatype

인프라 보안

TeraGRID
CLAROTY

AI 공급망 보안

SPLX

조선/해양

TGM
KR-CyberOne
KR-Tester

공격표면 보안

Cyber Hawk Eye
penzzer

임베디드 보안

SecureALPS
SECURE-IC

임베디드 가상화

FastVLabs
RAPITA Systems
PikeOS
RTOS & Hypervisor

5G 특화망

NXTCore

AEZIZ 오픈소스와 바이너리 취약점 분석 결과의 통합 관리를 위한 SDLC 기반 공급망 보안 솔루션

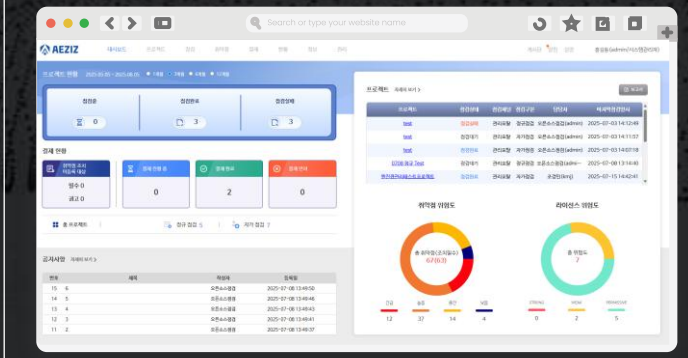
취약점 분석
라이브러리 취약점 점검 및 위험도 제공

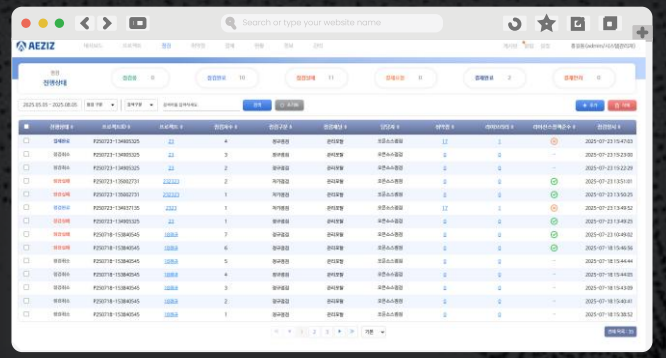
유연한 권한 관리
사용자별로 기능과 페이지 접근 제어 가능

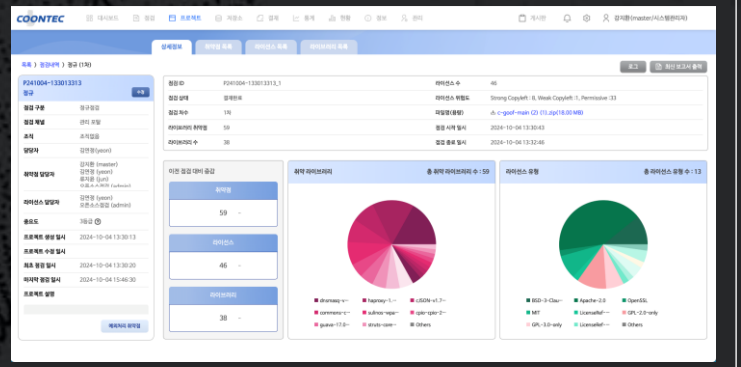
통합 관리

통계 및 시각화
취약점, 라이브러리, 라이선스 등 점검 결과를 그래프로 제공

보안 강화
단계 채널 인증 기반 로그인, 개인정보 암호화 관리

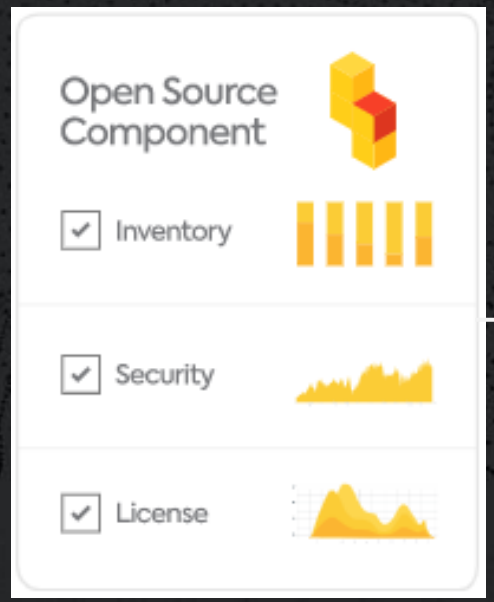






MEND

디지털 시그니처 기반으로 오픈소스를 분석하여 SBOM을 생성하고 SaaS로 구축된 실시간 DB를 통해 빠르고 정확하게 보안 취약점을 관리하는 오픈소스 통합 관리 솔루션



SBOM 및 라이선스관리

- GitHub, GitLab 등 30개 이상의 오픈소스 저장소 기반의 오픈소스 컴포넌트 및 라이선스 정보
- 1억 개 이상의 오픈소스 컴포넌트와 바이너리 파일
- 3억 개 이상의 소스파일

보안 취약점 관리

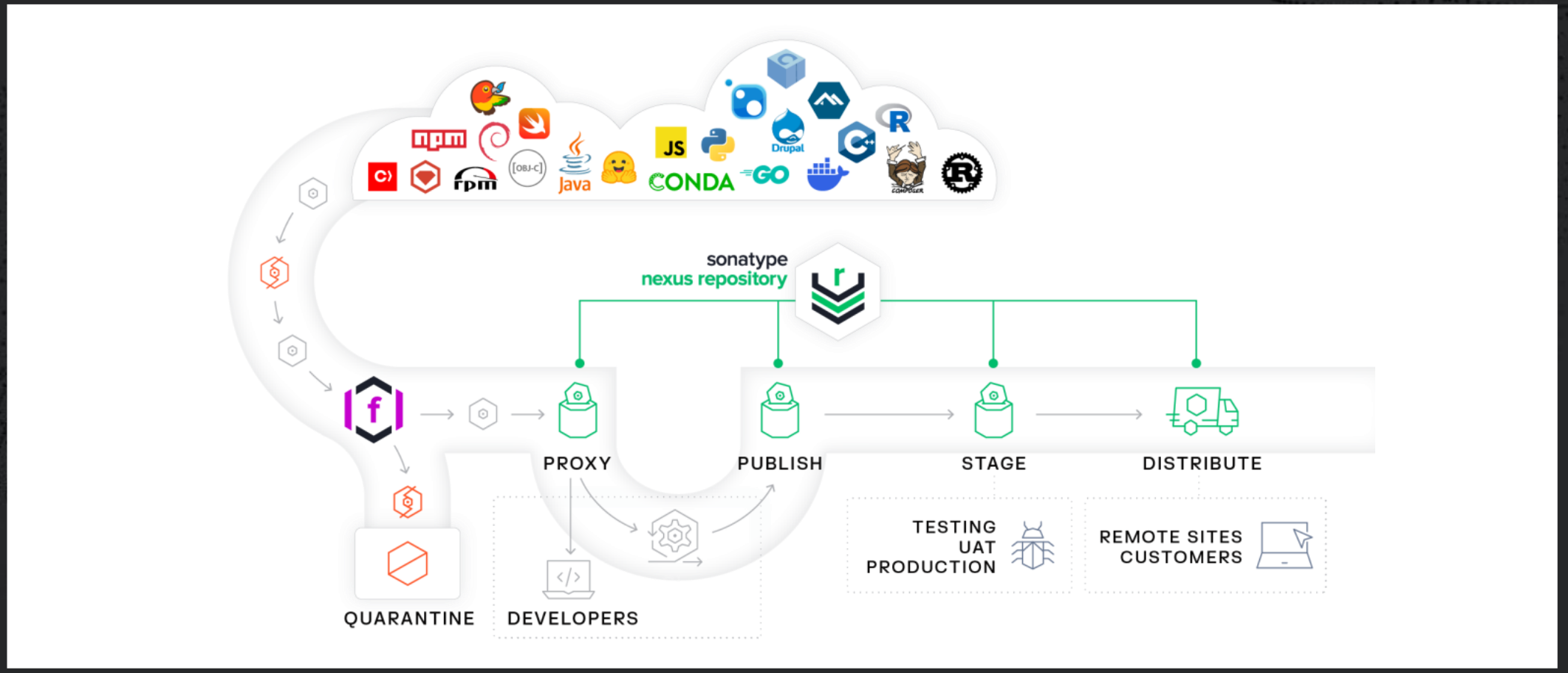
- NVD, GitHub 이슈 트래커, RubyOnRails, NodeSecurity
- 오픈소스 프로젝트에서 수집된 60만 건 이상의 공개 취약점 정보
- MEND 자체 보안팀에서 검증한 2만 건 이상의 고유한 취약점 정보

품질 관리

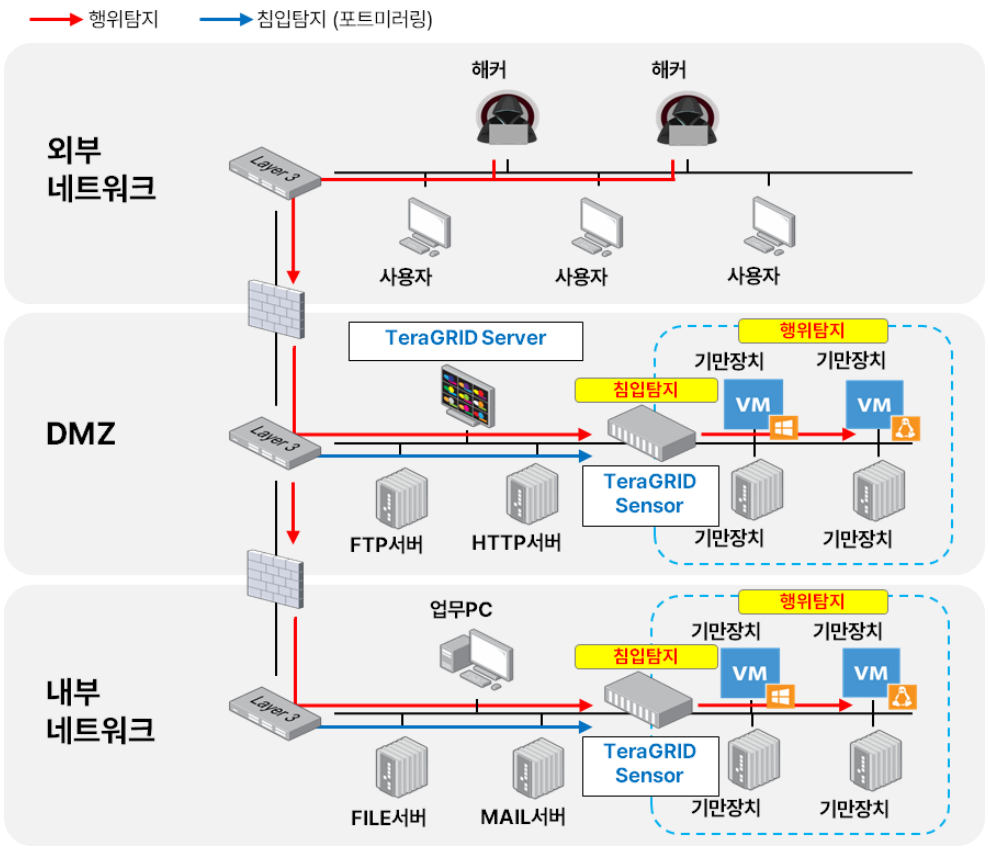
- 오픈소스 커뮤니티 활성화 지표 - Commit
- 라이브러리 버그 및 수정 현황 – Fix Rating
- 미해결 버그의 개수 및 심각도 – Bug Statistics

Sonatype

소프트웨어 애플리케이션과 AI/ML 모델, 구성 요소를 빠르고 안정적이며 제어 가능한 방식으로 대규모 관리·저장·배포할 수 있는 바이너리 아티팩트 저장소 솔루션



TeraGRID 사이버 공격에 대한 확장된 감시 및 대응 기술인 XDR 기반의 유인기만 솔루션



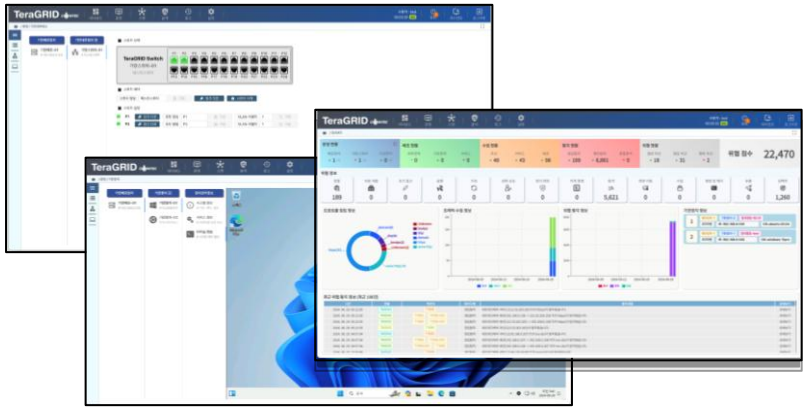
TeraGRID Server

- 유인기만 배포서버 관리
- 공격자 위협 정보 수집/분석
- 유인기만 관리 시각화

TeraGRID Sensor

- 기만장치 관리 및 수집/분석
- 공격자 행위 수집/분석
- 실 자산 트래픽 수집/분석

관리 및 통합 TeraGRID SOC



Claroty

OT/IT 융합 환경의 복잡한 네트워크에서 사각지대 없는 자산 식별과 실시간 위협 탐지를 통해 운영 중단 없는 안전한 스마트 팩토리 환경 보장

핵심 기능 (Key Features)

완벽한 자산 식별

자산 목록화 및 운영 현황 파악
숨겨진 OT/IoT 장비 100% 가시화
상세 속성 정보 자동 수집

실시간 위협 탐지

이상 행위 및 비인가 통신 탐지
알려진/알려지지 않은 위협 분석
공격 경로 시각화

취약점 & 위험 관리

자산별 CVE 매핑 및 위험도 스코어링
우선순위 기반의 패치 관리 가이드
설정 변경 이력 추적

네트워크 보호

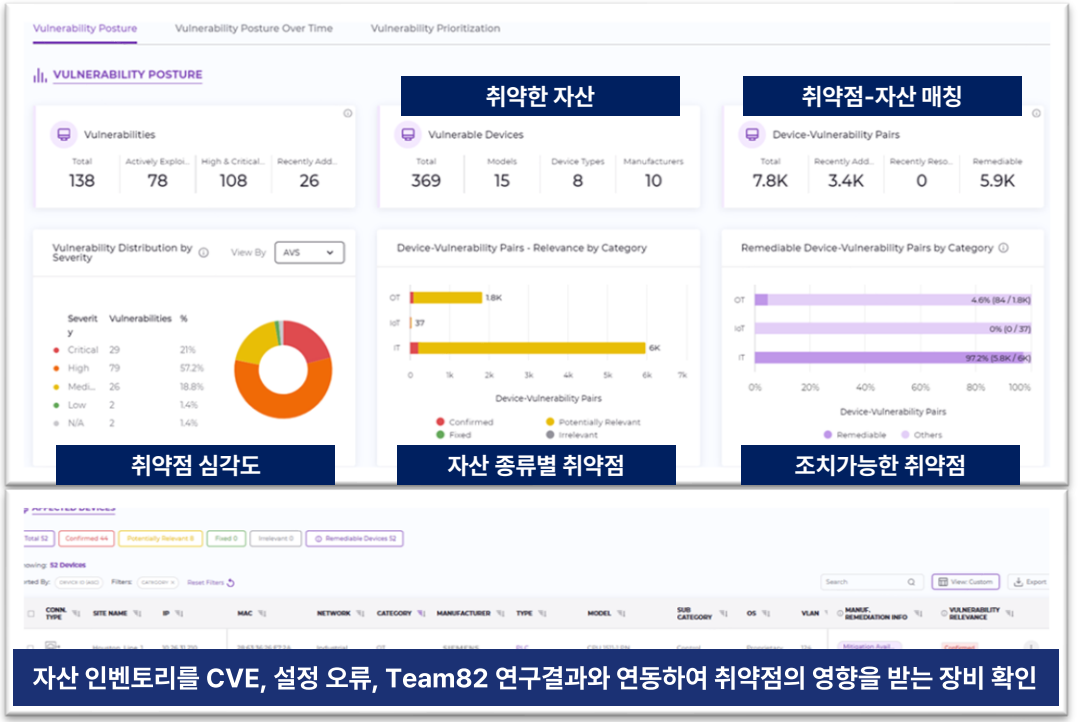
네트워크 세그먼테이션(망분리) 지원
Zero Trust 정책 수립 지원
원격 접속 보안 통합

Trusted by Industry Leaders

- **2025년 가트너 매직쿼드런트 리더 선정**
- **17개 기업 중 실행 역량/비전 완성도 최상위 평가**

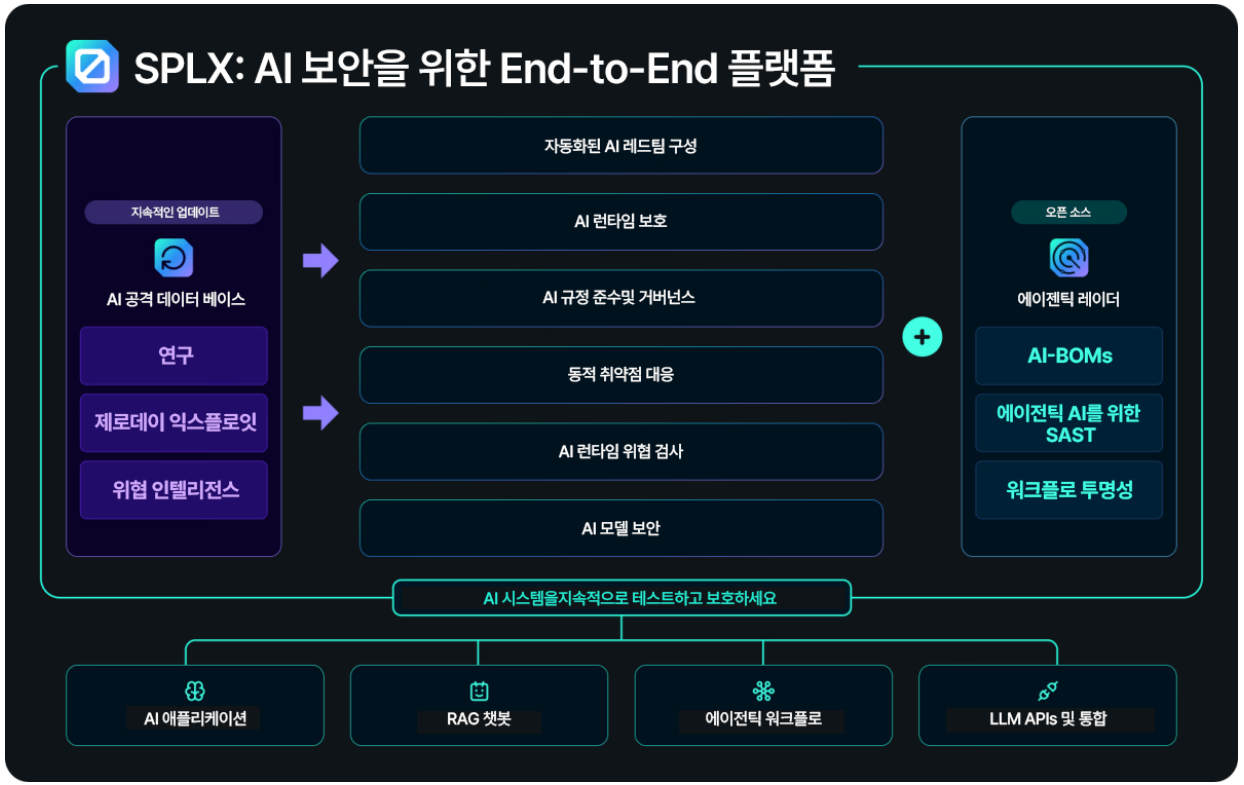
출처: https://claroty.com/press-releases/claroty-named-a-leader-in-2025-gartner-magic-quadrant-for-cps-protection-platforms

통합 대시보드 (Integrated Dashboard)



SPLX

AI 라이프사이클 전반에서 레드팀 활동, 런타임 보안, 거버넌스 및 문제 해결까지 포괄적으로 지원하여 AI 시스템을 안전하게 구축·배포·확장할 수 있도록 설계된 풀스택 AI 보안 솔루션



자동화된 AI 레드팀 구성	대규모 공격 데이터와 맞춤형 데이터로 AI 시스템의 실제 취약점을 자동 탐지
AI 런타임 보호	실시간 가드레일로 악성 입력·출력과 민감 데이터 유출을 즉시 차단
AI 거버넌스 및 규정 준수	글로벌 및 내부 보안·규제 기준에 AI 시스템을 자동 매핑하여 준수 보장
지속적 방어 고도화	레드팀 결과를 반영해 시스템 프롬프트를 강화·수정하여 공격 표면 최소화
AI 런타임 위협 검사	LLM 로그를 분석해 탈옥·프롬프트 주입·악성 쿼리를 실시간에 가깝게 탐지
검증 기반의 AI 안심 도입 체계	상용·오픈소스 LLM 보안 평가를 통한 고신뢰 LLM 모델 도입 지원

KR-CyberOne

IACS UR E26/E27 규정에 맞춰 선박 설계부터 운영까지 전 생애주기의 보안 통합 관리, 복잡한 인증 절차 및 업무 자동화

설계 → **건조 (E26 & E27)** 시스템 무결성 → 운항 → **운영 (E26)** 공급망 보안 → 유지보수, 폐선

KR-Tester

- 네트워크 스캐닝
- 자산목록 및 구성도 자동화
- 복원력 테스트 (네트워크 부하 시험)
- CSDD 검증

KR-CyberOne

- 디지털 자산 관리
- 동적 네트워크 시각화
- 자동화된 리스크 평가
- CSDD, CSRP, 규제 문서 생성

TGM

- 원클릭 보고서 생성-제출-승인
- 취약점 관리, 통합 모니터링
- 시스템 백업 및 복구 지원
- 위협 인텔리전스(CTI), 기만 기술(Deception)

'설계-문서화-검증' | '탐지-대응-복구'

TGM
(TeraGRID for Maritime)

규제를 우회하는 지능형 위협(APT)은 NMS, F/W로 탐지 불가능하며 인증 및 대응까지 지원 가능한 선박용 통합 보안 'All In One' 솔루션

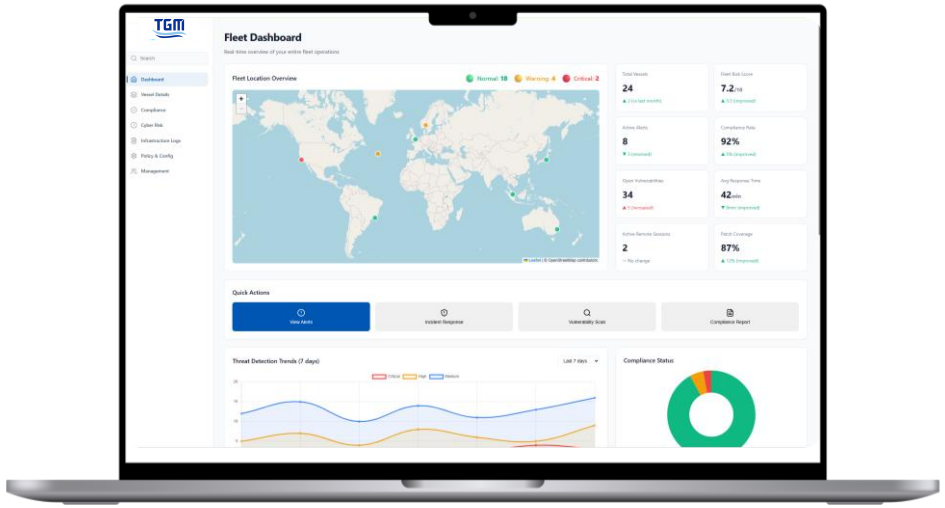
선박용 통합 보안 솔루션

통합 보안 솔루션

SIEM
IDS
EDR
NMS

검사 대응 자동화

KR-CyberOne
"복원력 인증+검사"



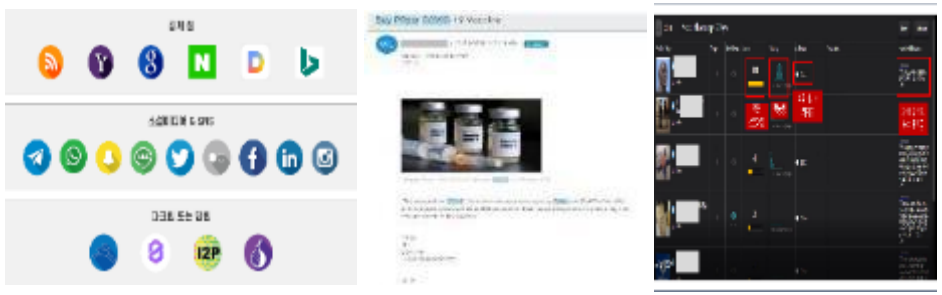
SIEM, IDS, EDR, NMS 기능을 하나로 통합하여, 선박 OT 장비와 IT 시스템을 보호하고
지능적인 사이버 위협을 실시간으로 탐지 및 대응하는 차세대 해상 보안 솔루션

Cyber Hawk Eye

OSINT 기반의 위협 정보 수집 분석 플랫폼으로 서피스웹, 딥웹, 다크웹 상에서의 정보 수집에 최적화되어 효과적으로 위협 정보 및 범죄 관련 정보를 수집 및 분석

서피스웹, 다크웹, 딥웹에 존재하는 정보 수집의 최적화된 솔루션 제공

사이버 상에 게시된 범죄 활동, 군사정보, 금융범죄, 개인정보 유출에 대한 증거수집 및 분석



- 아바타로 안전한 데이터 수집
- 모듈식 고객 맞춤형 옵션 제공
- SNS 연계 분석을 통한 사이버 범죄 데이터 수집

Penzzer

펜테스트 동적 분석(DAST)과 퍼징(Fuzzing) 통합 솔루션으로 단일 플랫폼으로 알려진 취약점, 알려지지 않은 취약점 등 다양한 보안 위협을 탐지하고 각종 규제 요구사항 준수 지원

All-in-one

자동차, 의료기기, IoT, 임베디드 등 퍼징, 펜테스트을 하나의 솔루션에서 모두 지원하여 알려진 취약점/알려지지 않은 취약점 모두 탐지가 가능

Compliance

ISO/SAE 21434, FDA 및 각종 ISO 표준과 보안 규정을 지원하며, IoT 지원 공급망 전체에 대한 보안 관리 제공

Plug-and-play

모든 하드웨어와 소프트웨어를 키트로 제공하여 테스트에 사용될 장치(DUT, Device Under Test)에 연결하여 즉시 침투테스트 및 동적 분석(DAST)

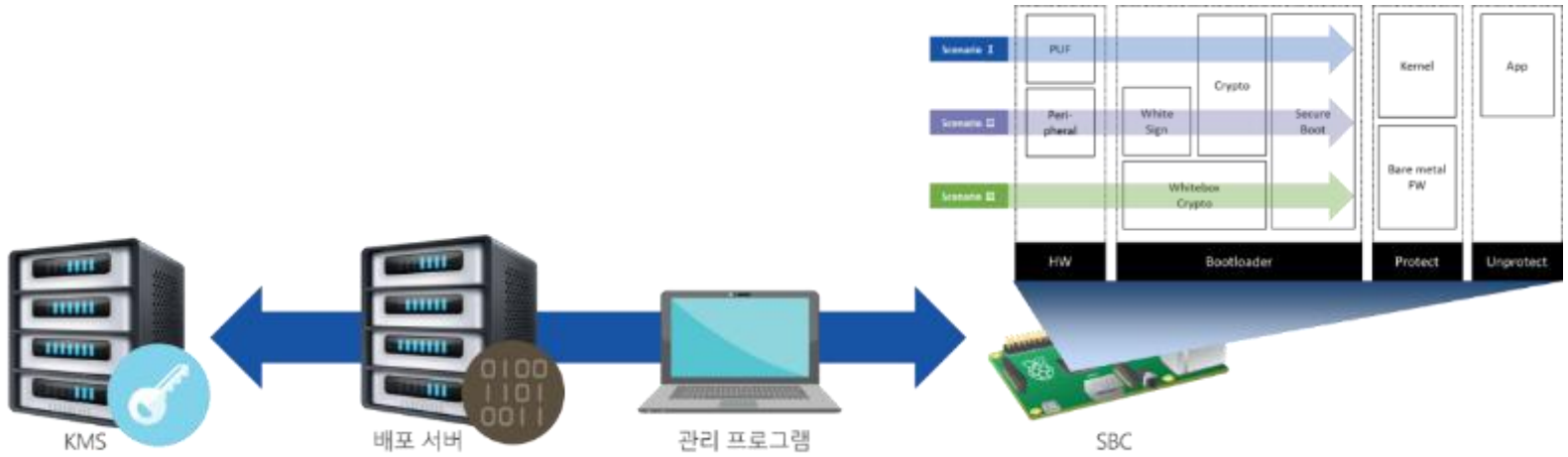
Easy-to-use

쉽고 명료한 UI를 통해 사용자의 편의성을 극대화하여 퍼징과 펜테스트를 쉽고 빠르게 테스트

Secure ALPS (1/2)

ALPS-Crypto | 임베디드 환경에서 안전한 펌웨어 및 키 관리 체계 제공

- 임베디드 장비 내에 설치되어 있는 펌웨어의 무결성과 기밀성을 보호 하여 변조 방지 및 핵심 기술을 보호
- 제조 단계에서의 펌웨어 설치 뿐만 아니라 업데이트 시에도 상호인증과 암호화를 통해 안전하게 임베디드 소프트웨어를 전달
- 세 가지(PUF, White-Sign, 화이트박스 암호) 암호 키 보호 기술 중 장비 특성에 맞춰 하나를 사용하여 암호 키를 보호
- 임베디드 장비에 대해 부트 단계에서부터 보호 기술을 적용



Secure ALPS (2/2)

ALPS-Shield | 임베디드 환경에서의 응용프로그램 자체 보호

제공 솔루션

코드 난독화
: 응용 프로그램 정적 분석 (역컴파일) 하는 공격에 대응하는 방어

바이너리 암호화
: 응용 프로그램의 핵심 바이너리를 암호화하여 핵심 응용을 보호

바이너리 무결성
: 응용 프로그램 바이너리 변형하여 공격에 대응하는 방어

리소스 암호화
: 응용 프로그램에서 사용하는 리소스 파일을 암호화하여 리소스 파일 보호

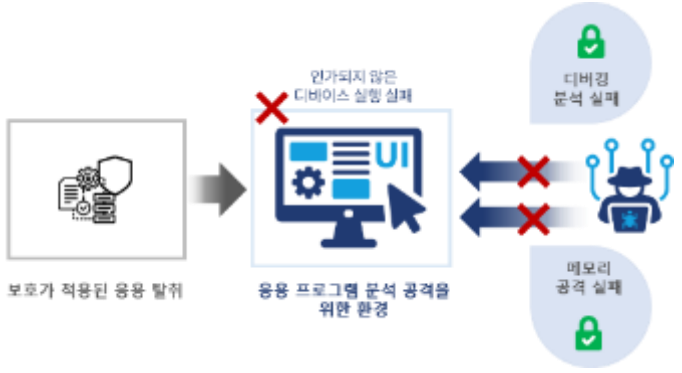
디바이스 바인딩
: 인가되지 않은 디바이스에서 실행할 수 없도록 하는 방어

안티 디버깅
: 디버깅 환경에서 실행

바이너리 하드닝
: 메모리에 로드되어 실행 중인 응용 프로그램 공격을 방어

코드 난독화,
바이너리 암호화,
바이너리 무결성,
리소스 암호화

디바이스 바인딩,
안티 디버깅,
바이너리 하드닝

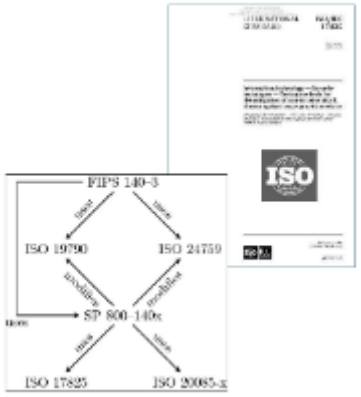


Secure-IC

다양한 부채널&오류주입 분석 기법, HW Trojan 탐지 방법을 활용하여 임베디드 환경에서의 HW 보안 위협 요소들을 탐지하고 잠재적인 HW 보안 위협에 대한 완화 방안(IP)를 공급하고 평가를 기반으로 보안 컴플라이언스 지원

포괄적인 분석 방법 지원

PASSIVE (SCA) / ACTIVE (FIA)
화이트박스, 블랙박스 지원하며 분석을
위한 장비 및 솔루션과 방법론 제공



컴플라이언스 지원

임베디드 환경의 보안 검증
ISO/IEC 17825, 20085, 평가 표준 CC,
ISO/IEC 15408, FIPS 140

장기 지원 및 유지 관리

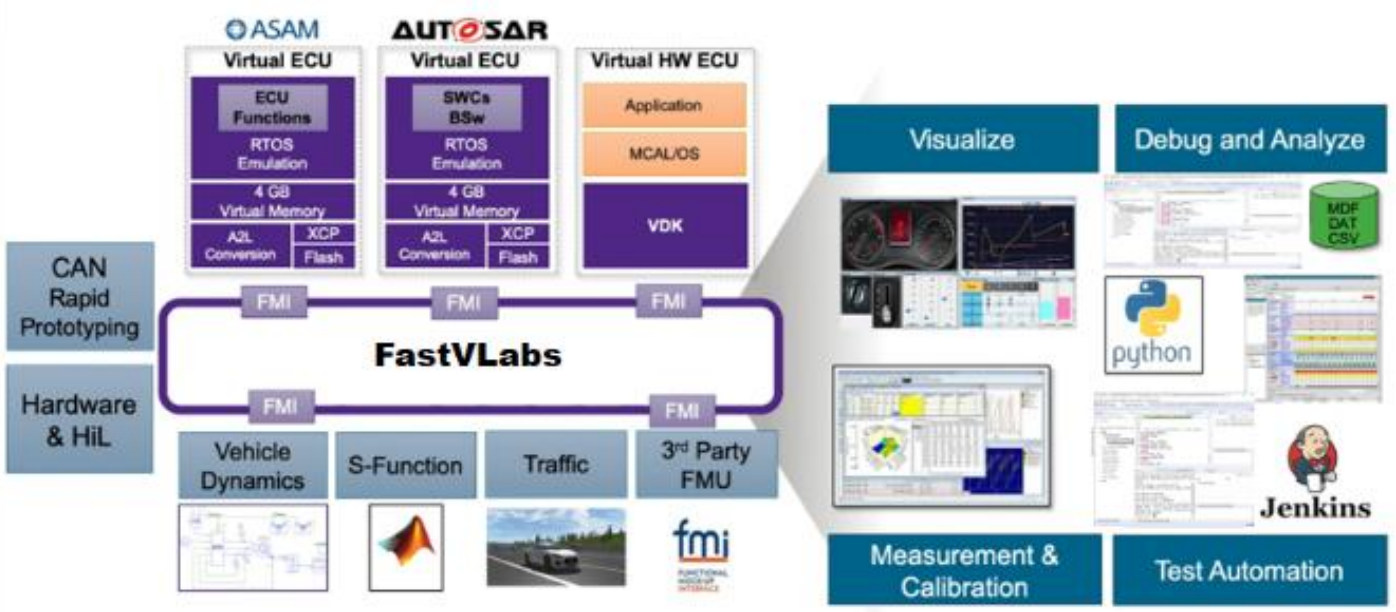
최신 보안 후속 조치 지원
ASIC, FPGA, SMART CARD 지원
지속적인 업데이트와 최신 취약점 반영

FastVLabs

고신뢰성 L4 vECU 기반의 시뮬레이션 엔진을 보유한 임베디드 소프트웨어 개발 검증 솔루션으로 유연한 클라우드 환경에서의 운영을 통해 효율적인 테스트 지원하는 차량 SW 개발 검증 및 가상화 솔루션

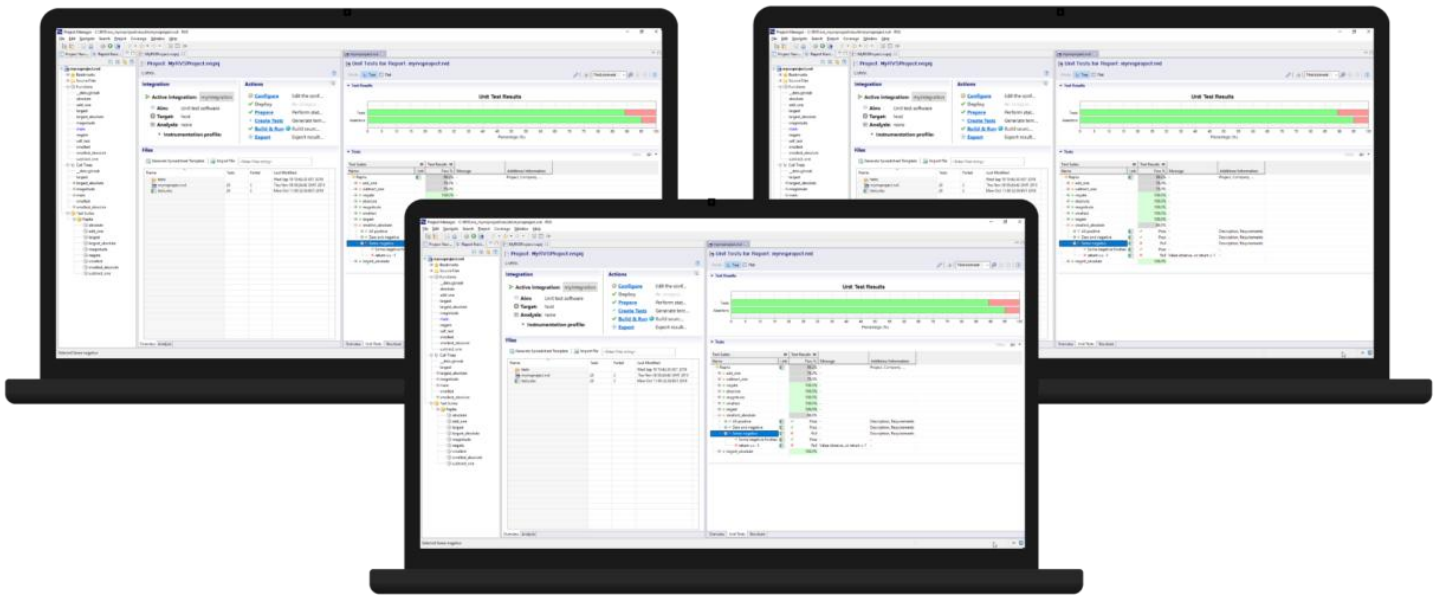
FEATURE

- 대상 바이너리 변경 없이 가상 ECU 상에서 실행
- TriCore, ARM, PowerPC, Renesas 등 주요 모델 지원
- dSPACE, Vector 외 주요 솔루션 연동 지원
- Dynamic Fault Injection 테스팅
- 코드 커버리지, 함수 프로파일링 기능
- 스크립트 기반 시험 자동화
- 실시간 SW 디버깅
- 차량 기능 시각화
- 요구사항에 맞춘 Customizing 기술 지원



RVS
(Rapita Verification Suite)

실제 타겟 환경 기반 검증으로 임베디드 소프트웨어의 신뢰성을 보장하며, 항공(DO-178C) 및 자동차 (ISO 26262) 등 국제 안전 표준 준수를 위한 효과적인 검증 솔루션



RVS

FEATURE

RapiTest
: 소스코드 작성 없이 멀티스레드 및 요구사항 기반 단위·통합·시스템 테스트를 효율적으로 작성·실행

RapiCover
: 코드 자동 계측으로 BC/DC, MC/DC 등 구조적 커버리지를 수집·분석해 검증 작업을 최대 40% 절감

RapiTime
: 정적 분석과 측정 기반 방식을 결합해 실제 하드웨어에서 안전한 WCET 상한 값을 산출

RapiTask
: 태스크 수준의 타이밍을 시각적으로 분석해 플랫폼·RTOS와 무관하게 병목과 희귀 이벤트를 식별

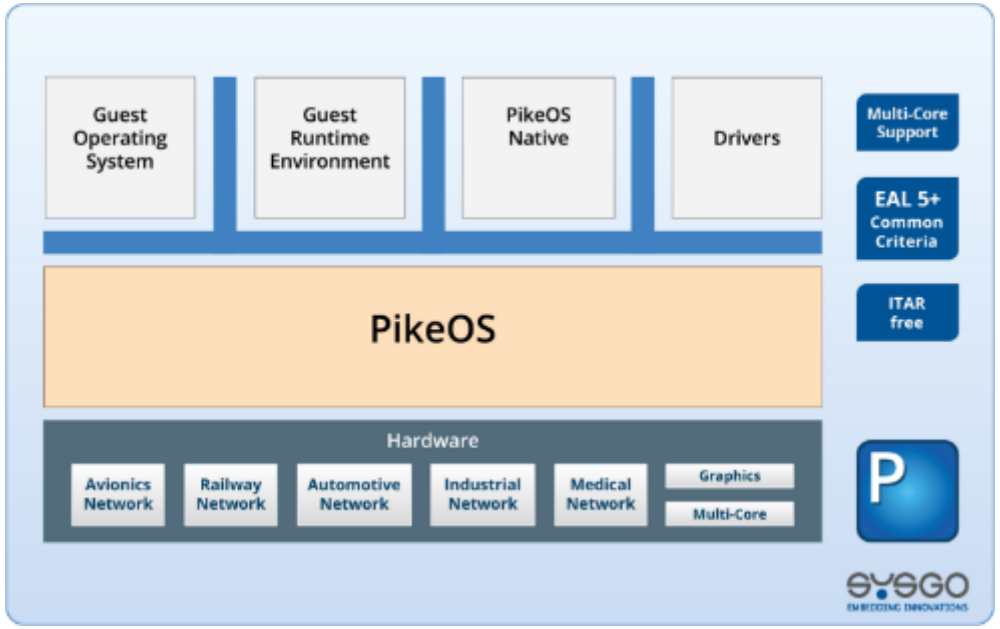
DO-178C / ISO 26262 인증 근거 자료 제공
: 검증 키트와 타깃 통합 서비스를 통해 DAL A를 포함한 항공·자동차 안전 인증을 지원

PikeOS

고신뢰성 임베디드 시스템 개발을 위한 Real-Time OS 및 인증 솔루션으로 높은 안정성과 보안성과 임베디드 시스템에 최적화된 Linux 솔루션

항공우주, 철도, 자동차, 방위 산업 등 고도의 안전성 및 보안이 요구되는 산업 분야에 적용하는 임베디드 시스템의 경우 높은 신뢰성 확보가 필수로 요구되고 있습니다.

쿤텍은 다양한 플랫폼에 적용한 사례와 많은 경험을 보유한 SYSGO 솔루션을 통해 모듈식 인증 키트 제공과 높은 수준을 요구하는 국제표준을 준수함에 있어서 시간과 비용을 절감할 수 있도록 지원합니다.



NXTCore

국내 최초로 3GPP 17 표준을 준수하는 올인원 특화망 5G 코어로 향후 6G를 포함한 이동통신 시스템의 핵심 역할을 수행하며 5G 특화망 인프라 구축에 필요한 모든 솔루션, 운영, 교육, 서비스, 개발을 All In One & Service로 제공

- 검증된 글로벌 5G 코어 시스템과 패키지를 최고의 가격으로 제공
- 5G 표준 완벽 준수로 Vendor Lock-in 없이 지원
- 코어 개방형 정책을 통한 B2B 서비스 개발 및 B2B 서비스와 연동 용이(소스코드 제공)
- 5G 인프라 구축에 필요한 모든 솔루션 제공(5G Core, gNB, CPE, UE, USIM, eSIM 및 5G특화 어플리케이션 등)
- 구축 후 전문인력 교육 / 운영 서비스 제공
- 특화망 5G 주파수 신청/허가 업무 지원

제품 특장점

- 최고 처리 속도 80Gbps 지원
- 최대 10만 이하 동시 접속시에도 안정적인 서비스 지원
- 특정 제조사에 대한 종속성이 없는 5G 코어 제공
- 실시간 데이터 전송과 분석을 통해 잠재적 위험 사전 감지 가능
- 데이터 운영에 적합한 5G Core NF 구성 및 유연한 Bandwidth 커스터마이징
- 높은 이식성, HW 종속성 없음, 외부라이브러리 종속성 없음
- 컨테이너화, 도커화 된 형태 뿐만 아니라 가상 시스템에서도 작동
- 클라우드 뿐만 아니라 사내 COTS 서버에서도 배포 가능
- 멀티인스턴스 구축으로 확장 가능

03 Service

1. 솔루션 구축
2. 교육/컨설팅

COrporation **ON** by **TEC**hnology

다양한 분야에 걸친 솔루션 구축

심층적인 요구사항 분석을 토대로 완성도 높은 보안 솔루션 운영 환경 구축을 지원
주요 구축 분야 | 국방, 공공, 금융, 제조, 민간 분야 등

다양한 프로젝트 경험과 산업환경 구축 경험을 토대로 네트워크에 대한 전문 지식과 심층적인 요구사항을 분석하여 완성도 높고 안정적인 고객 맞춤형 환경 구축 및 보안 솔루션 공급 수행

쿤텍 아카데미 운영

쿤텍은 전문 장비를 갖춘 아카데미를 활용한 실습(Hands-on) 기반 교육과 산업분야별 요구사항에 특화된 컨설팅을 통해 실제 산업분야의 보안 관리 역량 강화를 지원

실무 역량 강화 보안 교육

- 임베디드 가상화 시스템 교육
- 오픈소스 보안 취약점 교육
- OT/ICS 보안 교육
- OSINT 교육


교육장

보안 컨설팅

- 오픈소스 거버넌스 컨설팅
- CSMS 보안 내재화 컨설팅
- OT/ICS 보안 모니터링 컨설팅
- 사이버 위협 및 범죄 데이터 조사 분석 컨설팅
- 소스코드 기반 보안 점검 컨설팅

실습 장비를 갖춘 쿤텍 아카데미


온라인 강의 녹화 장비


제어시스템 시뮬레이터

디지털 전환 시대, DX 융합보안 전문기업

COrporation ON by TECHnology

COONTEC

쿤텍은 디지털 전환으로 대표되는 시대 변화의 흐름 속에서
안전하고 믿을 수 있는 환경을 구축하여
모두가 앞서 나갈 수 있는 세상을 만들기 위해 노력하고 있습니다.

A. 경기도 성남시 수정구 창업로 54, 가동 609호 T. 031-751-9088 H. www.coontec.com
제품문의 marketing@coontec.com 제휴문의 sales@coontec.com 채용문의 hr@coontec.com