Powering DX with Convergence Security

COONTEC

CORporation ON by TECHnology

CONTENTS

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

A sweeping digital transformation is reshaping every industry.
When we look back fifty years from now, we will recognize this moment as the beginning of a powerful new wave.
At COONTEC, we place security at the core of convergence industries essential to digital transformation. We help our customers accelerate digital connectivity with confidence—and go beyond that. Through our people, our technology, and our corporate culture, COONTEC is committed to leading this era of transformation and shaping the future.

COONTEC CEO Joon Pang

We live in an era where we are born too late to explore the world and discover new continents, yet too early to travel through space.
In navigating the new wave of the Fourth Industrial Revolution, COONTEC seeks to journey alongside our customers—reflecting together on where we should go and how we should move forward—and to present a clear, responsible, and growth-oriented direction for the future.

01 COMPANY

1. Company Overview
2. Corporate Milestones & Achievements
3. Our organization
4. Annual Revenue Trend
5. Core Competitiveness
6. Customers

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

Company Name	COONTEC Co., Ltd.	CEO	**Joon Pang**
Start up	Jan 22, 2016	Employees	88 (‘26.02)
Business Area	**Powering Digital Transformation with DX Convergence Security** ICS/OT security monitoring solution, Embedded virtualization solution supply, Network security solution, Providing security professional education and consulting services, AI/Cloud solution supply, Shipbuilding & Maritime Security		
Offices	Headquarters / R&D Center / Academy		

2016~2018 | Foundation & Growth

- Founded COONTEC (2016)
- Established Corporate R&D Center
- Certified as a Venture Company
- Built IoT Security Testbed

2018~2020 | Solution Portfolio Expansion

- Developed Linux-based behavior detection & prevention solution
- Developed AI-based behavior detection framework for smart factories
- Developed sandbox-based IoT malicious behavior detection solution
- Supplied open-source inspection solutions to leading automotive technology company (T Company)

2020~2022 | Establishing a Solution Business Framework

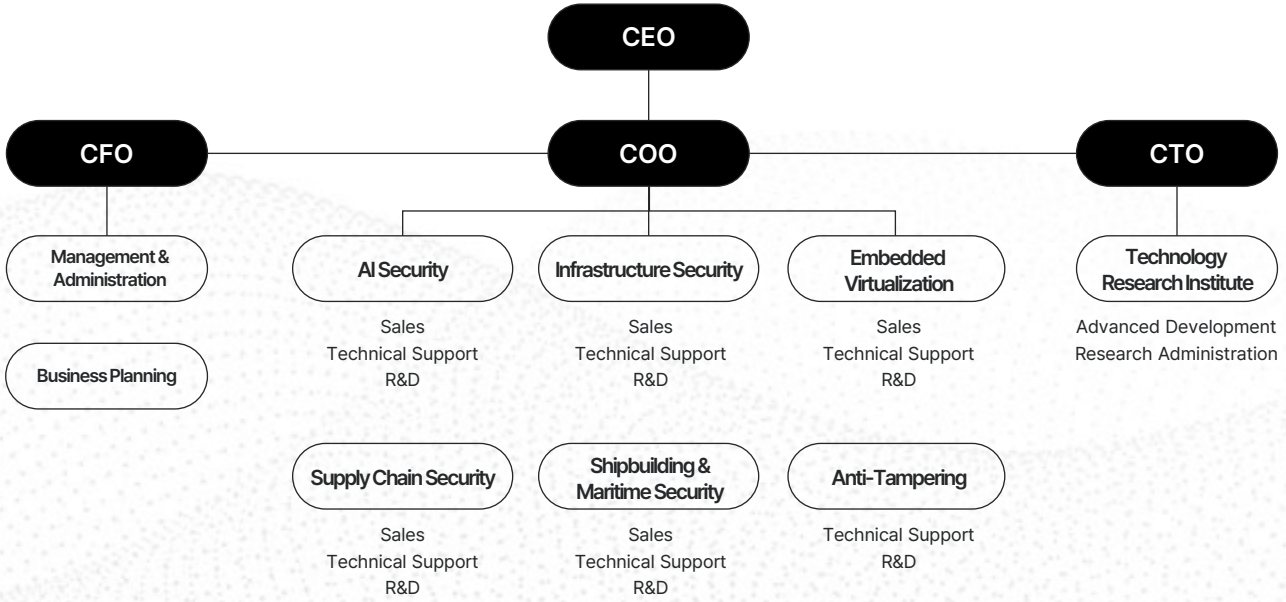
- Supplied next-generation hacking response system for power plant networks
- Delivered white-box cryptographic libraries for enterprise applications
- Provided OT network security consulting
- Developed defense simulation training program
- Built open-source vulnerability assessment system for financial institution
- (S Bank)

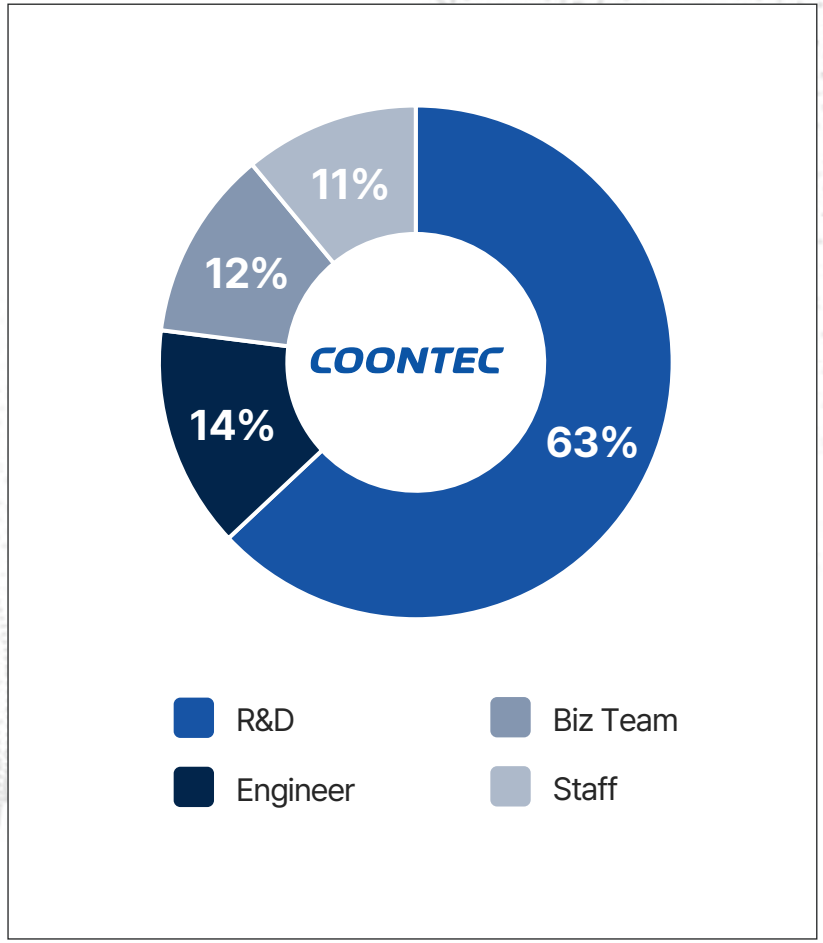
2022~2024 | Business Expansion

- Launched COONTEC Academy
- Supplied binary vulnerability analysis tool to K Bank
- Established open-source governance framework for major enterprise (H Company)
- Built open-source management system for N Bank
- Established cybersecurity system for C Company
- Implemented online counterfeit product distribution monitoring

2024~Present | New Leap Forward

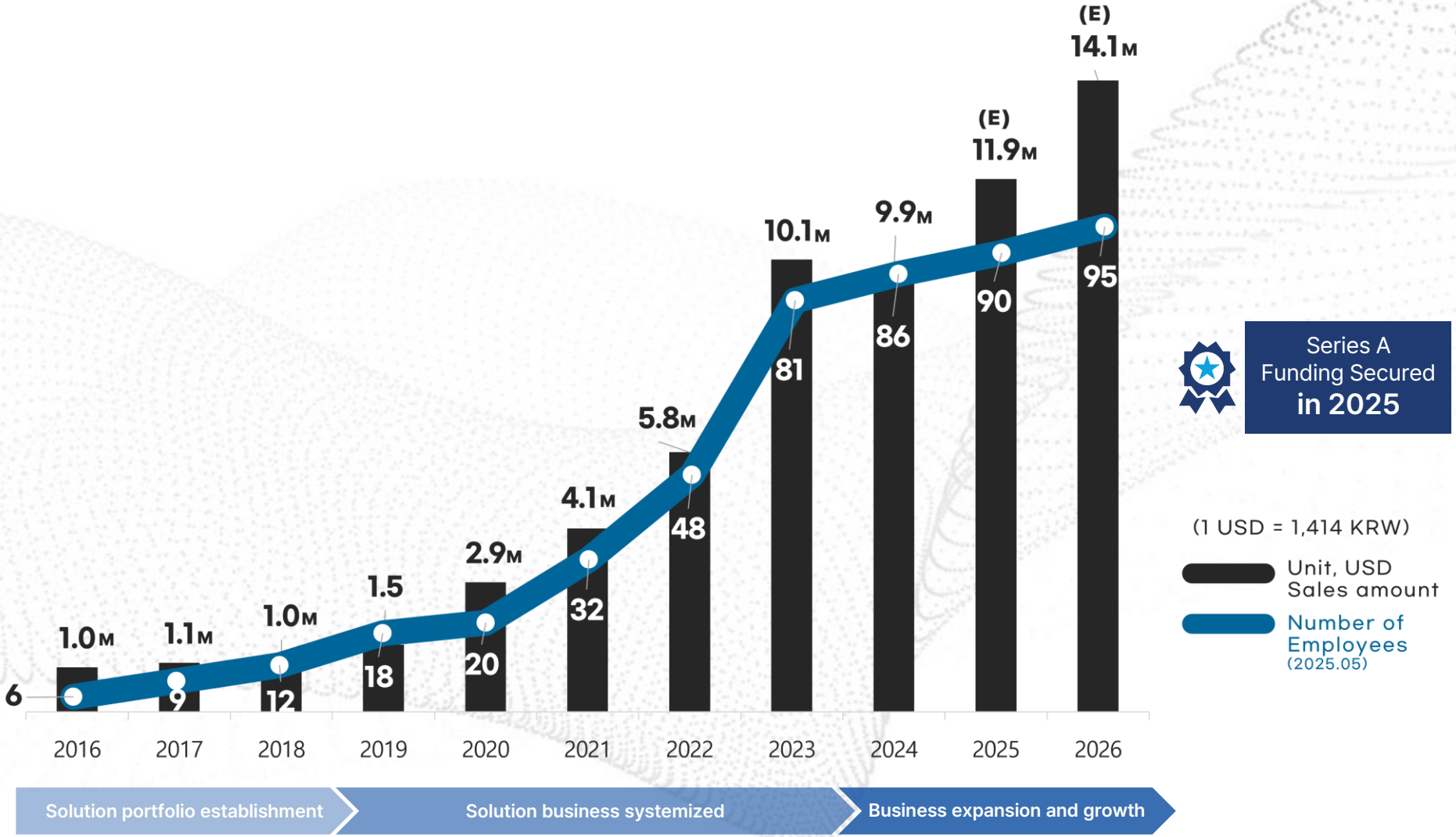
- Built open-source management systems for multiple financial institutions (L Life Insurance, S Bank, M Securities, W Card)
- Conducted SBOM-based software supply chain security validation project
- Secured Series A investment (HS Investment, NH Venture)





77% of the total employees are R&D and technical support personnel, and they are composed mainly of those with more than **15 years of experience** in embedded virtualization and supply chain security, so they have excellent project performance capabilities.

In addition to the R&D and technical support departments, the business execution and business support departments are also composed of high-quality personnel with experience in carrying out projects in a number of related fields, supporting stable and high-quality projects.


(E)
14.1M
(E)
11.9M
10.1M
9.9M
5.8M
4.1M
2.9M
1.5
1.0M
1.1M
1.0M
6
9
12
18
20
32
48
81
86
90
95
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
Solution portfolio establishment
Solution business systemized
Business expansion and growth
Series A Funding Secured in 2025
(1 USD = 1,414 KRW)
Unit, USD Sales amount
Number of Employees (2025.05)

Various portfolios

We have a portfolio of security solutions that can manage organically from embedded SW to supply chain.

Specialized performance

Several performance and experience in specialized fields that require solutions such as defense, finance, and public.

Development Capabilities

Operating a corporate-affiliated research institute composed mainly of developers with more than 10 years of experience and developing new solutions.

Automotive

AUTOCRYPT, 03IGO, HYUNDAI AutoEver, THINKWARE, HYUNDAI MOTOR GROUP, GIGA, HL Klemove

Defense/Aerospace & Railway

Ministry of National Defense Republic of Korea, KORAIL, LIG Nex1, 방위산업기술지원센터, Agency for Defense Development, HYUNDAI Rotem, KRRI Korea Railroad Research Institute

Finance

true friend Korea Investment & Securities Co., Ltd., Hana Financial Group, toss, MIRAE ASSET, KB Kookmin Bank, WOORI CARD, Sh 수협은행, Shinhan Bank

Manufacturing & Energy

SAMSUNG 삼성전자, SAMSUNG 삼성SDS, posco, KINAC, KOEN, KEPRI

Public

ETRI Electronics and Telecommunications Research Institute, NIS 국가정보원, KISA, gca, KEIS Korea Employment Information Service, IITP Institute of Information & Communications Technology Planning & Evaluation, ktl 한국산업기술시험원 Korea Testing Laboratory, NSR 국가보안기술연구소, DGTP 대구테크노파크 DAEGU TECHNOPARK, GWANGJU TECHNOPARK

Enterprise IT, etc.

CJ CHEILJEDANG, kt, SK ecoplant, Hanwha Corporation, LG Electronics, SK discovery, SHINSEGAE I&C

02 Solutions

1. Supply Chain Security
2. Infrastructure Security
3. AI Supply Chain
4. Shipbuilding & Maritime Security
5. Attack Surface Security
6. Embedded Security
7. Embedded SW
8. DX Solution

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

Supply Chain Security

AEZIZ
AEZIZ Binary
mend.io
sonatype

AI Supply Chain

SPLX

Infrastructure Security

TeraGRID
CLAROTY

Shipbuilding & Maritime Security

TGM
KR-CyberOne
KR-Tester

Attack Surface Security

Cyber Hawk Eye
penzzer

Embedded Security

SecureALPS
SECURE-IC

Embedded Software

FastVLabs
RAPITA Systems
PikeOS
RTOS & Hypervisor

DX Solution

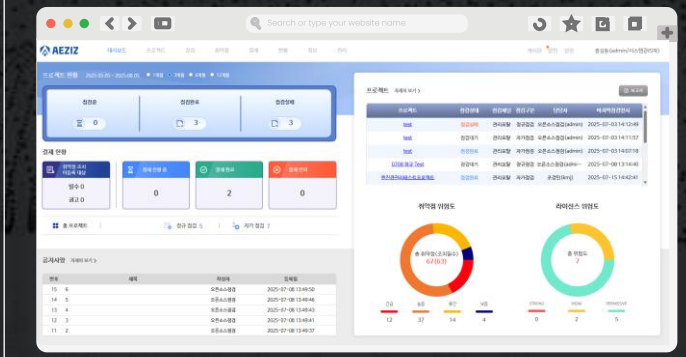
NXTCore

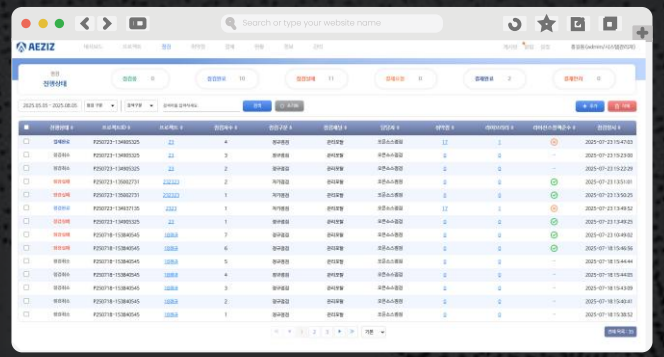
AEZIZ

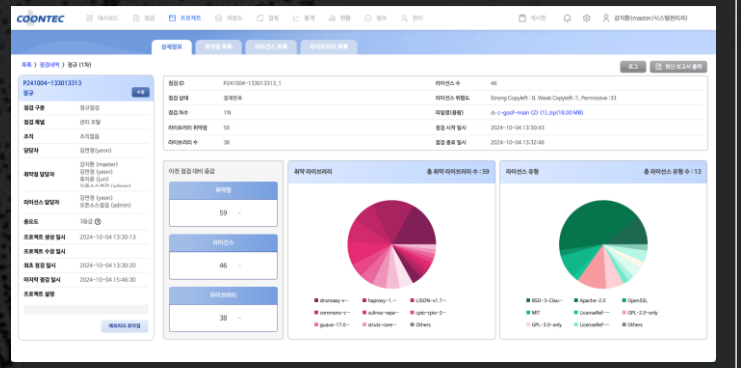
SW supply chain security solution for integrated management of open source and binary vulnerability analysis results.

In-house Developed

- Vulnerability Analysis
- Flexible Rights Management
- Integrated management
- Statistics and visualization
- Enhanced Security

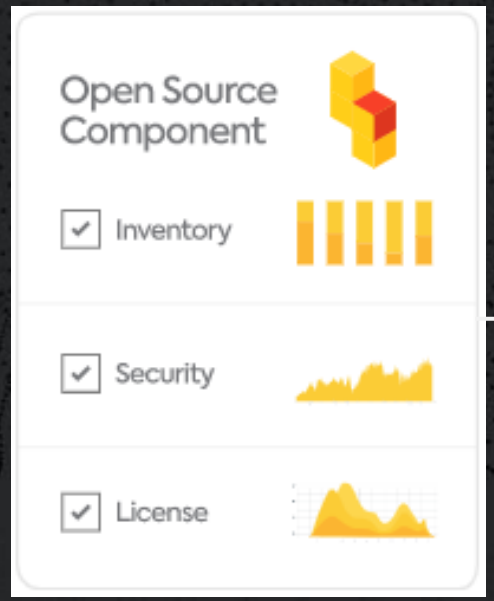






MEND

A digital signature-based, integrated, open-source management solution that quickly and accurately checks for open-source security vulnerabilities with a real-time DB built as SaaS.



Components /Licenses

- More than 30 open source storage-based open source components and licensing information, including GitHub and GitLab
- More than 100 million open source components and binary files
- More than 300 million source files

Vulnerability

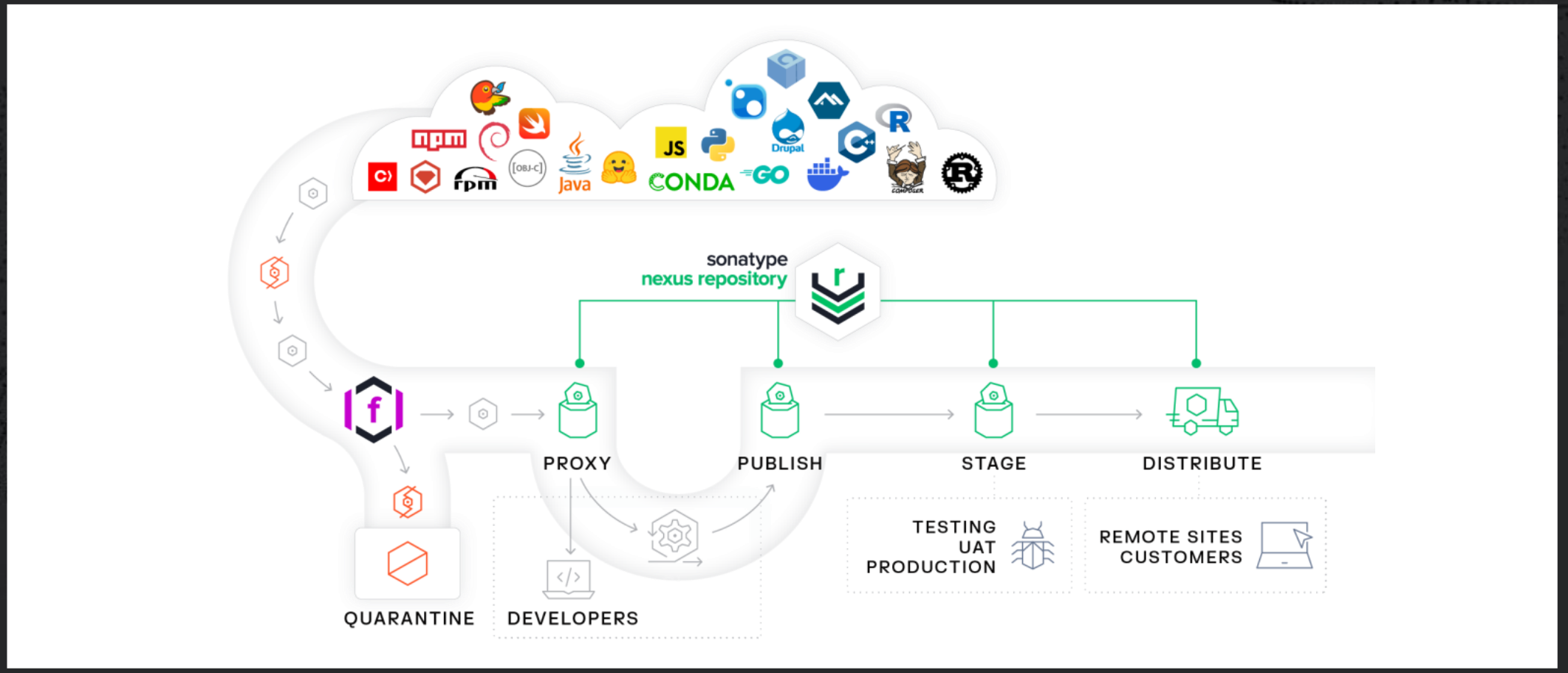
- More than 600,000 public vulnerabilities collected from NVD. GitHub Issue Tracker, RubyOnRails, and NodeSecurity Open-Source Projects
- More than 20,000 unique vulnerabilities verified by MEND's own security team

Quality

- Open-Source Community Revitalization Indicators
- Library bugs and fixes
- Number and severity of outstanding bugs

Sonatype

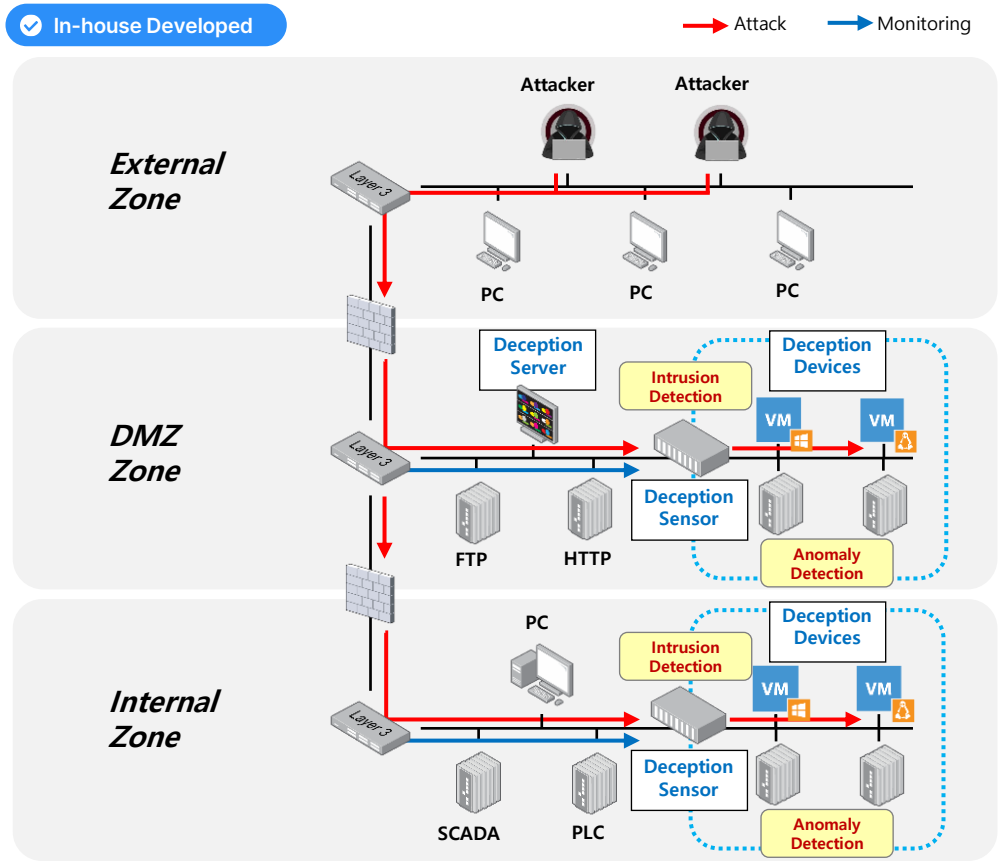
A binary artifact repository solution that enables organizations to securely and efficiently manage, store, and distribute software applications, AI/ML models, and components at scale—with speed, stability, and full control.



TeraGRID

Based on evolved honeypots, it is a cyber-based technology solution that enables you to quickly deploy large networks into Darkweb, regardless of device type, to respond to instant cyberattacks.

In-house Developed



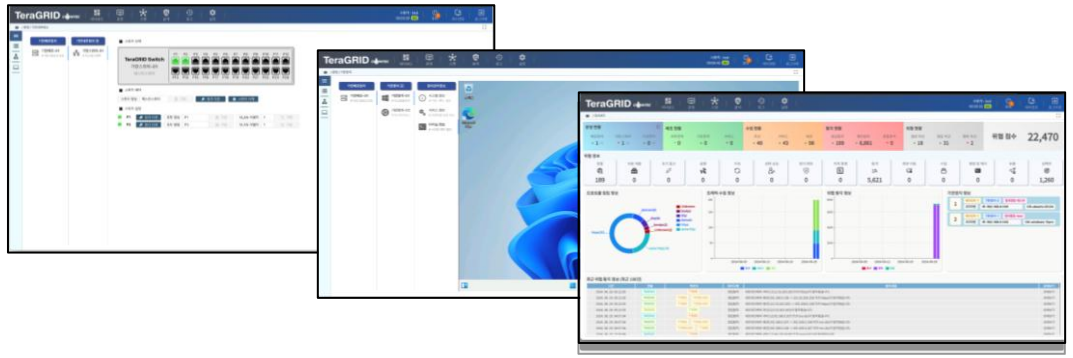
TeraGRID Server

- Management of deception deployment servers
- Collection and analysis of attacker threat intelligence
- Centralized visualization and management of deception assets

TeraGRID Sensor

- Management and monitoring of deception devices
- Collection and analysis of attacker behaviors
- Collection and analysis of real asset network traffic

TeraGRID SOC (Management & Integration)



Claroty

A monitoring solution that detects, analyzes, and continuously manages security threats based on visibility into the different types of assets, communications processes, and network sessions that make up OT/ICS.

Key Features

Comprehensive Asset Visibility

- Complete asset inventory and operational insight
- 100% visibility into hidden OT/IoT devices
- Automatic collection of detailed asset attributes

Real-Time Threat Detection

- Detection of anomalous behavior and unauthorized communications
- Analysis of known and unknown threats
- Visualization of attack paths

Vulnerability & Risk Management

- Asset-level CVE mapping and risk scoring
- Priority-based patch management guidance
- Tracking of configuration change history

Network Protection

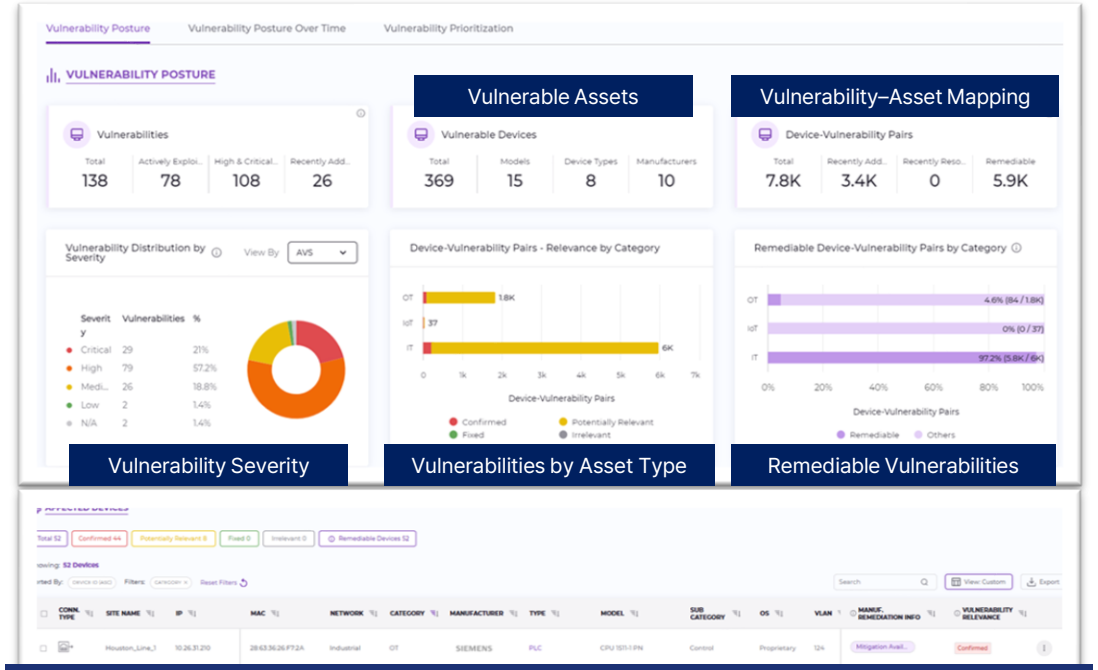
- Support for network segmentation
- Zero Trust policy implementation support
- Integrated secure remote access

Trusted by Industry Leaders

- **Named a Leader in the 2025 Gartner® Magic Quadrant™**
- **Ranked highest among 17 vendors for both Ability to Execute and Completeness of Vision**

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

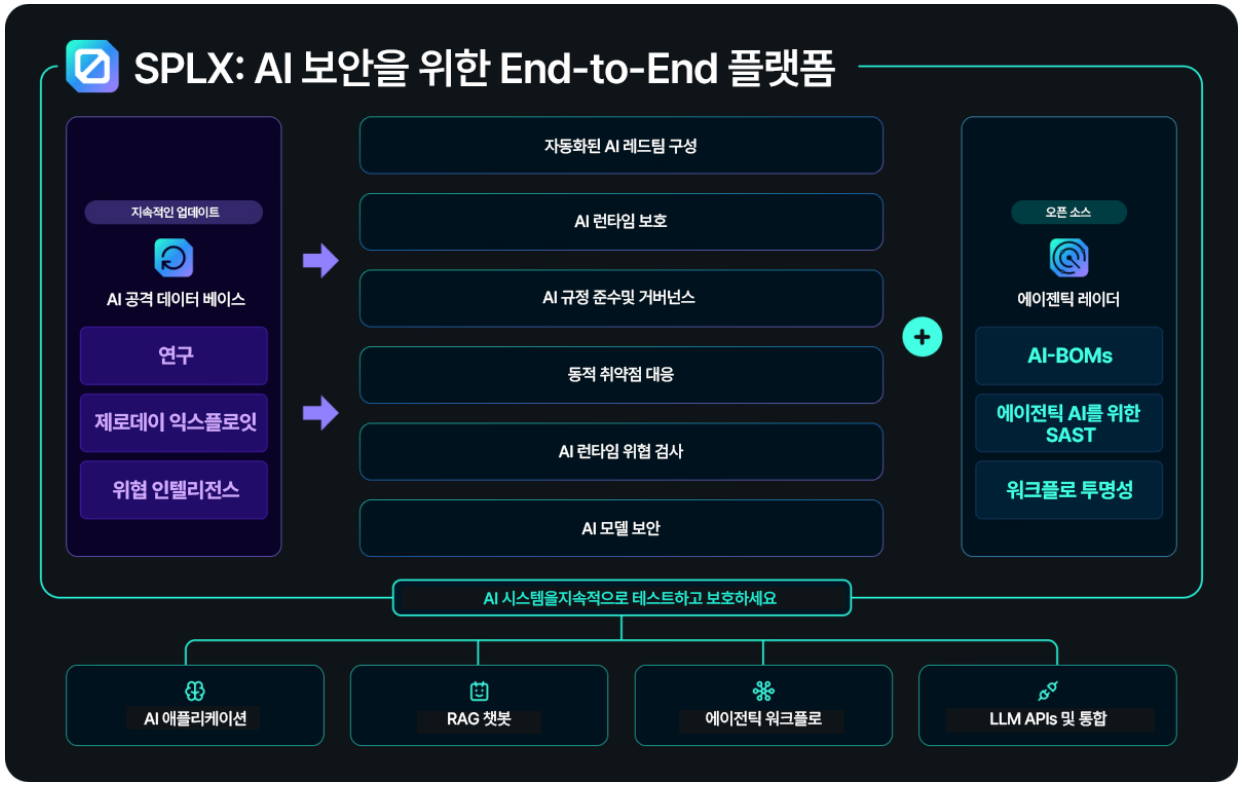
Integrated Dashboard



Identify Affected Devices by Correlating Asset Inventory with CVEs, Misconfigurations, and Team82 Research

SPLX

A full-stack AI security platform that safeguards AI systems across the lifecycle—from red teaming and runtime security to governance and risk management.



Automated AI Red Teaming	Automatically identifies real-world vulnerabilities in AI systems using large-scale attack datasets and customized testing scenarios.
AI Runtime Protection	Blocks malicious inputs and outputs, as well as sensitive data leakage, in real time through advanced guardrails.
AI Governance & Compliance	Ensures compliance by automatically mapping AI systems to global regulations and internal security standards.
Continuous Defense Optimization	Minimizes the attack surface by refining and strengthening system prompts based on red teaming results.
AI Runtime Threat Detection	Analyzes LLM logs to detect jailbreak attempts, prompt injection, and malicious queries in near real time.
Verified & Trusted AI Adoption Framework	Supports the secure adoption of commercial and open-source LLMs through comprehensive security assessments.

KR-CyberOne

A lifecycle security management solution for vessels aligned with IACS UR E26/E27, simplifying certification and automating compliance processes.

In-house Developed

Design

건조 (E26 & E27)
System Integrity

운항

운영 (E26)
Supply Chain Security

Maintenance & Decommissioning

KR-Tester

- Network scanning
- Automated asset inventory and topology mapping
- Resilience testing (network load testing)
- CSDD validation

KR-CyberOne

- Digital asset management
- Dynamic network visualization
- Automated risk assessment
- Generation of CSDD, CSRP, and regulatory documentation

TGM

- One-click report generation, submission, and approval
- Vulnerability management and integrated monitoring
- System backup and recovery support
- Cyber Threat Intelligence (CTI) and deception technology

'Design – Documentation – Verification'

'Detection – Response – Recovery'

TGM
(TeraGRID for Maritime)

An integrated “all-in-one” vessel security solution that detects and responds to advanced threats beyond the capabilities of traditional NMS and firewalls.

In-house Developed

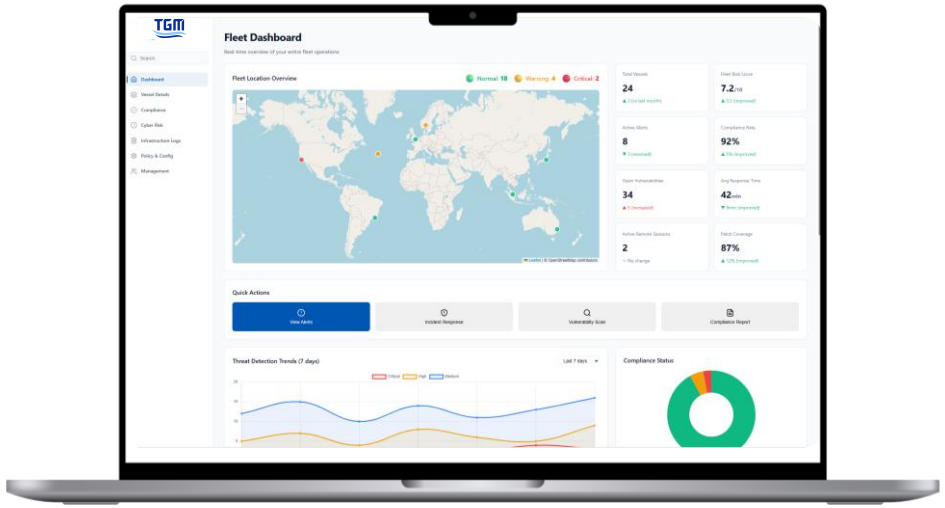
Integrated Maritime Security Solution

통합 보안 솔루션

SIEM
IDS
EDR
NMS

검사 대응 자동화

KR-CyberOne
“resilience certification and inspection support”



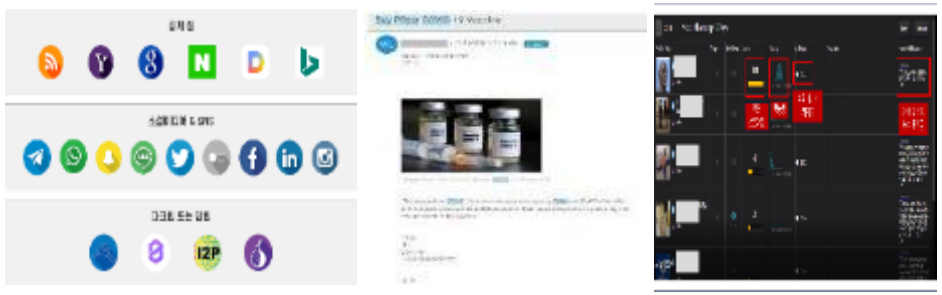
By consolidating SIEM, IDS, EDR, and NMS capabilities into a single platform, TGM protects both vessel OT equipment and IT systems while detecting and responding to sophisticated cyber threats in real time—delivering a next-generation maritime cybersecurity solution.

Cyber Hawk Eye

OSINT-based threat information collection and analysis platform is optimized for information collection on the Open Web, Deep Web, and Dark Web to effectively collect and analyze threat and crime-related information.

Provides optimized solutions for Surface, DeepWeb, and DarkWeb information collection

Various crime information evidence collection and analysis technologies that exist in the cyber world



- Secure data collection with avatars
- Provides modular, customized options
- SNS Link Analysis Cyber Crime Collection

Penzzer

An integrated solution combining penetration testing, dynamic analysis (DAST), and fuzzing to detect a wide range of security threats—including known and unknown vulnerabilities—through a single platform, while also supporting compliance with various regulatory requirements.

All-in-one

Both purging and pen tests are supported in one solution to detect both known and unknown vulnerabilities

Compliance

It supports ISO/SAE 21434, FDA, and various ISO standards and security regulations, and provides security management for the entire IoT-enabled supply chain.

Plug-and-play

All hardware and software are delivered as kits, connected to devices to be used for testing, enabling instant penetration testing and DAST.

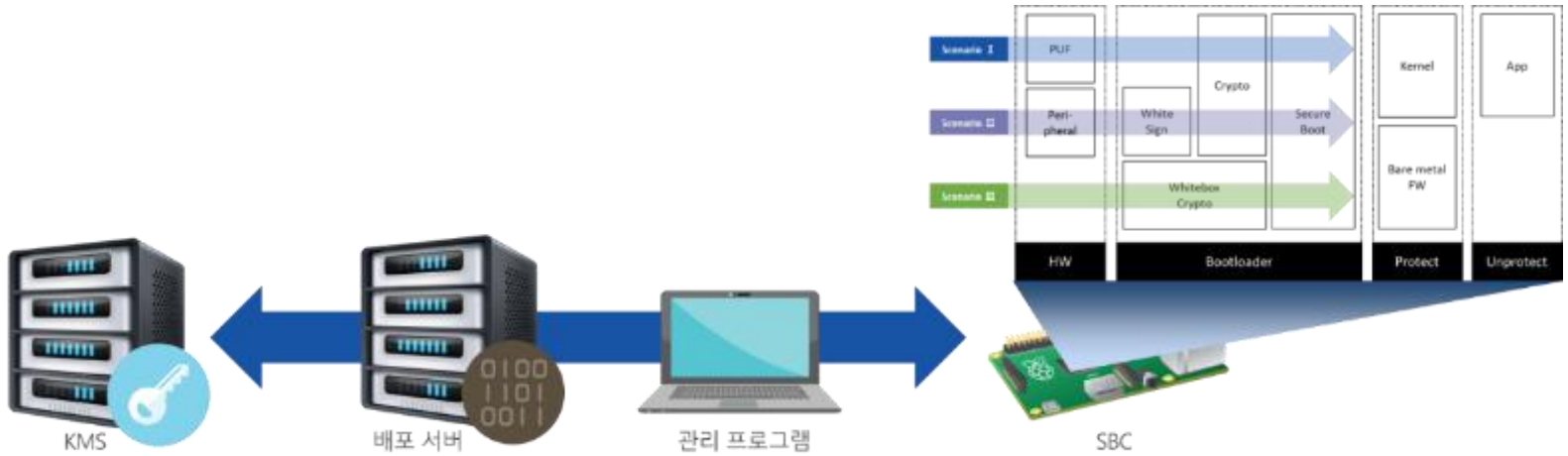
Easy-to-use

The easy and clear UI maximizes user convenience, making it easy and quick to test purging and pen tests.

Secure ALPS (1/2)

ALPS-Crypto | Provides a secure firmware and cryptographic key management framework for embedded environments.

- Protects the integrity and confidentiality of firmware installed in embedded devices, preventing tampering and safeguarding proprietary technologies.
- Ensures secure delivery of embedded software not only during manufacturing but also during updates through mutual authentication and encryption.
- Protects cryptographic keys by applying one of three key protection technologies—PUF, White-Sign, or White-Box Cryptography—selected based on device characteristics.
- Applies protection mechanisms from the boot stage to secure embedded devices from the earliest point of execution.



Secure ALPS (2/2)

ALPS-Shield | Provides application self-protection for embedded environments.

Solutions

Code Obfuscation
Defends against static analysis and reverse engineering (decompilation) attacks targeting application code.

Binary Encryption
Encrypts core application binaries to protect critical functionalities.

Binary Integrity Protection
Detects and prevents unauthorized modification of application binaries.

Resource Encryption
Encrypts application resource files to prevent unauthorized access or extraction.

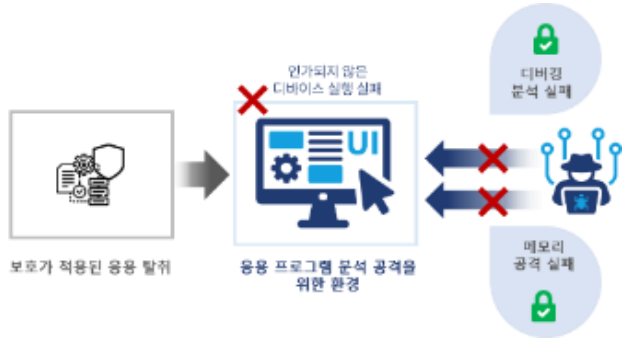
Device Binding
Prevents execution on unauthorized devices.

Anti-Debugging
Detects and blocks execution in debugging environments.

Binary Hardening
Protects applications loaded in memory against runtime attacks.

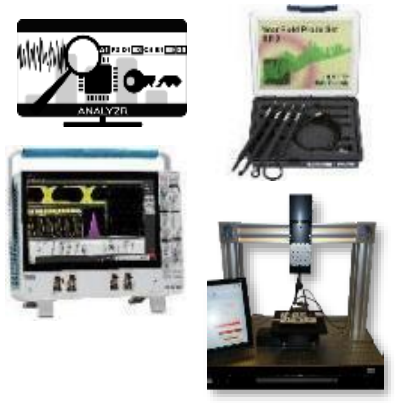
Code Obfuscation, Binary Encryption, Binary Integrity Protection, Resource Encryption

Device Binding, Anti-Debugging, Binary Hardening



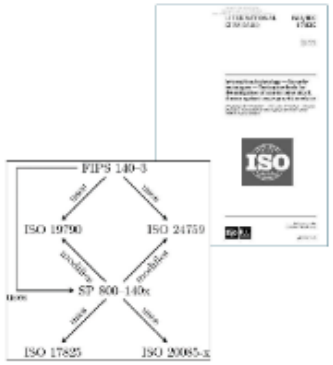
Secure-IC

A hardware security solution for embedded environments that detects threats through advanced SCA, FIA, and hardware Trojan analysis—providing mitigation IP and compliance support based on comprehensive evaluation.



Comprehensive Analysis Support

- Supports PASSIVE (SCA) and ACTIVE (FIA) attack analysis
- Enables both white-box and black-box evaluation approaches
- Provides testing equipment, analytical solutions, and proven methodologies



Compliance Support

Supports security validation for embedded environments in accordance with :
ISO/IEC 17825, ISO/IEC 20085, Common Criteria (CC) / ISO/IEC 15408, FIPS 140

Long-Term Support & Maintenance

- Ongoing security updates and post-certification support
- Support for ASIC, FPGA, and Smart Card platforms
- Continuous updates reflecting the latest vulnerabilities and security requirements

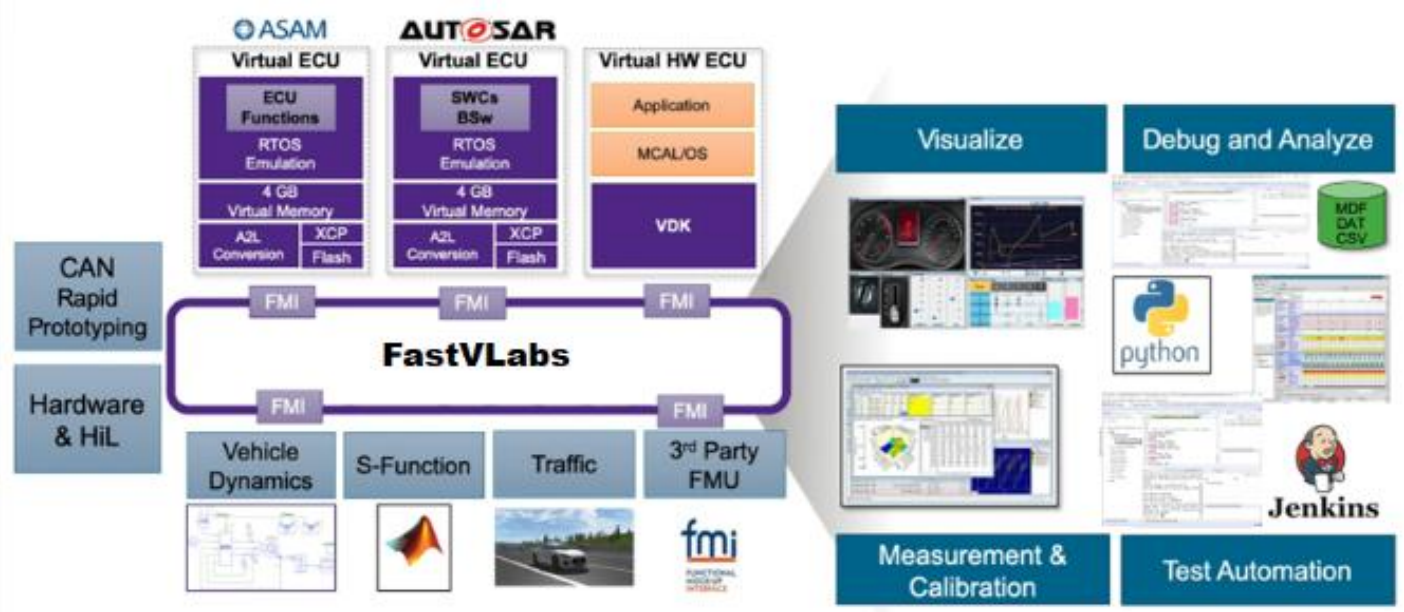
FastVLabs

Software development verification solution with a highly reliable L4 vECU-based simulation engine that enables efficient testing through operation in a flexible cloud environment.

In-house Developed

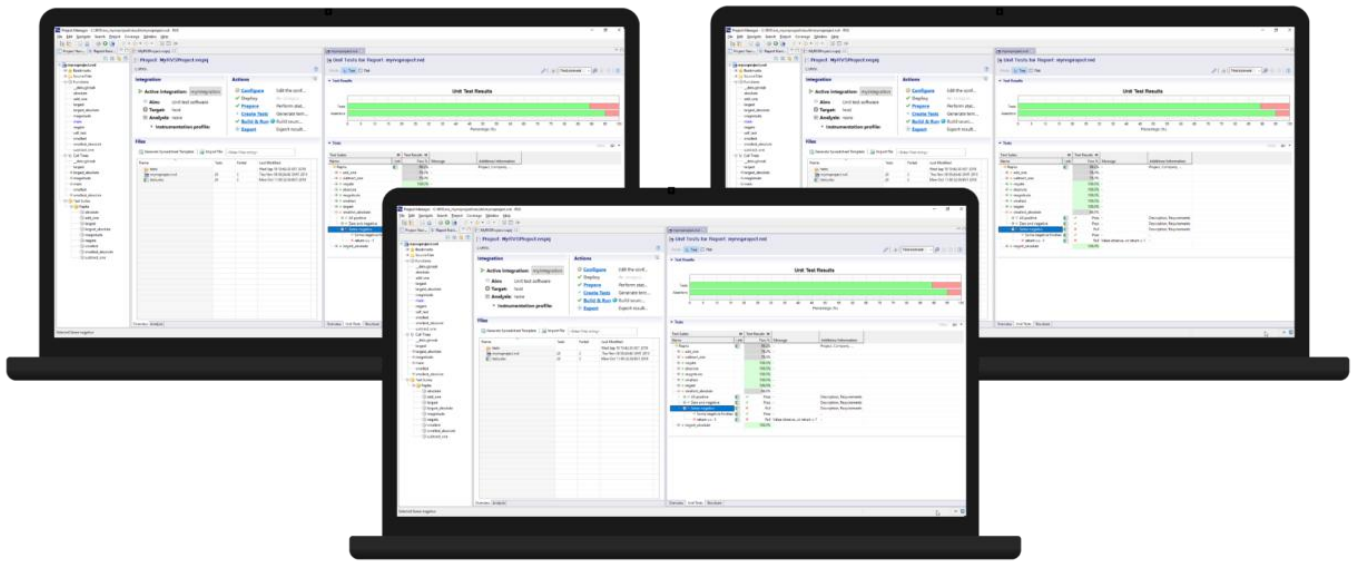
FEATURE

- Run on a virtual ECU without changing the destination binary
- Support for key models such as TriCore, ARM, PowerPC, Renesas, etc
- Support for interworking of key solutions other than dSPACE and Vector
- Dynamic Fault Injection Testing
- Code coverage, function profiling capabilities
- Automated script-based testing
- Real-time SW Debugging
- Visualize vehicle function
- Customizing technical support to your requirements



RVS
(Rapita Verification Suite)

A target-based verification solution that guarantees embedded software reliability and supports compliance with global safety standards, including DO-178C and ISO 26262.



RVS

FEATURE

RapiTest
: Efficiently creates and executes multi-threaded, requirements-based unit, integration, and system tests—without the need for source code instrumentation.

RapiCover
: Collects and analyzes structural coverage metrics, including BC/DC and MC/DC, through automatic code instrumentation—reducing verification effort by up to 40%.

RapiTime
: Combines static analysis with measurement-based techniques to calculate safe upper bounds for Worst-Case Execution Time (WCET) on real hardware.

RapiTask
: Provides visual task-level timing analysis to identify bottlenecks and rare events, independent of platform or RTOS.

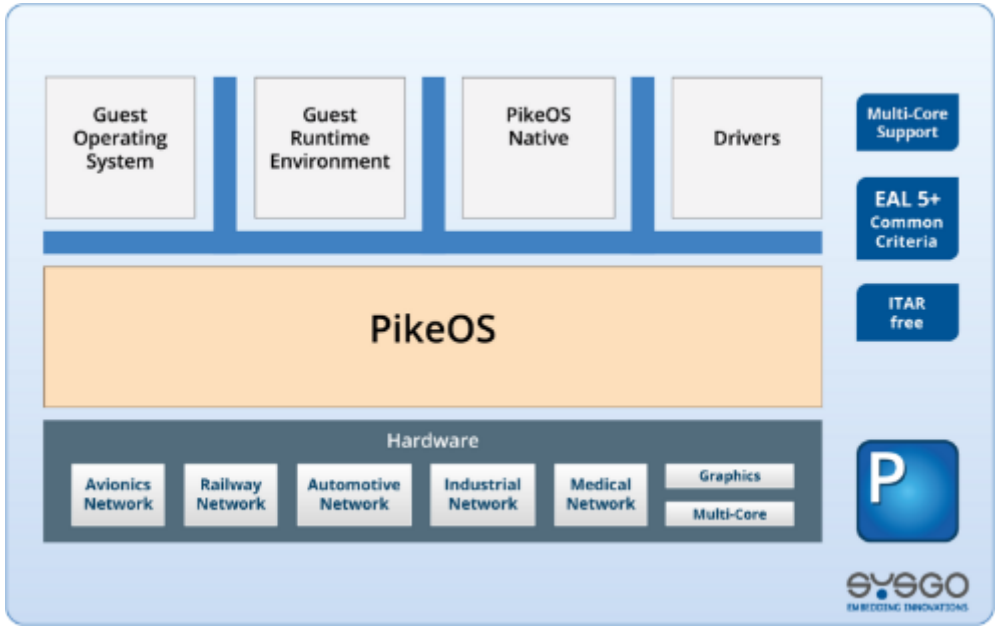
Certification Evidence Support for DO-178C & ISO 26262
: Supports aerospace and automotive safety certification—including DAL A—through verification kits and target integration services.

PikeOS

Real-Time OS and certification solutions for the development of highly reliable embedded systems provide high reliability, security, and Linux solutions optimized for embedded systems.

High reliability is required for embedded systems applied to industries that require high safety and security, such as aerospace, railroads, automobiles, and defense industries.

COONTEC helps you save time and money in delivering modular authentication kits and complying with high-level international standards through SYSGO solutions with examples and experience in a wide range of platforms.



NXTCore

The first all-in-one private 5G core in Korea compliant with 3GPP Release 17, NXTCore enables next-generation mobile networks—including future 6G—through a complete infrastructure and service delivery model.

In-house Developed

Key Strengths

- Provides a validated global 5G core system and package at competitive pricing
- Fully compliant with 5G standards, ensuring no vendor lock-in
- Open-core architecture enabling seamless B2B service development and integration (source code provided)
- Comprehensive solutions for private 5G infrastructure, including 5G Core, gNB, CPE, UE, USIM, eSIM, and specialized 5G applications
- Professional training and operational services after deployment
- Support for private 5G spectrum application and licensing processes

Product Differentiators

- Up to 80 Gbps throughput
- Stable service support for up to 100,000 concurrent connections
- Vendor-independent 5G core architecture
- Real-time data transmission and analytics for proactive risk detection
- Optimized 5G Core NF configuration and flexible bandwidth customization
- High portability with no hardware or external library dependencies
- Operates in containerized (Docker) and virtualized environments
- Deployable in both cloud environments and on-premise COTS servers
- Scalable through multi-instance architecture

03 Service

1. Solution Development
2. Training / Consulting

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

Service | Solution Development | Training / Consulting

In-house Developed

AEZIZ FastVLabs TeraGRID

Based on an in-depth requirement analysis help you build a high-quality security solution production environment.
Major Area | Defense, finance, public, manufacturing, private sector, etc.

Based on diverse project experience and experience in building an industrial environment, the network's expertise and in-depth requirements are analyzed to build a high-quality and reliable customized environment and provide security solutions.

COONTEC helps strengthen security management capabilities in real-world industries through hands-on training and consulting specialized in industry-specific requirements using professional-equipped academies.

Training

- Embedded Virtualization System Training
- Training Open-Source security vulnerabilities
- OT/ICS Security Training
- OSINT Training

Professional Training Facility

Consulting

- Open-Source Governance Consulting
- CSMS Security Internalization Consulting
- OT/ICS Security Monitoring Consulting
- Cyber Threat and Crime Data Investigation Analysis Consulting
- Source code-based security inspection consulting

Devices for Hands-on

Online Course Recording Studio & Equipment

Industrial Control System (ICS) Simulator

디지털 전환 시대, DX 융합보안 전문기업

COrporation ON by TECHnology

COONTEC

In the midst of the transformative wave represented by digital transformation,
Coontec is committed to building a safe and trustworthy environment, striving to create
a world where everyone can move forward together.

A. Gadong 609, 54, Changjang-ro, Sujeong-gu, Seongnam-si, Gyeonggi-do T. +82 31-751-9088 H. www.coontec.com

Product Inquiry marketing@coontec.com Partnership Inquiry sales@coontec.com Recruitment Inquiry hr@coontec.com

blog