COrporation ON by TEChnology

쿤텍 회사소개서

COrporation ON by TEChnology

COONTEC

CONTENTS

COrporation ON by TEChnology

CEO 인사말

모든 산업 분야에 **디지털 대전환**이 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

COrporation ON by TEChnology

VISION

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.

Extreme Engineering

Our Company

COrporation ON by TEChnology | 쿤텍

01

01 회사개요

쿤텍㈜ | COONTEC Co., Ltd.

쿤텍은 진화하는 보안 위협에 대한 빠르고 전문적인 대응 방안을 제시하여
다양한 환경의 고객 자산을 보호합니다.

회사명	쿤텍㈜	대표자	방혁준
설립연도	2016년 01월 22일	임직원수	81명 ('23. 08 기준)
주소	HQ 경기도 성남시 수정구 창업로 54, 가동 609호 Lab 경기도 성남시 수정구 창업로 54, 나동 232호 Academy 경기도 성남시 수정구 달래내로 46, A타워 507호		
홈페이지	https://coontec.com		
주요 사업영역	**디지털 전환 시대, DX 보안 전문 기업 COONTEC** ▪ 인프라 보안 ▪ 개발 보안 ▪ 임베디드 보안 ▪ 공격표면 보안 ▪ 임베디드 SW ▪ DX 솔루션 ▪ 교육 및 컨설팅 서비스 제공		

02 주요 연혁 및 실적

2016 ~ 2017

- **쿤텍㈜ 설립**
- **기업부설연구소 설립**
- **벤처기업인증**
- IoT 보안테스트베드 구축

2018

- 이기종 리눅스 악성코드 행위기반 탐지/예방 솔루션 개발
- 스마트교통 보안위협 체험환경 구축
- 스마트 팩토리 IoT 지능형 악성코드 분석 및 탐지 프레임워크 개발

2019

- 샌드박스 기반 IoT기기 악성코드 탐지 및 대응 솔루션 개발
- 산업용 무선프로토콜 어댑터 개발
- RISC-V 가상머신 기반 보안 취약점 동적 분석환경 구축
- T사(첨단 차량IT기술 전문 상장사) 오픈소스 점검 솔루션 공급

2020

- **쿤텍 디자인센터 설립**
- 발전소 네트워크기반 차세대 해커유인시스템 공급
- Toss 애플리케이션 내 화이트박스 암호 라이브러리 공급

2021

- **이노비즈기업 인증**
- OT 네트워크 융합보안 컨설팅
- 융합보안 인력양성 스마트 자동차 분야 교육과정 운영
- 함정 사이버보안 프레임워크 개발
- S은행 오픈소스 보안 취약점 점검 시스템 구축

2022

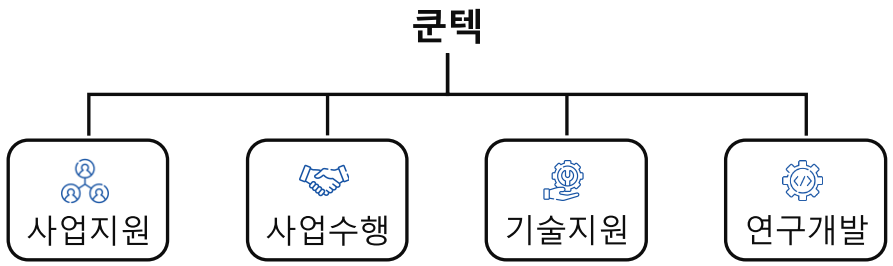
- **쿤텍 아카데미 개원**
- KB국민은행 바이너리 취약점 분석 도구 공급
- H사(대기업 계열 금융사) 오픈소스 거버넌스 구축
- 자동차 사이버 보안 교육 운영

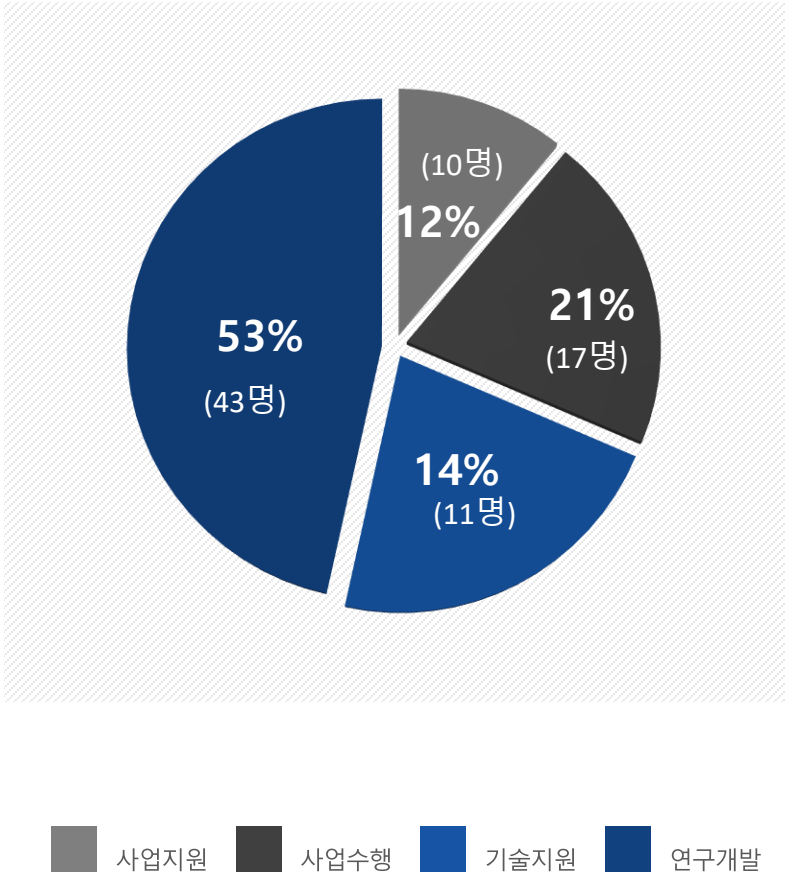
03 조직도 및 인력 현황

분야별 전문가로 구성된 기술 중심의 조직 운영

전체 임직원 중 67%가 연구개발 및 기술지원 인력으로 구성되어 있으며, 임베디드 가상화 및 공급망 보안 분야의 경력이 **15년 이상인 경력자 위주**로 구성되어 있어 뛰어난 프로젝트 수행 능력을 갖추고 있습니다.

연구개발, 기술지원 부서 외 사업수행, 사업지원 부서 역시 **다수의 관련 분야 프로젝트 수행 경험**을 보유한 고급 인력으로 구성되어 있어 **안정적이고 완성도 높은 프로젝트 수행을 지원**합니다.





04 지적재산권 현황

COONTEC

특허권

No.	명칭	상태	출원일자
1	리눅스 환경의 악성 코드 검출 방법 및 장치	등록	19-05-29
2	하이퍼바이저 시스템 및 하이퍼바이저 동작 방법	등록	22-05-30
3	가상머신 시스템 및 이를 이용한 가상머신 프로비저닝 방법	등록	22-11-29
4	인메모리를 이용한 가상 머신 시스템 및 그 동작 방법	등록	23-01-19
5	펌웨어 위변조 검출 장치	출원	21-10-20
6	기만 기술에 사용되는 동적 트랩 생성 방법	출원	21-12-03
7	블록체인을 이용한 SBOM의 무결성 보존 방법	출원	22-11-17
8	가상머신을 이용한 난독화 복잡도 평가 방법	출원	22-11-17
9	가상머신 시스템에서 인메모리 기반의 오버레이 스토리지 서비스 방법	출원	22-11-22
10	실자산 및 주변환경 스캔으로 주변환경과 유사한 사이버트랩 생성 방법	출원	22-11-22
11	블록체인을 이용한 SBOM 관리 시스템 및 방법	출원	23-06-02
12	PUF 기반의 리소스 암복호화 장치	출원	23-08-23
13	화이트박스 암호의 비밀키 보호를 위한 방법 및 시스템	출원	23-08-24

저작권

No.	명칭	상태	등록일자
1	SDR(소프트웨어 디파인 라디오) 기반 다중 Protocol(프로토콜) 패킷 분석기	등록	18-06-05
2	SDR(에스디알) 기반 WiFi BLE IoT(와이파이비엘이 아이오티) 무선 패킷	등록	18-08-17
3	임베디드 전용 가상 플랫폼 기반 악성 행위 분석 방법	등록	19-10-29
4	이기종 리눅스 악성코드 동적분석 동작 모니터링 프로그램	등록	21-04-07
5	펌웨어 위변조 검출 프로그램	등록	21-10-06
6	개방형 차량 인포테인먼트 모의제어 프로그램	등록	21-11-19
7	트랩배포서버 프로그램(등록번호 : C-2022-044090)	등록	22-11-07
8	트랩배포서버 프로그램(등록번호 : C-2022-044091)	등록	22-11-17
9	취약점 탐지 자동화 도구 상용 시제품 RestAPI(백엔드) 서버 소프트웨어	등록	22-11-22

특허권	저작권	상표권
총 13건 (등록 4건/출원 9건)	**총 9건** (등록 9건)	**총 7건** (등록 1건/출원 6건)

06 핵심 경쟁력

다양한 보안 포트폴리오

임베디드 SW부터 공급망까지
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

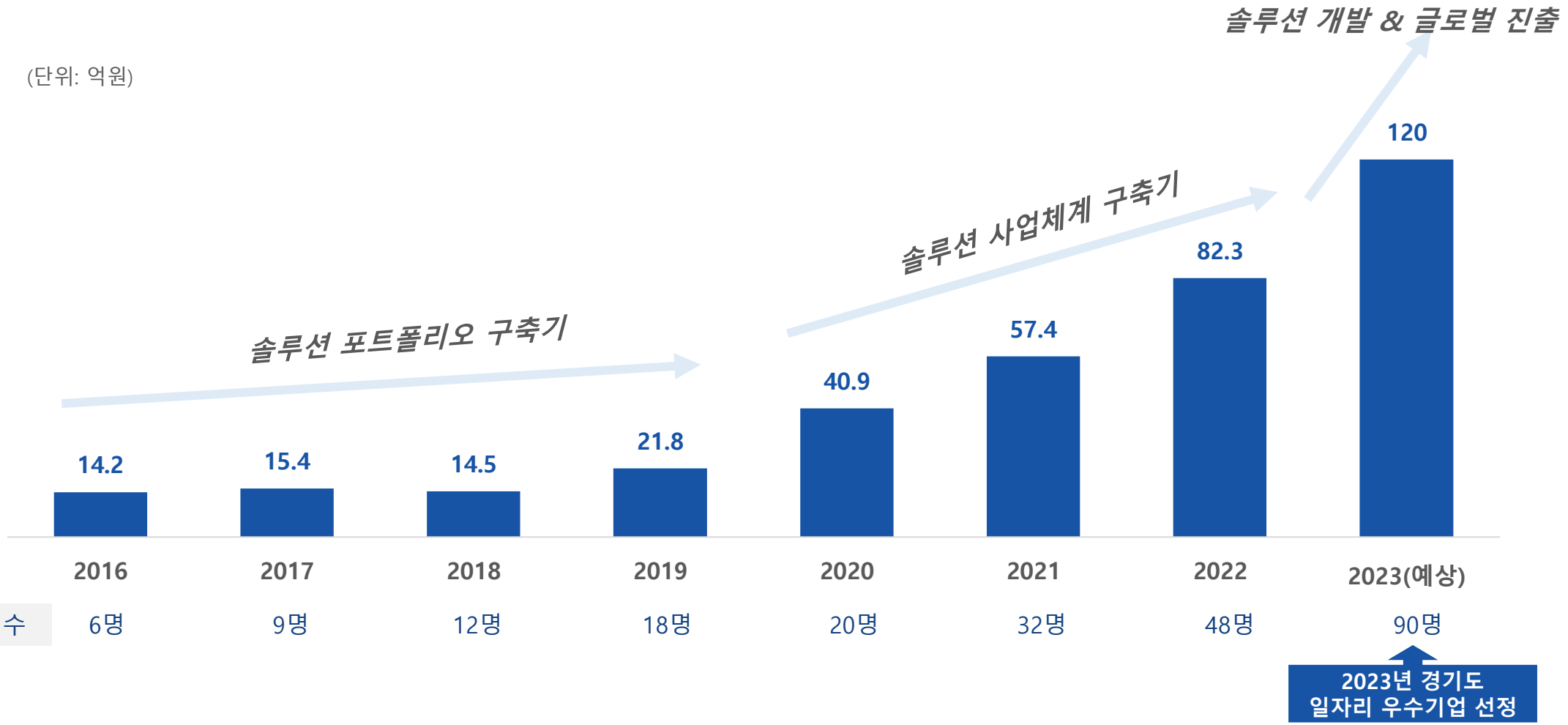
경력 10년 이상의 개발자 위주로
구성된 기업부설연구소 운영,
신규 솔루션 개발 중

다수의 정부 과제 수행

'23년 예산 66억, 12개 정부 과제 수행
'24~'27년 진행 예정 정부 과제 9개
잔여 예산 101억 확보

05 매출 및 임직원수 추이

(단위: 억원)



Extreme Engineering

Our Solutions

02

Extreme Engineering

Our Solutions

Part 1. 보안

Part 2. 임베디드SW

Part 3. DX솔루션

COrporation ON by TEChnology | 쿤텍

02

00 솔루션 포트폴리오

COONTEC

인프라 보안

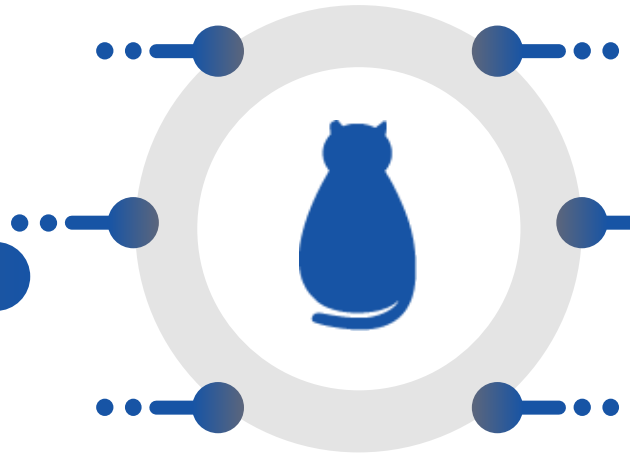
- **테라그리드(TeraGRID)**
- 오르카(ORCA)
- 트리트와이즈(TreatWise)
- 클래로티(Claroty)
- 비욘드트러스트(BeyondTrust)
- 세이프브리치(SafeBreach)

개발 보안

- **이지스(AEGIS)**
- 멘드(Mend)
- 사이벨리움(Cybellum)

임베디드 보안

- 펜저(Penzzer)
- **시큐어알프스(SecureAPLS)**
- 시큐어아이씨(Secure-IC)



공격표면 보안

- 사이버호크아이(Cyber Hawk Eye)
- 체이널리시스(Chainalysis)
- 파노레이(Panorays)

임베디드 SW

- 임페라스(Imperas)
- 시스고(Sysgo)
- 패스트브이랩(FastVLABS)

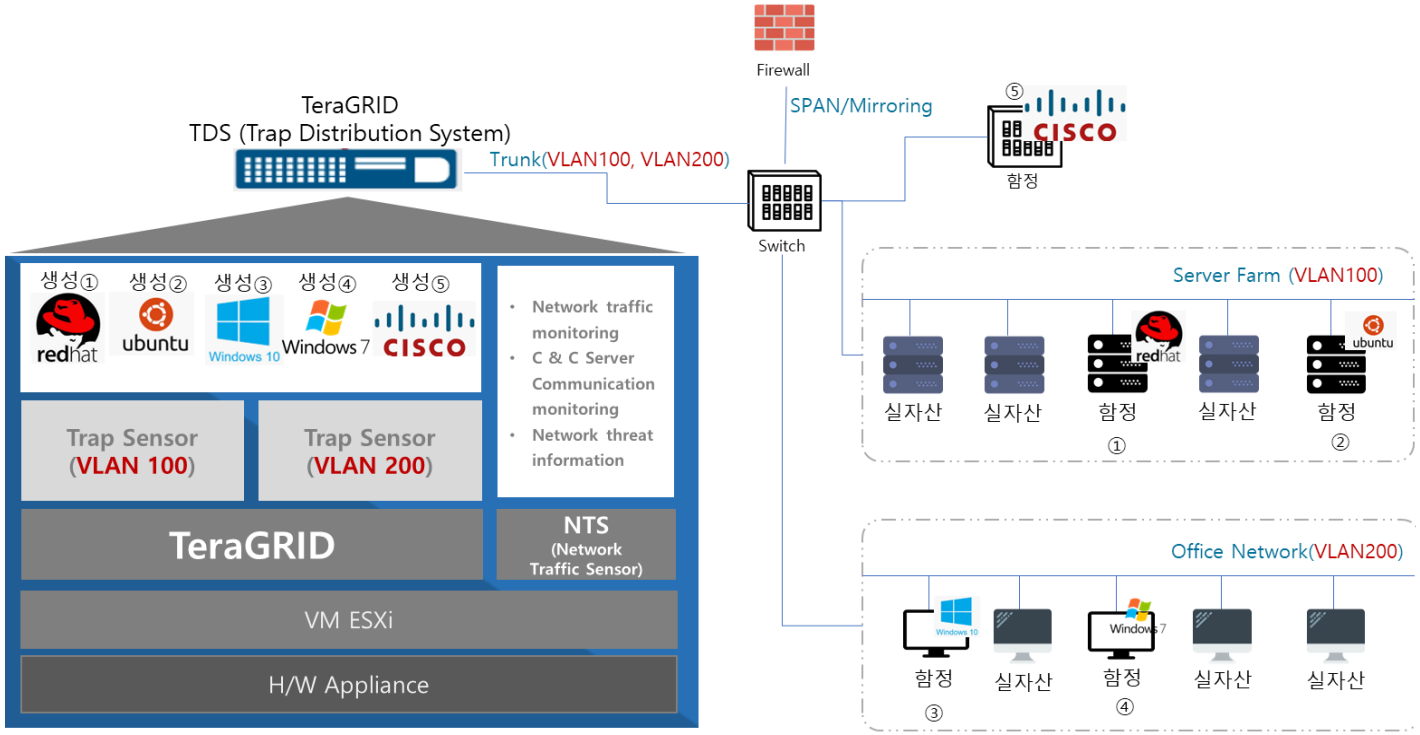
DX솔루션

- 데이터이쿠(Dataiku)
- 스노우플레이크(Snowflake)
- 스플렁크(Splunk)
- 데이타팍(dataPARC)
- 넥스트이피씨(NextEPC)
- 소프팅(Softing)

* 파란색은 쿤텍 자체 개발 솔루션

01 인프라보안 - TeraGRID - 사이버 기만 기반 APT 탐지

진화한 허니팟을 기반으로 장치의 유형에 관계 없이 대규모 네트워크를 신속하게 Shadow Network로 구축하여
즉각적인 사이버 공격 대응이 가능한 **사이버 기반 기술** 솔루션입니다.



정교한 미끼와 함정

공격자 유인을 위한 문서, 인증 정보, 전자메일, 프로토콜 기반의 다양하고 정교한 미끼 기능 및 에뮬레이트 함정, FullOS 함정 기능 지원

다양한 장치 Emulation

Server, Workstation, IOT Devices, Network Devices 등

악성행위 모니터링

공격 IP, Port 및 공격 당한 Trap 정보 제공

MITRE ATT&CK 기반 공격 정보 제공

악성파일 다운로드 및 정적분석 정보 제공

시계열 기반 공격 분석 정보 제공

3rd Party 보안 솔루션 연동 및 보안 정책 적용

대규모 트랩 생성 및 배포

02 인프라보안 - ORCA - 통합 클라우드 보안 솔루션 (CNAPP with CSPM, CWPP)

COONTEC

통합 데이터 모델(Unified Data Model)을 지향하는 **Agentless 기반**의 클라우드 보안 플랫폼입니다.

기대 효과

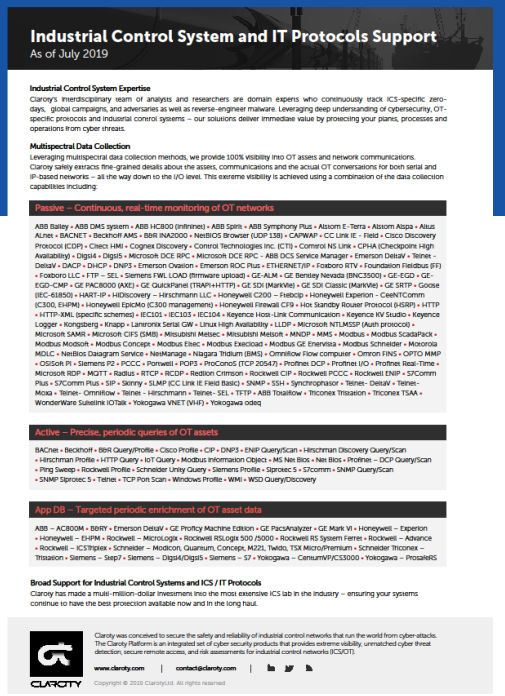
- 자산 인벤토리 관리
- 우선 순위에 따른 알림/경고
- 아이덴티티/액세스 위험 관리
- 클라우드 컴플라이언스 준수
- 문제 해결을 위한 통합 오케스트레이션
- 클라우드 특화 탐지 및 대응
- DevOpsSec을 위한 CI/CD 컨트롤

03 인프라보안 - Claroty - OT 보안 위협 통합 관제 모니터링

OT/ICS를 구성하는 다양한 유형의 자산, 통신 프로세스, 네트워크 세션에 대한 **가시성 확보**를 기반으로 보안 위협을 탐지 및 분석하며 지속적으로 관리하는 모니터링 솔루션입니다.

사이버 킬체인 기반 위협 분석 엔진

- 비정상 이상징후 분석
- ICS/OT 사용자 정의 분석
- 시그니처 기반 분석
- 운영적인 행동 분석
- 보안적인 행동 분석


Industrial Control System and IT Protocols Support
As of July 2019

Industrial Control System Expertise

Claroty's interdisciplinary team of analysts and researchers are domain experts who continuously track ICS-specific zero-days, global campaigns, and adversaries as well as reverse-engineer malware. Leveraging deep understanding of cybersecurity, OT-specific protocols and industrial control systems – our solutions deliver immediate value by protecting your plants, processes and operations from cyber threats.

Multispectral Data Collection

Leveraging multispectral data collection methods, we provide 100% visibility into OT assets and network communications. Claroty safely extracts fine-grained details about the assets, communications and the actual OT conversations for both serial and IP-based networks – all the way down to the I/O level. This extreme visibility is achieved using a combination of the data collection capabilities including:

Passive – Continuous, real-time monitoring of OT networks

ABB Bailey • ABB DMS system • ABB HC800 (mininet) • ABB Spirit • ABB Symphony Plus • Alstom E-Terra • Alstom Atspa • Alsus ALnet • BACNET • Beckhoff AMS • BMR INA2000 • NetBIOS Browser (UDP 138) • CAPWAP • CC Link IE - Field • Cisco Discovery Protocol (CDP) • Cisco HMI • Cognex Discovery • Comrol Technologies Inc. (CTI) • Comrol NS Link • CPHA (Checkpoint High Availability) • Digi44 • Digi45 • Microsoft DCE RPC • Microsoft DCE RPC - ABB DCS Service Manager • Emerson DeltaV • Telnet - DeltaV • DMCP • DHCP • DNP3 • Emerson Ovation • Emerson ROC Plus • ETHERNET/IP • Foxboro RTV • Foundation Fieldbus (FF) • Foxboro LLC • FTP – SEL • Siemens FWL LOAD (firmware upload) • GE-ALM • GE Bentley Nevada (BNC3500) • GE-EGD • GE-EGD-CMP • GE PAC8000 (AKE) • GE QuickPanel (TRAP)+HTTP) • GE SDI (MarkVIe) • GE SDI Classic (MarkVIe) • GE SRTP • Goose (IEC-61850) • HART-IP • HIDiscovery – Hirschmann LLC • Honeywell C200 – Fieldcp • Honeywell Experion - CeeNTComm (C300, EHPM) • Honeywell EpicMo (C300 management) • Honeywell Firewall CF9 • Hot Standby Router Protocol (HSRP) • HTTP • HTTP-XML (specific schemes) • IEC101 • IEC103 • IEC104 • Keyence Host-Link Communication • Keyence KV Studio • Keyence Logger • Kongsberg • Knapp • Lansonix Serial GW • Linux High Availability • LLDP • Microsoft NTLMSSP (Auth protocol) • Microsoft SAMR • Microsoft CIFS (SMB) • Mitsubishi Melsec • Mitsubishi Melsoft • MNDP • MMS • Modbus • Modbus ScadaPack • Modbus Modsoft • Modbus Concept • Modbus Etec • Modbus Execload • Modbus GE Enervisa • Modbus Schneider • Mocorola MOLC • NetBios Daagram Service • NexManage • Niagara Tridium (BMS) • Omnilow Flow compuser • Omron FINS • OPTO MMP • OSISoft PI • Siemens PZ • PCCC • Pomwell • POP3 • ProCon/OS (TCP 20547) • Profinet DCP • Profinet I/O • Profinet Real-Time • Microsoft RDP • MQTT • Radius • RTCP • RCDP • Redlion Crimson • Rockwell CIP • Rockwell PCCC • Rockwell ENIP • S7Comm Plus • S7Comm Plus • SIP • Skinny • SLMP (CC Link IE Field Basic) • SNMP • SSH • Synchrophasor • Telnet- DeltaV • Telnet- Mosa • Telnet - Omnilow • Telnet - Hirschmann • Telnet - SEL • TFTP • ABB TotalFlow • Triconex Tricsation • Triconex TSAA • WonderWare Suitelink IOTalk • Yokogawa VNET (VHF) • Yokogawa odeq

Active – Precise, periodic queries of OT assets

BACnet • Beckhoff • BMR Query/Profile • Cisco Profile • CIP • DNP3 • ENIP Query/Scan • Hirschman Discovery Query/Scan • Hirschman Profile • HTTP Query • IOT Query • Modbus Information Object • MS Net Bios • Net Bios • Profinet – DCP Query/Scan • Ping Sweep • Rockwell Profile • Schneider Unity Query • Siemens Profile • Siprotec 5 • S7comm • SNMP Query/Scan • SNMP Siprotec 5 • Telnet • TCP Port Scan • Windows Profile • WMI • WSD Query/Discovery

App DB – Targeted periodic enrichment of OT asset data

ABB – AC800M • BMR • Emerson DeltaV • GE Proficy Machine Edition • GE PacsAnalyzer • GE Mark VI • Honeywell – Experion • Honeywell – EHPM • Rockwell – MicroLogix • Rockwell RSLogix 500 /5000 • Rockwell RS System Ferret • Rockwell – Advance • Rockwell – ICS Triplex • Schneider – Modicon, Quantum, Concept, M221, Twido, TSX Micro/Premium • Schneider Triconex – Tricsation • Siemens – Step7 • Siemens – Digsi4/Digsi5 • Siemens – S7 • Yokogawa – CentumVP/CS3000 • Yokogawa – ProsafeRS

Broad Support for Industrial Control Systems and ICS / IT Protocols

Claroty has made a multi-million-dollar investment into the most extensive ICS lab in the industry – ensuring your systems continue to have the best protection available now and in the long haul.

Claroty was conceived to secure the safety and reliability of industrial control networks that run the world from cyber-attacks. The Claroty Platform is an integrated set of cyber security products that provides extreme visibility, unmatched cyber threat detection, secure remote access, and risk assessments for industrial control networks (ICS/OT).

www.claroty.com | contact@claroty.com

CLAROTY

Copyright © 2019 Claroty Ltd. All rights reserved

04 인프라보안 - BeyondTrust - 계정 및 권한 제어 관리

COONTEC

특권 권한과 접속 세션, 패스워드 관리 기능 등을 제공하여
컴플라이언스 준수 및 제로트러스트 활성화에 기여하는 솔루션입니다.

**디지털 트랜스포메이션 시대,
중요 과제는 '보안'**

**다양한 보안과제를 해결할 수 있는
통합 솔루션 제공**

다양한 보안 과제

- 사내의 모든 특권 계정 확인
- 네트워크 상에서 수행중인 벤더의 작업 확인
- 반드시 필요하지 않은 관리자 계정의 제거
- 컴플라이언스 감사 통과
- 특권 관리의 ITSM 워크플로우와의 통합
- 네트워크 상의 모든 특권 자격 증명의 안전성
- 최소 특권 부여의 베스트 프랙티스 적용
- 특권 관리의 변경 관리 워크플로우와의 통합
- 컴플라이언스에 준하지 않거나 유해한 SW 차단

* 제로 트러스트란 보안 경계를 통과한 데이터와 트랜잭션을 신뢰하지 않고 시스템 내외부의 모든 데이터와 작업을 검증하는 것을 말한다.

The BeyondTrust Solution

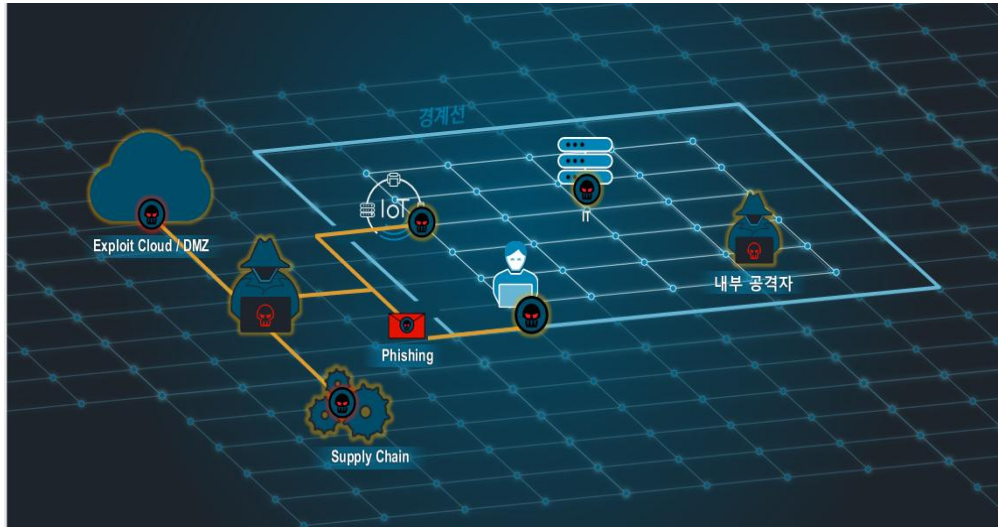
05 인프라보안 - DeceptionGrid - 사이버 기만 기반의 APT 탐지

COONTEC

진화한 허니팟인 **사이버 기만술을 기반으로** 빠르고 정확하게 공격자를 기만 및 유인하고
공격자 및 내부 악성 행위자를 **노이즈 없이 탐지**하는 APT 탐지 솔루션입니다.

실제 자산과 유사한 에뮬레이션 된 함정 기술로
공격자 유인을 위한 함정과 미끼 전략배포 탐지

MITRE ATT&CK Framework 기반 공격 식별 및
분류 탐지 및 모니터링에 최적화된 시스템



공격 행위 (Time Stamp)

15:25:34	Establish Connection:	from port 59669
15:25:34	Establish Connection:	from port 59671
15:25:37	Establish Connection:	from port 60054
15:25:37	Tree Connect:	\\192.168.56.20\IPC$
15:25:37	Exploit:	WannaCry Ransomware exploit detected
15:25:48	Disconnected	

공격 경로 (Visualization)

- **국방 무기체계 방어시스템 구축 활용**
- **주요 기관/기업 전산장비 서버 보안 체계 구축**

06 인프라보안 – SafeBreach – 실제 해킹 기술 기반의 네트워크 보안 검증

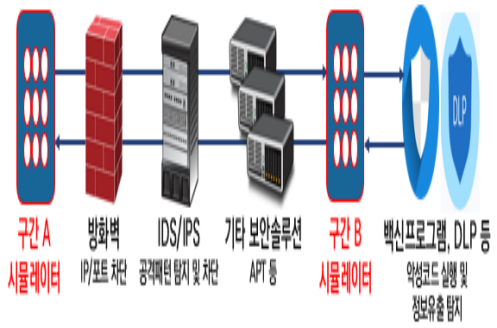
COONTEC

네트워크 전반에 **Cyber Kill Chain**과 **MITRE ATT&CK 관점을**
접목 및 응용하여 시뮬레이션 함으로써 궁극적으로 **공급망 보안을 강화**하는 솔루션 입니다.

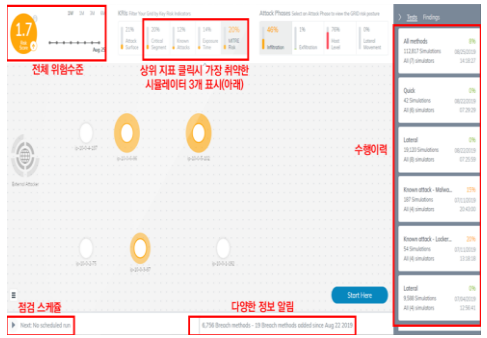
최신 공격 유형을 반영한 시뮬레이션 자동화 및
공격 유형과 추세를 파악하여 동향분석&Alert 리포팅 제공

전체 네트워크에 대해 실제 해킹 기술을 이용하여 지속적이고
포괄적인 보안 점검&검증과 IT 인프라에 영향 없는 시뮬레이션 가능

검증 방법

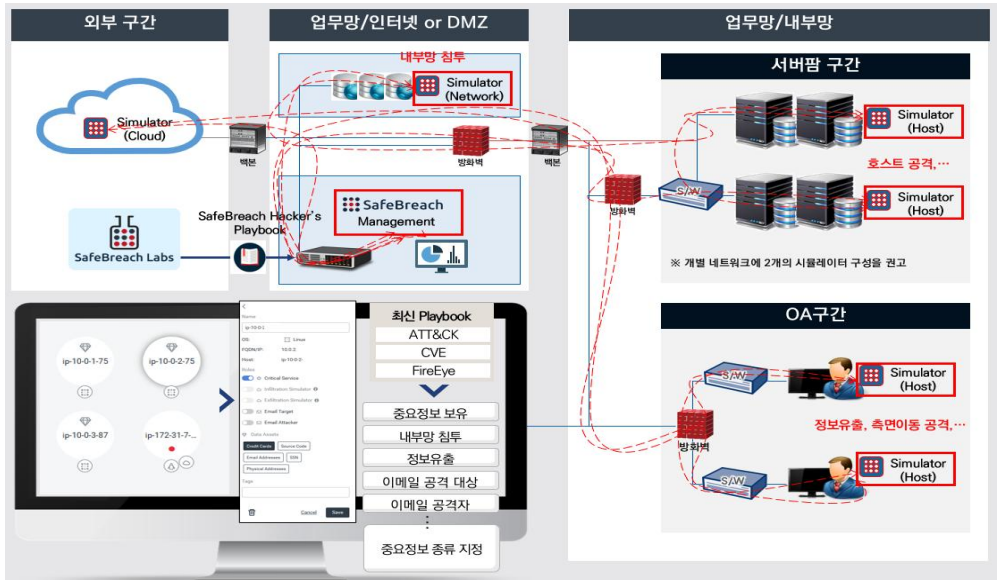


대쉬보드



- 실제 공격 대비 사전 차단 및 피해 규모 최소화
- 고객사의 대응 능력을 정확히 파악

SafeBreach Architecture



07 개발보안 - 이지스 - 공급망 취약점 점검 및 분석

COONTEC

오픈소스와 바이너리 취약점 분석 결과의 통합 관리를 위한 **SW 공급망 보안** 솔루션

취약점 분석
라이브러리 취약점 점검 및 위험도 제공

유연한 권한 관리
사용자별로 기능과 페이지 접근 제어 가능

통합관리

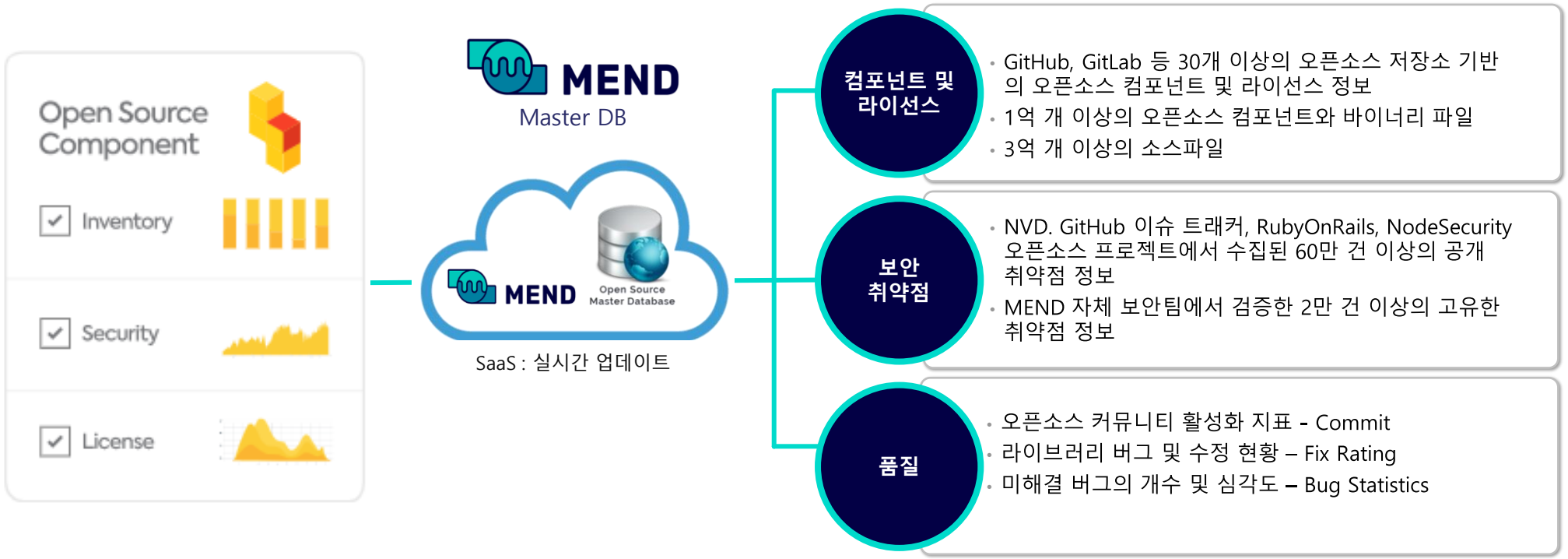
통계 및 시각화
취약점, 라이브러리, 라이선스 등 점검 결과를 그래프로 제공

보안 강화
2단계 채널 인증 기반 로그인, 개인정보 암호화 관리

08 개발보안 - MEND - 오픈소스 통합 관리 플랫폼

COONTEC

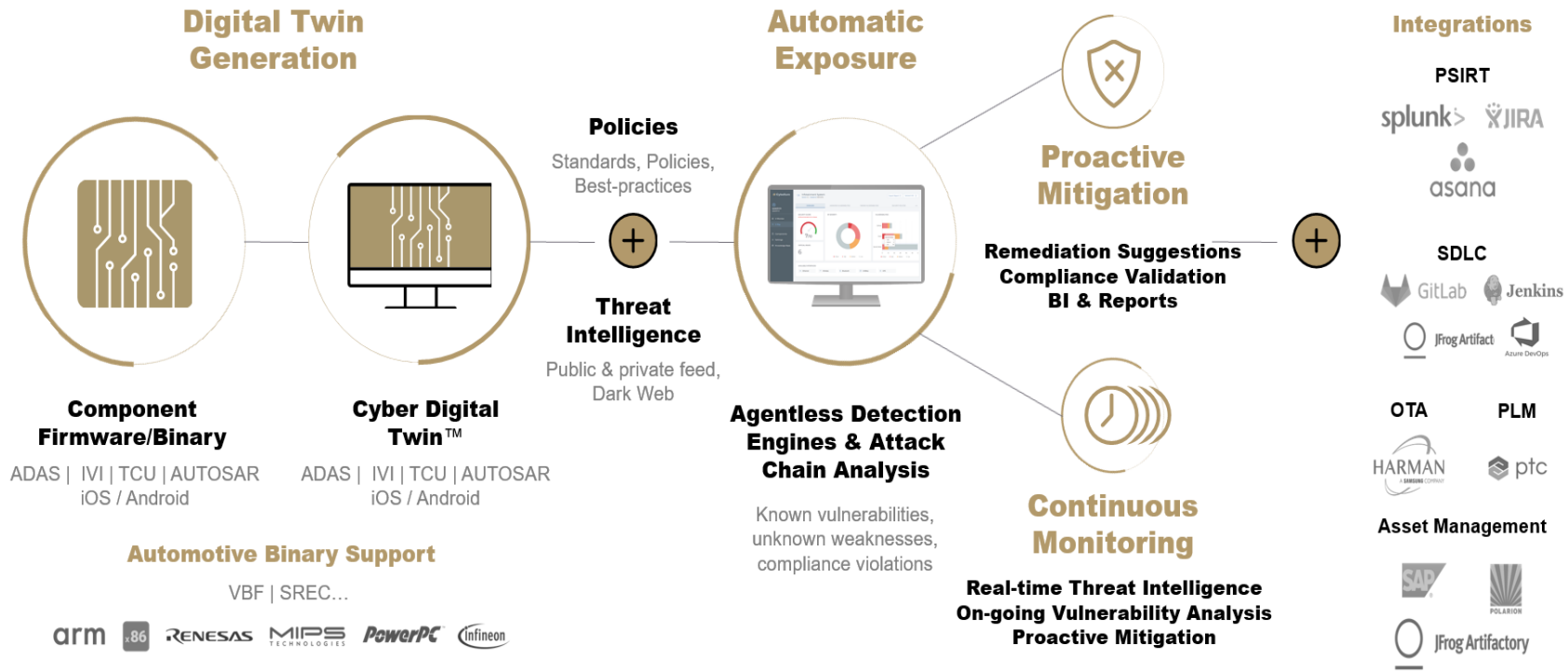
디지털 시그니처 기반의 오픈소스 통합 관리 솔루션으로 SaaS로 구축된 실시간 DB를 통해
빠르고 정확하게 오픈소스 보안 취약점을 점검합니다.



09 개발보안 - Cybellum - 멀티 플랫폼 바이너리 분석 플랫폼

COONTEC

별도의 에이전트 설치 없이 웹 UI를 통해 바이너리를 분석하고 실시간 모니터링할 수 있어
빠르고 정확한 취약점 탐지 및 대응을 지원하는 솔루션입니다.



10 개발보안 - Supplier Check

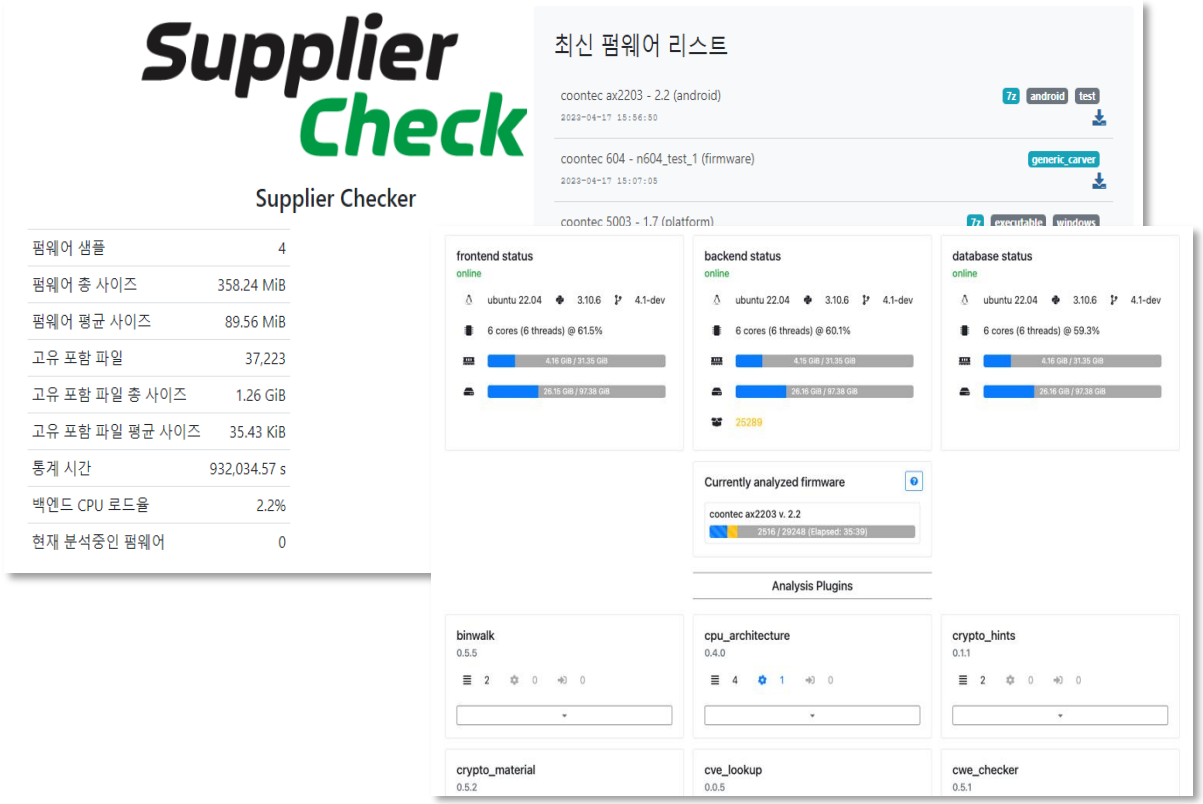
신속하고 편리하게 바이너리를 분석하여 취약점을 검출하고 지속적으로 관리 할 수 있는 바이너리 분석 / 진단 통합 관리 도구

바이너리 분석 및 관리의 편의성

- Package 정보, CVE, CWE, binwalk, IP, URI 정보 분석 및 획득
- Device class, Vendor 별 통계를 통해 분석에 필요한 정보의 시각화
- 분석된 바이너리의 새버전과 이전 버전의 결과를 비교 / 관리

다양한 유형의 플랫폼 지원

- 프로그램 언어 분석 유형
  - C++ / Java / Python / Xml / html / javascript / Perl / ruby
- 파일 포맷 분석 유형
  - rar / adf / Alzip / bzip2 / cab / debian-package / dms / iso9660-image / lrzip / lzh / lzip / zlib 등
- 운영체제 분석 유형
  - Linux / Android / QNX / FreeRTOS / Proprietary RTOS / RIOT / Fuchsia OS / OSEK OS / VxWorks 등



11 임베디드보안 - Penzzer

COONTEC

penzzer

임베디드 및 IoT 펜테스트/퍼징 통합 솔루션

Penzzer는 펜테스트 동적 분석(DAST)과 퍼징을 결합한 통합 솔루션으로, 하나의 도구로 알려진 취약점/알려지지 않은 취약점 등을 탐지하여 다양한 보안 위협으로부터 자산을 지킬 수 있도록 하며, 각종 규제에 대한 요구사항 준수를 지원합니다.
또한 즉시 사용할 수 있는 하드웨어 및 소프트웨어 키트로 제공되어 퍼징, 침투테스트 및 동적 분석(DAST)을 통해 주요 취약점을 신속하게 해결하고 안전한 제품의 생산을 지원합니다.

All-in-one

자동차, 의료기기, IoT 및 임베디드 등 자동화된 보안테스팅(퍼징, 펜테스트)을 하나의 솔루션에서 모두 지원함으로서 알려진 취약점/알려지지 않은 취약점 모두 탐지가 가능합니다.

Compliance

ISO/SAE 21434, FDA 및 각종 ISO 표준과 보안 규정을 지원하며, IoT 지원 공급망 전체에 대한 보안 관리를 제공합니다.

Plug-and-play

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

Easy-to-use

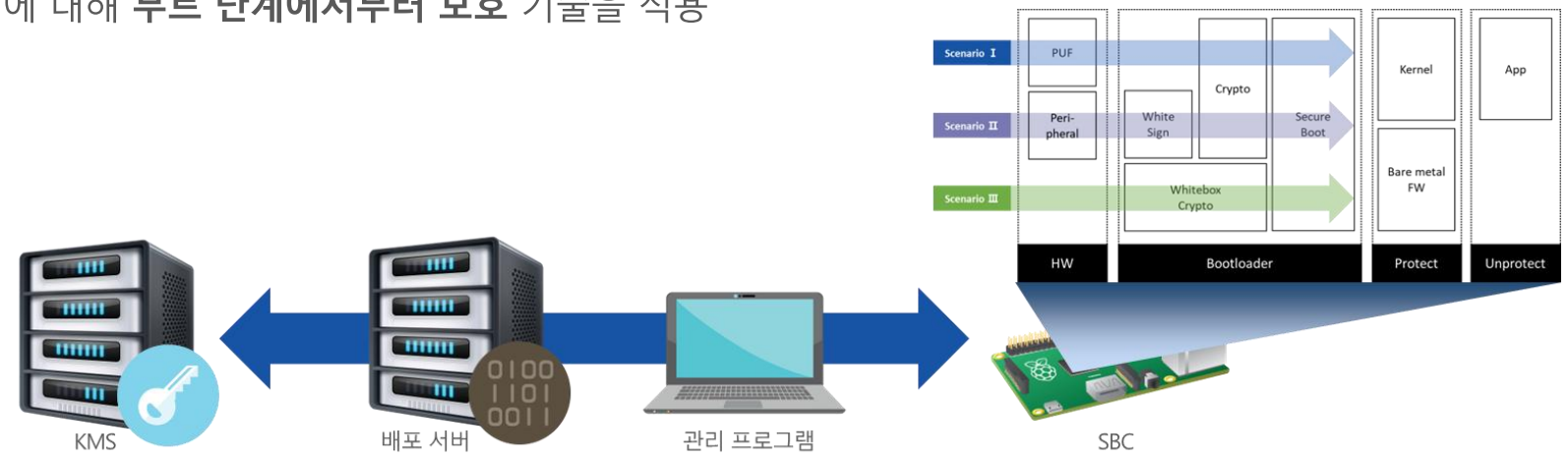
쉽고 명료한 UI를 통해 사용자의 편의성을 극대화하여 퍼징과 펜테스트를 쉽고 빠르게 테스트할 수 있습니다.

12 임베디드보안 - Secure ALPS - 펌웨어 및 키 보안 관리 (1/2)

COONTEC

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

- 임베디드 장비 내에 설치되어 있는 펌웨어의 **무결성**과 **기밀성**을 보호 하여 **변조 방지 및 핵심 기술을 보호**
- 제조 단계에서의 펌웨어 설치 뿐만 아니라 업데이트 시에도 **상호인증**과 **암호화**를 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



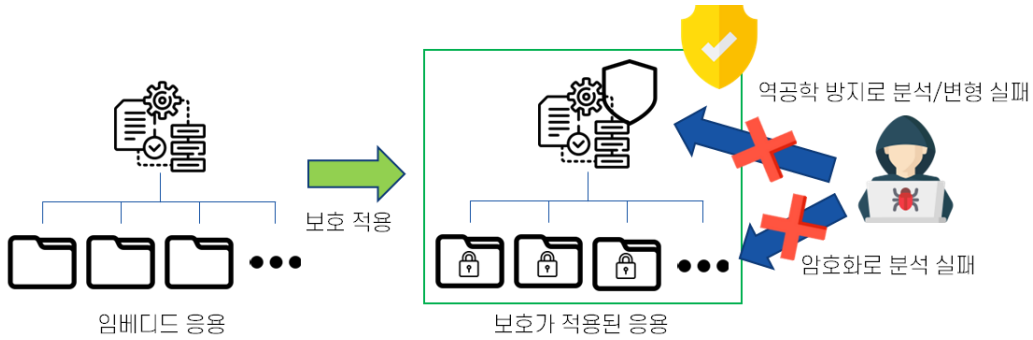
13 임베디드보안 - Secure ALPS - 펌웨어 및 키 보안 관리 (2/2)

COONTEC

ALPS-Shield
임베디드 환경에서의 응용 프로그램 자체 보호 (RASP)

RASP (Runtime Application Self Protection)

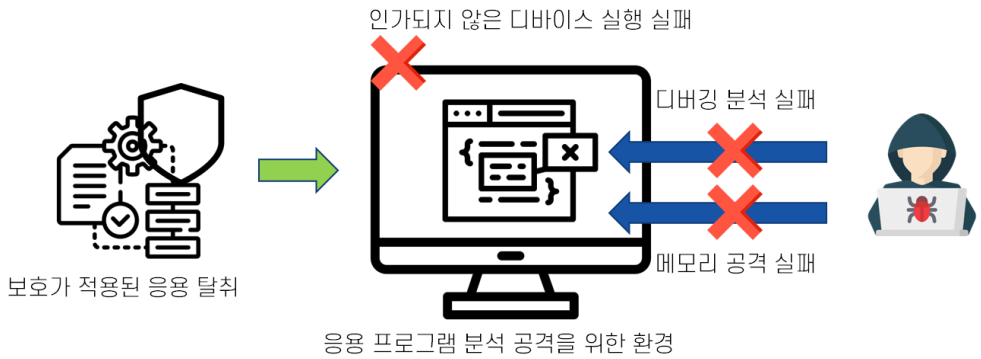
응용이 자체적으로 자신을 보호하는 기법



코드 난독화, 바이너리 암호화, 바이너리 무결성, 리소스 암호화

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



디바이스 바인딩, 안티 디버깅, 바이너리 하드닝

14 임베디드보안 - Secure-IC

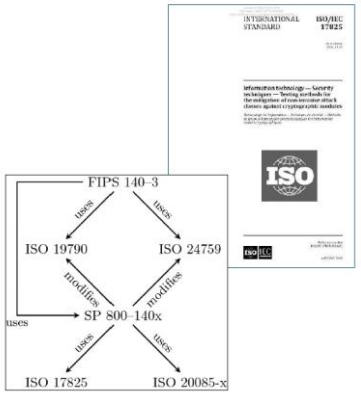
COONTEC

**다양한 부채널&오류주입 분석 기법, Secure-IC의 특화된 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 컴플라이언스를 지원합니다.**

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

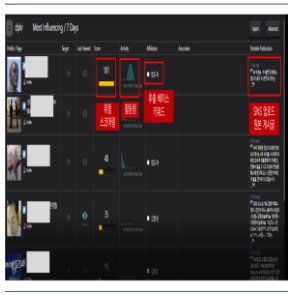
15 공격표면보안 - Cyber Hawk Eye – OSINT 위협 정보 수집 분석 플랫폼

COONTEC

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

Surface. DeepWeb, DarkWeb
정보 수집의 최적화된 솔루션 제공

사이버 세상 안에 존재하는 범죄 활동, 군사정보유출,
금융범죄, 개인정보 유출에 대한 증거수집 및 분석 기술



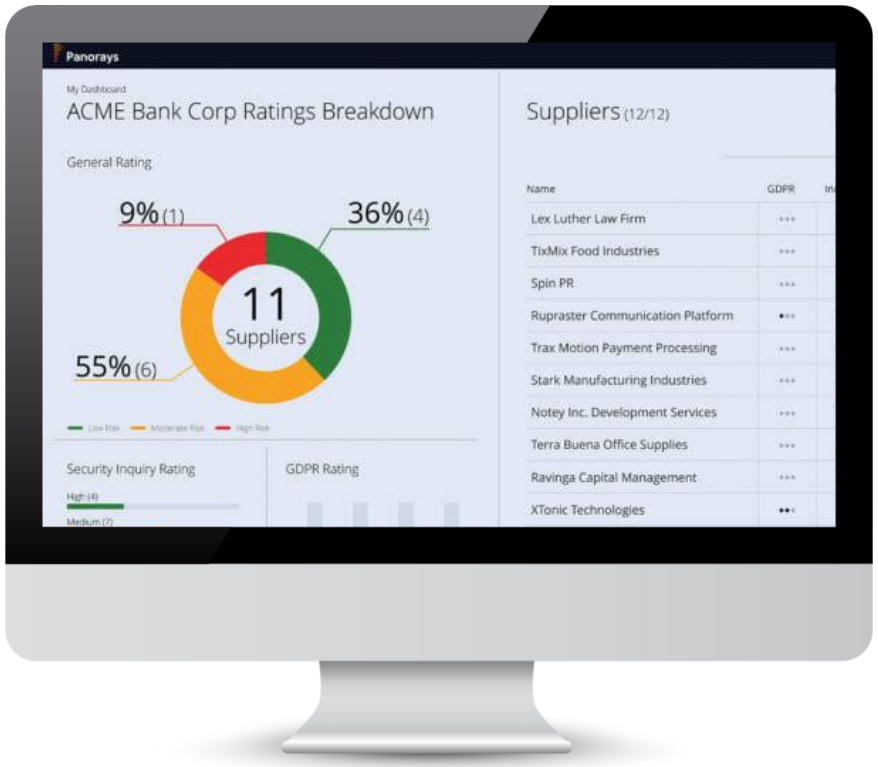
- 아바타로 안전한 데이터 수집
- 모듈식 고객 맞춤형 옵션제공
- SNS연계분석 사이버 범죄수집

16 공격표면보안 - Panorays - 공급업체 위험관리 플랫폼

COONTEC

파트너, 협력사 등 공급업체에 대한 360도 보안 평가를 토대로 지속적인 공격 표면 모니터링을 실시하는
유일한 공급업체 위험관리 자동화 솔루션입니다.

- **보안 질문지 자동화 및 가속화 (Inside-Out)**
  - ✓ 더 이상 수동 평가 및 관리 불필요
  - ✓ 규정 준수 및 내부 정책 검증
  - ✓ 공급업체와 협력하고 상호 작용하며 정책 변경 사항에 대한 알림 설정
- **사이버 격차 모니터링 및 개선 (Outside-In)**
  - ✓ 공급업체의 외부(public) 디지털 풋프린트에 대한 지속적인 스캔
  - ✓ 사이버 태세에 대한 실시간 보안 점수 제공
  - ✓ 다양한 공급업체의 위험 감소



Extreme Engineering

Our Solutions

Part 1. 보안

Part 2. 임베디드SW

Part 3. DX솔루션

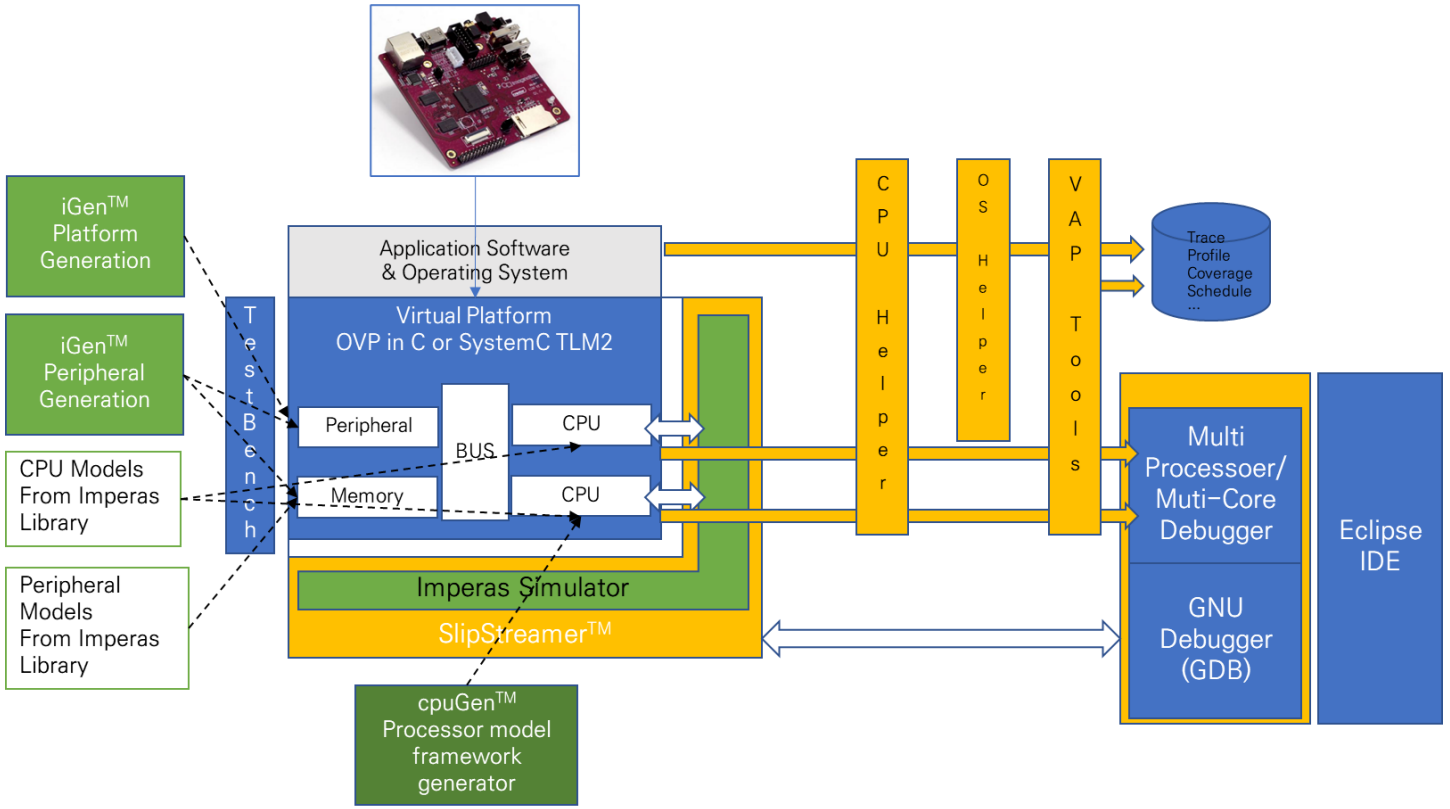
COrporation ON by TEChnology | 쿤텍

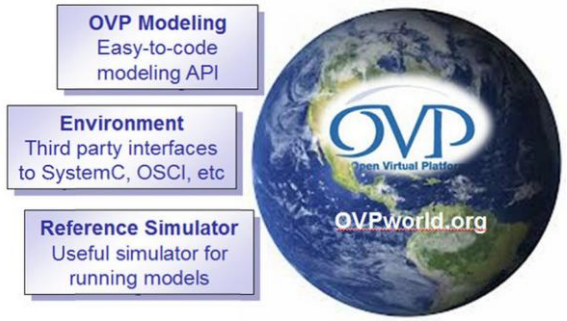
02

01 임베디드SW – Imperas - 임베디드 가상화 플랫폼

COONTEC

하드웨어 의존성을 배제하여 물리적인 **제한 없이** 소프트웨어 테스트를 수행할 수 있어
테스팅 품질 향상을 지원하는 플랫폼입니다.





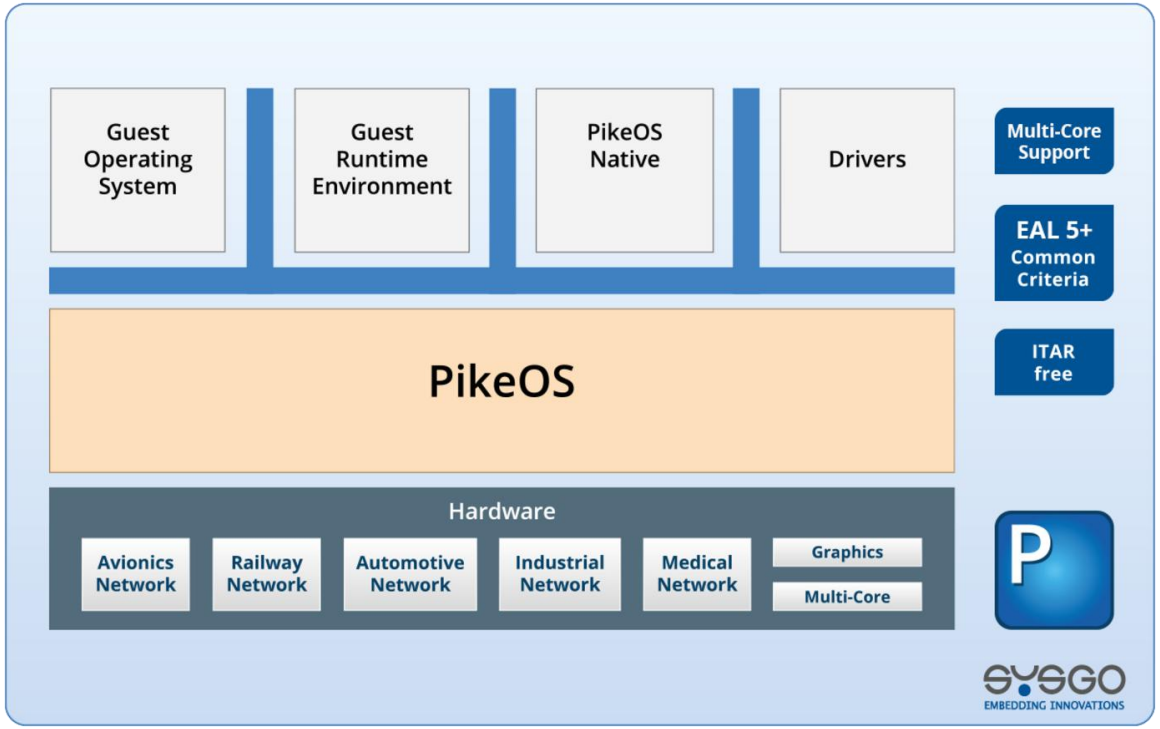
02 임베디드SW - SYSGO - RTOS 및 인증 솔루션

COONTEC

고신뢰성 임베디드 시스템 개발을 위한 **Real-Time OS 및 인증** 솔루션으로
높은 안정성과 보안성과 임베디드 시스템에 최적화된 **Linux** 솔루션을 제공합니다.

항공우주, 철도, 자동차, 방위 산업 등 고도의 안전성 및 보안이 요구되는 산업분야에 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.

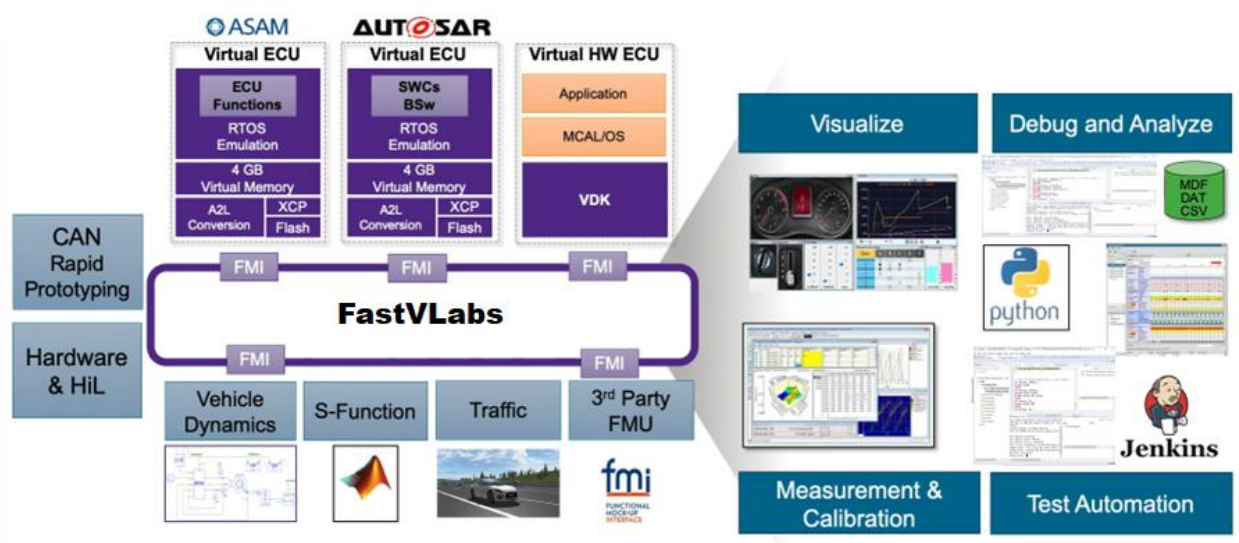


03 임베디드SW - FastVLabs - 차량 SW 개발 검증

고신뢰성 L4 vECU 기반의 시뮬레이션 엔진을 보유한 **차량용 소프트웨어 개발 검증 솔루션으로**
유연한 클라우드 환경에서의 운영을 통해 효율적인 테스트가 가능합니다.

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



Extreme Engineering

Our Solutions

Part 1. 보안

Part 2. 임베디드SW

Part 3. DX솔루션

COrporation ON by TEChnology | 쿤텍

02

01 AI/BigData - Dataiku - End to End 데이터 사이언스 플랫폼

COONTEC

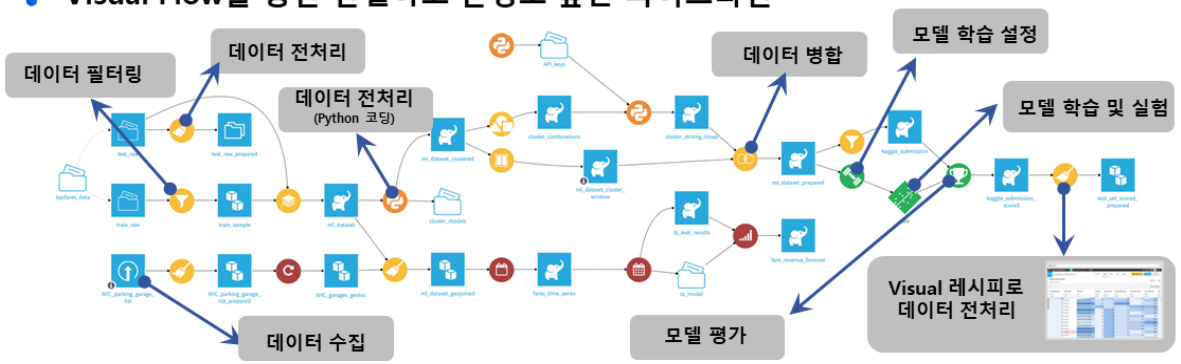
데이터의 수집부터 전처리, 분석 및 시각화, ML/DL 모델 개발 및 배포의 모든 과정을 지원하는,
단일 End to End 데이터 사이언스 솔루션입니다.

데이터 연결 | 전처리 | 분석 | 시각화 | ML 모델링 | 모델 배포

snowflake, databricks, hadoop, Google Cloud, amazon REDSHIFT, ORACLE DATABASE, cassandra, mongoDB, memSQL, PostgreSQL, MySQL, AVRO, salesforce, NETEZZA, Microsoft SQL Server, IBM DB2, Pivotal Greenplum, VERTICA, Exasol, SAP S/4 HANA

No Code부터 Full Code까지 누구나 사용 가능한 플랫폼

Visual Flow를 통한 간결하고 완성도 높은 파이프라인



클라우드 및 On-Premise 환경을 모두 지원

aws, Microsoft Azure, Google Cloud Platform, On-premise

실시간 API

API

자동화 배포

Alation

시각화 연동

+ableau, Power BI, CARTODB, Qlik, esri

02 AI/BigData - Snowflake - 클라우드 데이터 플랫폼

Snowflake는 데이터의 유형 또는 규모에 상관 없이 다양한 워크로드에 걸쳐 비즈니스를 연결하고
데이터 협업을 가능하게 하도록 설계된, **100% Cloud Stack 기반으로 개발된 클라우드를 위한 단일 데이터 플랫폼**입니다.

03 AI/BigData – Splunk – 에지, 분산 환경 데이터 수집 및 전송 솔루션

데이터 접근에 대한 장벽과 데이터의 격리를 제거하여 에지 데이터 수집과 조사를 간소화하며,
다른 공급업체의 플랫폼으로부터 데이터를 집계할 수 있는 **완전한 산업용 IoT 데이터 통합 솔루션**입니다.

빛
High sensitivity light sensor
항온
(±0.2°C from 0°C to 90°C, IP67 rated membrane
항습
(±2% from 0°C to 90°C)
소리
Microphone - Vesper VM1000 Spec Sheet
진동
3-Axis Accelerometer - Bosch BMA456
자이로 스코프 (가속화)
6-Axis Gyro & Accelerometer - TDK ICM20600
옵션 : 압력, VOC w/ 가스 분석
(300...1100 hPa) ± 0.12 hPa for Pressure,
< 1s response with IAQ Score Output for Gas

유선센서


무선센서

GPS
무선 공용 / 사설
4G/5G 네트워크 / 서비스
5G
IoT Edge Hub
내장 5G 모델 (eSIM)
Splunk 데이터
Kepware / Advantech
TCP/IP 지원 설비
IoT / 센서 케이트웨이 서비스
지원 가능 무선 규격
Bluetooth Wi Fi LoRa
MQTT OPC UA
유선


산업용 카메라

산업용 마이크

PLCs / RTUs
Programmable Logic Controls, Remote Terminal Units

OPC 서버
Industrial Control system statistical acquisition

SCADAs / HMIs
ICS control / management applications

Historians
Manufacturing statistical database

SPCs
Statistical Process Control applications

04 Private 5G - Next 5G Core

COONTEC

5G 특화망 인프라 구축에 필요한 모든 솔루션, 운영, 교육, 서비스, 개발을 All In One & Service로 제공합니다.

- 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

5G Core 기본기능

- 3GPP Release 17 (최신)
- AMF/UPF/SMF/NRF/NSSF/AUSF/UDM/UDR/PCF/SCP/BSF
- Hand-over 및 QoS 프로비저닝을 포함한 모든 5G 및 LTE 기본 기능 지원
- 싱글 5G Core 서버당 최대 30,000개의 UE와 최대 128개의 eNodeB 지원
- 많은 상용 gNodeB 공급 업체와의 상호 운용성 테스트를 통해 검증
- 5G SA와 NSA 모두 지원

특장점

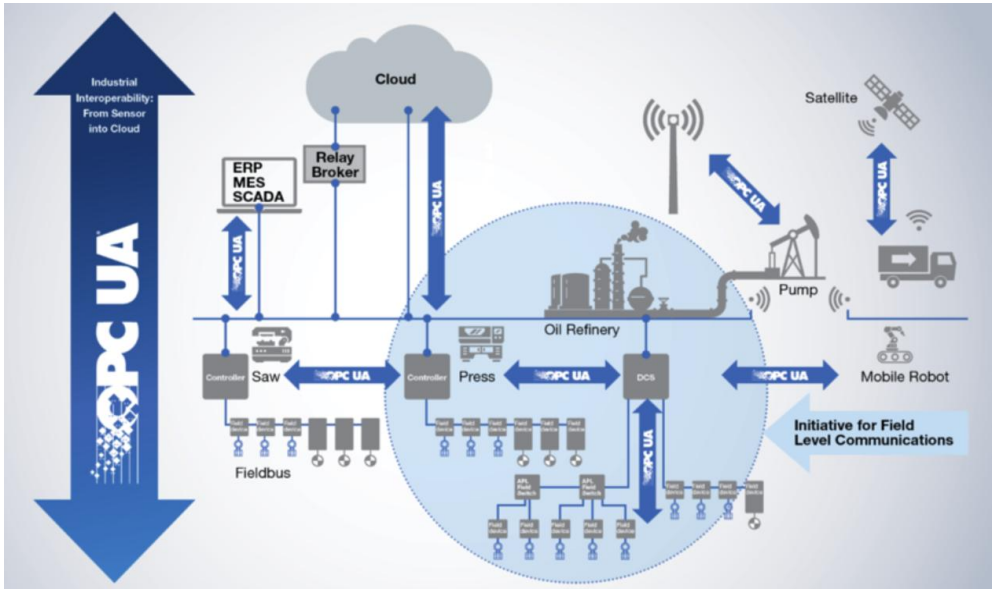
- 데이터 운영에 적합한 5G Core NF 구성 및 유연한 Bandwidth 커스터마이징
- 높은 이식성, HW 종속성 없음, 외부라이브러리 종속성 없음
- 컨테이너화, 도커화 된 형태 뿐만 아니라 가상 시스템에서도 작동
- 클라우드 뿐만 아니라 사내 COTS 서버에서도 배포 가능
- 멀티인스턴스 구축으로 확장 가능

05 산업제어 - OPC(Softing)

COONTEC

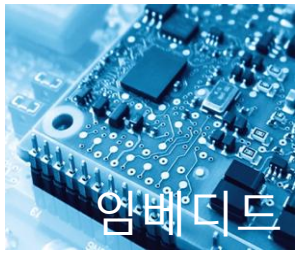
IEC 62541 산업 표준 프로토콜인 OPC UA 서버 및 클라이언트 개발 도구 공급을 통하여
산업용 프로토콜의 변조와 해킹 위협으로부터 **안전하게 데이터 전송을 보장**하는 솔루션입니다.

센서,PLC,SCADA등 다양한 제조설비에 적용 및 OT보안에 최적화된 산업표준 프로토콜-OPC UA



COONTEC

이기종 및 다양한 형태의 산업용 데이터를 안전하게 전송할 수 있는 OPC UA 개발솔루션 제공



CERTIFIED
FOR COMPLIANCE
OPC FOUNDATION

- 산업용 프로토콜 표준화
- OT/ICS 프로토콜 보안
- IEC62541 & OPC Certification

Extreme Engineering

Our Service

COORPORATION ON by TECHNOLOGY | 쿤텍

03

01 제공 서비스 1. 솔루션 구축

COONTEC

심층적인 요구사항 분석을 토대로
완성도 높은 **보안 솔루션 운영 환경 구축 지원**

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

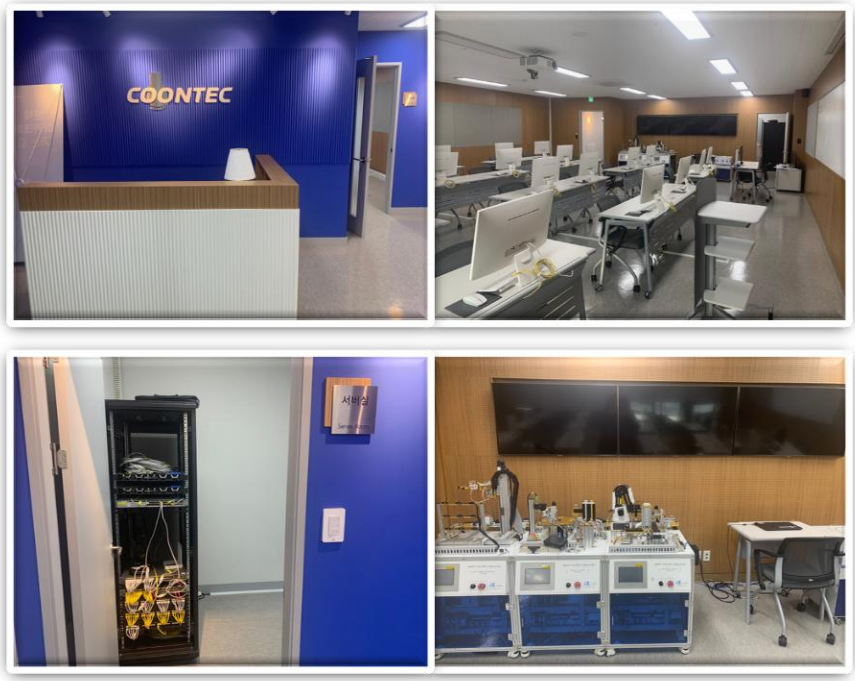
주요 구축 분야

국방, 공공, 금융, 제조, 민간 분야 등

02 제공 서비스 2. 교육/컨설팅

쿤텍은 **전문 장비를 갖춘 아카데미를 활용한 실습(Hands-on) 기반 교육**과 **산업분야별 요구사항에 특화된 컨설팅**을 통해 실제 산업분야의 보안 관리 역량 강화를 지원합니다.

교육	▪ 임베디드 가상화 시스템 교육 ▪ 오픈소스 보안 취약점 교육 ▪ OT/ICS 보안 교육 ▪ OSINT 교육 ▪ AI/Data 교육
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



쿤텍 아카데미

COrporation ON by TEChnology

CONTACT US

COONTEC

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

경기도 성남시 수정구 창업로 54, 가동 609호 | 031-751-9088 | www.coontec.com

제품문의 marketing@coontec.com
제휴문의 sales@coontec.com
채용문의 hr@coontec.com

COrporation ON by TEChnology

THANK YOU