'간편하지만, 탄탄하게'

NAONWORKS
an AhnLab Company

나온웍스 가 제시하는
OT 사이버보안 프레임워크 및 케이스

NAONWORKS
an AhnLab Company

윤 용 관
마케팅 전략기획실 / 실장

M 010-7212-3040 **T** 02-2025-1630
E mac.yoon@naonworks.com
본사 서울시 구로구 디지털로 271, 711호
판교 경기도 성남시 분당구 판교역로 240, A-301호

목 차

1. 간편하지만, 탄탄하게?

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

NAONWORKS
an AhnLab Company

보안 플랫폼

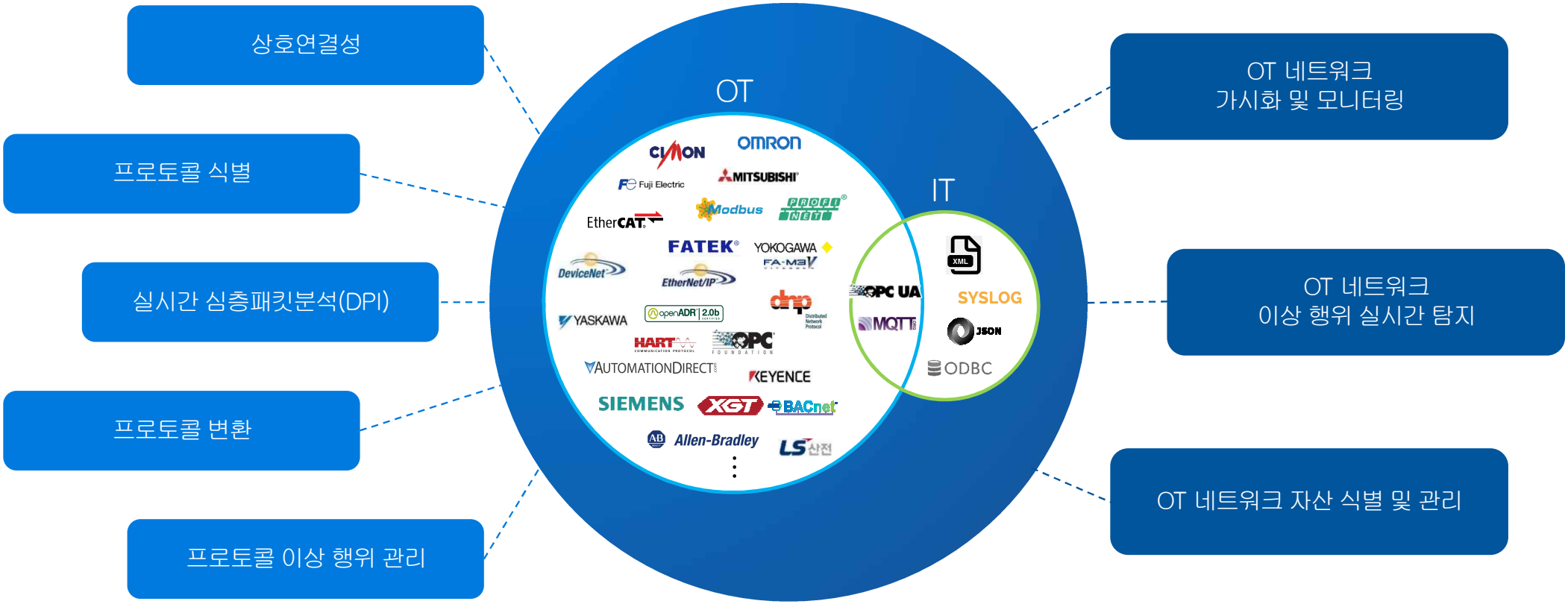
OT 프로토콜 분석 기술

개방형 아키텍처 플랫폼

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

1. 간편하지만, 탄탄하게?

나온웍스는 다양한 산업용 프로토콜에 대한 식별 및 분석 기술을 기반으로 OT 전용 솔루션을 개발·공급하고 있습니다.



NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

1. 간편하지만, 탄탄하게?

How much will you pay?

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

1. 간편하지만, 탄탄하게?

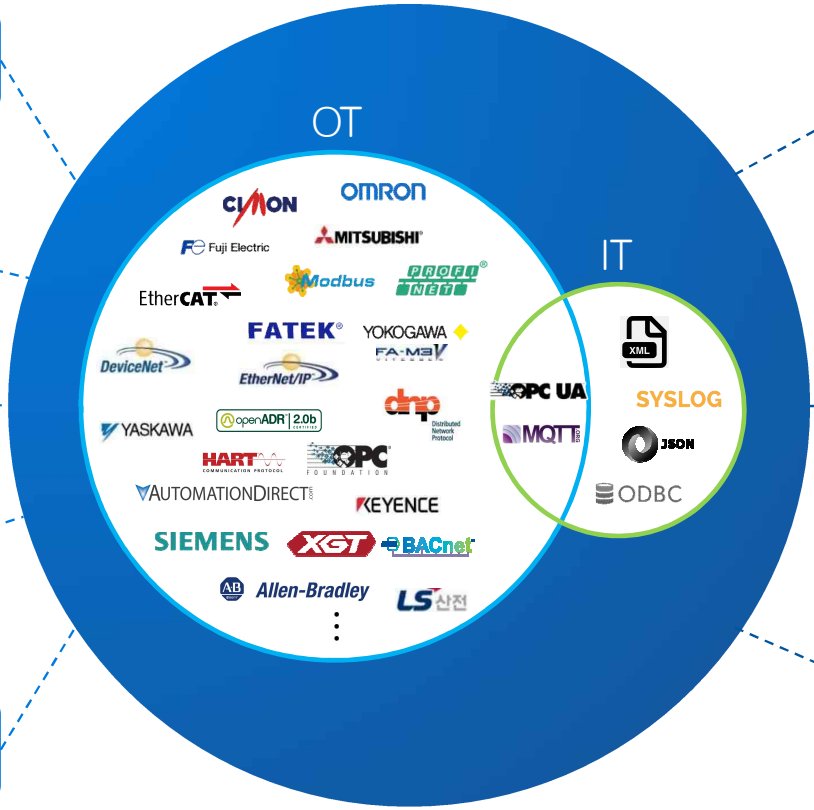
'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

2. OT, What's different?

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

1. 상호연결성
2. 프로토콜 식별
3. 실시간 심층패킷분석(DPI)
4. 프로토콜 변환
5. 프로토콜 이상 행위 관리



OT 네트워크
가시화 및 모니터링

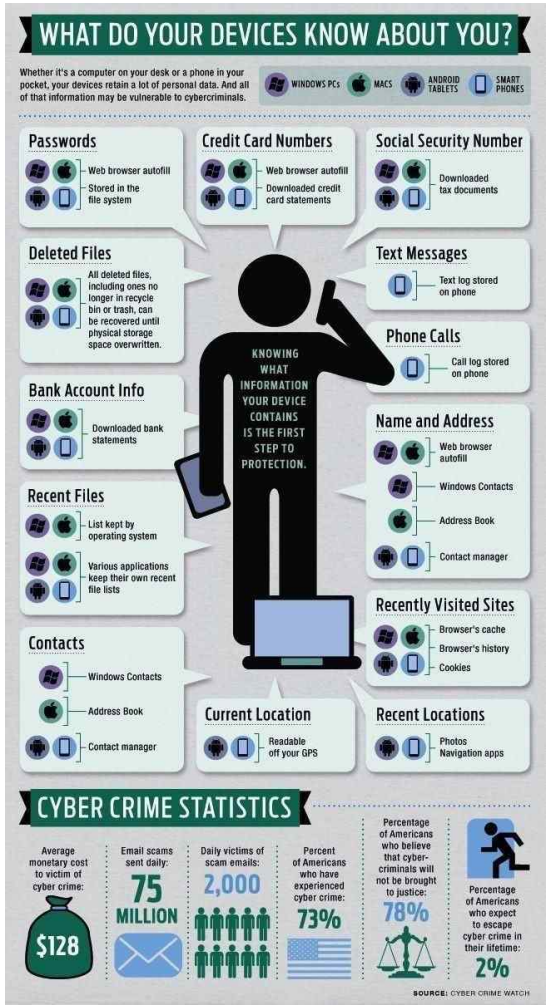
OT 네트워크
이상 행위 실시간 탐지

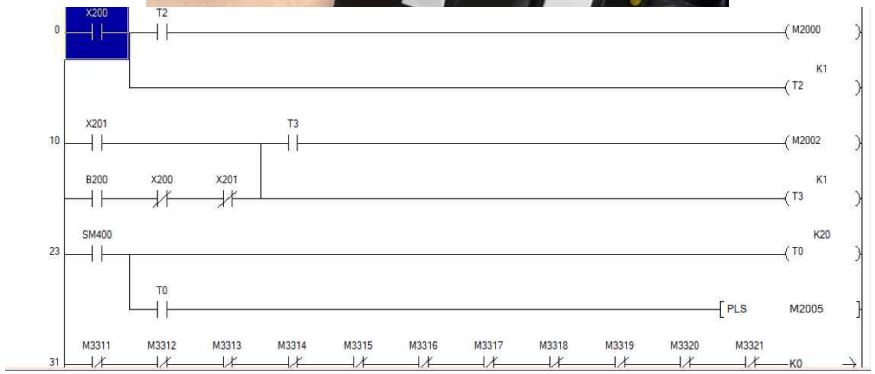
OT 네트워크 자산 식별 및 관리

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

2. OT, What's different?

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스





NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

2. OT, What's different?

#1

2021년 가장 많은 공격을 받은 산업

제조업(23%)

90.6%

22년 상반기 악성코드 경향

정보 수집 + 백도어 설치 + 추가 공격의

Infostealer Backdoor Downloader

연쇄적인 단계로 악성코드 고도화

OT 대상 고도화 악성코드 비율

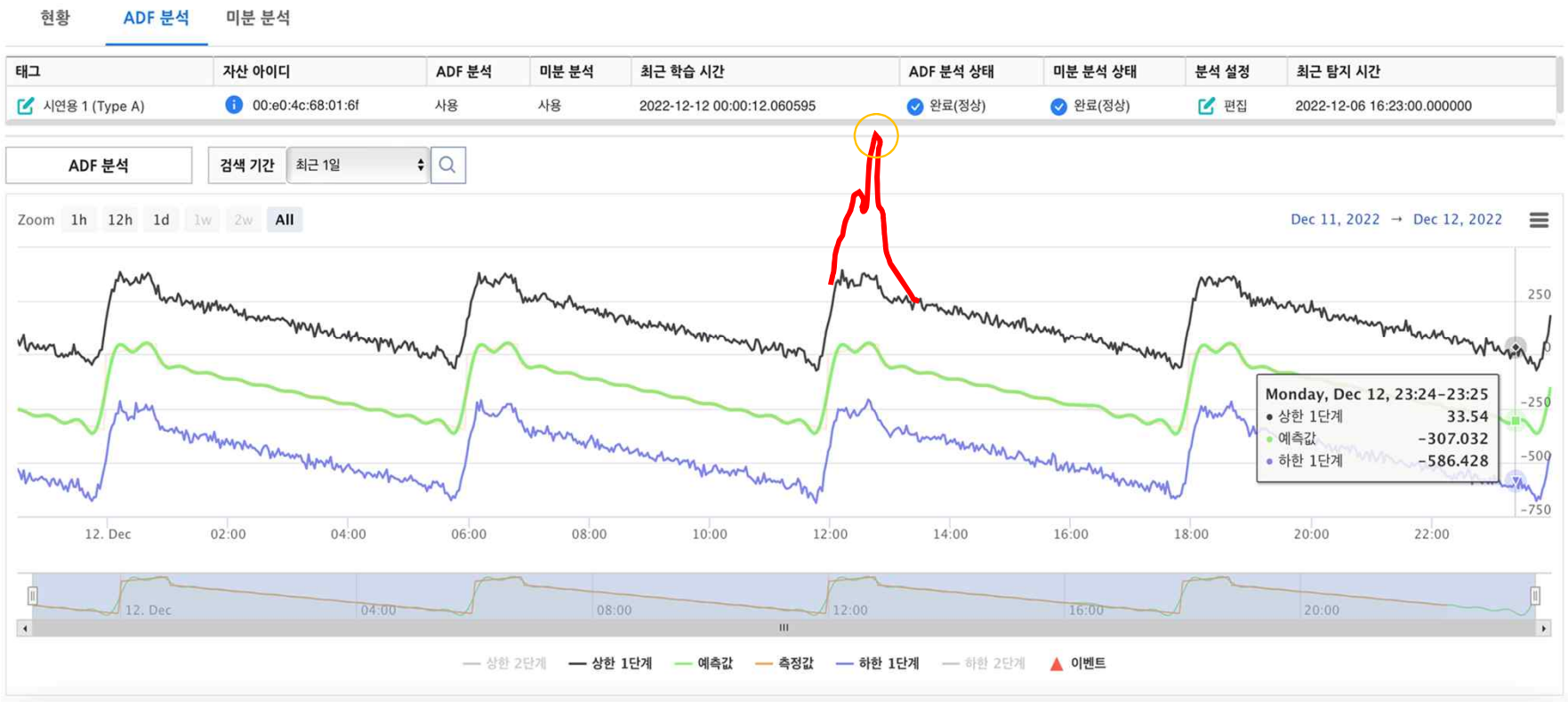
자료: IBM Security X-Force Threat Intelligence Index 2022

	주요 피해 사례	공격 및 이슈
2022	도요타	도요타 일본 부품 공급사 대상 랜섬웨어 공격 일본 내 모든 공장 가동 중단, 하루 기준 1만 300대 생산 차질
2021	플로리다 올즈마 수처리 시설	수돗물 급수 시스템 해킹 유해 화학물질 농도 조작 시도
	미국 콜로니얼 파이프라인	랜섬웨어 범죄 집단에 의한 공격으로 모든 인프라 마비
	JBS Foods	랜섬웨어 공격으로 대부분 공정 가동 중단, 1,100만 달러 비트코인 지불
2020	혼다	랜섬웨어 공격으로 미국과 브라질 등 9개 공장 생산 일시 중단
	이스라엘 수처리 시설	이스라엘 상수도 시설 담당 산업용 컴퓨터 공격 국가 수원에 혼합되는 화학 물질 비율 조작 시도
2019	노르웨이 노르스크 하이드로	랜섬웨어(LockerGoga) 감염으로 다수 금속 압출 공정 가동 중단 약 477억 원 피해
	듀크에너지	사이버보안 컴플라이언스 미준수로 벌금 납부
2018	사우디 페트로케미칼	ICS 타깃 멀웨어(Triton) 감염 트리코넥스 SIS 취약점 이용 안전 제어 시스템 실행 차단, 공장 마비
	대만 TSMC	오염된 USB를 통한 랜섬웨어(WannaCry) 감염 일부 공장 생산라인 가동 중단, 하루 기준 약 110억 원 손실
2017	머스크	시스템 파괴 목적 랜섬웨어(NotPetya) 감염
	몬델레즈	시스템 파괴 목적 랜섬웨어(NotPetya) 감염
2016	우크레네르고	ICS 타깃 멀웨어(Industroyer) 감염으로 대규모 정전 발생
2015	우크라이나 전력 발전소	악성코드(BlackEnergy) 유입으로 제어시스템 서비스 중단
2012	사우디 아람코	데이터 삭제형 멀웨어(Shamoon) 감염으로 약 1조 이상의 피해

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

2. OT, What's different?

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

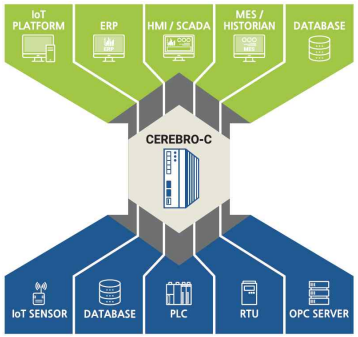


NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

3. 연결부터 보호까지, NAONWORKS Way

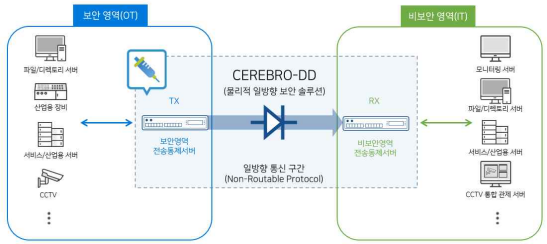
'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

1. 필기하고,



2. 번역하고,

3. 학습하고,



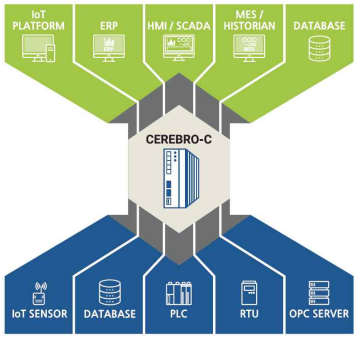
4. 시험보고,

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

3. 연결부터 보호까지, NAONWORKS Way

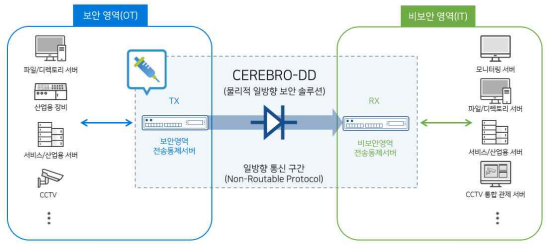
'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

1. 프로토콜을 변환하고,



2. 가시성을 확보하고,

3. 안전하게 사용하고,

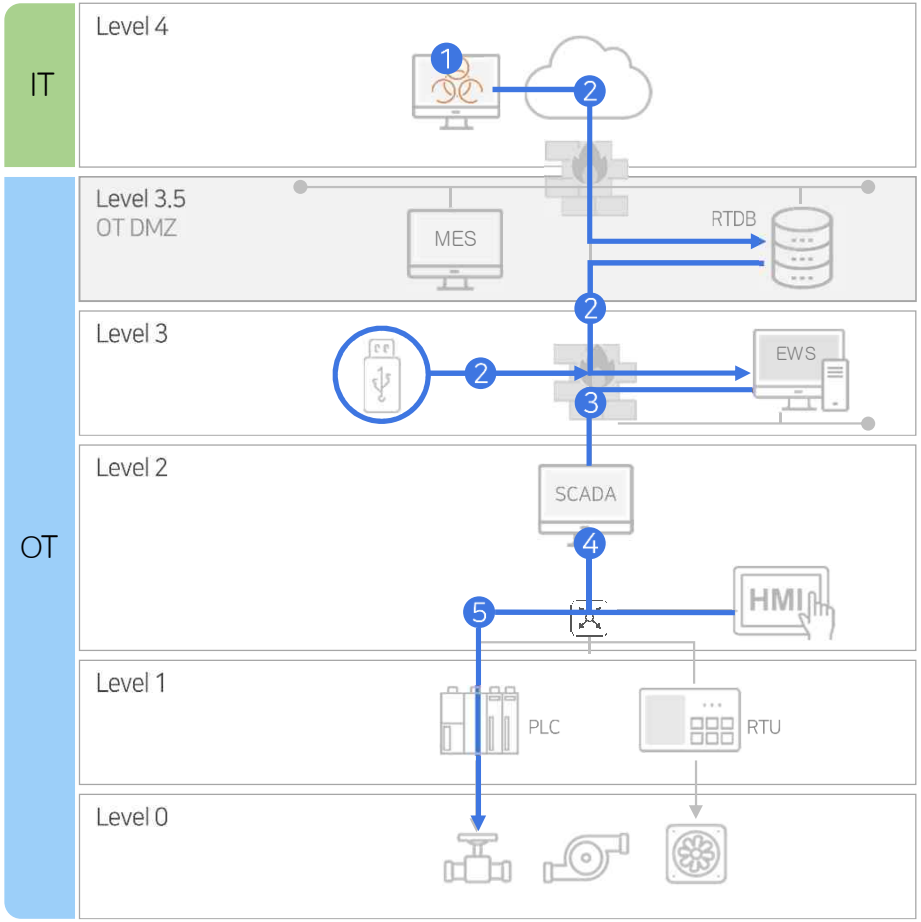


4. 안전한지 확인하고,

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

3. 연결부터 보호까지, NAONWORKS Way

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스



1 IT 망 시스템 침해

- 각종 피싱/스푸핑을 통한 관리자 계정 및 프로파일 정보 취득

2 OT 망 침투

- 허술한 망분리로 외부로부터의 비인가 침투와 C&C IP 접속
- USB 등 비인가 매체, 모바일 테더링 기반 불법 접속
- 제조사 유지보수를 위한 원격 접속

3 악성코드 내부 전파 및 타깃 시스템 탐지

- 파일 공유 프로토콜 SMB, FTP 등의 빈번한 사용
- 노후 시스템 취약점 패치 미흡

4 SCADA/HMI 연결

- OT 망 세그먼테이션(세분화) 및 ACL 통제 미흡
- 외부 침투 공격 기반 HMI, OWS 권한 탈취 취약

5 PLC 제어 명령/설정 변조

- 전송 데이터 변조(명령 코드 변경, 버퍼 오버플로우 등)
- 악성코드에 취약한 제조사 SW 업데이트로 악성코드 감염
- 작업자 오류로 인한 잘못된 제어 명령

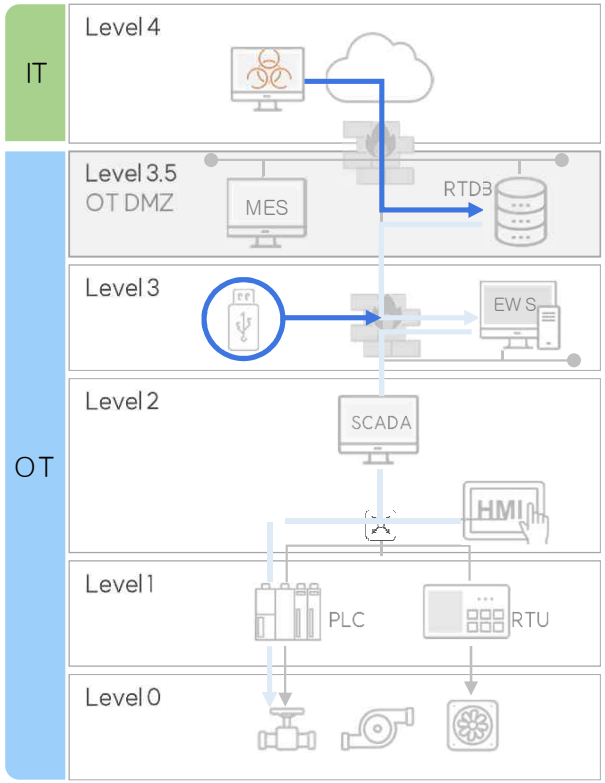
NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

3. 연결부터 보호까지, NAONWORKS Way

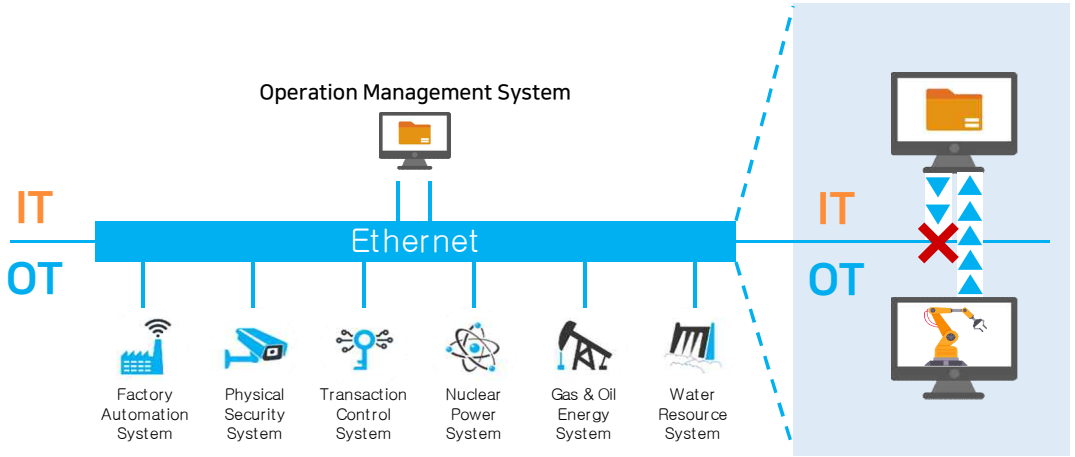
'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

① 위협 유형 : OT망 침투

- IT-OT 망간 연결 접점을 통한 침투 및 C&C 통신
- USB, 노트북 등 비인가 장치의 연결
- 제조사 기술지원을 위한 원격 연결 등 채널



IT-OT간 네트워크 연결 접점 보안



물리적 일방향 보안 장치 (CEREBRO-DD)

- ✓ 일방향 통신으로 완벽하게 OT 네트워크 보호
- ✓ IT-OT망간 물리적 일방향 연결로 보안 위협 원천 차단
- ✓ 물리적인 일방향 연결 구성으로 OT네트워크의 폐쇄성을 유지하고,
  선별적 서비스 프로토콜 연계 (Protocol Access List 기반 접근 제어) 기능을 통해 인가된 데이터만 전송

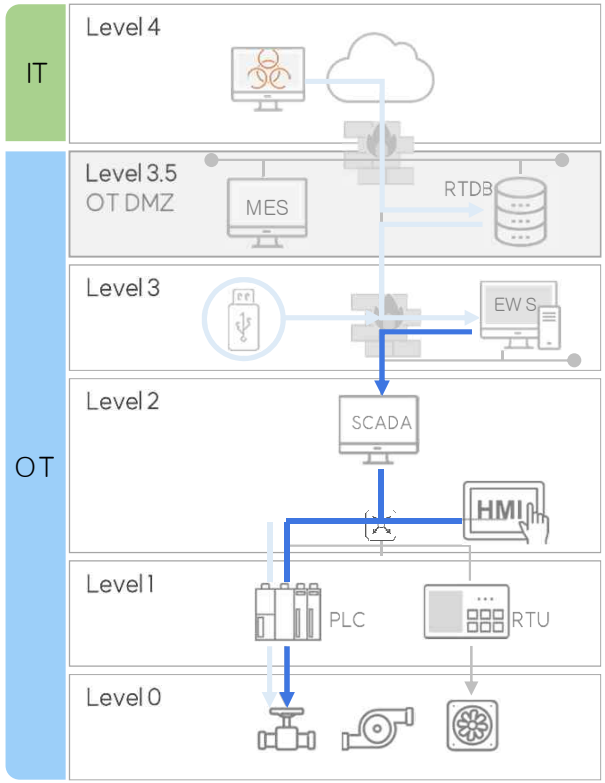
NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

3. 연결부터 보호까지, NAONWORKS Way

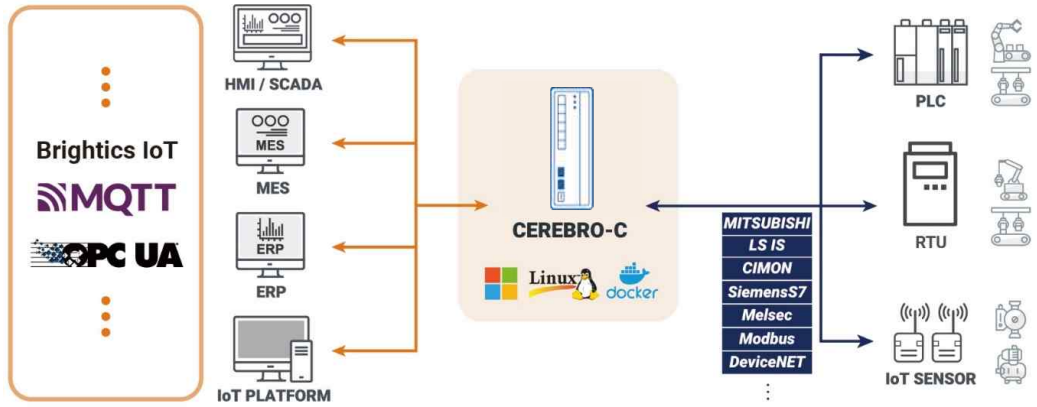
'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

② 위협 유형 : 타깃 시스템 탐지, SCADA/HMI 연결

- OT프로토콜 사용 시스템의 탐색
- 제어설비에서 사용하는 프로토콜 식별
- 프로토콜 분석을 통한 제어명령의 학습



OPC-UA 적용으로 엔드포인트 설비 보호 및 프로토콜의 표준화



산업용 프로토콜 게이트웨이 (CEREBRO-C)

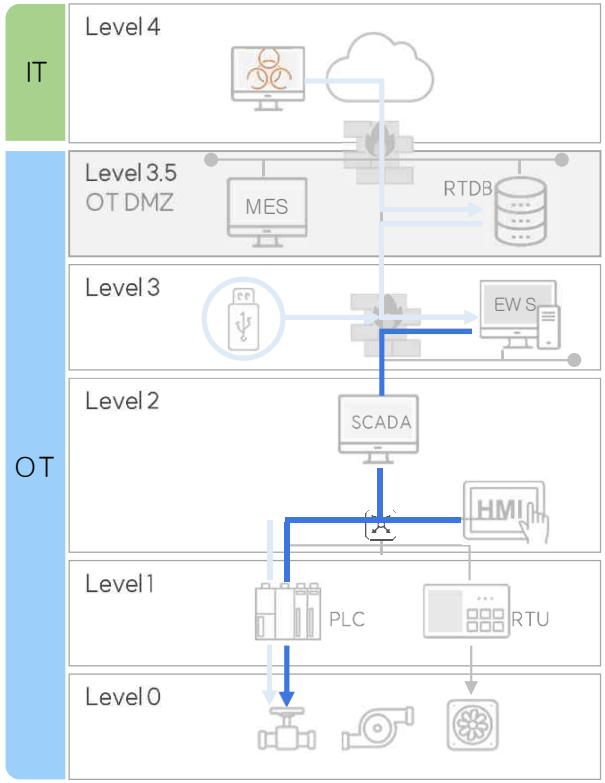
- ✓ 게이트웨이 방식을 통한 Topology Hiding 으로 내부 제어 설비의 네트워크 정보 식별 불가
- ✓ 보안에 취약한 기존의 산업용 프로토콜을 암호화된 표준 프로토콜로 변환/제공 하여 스니핑, 하이재킹 등 통신 감청을 통한 위협 대응
- ✓ 다양한 이기종의 산업용 프로토콜을 표준 프로토콜로 변환
- ✓ 설비 도입 시 제조사 및 프로토콜 의존성 제거

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

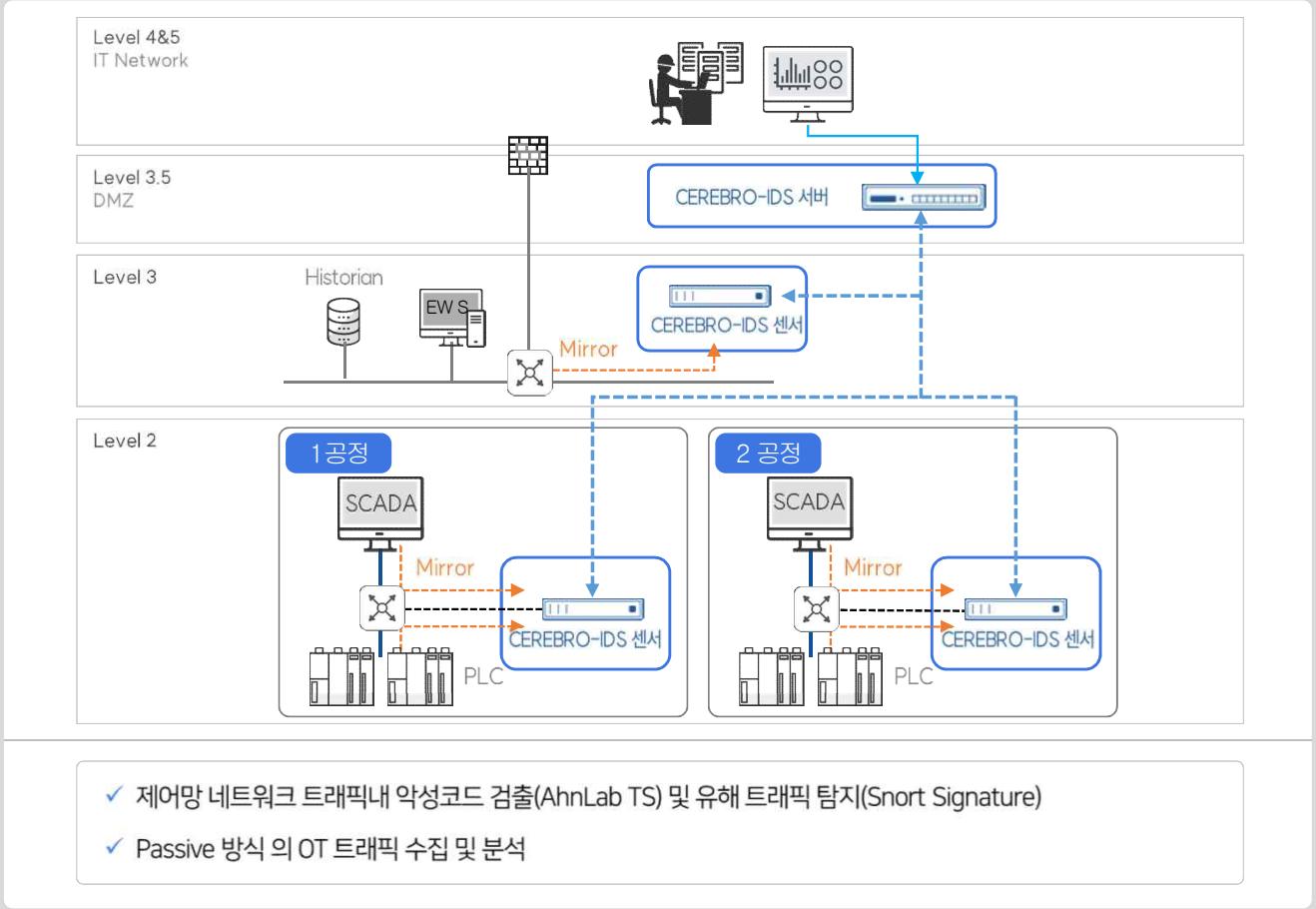
3. 연결부터 보호까지, NAONWORKS Way

③ 위협 유형 : 악성코드 내부 전파

- 파일 공유 프로토콜(SMB), FTP 등의 빈번한 사용
- 노후 시스템 취약점 패치 미흡
- 제조사 SW 업데이트로 악성코드 감염



센서-서버 구조의 침입탐지시스템으로 보안 위협 실시간 탐지



- ✓ 제어망 네트워크 트래픽내 악성코드 검출(AhnLab TS) 및 유해 트래픽 탐지(Snort Signature)
- ✓ Passive 방식 의 OT 트래픽 수집 및 분석

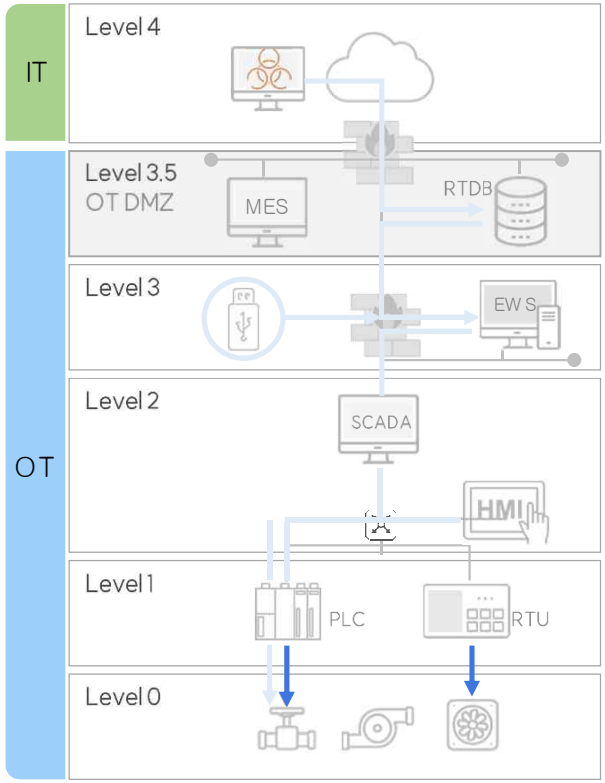
NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

3. 연결부터 보호까지, NAONWORKS Way

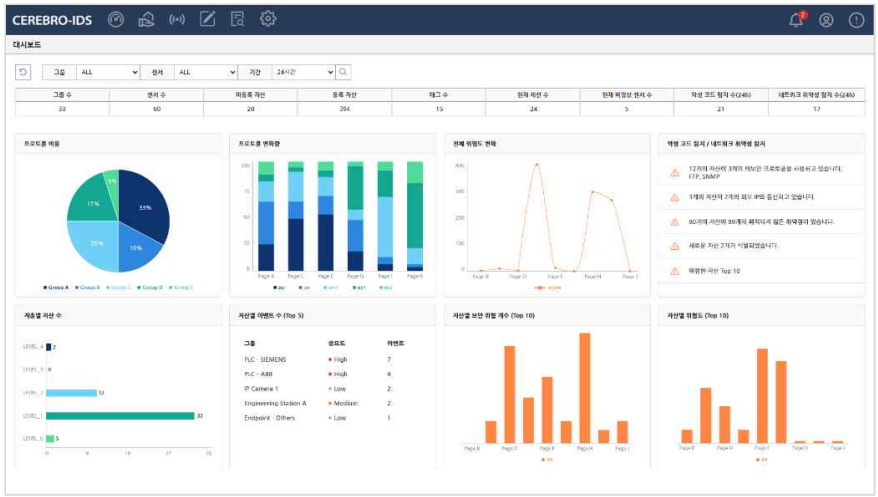
'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

④ 위협 유형 : PLC 제어 명령/설정 변조

- 전송 데이터 변조(명령 코드 변경, 버퍼 오버플로우 등)
- 작업자 오류로 인한 잘못된 제어 명령



센서-서버 구조의 침입탐지시스템으로 보안 위협 실시간 탐지

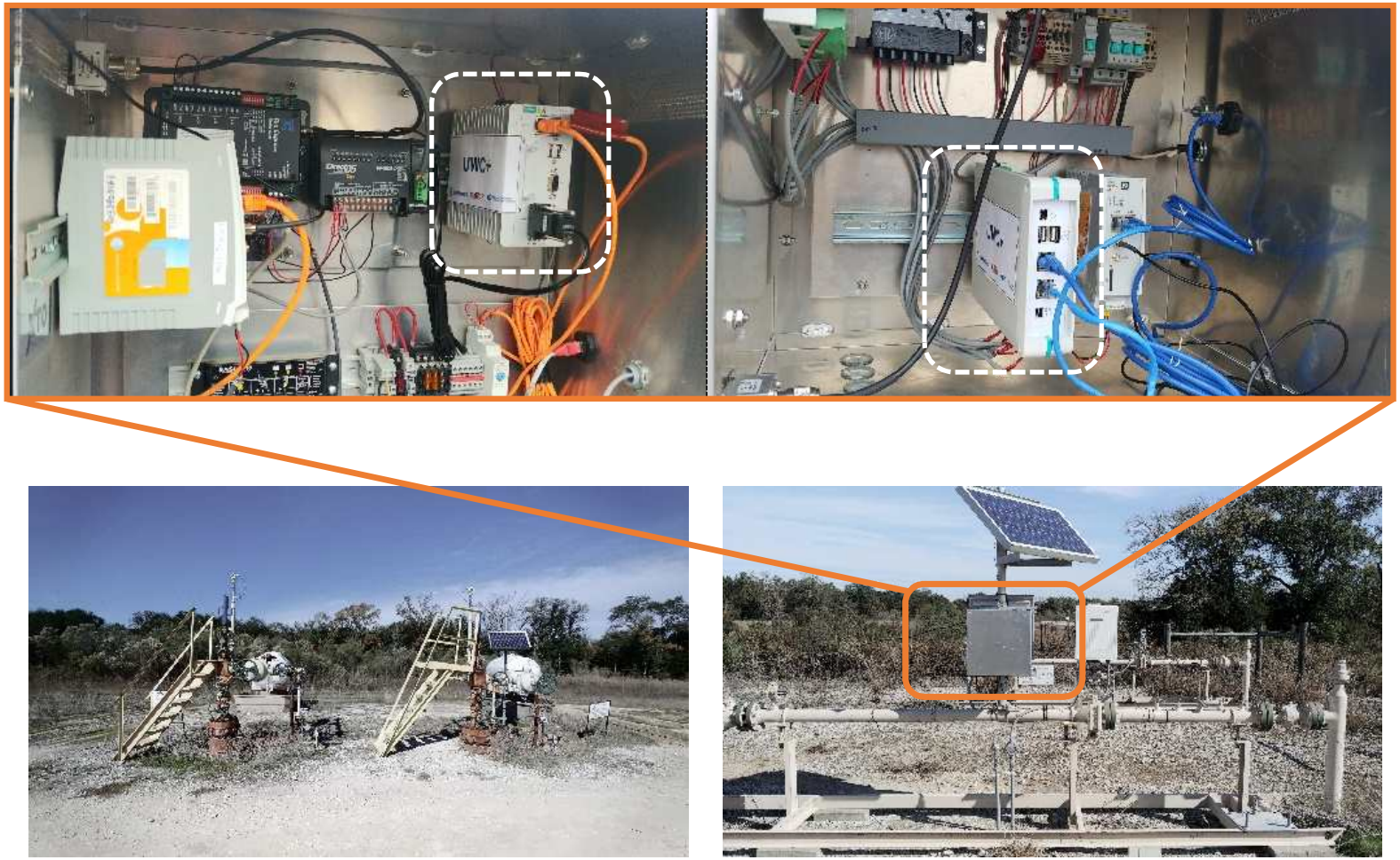


산업용 프로토콜 기반 침입탐지 시스템 (CEREBRO-IDS)

- ✓ 제어설비 자산 정보 및 자산간 세션 및 서비스 정보, 프로토콜, 펌듀모델/네트워크 토폴로지 등 제어시스템 설비 가시성 확보
- ✓ OT프로토콜 심층 분석(DPI)기반 제어 로직(Function Code, Address, Values)의 변조 등 제어 명령 이상 탐지
- ✓ 비인가 장치, Unknown 프로토콜 사용 등 프로토콜 이상행위 탐지
- ✓ ML 기법을 적용한 임계값 예측 등 이상행위 탐지

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

4. USE CASE 1 - RTU 보안



 ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

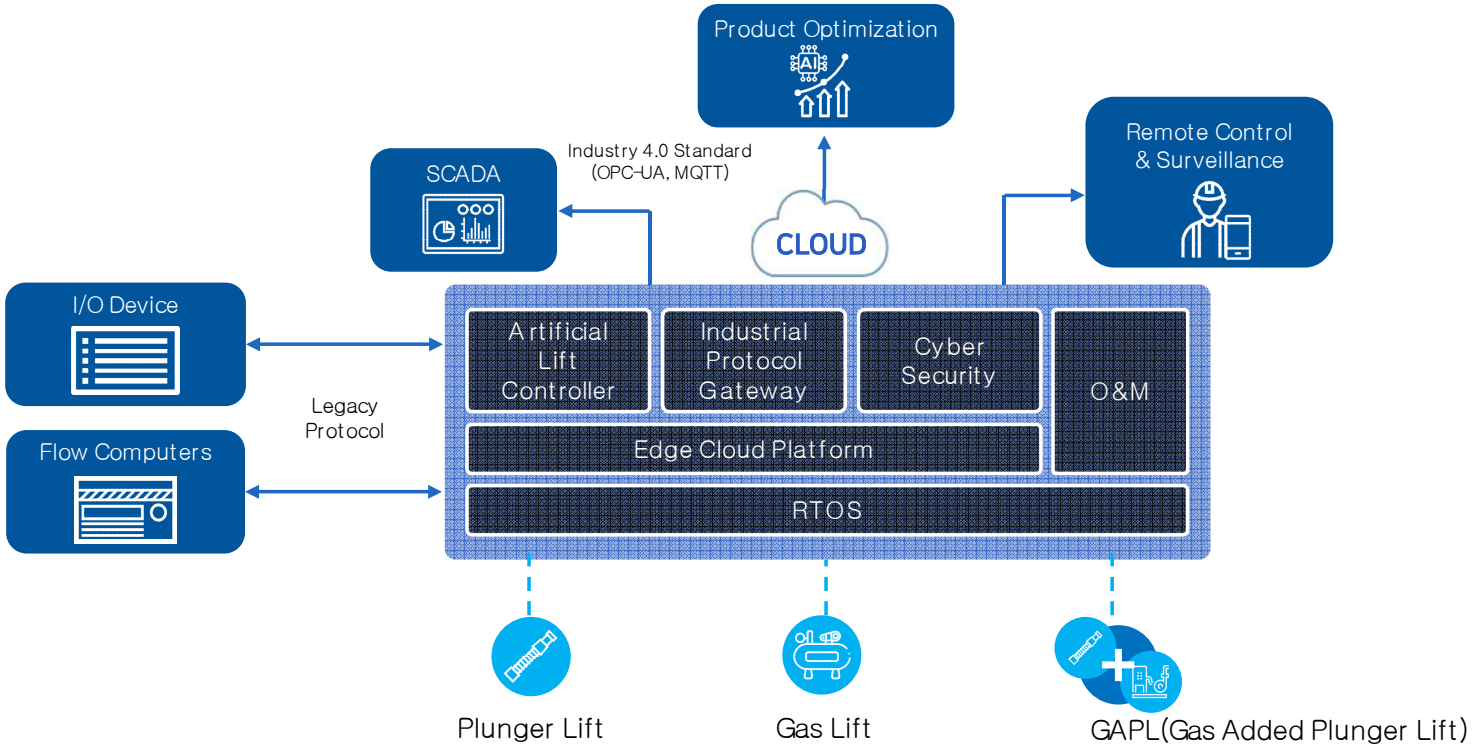
4. USE CASE 1 - RTU 보안

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

개방형 아키텍처
역할별 개방형 모듈 구성
표준 프로토콜 연동

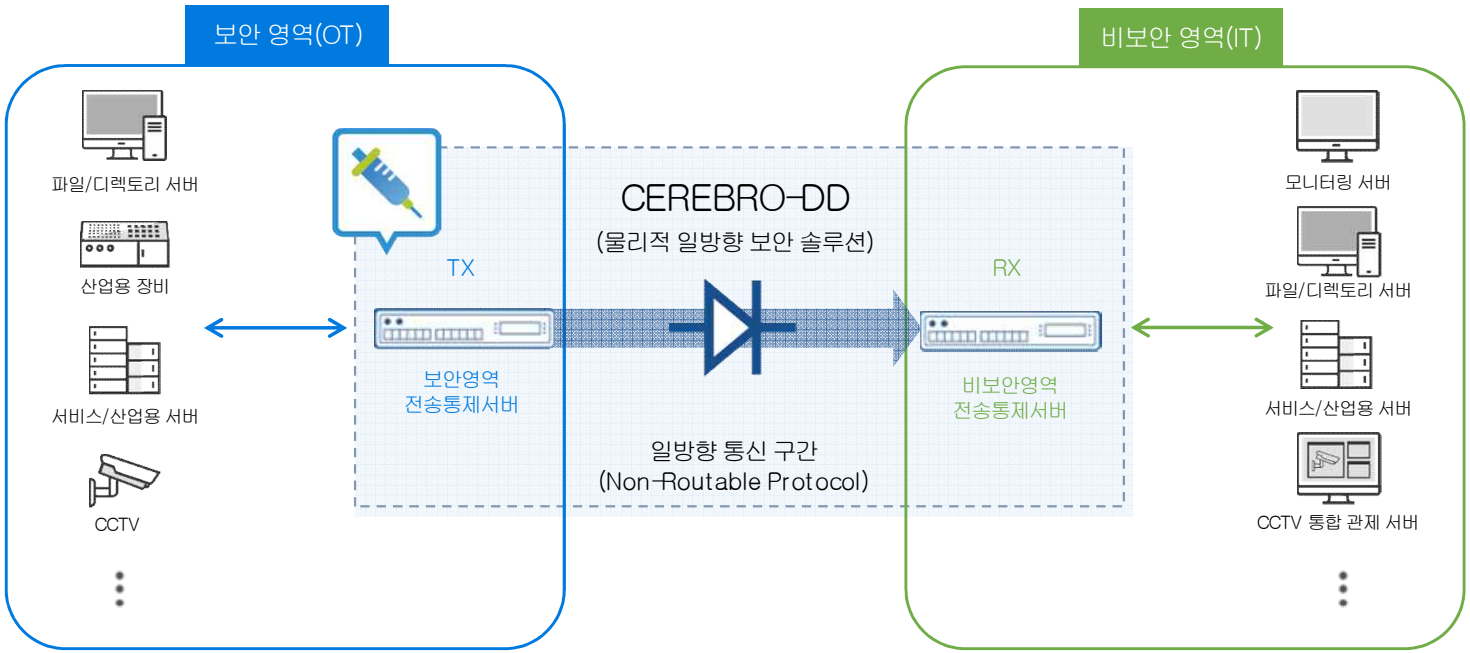
CAPEX & OPEX 감소
유·가스정(Well) 자동 제어
유·가스정 원격 감시

생산 최적화
멀티 유·가스정 동시 제어 및 상태 동조
자동 제어 최적화



NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

4. USE CASE 2 - 안전한 자료수집

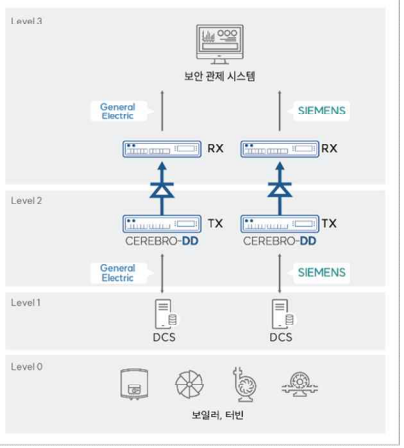


NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

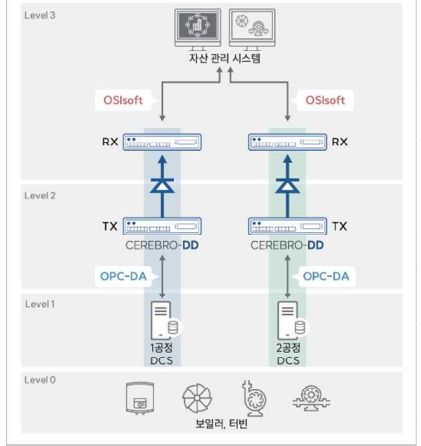
4. USE CASE 2 - 안전한 자료수집

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스

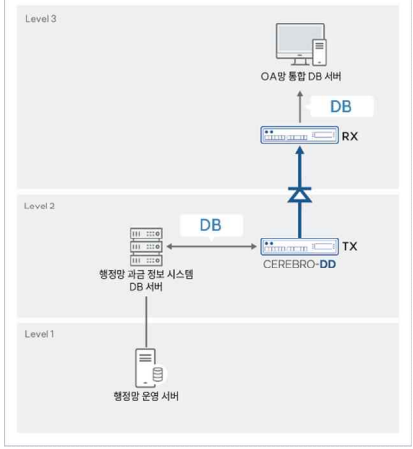
보안 관제 시스템



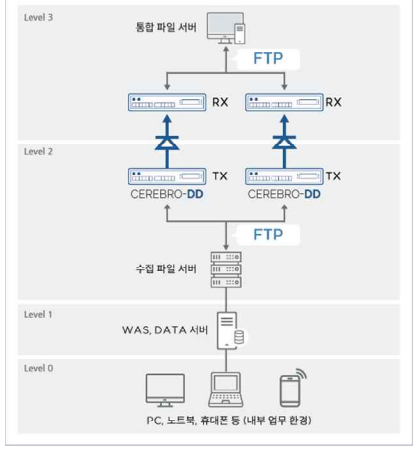
운전 정보 연계 시스템



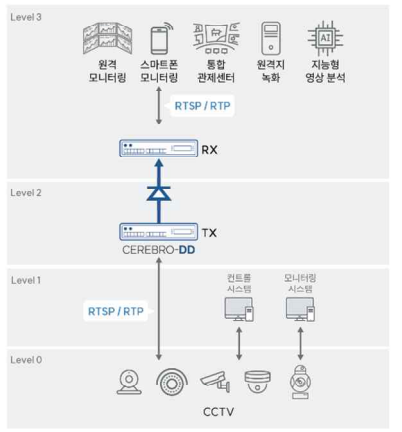
과금 정보 시스템



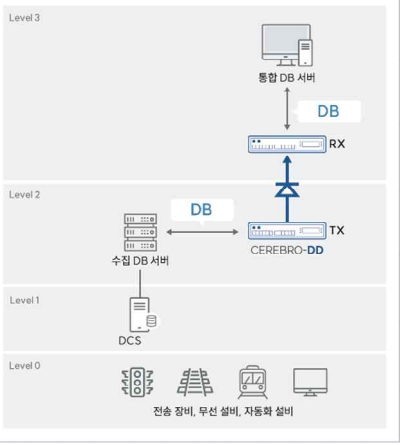
OA망 데이터 수집 시스템 이중화 구성



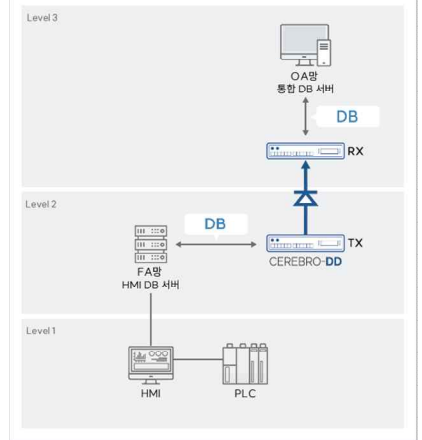
CCTV 영상 관제 시스템



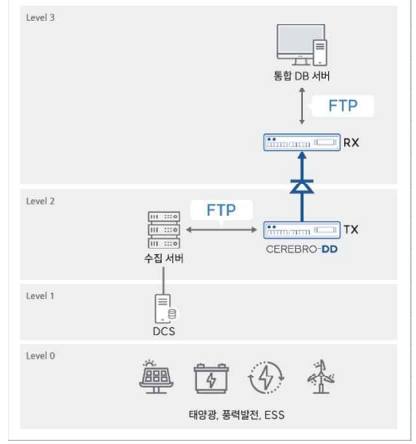
제어 설비 데이터베이스 시스템



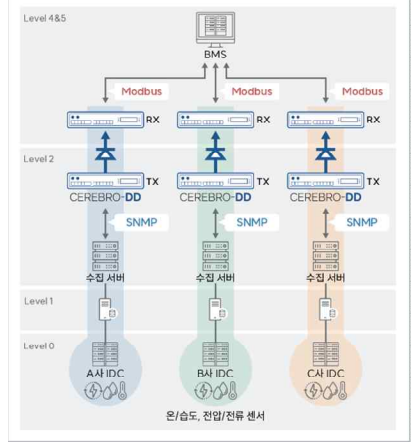
HMI 데이터 수집 시스템



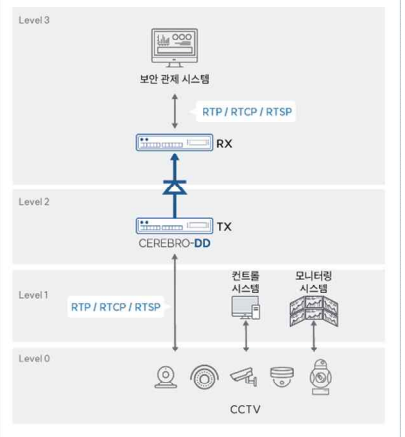
신재생 에너지 운영 정보 시스템



IDC 관리 시스템



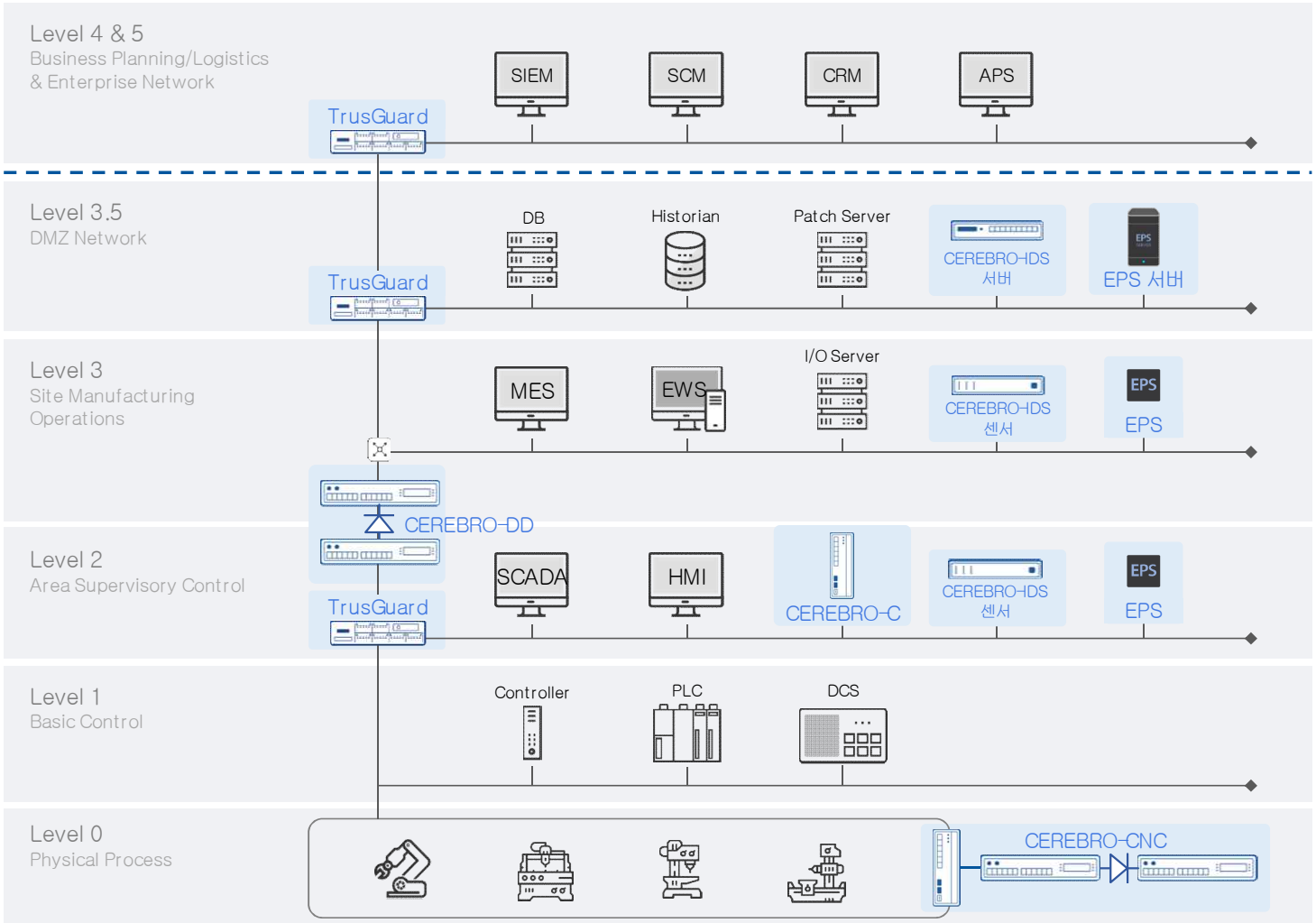
CCTV 영상 데이터 분석 시스템



NAONWORKS © 2023 NAONWORKS Co., Ltd. all rights reserved

4. USE CASE 3 – OT망 네트워크 보안

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스



CEREBRO-IDS

- ✓ OT 자산 및 트래픽 가시화
- ✓ 악성코드 및 유해 트래픽 탐지

CEREBRO-DD

- ✓ 물리적 일방향 데이터 전송
- ✓ 외부 보안 위협 침입 원천 차단

AhnLab TrusGuard

- ✓ OT망 경계 보호
- ✓ 네트워크 세그먼테이션

CEREBRO-C

- ✓ 보안 통신 환경 제공
- ✓ OT 프로토콜 통합 모니터링 및 관리

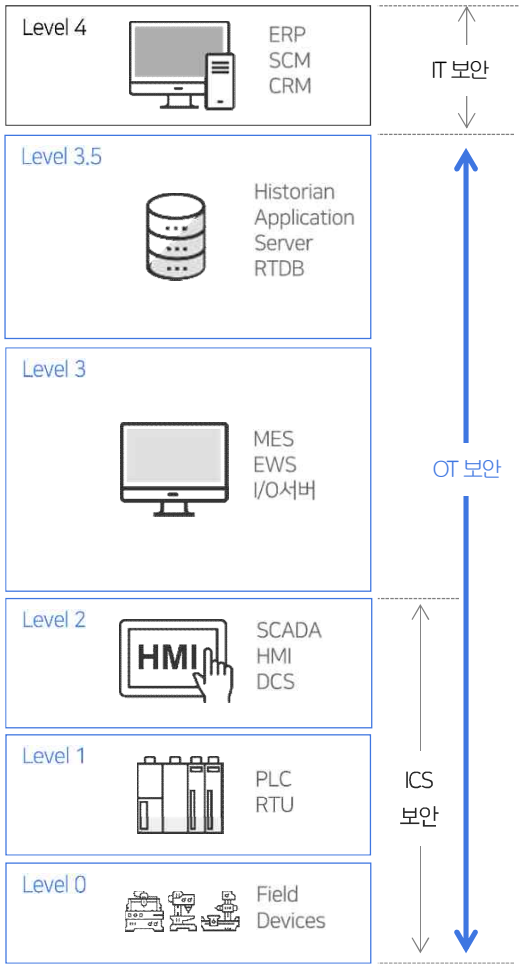
AhnLab EPS

- ✓ 화이트리스트 기반 제어
- ✓ 악성코드 검사/매체 제어

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

5. 간편하지만, 탄탄하게!

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스



엔드포인트 보안

- OPC-UA 기반 보안 통신
- Topology Hiding
- 화이트리스트 기반 제어
- 악성코드 검사
- 매체 제어

CEREBRO-C

EPS

AhnLab EPS

네트워크 모니터링

- 자산 및 네트워크 가시화
- 현장 가용성 보장
- 산업용 프로토콜 심층 분석
- 비정상 데이터 실시간 탐지
- 보안 위협 실시간 탐지

CEREBRO-DP

CEREBRO-IDS

네트워크 경계 보안

- 외부 위협 차단(악성코드URL 등)
- OT 네트워크 보호 및 보안 통신
- 일방향 전송 환경 구축
- 비보안 영역 접근 차단
- 전송 정책 기반 선별적 연계
- 악성코드 검사

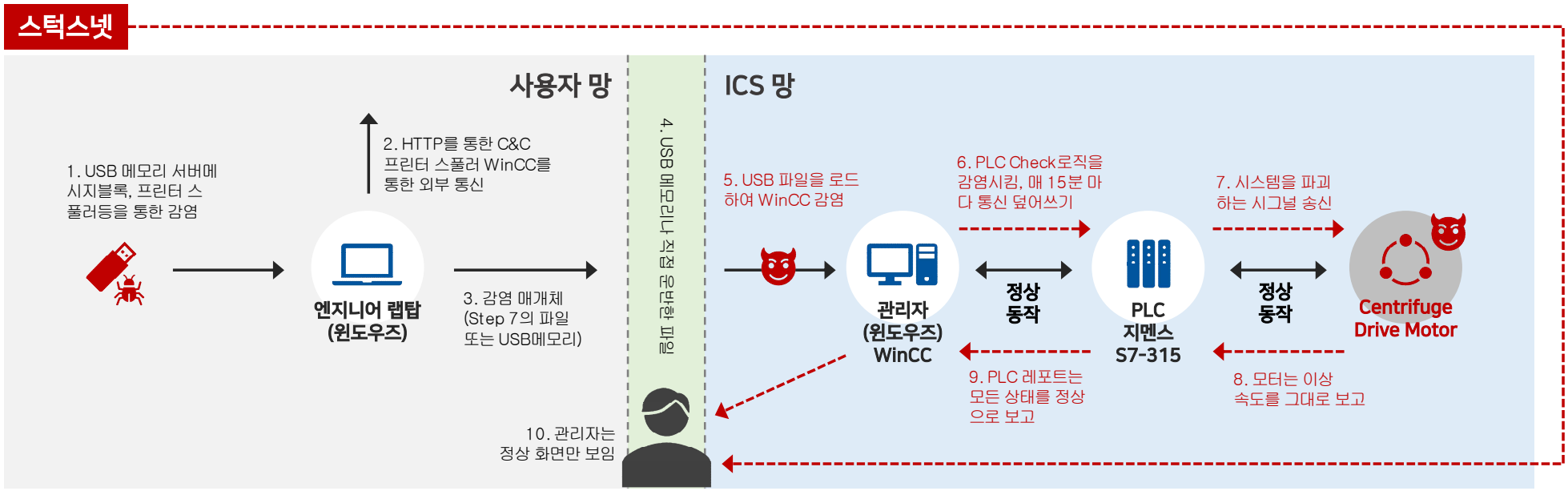
AhnLab
TrusGuard

CEREBRO-DD

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserv

5. 간편하지만, 탄탄하게!

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스



ICS/SCADA 망 침투 이전 시점 파악

2 Stuxnet 멀웨어의 Beaconing 단계 파악

단 한번도 접속한적 없는 PC가 (확률 xx%)
비 정상적인 유저 브라우저 (확률 xx%)
비 정상적인 시간에 (확률 xx%)
비 정상적인 주기로 접속 시도 (확률 xx%)

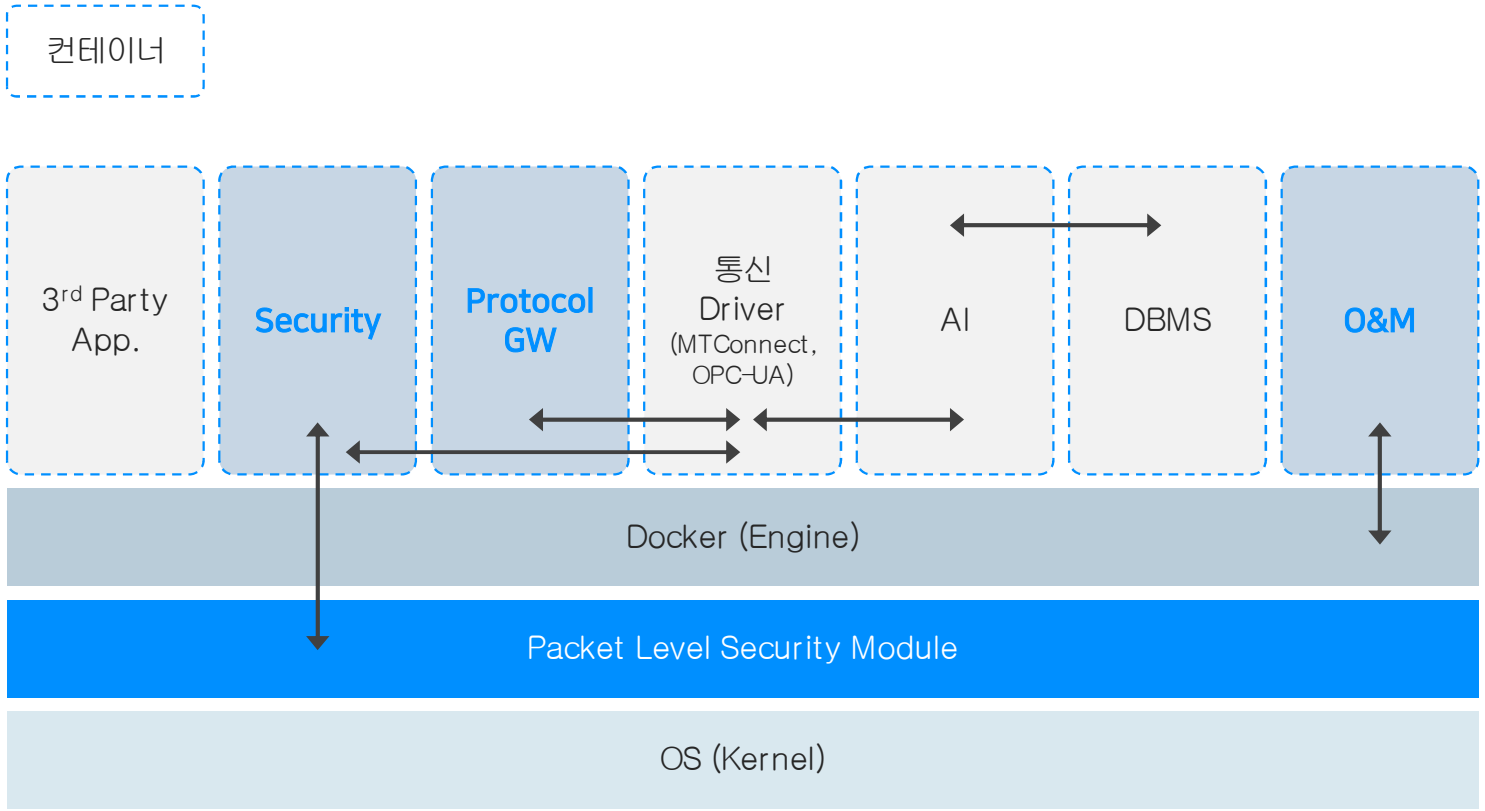
ICS/SCADA 망 침투 이후 시점 파악

6 Stuxnet 멀웨어의 PLC Overwrite 행위 파악

단 한번도 접속하지 않은 Control 서버가 (확률 xx%)
비 정상적인 트래픽을 (확률 xx%)
비 정상적인 시간에 (확률 xx%)
이전에 없던 일정한 주기로 통신 (확률 xx%)

NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

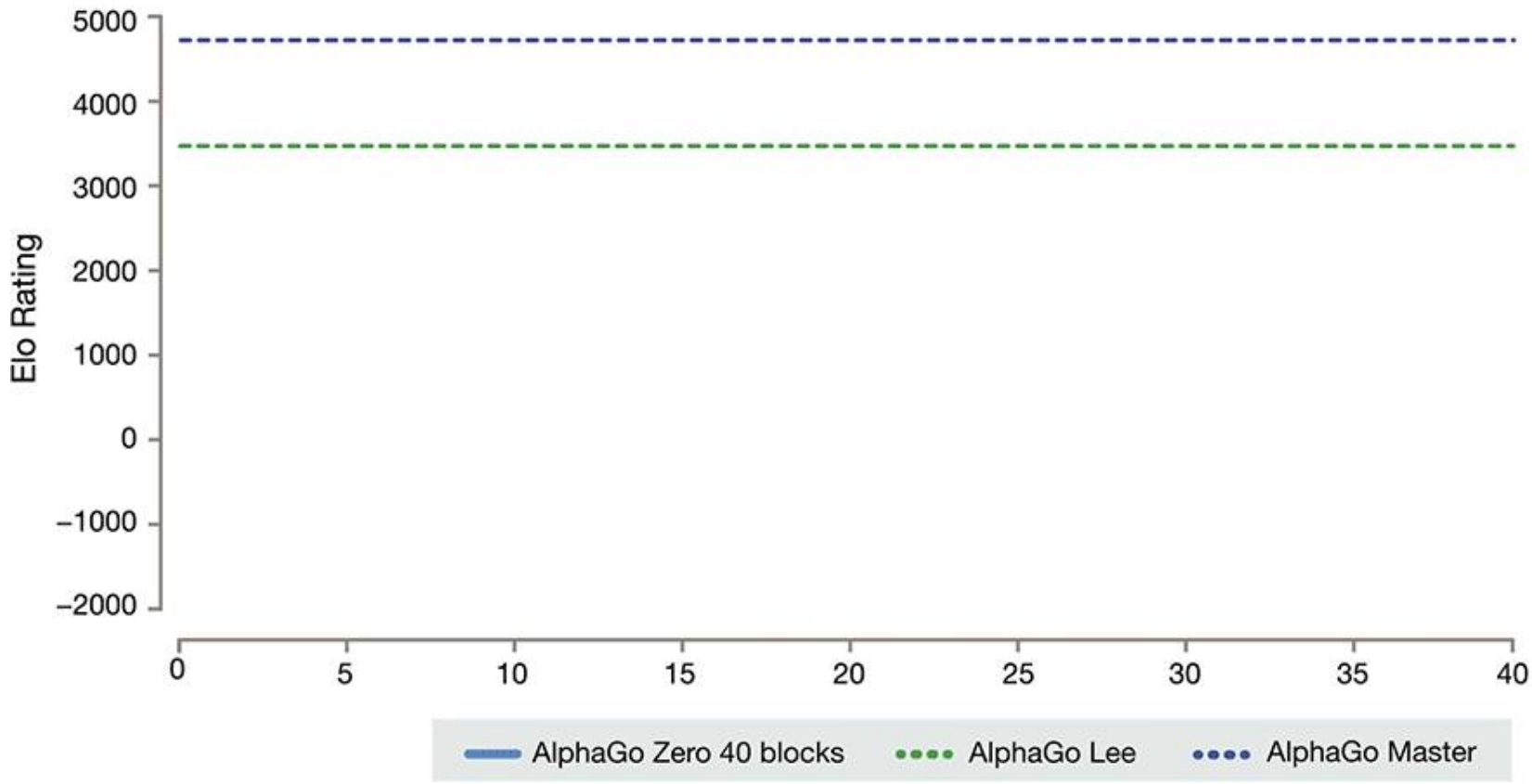
5. 간편하지만, 탄탄하게!



NAONWORKS ⓒ 2023 NAONWORKS Co., Ltd. all rights reserved

6. Demonstration

'간편하지만, 탄탄하게' **나온웍스**가 제시하는
OT 사이버보안 프레임워크 및 케이스



NAONWORKS © 2023 NAONWORKS Co., Ltd. all rights reserved

스마트한 세상을 위한 보안 솔루션

㈜나온웍스

본사 서울시 구로구 디지털로 271, 711호
판교 경기도 성남시 분당구 판교역로 240, A-301호

전화 02-2025-1630
팩스 02-2025-1620
메일 sales@naonworks.com

www.naonworks.com

설문조사 EVENT

세미나 내용에 만족하셨나요? ☺

만족도 설문조사에 참여하시면
스타벅스 기프티콘을 드립니다 ☺