More security,
More freedom

OT 보안 위협과 구축 사례로 알아보는 대응 전략

안랩 황재훈 부장

AhnLab

목차

AhnLab

01.
OT보안의 필요성

1. OT 보안 사고 동향
2. 주요 보안 사고 – TSMC 반도체
3. 주요 보안 사고 – 올즈마 수처리 시설
4. OT 보안 위협 시나리오
5. OT 프로토콜 분석 필요성
6. OT 보안 적용 현황

AhnLab

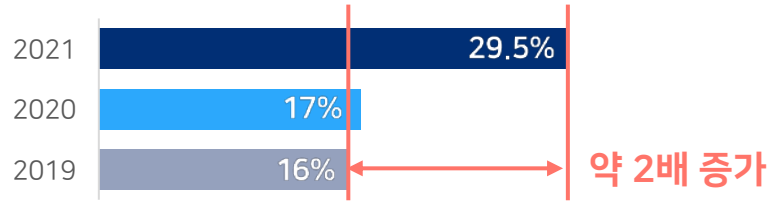
OT 보안 사고 동향

최근 국내/외 제조 및 산업 기반 시설 대상 보안 사고가 증가하고 있습니다.

1위 2020년 글로벌 시장에서 **제조산업의 해킹 피해 비중 순위**(24.4%)

29.5% 2021년 상반기 국내 해킹 사고 중 **제조산업이 차지하는 비율**

국내 해킹사고 중 제조업 비중 추이



출처 : https://www.sedaily.com/NewsView/22Q31LC00S

최근 주요 OT 보안 침해 사례

제조 분야

피해 조직	산업	년도	공격 종류
콜로니얼 파이프라인	에너지	2021	랜섬웨어 (DarkSide)
솔 오리엔스	국방	2021	랜섬웨어 (Revil)
JBS 푸드	식품	2021	랜섬웨어 (Revil)
올즈마 수처리	수도	2020	워터링홀 & APT 공격
솔라윈즈	에너지	2020	공급망 해킹
신풍제약, 셀트리온	제약	2020	도메인 미믹킹
혼다	자동차	2020	랜섬웨어 (EKANS)
노르스크 하이드로	금속	2019	랜섬웨어 (LokerGoga)
TSMC 반도체	반도체	2019	랜섬웨어 (Wannacry)
레이크시티	공공	2019	랜섬웨어 (Ryuk)

주요 사고 사례 1 - TSMC 반도체

피해규모 48시간 공장 가동 중단으로 약 3,000억원(연매출 3%) 손해 발생

원인 및 문제점
- Initial Access : 망분리 정책을 우회한 비인가 매체(USB 사용)의 내부망 직접 연결
- **내부망 전파** : 파일공유 프로토콜 SMB의 빈번한 사용으로 악성코드 전파 용이
- **시스템 취약점** : OT망 설비 보안 취약점 패치 부족

01 랜섬웨어 감염 (Wannacry 변종)

- OT망 내부 설비에 바이러스 검사없이 감염된 비인가 USB 사용

02 내부망 전파

- 원격 파일 공유 프로토콜 SMB 취약점(이터널 블루)
- 다른 공장으로 감염 확산 (신주, 타이난, 대중 3개 공장)

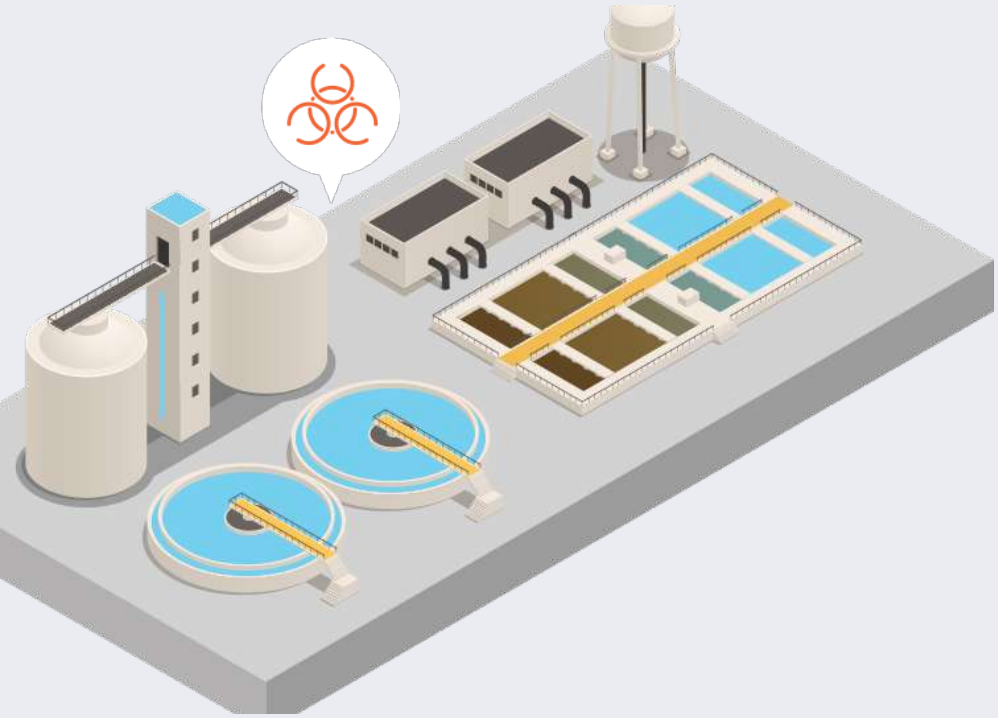
03 생산 가동 중단

- 생산 기기 1만 여대 이상 감염
- 데이터 암호화 및 무결성 손상

주요 사고 사례 2 – 올즈마 수처리 시설

피해규모 최종 시도 불발되었지만, 1만 5천명 시민의 식수를 양잿물로 바꾸는 테러 시도

원인 및 문제점
- Initial Access : 업무용 시스템에서 비인가 사이트 접속으로 인한 악성코드 다운로드
- **허술한 계정 관리** : 업무용 시스템의 동일한 PW 사용
- **노후 시스템의 취약점** : 단종된 운영체제(Windows7) 사용 및 취약점 패치 미흡



01 악성코드 다운로드

- 워터링 홀(watering hole) 기법으로 웹사이트 취약점 통한 악성코드 다운로드
- 관리자 계정 정보 및 시스템 프로파일 탈취

02 내부 설비 접근

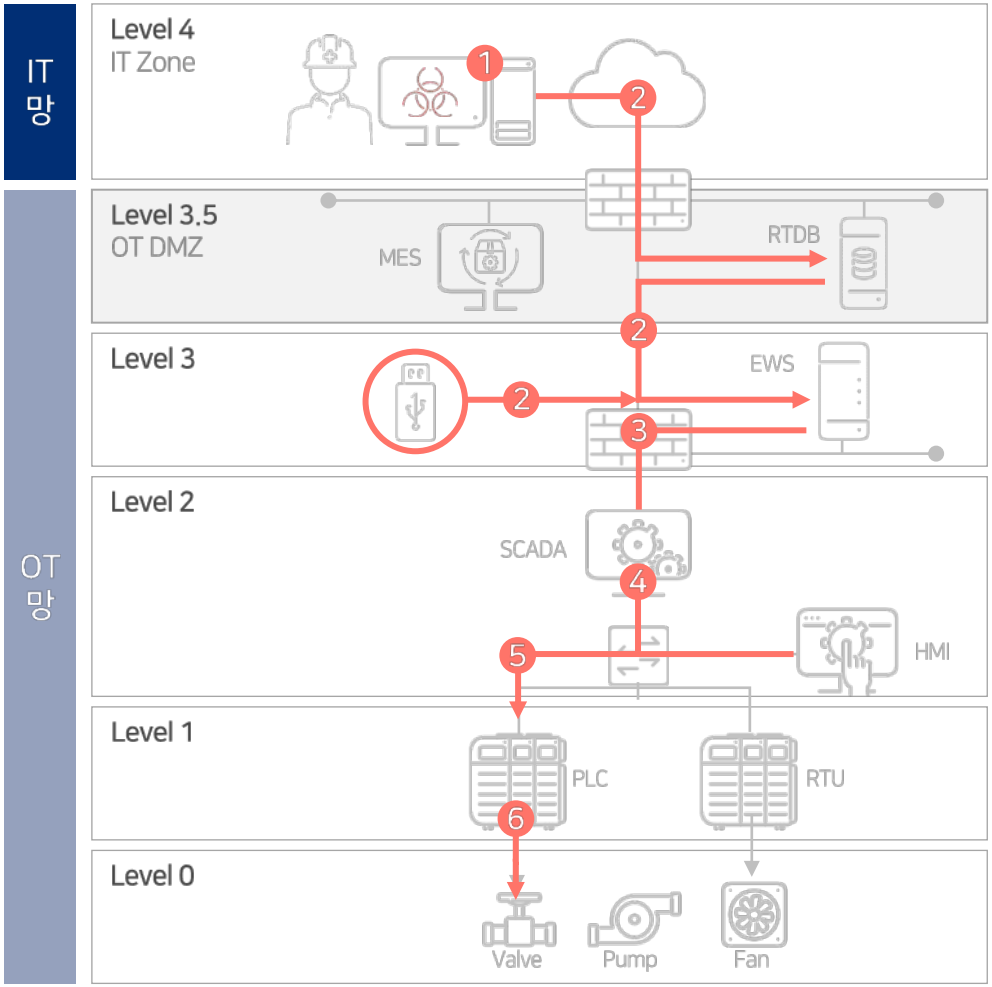
- 허술한 네트워크 Access 정책 악용
- TeamViewer로 설비 HMI 원격 접속

03 설비 설정 변조

- 잿물(수산화 나트륨) 농도 조작
  100 PPM → 11,100 PPM

OT 보안 위협 시나리오

IT 망과 OT망이 서로 연결되어 있고, 엔드포인트 및 네트워크 보안 위협이 혼합된 형태로 진행



1 IT 망 시스템 침해

- 각종 피싱/스푸핑을 통한 관리자 계정 및 프로파일 정보 취득
  ex. Spearphishing, Watering hole, Web Spoofing, Domain Mimicking

2 OT 망 침투

- 허술한 망분리로 외부의 비인가된 침투와 C&C IP 접속
- OT망 직접 접속 (ex. 비인가 매체, 모바일 테더링 등)

3 악성코드 내부 전파 및 타겟 시스템 탐지

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

4 SCADA/HMI 연결

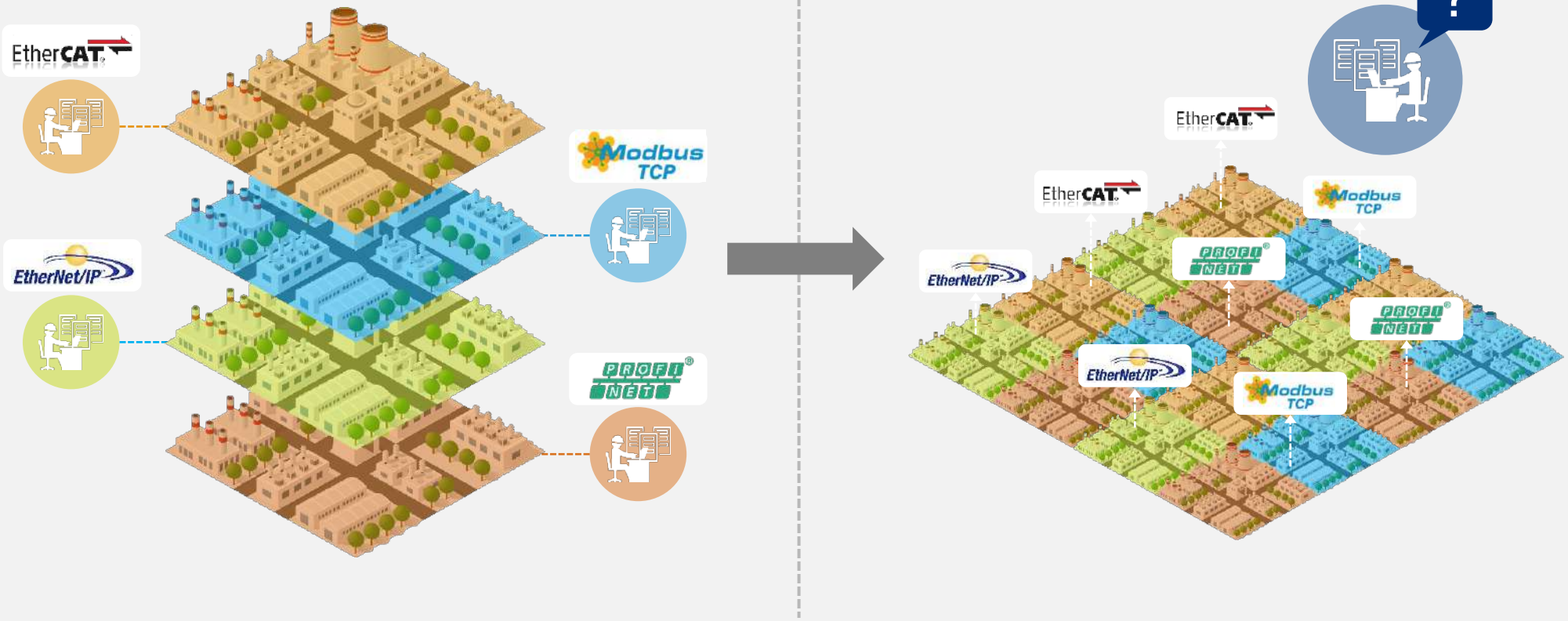
- OT망 세그멘테이션 및 ACL 통제 미흡

5 PLC 제어 명령/설정 변조

6 설비의 비정상 운영

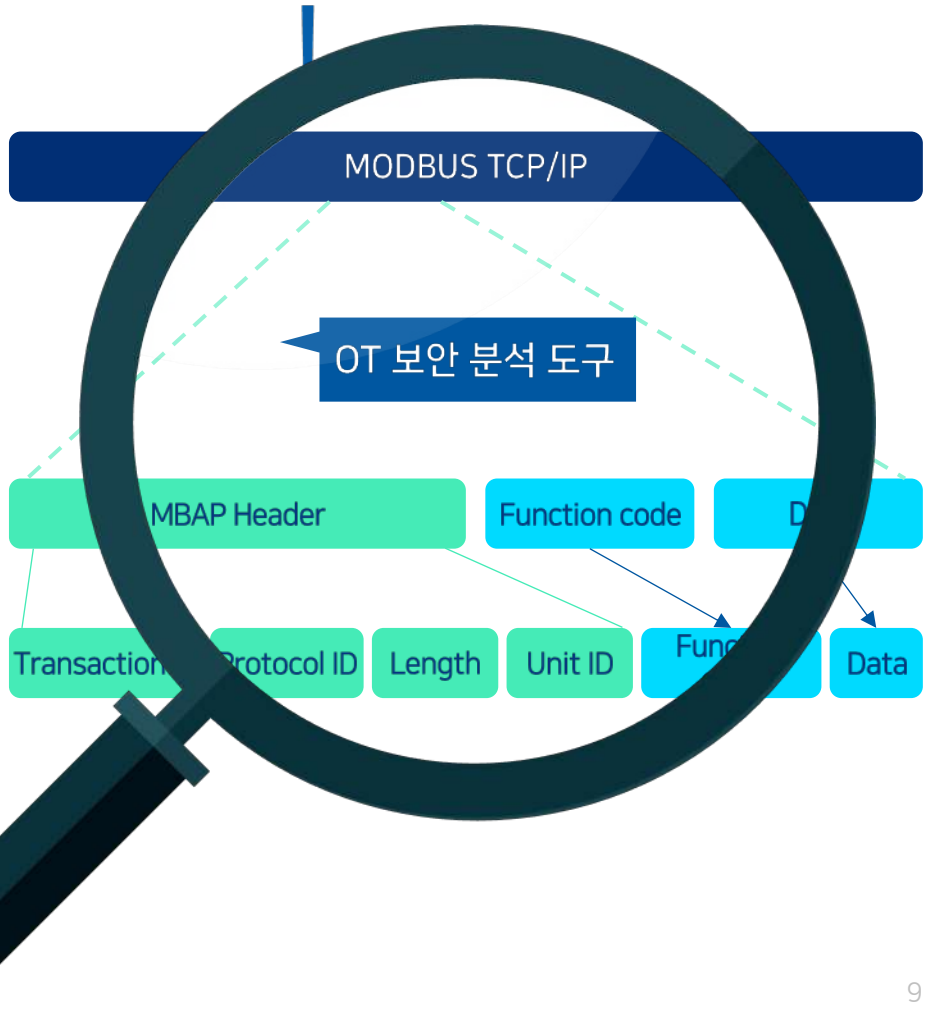
OT 프로토콜 분석 필요성 (1/2)

OT망의 설비들이 제조사별로 별도의 프로토콜 사용, 다양한 프로토콜에 대한 통합 운영 및 모니터링 필요성 증가



OT 프로토콜 분석 필요성 (2/2)

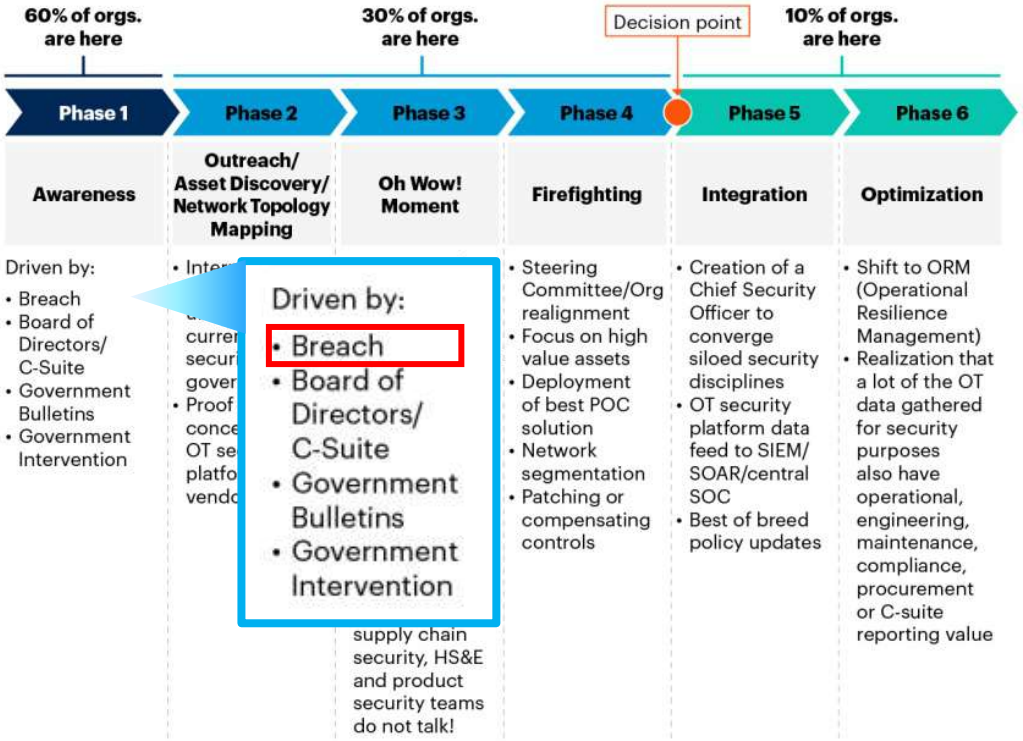
OT 보안을 위해서는 기본적으로 OT 프로토콜 분석이 필요



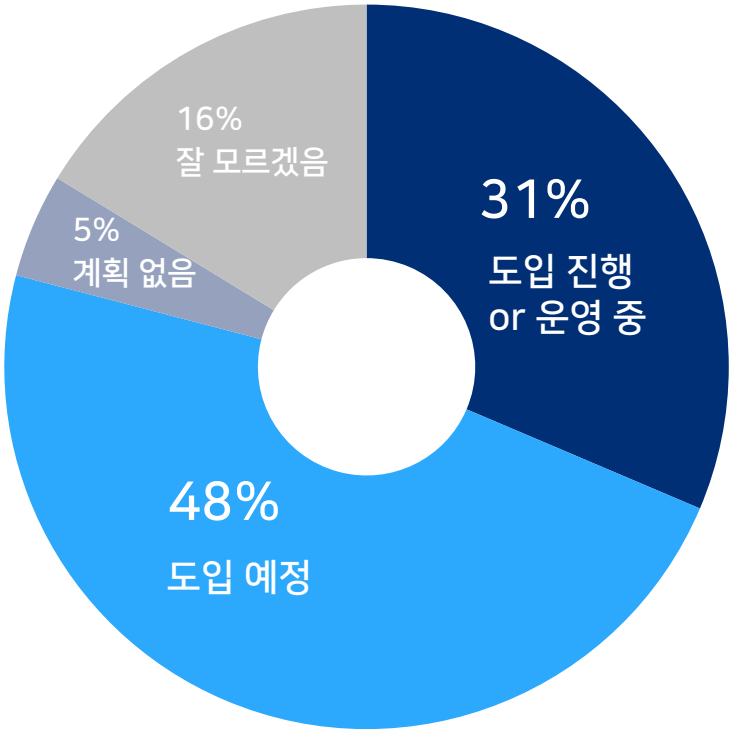
OT 보안 적용 현황

OT 보안의 필요성에 대해서 인식하고 있으나, 국내/외적으로 30~40%만 적용

Gartner OT 보안 적용 단계



국내 OT/IoT 보안 솔루션 도입 현황



※ 출처: Gartner 2021_Market Guide for Operational Technology Security
[안랩] 제조혁신코리아2021 설문조사

02.
안랩 OT보안 전략

1. OT 보안 솔루션 전략 (w/나온웍스)
2. OT 보안 솔루션 프레임워크
3. 단계별 솔루션 구축 전략
4. [도입효과 #1] OT망 경계 보안 및 내부망 보안 강화
5. [도입효과 #2] 안전한 망분리 및 단방향 데이터 전송
6. [도입효과 #3] 생산망에 최적화된 악성코드 대응
7. [도입효과 #4] 생산망 보안 위협의 탐지 고도화
8. [도입효과 #5] OT망 가시성 및 보안 위협 탐지

AhnLab

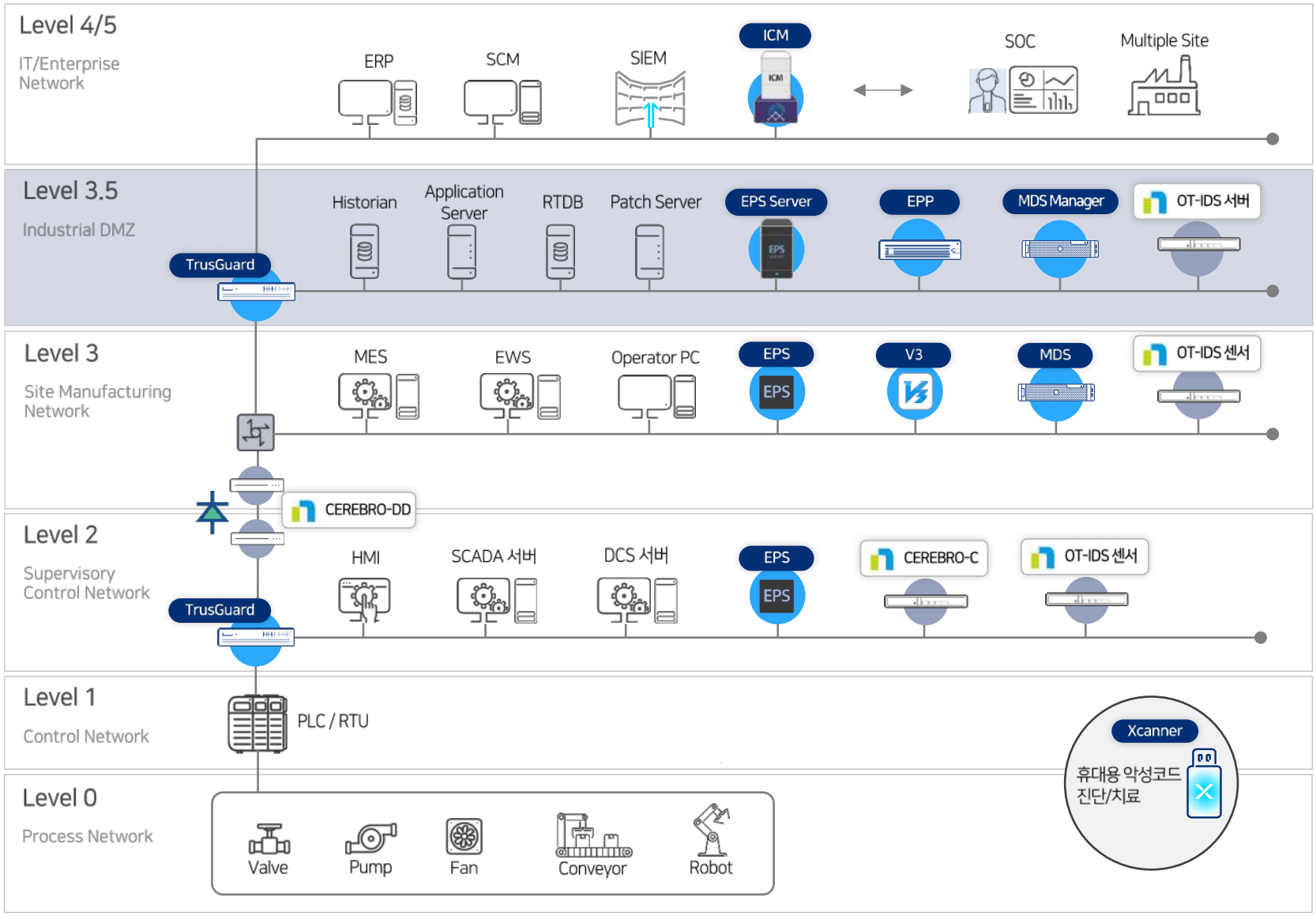
OT 보안 솔루션 전략 (w/나온웍스)

보안 위협 분석 기술 AhnLab × NAONWORKS 산업용 프로토콜 분석

	식별	탐지	대응
OT 보안 > 운영망	**엔드포인트** • AhnLab EPS (엔드포인트 자산/프로세스 식별)	**엔드포인트** • AhnLab EPS (악성코드 검사/비인가 프로세스 탐지)	**엔드포인트** • AhnLab EPS (Whitelist 제어/매체 제어) • AhnLab Xcanner (비상주형 악성코드 검사/치료)
OT 보안 > 운영망	**네트워크** • OT-IDS (OT자산/트래픽 식별)	**네트워크** • OT-IDS (비정상 제어명령/보안 위협 탐지) • AhnLab MDS (생산망 파일 분석/감염장비 탐지) • AhnLab TrusGuard (비인가 트래픽 탐지)	**네트워크** • CEREBRO-DD (단방향 데이터 전송) • AhnLab TrusGuard (비인가 트래픽 차단)
OT 보안 > 제어망	**ICS 설비** • OT-IDS (OT자산/트래픽 식별) • CEREBRO-C (OT프로토콜 식별/변환)	**ICS 설비** • OT-IDS (OT프로토콜 분석/위협 탐지)	ICS 설비 업체 대응

※ SCADA, HMI는 AhnLab EPS/Xcanner를 통한 엔드포인트의 식별/탐지/대응을 제공합니다.

OT 보안 솔루션 프레임워크



AhnLab ICM
- 통합 이벤트 모니터링/가시성
- 고객사 SIEM/SOC 연계

AhnLab EPS
- 화이트리스트기반 제어
- 악성코드 검사/매체제어

AhnLab Xcanner
- 비상주형 악성코드 검사/치료

AhnLab V3 / EPP
- 서버/업무PC 악성코드 검사/치료
- V3 통합 관리

AhnLab MDS
- 생산망 네트워크 악성코드 추적
- 악성코드 감염장비 탐지

AhnLab TrusGuard
- OT망 경계 보호
- 네트워크 세그멘테이션

OT-IDS
- OT 자산/트래픽 가시성
- 악성코드/유해 트래픽 탐지

CEREBRO-DD
- 물리적 단방향 데이터 전송

CEREBRO-C
- 다양한 산업용 프로토콜의 통합 모니터링/관리

단계별 솔루션 구축 전략

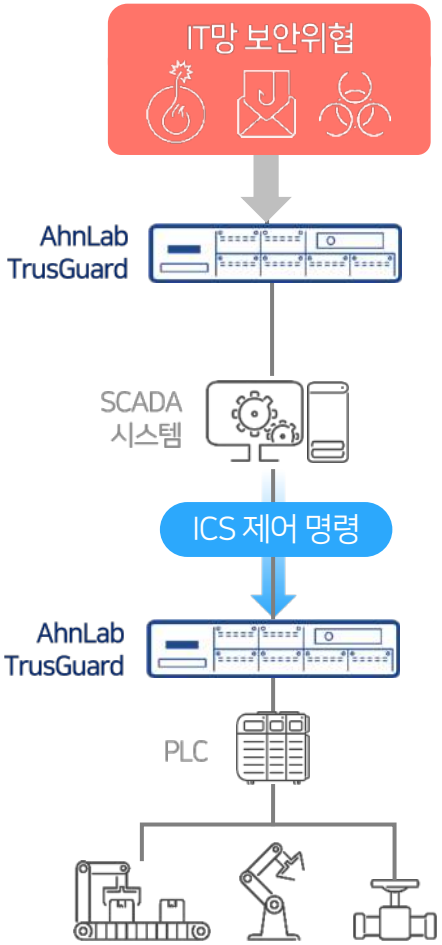
	1단계 : Segmentation & Prevention	2단계 : Visibility & Detecting	3단계 : Monitoring & Managing
	• OT망 NW경계 보안 및 제어망 접근 보호 • EWS, HMI등 OT 시스템의 악성코드 검사 및 어플리케이션 보호	• OT망 설비/트래픽 가시성, NW 위협 탐지 • 악성코드 심층 분석	• 보안 위협 탐지 이벤트 통합 모니터링 • 통합 정책 관리
IT망			통합 관리/모니터링 — AhnLab ICM 3rd Party — SIEM, 고객 Portal
OT망 > 운영망	NW 경계 보안 — UTM : AhnLab TrusGuard 1 EP 보안 — Anti-Virus : AhnLab V3 / EPP Whitelisting : AhnLab EPS / Xcanner 3rd Party — NW : NAC, 보안스위치	NW 경계 보안 — UTM : AhnLab TrusGuard 1 EP 보안 — Anti-Virus : AhnLab V3 / EPP Whitelisting : AhnLab EPS / Xcanner NW 가시성/위협 탐지 — IDS : OT-IDS (가칭) NW 악성코드 탐지 — APT : AhnLab MDS 3rd Party — EP : Backup, DLP, 매체제어 NW : NAC, 보안스위치, WIPS	NW 경계 보안 — UTM : AhnLab TrusGuard 1 EP 보안 — Anti-Virus : AhnLab V3 / EPP Whitelisting : AhnLab EPS / Xcanner NW 가시성/위협 탐지 — IDS : OT-IDS (가칭) NW 샌드박싱 — APT : AhnLab MDS 3rd Party — EP : Backup, DLP, 매체제어 NW : NAC, 보안스위치, WIPS
OT망 > 제어망	NW 경계 보안 — 단방향 GW : CEREBRO-C UTM : AhnLab TrusGuard 2 프로토콜 변환 — CEREBRO-C	NW 경계 보안 — 단방향 GW : CEREBRO-DD UTM : AhnLab TrusGuard 2 프로토콜 변환 — CEREBRO-C NW 가시성/위협 탐지 — IDS : OT-IDS (가칭)	NW 경계 보안 — 단방향 GW : CEREBRO-DD UTM : AhnLab TrusGuard 2 프로토콜 변환 — CEREBRO-C NW 가시성/위협 탐지 — IDS : OT-IDS (가칭)

※옵션 가이드 1 시스템 환경에 따라서 V3/EPP 또는 EPS/Xcanner 선택 필요 2 다양한 프로토콜을 통합 운영하는 환경에 적용

[도입효과 #1] OT망 경계 보안 및 내부망 보안 강화

식별 > 탐지 > 대응

AhnLab TrusGuard를 통해 OT망/IT망 경계의 유해 트래픽 및 네트워크 접근 차단으로 안전한 망분리 환경을 제공하며,
내부 네트워크 세그멘테이션 및 ICS 프로토콜 제어 기능을 통해서 OT망 내부의 보안 위협을 효율적으로 탐지하고 대응합니다.



1 OT망 관문 보호

- 외부 위협 차단 (악성코드, URL, NW위협)
- 보안통신 (IPSec/SSL VPN)
- 네트워크 세그멘테이션

2 ICS 프로토콜 제어

- 프로토콜별 제어
  1) Modbus, DNP3 등 프로토콜별 허용/차단
- 프로토콜 Function 코드 상세 제어
  1) 사용하지 않는 명령어 코드 상세 제어
  ex. "Write single coil(0x05)" 만 차단 가능

- 네트워크 세그멘테이션
- OT망 접근 제어
- 악성코드 탐지
- IPS
- Application 제어
- VPN (IPSec, SSL)

→ 차세대 방화벽 네트워크 위협 탐지/차단

+

- ICS 프로토콜별 제어
- ICS 프로토콜 Function 코드 제어

→ ICS 프로토콜 제어 기능

[도입효과 #2] 안전한 망분리 및 단방향 데이터 전송

식별 > 탐지 > 대응

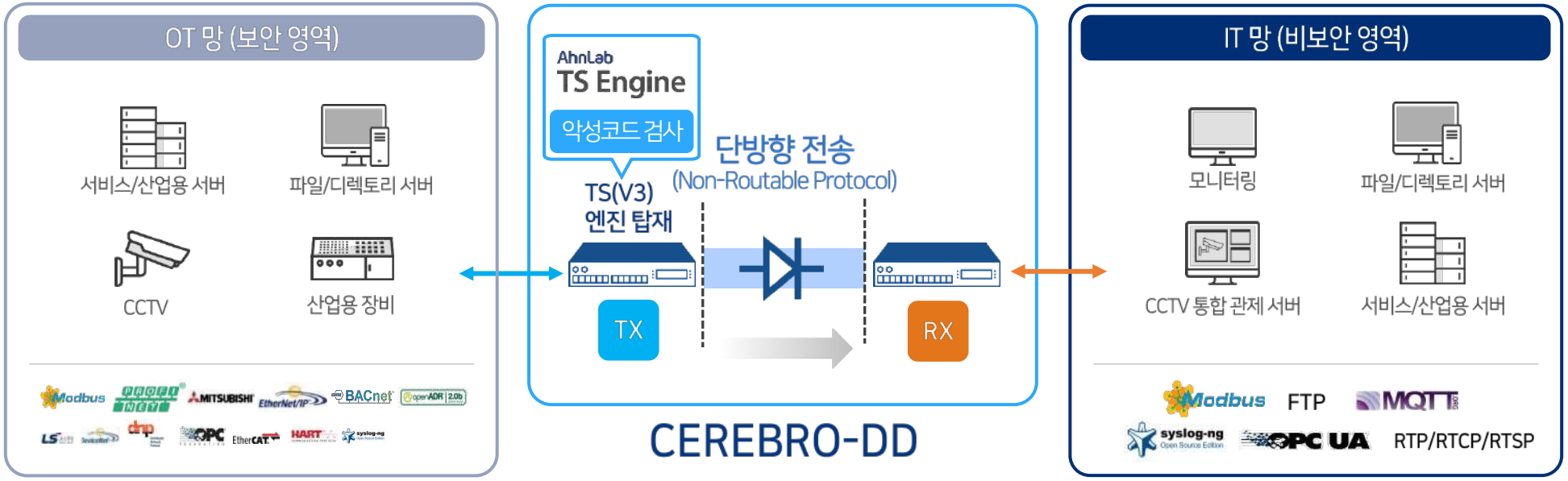
OT망 보안 영역에 대한 안전한 망분리를 위해 데이터를 비보안 영역으로 전송하는 물리적 단방향 데이터 전송을 지원합니다.

1 OT-IT망간 물리적 망분리와 데이터 전송

- 보안 영역 데이터에 대한 비보안 영역으로부터의 접근 차단
- 독자 개발 일방향 데이터 전송 프로토콜(Non-Routable) 적용 (1G/10G)
- FTP 등 File 전송 및 CCTV 등의 TCP/UDP 스트리밍 데이터 전송 지원

2 보안성 제공

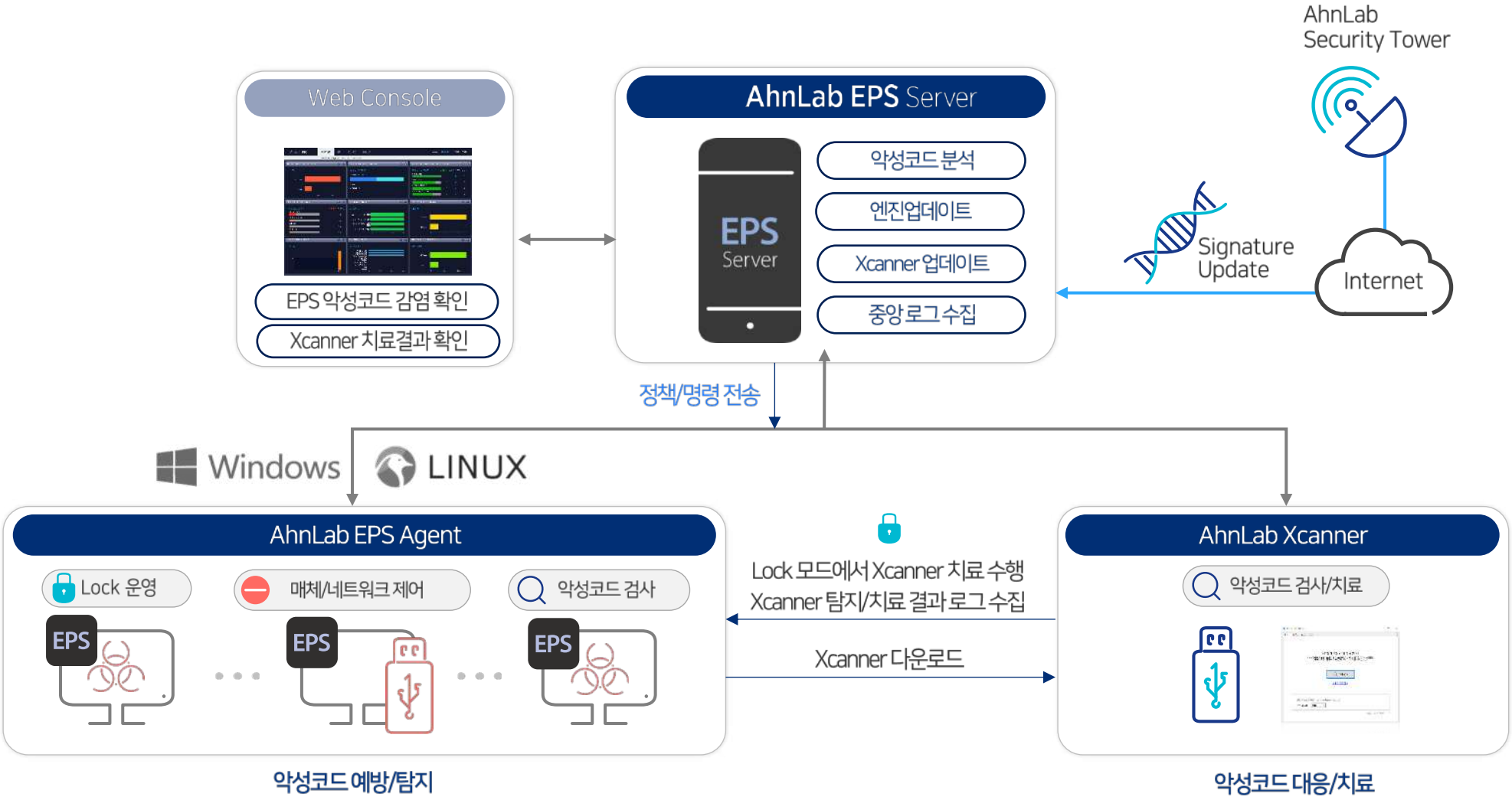
- TS엔진 적용을 통한 멀티 백신 검사 기능 제공
- 구성 노드 간 데이터 암호화를 통한 일방향 통신 수행
- 선별적 서비스 프로토콜 연계 (Access List 에 의한 접근 제어)



[도입효과 #3] 생산망에 최적화된 악성코드 대응

식별 > 탐지 > 대응

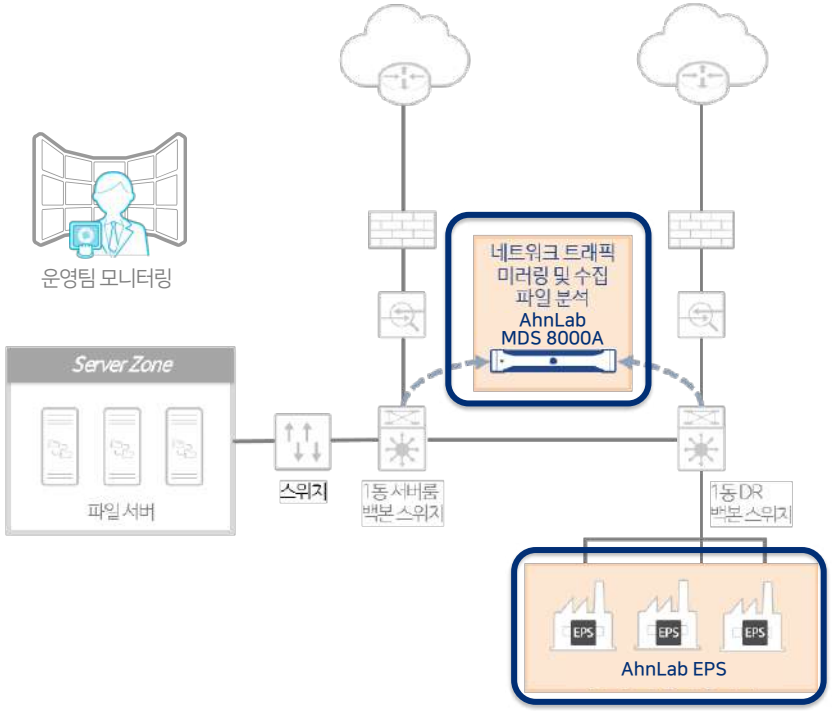
AhnLab EPS의 락다운 및 실시간 탐지를 통해 악성코드 사전 방역을 제공하고, AhnLab Xcanner를 통해 프로그램 설치 없이 악성코드 치료



[도입효과 #4] 생산망 보안 위협의 탐지 고도화

식별 > 탐지 > 대응

AhnLab EPS와 AhnLab MDS의 연동을 통해 생산망 네트워크 내 다양한 악성코드 확산 경로 모니터링과 감염 장비에 대한 치료 및 대응 제공



※ 상기 구성도는 AhnLab MDS의 구성을 설명하는 자료로 실제와 다를 수 있습니다.

고도화 효과

- ✓ 설비 단말과 생산망 네트워크 구간을 실시간으로 분석하여 악성코드의 진원지와 목적지 확인
- ✓ 탐지 결과에 대한 모니터링 기반으로 단시간내 효율적인 악성코드의 표적 치료 수행

연동 운영 방식

AhnLab MDS

1. 생산망 트래픽에 존재하는 파일 수집/분석
2. 감염 장비 상세정보 조회

AhnLab EPS

1. 기간별 MDS 탐지건수 조회
2. 목적지 IP에 대한 EPS Agent 설치 여부 조회
3. Agent 설치된 PC에 감염된 위협의 위험도 확인
4. 비상주형 백신 Xcanner를 활용한 악성코드 조치

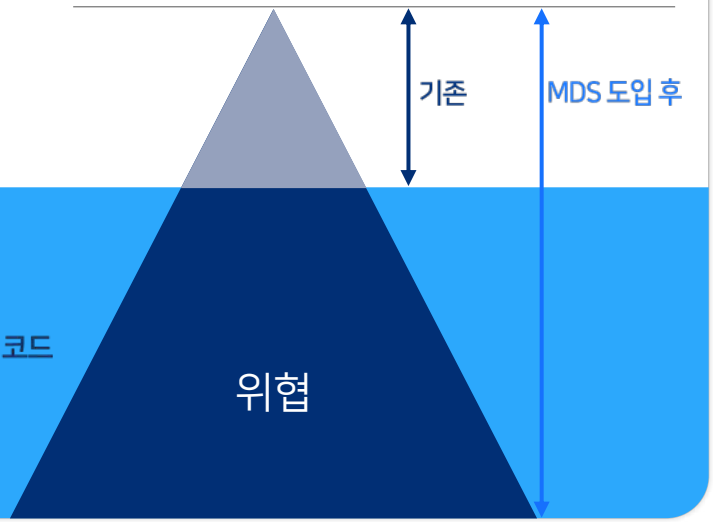
위협 커버리지 확대

AhnLab EPS

- ✓ Known 악성코드
- ✓ 실행형 악성코드

AhnLab MDS

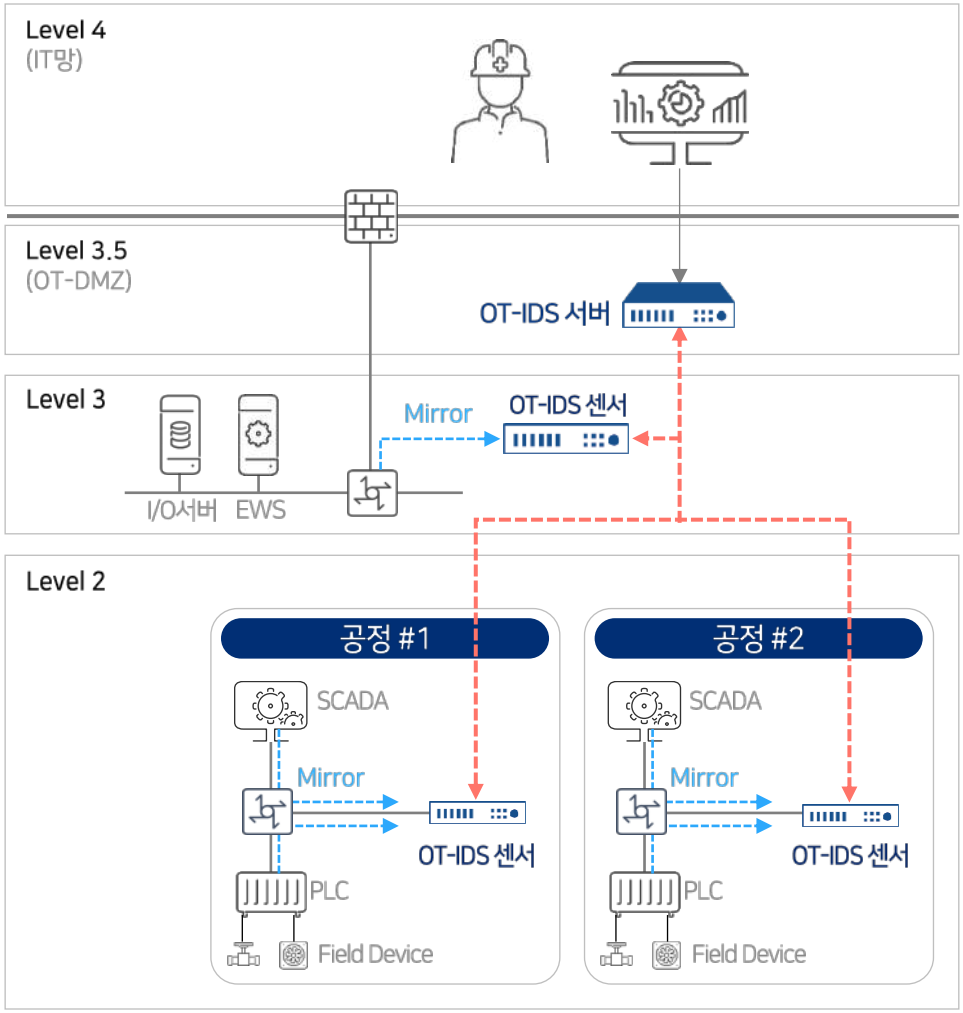
- ✓ Unknown 악성코드
- ✓ 비실행형(Non-PE)악성 코드
- ✓ 유해 트래픽
- ✓ C&C, 취약점



[도입효과 #5] OT망 가시성 및 보안 위협 탐지

식별 > 탐지 > 대응

OT-IDS는 자산 및 트래픽의 가시성을 제공하고, 내부망에 전파되는 악성코드 및 유해 트래픽을 탐지하여 신속한 대응 지원



1 자산/트래픽 가시성

- ✓ ICS 설비/IT/IoT 디바이스 자산 정보
- ✓ 네트워크 세션 및 토폴로지

+

2 내부망 보안 위협 탐지

- ✓ 내부망 악성코드 전파 및 취약점 공격 트래픽
- ✓ C&C IP 및 악성 URL 접속 시도

+

3 자사 제품 연동을 통한 유기적인 대응

- ✓ ICM 연동을 통한 통합 모니터링/분석
- ✓ 방화벽 연동을 통한 세션 차단
- ✓ EPS/MDS 등 엔드포인트 연동을 통한 위협 정보 수집

OT 자산 위협의 통합적인 식별, 탐지 대응

More security, More freedom

AhnLab