ICS 보안 트렌드와 안랩의 ICS 보안 전략

More security,
More freedom

AhnLab 황재훈 부장

AhnLab

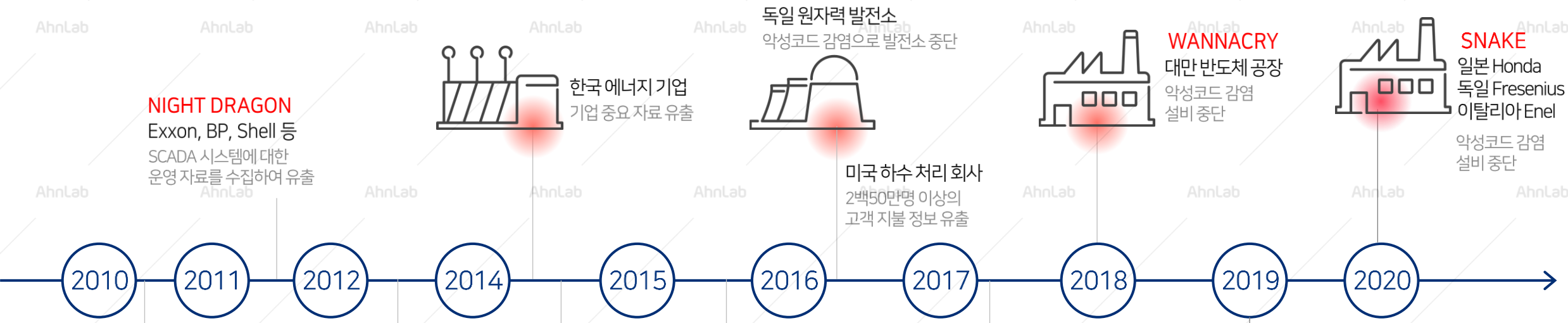
목차

AhnLab

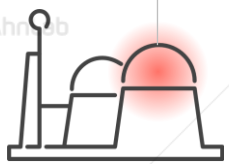
ICS 보안 동향

AhnLab

ICS 보안 사고



2010



이란 원자력 시설
Stuxnet 감염
약 50개 원심 분리기 파괴
STUXNET

2011

NIGHT DRAGON
Exxon, BP, Shell 등
SCADA 시스템에 대한
운영 자료를 수집하여 유출

2012

이란 석유 시설
이란 국영 석유 회사의
중요 자료 유출

사우디 아람코
악성코드 감염으로 인한
석유 생산 차질 발생
SHAMOON

2014

한국 에너지 기업
기업 중요 자료 유출

2015

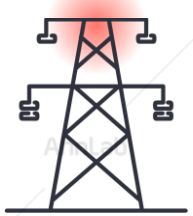
독일 제철소
제어시스템 파괴
HAVEX

2016

독일 원자력 발전소
악성코드 감염으로 발전소 중단

미국 하수 처리 회사
2백50만명 이상의
고객 지불 정보 유출

한국 교통시설
항만, VTS, 지하철 등
교통시설 공격 발생



우크라이나 전력시설
22만 여 가구의 전력 차단
BLACK ENERGY
CRASHOVERRIDE

2017

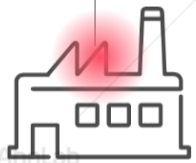
미국 미주리주 도서관
랜섬웨어 감염으로 시스템 정지

미국 달라스 비상사이렌
무선 통신망 해킹으로
비상사이렌이 15시간 동안 오동작

2018

WANNACRY
대만 반도체 공장
악성코드 감염
설비 중단

2019



노르웨이 알루미늄 공장
악성코드 감염으로
생산 중단
LOCKERGOGA

2020

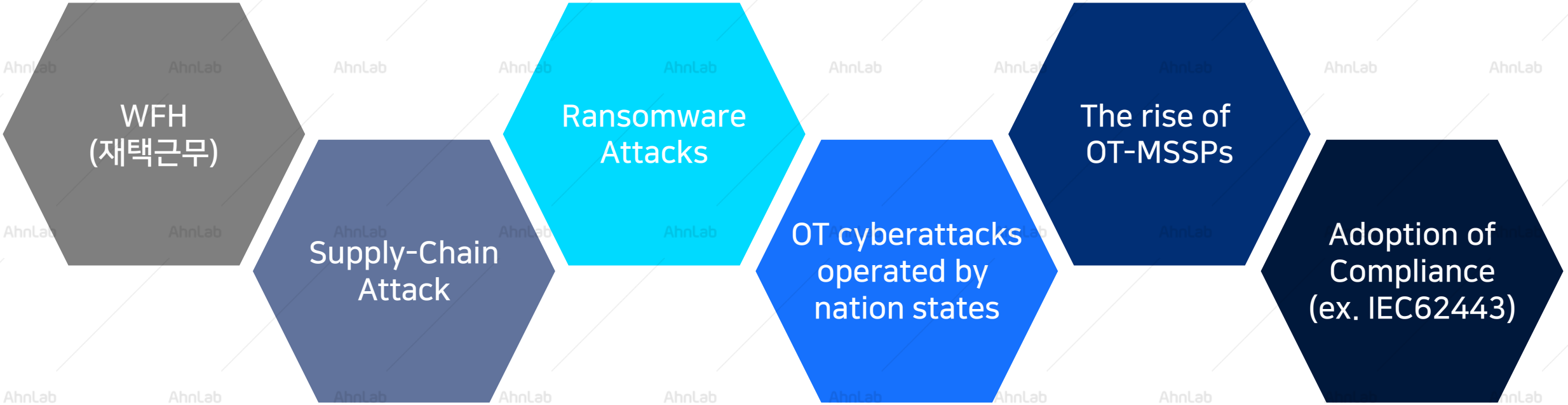
SNAKE
일본 Honda
독일 Fresenius
이탈리아 Enel
악성코드 감염
설비 중단

최근 ICS 보안 주요 이슈

COVID-19로 인한 재택근무
원격 운영 관리 정책, 보안 접근 기술

LockerGoga, Ryuk, Maze, Snake/ekans
► 랜섬웨어 대비 백업 및 대응안 수립, 관제 검토

클라우드 기반 관제 서비스 (ex. KAMP)
► OT 관제에 대한 관심 증가

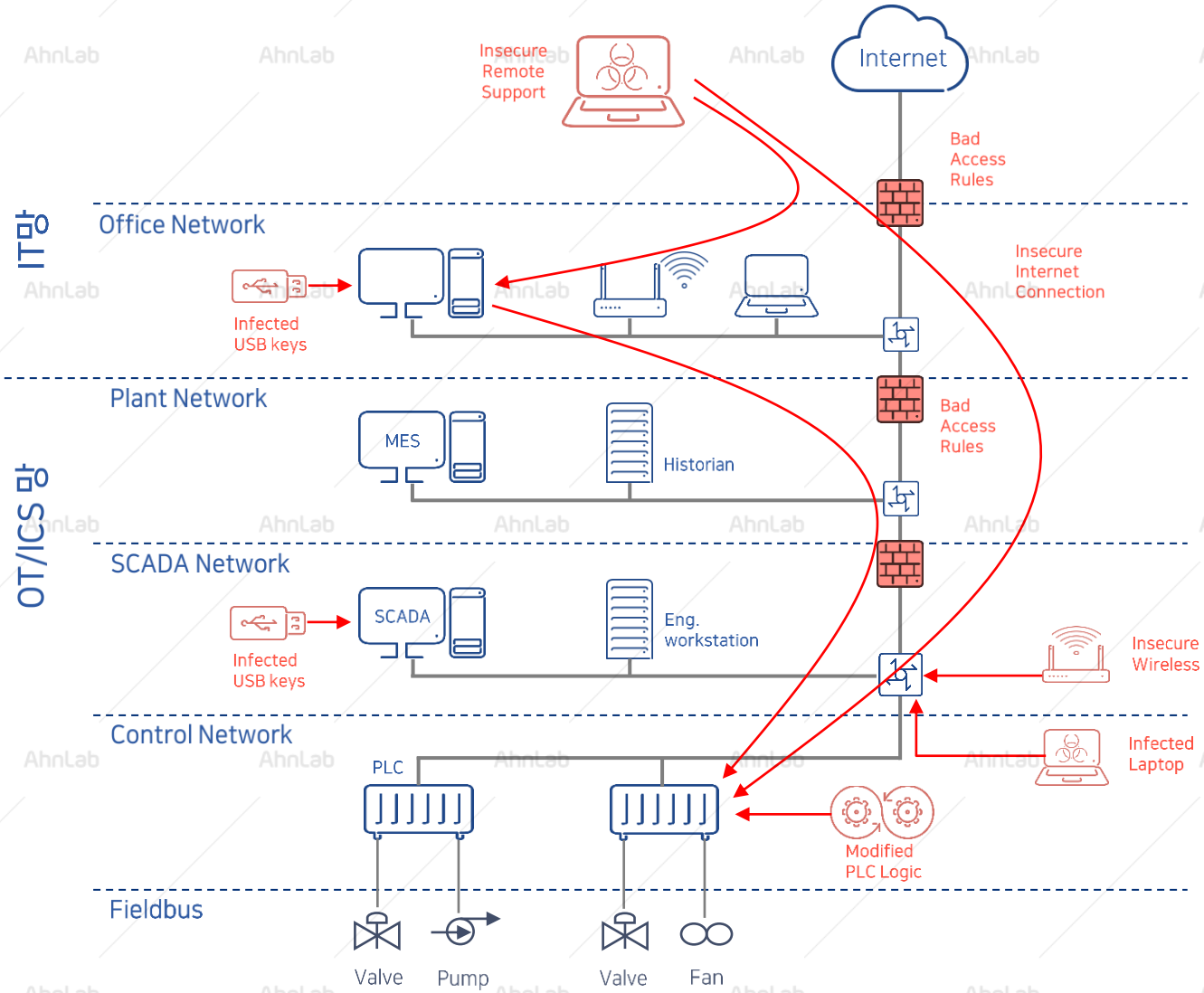


SolarWinds 공급망 공격
► 네트워크 패턴 변화 지속적인 모니터링

아제르바이잔 에너지, 이스라엘 상수도, 이란 원전
► 많은 국가들의 기반 시설 보안 상태가 미비

네트워크 환경 및 내부 위험 평가의
중요성에 대한 인식이 증가할 것으로 예상

ICS 환경의 주요 공격 가능 경로



불안전한 폐쇄망 환경

- **IT/OT 융합시대에 Air-Gap 은 이상적 개념이며 실존 불가**
  - ➢ Inbound/outbound 통신 보안에 취약한 hole 존재
  - ➢ VNC, RDP, SMB 등 위험한 원격 제어/전송 프로토콜 사용

OT망 내부에 Direct로 침투하는 위협

- **실제로 발생하는 가장 위협적인 원인**
  - ➢ USB key : 대만 TSMC, 노르웨이 LockerGoga 사고 등
  - ➢ 3rd Party 유지보수 Laptop의 악성코드 전염

PLC 로직 변조

- **생산성 저하 및 HSE(Health & Safety Execution) 이슈**
  - ➢ 악성코드, 내부 직원의 Human Error에 의한 명령어 로직 변경

ICS 주요 공격 방법 – Mitre ATT&CK for ICS

은밀한 침투	네트워크를 통한 내부 전파			타격	
Initial Access	Execution	Discovery	Lateral Movement	Impair Process Control	Impact
Data Historian 감염	CLI	제어 설비 식별	취약점을 이용한 내부 전파	제어 명령 변조	제어 설비의 손상
Engineering Workstation 감염	API	네트워크 연결 탐색	파일 공유 프로토콜을 이용	제어 로직 변조	가용성 손실
원격 접속을 통한 감염	GUI	네트워크 서비스 검색	자격 증명 악용	데이터 파괴	제어 기능 상실
Supply Chain을 통한 감염	Scripting	네트워크 Sniffing		서비스 중지	정보 유출
Spear phishing	Man in the Middle	원격 시스템 검색		비인가 제어 명령	데이터 손상
이동식 디스크를 통한 감염	User Execution	시리얼 연결 탐색		프로그램 다운로드	

출처 : MITRE ATT&CK for ICS

IT와 OT의 환경적 차이 (1/2)

Skills Gap

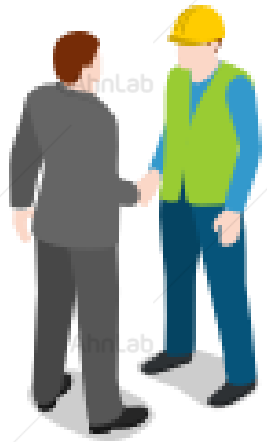
운영 편의성, 사용성 부여 필수적

악성코드/취약점 방어! 도대체 장비 어디 있어요?

IT전문가. 소수 전문 인력

수율 향상 목표! 공정 운영 영향 금지

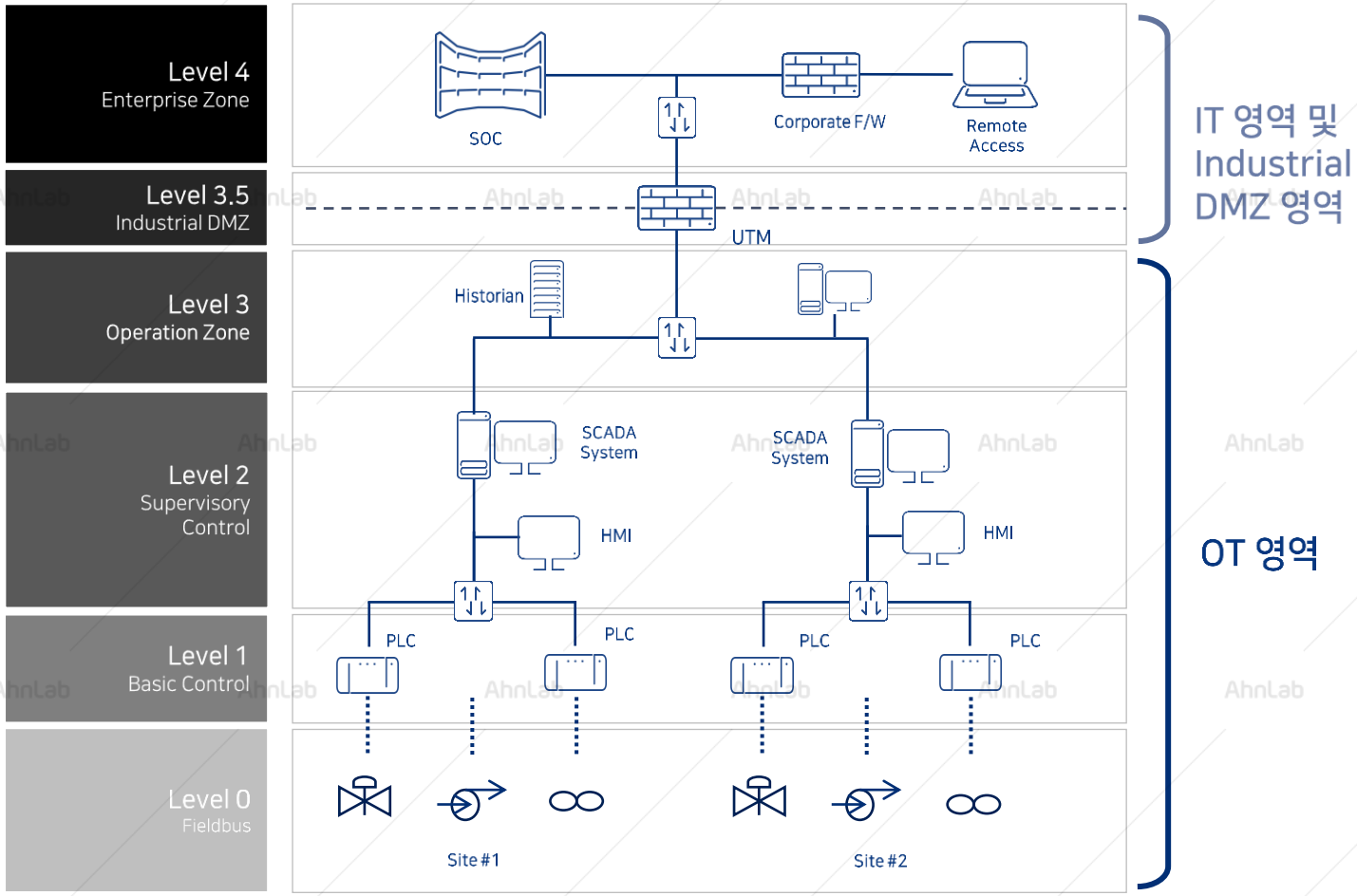
IT는 잘 모름. 난 다른 전문가



	IT	OT
우선순위	C.I.A (기밀성, 무결성, 가용성)	A.I.C (가용성, 무결성, 기밀성)
시간 지연	Acceptable	Critical
시스템 수명	3 - 5년	15 - 25년
통신 프로토콜	TCP/IP	TCP/IP 및 Serial, modbus 등 각종 산업용 프로토콜
시스템 다운타임 (재부팅)	Acceptable	불허
시스템 패치	필수	공정 운영 영향 우선
상대적 기술 이해도	OT 이해 부족	IT보안 이해 부족
Compliance	ISO/IEC 27001 ISMS, CC인증, 보안적합성	ISA/IEC 62443

IT와 OT의 환경적 차이 (2/2)

OT 망 외부의 IT 영역에 대해서는 충분한 보안성과 가시성을 제공하지만, OT망 내부의 보안성과 가시성은 부족하다.



보안 이슈 대응 용이

다양한 솔루션 운영

- 방화벽, IPS, Sandboxing
  Anti-virus 등

신속한 진단/대응 용이

모니터링/관제 운영

- MSSP (NMS, SIEM 등)

보안 이슈 대응

보안 상태 모니터링

보안 이슈 대응 어려움

보안솔루션 부족

- 방화벽 등 최소 운영

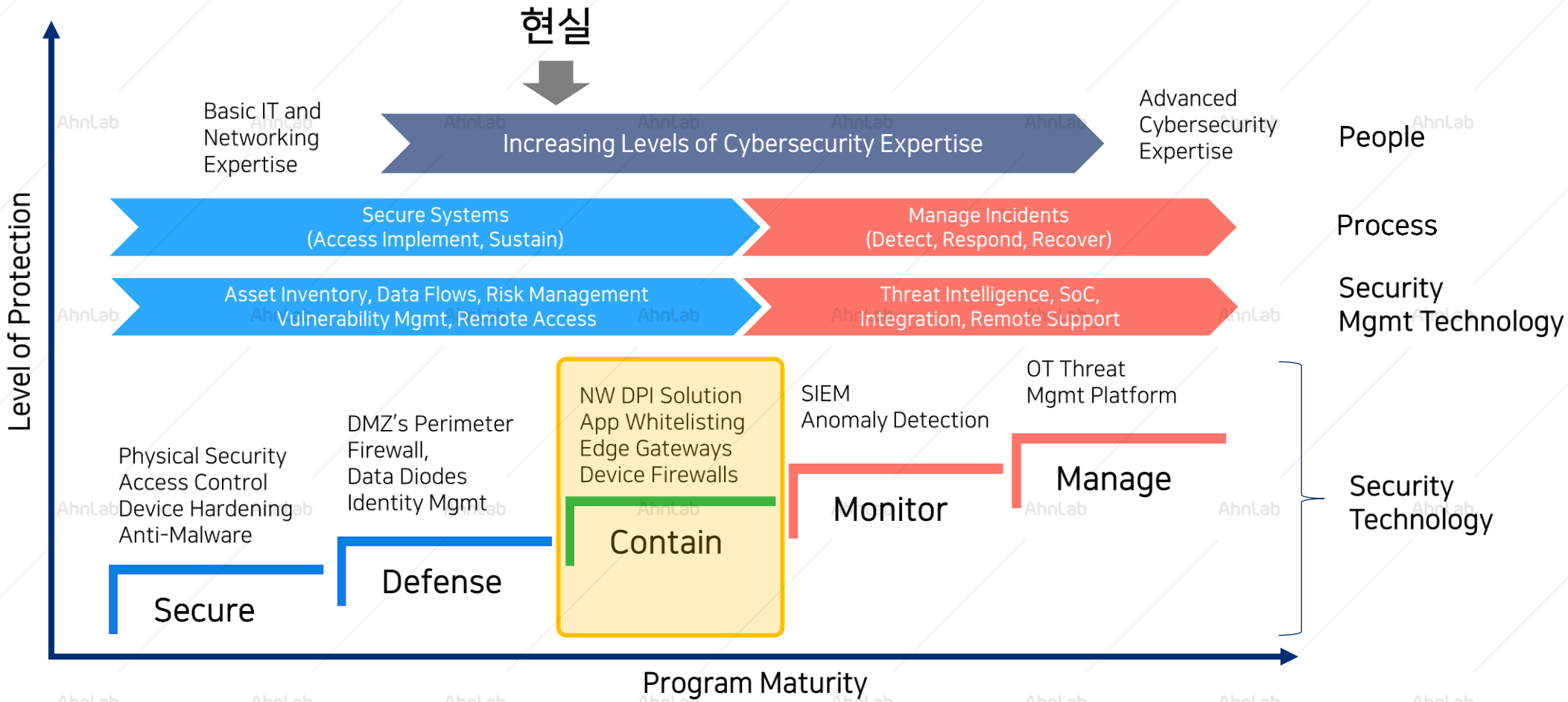
**서비스 문제,
보안 상태 진단 어려움**

보안 모니터링/관제 미비

ICS 보안 성숙도 모델

아직은 기술과 관리 측면의 성숙도가 낮지만, 최근에 점차 향상하는 방향으로 나아가고 있다.

- Device 의 Hardening 측면의 Secure 와 경계/차단 측면의 Defend 의 준비도는 높으나, Contain 측면의 DPI 솔루션 및 App Whitelisting 관심 증가



<출처> https://www.arcweb.com/blog/dragos-platform-combines-continuous-monitoring-rapid-detection-rapid-response

AhnLab의
통합 OT 보안 전략

AhnLab

AhnLab의 통합 OT 보안 전략

IT/OT 융합기술의 시대에 IT보안과 OT보안은 함께 균형을 맞춰야하는 양날개와 같다.

수동적인 탐지와 함께 능동적인 대응도 함께 고려해야 한다.

솔루션 포트폴리오

End-Point 제품
- System Hardening
- Malware Detection

Network 제품
- Segmentation
- Vulnerability Detection

보안 위협 분석 기술

악성코드 탐지
- TS 엔진(V3엔진)
- 다양한 OT Malware 분석

네트워크 취약점
- 다양한 취약점 및 패턴 분석

다양한 OT 레퍼런스

다양한 레퍼런스
- 국내외 굴지의 제조 공장 레퍼런스 다수 보유

Segmentation Firewall
- OT망 경계 방화벽

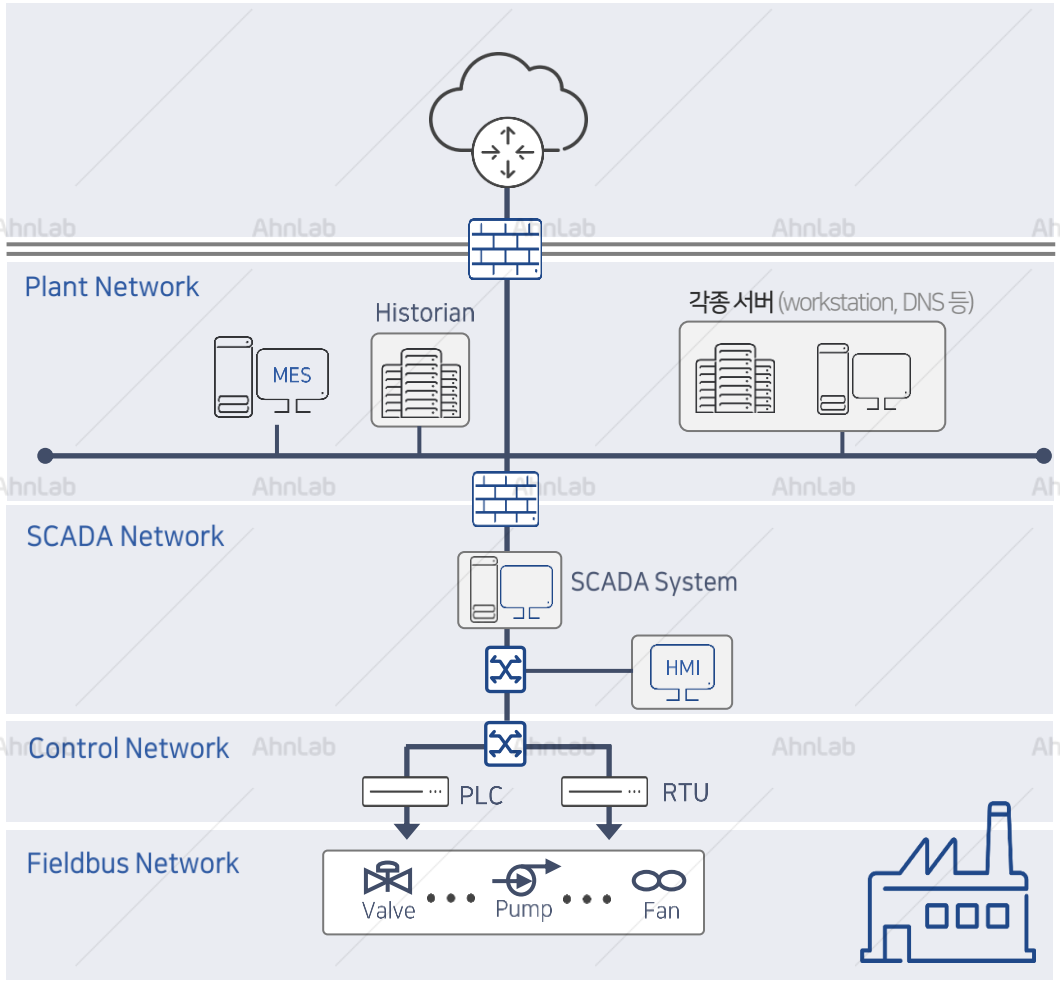
Local 벤더로서 대응

OT 관제
- OT 원격 관제 서비스

제품 기술지원
- 로컬 벤더로서 빠른 대응

AhnLab의 OT 보안 제품 Framework

제어망, 생산망에 Network, Endpoint, Service 영역까지 다양한 포트폴리오를 제공합니다.



IT망(OA 망)

- OT 관제
- Sefinity(SOAR)
- EDR

생산망

- EPS (Lockdown)
- Xcanner (휴대용 AV)
- ICM (OT통합 Mgmt)
- MDS (Sandboxing)
- V3 (Anti-Virus)
- TrusGuard (NGFW)
- PoShield+A (OT-IDS)

제어망

- PoShield+A (OT-IDS)
- Xcanner (휴대용 AV)
- EPS (Lockdown)

포스코ICT와 OT보안 통합 제품

양사 보유 솔루션의 결합과 핵심 역량 공유를 기반으로 국내 스마트팩토리 보안 사업에서 협력 추진

- MOU 체결 : 스마트팩토리 보안 솔루션 공동 사업 추진 ('20년 10월)
- 제품 출시 : 통합OT보안 제품 PoShield+A 출시 ('21년 4월)

AhnLab

- 국내 최대 통합 보안 기업
- 악성코드 탐지 기술 국내외 높은 경쟁력
- 지능형 NW위협 탐지 보안솔루션 보유

포스코ICT

- 스마트팩토리 국내 선도 기업
- AI기반 비정상 제어명령 탐지 솔루션
  - 중공업 분야 최적화 솔루션 등

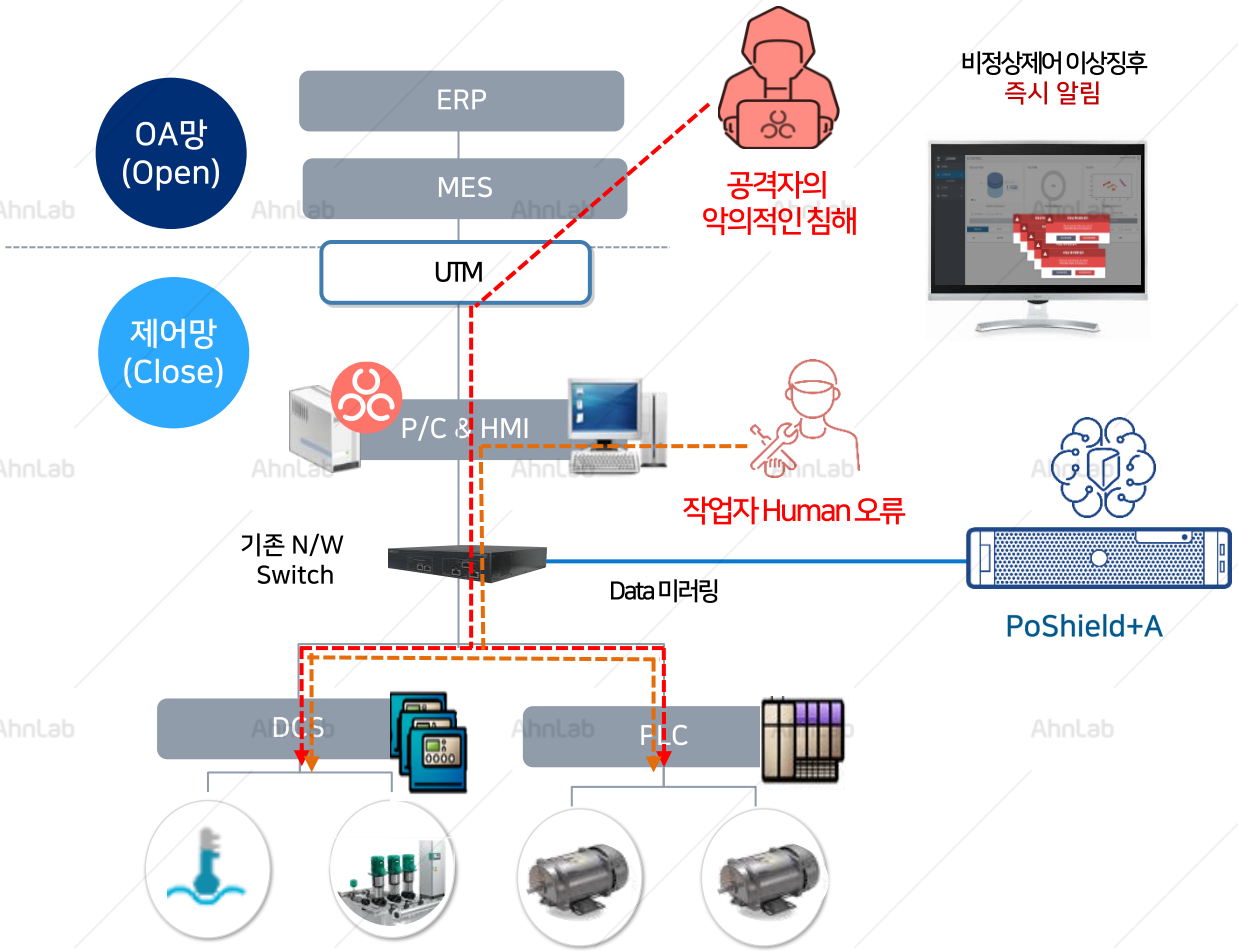
- **Threat Detection + 보안 유관 가시성**
  - Threat Detection : 악성코드, NW취약점
  - 가시성 : Traffic, Application 탐지

- **ICS 제어명령 이상 탐지**
  - AI 기반 : 명령어 + 변수 값 이상 탐지
  - Network Topology (w/ ICS 설비 명)

안랩의 보안 위협 탐지 기술과 포스코ICT의 AI기반 스마트 팩토리 기술의 시너지

PoShield+A - 비정상 제어명령 탐지

스마트팩토리의 제조 공정에 특화된 포스코ICT의 AI 기반 비정상 제어명령(PLC Logic) 탐지



비정상 제어명령 이상 징후 탐지

- 정상 제어 명령 학습을 통한 자동 White List 생성
- 제어명령 위변조 방식의 내·외부 보안 침해 탐지
- 제어 시스템의 비정상적인 Data 전송과 운전자의 Set value 오류 입력에 대한 상시 탐지 및 정보 제공
  - 탐지 속도 : 평균 1초 미만
  - 생산 제품 변경 시 추가 정상 상태에 대하여 반복 학습(White List 보강)

제어명령 송신 상태 및 통계 Data 제공

- 『Process Computer → PLC』間 제어 명령 송신/연결 상태
- 제어명령 송신 통계 Board
  - code 별 전송 주기, 일일 발생 건수 등 Code 관련 통계 수치
  - 이상 탐지 데이터에 대한 이력 로그 조회 및 Report 기능
- 비정상 이상징후 탐지 제어 명령의 오류 변수 항목(위치) 정보

무결성 검사 및 NW 토폴로지 자동 생성

- 주기적 무결성 검사 및 이력관리
- 공정내 NW 토폴로지를 자동으로 생성하고 관리

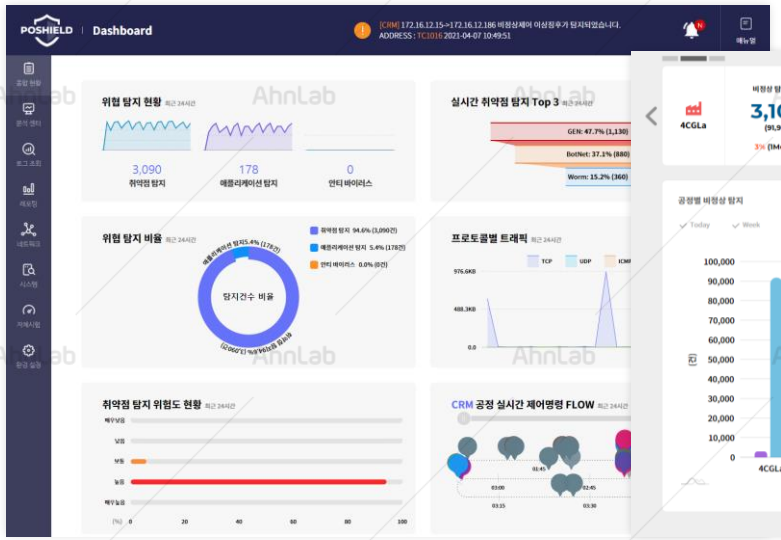
PoShield+A - 주요 기능

비정상 제어명령 탐지 전문 포스코ICT의 PoShield 제품에 안랩 ICS 위협 탐지 제품 AhnLab ITS의 위협 탐지 모듈 적용

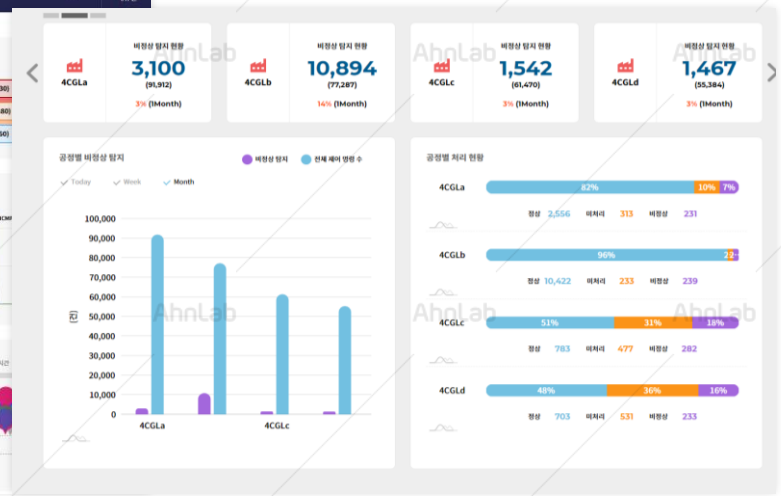
"AhnLab ITS" 탐지 모듈

PoShield+A

기존 "PoShield" SW



보안 위협 탐지(취약점, 악성코드 등)



비정상 제어 명령 탐지

- AI 기반 비정상
- 제어명령 탐지
- 자산 Topology

포스코ICT "PoShield"

- 악성코드 탐지
- NW취약점 탐지
- Application 탐지
- 트래픽 통계

AhnLab ITS 탐지 모듈

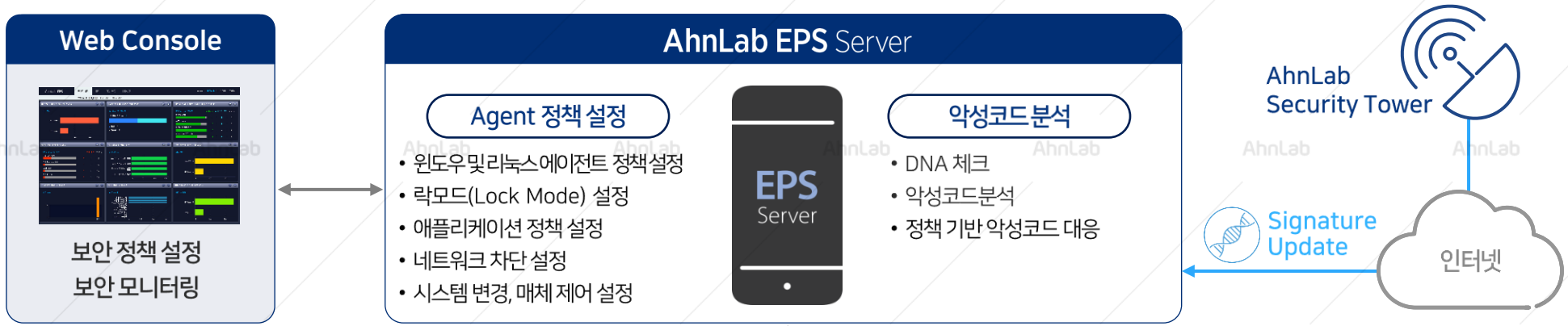
PoShield+A

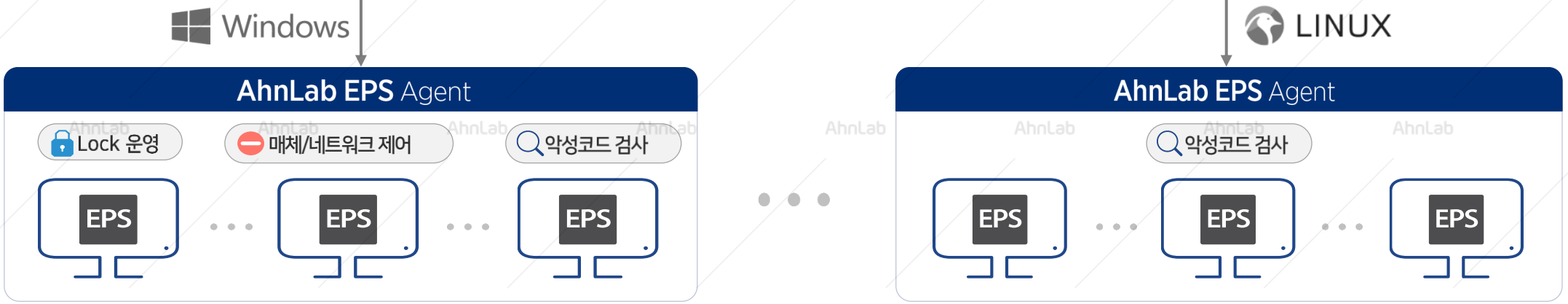
대시보드 | 토폴로지 | 통계/모니터링 | 로그/보고서

AhnLab EPS – 특수 목적 시스템 Application 제어

산업 제어 시스템 등의 특수 목적 시스템의 안정적 운용을 위해 정해진 프로그램만 사용하는 최적화된 전용 보안 솔루션

- 단말 시스템에 설치되는 초경량 에이전트(EPS Agent)와 중앙 모니터링 및 정책 관리 서버(EPS Server)로 구성





AhnLab Xcanner – 휴대용 악성코드 진단 · 치료 SW

악성코드 엔진 최신 업데이트가 불가한 폐쇄망 환경의 시스템 등의 특수 목적 시스템의 악성코드를 수동 진단/치료

- ICS망의 매체제어 정책에 따라 인가된 이동식 매체에 탑재하여 악성코드 검사/치료

AhnLab Xcanner

수동 검사 기반 진단 및 치료

- 기존 설치된 보안 에이전트 삭제 없이 충돌 최소화
- 감염된 시스템에 대한 사후 치료
- 보안 에이전트 설치 전 사전 방역을 위한 시스템 전체 영역 검사
- 검사 시간 단축을 위한 사용자 지정 검사

운용을 위한 다양한 설정

- 운영 상황에 맞게 대응할 수 있는 검사/치료 옵션 설정
- 검사 불필요 항목에 대한 예외 설정(폴더, 파일, 확장자)
- 드라이버 구동 불가 환경을 대비한 바로가기 제공

사용 및 관리 편의성 제공

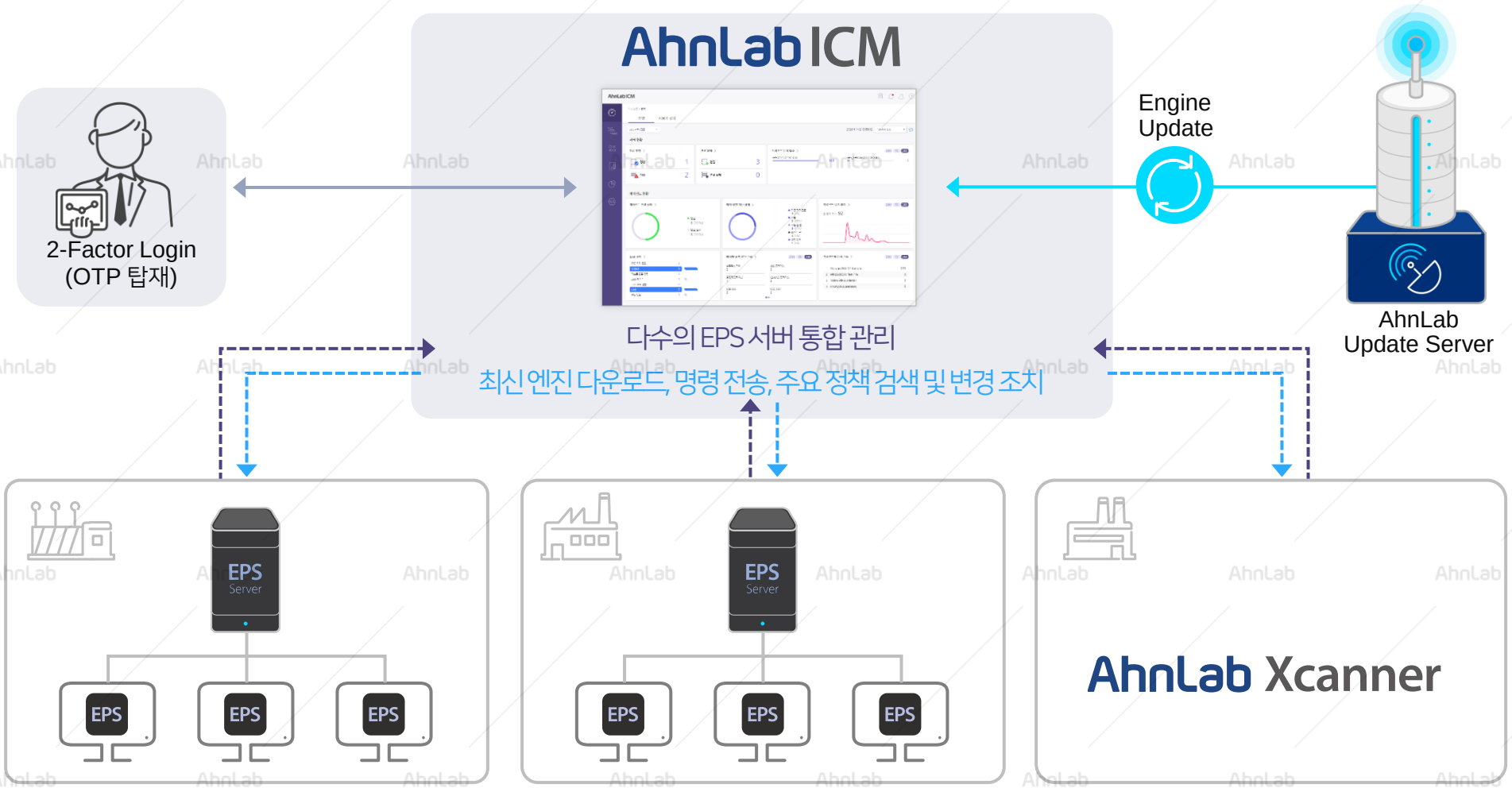
- 검사 후 선택 치료 제공
- 필수 프로그램 감염으로 인한 삭제, 오진 대응을 위한 검역소 기능 제공
- 이벤트 및 진단 로그 기간별, 검색어 조회, 파일 저장

※ 자동 업데이트를 통한 실시간 보호를 위해서는 AhnLab V3 또는 AhnLab EPS를 사용해야 합니다.

AhnLab ICM – OT보안 통합 관리 솔루션

중앙 집중화된 보안을 구성하고 관리하는 중앙 관리 솔루션으로 연동 시스템을 효율적으로 모니터링

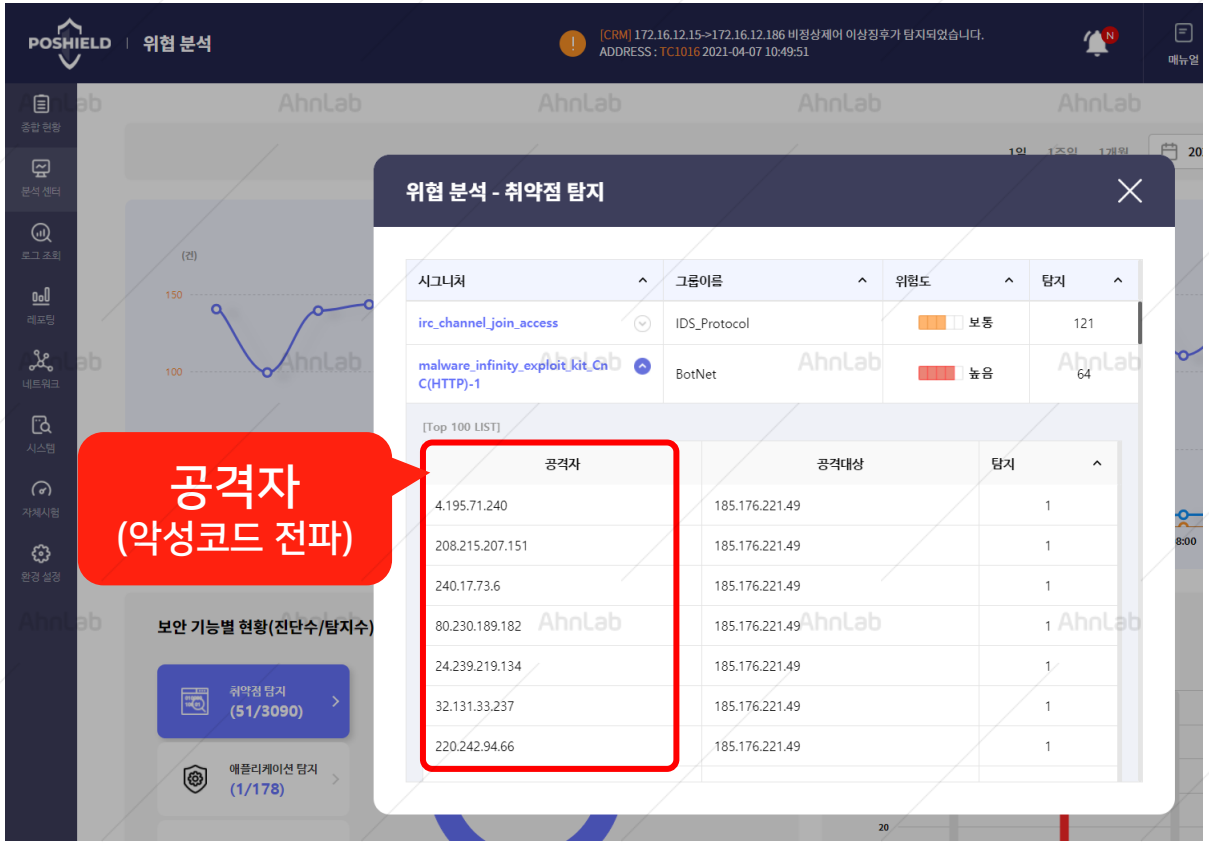
- 다수의 EPS 서버를 관리하고, Xcanner와 MDS의 이벤트에 대한 통합 모니터링 인터페이스 제공

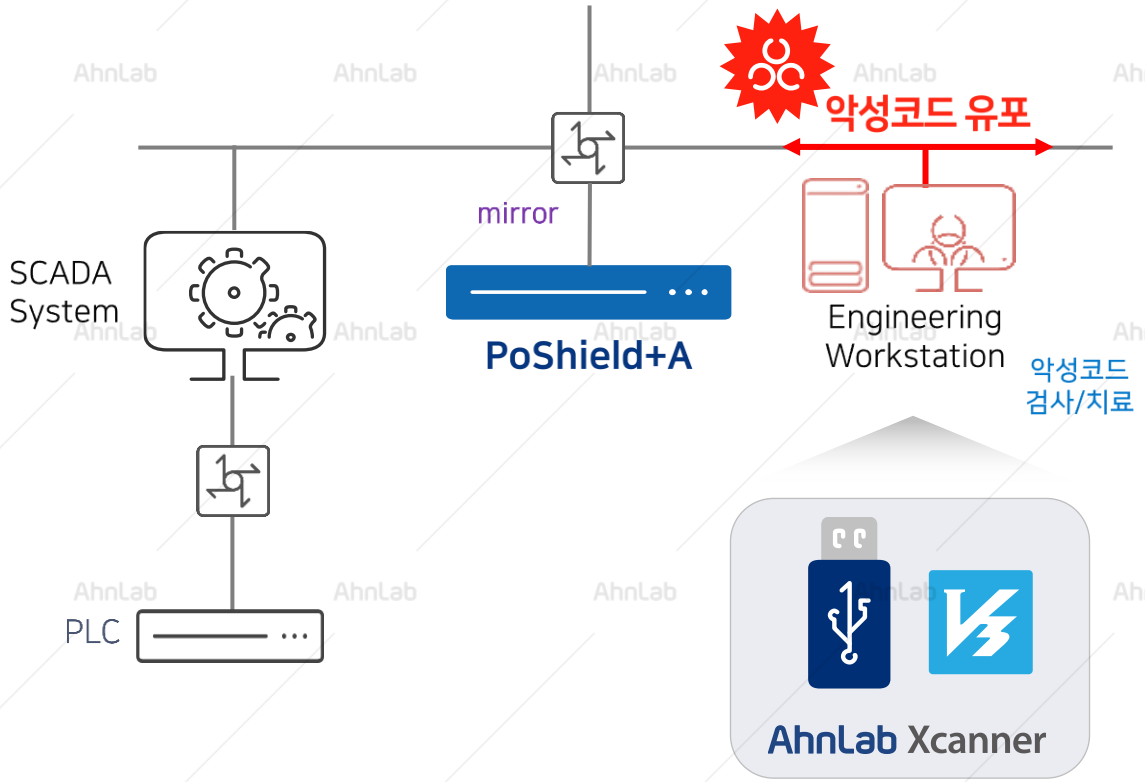


OT 보안 프레임워크 Use Case #1

보안 위협의 탐지/가시성 뿐만 아니라 악성코드 유포지에 대한 검사 제어망에서 탐지

- PoShield+A 에서 탐지한 악성코드 유포 및 취약점 공격 출발지에 대한 악성코드 검사/치료

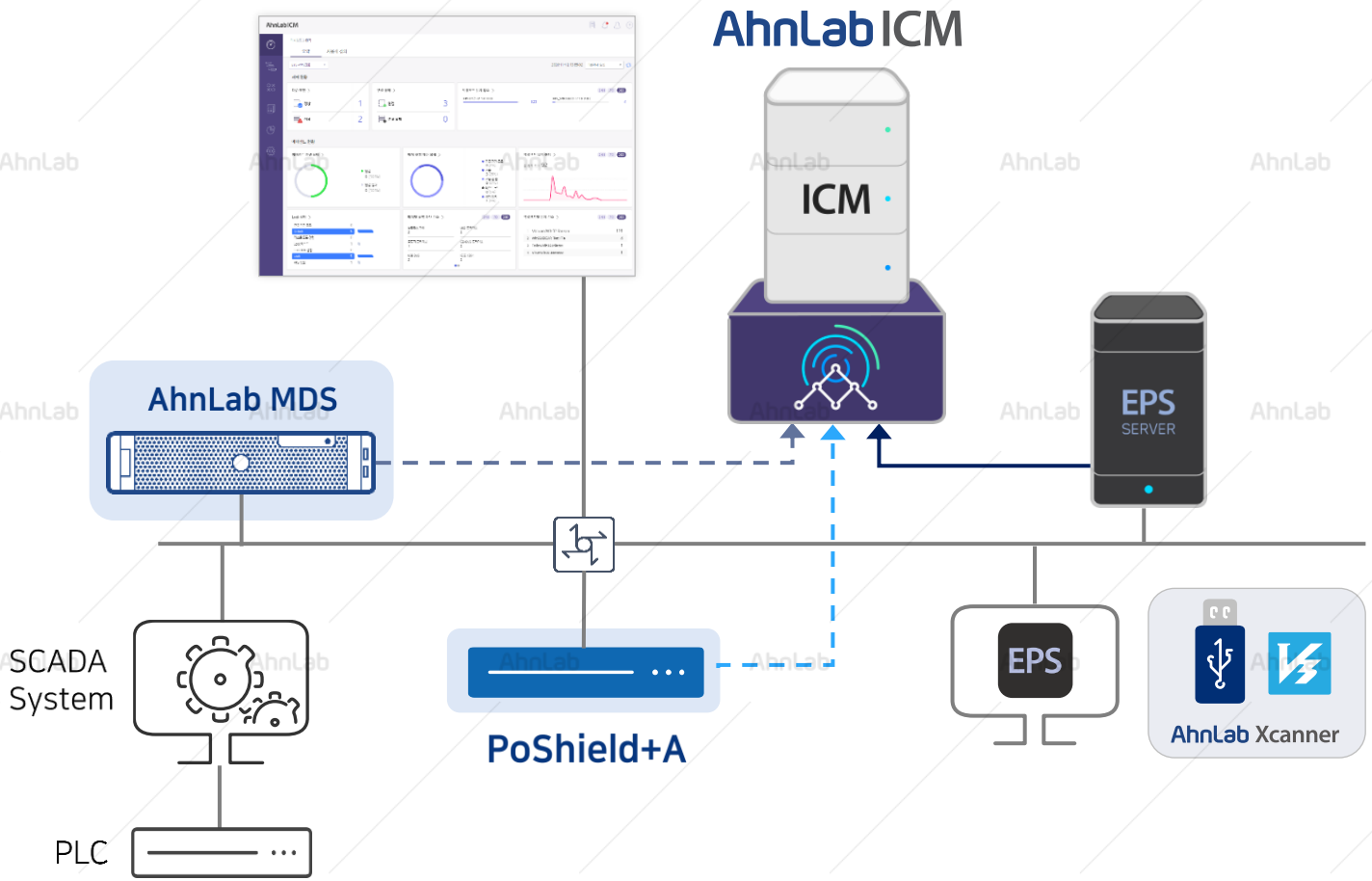




OT 보안 프레임웍 Use Case #2

AhnLab ICM을 중심으로 OT망 내부의 연동 제품의 이벤트 수집, 가시성, 통합 정책관리 제공

- 자사 제품간 연동으로 종합적인 모니터링과 대응을 제공



통합 이벤트 수집

- ICM이 EPS 및 Xcanner 에서 발생하는 이벤트 수집
- MDS 및 Poshield+A의 이벤트 수집 확장 진행중

통합 모니터링 & 가시성

- 수집된 이벤트에 대한 통합 모니터링
- 탐지 정보 및 각종 가시성 정보 제공

통합 정책 관리

- 다수의 EPS에 대한 통합 보안 정책 설정

※ AhnLab ICM 은 지속적으로 ICS 제품의 로그 수집과 모니터링의 범위를 넓혀가고 있습니다.

More security, More freedom

AhnLab