AhnLab

White Paper

CPS 환경에 '통합 보안'이 필요한 이유

IT, OT, 그리고 CPS 이해하기

이제 조직들에게 IT(Information Technology)는 굉장히 익숙한 개념이다. 그리고, OT(Operation Technology)에 대해서도 어느 정도의 이해도를 갖춰가는 가운데, CPS (Cyber-Physical System)이라는 개념이 등장했다. 이들에 대한 정의는 어떻게 될까? 서로 어떤 연관성을 갖추고 있을까? 또, 효과적인 통합 보안 전략은 무엇일까?

먼저, OT는 산업의 운영기술 환경으로, 산업제어시스템(Industrial Control System: ICS) 등 광범위한 영역을 일컫는다. 그 연장선에서, OT 보안은 OT 환경을 보호하는 행위나 체계를 일컫는다.

이어서, IT 보안과 OT 보안의 개념적 차이에 대해 이해할 필요가 있다. 기본적인 해답은 단어 자체에 포함되어 있다. IT 보안은 '정보(Information)'에 초점을 두는 반면, OT 보안은 '운영(Operation)'에 초점을 둔다. 단순히 보기에는 크게 다르지 않을 수 있지만, 이러한 본질의 차이는 근본적인 접근법을 다르게 한다.

보안의 3가지 속성 측면에서 IT와 OT 보안을 살펴보자. 보안의 3가지 속성은 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이다. 3가지 모두 보안에서 필수적으로 충족되어야 하는 요소이지만, 우선순위를 나눠볼 수는 있다.

통상적으로 IT 보안에서는 기밀성을 가장 우선시 하며, 무결성과 가용성 순으로 중요도를 보고 있다. 이를 영문 약자로는 'C.I.A'라 한다. OT 보안은 우선순위가 조금 다르다. 가용성을 보장하는 것이 가장 중요하고, 무결성과 기밀성 순으로 우선순위가 정립된다. 영문 약자로는 'A.I.C'로 볼 수 있다. 그럼 왜 이와 같은 차이가 있는 것일까? 이유는 생각보다 간단하다. 컴퓨터는 재부팅하면 되지만 공장 설비는 안정성이 최우선이고 절대 멈춰서는 안되기 때문이다.

IT와 OT 환경은 구성되는 기기에도 차이가 있다. IT 환경은 잘 알려진대로 PC, 노트북, 모바일, 서버 등의 IT 기기로 구성된다. 반면, OT 환경은 기존 IT 기기에 산업제어시스템(Industrial Control System: ICS)이 추가된다. 산업제어 설비는 대표적으로 PLC(Programmable Logic Controller)를 꼽을 수 있다. PLC는 쉽게 설명하면 펌프, 밸브, 로봇 팔 등 공장 내 기기에 제어 명령을 내리는 설비다. 사용 연한에도 차이가 있는데, IT 기기의 수명은 약 3~4년으로 짧은 반면, OT 기기는 20~25년 정도 오래 사용하는 경향이 있다.

종합하면, IT와 OT 환경에는 본질적인 차이가 존재하며, 이는 IT망과 OT망을 나누는 이유이기도 하다. 그 동안, OT 영역은 외부에서의 접근이 엄격히 통제되는 환경의 폐쇄성으로 인해 보안의 중요성이 상대적으로 덜 부각되었다. 하지만, 디지털화가 빠르게 진행되고 IT 영역과의 접점이 늘어나면서 OT 환경을 노리는 공격이 증가하고 있고, 피해 규모 역시 커지고 있는 상황이다.

이제 조직들은 (최소) IT와 OT를 연계한 통합 보안 전략을 바탕으로 비즈니스를 보호해야 한다. 바로 'CPS 보안'이라는 개념이 탄생한 배경이다.

CPS는 OT, IT, IoT, 클라우드 등 폭 넓은 영역의 사이버(cyber) 및 물리(physical) 요소들을 아우르는 개념이다. 기존 제조업을 넘어 스마트 팩토리, 메디컬 시스템, 자율주행차 등 다양한 활용 사례(use case)들을 포괄한다. 여러 영역들이 포함된 CPS를 보호하기 위해서는 시스템 가용성을 보장하는 가운데, 다양한 보안 모듈에 대한 통합 관리를 통해 보안 효율성을 확보해야 하며, 자산에 대한 폭 넓은 가시성도 갖춰야 한다.

침해 사례

기존 OT 환경은 10년 혹은 그 이상 운영하고 노후화된 운영체제를 사용하는 경우가 많으며, 패치가 미흡해 취약점이 다수 존재한다. 사이버 공격으로 인한 피해가 쉽게 확산될 수 있는 이유이기도 하다. 이로 인해 CPS 환경과 비즈니스 전체가 위험에 빠질 수 있다.

최근 주요 CPS 보안 사고를 보면, 공격은 제조업에 집중되고 있으며, 발전, 에너지 등 사회기반 시설을 노리기도 한다. OT 환경을 향한 공격의 형태를 보면 크게 두 가지로 분류할 수 있다. 첫째는 IT 환경의 공격 기법을 OT 환경에 적용하는 것이다. IT 환경만큼 OT 환경에서도 랜섬웨어 감염이 증가하는 추세를 보이고 있으며, 미흡한 내부 시스템 보안 패치로 인해 잔존하는 취약점을 악용한 악성코드 감염 사례도 많다. 또 하나는 제어명령을 변조해 공정 자체를 타격해 피해를 입히는 것이다. 각 공격 형태의 대표적인 사례들을 하나씩 살펴보자.

우선, 2019년 대만 반도체 기업 TSMC의 워너크라이(WannaCry) 랜섬웨어 감염사례가 있다. TSMC는 해당 사고로 인해 48 시간 가량 공장 가동이 중단되었고, 상당한 금전적 손해를 입은 바 있다. TSMC의 랜섬웨어 감염은 OT망 내부 설비에 감염된 USB를 사용하면서 시작되었고, '이터널 블루(Eternal Blue)' SMB 취약점을 통해 빠르게 확산되었다. 해당 공장과 연결된 해외 다른 공장까지 랜섬웨어가 전파되며 피해가 커졌다.

다음은 미국 플로리다 주의 도시 올즈마(Oldsmar) 수처리 시설 해킹사건이다. 공격자는 취약점을 통해 시설 관리자가 방문할 만한 웹사이트에 악성코드를 심었고, 업무망 시스템에 침투하여 계정 정보와 제어설비 연결 정보를 탈취했다. 이후, 원격 접속 프로그램 팀뷰어(TeamViewer)를 통해 물의 수산화 나트륨 농도를 조작하려 했으나, 다행히 모니터링 중이던 관리자가 마우스의 이상한 움직임을 포착하여 공격을 막아냈다. 하지만, 자칫 수 만명 시민의 식수를 '양잿물'로 바꾸는 대형 테러로 연결될 뻔한 사건이었다.

CPS 위협 이해하기

CPS를 향한 공격은 OT 시스템의 외부 노출이 확대됨에 따라 점차 복잡해지고 있다. 다만, 이를 쉽게 풀어보면 CPS 환경 전체를 공격하기 위해 IT(혹은 외부) 네트워크, 자산 및 공격 방법을 활용하여 OT 시스템을 침해하는 것으로 이해해볼 수 있다.

이 관점에서, CPS를 노리는 공격은 크게 ▲IT망 ▲원격 제어 프로그램 ▲스토리지 디바이스 ▲써드파티 접근 ▲공급망을 통해 일어나곤 한다.

1. IT망

OT망은 보통 외부와 인터넷 연결이 단절되어 있어 직접적인 공격은 쉽지 않다. 하지만, IT망과 연결된 OT망 내 시스템은 IT망을 통해 악성코드가 유입될 수 있다. 공격자는 OT망을 직접 공격하지 않고 IT망을 통해 OT망 공격을 시도한다. OT망 시스템도 IT망에서 사용하는 일반적인 윈도우나 리눅스를 사용하는 경우가 많기 때문에, 악성코드가 IT 환경과 동일하게 사용될 수 있다. 또한, 온전치 않은 네트워크 세그멘테이션도 OT 환경 공격의 빌미가 된다.

2. 원격 제어 프로그램

많은 OT 설비들이 원격 제어 프로그램에 의해 관리된다. 공격자들이 이 프로그램들을 제어할 수 있게 되면, OT 시스템을 쉽게 침해하거나 조작할 수 있다. 따라서, 조직들은 해당 프로그램의 크리덴셜 정보들이 탈취당하지 않도록 각별히 주의해야 한다.

3. 스토리지 디바이스

OT 시스템을 USB 등 스토리지 디바이스로 직접 연결하는 경우가 많다. 원칙적으로 유지 보수 담당자가 생산 라인 시스템에 연결되는 저장 매체를 백신 프로그램으로 검사하고 반입해야 한다. 하지만, 이를 제대로 확인하지 않고 저장 매체를 사용할 때 웜이나 랜섬웨어와 같은 악성코드에 감염되기도 하고, 저장매체가 내부의 취약한 시스템으로부터 감염되어 다른 시스템에 연결할 때 전파되기도 한다. 심한 경우 대만 TSMC 사례와 같이 자체 전파 기능을 가진 랜섬웨어에 감염되면서 생산 라인이 중단되기도 한다.

4. 써드파티 접근

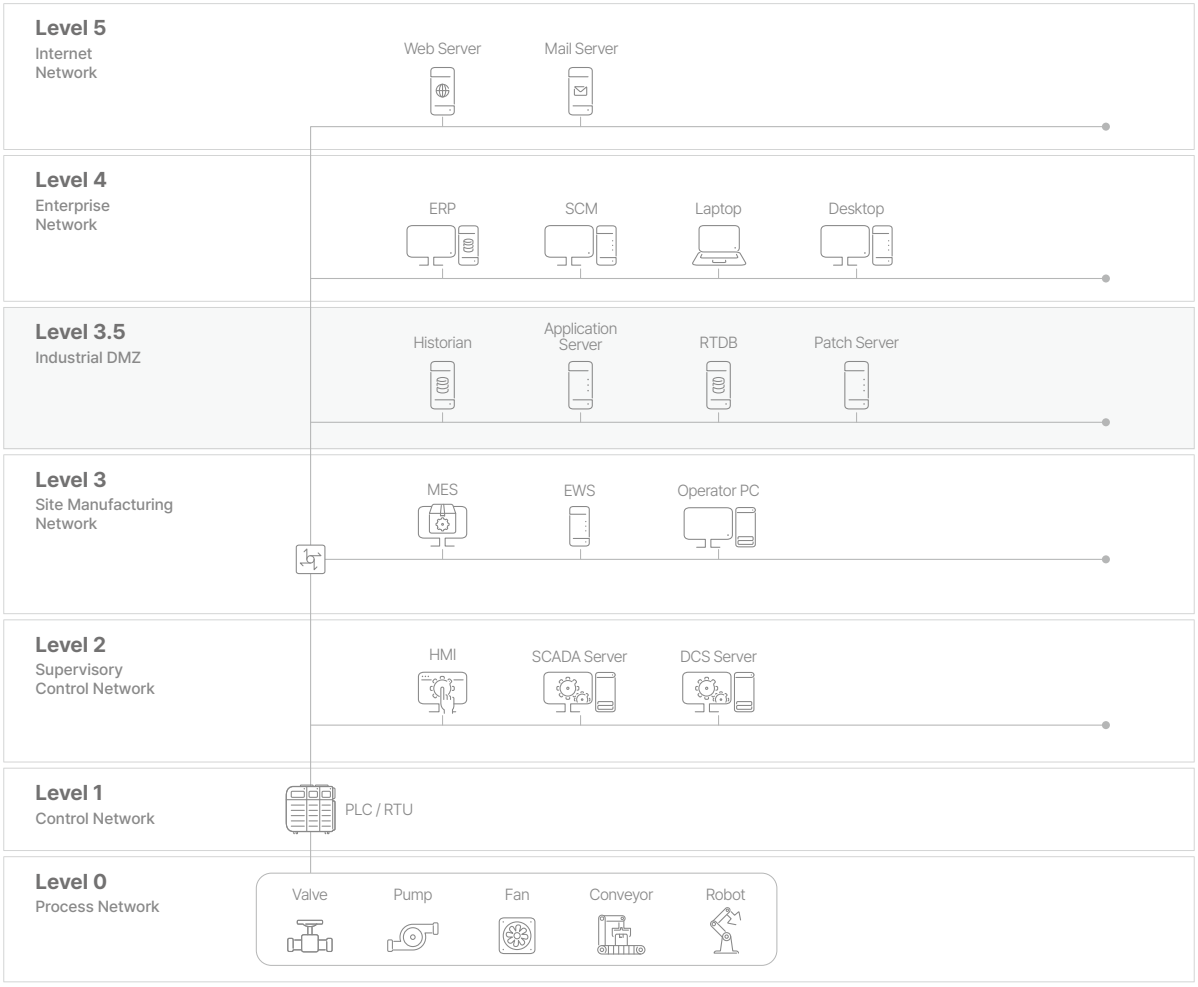
유지보수 등을 수행하는 협력 업체는 OT망 내 시스템에 직접 접근하는 경우가 많다. 공격자가 협력 업체에서 사용하는 저장 매체 등에 악성코드를 삽입하면 내부 시스템에 바로 침투할 수 있다.

5. 공급망

OT망 내에서 운영되는 시스템은 전문 제작업체에서 제공한다. 공격자는 이들 회사를 공격해 제작되는 프로그램에 악성코드를 포함시키거나 악성코드가 담긴 설치파일로 교체하기도 한다. 2013년 발견된 'Havex 악성코드'는 OT망에서 운영되는 소프트웨어 제작자 사이트를 해킹해 설치파일에 악성코드를 심은 대표적인 케이스다. 이처럼, 공급망에서 제공되는 소프트웨어에 악성코드가 포함되어 있을 경우 감염 사실을 알기 어렵다.

CPS 아키텍처

효과적인 CPS 보안 전략을 수립하기 위해서는 먼저 CPS의 구조를 제대로 이해해야 한다. 이에 관해, OT 계층을 Level 0부터 5까지 세분화하는 '퍼듀 모델(purdue model)'은 OT 보안 아키텍처를 구성하는데 있어 표준으로 널리 받아들여지고 있다. 물론, 먼 미래의 CPS는 퍼듀 모델을 넘어선 접근이 필요할 것으로 예상되지만, IT와 OT를 연계한 보안 요구사항을 해결한다는 관점에서 퍼듀 모델은 현재, 그리고 가까운 미래의 CPS 보안에 있어 여전히 효과적인 모델이다.



[그림 1] 퍼듀 모델

Level 0: Process Network – 현장에서 운영되는 설비들이 있는 계층이다. 밸브, 펌프, 컨베이어, 로봇 등 생산 설비, 장치들의 데이터를 수집하는 센서(sensor), 개폐 장치와 같이 1계층의 명령을 받아 동작하는 액추에이터(Actuator) 등으로 구성된다.

Level 1: Control Network – 1계층은 2계층에서 내려오는 명령을 처리하고 0계층으로 보낸다. 또, 0계층에서 수집된 정보와 데이터를 2계층으로 올려 보내기도 한다. 대표적인 장치로는 서두에 소개한, 현장 설비에 명령을 내리고 통제하는 PLC(Programmable Logic Controller), RTU(Remote Terminal Unit) 등이 있다.

Level 2: Supervisory Control Network – 2계층은 현장 설비들을 원격으로 관리하고 운영하는 시스템들로 구성되어 있다. 주요 시스템으로는 SCADA(Supervisory Control And Data Acquisition)와 HMI(Human Machine Interface)가 있다. SCADA는 현장 데이터를 1계층 PLC와 RTU를 통해 수집하고, 여러 현장 장치들을 한 번에 제어한다. HMI는 관리자가 공정 과정 특정 영역의 디바이스를 제어할 수 있도록 해준다.

Level 3: Site Manufacturing Network – 3계층은 전체적인 생산 체계를 관리하고 운영 효율성을 더한다. 해당 계층은 생산 활동 전반을 최적화하는 MES(Manufacturing Execution System), 기기 제어를 위한 EWS(Engineering Workstation), 제품 수명 주기를 관리하는 PLM(Product Lifecycle Management) 등으로 구성된다. 또한, 메인 HMI를 호스팅해 시설 전체를 관리한다.

Level 3.5: Industrial DMZ – 산업용 DMZ라고도 불리는 이 계층은 OT 환경과 외부 IT 환경이 연결되는 지점이다. 센서 데이터를 저장하는 RTDB(Real-Time Database)와 Historian, 애플리케이션 서버 및 패치 서버 등이 Level 3.5에 속한다. OT 보안 침해사고가 증가하고, 이후 설명할 IT-OT 융합보안의 중요성이 부각되면서 주목받고 있는 계층이다.

Level 4: Enterprise Network – 자원관리(ERP), 공급망관리(SCM), 고객관계관리(CRM) 등 기업이 일반적으로 IT 환경에서 사용하는 자원들로 구성된다. 공정과 관련된 전사적 비즈니스를 관리한다.

Level 5: Internet Network – 5계층은 인터넷 혹은 외부 환경과 일선에 맞닿는 자산들이 있는 계층이다. 설비로는 웹 서버, 메일 서버 등이 있다.

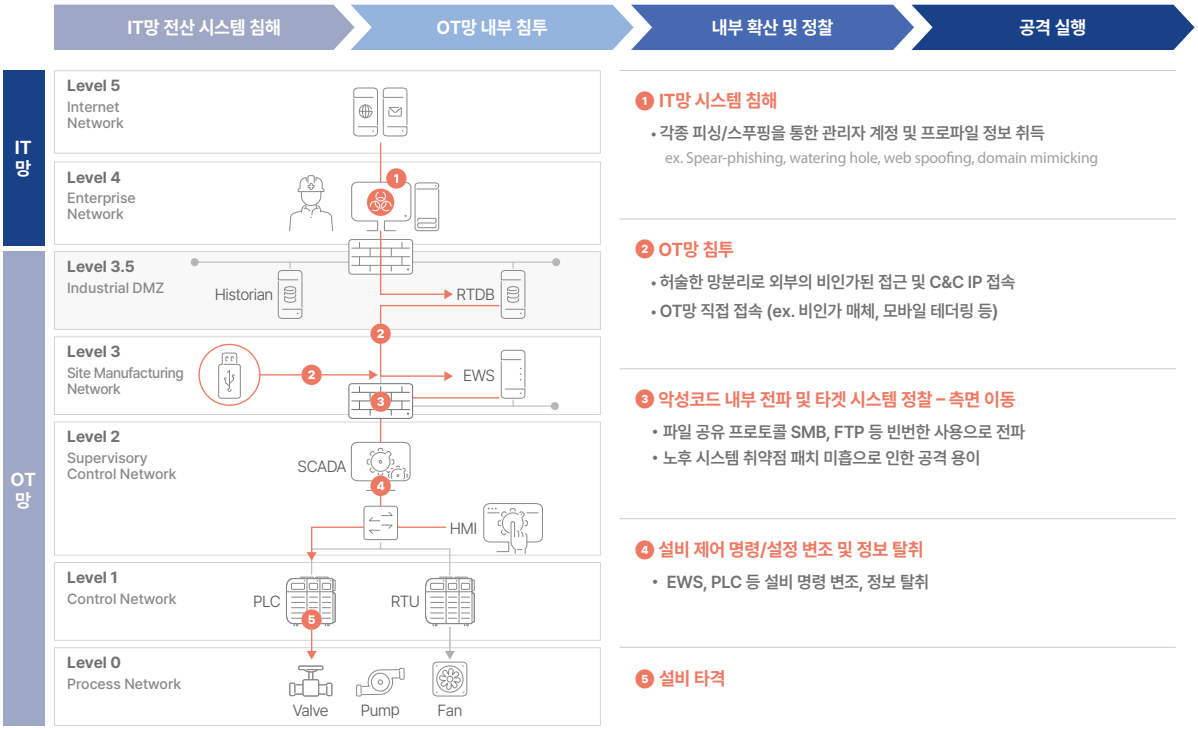
CPS 공격 전개 과정

보안 관점에서 보면, 앞서 살펴본 Level 0~5를 네트워크 망을 기준으로 다음과 같이 구분할 수 있다. 크게 보면 IT망(Level 4~5)과 OT망(Level 0~3.5)이 있고, OT망은 다시 제어망(Level 0~2)과 운영망(Level 3~3.5)로 나뉜다. 다음은 OT 환경의 계층과 네트워크 망 별 구조와 구성요소를 종합해 정리한 것이다.

Level	구분	주요 구성요소	설명
0	제어망(OT)	· Sensors · Actuators · Production devices	현장에서 작업을 수행하는 설비
1		· PLC · RTU	현장 설비에 명령을 내리고 통제
2		· SCADA · HMI · DCS	현장 설비를 원격 관리하고 운영하는 시스템
3	운영망 (OT)	· MES · PLM	전체적인 생산 체계 관리 및 운영
3.5	DMZ	· RTBD · Historian · Application servers	OT와 IT 영역의 접점 혹은 완충지대
4	기업 네트워크 (IT)	· ERP · SCM · CRM	공정과 관련된 전사적 비즈니스 관리
5	인터넷 네트워크 (IT)	· Web servers · Mail Servers	외부 네트워크와 맞닿는 자산

[표 1] 네트워크 계층 별 구성요소 및 역할

위 내용을 토대로 CPS 환경을 침해하는 최신 공격의 흐름도를 살펴보자.



[그림 2] CPS 공격 전개 과정

다시 한 번 복기해보면, CPS 공격은 IT 환경에서 시작되는 경우가 많다. OT망에 비인가 매체를 곧바로 연결하는 경우도 있지만, 대부분은 IT망 시스템이 침해된 후 OT망으로 연결된다. OT 환경은 일반적으로 폐쇄망이고, 에어갭(Air-Gap)을 통한 망분리와 네트워크 세그멘테이션(Segmentation)으로 구성되어 공격 표면(Attack Surface)이 제한적이다. 다만, OT 환경은 IT망 관리자 시스템과 연결되어 있어, IT망 시스템이 먼저 보안 위협에 노출되면 OT망 시스템의 네트워크 연결 정보와 계정 정보가 공격자에게 탈취당할 수 있다.

과정을 살펴보면, 공격자는 OT망을 관리하는 IT망 시스템을 피싱이나, 지능형지속위협(Advanced Persistent Threat: APT)과 같은 다양한 기법으로 침투한다. 이후, OT망 시스템 접속을 위한 관리자 계정과 IP, URL 등 다양한 프로파일 정보들을 탈취한다. 이후, 허술한 망분리 정책이나 관리가 미흡한 지점을 포착해 OT망으로 침입한다. 이 밖에, 보안 관리가 되지 않은 USB를 통해서도 OT망에 악성코드가 전파될 수 있으며, 모바일 테더링을 통해 비인가된 노트북을 설비에 직접 연결할 경우에도, OT망 경계 보안을 우회한 악성코드가 침투할 수 있다.

이후 공격 작업은 공격자 입장에서 수월한 편이다. 공격 타깃 시스템을 탐지해 악성코드를 전파하는데, OT 환경의 업무 특성상 SMB 포트, 원격 파일 전송, 원격 접속을 빈번하게 사용하고, 패치가 미흡한 노후화 시스템이 많은 관계로 빠르게 확산된다. 이후, SCADA나 HMI와 같은 운영 시스템에 연결하여, EWS 혹은 PLC를 통해 비정상적인 제어 명령을 내리거나 설비 설정을 조작하는 등 운영에 직접적인 타격을 가한다.

지금까지 CPS 공격의 전개 과정을 알아봤다. 거듭 강조하지만, CPS 보안을 위해서는 OT 보안을 넘어 IT와 OT를 연계한 통합 보안 전략이 필요하다.

CPS 보안 요구사항과 통합 보안 접근법

CPS 보안은 기본적으로 '식별 > 탐지 > 대응' 프로세스가 요구된다. OT 영역 뿐만 아니라, IT와 OT의 접점, 그리고 IT 영역까지 아우르는 'IT & OT 융합보안' 체계를 갖춰야 한다는 사실을 유념해야 한다. IT & OT 융합보안은 '식별 > 탐지 > 대응' 프로세스에 따라 엔드포인트, 네트워크, ICS 보안까지 두루 갖춰야 한다. 다음은 전체 프로세스와 보안영역 별 요구사항을 정리한 내용이다.

[그림 3] CPS 보안 프로세스 및 보안영역 별 요구사항

A. 식별

CPS 보안에서 '식별'이라 함은 운영 중인 자산과 관련 정보에 대한 투명한 '가시성' 확보를 의미한다. CPS 환경에서 가시성이 필요한 이유는 효율적인 보안을 위한 근간이 되기 때문이다. OT망에는 다양한 자산들이 존재하고 사용 연한도 길기 때문에 자산의 위치, 상태, 네트워크 통신 등을 종합적으로 관리하기가 쉽지 않다. 따라서, 각 자산이 정확히 식별되지 않으면, 보안 위협이나 가용성을 침해하는 설비 오동작을 탐지하고 대응하기 어렵다.

가시성의 기준은 자산 관점과 네트워크 관점으로 구분할 수 있다. 자산 관점에서는 제어망의 각종 설비들과 운영망의 다양한 서버나 워크스테이션으로 구분할 수 있고, 네트워크 관점에서는 각 자산 간 맺고 있는 네트워크 세션과 이들이 사용하는 다양한 IT/OT 애플리케이션 프로토콜을 들 수 있다.

OT망의 환경적 특성상 IT 환경보다 자산이나 네트워크의 변화가 빈번하지 않기 때문에 식별된 요소들을 베이스라인으로 삼고 식별되지 않은 보안 위협과 이상 행위를 탐지하면 된다.

OT망 네트워크를 기준으로 제어망부터 살펴보면, 자산 종류와 제공 벤더, 소프트웨어 버전 등의 자산 정보와 설비의 산업용 프로토콜 및 트래픽 세션을 모니터링해야 한다. 특히, 혼재되어 있는 서로 다른 산업용 프로토콜을 표준으로 통합해 분석할 수 있는 역량이 필수적이다.

운영망으로 넘어가면, 엔드포인트와 네트워크 영역 별로 보안 요구사항이 존재한다. 우선, 엔드포인트 영역에서는 시스템 정보에 대한 가시성을 확보해야 한다. 시스템 정보란 시스템 종류와 제공 벤더, 소프트웨어 버전 등 다양한 정보를 포괄한다. 또한, 공정 전체에 걸쳐 사용 중인 애플리케이션과 프로세스, 그리고 이동식 매체까지 파악이 필요하다. 네트워크 영역은 네트워크 프로토콜과 트래픽 세션에 대한 모니터링이 요구된다.

B. 탐지

식별을 통해 가시성을 확보한 뒤에는 CPS 환경에 존재하는 위협 요소와 이상징후를 탐지해야 한다.

먼저, 제어망에서는 OT 설비 이상징후를 파악해야 한다. 제어 명령 오작동, 설비 장애 여부부터 비인가 프로토콜 및 트래픽 세션 존재 여부를 종합적으로 모니터링해 항상 설비의 안정성을 보장해야 한다.

운영망에서는 일단 엔드포인트 영역에서의 악성코드 탐지가 기본적으로 요구된다. 아울러, 인가되지 않은 애플리케이션과 이동식 매체의 존재 여부를 확인해야 한다. 네트워크 영역에서는 악성코드 전송, 비인가 트래픽 등의 위협 요소가 있는지 지속적인 탐지가 필요하다.

C. 대응

마지막으로, 대응은 앞서 식별하고 탐지한 내용을 기반으로 최적의 대응 방안을 모색해 공정에 미치는 영향을 최소화하는 것을 뜻한다. CPS 환경의 특수성을 고려했을 때, 최적화된 대응을 위해서는 설비 관리자와 보안 전문가의 협력이 요구된다. CPS 보안의 최우선 과제는 운영의 연속성을 저해하지 않는 것이다.

OT 환경은 IT 환경에 비해 위협 대응에 제약이 있지만, 운영망에 대해서는 능동적인 대응이 가능하다. 엔드포인트 보안 위협을 탐지했을 경우에는 악성코드 검사와 치료를 진행해 피해를 최소화할 수 있다. 매체 제어와 취약점 패치를 통한 전반적인 보안 강화도 가능하다. 네트워크 보안 위협에 대해서는 기본적으로 '세그멘테이션(segmentation)'을 통해 네트워크를 세분화하고 모니터링 및 위협 대응 효율성을 향상시킬 수 있다. 또한, IT와 OT간 망분리를 통해 OT 환경을 보호하고 접근 제어를 강화하는 것도 효과적이다.

이처럼 체계적인 보안 아키텍처를 갖추기 위해서는 어떤 보안 모듈들이 필요할까? 먼저 네트워크 쪽을 보면, 사이버 위협 탐지와 자산 가시성 확보를 위한 전용 IDS가 요구된다. 또한, 방화벽을 통한 네트워크 세그멘테이션도 필요하다. 일방향 데이터 전송 모듈을 활용하면 OT망과 외부망 간 통신에 대한 보안을 강화할 수 있다.

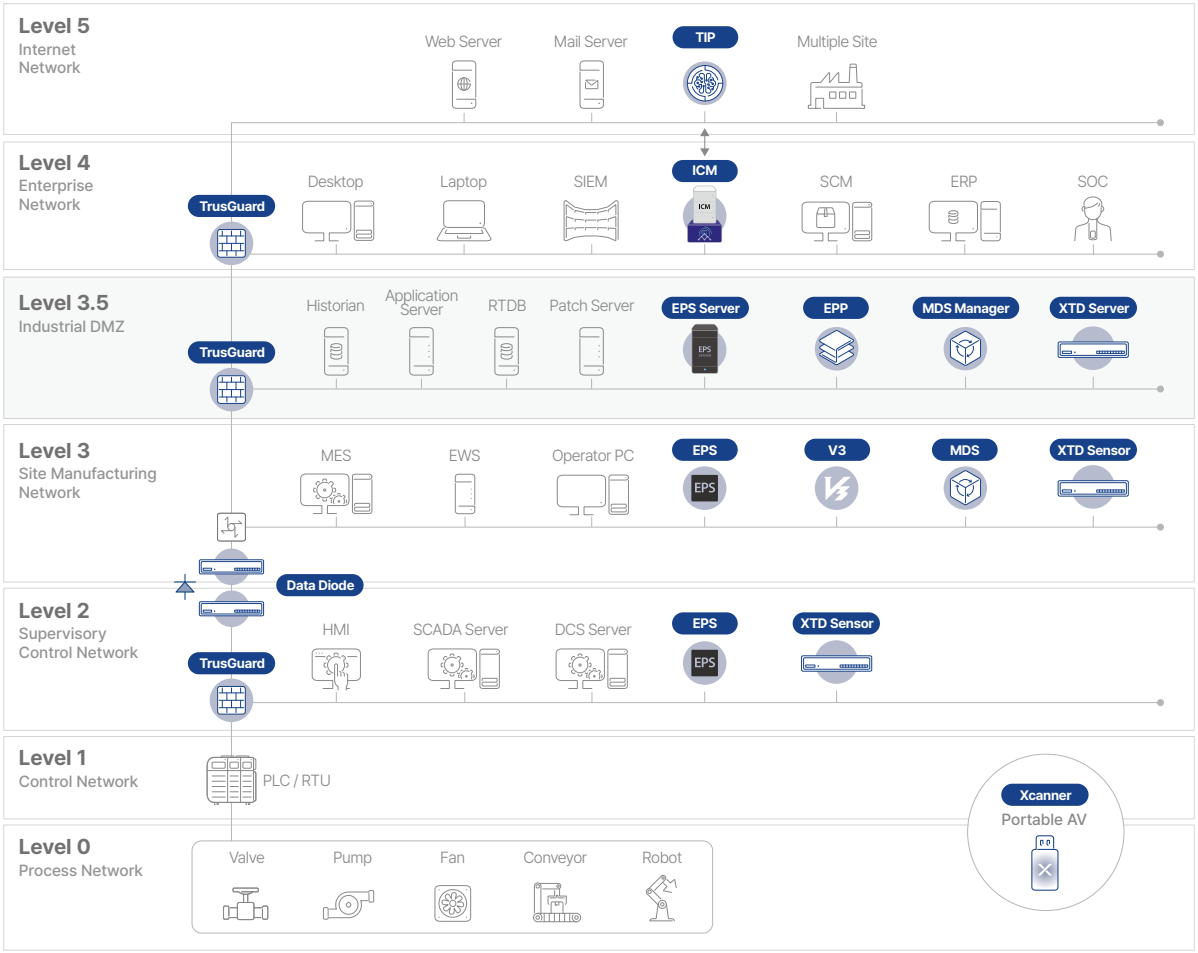
CPS의 엔드포인트 보호를 위해서는 비인가된 실행을 방지하기 위해 허용리스트 기반 애플리케이션 및 디바이스 제어가 필요하다. 패치 관리와 휴대용 멀웨어 모듈은 CPS 설비의 공격 표면을 줄이고 악성코드에 대응하는데 도움이 된다. 아울러, CPS 환경을 효과적으로 보호하기 위해서는 사용 중인 IT 기기들의 보안도 갖춰야 한다. 강력한 EPP를 사용하는 것이 좋은 시작이 될 수 있다.

이에 더해, 여러 보안 모듈들이 통합 관리되어야 한다. 현재의 CPS 보안 위협은 단일 솔루션으로 대응이 어렵다. 조직들은 플랫폼 기반 접근을 통해 통합 모니터링 및 관리 역량을 갖춰야 한다.

AhnLab CPS PLUS: 통합 CPS 보안 플랫폼

안랩의 CPS 통합 보안 플랫폼 'AhnLab CPS PLUS'는 OT 엔드포인트, 네트워크, 그리고 OT망과 연결된 IT 영역까지 포괄하는 CPS 환경을 보호한다. 해당 플랫폼은 제조, 에너지, 운송 등 다양한 산업군 고객들의 비즈니스를 보호해왔다.

AhnLab CPS PLUS는 경쟁사들 대비 가장 넓은 보안 커버리지를 제공한다는 점에서 차별화된다. 구성 모듈들의 유연한 연동에 기반한 플랫폼 전략은 고객들에게 강력한 보안 효율성과 비즈니스 생산성을 제공한다.



[그림 4] AhnLab CPS PLUS 구조도

AhnLab ICM
CPS 통합 모니터링 기반 가시성 제공 및 보안 모듈 관리

AhnLab EPS
OT 엔드포인트 프로세스 및 매체 제어, 악성코드 진단

AhnLab XTD
OT 네트워크 가시성 확보 및 이상 행위 등 위협 탐지

AhnLab Xcanner
OT 엔드포인트 악성코드 진단 및 치료를 위한 휴대용 안티멀웨어

AhnLab TrusGuard
OT 네트워크 보안 및 세그멘테이션

AhnLab Data Diode
물리적 일방향 데이터 전송을 통한 OT 환경 접근 제어

AhnLab MDS
네트워크 샌드박스 분석으로 알려지지 않은 악성코드 탐지

AhnLab EPP/V3
CPS 환경 내 IT 기기에 대한 안티멀웨어 및 통합 패치 관리

AhnLab TIP
IT와 OT 환경에 걸친 CPS 위협 인텔리전스

안랩의 위협 탐지 & 대응 역량과 OT 보안 기술을 결합한 AhnLab CPS PLUS는 CPS 환경 전반에 걸쳐'식별 > 탐지 > 대응'으로 이어지는 통합 보안 프로세스를 구축한다. 플랫폼은 총 9개 보안 모듈로 구성되어 있으며, 통합 관리 모듈인 AhnLab ICM을 통해 모니터링 및 중앙 관리된다.

Domain	Module	1단계 : 모니터링 & 식별	2단계 : 위협 탐지	3단계 : 대응	4단계 : 후속조치
IT & OT	ICM	• IT & OT 자산 목록 수집	• 로그 분석 • 상세 분석 리포트 조회	• Lockdown 예외처리 항목 변경 • 악성코드 정책 미적용 에이전트 확인	• 치료여부 확인 • Rest API 대응 정책 적용
Endpoint (OT)	EPS	• 생산설비 자산 식별	• Known 악성코드 탐지	• 악성코드 검사 • 비인가 프로세스 차단 • 매체 실행 차단	• Lock모드 전환 • AhnReport 분석 요청
Network (OT)	XTD	• OT 자산 식별 • 자산별 트래픽 식별	• 악성코드 전파 탐지 • 취약점 등 네트워크 위협 탐지 • 비정상 PLC 로직 탐지	• 위협 탐지 대응 경보	
Endpoint (OT)	Xcanner			• 감염 설비 악성코드 진단/치료	
IT & OT	TrusGuard		• 네트워크 보안위협 탐지 • 비인가 트래픽 탐지	• ACL 기반 비인가 세션 차단 • 유해 트래픽 차단	• 방화벽 정책 설정 • 네트워크 세그멘테이션
Network (OT)	Data Diode			• 단방향 데이터 전송	
IT & OT	MDS		• Known/Unknown 악성코드 탐지 • 감염 장비의 네트워크 이상행위 탐지 • 행위 분석 우회 위협 탐지	• 정오탐 여부 확인 • 핀포인트 검사	
Endpoint (IT)	EPP/V3	• 패치 관리	• IT 악성코드 탐지	• IT 악성코드 치료	• EPP/AV 정책 설정
IT & OT	TIP				• 위협정보 조회

[그림 5] AhnLab CPS PLUS 모듈 별 역할

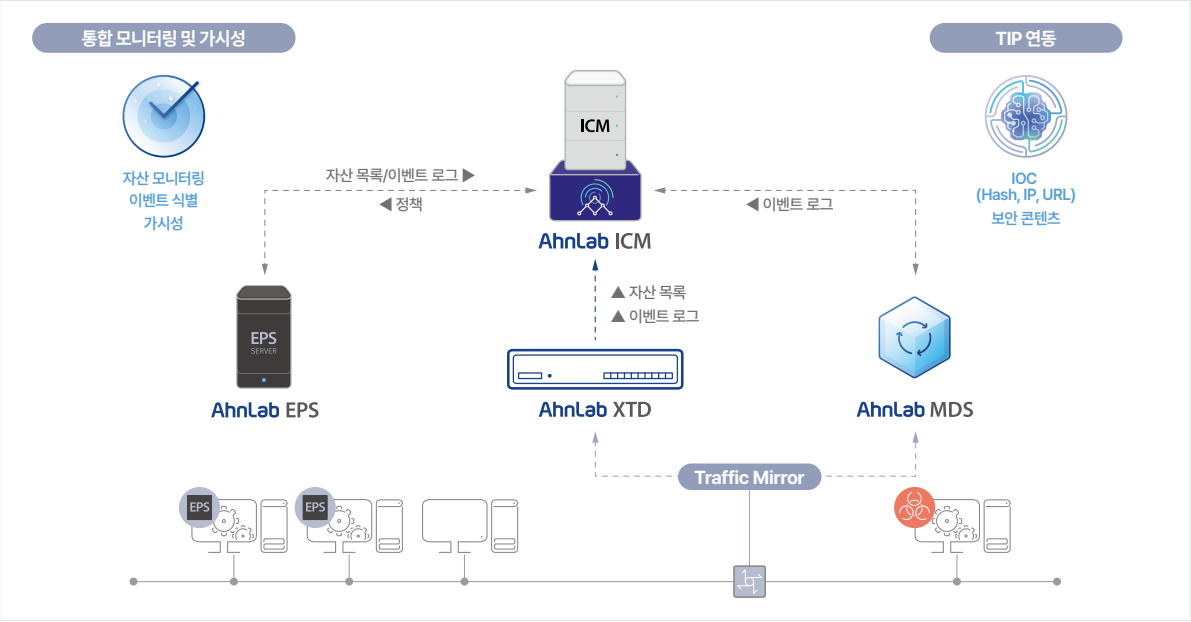
AhnLab CPS PLUS 보안 모듈의 역할

AhnLab CPS PLUS의 9개 보안 모듈들은 CPS를 보호한다는 공통된 목적을 갖고 다른 역할들을 수행한다. 각 보안 모듈들의 역할과 상호 간 어떻게 연동되는지 살펴보자.

ICM (+TIP)

보안 플랫폼에 있어 가장 중요한 역량은 연동되는 모듈들을 통합 모니터링 및 관리하는 것이다. 바로 AhnLab ICM이 AhnLab CPS PLUS에서 수행하는 역할이다. 관리자는 직관적인 대시보드를 통해 CPS 환경 전반에 대한 가시성을 확보하고, CPS 보안의 핵심 모듈들을 중앙 관리할 수 있다.

AhnLab EPS, XTD, MDS 등 CPS 보안 모듈들과 연동하는 ICM은 모듈 현황과 로그 통합 조회 및 검색 기능을 제공하여, 관리자로 하여금 조치가 필요한 이슈들을 즉각 확인할 수 있도록 한다. 고객들은 ICM을 활용해 비즈니스 연속성, 효율성 및 생산성을 강화하고 진정한 'CPS 보안 플랫폼'의 혜택을 누릴 수 있다.

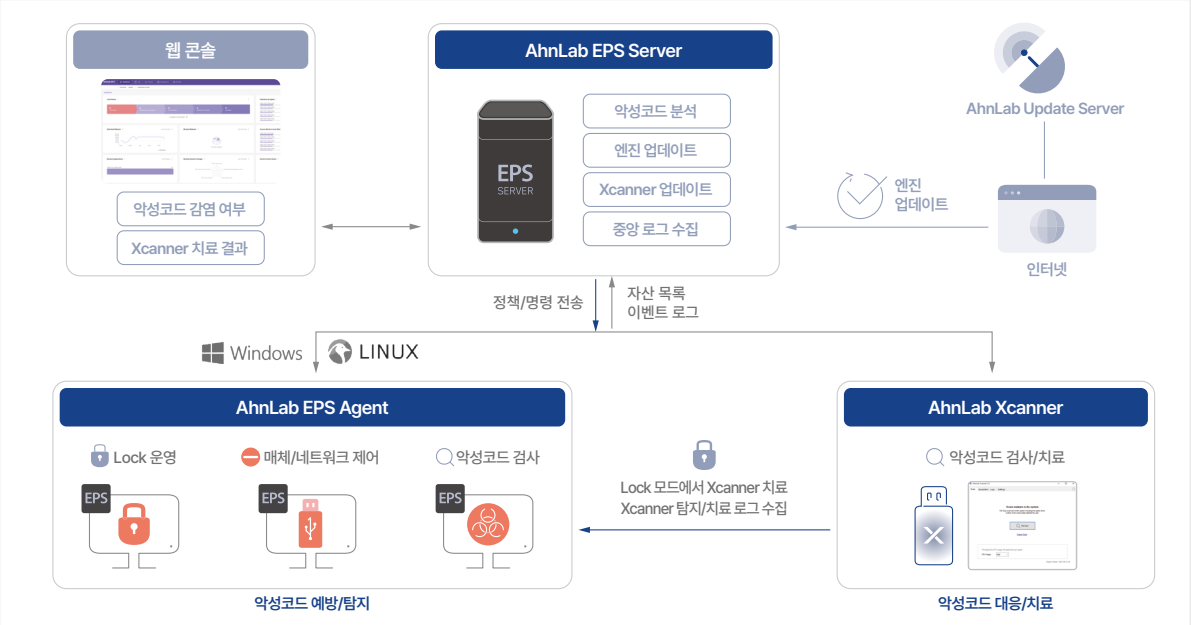


[그림 6] AhnLab ICM의 중앙 관리 아키텍처

또한, ICM은 자사 위협 인텔리전스 플랫폼 AhnLab TIP 연동을 통해 진정한 인텔리전스 기반 CPS 보안을 실현한다. 관리자는 IT와 OT를 아우르는 CPS 환경의 보안 위협에 대한 침해지표(IoC)를 통해 보다 자세한 정보를 실시간으로 확인할 수 있다.

EPS (+Xcanner)

OT 엔드포인트 보안 모듈 AhnLab EPS는 오랫동안 제조업체, 발전소 등 다양한 산업군 기업들의 CPS 환경을 보호해 왔다. EPS의 직관적인 웹 기반 콘솔은 사업장 내 OT 설비들을 정확하게 식별하고 관리할 수 있도록 한다. OT 설비의 운영 안정성을 위해 에이전트를 최대한 가볍게 했으며, 각종 검사 및 분석 등 부하를 줄 수 있는 작업들은 서버에서 수행하는 구조다. EPS는 윈도우, 리눅스 등에 걸쳐 보안 업데이트와 패치가 제대로 되지 않은 구형 운영체제까지 원활하게 지원한다.



[그림 7] AhnLab EPS와 Xcanner 구조

EPS의 핵심 역량은 허용리스트(allowlist) 기반 제어 기술을 적용해 인가된 디바이스와 네트워크만 실행되도록 하여, 잠재적인 침해 가능성을 최소화하는 것이다. 인가된 허용리스트는 자동으로 생성되어 적용되므로, 정책 설정에 대한 관리자의 부담을 덜어준다.

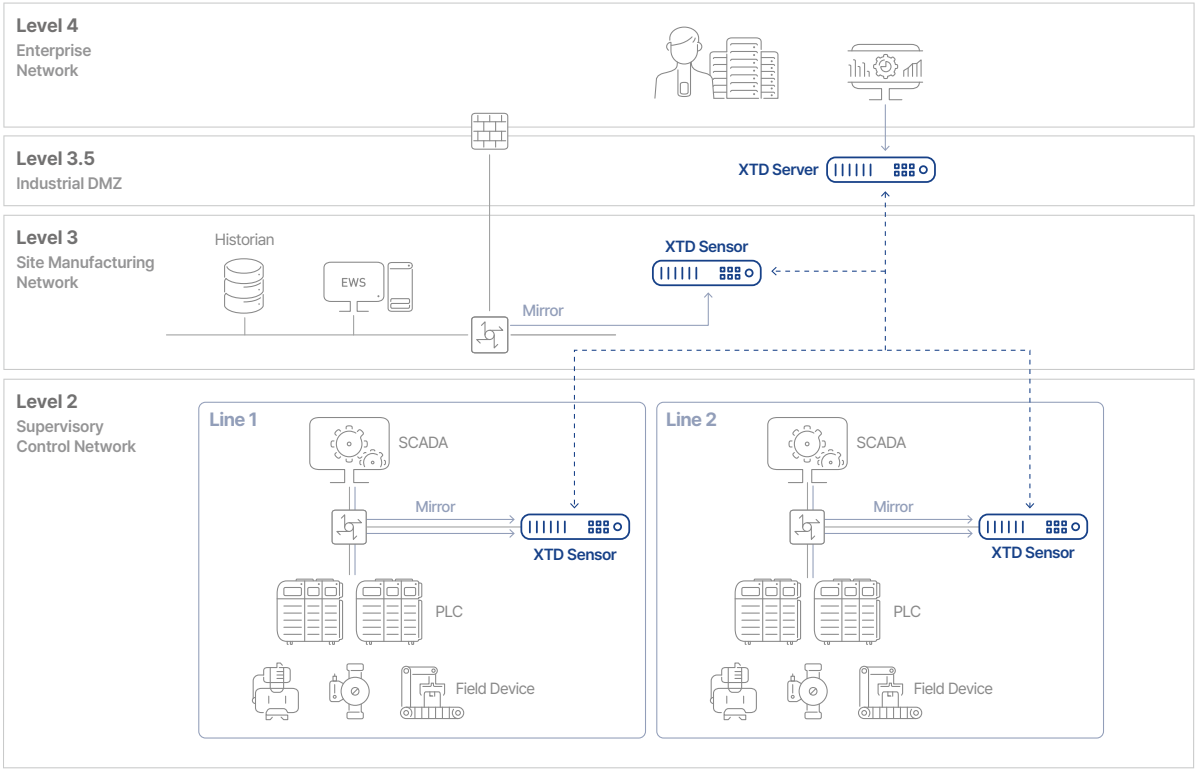
EPS는 3단계 운영모드를 지원해 고객의 운영 편의성과 보안 설정의 안정성을 강화한다. 먼저, 3단계 운영모드는 시스템 업데이트를 위해 잠금을 해제하는 Unlock Mode, 운영 정비를 위해 Lock Mode 운영 전 정책을 검증하는 Lock Test Mode, 그리고 실제 시스템 운영 시 적용하는 Lock Mode가 있다. Lock Mode는 운영 안정성과 연속성 보장을 위해 시스템 상에서 예외 처리한 사항을 제외한 그 어떤 변경도 허용하지 않는다.

또한, EPS는 OT 설비를 노리는 알려진 악성코드를 탐지 및 차단한다. 에이전트 단에서 악성코드를 탐지하고, 서버에서 상세 분석을 진행한다. 이를 통해, 시스템 부하 없이 악성코드에 대한 실시간 탐지, 분석 및 차단이 가능하다.

OT 설비가 악성코드에 감염되면, 휴대용 안티바이러스 AhnLab Xcanner를 활용해 악성코드를 치료할 수 있다. Xcanner는 인가된 USB에 설치하거나 EPS 에이전트를 활용해 다운로드 받을 수 있다. Xcanner의 검사 및 치료 내역과 관련 로그들은 EPS 서버에서 모니터링 및 관리된다. Xcanner의 장점은 악성코드 대응 프로세스를 쉽고 직관적으로 설계해 비전문가도 침해 사고에 쉽게 대응할 수 있도록 한 것이다.

XTD

AhnLab XTD는 네트워크 기반 OT망 가시성을 제공하며, 보안 위협 및 이상 행위를 실시간으로 탐지한다. 가용성을 중시하는 OT 환경의 특성을 고려해 설비 운영에 영향을 주지 않도록 네트워크 트래픽을 미러링하는 '패시브 모니터링' 방식으로 동작해 운영 안정성을 보장한다.



[그림 8] AhnLab XTD 운영 구조

XTD는 OT 엔드포인트 보안 모듈과 연동해 엔드포인트 영역에 대한 가시성과 악성코드 검사와 치료까지 제공하는 것이 특징이다. 또한, 다수 OT 프로토콜에 대한 DPI(Deep Packet Inspection) 분석 기술을 통해 다양한 종류의 설비 식별과 비정상 제어 로직에 대한 탐지 및 분석 역량을 제공한다.

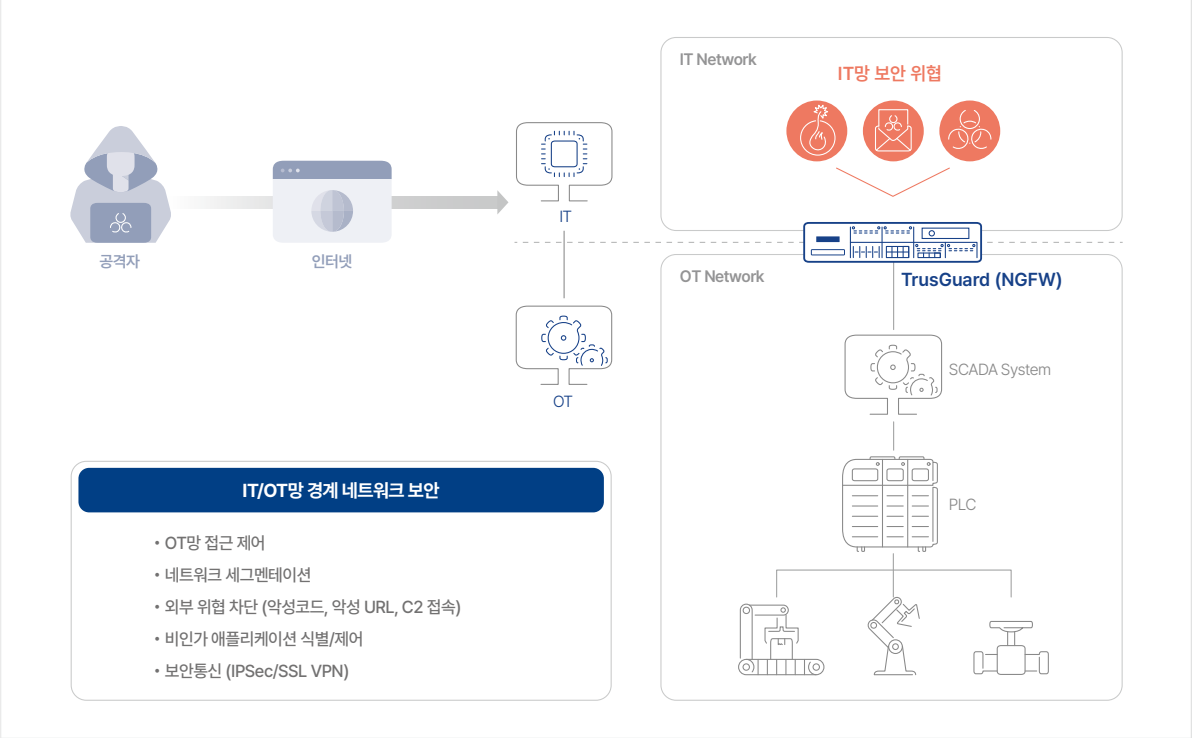
XTD를 EPS와 연동하면 OT망에 연결되어 있는 엔드포인트까지 가시성을 확대할 수 있다. 일반적인 동종 솔루션은 대부분 네트워크 영역까지 자산 현황을 제공한다. 그러나 XTD는 EPS와 연동해 네트워크 영역 뿐만 아니라 OT망에 연결된 서버 및 워크스테이션(Workstation)의 운영체제 패치 버전 등 엔드포인트의 상세정보까지 가시성을 확대할 수 있다.

Xcanner 연동 시, 악성코드 검사 영역도 확장할 수 있다. 일차적으로 네트워크에서 악성코드 전파 또는 취약점 악용 유해 트래픽이 탐지되면, 엔드포인트 영역에 위치한 의심 시스템에 대해서도 다시 한번 악성코드 검사를 실시할 수 있다. 또한, 네트워크에서 보안 위협 탐지만 제공하는 대부분의 동종 솔루션과 달리 위협의 근원에 대한 악성코드 검사까지 가능하므로 보다 능동적인 위협 대응이 가능하다.

이 밖에, 탐지된 위협의 유포 경로를 역추적해 위협 정보를 알려주는 '위협 추적(Threat Tracking)' 기능도 제공한다. 이 기능을 공격이 전파된 이전 유포지를 확인하여 공격의 전파 및 이동 경로를 파악할 수 있도록 한다. 이를 통해, 사용자는 탐지된 위협 이벤트의 유포 경로 및 최초 발생 자산 등 위협 간 연결성을 확인해 체계적인 위협 대응을 수행할 수 있다.

TrusGuard

방화벽 모듈 AhnLab TrusGuard는 OT망 경계에서 인바운드 및 아웃바운드 트래픽을 제어하고, 악성코드, URL, C2 연결 트래픽 등 유해 트래픽을 차단하며, IPSec/SSL VPN 등 보안 통신과 네트워크 세그멘테이션 등의 기능도 지원한다.

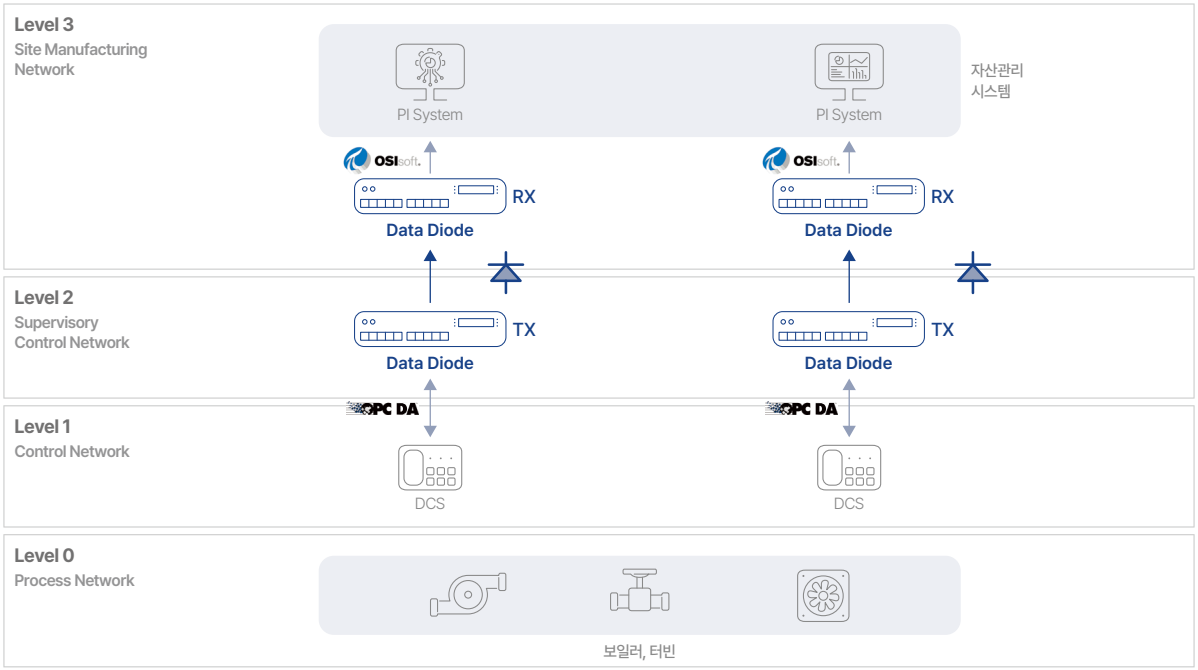


[그림 9] AhnLab TrusGuard의 네트워크 경계 보안 구조

또한, OT 프로토콜 분석 기술을 적용해 OT망 내부에서 산업용 프로토콜을 상세하게 제어할 수 있다. 구체적으로는 Modbus, DNP3 등 프로토콜 별 제어 뿐만 아니라 Function Code 까지 식별하여 제어가 가능하다.

Data Diode

AhnLab Data Diode는 보안 수준이 서로 다른 네트워크 간 연결에서 보안 수준이 높은 곳으로의 접근을 강화하기 위해 물리적 일방향 전송을 바탕으로 필요한 데이터만 안전하게 외부로 전송하도록 한다. 데이터 암호화, 전진 오류 수정(Forward Error Correction, FEC), 데이터 송신 오류 제어, 악성코드 검사 등 다양한 기술들을 적용하여, 전송 데이터의 신뢰도와 안정성을 극대화했다.



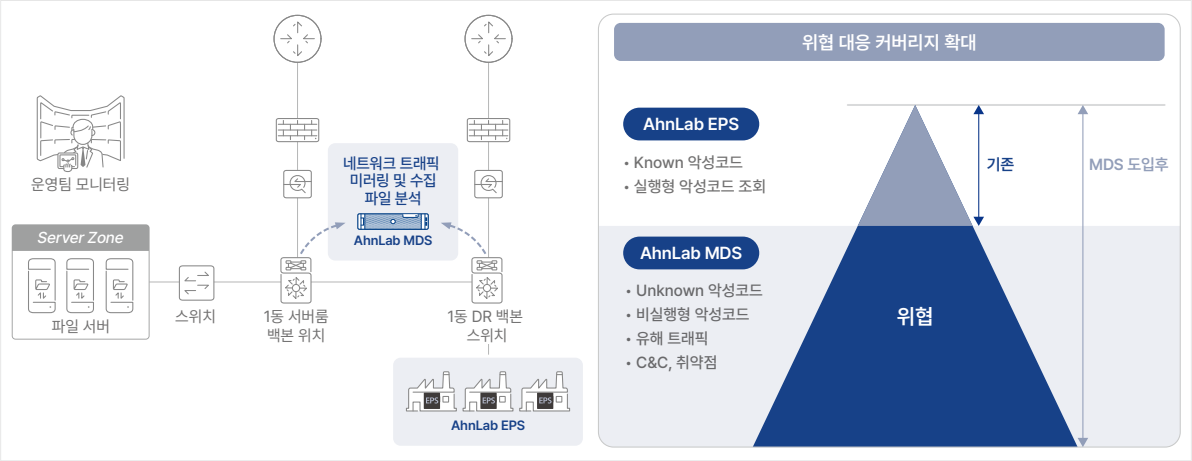
[그림 10] AhnLab Data Diode 구조도

또한, IT와 OT 환경을 아우르는 광범위한 프로토콜 지원 기술을 기반으로 다양한 환경에 최적화된 형태로 배포 가능하다. 각종 IT/OT 프로토콜, CCTV 스트리밍 데이터, 데이터베이스 등 여러 활용 사례(use case)들을 맞춤형으로 지원하는 유연성도 갖추고 있다.

MDS

최근, 사이버 위협이 지속적으로 고도화되면서 지능형지속위협(Advanced Persistent Threat: APT)과 신/변종 악성코드가 증가하는 추세다. 따라서, 기존 알려진(Known) 악성코드 뿐만 아니라 알려지지 않은(Unknown) 악성코드에 대한 분석과 대응이 필요해졌다.

네트워크 샌드박스 모듈 AhnLab MDS는 생산망 트래픽에 존재하는 파일을 수집해 분석하고, 알려지지 않은 악성코드에 대한 동적 분석을 진행한다. 또한, 공격자의 C&C IP 연결까지 탐지하여 분석하므로 OT망 악성코드 확산 경로, C&C, 취약점 등 다양한 보안 위협에 대한 모니터링과 감염 장비에 대한 치료 및 대응을 제공한다.

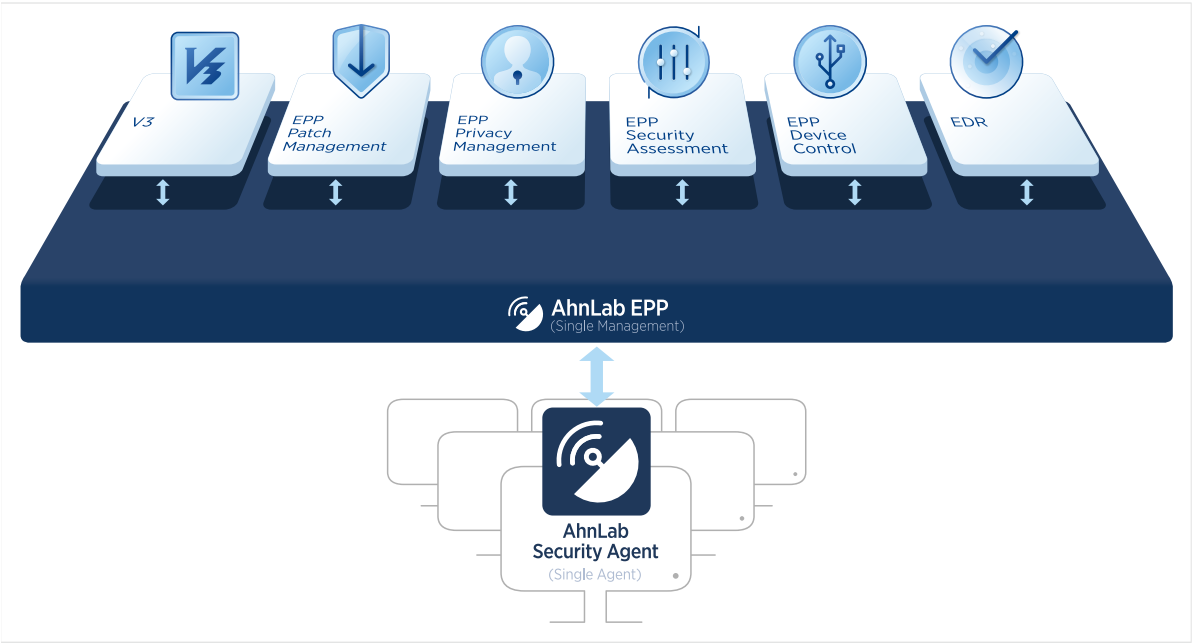


[그림 11] AhnLab EPS & AhnLab MDS 연계를 통한 위협 커버리지 확대

특히 EPS 연동 시, MDS의 동적 분석 기능을 바탕으로 신종, 변종 및 알려지지 않은 악성코드까지 모두 방어가 가능해 종합적인 위협 대응 커버리지를 확대할 수 있다.

AhnLab EPP/V3

CPS 환경에서는 OT 보안 뿐만 아니라, OT 환경과 연결된 혹은 OT 환경을 관리하는 IT 영역의 보안까지 고려해야 하며, 필수적으로 요구되는 역량은 패치 관리를 통한 취약점 최소화와 안티멀웨어를 통한 강력한 위협 차단이다.



[그림 12] AhnLab EPP 구조도

AhnLab EPP는 안티멀웨어부터 패치 관리까지 다양한 모듈을 유기적으로 연동하여, IT 환경에서의 위협이 OT 환경을 침해하는 것을 방지한다. 우선, 다수 엔드포인트 시스템에 대해 안정적이고 폭 넓은 패치 관리 기능을 제공하여, 엔드포인트 공격 표면을 줄인다. 또한, 안티멀웨어 모듈(V3)은 AV-TEST 등 글로벌 인증 평가에서 오랜 기간 최상위 수준 진단율을 기록하고 있으며, 검증된 기술력을 바탕으로 세계 최고 수준의 위협 차단 역량을 제공한다.

도입효과

AhnLab CPS PLUS는 IT-OT 융합 보안을 바탕으로 CPS 보안 요구사항을 효과적으로 해결한다. 이를 통해, 고객들은 진정한 디지털 혁신 여정에 박차를 가할 수 있다.

도입효과 #1: 운영 가용성 보장

CPS 환경의 최우선 과제는 설비 운영 가용성을 보장하는 것이다. AhnLab CPS PLUS는 CPS 환경의 특수성에 최적화된 여러 보안 모듈들을 통해 시스템 부하 없이 강력한 보안을 구현한다.

도입효과 #2: 체계적인 위협 관리 프로세스

AhnLab CPS PLUS는 '식별 > 탐지 > 대응'으로 이어지는 체계적인 위협 관리 프로세스를 갖추고 있다. CPS 자산들을 상세하게 식별하고, OT망 내부에 유포되는 각종 위협과 이상 징후를 탐지하며, 공정에 영향을 미치지 않는 최적의 대응 역량을 제공한다.

도입효과 #3: 편리한 통합 관리 및 모니터링

AhnLab CPS PLUS는 통합 관리 콘솔 AhnLab ICM을 통해 CPS 엔드포인트 및 네트워크 보안 모듈 뿐만 아니라 SIEM, TIP와도 유연하게 연동한다. 이를 통해, CPS 환경의 보안 위협을 효과적으로 관리할 수 있도록 운영 편의성을 제공한다.

결론

CPS 환경을 향한 사이버 공격은 지속적으로 증가하고 있고, 피해 규모 역시 점점 커질 것으로 예상된다. 조직들은 이제 OT 보안에 대한 이해도를 높여가고 있지만, 앞으로는 서로 다른 IT와 OT 환경을 통합한 CPS 보안 관점에서 생각해야 한다. 물론 쉽지 않은 과제이지만, CPS 보안의 접근법과 아키텍처를 올바르게 이해한다면 불가능한 미션은 아니다.

조직들이 CPS 보안 이니셔티브를 추진하는데 있어 명심해야 할 세 가지 권고사항은 다음과 같다.

#1. OT 보안 뿐만 아니라 IT 보안도 함께 생각할 것

본 문서에서 여러 차례 언급했듯, OT 환경을 향한 위협은 OT와 연결된 IT 영역에서부터 시작된다. 따라서, CPS 보안을 효과적으로 수행하기 위해서는 IT와 OT를 융합한 통합 보안 접근을 지향해야 한다. 먼 미래에는 CPS의 연결 지점이 IT와 OT를 넘어 다양한 영역으로 확대될 전망이다.

#2. '식별 > 탐지 > 대응'으로 이어지는 보안 프로세스 구축하기

자산 식별과 위협 탐지 및 대응은 CPS 보안의 근간이다. 특히, OT 환경에서는 자산과 네트워크에 대한 변경이 많이 일어나지 않으므로, 충분한 자산 가시성과 정확한 위협 탐지 역량을 기반으로 위협 대응 프로세스를 구축한다면, 장기적으로 큰 효과를 볼 수 있다.

#3. 단일 솔루션이 아닌 플랫폼 기반 접근을 지향할 것

오늘날의 CPS 보안 위협은 이미 단일 솔루션으로 해결할 수 있는 수준을 넘어섰다. 그리고, 위협은 앞으로 더 고도화될 것이다. 따라서, 여러 보안 모듈들이 유연하게 상호연동하는 CPS 보안 플랫폼이 필요하다. 최적화된 보안 기능과 통합 가시성 및 관리 역량을 제공하는 CPS 보안 플랫폼은 나날이 진화하는 CPS 위협에 대응할 유일한 길이다.

안랩은 날로 증가하는 CPS 보안 요구사항을 해결할 최적의 파트너로 자리매김하고 있다. AhnLab CPS PLUS는 IT와 OT 환경에 걸쳐 연동하는 여러 보안 모듈들을 중앙 관리 및 모니터링하며, 플랫폼의 폭 넓은 보안 커버리지는 경쟁사 대비 차별화되는 요소다. 여러 산업에 걸친 다양한 고객 레퍼런스는 플랫폼의 우수성을 입증하며, 앞으로도 각 모듈의 기능을 강화하는 동시에 연계와 연동을 강화하여 미래지향적인 활용 사례(use case)들을 지원할 예정이다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901