AhnLab CPS PLUS

AhnLab XTD

OT 가시성 및 위협 탐지 모니터링 솔루션

AhnLab XTD는 OT망 가시성을 제공하고 이상 행위와 보안 위협을 실시간으로 탐지하는 OT 환경 특화 보안 솔루션입니다.

제품 개요

AhnLab XTD는 OT 환경의 자산 가시성을 확보하고 보안 위협을 탐지해 모니터링 및 관리할 수 있도록 지원하는 OT 전용 네트워크 보안 솔루션입니다. OT 환경의 가용성을 보장하는 패시브 스캔(passive scan) 방식으로 동작하며, 자체 개발한 프로토콜 프로파일링 기술과 심층 패킷 분석(DPI) 기능을 바탕으로 다양한 종류의 자산을 식별하고 모니터링합니다. 또한, IT망으로부터 유입되거나 OT망 내부 시스템 간 전파되는 악성코드, 취약점 등 보안 위협을 실시간으로 탐지하고 관리할 수 있도록 지원합니다.

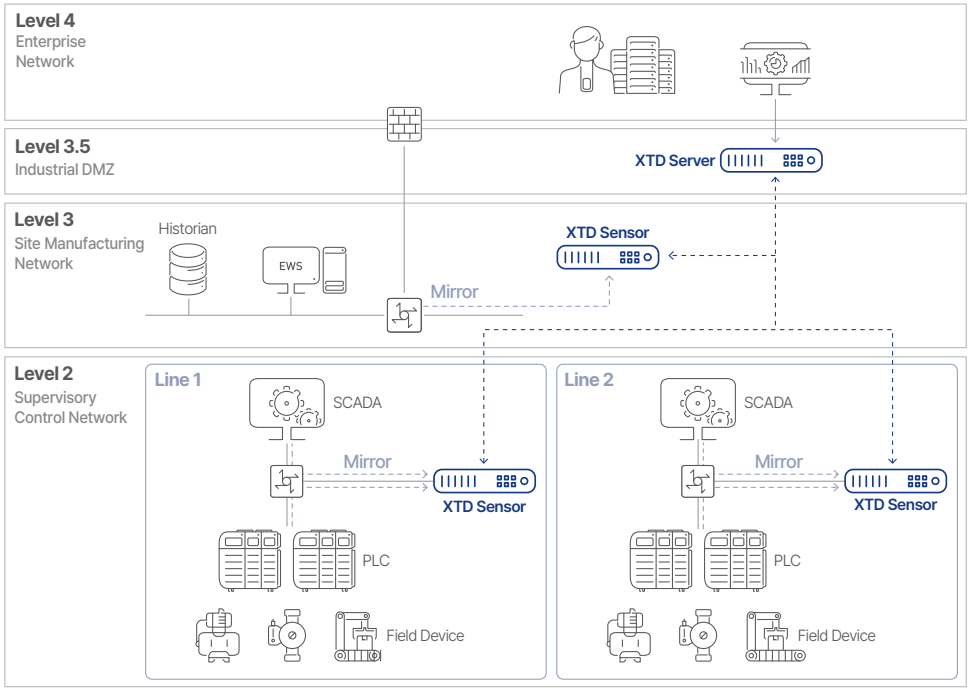
자산 및 DPI 기반 프로토콜 분석
네트워크 세션 및 토폴로지

악성코드, 취약점 등 위협 탐지
ICS 프로토콜 및 제어 로직 이상 탐지

가용성을 위한 미러 모드 구성
네트워크 구성 변경 불필요

시스템 구성

AhnLab XTD의 기본 구성은 중앙의 서버와 각 네트워크 구간별로 구축되는 센서로 이루어져 있습니다. 네트워크 구간별로 설치된 센서는 미러링된 트래픽 분석 정보와 보안 위협 탐지 결과를 중앙 관리 서버로 전달합니다. 중앙 관리 서버는 수집된 정보를 분석하여 각종 가시성 및 위협 정보를 모니터링하고 보안 정책 설정을 제공합니다. 소규모 자산이 운영되는 환경에는 센서와 서버가 결합된 올인원 서버로 구성도 가능합니다.



주요 기능

가시성 확보

OT와 IT를 아우르는 CPS(Cyber-Physical System) 환경의 효과적인 보안 관리를 위해서는 자산 관련 여러 정보를 실시간으로 수집하고 모니터링하는 것이 중요합니다. AhnLab XTD는 OT 환경의 가용성 보장을 위해 패시브 모니터링 방식으로 트래픽을 분석하고, 폭 넓은 가시성을 확보합니다.

AhnLab XTD는 OT 자산의 상세 정보들을 수집해 직관적으로 제공합니다. 또한, 자산의 트래픽, 토폴로지 등 각종 네트워크 정보 뿐만 아니라 다양한 IT, OT 및 ICS 프로토콜 분석 정보도 함께 제공합니다.

AhnLab XTD는 효율적인 가시성 제공과 보안 관리를 위해 학습 모드와 운영 모드를 제공합니다. 학습 모드에서는 구축 후 일정 기간 동안 관리 대상 자산을 식별해 등록합니다. 그리고, 운영 모드에서 식별되지 않은 미등록 Unknown 자산을 별도 관리할 수 있어 빈틈 없는 보안과 운영 효율성을 동시에 확보할 수 있습니다.

- 자산 유형, 제조사
- IP/MAC, Zone, 그룹
- OS 정보, 위험도 등

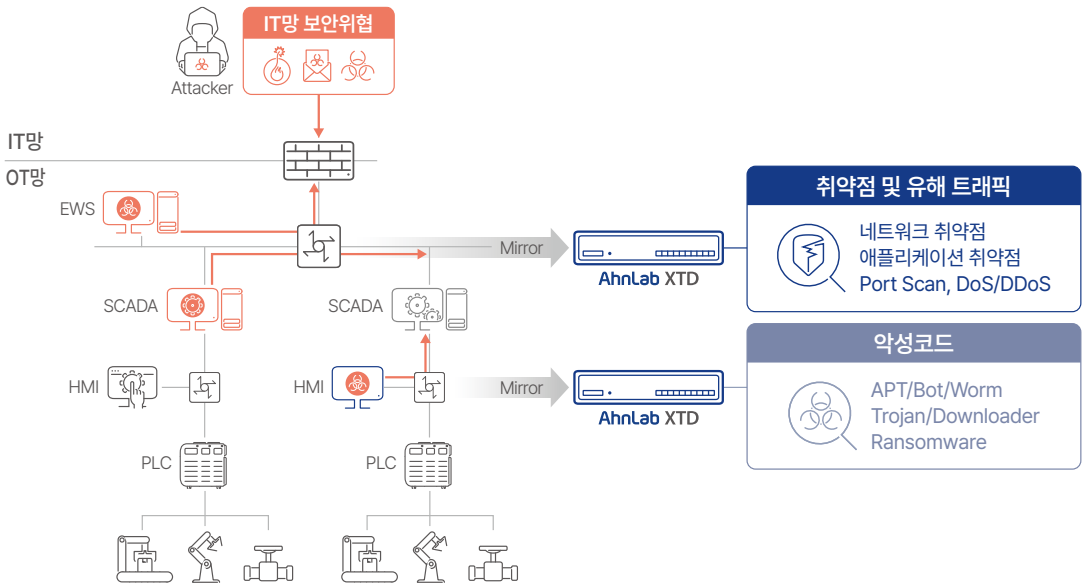
- 서비스, 세션
- 트래픽
- 토폴로지

- ICS 프로토콜
- Function code, value 등

위협 탐지 및 관리

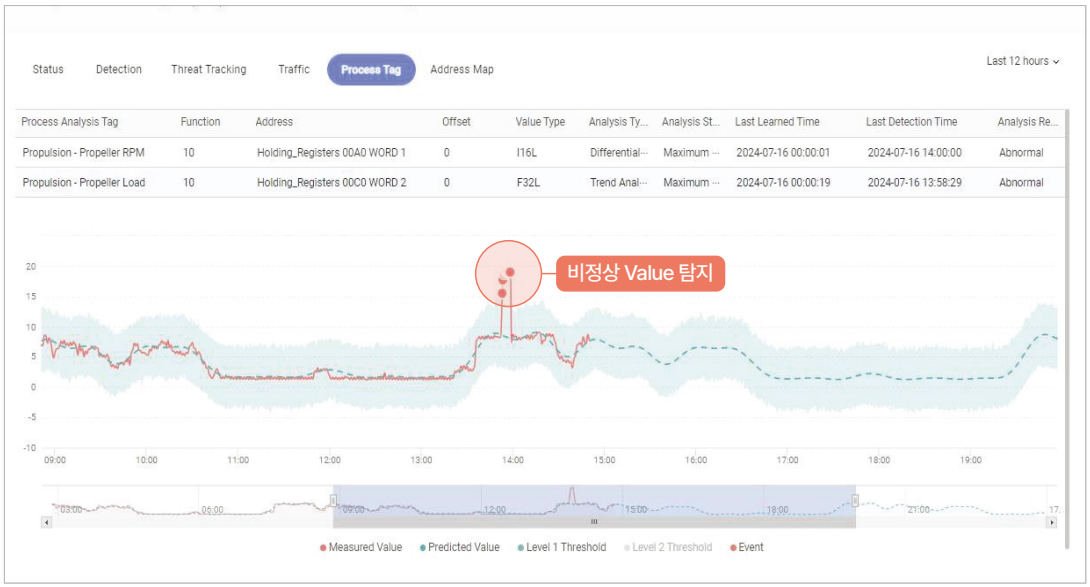
일반적으로 CPS 환경은 폐쇄망으로 운영되어 외부 위협에 대한 노출이 적지만 구형 OS 사용, 미흡한 보안 패치, 관리되지 않은 이동식 디바이스 사용으로 인해 보안 위협에 취약합니다. 하지만, 내부망 위협 탐지 및 모니터링은 상대적으로 부족합니다.

AhnLab XTD는 OT망 내부 트래픽을 통해 전파되는 각종 보안 위협을 탐지 및 관리합니다. 랜섬웨어를 포함한 여러 악성코드, 소프트웨어 취약점 악용 트래픽, 스캔(scan), 도스(DoS) 등 유해 트래픽을 실시간으로 탐지하고 관리자에게 알립니다. 특히, 안랩의 오랜 기술력이 반영된 자체 안티바이러스 엔진을 적용해 현존하는 악성코드와 새로운 악성코드까지 빠르고 정확하게 탐지합니다.



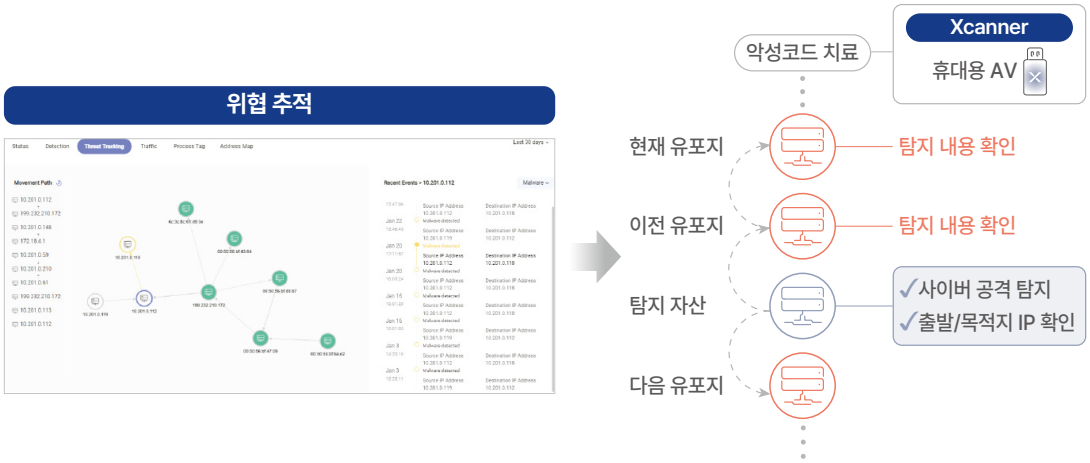
Baseline 이상 탐지

AhnLab XTD는 다양한 ICS 프로토콜에 대한 DPI(Deep Packet Inspection) 분석 기술을 기반으로 베이스라인(Baseline) 이상 탐지 기능을 제공합니다. 관리자가 설정한 특정 프로세스 값(Value)을 통계 기반으로 학습하고 기준치에 해당하는 베이스라인을 세팅합니다. 그리고, 베이스라인을 미달 혹은 초과하는 값을 이상 변경으로 탐지합니다. 이를 통해, 오작동에 관한 실시간 알림을 보내며, 보안 관리자는 악의적인 공격자가 일으키는 제어 시스템 오작동, 관리자의 실수로 인한 설비 오작동을 실시간으로 탐지할 수 있습니다.



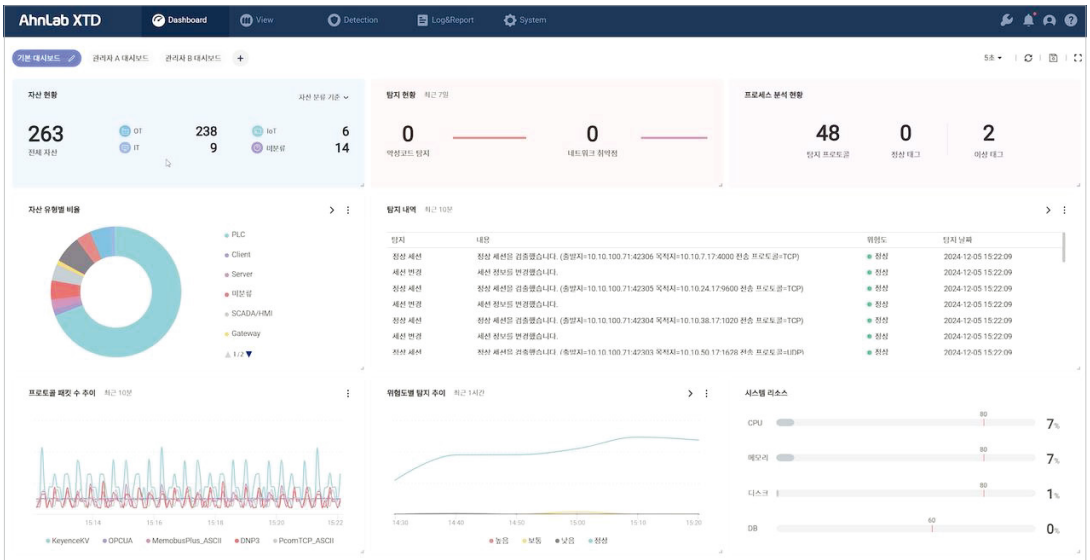
위협 근원지 추적

AhnLab XTD는 OT망 내부에서 전파되는 보안 위협의 근원지를 추적하여 가시성이 확보되지 않은 환경에서 보안 위협의 가시성을 높여줍니다. 공격이 전파된 이전 유포지를 확인하여 공격의 이동 경로를 파악할 수 있고, 공격이 전파되는 경로를 추적할 수 있습니다. 또한, 휴대용 AV 솔루션 'AhnLab Xcanner'를 활용해 보안 위협이 전파된 시스템들에 대한 악성코드 검사 또는 치료를 수행할 수 있습니다.



대시보드 모니터링

AhnLab XTD는 편리한 솔루션 운영을 위해 웹 기반 관리 콘솔과 다양한 관리 메뉴를 제공합니다. 동적 UX 기반 직관적인 대시보드를 통해 각종 자산 가시성 및 위협 정보를 실시간으로 모니터링 할 수 있도록 지원합니다. 또한, 사용자 정의 대시보드를 통해 관리자가 추가로 확인이 필요한 정보를 별도 대시보드 패널과 위젯으로 생성하여 구성할 수 있습니다.

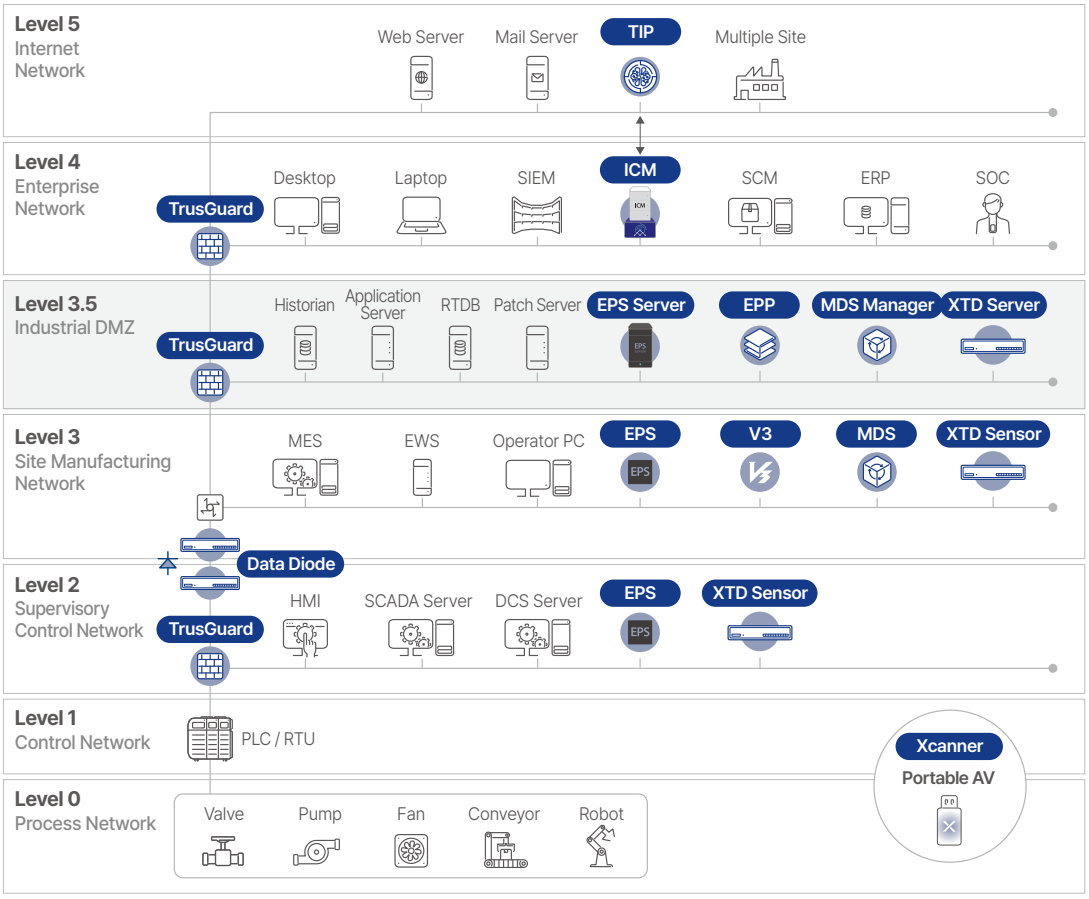


Why AhnLab XTD

플랫폼 기반 CPS 보안

안랩은 통합 CPS 보안을 위해 OT 엔드포인트와 네트워크, 그리고 OT와 연결된 IT 환경까지 폭 넓게 보호하는 CPS 보안 플랫폼 "AhnLab CPS PLUS"를 운영하고 있습니다. 안랩의 위협 탐지 & 대응 전문성과 OT 기술력을 결합한 AhnLab CPS PLUS는 엔드포인트와 네트워크 보안 기술을 바탕으로 IT와 OT를 아우르는 CPS 환경에서 ▲식별(가시성) ▲위협 탐지 ▲대응으로 이어지는 빈틈없는 보안을 제공합니다. 유연하게 연동되는 AhnLab CPS 보안 모듈들은 CPS 보안 통합 관리 솔루션 "AhnLab ICM"을 통해 중앙 관리 및 모니터링됩니다.

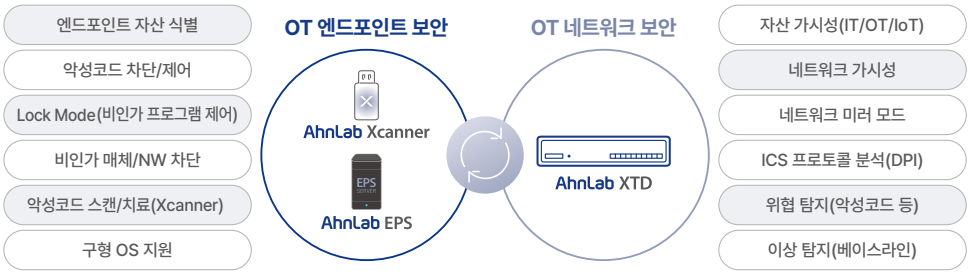
AhnLab CPS PLUS는 현존하는 CPS 보안 플랫폼 중 가장 폭 넓은 커버리지를 자랑합니다. 여기에, 탁월한 기술력과 통합의 시너지가 더해져 고객들에게 차별화된 CPS 보안 경험을 제공합니다.



엔드포인트-네트워크 연계 보안

AhnLab XTD는 OT 엔드포인트 보안 솔루션 AhnLab EPS 연동을 통해 타사 보안 오퍼링을 통해서는 경험할 수 없는 독보적인 OT 엔드포인트-네트워크 연계 보안을 제공합니다.

우선, AhnLab XTD가 식별한 네트워크 및 자산 가시성 정보에 AhnLab EPS 에이전트가 수집한 엔드포인트 자산 정보를 더해 CPS 환경 내 가시성을 확장 및 검증할 수 있습니다. 또한, 탐지된 위협에 대해서도 AhnLab EPS 연동을 통해 의심 시스템의 악성코드를 원격 진단하고 실시간으로 대응할 수 있습니다.



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

AhnLab