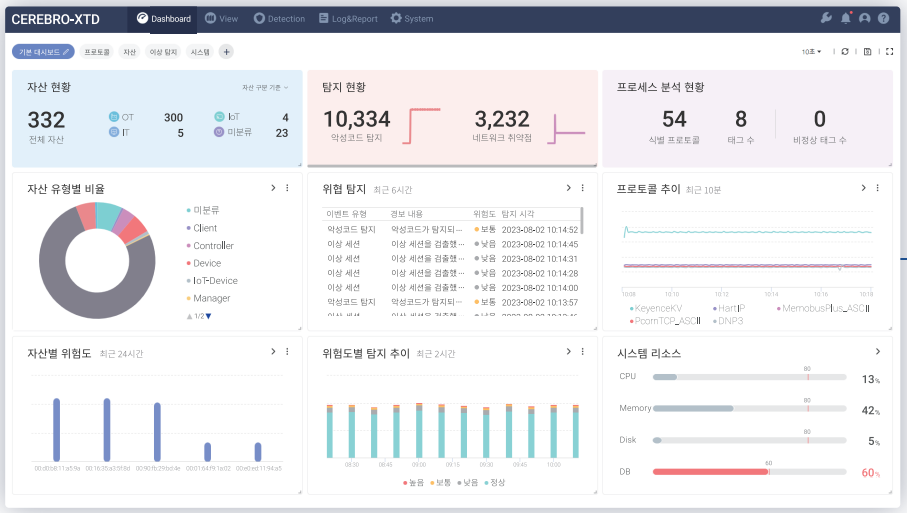
NAONWORKS
an AhnLab Company

CEREBRO-XTD

OT 가시성 및 위협 탐지 모니터링 솔루션

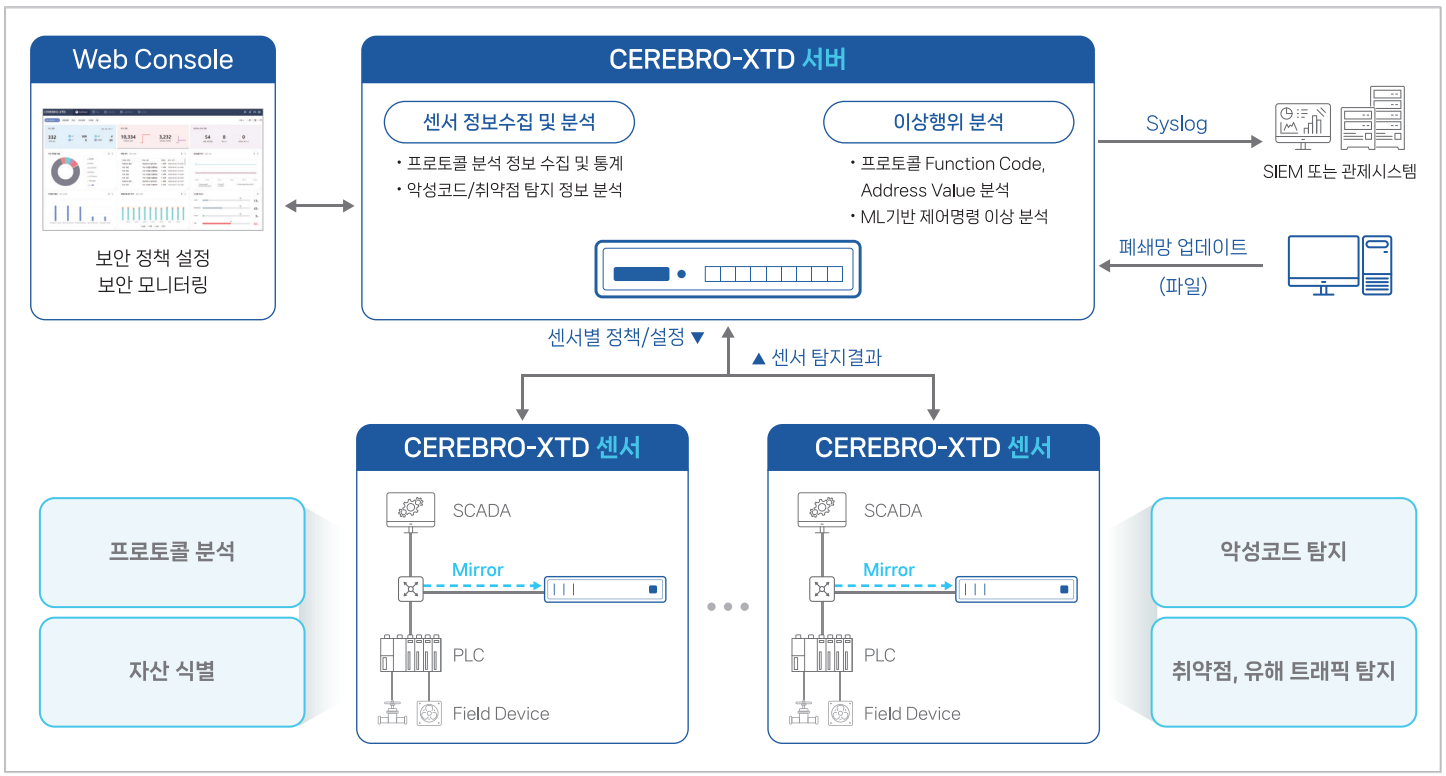
CEREBRO-XTD는 OT망 가시성을 제공하며, 보안 위협 및 이상 행위를 실시간으로 탐지하는 산업제어시스템 특화 보안 솔루션입니다. 설비 운영에 간섭하지 않는 패시브 모니터링 방식으로 동작하여 네트워크 운영의 안정성을 지원합니다.



- 통합적인 자산 가시성
- 보안 위협 탐지 및 대응
- 설비 운영 가용성 보장

시스템 구성

CEREBRO-XTD의 기본 구성은 중앙의 서버와 각 공정별 센서로 이루어져 있습니다. 공정별로 설치된 센서는 미러링된 트래픽을 분석하여 탐지 결과를 중앙 서버로 전달하며, 중앙 서버는 수집된 정보를 분석하여 가시성 및 위협 정보를 제공합니다. 소수 공정으로 이루어진 환경을 위하여 센서와 서버가 결합된 올인원 구성 또한 가능합니다.



주요 기능

자산 가시성

IT/OT/IoT 디바이스 식별 및 정보 수집
네트워크 세션/서비스 및 토폴로지

보안 위협 탐지

안랩 TS엔진 기반의 악성코드 탐지
취약점 및 유해 트래픽 탐지

ICS 프로토콜 DPI

국내외 설비의 표준/비표준 프로토콜 분석
Function Code /Address Value의 상세한 DPI

안랩 EPS 연동 통한 가시성/대응 고도화

AhnLab EPS 연동을 통한 자산 가시성 고도화
AhnLab Xcanner 연동을 통한 의심시스템 악성코드 원격 진단

베이스라인 기반 이상 징후 탐지

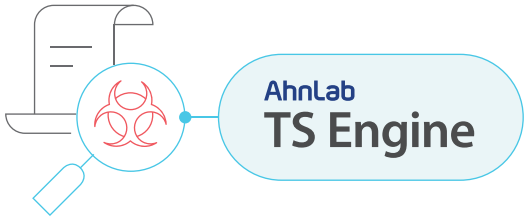
학습을 통한 베이스라인 관리
ML기반 제어 설정 이상 탐지

외부 관제 시스템 연동

고객사 관제시스템 연동을 위한 Syslog 연동
AhnLab ICM을 통한 통합 이벤트 모니터링

악성코드 탐지

CEREBRO-XTD는 랜섬웨어와 같은 악성코드의 침투 및 내부 전파를 탐지하는 핵심 기능을 제공합니다. 안랩 TS 엔진이 보유한 수백만 이상의 탐지 패턴과 고도화된 진단 기법을 적용하여 신/변종 악성코드에 대한 정밀 검사를 수행합니다. 다양한 통신 프로토콜과 다중 압축 파일, 실행파일 및 모바일 악성코드를 통합적으로 진단할 수 있습니다.



ICS 제어로직 이상 탐지

제어시스템 타깃 공격과 휴먼 에러로 인한 오작동에 대한 머신 러닝 기반 탐지로 안정적인 설비 운용 환경을 제공합니다.
산업제어시스템 프로토콜에 대한 심화된 DPI 기술을 기반으로 제어 명령 밸류(Value)에 대한 이상 행위를 분석합니다. 특히, 모니터링 대상이 되는 특정 태그에 대한 머신러닝 분석을 통해 이상(Anomaly)을 탐지할 수 있습니다.

보안 위협 이슈 트래킹

OT망 내부에서 전파되는 보안 위협의 근원지를 추적(Issue Tracking)하여 보안 위협에 대한 가시성을 높여줍니다. 공격이 전파된 이전 유포지를 확인하여 공격의 이동 경로를 파악할 수 있으며, 전파 경로를 추적합니다. 보안 위협 이슈 트래킹 기능은 지속적으로 유포되는 공격에 대해 관리자가 효과적으로 대응할 수 있도록 지원합니다.

NAONWORKS
an AhnLab Company

(주)나온웍스
서울시 구로구 디지털로 271 벽산디지털3차 711호, 08381
TEL 02-2025-1630 **E-MAIL** info@naonworks.com
www.naonworks.com