AhnLab

White Paper

OT 환경에도 '통합 보안'이 필요한 이유

OT 보안이란?

이제 범용적으로 쓰여지는 'OT'의 정의는 무엇일까? OT(Operation Technology)란 산업의 운영기술 환경으로, 산업 제어시스템(Industrial Control System: ICS) 뿐만 아니라 IT와 연결되거나 함께 사용되는 광범위한 영역을 뜻한다. 그리고, OT 보안은 위와 같은 OT 환경을 보호하는 행위나 체계를 일컫는다.

자연스럽게 또 하나의 질문이 생긴다. 'IT 보안과 OT 보안은 어떻게 다른가?'. 이 질문은 IT 보안 체계로 OT 환경을 보호할 수 없는지에 대한 의문이기도 하다. 이 질문에 대한 답을 내리기 위해서는 IT와 OT의 본질과 차이점을 이해해야 한다.

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

우선, 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 절대 멈춰서는 안되기 때문이다.

IT와 OT 환경은 구성되는 기기에도 차이가 있다. IT 환경은 잘 알려진대로 PC, 노트북, 모바일, 서버 등의 IT 기기로 구성이 된다. 반면, OT 환경은 기존 IT 기기에 산업제어시스템(Industrial Control System: ICS)가 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 설비이다.

종합하면, OT 보안은 IT 보안과 본질적인 차이가 있으며, 기존 IT 기기에 대한 위협에 ICS 보안까지 고려해야 한다는 결론에 이르게 된다.

OT 보안 침해 사례

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. 특히, OT 환경은 설비를 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.

최근 주요 OT 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.

OT 보안 위협 이해하기

OT 환경을 노리는 악성코드를 보면, 웜이나 랜섬웨어와 같이 자체 전파 기능을 가진 악성코드가 사용자 부주의로 내부에 들어오거나, 인터넷에 연결된 IT망을 통해 감염이 일어나곤 한다. 일반 악성코드와 달리, ICS 관련 시스템을 공격하기 위해 제작된 악성코드는 산업 기밀 유출이나 설비 가동 중단과 같은 심각한 피해를 발생시킨다.

그렇다면 OT 환경은 어떻게 침해되는 걸까? 일반적으로는 다음 두 가지 경우에 해당된다.

1. 해킹

보통 OT망 내 시스템은 외부에서 접속할 수 없게 분리되어 있지만, IT망의 일부 시스템과는 연결되어 있다. 원격 제어 프로그램으로 시스템을 관리하기도 하므로 원격 제어 프로그램의 계정 정보가 유출되지 않도록 주의해야 한다. 또한, 악의적인 의도를 가진 내부 직원에 의한 내부자 위협(Insider Threat)에 대해서도 유의해야 한다.

2. 악성코드 – 웜, 바이러스, 랜섬웨어 등

OT망 내에서는 정해진 보안 절차를 지키지 않아 악성코드 감염이 종종 발생하곤 한다. 일반적인 악성코드는 OT 환경 공격 기능을 가지고 있지 않아 트래픽 발생 및 충돌 등의 문제가 발생할 수 있지만 시스템 운영에 큰 영향을 주지 않는다. 하지만, 특정 OT/ICS 환경을 노린 악성코드의 경우 공격자가 원하는 내용의 데이터 조작, 손상 등이 발생할 수 있다.

또, OT 시스템은 USB 메모리 등 저장 매체를 직접 연결할 수 있다. 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.

다음으로 공격 경로를 보면, OT 환경을 노리는 공격들은 보통 ▲IT망 ▲직접 접근(협력 업체) ▲공급망을 통한다.

1. IT망

OT 망은 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.

2. 직접 접근(협력 업체)

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. 다만, 공격자는 외부와 통신할 수 없으므로 OT망 내에서 사용 중인 시스템 종류, 버전 등의 정보를 최대한 수집하고 그에 맞는 맞춤형 악성코드를 제작해야 한다.

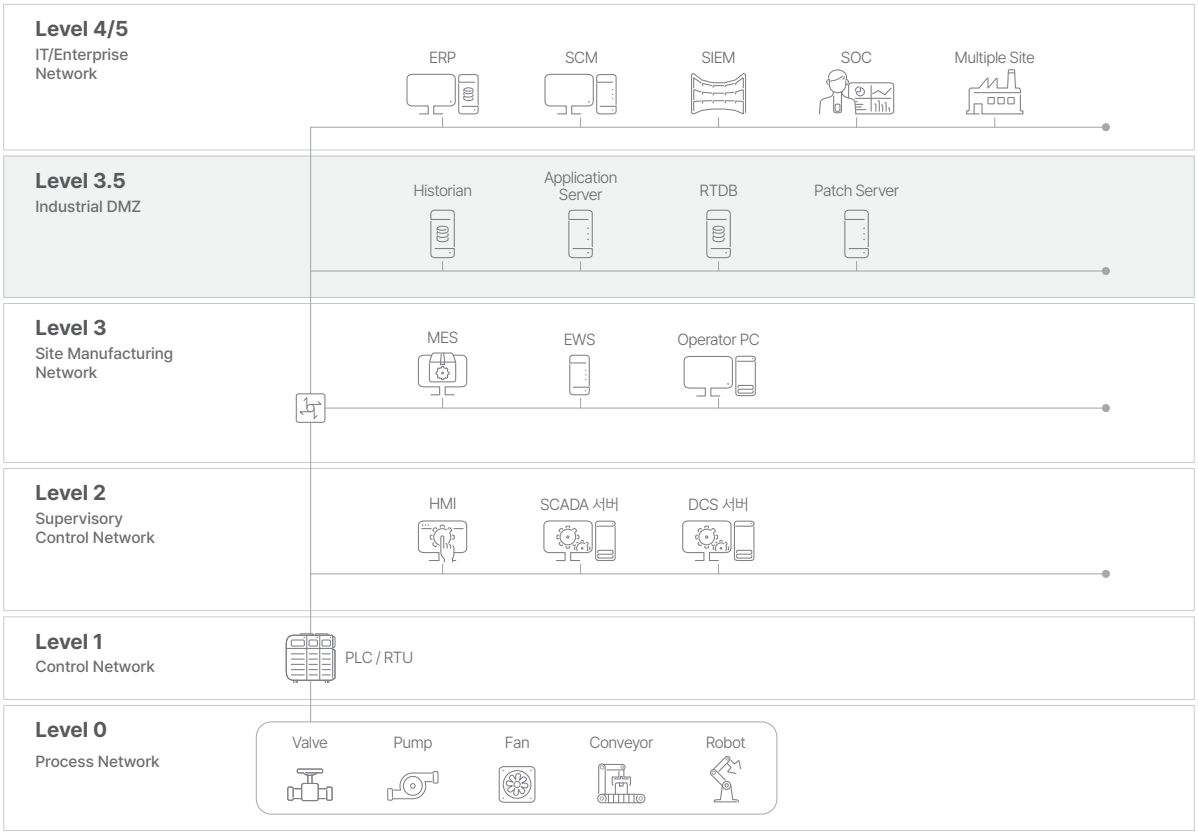
3. 공급망

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.

OT 환경 구조 이해하기

OT 보안은 그 동안 여러가지 이유로 우선순위에 오르지 못했지만, 더 이상 미룰 수 없는 과제가 되었다. OT 환경을 향한 위협이 날로 커지는 가운데, 진정한 제조혁신을 위해서도 OT 보안은 선택이 아닌 필수로 자리 잡았다. 그렇다면, 현 상황에서 OT 보안 체계는 구체적으로 어떻게 수립해야 할까?

효과적인 OT 보안 전략을 수립하려면 먼저 OT 환경 구조를 이해해야 한다. OT 보안 구조를 이야기할 때 일반적으로 많이 사용하는 '퍼듀 모델(Purdue Model)'을 기준으로 OT 환경은 레벨 0부터 5까지 총 6개 계층으로 나뉜다.



[그림 1] 퍼듀 모델

다만 Level 3의 특성을 고려하여 Level 3.5로 하나의 계층을 추가적으로 세분화하여 보기도 한다. 각 계층에 대한 설명은 다음과 같다.

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 1계층으로 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 현장에서 수집한 데이터를 은행 ATM과 같이 화면으로 변환해 효과적인 운영이 가능하도록 한다.

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.

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 4~5: Enterprise Biz System – 자원관리(ERP), 공급망관리(SCM), 고객관계관리(CRM) 등 기업이 일반적으로 IT 환경에서 사용하는 자원들로 구성된다. 공정과 관련된 전사적 비즈니스를 관리한다.

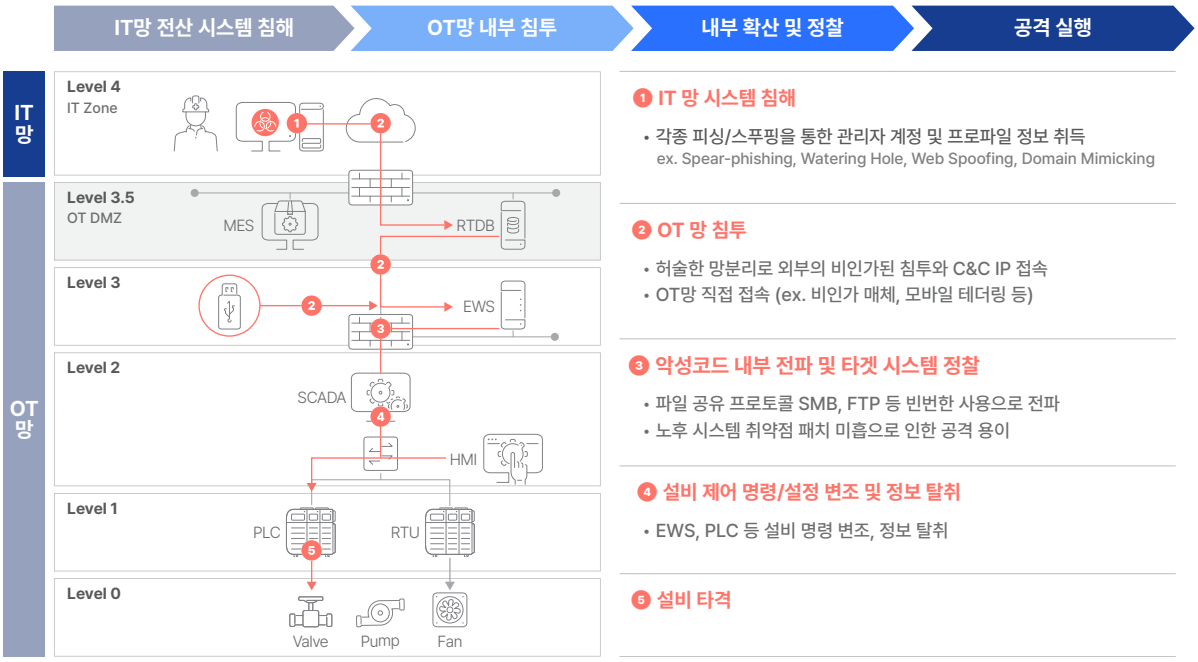
OT 환경 공격 전개 과정

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)	· Sensor · Actuator · 생산 설비	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		· RTBD · Historian · 애플리케이션 서버	OT와 IT 영역의 접점 혹은 완충지대
4~5	IT망	– ERP – SCM – CRM	공정과 관련된 전사적 비즈니스 관리

[표 1] OT 환경 계층 별 내용 정리

위 내용을 토대로 OT 환경을 침해하는 최신 공격의 흐름도를 살펴보자.



[그림 2] OT 환경 공격 전개 과정

OT 환경의 보안 위협은 IT 환경으로부터 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.

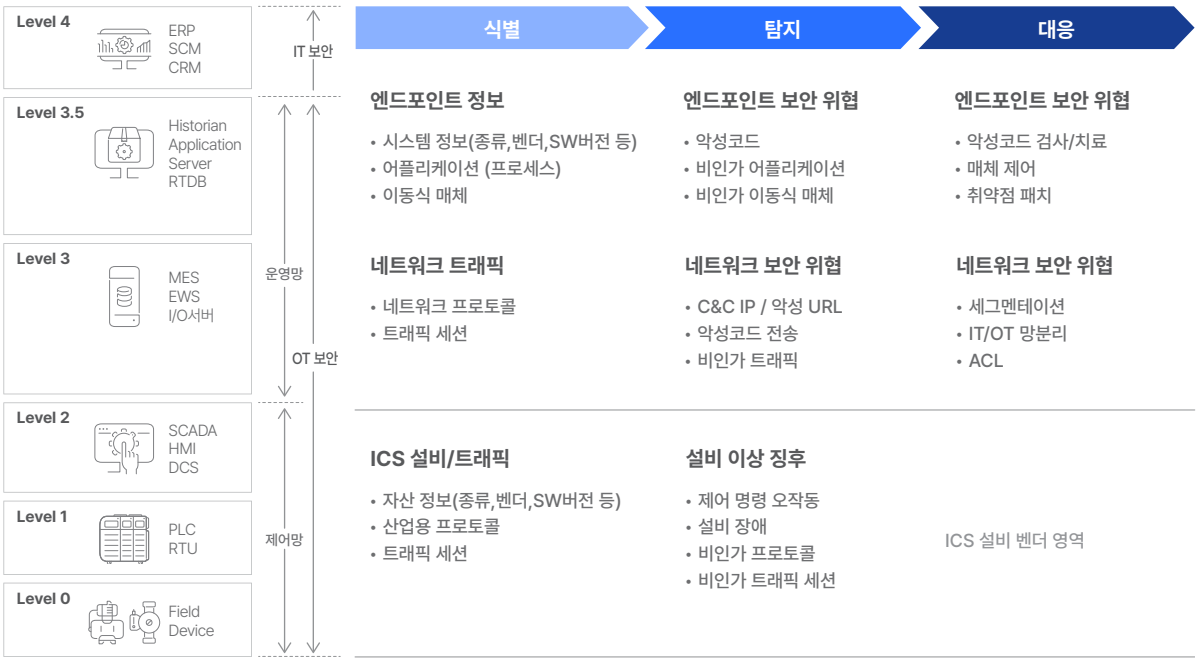
과정을 살펴보면, 공격자는 OT망을 관리하는 IT망 시스템을 피싱이나, 지능형지속위협(Advanced Persistent Threat: APT)과 같은 다양한 기법으로 침투한다. 이후, OT망 시스템 접속을 위한 관리자 계정과 IP, URL 등 다양한 프로파일 정보들을 탈취한다. 이후, 허술한 망분리 정책이나 관리가 미흡한 지점을 포착해 OT망으로 침입한다. 이 밖에, 보안 관리가 되지 않은 USB를 통해서도 OT망에 악성코드가 전파될 수 있으며, 모바일 테더링을 통해 비인가된 노트북을 설비에 직접 연결할 경우에도, OT망 경계 보안을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

이는 OT망 공격의 시작점이 될 수 있다. 거듭 강조하지만, OT 보안을 별도로 볼 것이 아니라, IT 보안과 연결하여 함께 고려해야 한다.

OT 보안 요구사항 및 접근법

OT 보안은 기본적으로 '식별 > 탐지 > 대응' 프로세스가 필요하다는 점에서 IT 보안과 다르지 않다. 다만, 최신 OT 보안 위협에 효과적으로 대응하기 위해서는 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] OT 보안 프로세스 및 보안영역 별 요구사항

A. 식별

IT & OT 융합보안에서 '식별'이라 함은 운영 중인 자산과 관련 정보에 대한 투명한 '가시성' 확보를 의미한다. OT 환경에서 가시성이 필요한 이유는 효율적인 OT 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/ICS 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 OT 환경에 존재하는 위협 요소와 이상징후를 탐지해야 한다.

먼저, 제어망에서는 ICS 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 공격자 서버(C&C) IP나 악성 URL, 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. 우선, 제어망 ICS 설비에 대한 위협 대응은 설비의 특수성으로 인해 설비 제조업체에서 지원을 받아야 한다.

다만, 운영망에 대해서는 능동적인 위협 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.

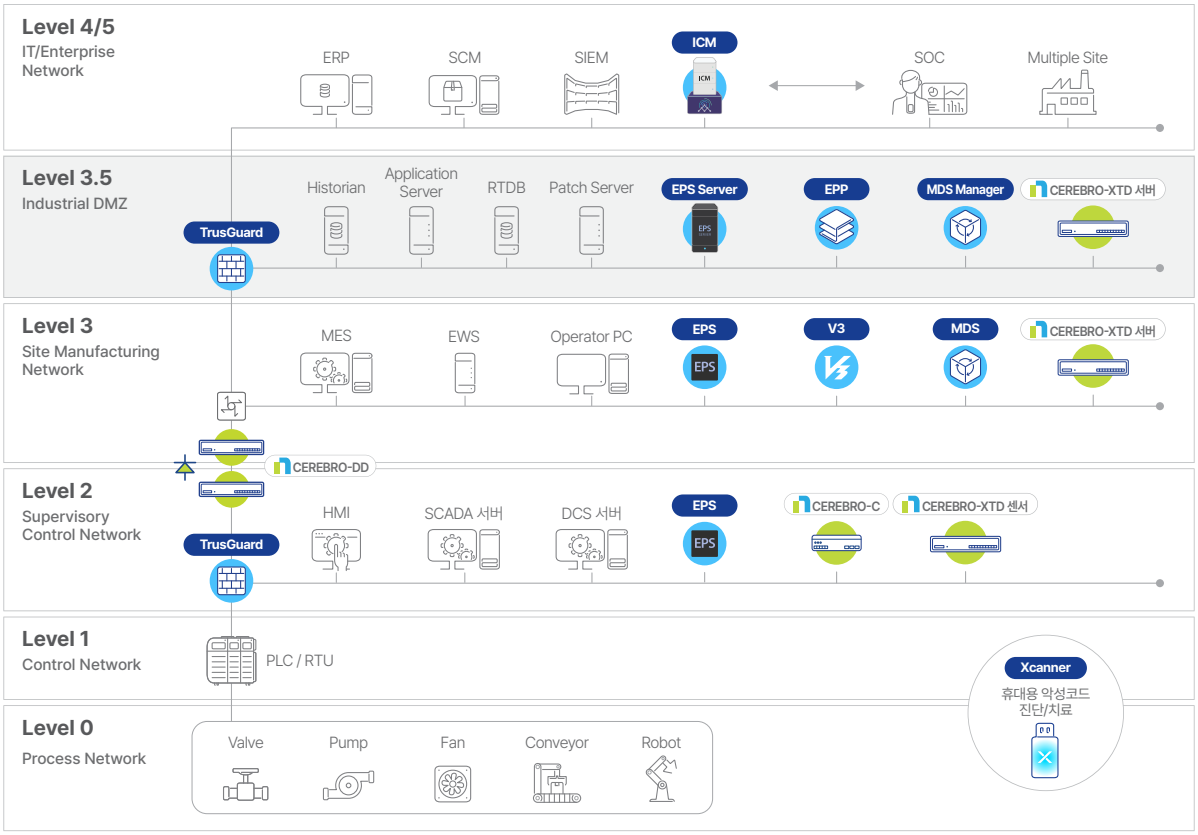
위와 같은 단계별 보안 역량을 갖추기 위해 필요한 보안 솔루션들을 간단히 살펴보면, 먼저 엔드포인트 영역에서는 안티멀웨어(Anti-Malware), 화이트리스트 기반 애플리케이션 및 매체 제어 솔루션, 패치 관리 솔루션 등이 필요하다. 네트워크에서는 자산 식별 및 위협 탐지를 위한 침입탐지시스템(IDS)이 기본적으로 요구되며, 대응을 위한 단방향 데이터 전송, 방화벽 등의 솔루션을 갖춰야 한다. 마지막으로, ICS 설비는 다양한 산업용 프로토콜에 대해 DPI(Deep Packet Inspection) 분석 기술을 기반으로 이상 징후를 분석하는 솔루션이 필요하다.

이처럼 여러 구성 요소로 이뤄진 IT & OT 융합 보안을 효과적으로 운영하기 위해서는 각각의 개별 솔루션을 넘어 통합 보안 프레임워크를 기반으로 유기적인 연동과 보안 체계가 요구된다.

안랩 통합 OT 보안 프레임워크 정의 및 도입효과

안랩은 지난 2021년 7월, 통합 OT 보안 수요 확대에 대응하기 위해 산업제어 프로토콜 융합 보안 솔루션 전문기업 나온웍스를 인수했다. 나온웍스는 2017년 OT 프로토콜 표준화를 위한 게이트웨이 솔루션 출시를 시작으로, 특화된 OT 프로토콜 식별 및 분석 기술과 보안 플랫폼, 개방형 아키텍처 기반 엣지 컴퓨팅 플랫폼을 기반으로 OT와 ICS 환경에 특화된 보안 솔루션 '세레브로(CEREBRO)' 시리즈를 공급해왔다.

기존 탁월한 IT 보안 역량을 갖춘 안랩은 나온웍스를 인수함으로써 자사의 보안위협 탐지 & 대응 및 분석 기술과 나온웍스의 산업용 프로토콜 분석 기술을 결합해 통합 OT 보안 프레임워크를 구축했다. 다음은 OT 환경 계층 별로 안랩 통합 OT 보안 프레임워크 구조를 정리한 것이다.



[그림 4] 안랩 통합 OT 보안 프레임워크

사용자 입장에서 안랩 통합 OT 보안 프레임워크의 가장 큰 가치는 OT 환경 전계층에 걸쳐 '식별 > 탐지 > 대응'으로 이어지는 통합 보안 프로세스를 구축할 수 있다는 것이다. 안랩과 나온웍스의 솔루션은 보안 프레임워크 하에서 필요한 역할을 수행하며 시너지를 낸다. 또한, 플랫폼 관점에서 연동을 지속적으로 강화해 엔드포인트-네트워크 보안에 걸쳐 사용자의 관리 효율성도 향상시키고 있다. 다음은 안랩 통합 OT 보안 프레임워크 구성 솔루션의 보안 단계 별 역할을 정리한 것이다.

	1단계 : 모니터링 & 식별	2단계 : 위협 탐지	3단계 : 대응	4단계 : 후속조치
AhnLab ICM	• 통합 로그 모니터링	• 로그 분석 • 상세 분석 리포트 조회	• Lockdown 예외처리 항목 변경 • 악성코드 정책 미적용 에이전트 확인	• 치료여부 확인 • Rest API 대응 정책 적용
AhnLab EPS	• 생산설비 자산 식별	• Known 악성코드 탐지	• 악성코드 검사 • 비인가 프로세스 차단 • 매체 실행 차단	• Lock모드 전환 • AhnReport 분석 요청
AhnLab Xcanner			• 감염 PC에서 악성코드 진단/치료	
AhnLab MDS		• Known/Unknown 악성코드 탐지 • 감염 장비의 네트워크 이상행위 탐지 • 행위 분석 우회 위협 탐지	• MDS 정오탐 여부 확인 • 핀포인트 검사	
AhnLab TrusGuard		• 네트워크 보안위협 탐지 • 비인가 트래픽 탐지	• ACL 기반 비인가 세션 차단 • 유해 트래픽 차단	• 방화벽 정책 설정 • 네트워크 세그멘테이션
CEREBRO-XTD	• OT 자산 식별 • 자산별 트래픽 식별	• 악성코드 전파 탐지 • C&C 등 유해 트래픽 탐지	• 위협 탐지 대응 경보	
CEREBRO-C	• 설비 프로토콜 식별		• 설비 프로토콜 변환	
CEREBRO-DD	• 설비 프로토콜 식별		• 단방향 데이터 전송	

[그림 5] 단계별 보안 솔루션 구성 및 역할

간단히 종합하면, 안랩은 엔드포인트와 네트워크 영역에서 OT 환경을 보호하는 다양한 솔루션들을, 나온웍스는 산업용 프로토콜 표준화 및 분석 솔루션과 물리적 단방향 데이터 전송 솔루션을 갖추고 있으며, 공동 개발을 통해 솔루션 간 시너지를 극대화하고 있다.

통합 OT 보안 구성 솔루션들의 역할

안랩 통합 OT 보안 프레임워크를 구성하는 솔루션들은 구체적으로 어떤 역할을 할까? 위 [그림 5]의 내용을 구성 솔루션 별로 자세히 알아본다.

AhnLab EPS

AhnLab EPS는 안랩의 대표적인 OT 엔드포인트 보안 솔루션으로, 국내외 반도체, 디스플레이, 자동차 등 다양한 제조 생산 공장에서 사용되고 있다. AhnLab EPS를 사용하면 우선 웹 기반 관리 시스템을 통해 각각의 설비 시설에 산재되어 있는 시스템을 식별해 효율적으로 통합 관리할 수 있다. 또한, 화이트리스트 기반으로 인가된 프로세스와 매체만 사용을 허용해 OT 환경에 가해질 수 있는 위협을 최소화한다. 관리자 입장에서는 별도의 애플리케이션 허용리스트 생성 작업을 할 필요가 없어 정책 설정 부담 없이 유연하게 관리할 수 있다.

EPS Agent **허용리스트 기반의 EPS Agent**	VS.	 **차단리스트 기반의 기존 백신 제품**
사전 예방	처리 방식	사후 처리
허용된 애플리케이션만 사용	애플리케이션 실행 범위	모든 애플리케이션 사용 가능
변경 없음	엔진 크기	지속적인 변동 발생
낮음	자원 점유율	높음
높음	보안 수준	보통
에이전트에서 업데이트 불필요 (EPS 서버에서 업데이트, 정기적인 시스템 점검 시 스케줄링 가능)	엔진 업데이트	주기적인 엔진 업데이트 필요

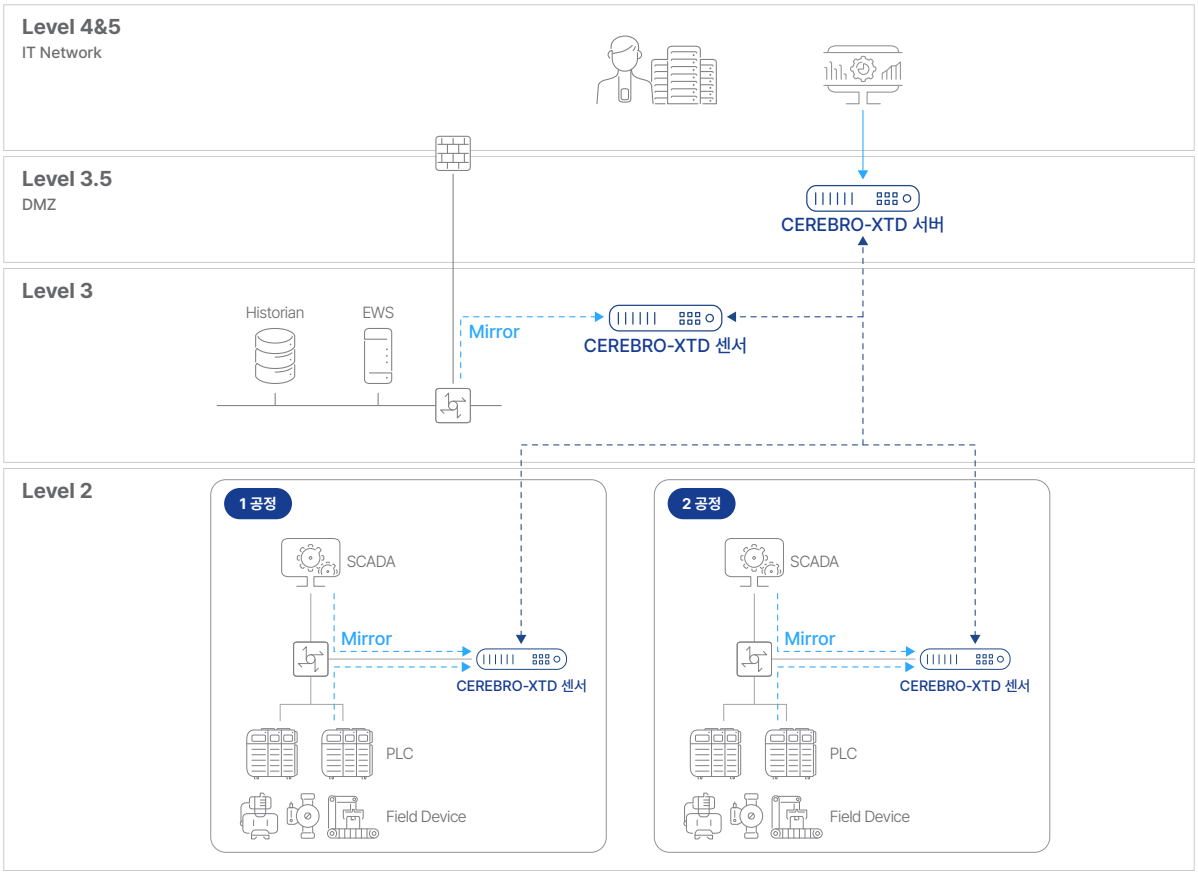
[그림 6] AhnLab EPS vs 기존 백신 제품

악성코드 탐지 및 분석은 EPS 중앙 관리 서버에서 수행해 운영 안정성을 보장한다. 단말 시스템에 설치되는 초경량 에이전트(EPS Agent)와 중앙 모니터링 및 정책 관리 서버(EPS Server)로 구성되는 것이 특징이다. 또한, 윈도우 XP와 같은 구형 운영체제와 다양한 리눅스 배포판 환경 및 임베디드 환경에서도 에이전트 운영을 지원한다.

또한, 안랩은 지난 2022년 말 OT 환경 내 자산에 대한 가시성 확보와 보안 관리를 제공하는 대형 제조장비 전용 보안 솔루션 'AhnLab EPS Relay'를 출시했다. 'AhnLab EPS Relay'는 ▲폐쇄망 내 위치한 다수 대형 자산에 대한 식별 ▲ 해당 자산에 미인가 애플리케이션 차단 · 매체제어 · 보안 정책 설정과 같은 'AhnLab EPS'의 주요 보안기능 일괄 적용 등 가시성과 보안관리 기능을 제공한다. 'AhnLab EPS Relay'를 이용하면 네트워크 패킷이나 프로토콜에 기반해 자산을 파악하는 기존 OT 보안 솔루션으로는 확인이 어려웠던 독립 폐쇄망 내 자산의 수량과 종류 식별, 보안 현황 등 정보를 파악할 수 있어 가시성 확보가 가능하다.

CEREBRO-XTD

안랩과 나온웍스가 공동 개발한 CEREBRO-XTD'는 종합적인 OT망 가시성을 제공하며, 보안 위협 및 이상 행위를 실시간으로 탐지한다. 가용성을 중시하는 OT 환경의 특성을 고려해 설비 운영에 영향을 주지 않는 '패시브 모니터링' 방식으로 동작해 운영 안정성을 더한다.



[그림 7] CEREBRO-XTD 운영 구조

CEREBRO-XTD는 안랩의 OT 엔드포인트 보안 제품군과 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.

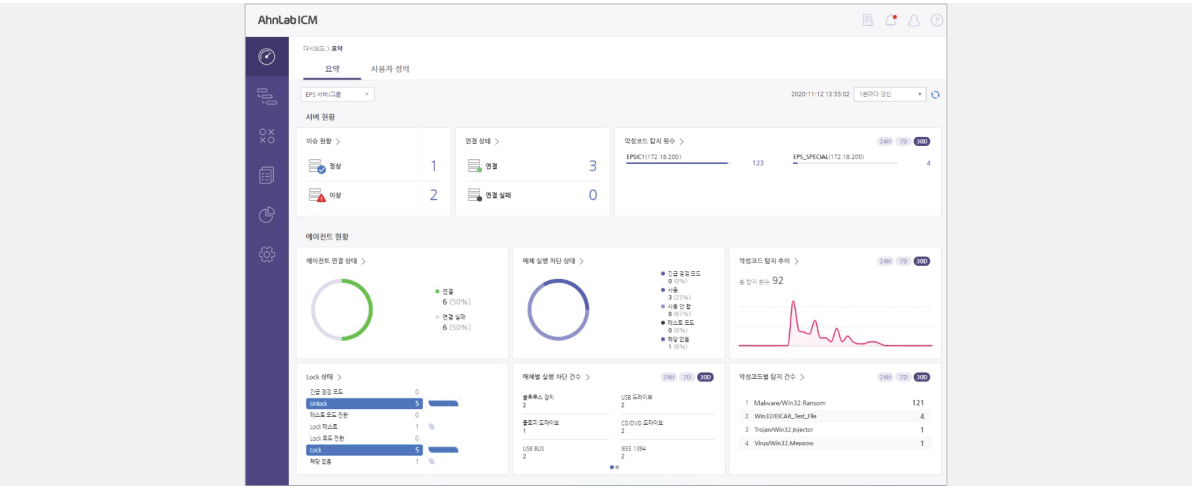
CEREBRO-XTD를 'AhnLab EPS'와 연동하면 OT망에 연결되어 있는 엔드포인트까지 가시성을 확대할 수 있다. 일반적인 동종 솔루션이 대부분 네트워크 영역까지 자산 현황을 제공한다. 그러나 CEREBRO-XTD는 AhnLab EPS와 연동해 네트워크 영역 데이터 뿐만 아니라 OT망에 연결된 서버 및 워크스테이션(Workstation)의 운영체제 패치 버전 등 엔드포인트의 상세정보까지 제공한다.

AhnLab 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.

AhnLab ICM

다양한 보안 솔루션을 운영할 경우, 솔루션이 탐지한 정보와 각종 이벤트를 통합적으로 수집해 모니터링 및 분석하여, 보안 복잡성을 해소하고 효율성을 향상 시켜야 한다. 이 관점에서 AhnLab ICM은 OT 환경 통합 매니지먼트를 제공한다.

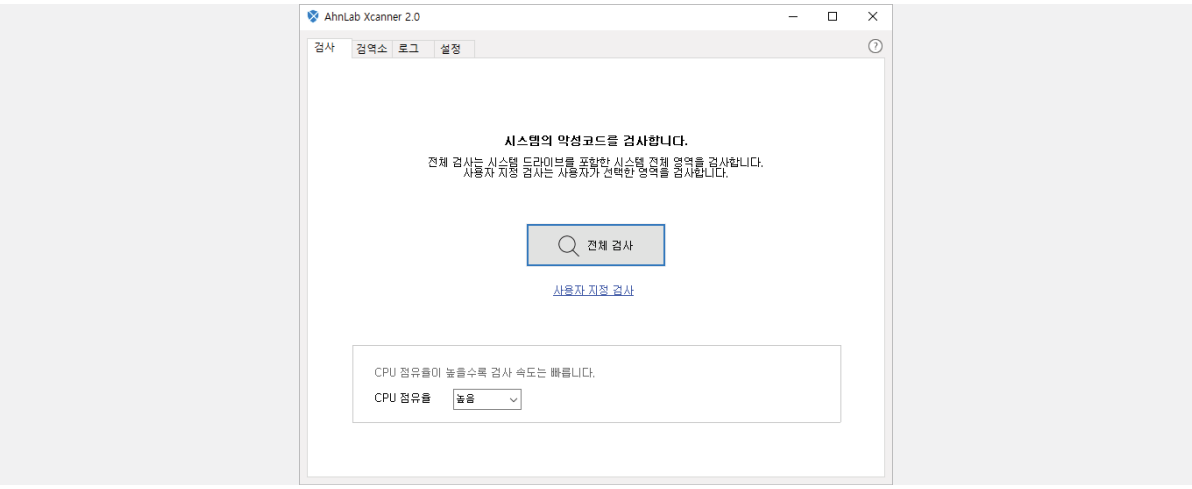


[그림 8] AhnLab ICM 대시보드

사용자는 직관적인 인터페이스로 시스템 모니터링 및 로그 분석을 진행할 수 있다. 또, 다양한 리포트와 알림 기능을 통해 적합한 조치를 취하고, 관리로 발생되는 총 소유 비용(TCO)을 절감하는 등 보다 효과적으로 시스템을 관리할 수 있다. 현재, 엔드포인트 솔루션인 AhnLab EPS, Xcanner, MDS와 네트워크 솔루션 CEREBRO-XTD를 통합 관리하며 향후 범위를 지속적으로 확대할 계획이다. 그리고, AhnLab ICM은 자사 위협 인텔리전스 플랫폼 'AhnLab TIP' 연동을 통해 여러 보안 솔루션에서 수집된 위협 정보들에 대한 추가적인 콘텐츠 분석 등을 제공한다.

AhnLab Xcanner

OT 환경의 특성 상, 에이전트를 설치할 수 없는 시스템들이 존재한다. 이와 같은 시스템에 대해 비상주형 안티바이러스 솔루션 AhnLab Xcanner를 통해 휴대용으로 악성코드 검사와 치료를 진행할 수 있다. 실시간 대응이 어려운 악성코드 감염 시스템에 대한 보안 조치 필요성이 높아짐에 따라, 관리자가 감염된 시스템을 효과적으로 사후 치료할 수 있도록 지원한다. 또한, AhnLab Xcanner는 Ahnlab EPS 연동을 통해 EPS 서버 관리자가 원격으로 AhnLab Xcanner를 실행시켜 추가적인 악성코드 검사와 치료를 수행할 수 있다.

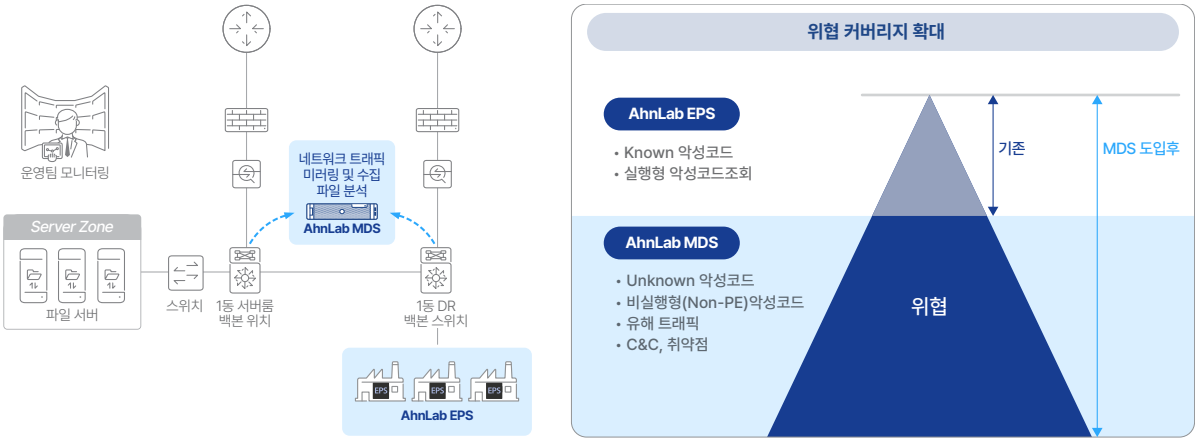


[그림 9] AhnLab Xcanner 화면

AhnLab Xcanner는 운영 상황에 맞게 대응할 수 있는 검사 및 치료 옵션을 설정할 수 있으며, 검사 불필요 폴더나 파일에 대한 예외를 둘 수 있어 사용자 입장에서 효율적으로 활용할 수 있다. 또한, 기존 설치된 보안 에이전트 삭제 없이 충돌을 최소화하기 때문에 운영에 대한 부담 없이 검사와 치료를 진행할 수 있다.

AhnLab 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.



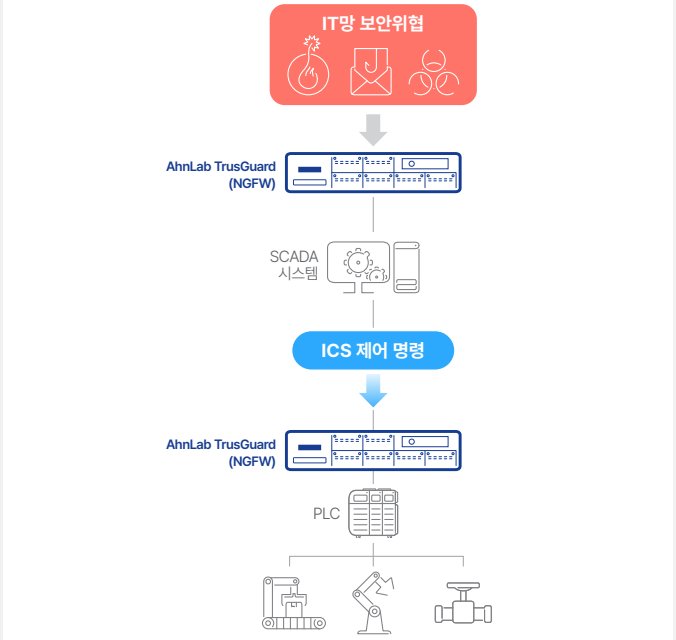
[그림 10] AhnLab EPS & AhnLab MDS 연계를 통한 위협 커버리지 확대

안랩의 샌드박스 기반 APT 대응 솔루션 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.

기존 알려진 악성코드를 탐지해 대응하는 AhnLab EPS와 연계하면, 알려진 혹은 알려지지 않은 악성코드까지 모두 방어가 가능해 종합적인 위협 대응 커버리지를 확대할 수 있다.

AhnLab TrusGuard

네트워크 영역에서는 차세대 방화벽 AhnLab TrusGuard가 중추적인 역할을 한다. 우선, OT망 경계에서 유해 트래픽을 탐지해 접근을 차단하고, IPSec/SSL VPN 등 보안 통신과 네트워크 세그멘테이션 등의 기능도 지원한다.

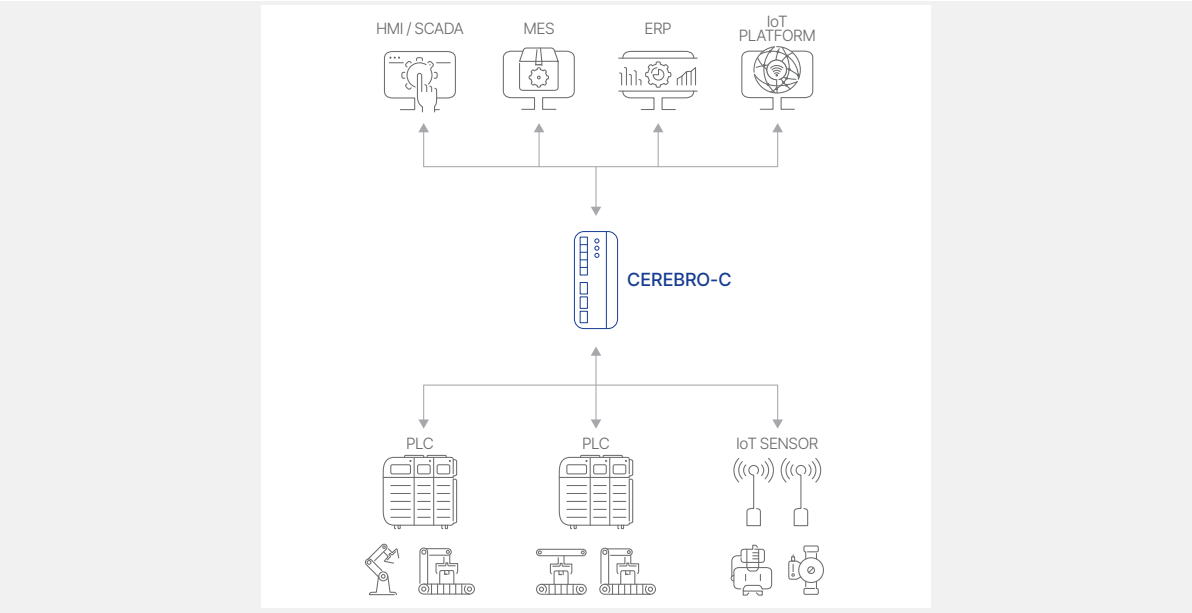


[그림 11] AhnLab TrusGuard OT 보안 위협 대응 구조

또한, 나온웍스의 ICS 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.

CEREBRO-C

나온웍스의 CEREBRO-C는 OT와 ICS 네트워크 통합 관리를 위한 산업용 프로토콜 게이트웨이다. 다양한 설비의 프로토콜을 보안성이 탑재된 OPC-UA, MQTT 등 표준 프로토콜 변환하여 전달함으로써 제어망의 보안을 강화한다.



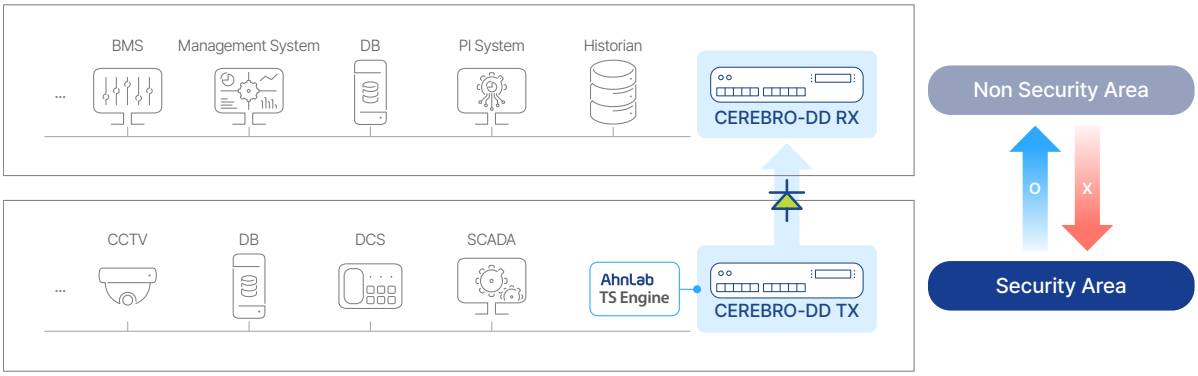
[그림 12] CEREBRO-C 동작 구조

CEREBRO-C는 필드버스(Fieldbus), 이더넷(Ethernet) 등 다양한 장치 연결, 상위 시스템 인터페이스 연동, 윈도우/리눅스/컨테이너 멀티 플랫폼 지원 등 탁월한 호환성을 자랑한다. 데이터 수집과 연계 및 현장 통합 관리를 위한 시스템을 구축하거나 신규 설비를 도입하는 경우, 기존 네트워크 구성 변경 없이도 서로 다른 통신 프로토콜로 인한 연동 문제를 해결할 수 있다.

CEREBRO-DD

OT 보안에서 중요한 요소 중 하나가 바로 망분리다. 이는 보안 수준이 높은 OT망의 데이터 유출을 막고, 외부망으로부터 악성코드 등 위협 및 접근을 차단하기 위함이다. 하지만 최근 OT와 IT 간 연계의 중요성이 커지면서 분리된 망 간 안전한 데이터 전송에 대한 요구가 높아지고 있다.

보안 수준이 서로 다른 망 간 데이터 연계를 가능하게 하면서 OT 등 보안 영역으로의 외부 보안 위협을 원천 차단하는 것이 바로 '물리적 일방향'이다. 물리적 일방향 보안 솔루션 CEREBRO-DD는 OT에서 IT로의 안전한 데이터 전송 환경을 조성하고, 완벽하게 OT망을 보호한다.



[그림 13] CEREBRO-DD 개념도 (TX: 송신 서버 / RX: 수신 서버)

CEREBRO-DD는 보안 강화를 위해 일방향 통신 구간에 알려지지 않은 프로토콜을 사용한다. 또한, 안랩 의 안티바이러스 엔진을 적용해 다각도의 검사를 진행한다. 자료 전송 시 정책 검사, 시그니처 검사, 악성코드 검사를 수행해 데이터의 안정성을 보장한다.

결론

OT 환경의 보안 위협은 날이 갈수록 심화되고 있다. IT 환경에 비해 피해 영향이 크고, 사회적인 문제로 연결되거나 기업에 막대한 손실을 입히기도 한다. 이러한 이유로 OT 보안에 대한 관심이 매년 높아지고 있다. 그러나, 기존 IT 환경과 다른 특성을 가진 OT 환경은 설비의 운영을 멈추고 보안 솔루션을 도입하기가 쉽지 않아, 아직까지는 적극적인 움직임을 취하지 않는 기업들이 많다. 하지만, 매년 OT 보안 사고 발생률이 증가하고 있는만큼, 관망하기 보다는 능동적으로 OT 보안에 대한 고민을 할 때라고 여겨진다.

아직은 OT 보안이 기술적으로 생소하고 어렵게 느껴질 수 있다. 만약 그렇다면, 다음 3가지를 꼭 기억해 두길 바란다.

#1. OT 환경을 보호하려면, IT 보안도 함께 고려해야 한다.

OT 환경의 보안위협도 OT 환경과 연결된 IT 환경으로부터 시작되며, OT 영역이 침해당하면 피해가 순식간에 확산된다. IT & OT 융합 보안이 필요한 이유다.

#2. OT 보안은 기본적으로 '식별 > 탐지 > 대응' 프로세스가 필요하다.

OT 환경은 자산이나 네트워크의 변경이 적다. 따라서, 자산에 대한 가시성을 확보하고 식별 베이스라인을 통해 보안 위협을 탐지하고, 적절히 대응해 나가는 프로세스가 필요하다.

#3. OT 보안을 위해서는 OT 환경 전 계층을 아우르는 통합 OT 보안 프레임워크가 필요하다.

IT & OT 융합 보안은 네트워크에 따라 IT망, OT 운영망, OT 제어망으로 나뉜다. 각 계층별 특징에 따라 적절한 보안 대책이 필요하며, 이를 위해 다양한 관점으로 관리적인 부분과 적절한 보안 솔루션들을 고려한 OT 보안 프레임워크를 구성해야 한다.

안랩은 나온웍스와 손잡고 최적의 OT 보안 파트너로서 통합 OT 보안 프레임워크를 계속해서 고도화해 나가고 있다. OT 보안의 중요성이 어느 때보다 부각되고 있는 만큼, 더 많은 기업들이 견고한 보안 체계를 수립해 안전한 비즈니스 환경을 조성하기 바란다.

AhnLab

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