GENIANS WHITEPAPER

Industrial Network and Security

산업용 네트워크와 보안

GENIANS, INC.
Next-Gen Network Access Control for the IoT era
mkt@genians.com

Genians

Introduction *

2019년 3월, 노르웨이에 위치한 세계 최대의 알루미늄 생산 공급사인 노르스크 하이드로(Norsk Hydro)가 랜섬웨어의 공격을 받았습니다. USB를 통해 유입된 악성코드(워너크라이 변종)는 외부와 차단된 공장 폐쇄망에 위치한 생산용 PC를 노렸습니다. 감염된 PC는 SMB(Server Message Block) 프로토콜과 AD(Active Directory) 서비스를 통해 확산을 시도하였으며 이를 탐지한 회사는 피해가 커지는 것을 방지하기 위하여 알루미늄의 압출 공정 다수를 중지시켰고 전 세계 모든 공장과 운영 네트워크를 분리하는 조치를 취하였습니다. 그러나 피해는 예견된 것이었습니다. 이 사고로 회사는 약 4,100만 달러(약 500억 원)의 피해가 발생했으며 주가는 3.4% 하락했을 뿐 아니라 전 세계 알루미늄의 가격이 1.3% 상승하였습니다.

최근 제조공장(Factory)과 산업 인프라 등 주요 산업시설을 대상으로 하는 사이버 공격이 증가하고 있습니다. IT 환경에서 발생하는 공격과 비교할 때 그 횟수는 미미한 수준이나 사고 발생 시 피해는 금전적 손실을 넘어 우리의 생활에 큰 영향을 줄 수 있으며 인명까지도 위협할 수 있는 심각한 수준입니다.

[주요 생산 시설 공격 사례]

이를 대비하기 위한 업계의 행보도 빨라지고 있습니다. 2020년 1월 액센추어(Accenture)가 시만텍(Symantec)의 사이버 보안 부문을 인수함과 동시에 레볼루셔너리 시큐리티(Revolutionary Security)를 인수할 계획을 발표했습니다. 인사이츠 파트너스(Insight Partners)가 이스라엘의 IoT 보안 전문 업체인 아미스(Armis)를 11억 달러에 인수하였으며, 산업 제어 시스템(ICS) 전문 회사인 록웰 오토메이션(Rockwall Automation)이 이스라엘의 사이버 보안 업체인 애브넷 데이터 시큐리티(Avnet Data Security)를 인수하였습니다. 이렇듯 자동화 전문 기업과 OT 보안 그리고 IT 기업과 OT 전문 업체 간 협력과 인수합병이 활발해지고 있습니다.

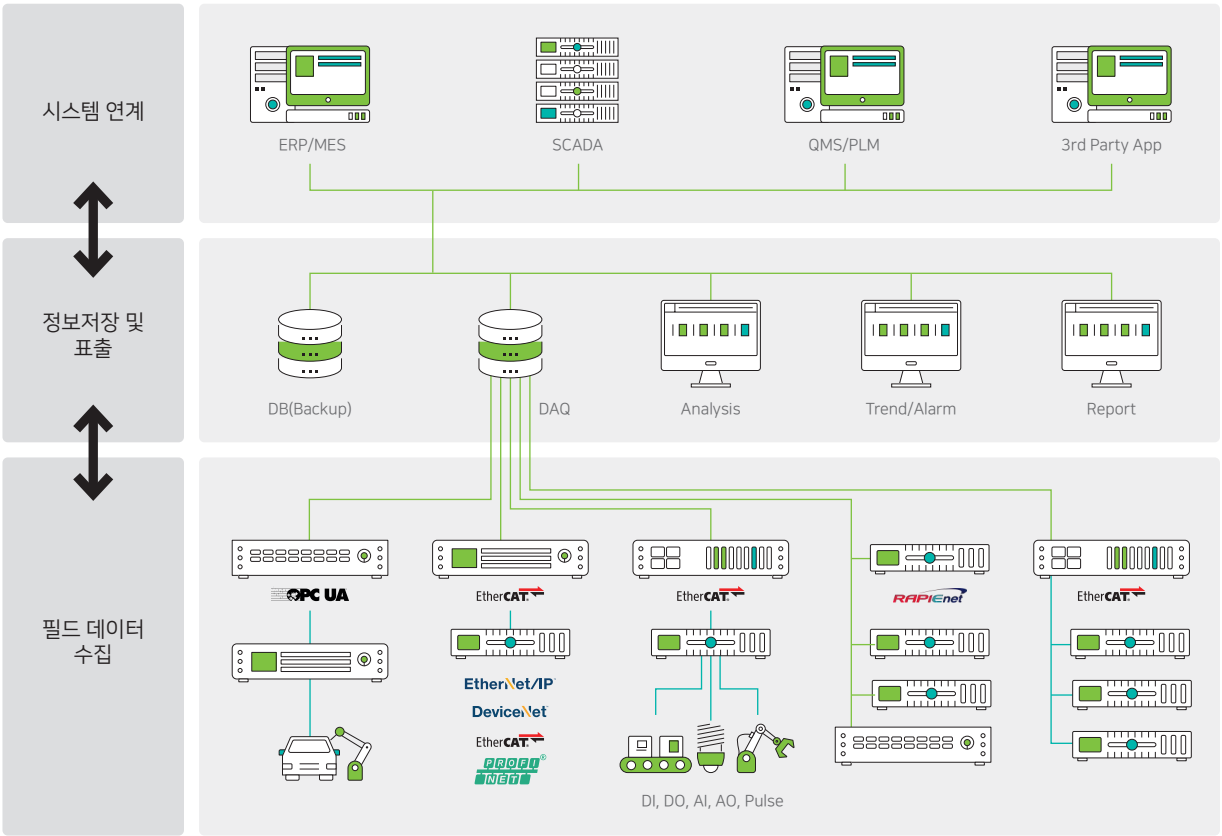
많은 보안 전문가들은 이제 사회 기반시설이나 생산시설에도 사이버 공격에 대한 대비가 필요하다고 언급하고 있습니다. 또한 이러한 인수합병의 사례를 통해 IT(Information Technology, 정보기술) 보안과 OT(Operational Technology, 제조운영기술) 보안 기술이 빠르게 융합될 것이라고 전망하고 있습니다.

단 하루라도 사이버 공격으로 전기와 수도가 단전 단수되고, 대중교통의 혼란과 인터넷이 불통되는 곳에서의 삶이란 끔찍하지 않을 수 없습니다.

산업용 제어시스템과 네트워크

생산시설을 위한 '산업 제어시스템(ICS, Industrial Control System)' 네트워크는 지난 수 십 년 동안 더디지만 꾸준히 발전해 왔습니다. 산업용 이더넷(Ethernet)은 전통적인 산업용 필드버스(Fieldbus) 프로토콜을 능가하고 있으며, Industry 4.0을 필두로 스마트팩토리(Smart Factory), IIoT(Industrial IoT), 그리고 클라우드 및 인공지능은 제조와 생산에도 큰 영향을 미치고 있습니다. 지능형 생산 시스템을 갖춘 스마트팩토리는 아직 우리에게 익숙하지 않지만 많은 기업들이 기존 산업용 기술을 유지하면서 스마트팩토리로의 변화를 염두에 두고 있습니다. 이에 따라 ICS 네트워크 환경 역시 이더넷 채택이 빠르게 확산되는 등 변화가 시작되고 있습니다.

일반적인 IT(정보기술) 환경과 달리, OT(제조운영기술) 환경에서는 데이터 전송 지연(Delay), 다운타임 및 패킷 유실 등의 이상 증상 또는 장애를 허용하지 않습니다. EtherNet/IP 및 EtherCAT 그리고 RAPIEnet과 같은 산업용 이더넷 프로토콜(필드버스)은 디바이스 간 데이터 통신이 100% 완벽하게 송-수신되도록 설계되었습니다. 만약 이러한 프로토콜들이 없다면 디바이스 간 연결을 위한 다양한 종류의 게이트웨이(프로토콜 변환을 위한) 및 통신 스위치가 필요합니다. 그러나 표준화된 이더넷 프로토콜 덕분에 10Mbps에서 10G까지 빠른 속도의 산업용 이더넷의 장점을 활용해 성공적으로 네트워크를 고도화하고 표준화할 수 있게 되었습니다. 또한 통신 거리 연장을 위한 광케이블 활용과 무선 광대역 LoRa, NB-IoT, LTE-M 및 5G 등 다양한 통신 인프라를 선택할 수도 있게 되었습니다.



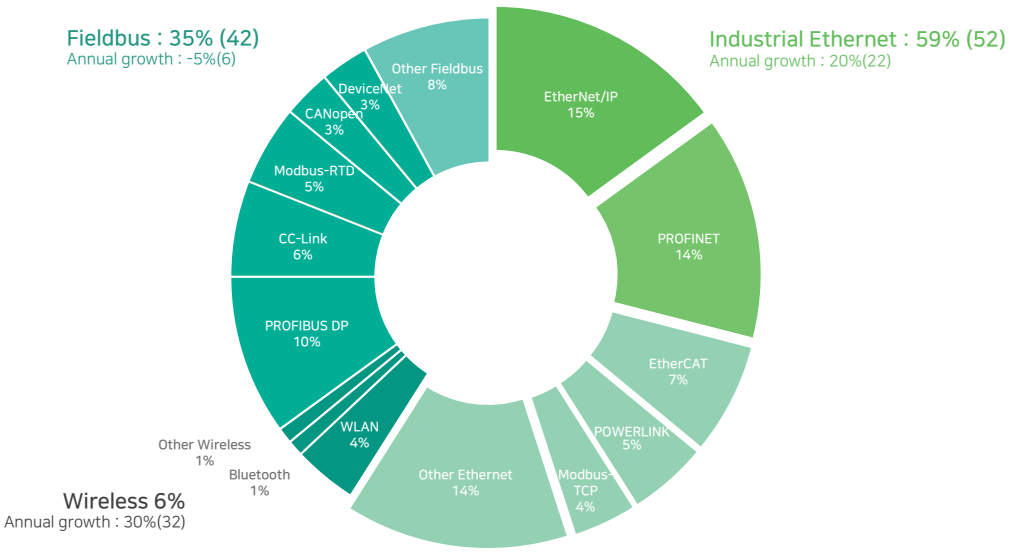
[스마트팩토리 개념, 지능형 공장으로의 진화를 의미]

스마트팩토리는 설계 및 개발, 제조 및 유통 등 전과정에 생산 자동화 솔루션과 정보통신기술(ICT)을 결합하고 데이터 분석 기술을 적용하여 생산성, 품질, 고객만족도를 향상시키는 지능형 생산공장으로 발전하고 있습니다. 이는 설비와 기계에 사물인터넷(IoT)을 설치하여 공정 데이터를 실시간으로 수집하고, 이를 분석해 스스로 제어할 수 있게 하는 미래형 공장으로의 발전을 의미합니다. 이제 공장 내 모든 설비가 연결되고 서로 데이터를 주고받으며 데이터를 기반으로 측정과 판단, 최적화가 이루어집니다. 우리가 집중하는 것은 바로 모든 것의 '연결'에 기반한 위험성 제거입니다.

산업용 네트워크 보안의 필요성

산업용 필드버스 프로토콜과 시리얼 통신은 현재도 사용 중이며 여전히 산업 인프라의 중추입니다. 일반적인 시각으로, 외부와 격리되어 폐쇄망으로 구성되어 운영되는 산업용 네트워크는 중요한 인프라의 가동을 보장하고 보안을 유지하는데 효과가 있었습니다. 그러나 스마트팩토리와 같이 IT(정보기술)와 OT(제조운영기술)를 연동해야 하는 요구가 높아지면서 유지 관리와 보안에 문제가 발생합니다. 이더넷과 TCP/IP는 오래된 기술이지만 클라우드와 모빌리티 등 다양한 인터넷 트래픽 요구에 부응하기 위해 지속적으로 발전되었습니다. 반면에 산업용 네트워크와 그 구성요소는 안정적인 지속 생산과 장애 예방을 최우선으로 하는 가용성에 중점을 두기 때문에 혁신에서 뒤쳐질 수밖에 없었습니다.

산업현장은 운영체제(OS) 제공 업체들이 더 이상 업데이트 지원을 하지 않음에도 불구하고 Windows 95 및 Windows XP가 탑재된 시스템을 여전히 사용하고 있습니다. 생산 설비는 엄격하게 통제되기 때문에 기계설비 운용 환경을 변경하려면 많은 시간과 비용이 수반되며 변화에 따른 위험도 감수해야 하는 특성이 있습니다. 그러나 이러한 어려움에도 불구하고 더 이상 이더넷을 이용한 네트워킹의 이점을 간과할 수 없게 되었습니다. 이더넷의 단순하고 효과적인 설계는 관리를 용이하게 할 뿐만 아니라 비교적 저렴한 하드웨어와 결합할 수 있어 산업용 네트워크에서 매력적인 수단이 되고 있습니다.

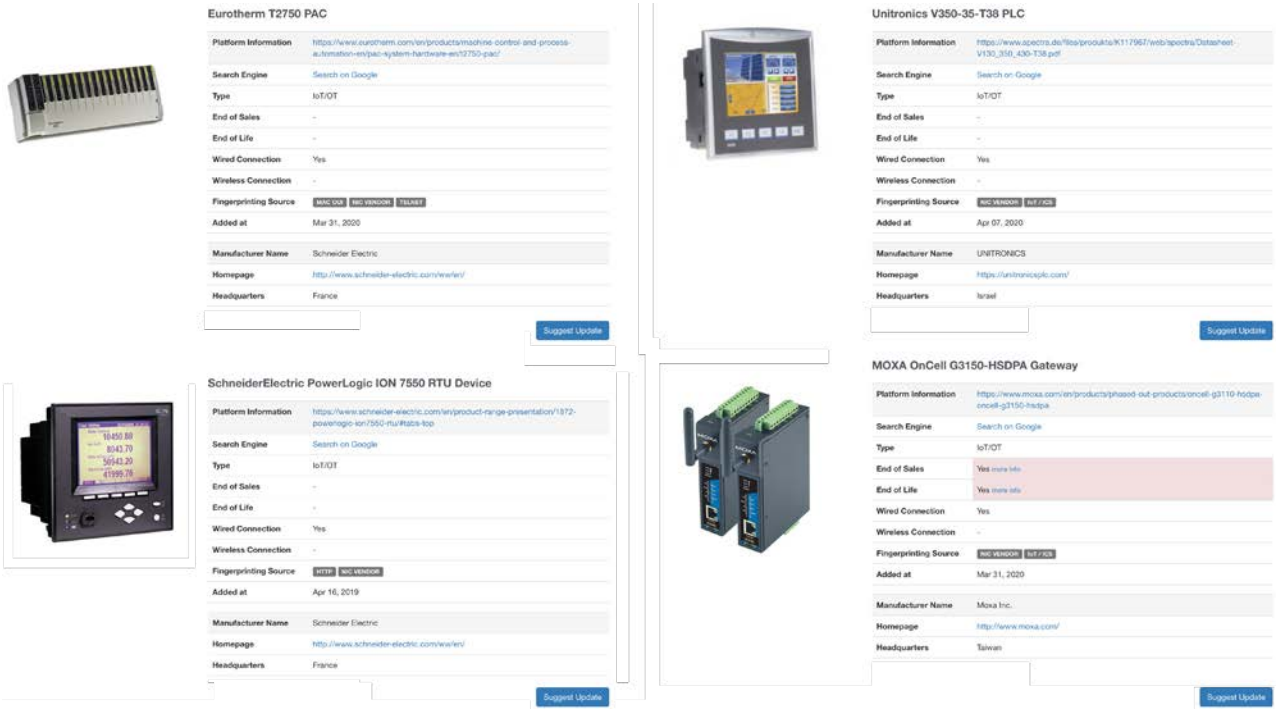


[ICS 프로토콜 시장 규모]

이더넷의 약점을 보완한 산업용 이더넷 프로토콜에 의해 에너지, 통신 및 철도 등 중요 인프라의 관리자는 이제 견고한 표준 이더넷으로 전환하여 산업 혁신의 발판을 마련할 수 있게 되었습니다. 산업용 이더넷은 의심할 여지없이 제조 자동화 및 중요 인프라 운용성 개선에 도움이 되고 있습니다. 제어 설비 공급사에 의존적이던 네트워크 인프라에서 이더넷 프로토콜로 이동함에 따라 산업용 OT 네트워크 보안은 더욱 중요해지고 있으며 주류시장으로 빠르게 성장하고 있습니다.

산업용 네트워크와 가시성(Visibility)

산업용 네트워크 역시 사이버 공격 및 네트워크 사각지대, 그리고 취약성(Vulnerability)을 포함하여 많은 잠재적 보안 문제를 내재하고 있습니다. 그러나 다수의 기업이 OT 영역 보호를 위한 효과적인 대응 방안을 확보하지 못하고 있습니다. 심지어 산업용 네트워크에 어떠한 장비나 설비가 어디에 얼마나 존재하는지조차 불분명한 경우가 많습니다. 산업용 네트워크에는 제어 시스템을 포함하여 다양한 하드웨어와 소프트웨어가 연결되어 유기적으로 각각의 기능을 수행하게 됩니다. 여기에는 계층(Level) 별로 자동화, 제어시스템(SCADA, DCS, IASC 등) 뿐 아니라 제어장치와 운용 서버(PLC, PAC, RTU 등) 및 통합 관리 시스템 등이 포함됩니다.



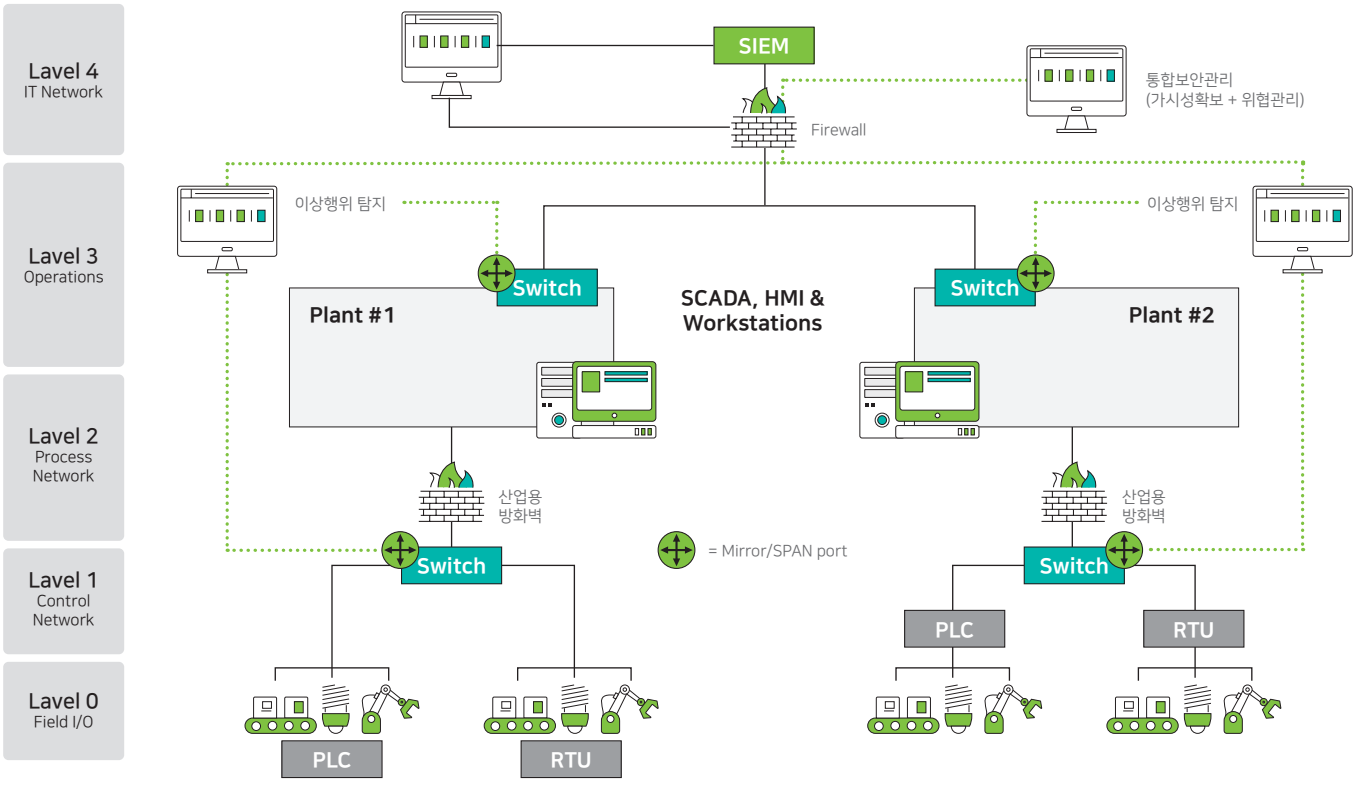
[산업용 네트워크에 존재하는 제어시스템 및 제어장치]

통상적으로 이러한 계층별 구성은 단일 네트워크 또는 폐쇄망(Closed Network)으로 구성되지만 경우에 따라서는 외부 시스템과의 연결이 필요하거나 또는 클라우드를 통해서 정보를 수집, 분석될 수도 있습니다. 이러한 구성과 요구 사항은 일반적인 제조뿐만 아니라 화학, 발전, 석유 및 가스 그리고 통신 인프라와 같은 산업에서 광범위하게 사용됩니다.

산업용 네트워크의 구축과 운용에 있어 가장 중요한 점은 가용성 일 것입니다. 가용성은 생산량을 결정지으며 이는 회사의 매출 및 수익으로 연결됩니다. 그러나 OT 보안 관점에서는 가용성만큼 중요한 것이 있습니다. 그것은 바로 가시성(Visiblity)입니다. 가시성의 확보는 산업용 네트워크 보안을 위한 첫걸음입니다. 그 대상은 네트워크에 존재하는 가상환경과 물리적 장치는 물론이며 네트워크를 통해 전달되는 다양한 (상태) 데이터와 (제어) 명령 등이 포함됩니다. 네트워크 트래픽의 이상 징후를 탐지하고 패킷 분석을 통한 데이터의 무결성 확인이 필요합니다. 우선적으로는 링크 최적화를 제공하는 탭(TAP) 센서 및 네트워크 패킷 브로커(Network Packet Broker)등을 이용한 가시성의 확보는 네트워크의 복잡성을 줄이고, 인프라를 보다 쉽게 업그레이드하고, 보안 규정을 충족시키며, 트래픽 증가에 대비하고, 도구 및 네트워크 성능의 효율성을 향상시킬 수 있습니다.

가시성 확보를 위한 아키텍처

다수의 산업용 보안 솔루션과 네트워크 모니터링 도구는 패킷을 기반으로 동작합니다. 이를 위해 가용성을 해치지 않으면서 네트워크에 존재하는 장비(설비)를 탐지 및 식별하거나 패킷을 수집하는 것이 중요합니다. 하지만 산업용 네트워크와 장비에는 몇 가지 고유한 문제가 존재할 수 있습니다. 산업용 스위치에서 SPAN 포트를 사용할 수 있지만 패킷을 복제하기 쉽지 않거나 이미 해당 포트가 사용 중일 경우도 있습니다. 일부 구형 레거시 스위치는 SPAN 포트가 없을 수도 있습니다.



* PLC : Programmable Logic Controller, 프로그래밍 가능한 RTU
* RTU : Remote Telemetric Unit, 원격 I/O 제어 및 신호 전달 장치
* SCADA : SupervisoryControl and Data Acquisition, 감시제어 데이터 수집 장치

[가시성 확보를 위한 아키텍처]

네트워크에 존재하는 장비의 가시성 확보 역시 쉽지 않습니다. IT 자산관리 솔루션을 OT 환경에서 그대로 사용하기 위해서는 많은 부분을 고려할 필요가 있습니다. 장비의 탐지를 위해 사용하는 액티브 스캐닝(Active Scanning) 은 네트워크에 과 부하를 발생시키게 되며 탐지를 위해 전달된 패킷을 수신한 장비는 오동작하거나 다운될 수도 있습니다. PLC HMI와 같은 자동화 디바이스들은 데이터 수집을 위한 에이전트를 설치하는 것도 불가능합니다. 따라서 가장 많이 사용되는 방법은 장비가 통신을 위해 사용(발생) 하는 패킷을 패시브(Passive) 하게 수집하고 분석하는 방법입니다. 결국 트래픽 분석을 통해서 장비와 네트워크에 대한 가시성을 확보하고 추가로 이상 징후까지도 탐지하는 방법이 가장 이상적이라고 할 수 있습니다.

위의 네트워크 구성도는 패킷을 수집하기 위한 장비(센서 등)와 구성을 보여줍니다. 이러한 장비는 TAP 또는 SPAN 기반으로 구성되어 네트워크 성능에 영향을 주지 않으면서 패킷을 수집할 수 있습니다. 또한 수집된 패킷을 분석하여 장비를 탐지하고 네트워크를 모니터링하거나 이상 유무를 확인할 수 있으며 추가적인 분석을 하거나 최적화를 위하여 상위(클라우드 등) 장비로 전송할 수 있습니다.

가시성 확보에 따른 효과

산업용 네트워크 내부에 대한 가시성을 확보함에 따라서 아래와 같은 효과를 기대할 수 있습니다.

✕ 네트워크 보안성

공격자는 네트워크 사각지대를 활용합니다. 이것은 관리되지 않는 장비 또는 네트워크 일 수 있습니다. 트래픽에 악성코드 등을 포함하여 전송하는 것으로 모니터링과 방어를 우회하고 공격 루트를 만들 수 있습니다. 조작된 패킷을 전송하여 네트워크에 과부하를 발생시키거나 특정 장비에 장애를 유발할 수도 있습니다. 패킷을 모두 분석할 수 없으면 악의적 활동을 놓칠 위험이 있습니다. 네트워크 가시성의 확보는 즉각적인 이상행위의 탐지와 상위 보안 솔루션이 잠재적 위협에 대해 경고하는 데 필요한 모든 분석을 가능하게 합니다.

✕ 성능 개선 및 효율화

운용 시스템의 성능 저하는 생산과 수익에 크게 영향을 줄 수 있습니다. 이러한 네트워크 지연과 성능 저하 방지는 이상 징후를 사전에 파악하고 조치하는데 달려 있습니다. 네트워크 가시성이 없으면 사태 파악이 그만큼 늦어질 수 있습니다. 적절한 네트워크 가시성은 모니터링 도구의 효용성을 높여 네트워크 관리에 보다 적극적인 대처가 가능하게 합니다.

✕ 솔루션 활용도 향상

네트워크 및 패킷 가시성의 확보를 통해 트래픽 로드 밸런싱 관리를 기대할 수 있습니다.
이는 보안 및 모니터링 도구가 실제 필요로 하는 데이터를 기반으로 트래픽을 분석하는 것을 의미합니다. 전체 네트워크 가시성을 확보하면 트래픽 폭주나 회선 낭비를 방지할 수 있습니다.

✕ 문제 해결 시간 최소화

네트워크 문제 파악과 조치 시간 최소화는 가용성(생산성) 유지를 위해 중요합니다. 네트워크와 트래픽에 대한 100% 가시성 확보와 로그 데이터의 활용은 문제의 근본 원인을 신속하게 식별하고 손쉽게 해결할 수 있게 합니다. ICS 전체 어플리케이션의 성능을 관리하는 네트워크 모니터링 및 보안 설계는 기존의 네트워크 가시성 확보와 유사합니다. 생산 라인 및 공장 네트워크 전체에서 주요 관심 포인트를 파악하는 것으로 모니터링 및 진단 기능을 향상시키고 효율적으로 운영할 수 있게 됩니다.

산업용 네트워크 보안과 고려 사항

다시 말씀드리지만, 가시성의 확보는 산업용 네트워크 보안의 첫걸음입니다. 그러나 이것은 비단 산업용 네트워크에 국한된 것은 아니며 IT 네트워크에서도 중요한 부분입니다. 마찬가지로 IT 영역의 보안을 산업용 네트워크에 적용하는 것을 고려해 볼 수 있습니다. 그러나 다음과 같은 산업용 네트워크의 특성을 이해할 필요가 있습니다.

✕ 접근통제: 네트워크 보안의 기본

네트워크 트래픽은 위 변조될 수 있으며 상태 정보 또는 제어 명령의 조작은 심각한 오류 및 장애를 발생시킬 수 있습니다. 이를 방지하기 위해 네트워크에 무단으로 접근하는 것을 방지하기 위한 포트(Port) 보안을 고려해야 합니다. 또 다른 예방 조치는 사용하지 않는 포트(USB, RS-232, Console, Ethernet 등)를 물리적으로 사용하지 못하게(Sealing) 하거나 비활성화(Deactive) 하여 권한이 없는 사용자가 접속하고 조작할 수 있는 가능성을 제거해야 합니다. MAC 주소와 통신 포트에 대한 실시간 관리 또한 비 인가 액세스를 방지할 수 있습니다. 시스템 관리자가 접근 가능 목록(Whitelist)을 작성하고 허용된 MAC 주소만 접근을 허용할 수 있어야 합니다. 또한 이 목록은 주기적으로 업데이트, 관리되어야 합니다.

✕ 단(일)방향(One-way) 게이트웨이

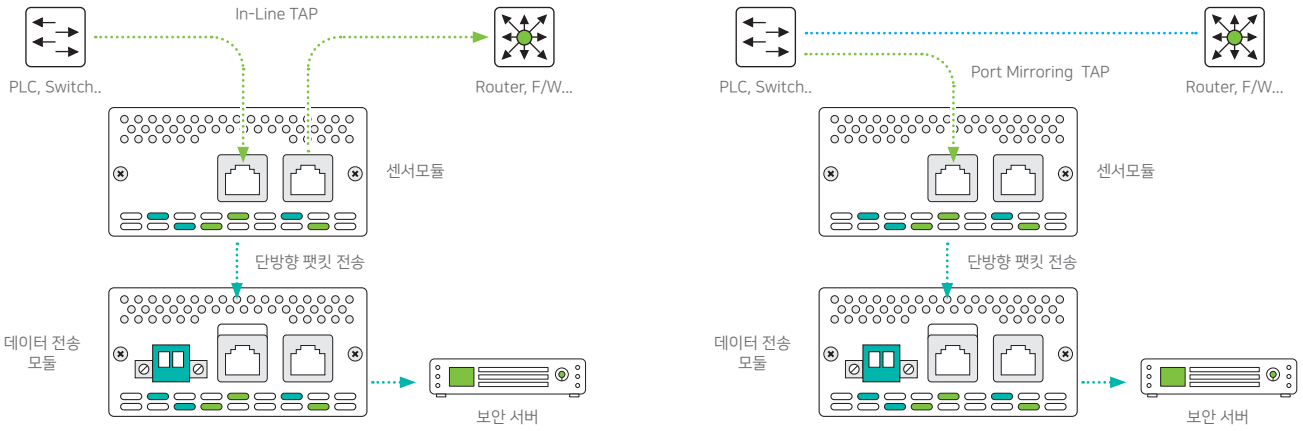
특정 산업의 경우 보안규정에 따라 데이터베이스를 복제하고 프로토콜 서버를 에뮬레이트 하는 등의 행위를 철저히 규제합니다. 이를 위해 시큐어 부팅, 인증서 관리, 데이터 무결성, FEC(Forward Error Correction)와 같은 보안 기능이 포함된 물리적 단방향 통신이 사용될 수 있습니다.

프랑스의 국가정보보안청(ANSSI) 등의 산업용 네트워크를 대상으로 하는 사이버 보안 규정에 따르면 "상호 연결은 기업 네트워크와 단방향 통신이어야 하며 이는 물리적(데이터 다이오드 등)으로 보장되어야 한다"라고 명시하고 있습니다. 이에 따른 네트워크 구성에서 SPAN 사용은 허용되지 않습니다. 네트워크 스위치의 SPAN 또는 포트 미러링은 양방향이므로 모니터링 또는 보안장치를 통해 공격자가 침투할 수 있습니다.

단방향 게이트웨이는 TCP/IP와 이더넷을 물리적으로 단절(Isolation) 시키고 원하는 데이터만을 한 방향으로 전송할 수 있게 하여 외부의 사이버 공격을 원천 차단해 산업 제어 시스템 내부망을 보호합니다. 단방향 통신 방식으로 설계된 TAP을 활용하면 제어망을 방해하지 않고 수집된 패킷을 외부 서버로 안전하게 전송할 수 있습니다.

✕ 패시브(Passive) TAP과 레거시 산업용 이더넷

많은 산업용 장비는 내부(제어) 네트워크 에서만 통신하도록 설계되었습니다.
장비 개발사의 비표준 통신 프로토콜을 이용하여 통신하는 경우 계층 간 또는 외부(클라우드 등)에서 데이터를 송/수신하기 위하여 추가적인 게이트웨이 설치가 필요합니다. 이때 게이트웨이는 전송과 프로토콜 변환 등의 역할을 수행합니다.
일종의 센서 역할을 하는 패시브 네트워크 탭(TAP)은 산업용 이더넷 데이터 수집을 위한 필수 연결 솔루션입니다.



[패시브 네트워크 탭(TAP)]

✕ IT 보안 솔루션의 OT 환경 적용 검토

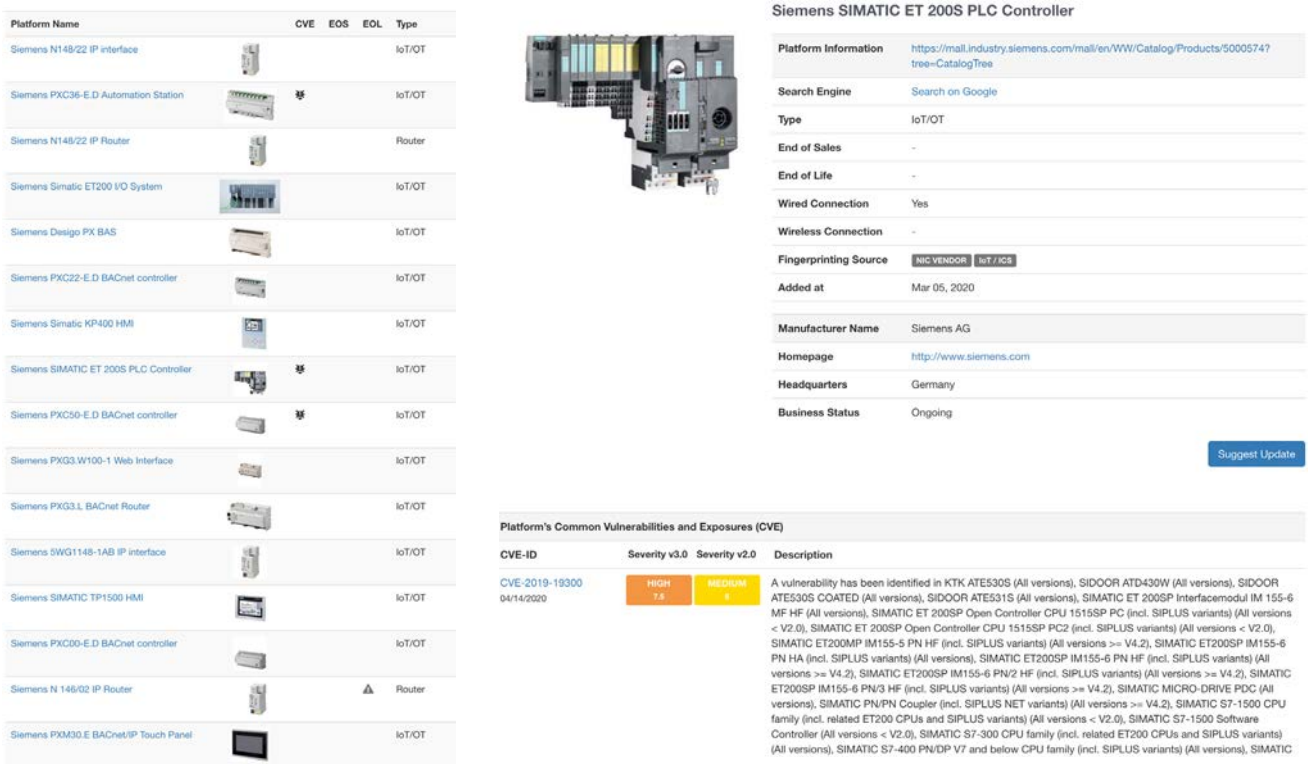
산업용 네트워크를 보호하기 위해서 IT 환경에서 동작하는 보안 솔루션을 적용할 수도 있습니다.
DPI(Deep Packet Inspection) 기능이 포함된 방화벽, 침입 탐지 시스템, IP 매니저 등의 보안 솔루션이 이에 해당합니다. 패킷은 네트워크 TAP 또는 SPAN을 통해 수집되고 전송되며, 기존의 IT 보안장비를 통해 분석될 수 있습니다. OT 환경과 일반적인 IT 환경에서의 차이점은 분석기술의 표준화 여부입니다.

IT 환경에서는 다수 사용자의 다양한 트래픽 요구를 처리하지만 OT 환경에서는 제한된 대상들 간의 동일하고 정확한 트래픽을 반복적으로 처리한다는 차이가 있습니다. IT 솔루션의 도입이 이러한 트래픽 패턴에 변형을 가져오고 이것이 OT 환경 내부에 혼란을 야기할 수 있으며 주요 보안 허점이 될 수도 있음을 간과 해서는 안 됩니다.

Genian NAC와 OT 보안

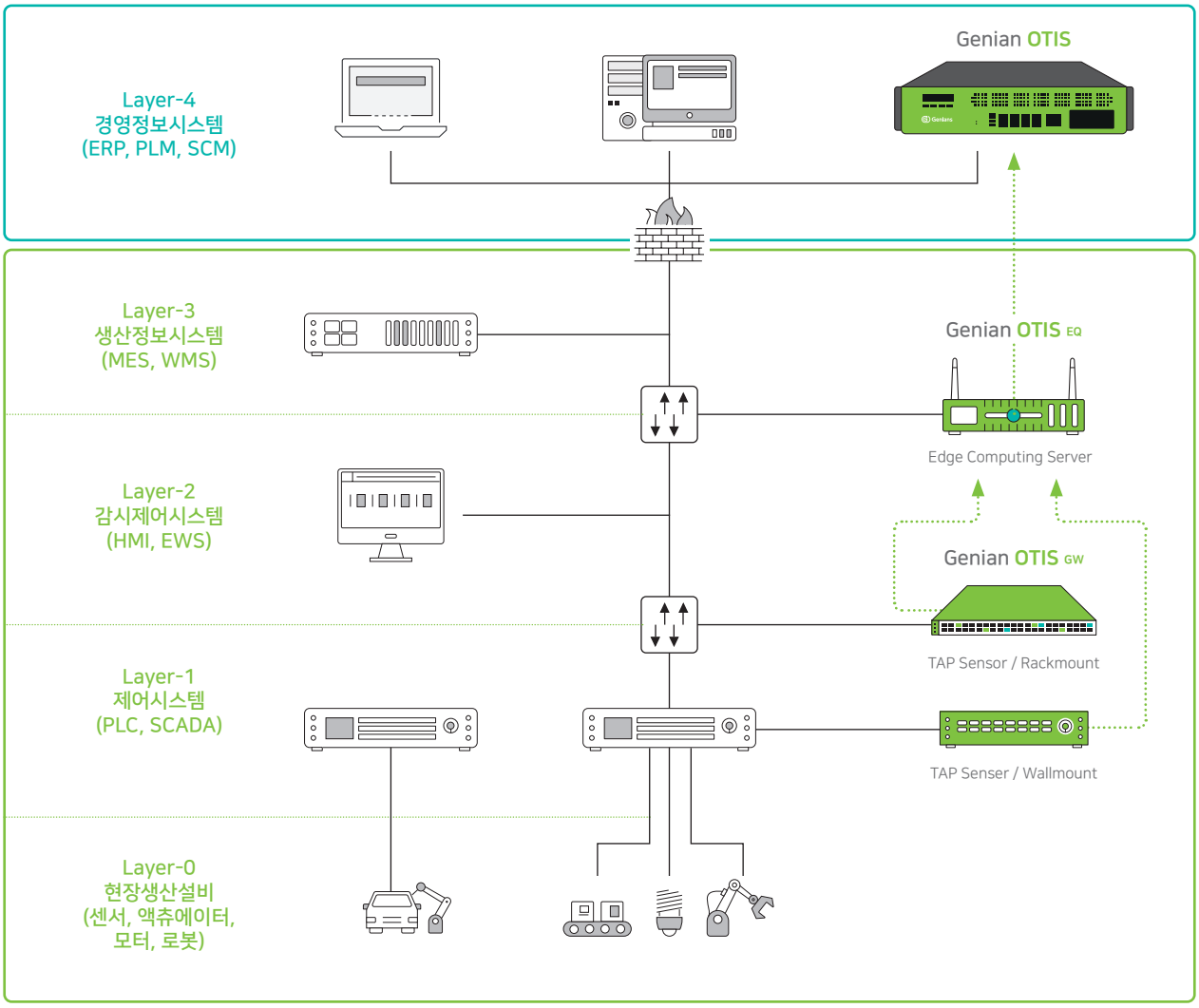
지니언스는 이미 스마트팩토리에 적용될 수 있는 보안 솔루션을 연구하고 있습니다.
앞서 언급한 바와 같이 OT 보안을 위한 가시성(Visibility)의 확보와 비 인가 사용자 및 단말에 대한 접근통제(Access Control)는 Genian NAC가 가장 잘 하는 부분이기 때문입니다.

우리가 미처 깨닫기도 전에 고객들은 이미 이러한 사실을 잘 알고 있습니다.
이미 고객사의 FA(Factory Automation) 네트워크나 OT 네트워크에 Genian NAC가 도입되어 운영되고 있으며 DPI(Device Platform Intelligence)에는 매일 다양한 산업용 제어 장치와 서버 등이 탐지되고 있습니다. 관리자는 가시성을 확보함과 동시에 IP/MAC 관리 등을 수행하고 있으며 일부 PC에 대한 접근통제와 패치, 업데이트 관리 등을 NAC를 통해 수행하고 있습니다.



[Genian NAC를 통해 탐지되는 산업용 기기리스트와 상세화면]

운영 중인 NAC 센서는 이미 OOB(Out of Band) 방식으로 설치되어 네트워크 성능에 영향을 주지 않으며 장애를 유발하지 않습니다.
향후 TCP/IP 등의 IT 프로토콜 이외에 산업용 프로토콜(필드버스)을 수집, 분석하는 기능과 머신러닝 등을 활용한 이상 징후(Anomaly Detection) 탐지 기능 등이 추가된다면 산업용 네트워크 보안 솔루션으로 부족함이 없을 것이라고 생각합니다. 그리고 이것이 스마트 팩토리와 인더스트리 4.0과 같은 미래 지향적인 제조와 생산이 가능한 시기를 조금 더 앞당길 수 있다고 확신합니다.



[스마트 팩토리 보안 솔루션, Genian OTIS 개념]

Conclusion *

1998년 미국 애리조나주 루스벨트 댐이 해킹을 당했습니다.
1999년 미국 워싱턴의 파이프라인 석유 송유관이 해킹되어 폭발로 3명이 사망했습니다.
2008년 터키 석유 압력 제어시스템이 해킹 되어 폭발 사고를 겪었습니다.
2010년 이란 나탄즈 원자력발전소의 PLC가 해킹 되어 발전소 운영이 1년 동안 중단되었습니다.
2015년 우크라이나 발전소가 해킹되어 23만여 명이 어둠과 추위 속에서 고통을 겪었습니다.

영화에 나오는 이야기가 아닙니다.
사이버 공격은 이제 IT 영역을 넘어 발전소 등의 국가 기반 시설과 민간 기업의 제조, 설비라인으로 빠르게 확대되고 있습니다. 이러한 공격에 의한 피해는 단순히 문서가 암호화되거나 사진이 삭제되는 것과는 비교할 조차 없습니다. 우리의 생활과 안전을 이러한 위협으로부터 보호할 수 있는 산업용 네트워크에 대한 보안이 그 어느 때보다 절실히 필요한 때입니다.

CONTACT US
본 자료 및 내용문의 : mkt@genians.com

Genians

Next-Gen Network Access Control for the IoT era

2005년 설립된 지니언스㈜는 국내 NAC(Network Access Control) 시장을 선도하며 글로벌 비즈니스 확장을 통해 보안 소프트웨어 전문기업으로 성장하고 있습니다. 네트워크 보안 및 단말 분석 분야 특화기술을 기반으로 내부 보안에 특화된 제품 라인업을 보유 중입니다. 네트워크에 접속하는 단말의 가시성을 확보하여 제어하는 네트워크 접근 제어 솔루션 '지니안 NAC (Genian NAC)'를 통해 국내 시장을 선도하고 있습니다. 2017년 단말 기반 지능형 위협 탐지 및 대응 솔루션 '지니안 인사이츠 E (Genian Insights E)'를 출시하며 EDR (Endpoint Detection & Response) 시장에 진출했습니다. 2016년 1월 해외사업 시작과 함께 미국 보스턴에 현지법인을 설립한 바 있으며 2017년 8월 코스닥에 상장했습니다.

Doc. v 1.0-KO