WHITE PAPER

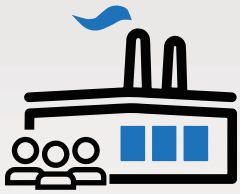
Industry 4.0 보안

OT고려 사항 및 영향

종합 요약

Industry 4.0 이니셔티브에는 비즈니스 프로세스 효율을 개선하고, 기존의 분리되어 있던 시스템을 연결해 의사결정에 풍부한 데이터를 제공하기 위한 운영기술(OT) 환경 현대화가 포함됩니다. 그러나 이들 시스템을 융합하는 동안 보안에 상당한 파급 효과가 생깁니다. 사실, 기업 10개 중 9개에서 침입이 발생해 생산성, 매출, 브랜드 신뢰도, 지적 재산, 물리적 보안과 관련된 피해를 입었습니다.[1] 설문조사에 참여한 유명 제조기업 대다수(70%)가 OT 사이버 보안이 회사 내에서 가장 큰 비즈니스 위험 5가지 안에 든다고 답했습니다.[2]

어디서나 디지털 전환, 그리고 데이터에 대한 의존성이 커지는 흐름이 나타나고 있습니다. McKinsey에 따르면, COVID-19로 인해 변화가 가속화되었다고 합니다. 고작 8주 만에 5년에 이르는 디지털 도입이 일어났습니다.[3] 대부분 산업에서 디지털 전환의 흐름은 더욱 가속화되었고 제조 산업도 예외는 아닙니다. 사이버 공격으로 인한 위협이 있다는 것은 확실하지만, 많은 기업에서 Industry 4.0 시대에 보안 위험을 완화하기 위한 구성 요소를 찾고 있습니다.



제조 기업 관계자의 80% 이상이 OT 보안을 위한 회사 예산이 다음 회계 연도에 증가할 것으로 예상했습니다.[4]

Industry 4.0, 그리고 OT와 IT의 융합

제조업에서는 4차 제조 혁명을 상징하는 Industry 4.0에 대한 기대로 디지털 전환이 시작되었습니다. 1차 산업 혁명은 기계화였고, 2차는 전기를 사용한 대량 생산과 조립 라인이었으며, 3차는 컴퓨터와 자동화의 도입이었습니다. Industry 4.0 시대에는 데이터와 머신 러닝으로 시스템 자동화를 강화합니다. Industry 4.0이 도래하면서 촉발된 이 여정은 운영기술(OT)과 정보기술(IT) 네트워크의 융합으로 이어졌습니다.

OT 환경에는 장비나 기계류를 작동하는 산업 제어 시스템(ICS)이 포함될 수 있습니다. 일반적으로 이들은 PLC(programmable logic controller)를 사용하여 관리하며, ICS용 그래픽 사용자 인터페이스를 제공하는 감시 제어 및 데이터 수집(SCADA) 서브셋 시스템이 포함될 수 있습니다. OT는 장비를 제어하고 IT는 데이터를 제어합니다. IT는 시스템과 데이터의 기밀 유지, 무결성, 가용성을 보장하지만, OT는 기계의 안전과 가용성에 집중합니다.

Industry 4.0 시대에는 제조 기술과 프로세스에 자동화와 데이터 교환이 도입됩니다. 예를 들어, 사물인터넷(IoT)과 산업 사물 인터넷(IIoT), 클라우드 컴퓨팅, 인지 컴퓨팅, 인공 지능(AI), 사이버 물리 시스템(CPS) 등이 있습니다. 그러나 Industry 4.0은 OT와 IT 네트워크의 융합으로 발생한 문제도 악화시킵니다. OT 네트워크는 전문화된 팀과 제어 시스템이 존재하고 기존 기술이 패치되지 않은 경우가 많아 연결이 확대된 이후의 직접적 결과에 크게 노출되었습니다. 지금까지 공장에서 지켰던 경계를 벗어나 내부 시스템과 자산을 연결하자 OT 보안 에코시스템 자체가 바뀌었습니다. IT와 OT 전문가들은 회사 인프라와 생산 환경을 모두 보호하기 위해 분투하고 있습니다.

Industry 4.0가 보안에 미치는 영향

Industry 4.0의 주요 목표에는 제조와 업무 프로세스를 일치시켜, 사업 동향에 따라 생산이 움직이도록 하는 것도 포함됩니다. 이렇게 데이터가 흐르려면 하나의 개념적 네트워크를 만드는 것이 가장 좋습니다. 그러나 외부 데이터 소스와 액세스를 도입하면 사이버 세계와 현실 세계에 혼란을 일으키려는 해커와 캠페인의 침입 가능성이 커집니다. 본래 산업보안은 IT와 OT 네트워크를 완전히 분리하는 것으로 유지했습니다. 이 프로세스는 "에어갭(망분리)"이라고 하는데, 취약한 OT 장비와 기술을 사내 네트워크와 분리합니다. 운영에 혼란을 일으키려는 외부 공격과 캠페인 대부분을 차단하는 것이 목적이었습니다.

제조 애플리케이션, 제조 요구 사항 계획(MRP) 시스템, PLC, 인력-기계 인터페이스(HMI), 기타 구성 요소를 비롯한 시스템이 서로 연결되었기 때문에, 기업에서 변화가 일어남에 따라 이러한 네트워크도 사이버 보안 모범 사례를 고려하고, 그에 걸맞은 투자를 바탕으로 운영하도록 바꿔야 합니다.

IT와 OT 네트워크를 제한적으로 연결했더라도 수많은 네트워크 공격 벡터에서 표적이 바뀔 수 있습니다. 원래 IT 네트워크 액세스를 노렸던 공격을 OT 표적을 공격하는 데 사용할 수도 있습니다. 중요한 인프라를 대상으로 한 사이버 공격은 그저 신문의 머리기사를 장식하는 데 그치지 않을 수도 있습니다. 제조 기업에서 산업 시스템이 중단되면 몇 시간 동안 생산이 멈추고, 민감한 원료가 가공 중에

망가져 수백만 달러의 추가 비용이 들어가고, 기업이 규정 위반으로 처벌받을 위험에 노출되기도 합니다. OT를 표적으로 삼는 새로운 공격 벡터는 시민들이 신뢰하는 사이버-물리 프로세스에 큰 영향을 미칠 수 있으므로 공격의 부수적 영향을 이해하는 것이 중요합니다. 예를 들어, 자원을 이동하는 중에 방해가 생기거나, 국가 방어 시스템이 망가지거나, 심지어 무고한 시민이 다치는 등의 피해를 입을 수 있습니다.

기업의 거의 3/4에서 현재 IT와 OT의 기본 연결을 최소한으로 보고하고 있습니다.[5]

OT 보안 위험

OT는 지능적 위협과 기존 위협에 특히나 취약합니다. 20~30년 전에 배포된 시스템이 많기 때문입니다. ICS는 대개 인증을 받지 않거나 암호화되지 않은 시스템을 사용해서 위험합니다. 장비의 설치 기반도 제품 수명 주기가 길고 서로 다른 산업 프로토콜을 사용하는 여러 공급업체의 제품을 다양하게 사용하는 경우가 많습니다. 안전하고 지속적인 운영을 가장 우선시하고 있어서 능동 스캔과 같은 간단한 조치만으로도 기기에 장애가 일어나 생산이 중단되고 심각한 결과를 초래할 수 있습니다.

사이버-물리 시스템에 대한 위협은 끊임없이 확장되고 진화합니다. 사실, 2020년 상반기에는 2019년 하반기보다 전체 공격 횟수가 약 35% 증가했습니다.[6] OT와 IT 네트워크의 디지털 혁신이 일어나면서, 더욱 복잡해지고 파편화된 보안 인프라가 새로운 취약성과 시스템 해킹 위험에 노출되었습니다. 많은 기업이 에어갭(망분리) 보호의 단점을 보완하기 위해 포인트 보안 제품을 추가했지만, 이런 제품은 따로 운영되는 경우가 많습니다. 부가적인 지표로 하나의 취약성이나 규정 준수 요구 사항을 제공하기는 하지만, 보안 인프라 전체에 가시성이나 인텔리전스 공유는 제공하지 않습니다. 어쩌면 당연하게도, 네트워크 분석가는 OT 네트워크 환경에서 보안 상태가 어떤지 명확하게 실시간으로 확인할 수 없습니다.

다행히 제조업 분야의 관계자 대부분은 현재 당면한 가장 중요한 비즈니스 위험 중 하나로 OT 보안을 꼽았고, 설문조사 대상자 중 1/3 이상(39%)이 그중 3위 이내로 생각했습니다.[7] 대부분 관계자는 이러한 우려에 대응 방법을 찾고 있는 듯합니다. MAPI 조사에 따르면, 83%가 OT 보안 지출에 할당된 회사 예산을 높일 계획이라고 답했습니다. OT와 IT의 복잡한 환경을 통합하면서 여러 가지 문제에 부딪힐 것이기 때문에 예산 증액이 먼저 취해야 할 필수 조치입니다.

리소스, 도구, 기술, 교육은 부족한데 위협은 빠르게 진화하는 현실을 고려하면 OT 네트워크에서 효과적인 대응 관리로 나아가는 길에 서 있는 장벽은 높고도 넓습니다. 이러한 장애물에도 불구하고 제조 관계자들은 Industry 4.0으로 전환하면서 사이버 보안 모범 사례를 강화하고 지원하기 위해서라면 무엇이든 할 준비가 되어 있습니다. 사실, 설문조사에 참여한 관계자의 94%가 OT 보안 위험을 해결할 새 솔루션을 구현할 계획이라고 답했습니다.[8]

거버넌스, 위험 및 규정 준수

OT 보안 문제를 해결하려면 규정 준수, 감사, 인력 충원, 비용, 효율에 초점을 맞추어야 합니다. 규정 준수와 보안을 절대 혼동해서는 안 되지만 이 두 가지는 서로 연결되어 있습니다. 보안 솔루션이 분산되어 환경이 복잡해졌는데, 규제 기관이 규정을 준수하기 위해 새로운 규제와 표준을 도입하거나 기존의 규제와 표준을 발전시키는 등의 변화를 시도하면서 복잡성은 더욱 커집니다. 자동 추적, 감사, 보고 기능이 있는 효과적인 솔루션을 갖추지 못한 기업에서는 데이터를 수동으로 집계하고 합치는 데 상당한 인력을 쏟아부어야 합니다.

주무 기관의 주요 표준을 준수하면 보안의 기본을 지킬 수 있습니다. 미국에서 대부분 ICS 관련 표준은 각 부문을 주관하는 기관이 이해관계자와 함께 중요한 인프라를 지키는 것을 목적으로 개발하여 공개합니다. 이들은 OTCI 부문에서 지켜야 하는 표준이 되는 경우가 많지만, 제조업의 일반적 ICS 요구 사항에 쉽게 적용하지 못할 때도 있습니다.

가장 흔히 참조되는 범용 ICS 프레임워크는 NIST(National Institute of Standards and Technology) SP 800-82dhk ISA(International Society of Automation) 62443입니다. 또한 ICS 네트워크의 동작 이상 탐지와 관련된 최신 NISTIR(NIST Interagency/Internal Report) 8219를 고려하는 것이 좋습니다.

Industry 4.0 보안의 기본 구성 요소

Industry 4.0 시대로 나아가기 위해 제조업계에서는 서로 분리된 포인트 보안 배포의 복잡성과 파편화를 낮추는 데 집중하여 기존 아키텍처를 재평가하고 있습니다. 또한, 하나의 통합된 보안 중심 전략에 따라 보안 사례와 비즈니스 이니셔티브가 함께 발전하도록 사이버 프로그램을 다시 평가해야 합니다. 현재 사용 가능한 리소스를 포함하여 현재의 위치도 파악해야 합니다. 그 다음에는 프로세스를 평가하고 민첩성과 보안을 개선하기 위한 옵션을 조사해야 합니다. 이 정보로 무장한다면 사이버 보안 OT 시스템 안정화를 향해 나아가는 데 도움이 되는 솔루션을 찾을 수 있을 것입니다.

기업의 44%는
업계 규정 준수를
추적하고 보고하지 않습니다.[9]

구성 요소 1: 현재 상태 평가

사이버 보안 표준은 보안 전략을 개발하고 이행하기 위한 방향성을 제시하고 가이드를 제공하는 데 도움이 될 수 있습니다. 기업은 기존의 표준(예: NIST, IEC 62443)에서 시작해서 현재 보안이 어느 정도인지, 어디까지 강화해야 하는지 알아내야 합니다. 관리자는 산업 전문가의 조언을 받아 지식을 쌓고, 회사의 보안 목표를 더욱 잘 달성할 수 있습니다.

NIST CSF(Cybersecurity Framework)는 융합된 보안 프로그램에 대한 프레임워크는 물론이고 IT와 OT 사이에 소통, 이해, 협업을 개선하기 위한 공통적 표현을 제공합니다. 제조 기업은 NIST CSF를 활용하여 디지털 혁신과 기업의 비즈니스 목표를 일치시키고, 인력, 프로세스, 기술과 관련하여 필수적인 인프라 변화를 찾아내고 운영에 적용할 수 있습니다.

IEC 62443 표준은 산업 자동화 제어 시스템에서 보안 취약성을 관리, 완화하는 데 사용하는 또 다른 공통적 프레임워크를 제공합니다. 기업의 ICS 방어 태세를 효과적으로 개선하면서도 비용에 미치는 영향과 위험을 낮추는 효과에 균형을 맞춰줄 제품을 선택하기 위한 지침도 제공합니다.

구성 요소 2: 인력 요구 사항 고려

OT 사업에서는 전체적인 인력 현황을 점검하고, IT와 OT 인력 간의 문화, 목적, 원칙에 따른 내부적 차이를 해결할 방법을 찾아야 합니다. 또한, 제조업체는 원격 근무자의 요구 사항도 고려해야 합니다. COVID-19 팬데믹이 확산되면서 전 세계적으로 원격 근무 솔루션이 급격히 도입되었지만 상당한 위험이 수반되었습니다. 원격 근무자를 보호하기 위한 요구 사항으로 인해 보안 시스템, 특히 클라우드 마이그레이션과 엔드포인트 확산과 관련하여 유례없는 부담이 생겼습니다. 팬데믹 이후에도 원격 근무가 사라질 것 같지는 않습니다.

사이버 보안에 대한 인식과 교육 이니셔티브를 강화했지만, 피싱은 여전히 엄청난 문제가 되고 있고, 기업에서도 내부자 위협이 상당히 커졌습니다. 내부자 위협은 행동과 의도가 매우 다양하기 때문에 내부자 활동으로 인한 피해를 추적하기 어렵습니다. 직원이 현장에 없으면 이 작업은 더욱 어려워집니다.

제조 기업은 어떤 위치에서 어떤 기기를 사용하든 모든 사용자를 안전하게 관리할 수 있어야 합니다. 여기에는 회사 내부, 공장, 창고의 내부 직원, 고위 임원, 계약직 근로자, 임시 근로자까지 모두 포함됩니다.

역할이 변화하고 여러 부서가 섞인 팀이 구성되어 협업이 강화되면서 보고 계통이 복잡해지고 책임 소재가 불분명하게 되었습니다. Industry 4.0 이전에는 서로 분리되어 있던 부서, 팀, 직원들은 목표가 대립되지만, 서로 균형을 이루고 각자의 가치관을 존중해야 하게 되었습니다. CISO, CTO, IT 아키텍트, CIO, 시설 관리자, 네트워크 분석가는 지속적인 운영의 필요성을 고려하고 기밀 유지(IT의 최우선 순위), 가용성(OT의 최우선 순위, 시설 직원의 물리적 보안 포함) 등의 문제에 대해 합의해야 합니다. 지속적인 비즈니스 회복성을 갖추기 위해서는 기업에서 서로 협업하여 회사의 보안 태세를 강화해야 합니다.

구성 요소 3: 검토 프로세스

기업이 디지털 전환을 추진하면 기술과 업무 프로세스에 모두 변화가 일어납니다. Industry 4.0에서는 기술로 프로세스를 자동화하여 단계를 줄이는 데 집중합니다. Industry 4.0 시대에는 데이터를 광범위하게 사용하여 공급망, 고객 환경을 비롯한 업무 프로세스 전체의 효율을 개선하고 정보에 입각한 결정을 내립니다.

이러한 개선으로 주문 처리, 제품 제조, 고객 대금 청구, 잠재적 보안 침해 탐지, 대응에 이르기는 다양한 프로세스가 도움을 받을 수 있습니다. 각 영역에서 사업에 대한 위험 대비 효율이 얼마나 증가했는지 평가해야 합니다.

기업에서 이런 체계적인 업무 프로세스 검토를 수행해야 하는 이유는 디지털화로 인해 예전에는 연결되지 않은 시스템과 프로세스에서 더 많은 데이터가 수집, 공유되기 때문입니다. 기업에서 개선하고 디지털화가 필요한 영역을 알아내는 동안, 그에 따라 발생할 수밖에 없는 보안의 결함이나 빈틈을 찾아내야 합니다.
효율과 비즈니스 최적화를 우선시하여 프로세스를 개선하는 과정에서 클라우드 서비스를 도입하는 기업이 늘어나고 있습니다.

제조 기업에서는 클라우드 기반 서비스(예: 제조 리소스 계획(MRP), 엔터프라이즈 리소스 계획(ERP) 시스템)를 빠른 속도로 도입하고 있습니다. 이런 시스템은 대개 빠르고 효과적인 의사결정을 위해 IT와 OT 시스템에서 모두 데이터를 가져옵니다. 아키텍처가 데이터 센터에서 산업 시스템, 여러 클라우드에까지 확장될 수 있으므로 이런 자산에 반드시 사이버 보안을 적용해야 합니다.

재택근무를 할 수 있는 직무의 54%는 COVID-19 팬데믹이 종식될 때까지 집에서 일하기를 원합니다.[10]

구성 요소 4: 기술 업데이트

기업에서 Industry 4.0을 지원하려면 아무리 지능적인 공격에도 견딜 수 있는 OT 및 IT 보안을 준비해야 합니다. 종합적인 사이버 보안 솔루션을 모든 공격면에 적용하고, 모든 보안 제품에서 위협 인텔리전스를 공유하며, 위협에 자동으로 대응해야 합니다. 융합된 Industry 4.0 환경을 보호하기 위한 모범 사례는 5가지가 있습니다.

1. **자산 식별, 분류, 우선순위 설정으로 네트워크 가시성 확보**
   기업의 IT 및 OT 환경과 자산의 최신 인벤토리를 유지하면 기본적인 보안 계획과 인식에 도움이 됩니다. 보이지 않는 인프라는 보호할 수 없기 때문에 네트워크에서 사용하는 기기와 애플리케이션의 최신 인벤토리가 필요합니다. 이런 기기와 애플리케이션은 특징과 동작에 따라 식별하고 프로파일링해야 합니다.

2. **네트워크 세그먼테이션**
   세그먼테이션은 네트워크 환경을 보호하는 데 가장 효과적인 아키텍처 개념입니다. IT/OT 세그먼테이션이 적용되지 않았거나 부적절한 경우, OT 네트워크에서 취약성이 드러났을 때 더욱 광범위하게 악용될 수 있습니다. 적절한 네트워크 세그먼테이션을 적용하면 네트워크는 일련의 기능적 세그먼트나 영역으로 분할되며, 여기에는 하위 영역이나 마이크로세그먼트가 포함될 수 있습니다. 각 영역은 사전에 승인을 받은 기기, 애플리케이션, 사용자만 액세스할 수 있습니다. 차세대 방화벽(NGFW)이 제어 영역을 정의하고 적용합니다. 또한, NGFW는 통로(필수적인 데이터와 애플리케이션이 영역을 안전하게 건너갈 수 있는 채널)를 정의합니다.

   영역과 통로로 구성된 아키텍처 모델은 광범위한 인프라 감염과 익스플로잇 위험을 크게 낮출 수 있습니다. 공격자가 OT 네트워크에서 수평(이스트-웨스트) 또는 수직(노스-사우스) 방향으로 움직이지 못하게 제한함으로써 잠재적인 해킹의 영향을 완화합니다. 특정 영역에서 특정 활동을 하도록 승인된 사용자나 기기는 해당 영역에서만 움직일 수 있습니다. 영역과 통로로 구성된 이 모델은 고정되어 있지 않고 움직여야 합니다. 세분화된 액세스 제어로 신뢰 수준을 지속적으로 모니터링하고 그에 맞게 보안 정책을 수정해야 합니다.

3. 트래픽 분석

방화벽은 네트워크를 영역, 세그먼트, 통로로 분리하는 데 사용되지만 네트워크 트래픽을 분석하여 알려진 위협과 알려지지 않은 위협을 탐지하는 데도 똑같이 중요합니다. OT 기업은 주요 ICS 제조사를 통해 애플리케이션과 기기에 대한 취약성 보호를 강화할 수 있습니다. 대부분 OT 기기는 패치 없이 작동하기 때문에 이런 익스플로잇을 찾아내 무력화하고 "가상 패치"로 보호하는 작업이 중요합니다. 네트워크 트래픽은 네트워크 이벤트에 따라 표시해야 합니다. 지능적 인프라 및 애플리케이션 검색 엔진은 데이터를 수동으로 교차 참조하는 대신, 기기나 애플리케이션에 대한 사전 지식 없이도 자격 증명을 사용하여 온프레미스, 퍼블릭 클라우드, 프라이빗 클라우드에 있는 물리/가상 인프라를 발견해 매핑합니다.

대부분의 기업(78%)은 OT환경의 가시성에 부분적으로만 중앙 집중화되었습니다.[11]

4. 액세스 제어

기기, 사용자 및 애플리케이션은 인증을 완료해야 OT 환경이나 세그먼테이션이 적용된 자산에 액세스할 수 있어야 합니다. 여기서 보안 인증이 중요합니다. 가장 피해가 큰 OT 보안 해킹 사례는 사용자 계정과 비밀번호가 유출된 건에서 발생하였고, 사용자에게 부적절한 액세스 권한을 할당한 경우에 그 피해가 더욱 컸습니다.

제조 기업은 네트워크에 무엇이, 누가 액세스하는지 컨텍스트에 따라 검증하고 필수 리소스에만 액세스하도록 제한할 솔루션이 필요합니다. 제어 솔루션을 사용하면 중요한 시스템에 지장을 주거나 이를 중단하지 않고도 정책을 적용하고 필요에 따라 적절한 조치를 취할 수 있습니다. 다단계 인증(MFA)과 인증된 사용자와 기기에만 네트워크를 개방하는 기능은 중요합니다. 네트워크 액세스 제어 솔루션은 하이브리드 클라우드와 퍼블릭 클라우드에서 엣지, 5G, IIoT 등을 비롯한 인프라의 각 부분에 모두 적용되어야 합니다.

5. 유무선 액세스 보안

원래 OT 네트워크 인프라는 시설 운영에서 무선 연결을 사용하는 경우가 드물었습니다. 그러나 OT 환경에 센서나 다른 IIoT 기기를 배포하고 무선 기술로 연결하는 OT 기업이 늘어나고 있습니다. 이런 연결의 범위와 사용 빈도를 늘리면 디지털 공격면도 그에 비례해서 늘어날 수밖에 없습니다. 무선 액세스 포인트(AP)와 네트워크 스위치는 사이버 공격의 매력적인 표적입니다. AP와 스위치는 설계 단계에서부터 보안이 필수이고, 여러 인터페이스에서 관리되는 부가적 포인트 보안 솔루션이 아닌 하나의 중앙 인터페이스에서 관리되어야 합니다. 중앙 집중식 보안 관리로 위험이 완화되고 쉽게 정책을 적용할 수 있을 뿐만 아니라, 가시성을 개선하고 보안 및 운영 팀의 관리 시간도 최소화됩니다.

구성 요소 5: 실천 가능한 인텔리전스 및 보고 기능 추가

Industry 4.0 대비한 종합적인 보안 전략을 세우려면 사이버 보안 모범 사례를 도입하는 것 외에도 통합적인 자동 위협 인텔리전스 공유와 규정 준수 보고가 필요합니다. CISO는 확장할 수 있고, 산업적 위협을 발견했을 때 OT 에코시스템에 자동으로 전달할 수 있는 선제적 OT 보안 솔루션 전략이 필요합니다. 실천 가능한 인텔리전스를 배포하여 미리 OT 환경과 각 보안 요소를 보호해야 합니다. 데이터 센터, 메인 캠퍼스에서 네트워크 엣지까지 모든 범위가 포함되어야 합니다.

Industry 4.0으로 가는 길

제조 기업에서 확장되는 기존의 디지털 사업 모델을 최대한 활용해 Industry 4.0 시대에서 가치를 창출하려면, OT 보안이라는 중요한 문제를 해결해야 합니다. Industry 4.0을 지원하고 OT 환경을 현대화할 때는 보안을 우선시하는 원칙에 따라 전환 전략을 분석하고 구조화해야 합니다. 업무 프로세스의 현황, 리소스, 개선 이니셔티브 분석이 선행된다면 기술 개선과 보안 적용을 통해 목표를 달성할 수 있을 것입니다.

가시성, 제어, 지속적 모니터링을 포함한 환경을 조성하면 Industry 4.0 이니셔티브를 지원하는 새로운 융합된 IT 및 OT 네트워크를 보안하는 데 도움이 됩니다. 전략을 민첩하게 이행하기 위한 조치를 통해 비즈니스, 산업, 기술 변화에 적응하는 능력을 기를 수 있습니다.

1 "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 2020년 6월 30일.

2 David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

3 Aamer Baig, et al., "The COVID-19 recovery will be digital: A plan for the first 90 days," McKinsey Digital, 2020년 5월 14일.

4 David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

5 "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, 2019년 6월 28일.

6 "Microsoft Digital Defense Report," Microsoft, 2020년 9월.

7 David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

8 상게서.

9 "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 2020년 6월 30일.

10 Kim Parker, et al., "How the Coronavirus Outbreak Has—and Hasn't—Changed the Way Americans Work," Pew Research Center, 2020년 12월 9일.

11 "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 2020년 6월 30일.

FORTINET

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 **전화:** 080-559-8989 **Email:** kr-callcenter@fortinet.com

989802-0-0-KR