SECURE

디지털 트랜스포메이션을 위한 사이버 보안

슈나이더 일렉트릭의 서비스 및 솔루션

se.com/cybersecurity

Life Is On | Schneider Electric

목차

사이버 보안의 가치

디지털 전환과 사이버 보안

클라우드 컴퓨팅, 모바일, 사물인터넷(IoT) 및 인공 지능과 같은 디지털 기술의 사용이 증가하면서 세상은 그 어느 때보다 긴밀하게 연결되었습니다. 그러나 향상된 연결성은 새로운 기회를 제공할 뿐 아니라 새로운 문제를 유발하고 취약점을 늘리는 원인이 되고 있습니다.

사이버 위협 및 사고는 모든 디지털 엔터프라이즈에 있어서 중대한 운영 및 비즈니스 위험입니다. 디지털화 시대에는 사이버 위협 및 위험을 파악하고 줄이고 대응할 수 있는 전략을 실행하는 것이 매우 중요합니다. 이는 운영을 보호하고 재무 목표를 달성할 수 있는 유일한 방법입니다.

2025년까지 IoT 커넥티드 장치의 증가

전 세계 인구의 61%
가 인터넷에 연결됨

754억 4천
개의 커넥티드 IoT 장치

28.7%
2018~2025년 동안 커넥티드 IoT 장치에서 생성하는 데이터 양의 CAGR

152,200
개의 IoT 장치가 1분마다 연결됨

출처:
IDC, GSMA, Accenture

사이버 보안의 최신 동향에 대해 자세히 알고 싶으세요?

사이버 보안 블로그 방문

사이버 보안 위협 증가

기업들이 인터넷과 커넥티드 자산에 점점 더 의존함에 따라 사이버 공격은 모든 산업의 기업들에게 지속적인 위협이 되고 있습니다. 따라서 대부분의 기업들이 사이버 보안 전략 수립의 중요성을 이해하게 되었습니다.

22%
의 보안 문제가 오래되고 패치가 적용되지 않은 소프트웨어에서 발생함

출처:
Bulletproof 연례 사이버 보안 보고서 2019

67%
지난 5년간의 보안 침해 증가율

출처:
Accenture의 2019년 연간 사이버 범죄 비용 연구

380만 달러
사이버 보안 침해의 평균 비용

출처:
Ponemon Institute의 2018년 데이터 침해 비용 연구

IT 예산의 2%만
보안에 사용됨

출처:
Canalys의 사이버 보안 분석, 2019년 3월

5분 이내
IoT 장치가 온라인으로 전환된 후 공격을 받기까지 걸리는 평균 시간

출처:
NETSCOUT

14초마다
랜섬웨어 공격 발생

출처:
Cybersecurity Ventures의 2019년 공식 연례 사이버 범죄 보고서

모든 산업의 서비스 및 솔루션

사이버 보안의 3가지 구성 요소

사이버 보안 전략의 힘은 가장 약한 연결고리에 의해 결정됩니다. 따라서 인력, 프로세스, 기술을 통합해야 하는 전체 방어선 전반에 표준과 모범적인 관행을 적용하여 위험을 식별하고 완화하는 것이 기본입니다.

직원

강력한 사이버 보호에는 보안 의식이 높은 숙련된 인력이 필요합니다. 많은 경우 직원들은 첫 번째 방어선이자 최종적인 방어선입니다. 이 영역의 중요한 요소는 전사적인 보안 문화를 조성 및 전달하고 지속적인 교육을 통해 그러한 문화를 발전시키는 것입니다.

최적화

사이버 위험을 식별하고 제거하기 위해서는 모범적인 프로세스, 관행 및 정책을 수립하고 준수해야 합니다. 기업들은 일관되고 정기적인 위험 및 위협 평가와 격차 분석에서부터 시작해야 합니다.

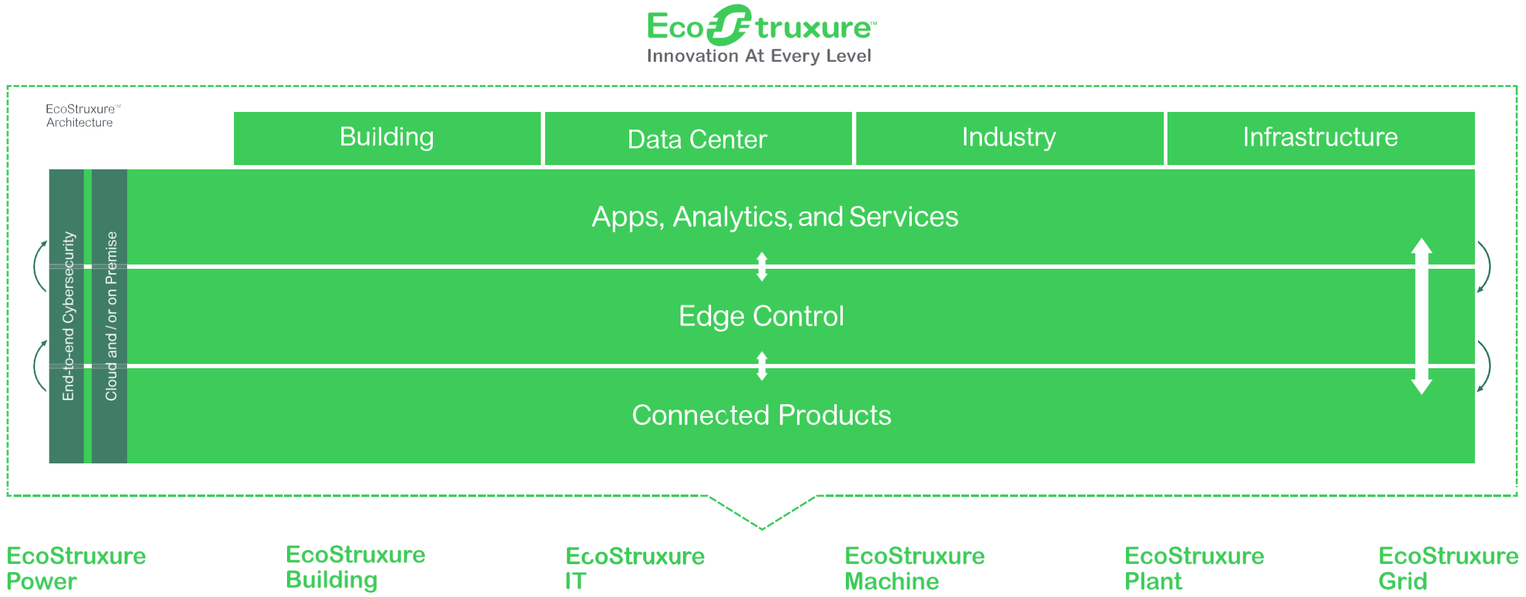
기술

사이버 방어의 힘은 운영을 관리하고 제어하기 위해 배포된 기술에 달려 있습니다. 이 측면은 회사에서 개발하고 배포하는 기술을 보호하고 외부 공급업체의 기술에 대한 보안이 보장되고 있는지 확인해야 합니다.

모든 수준에서의 혁신

제조업체 자체로서 슈나이더 일렉트릭은 IoT를 지원하는 중립적인 개방형 아키텍처 및 플랫폼인 EcoStruxure™ 전체에 보안 기능을 적용하였습니다.
여기에는 개방형이면서, 맞춤형 커넥티드 제품, 엣지 컨트롤 수준 솔루션 및 소프트웨어, 클라우드 기반 애플리케이션 분석 및 서비스 스택이 포함됩니다.

엔드 투 엔드 사이버 보안은 이러한 계층 전체에 내장된 애플리케이션 및 데이터 분석을 지원하며 6개의 전문 영역 내에 IT 및 OT 장비 및 솔루션, 소프트웨어, 서비스를 통합합니다.



심층적인 방어 접근 방식

기업들은 구매하는 제품에 사이버 보안 위험을 완화하는 데 필요한 모든 것이 포함되어 있을 것이라고 기대합니다. 그러나 제품만으로는 시작점에 불과합니다.
시스템을 구현하고 환경에 통합하는 방식도 중요합니다. 시스템 구현 및 통합 프로세스는 환경의 무결성을 보호해야 합니다.

시스템이 작동되면 위험 평가에 따라 다른 여러 측면을 전체 운영의 일부로 고려해야 합니다. 여기에는 간단한 방화벽에서부터 네트워크 분리 및 테스트에 이르는 여러 측면이 포함됩니다.

이 외에도 솔루션 설계 검토 또는 개발, 팀 교육 또는 지속적인 관리형 보안 서비스 제공 시 객관적인 관점과 더욱 폭넓은 경험을 제공하는 전용 서비스가 있습니다.

사이버 보안에 대해 심각하게 고려하고 있습니까?

슈나이더 일렉트릭 Cybersecurity Virtual Academy 등록

여러 수준에서 사이버 보안 문제 해결

효과적인 사이버 보안은
제품 및 시스템에서
지속적인 서비스에
이르기까지 전체
OT 환경을
포괄합니다.

운영 수명 주기를 위한 사이버 보안 솔루션: 컨설팅, 통합 및
관리형 보안 서비스

기술 파트너십:
상황 인식, 규정 준수, 변경 관리, 빅 데이터 보안

시스템 구축:
제품 또는 시스템 구축 시 안전한 프로젝트 및 서비스 제공

**설계 단계부터 고려한 사이버 보안:
보안 제품, 솔루션, 소프트웨어**

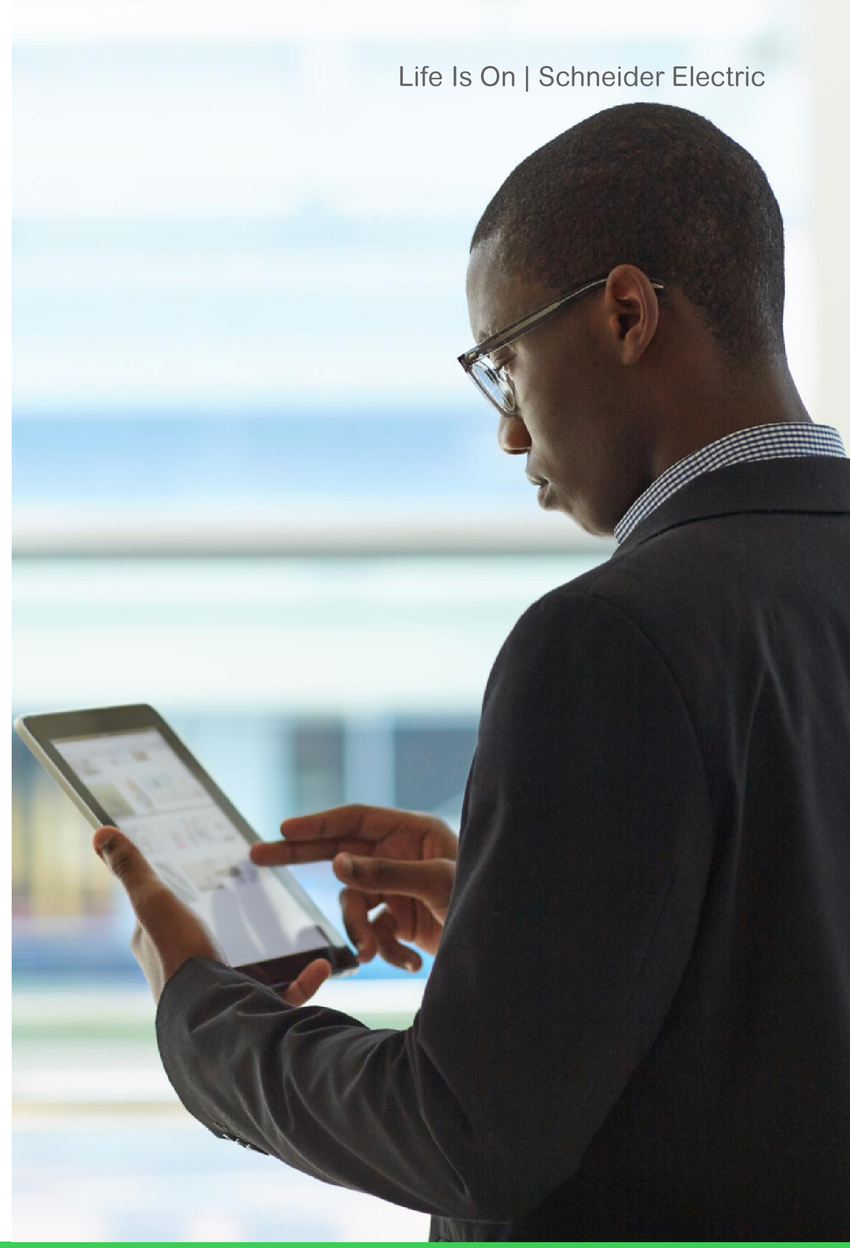
심층적인 방어 접근 방식

슈나이더 일렉트릭의 360˚ 사이버 보안 솔루션은 다음과 같습니다.

- 사이버 보안 전문가로 구성된 공인 팀이 프로세스 차원의 요구 사항, 엔터프라이즈 차원의 요구 사항, 비즈니스 환경을 정확히 파악
- 정부, 대학교, 공급업체 등으로 구성된 동적인 파트너 및 플랫폼 에코시스템이 연구, 정책, 공동 프로젝트를 추진하여 포괄적인 보안 관리 솔루션 개발
- 외부 알림, 취약성 공개 또는 고객 보고를 기반으로 ISO 준수 취약성 관리 프로세스 실행
- 첨단 글로벌 위협 인텔리전스 센터에서 사이버 공간을 적극적으로 모니터링하여 슈나이더 일렉트릭 제품과 고객에 대한 위협이 발생하지 않는지 모니터링
- 150개 이상의 제품이 전기 및 공정 설비 부문에서 사이버 보안 표준 인증 획득

슈나이더 일렉트릭의 사이버 보안 솔루션에 대해 자세히 알고 싶으세요?

슈나이더 일렉트릭 YouTube 채널 방문



엔드 투 엔드 사이버 보안

글로벌 사이버 보안 표준

ISA/IEC 62443-4-1 표준을 따르는 제품은 제품 개발 초기부터 수명 주기가 끝날 때까지 보안을 해결합니다. 이 표준은 슈나이더 일렉트릭 서비스 및 솔루션 내에서 채택되었습니다.

슈나이더 일렉트릭은 ISA 글로벌 사이버 보안 연합의 창립 회원입니다.

ISA GLOBAL CYBERSECURITY ALLIANCE

ISA/IEC 62443-4-1 표준

자동화 및 제어 시스템 애플리케이션을 위한 세계 유일의 합의 기반 표준

보안 시스템 구현을 위한 요구사항 및 절차 정의

현재 및 미래 보안 취약점을 해결 및 완화하는 유연한 프레임워크

총체적인 접근 방식을 활용하여 안전과 사이버 보안 간의 격차뿐 아니라 운영과 정보 기술 간의 격차 해소

운영 수명 주기를 위한 솔루션

슈나이더 일렉트릭은 모든 비즈니스 유형 및 산업 전반에 대해 사이버 보안에 대한 요구를 지원하는 솔루션을 제공하기 위해 노력하고 있습니다. 슈나이더 일렉트릭은 제품을 개발하고 솔루션을 구현하는 데 있어서 엄격한 사고방식, 정책 및 방법론을 적용하고 있습니다.

숙련된 공인 전문가가 사용자의 위치에서 시간이 지남에 따라 위험을 평가하고, 사이버 관련 솔루션을 구현하고, 방어를 유지할 수 있는 벤더의 제약이 없는 서비스를 제공합니다

보안 컨설팅
- 정책 및 절차
- 자산 인벤토리
- 격차 분석
- 위험 및 위협
- 규정 준수

설계 및 구현
- 심층적인 방어
- 보안 아키텍처
- 자산 관리
- 보안 보증 수준
- 시스템 강화
- 솔루션 통합

교육
- 보안 인식
- 보안 엔지니어
- 보안 관리자
- 고급 전문가

모니터링
- 방화벽 보안
- 장치 관리
- 위협 관리
- 장치 보안
- OT SIEM 지원

유지보수
- 시스템 업그레이드
- 보안 패치
- 사고 대응

운영 수명 주기 전반을 포괄하는 솔루션

보안 컨설팅

슈나이더 일렉트릭의 사이버 보안 컨설턴트는 고객 시스템을 평가하고 검토하여 결함과 위험을 감지하고, 보안과 관련된 모든 오류를 밝혀내고, 직원의 보안 역량을 평가하며, 비상 대응 서비스를 제공할 수 있도록 지원합니다.

설계 및 구현

엔지니어는 사용자의 고유한 요구, 요구사항 및 성공 사례 지식 및 산업 표준을 이해하여 효과적인 보안 아키텍처를 설계, 개발 및 구현할 수 있습니다. 슈나이더 일렉트릭은 기본 SL-1 규정 준수의 요소에서 종합적인 솔루션에 이르기까지 사용자의 요구를 충족할 수 있도록 맞춤화할 수 있는 '심층적인 방어' 기반 보안 접근 방식을 통해 중요 인프라를 보호합니다.

모니터링

사이버 보안 솔루션을 모니터링해 장치와 시스템이 전체적으로 원활하게 기능하는지 확인할 뿐 아니라 위협을 감지하고 패치를 적용할 수 있습니다.

유지보수

사이버 보안을 지속적으로 검토하고 업데이트하는 것은 매우 중요합니다. 슈나이더 일렉트릭은 고객 팀과의 긴밀한 협력하에 시스템과 기술을 최신 상태로 유지하고 정기적인 테스트를 수행하여 보안을 극대화함으로써 고객이 안심할 수 있도록 합니다.

교육

인력은 지속적이고 효과적인 사이버 보안 보호에서 가장 중요한 요소입니다. 조직의 다양한 역할을 위한 효과적인 교육을 설계 및 제공하는 것이 매우 중요합니다. 기본 인식에서 전문가 수준의 기술에 이르기까지 슈나이더 일렉트릭의 팀은 광범위한 훈련 및 교육을 설계 및 제공하여 사용자가 회사의 사이버 보안 문화를 개발하도록 도울 수 있습니다.

사이버 보안 솔루션 포트폴리오

슈나이더 일렉트릭이 설계 및 구현하는 솔루션은 유연하며 사용자의 특정 요구 및 요구사항을 충족하도록 맞춤화할 수 있습니다. 가장 중요한 사이버 보안 솔루션 요소는 4개의 범주로 정의됩니다.

허용 – 네트워크 및 물리적 제어를 통해 운영 시스템 및 정보에 대한 액세스를 관리합니다.

보호 – 지속적인 보호를 위해 운영 시스템의 일부로 특정 제어를 구현합니다.

감지 – 운영 환경을 모니터링하여 위협을 감지하고 전달합니다.

대응 – 공격을 억제하고 완화하기 위해 사이버 사고에 신속하게 대응할 수 있도록 지원하는 절차 및 시스템을 개발합니다.

허용

- 인증, 권한 부여, 계정
- 다중 인증
- 네트워크 세분화
- 보안 원격 액세스
- 물리적 보안

보호

- 엔드포인트 보호, 맬웨어 방지,
- DLP, HIPS, 화이트리스팅
- 이동식 미디어 제어
- 패치 관리

감지

- 보안 정보 및 이벤트 관리(SIEM)
- 네트워크 성능 모니터링
- 자산 식별
- 이상 감지
- 침입 감지

대응

- 백업/재해 복구
- 포렌식
- 사건 대응

디지털 시대의 사이버 보안

사이버 보안을 시작하는데 어려움을 겪고 있거나, 사이버 보안 전략을 구현하는 데 도움이 필요할 경우 경험과 역량을 갖춘 슈나이더 일렉트릭 전문가가 사용자의 상황과 요구사항을 고려하여, 사용자의 요구에 맞는 솔루션으로 사이버 보안 문제를 해결할 수 있습니다.

슈나이더 일렉트릭은 사용자의 운영 관점에서 사이버 보안 솔루션을 이해하고 적용하는 동시에 적절한 IT 정책 및 요구사항을 통합합니다. 이러한 부분이 바로 슈나이더 일렉트릭의 차별화된 서비스이며, 사용자는 이를 통해 이점을 얻을 수 있습니다.

슈나이더 일렉트릭의 360° 사이버 보안 솔루션

경쟁력 있고 신뢰할 수 있는 제품과 플랫폼 제공

핵심 제품과 상호운용되는 보안 제품.
최고 수준의 파트너십 에코시스템.

중앙 집중화된 보안 지식 및 상호운용 가능한 보안 솔루션

글로벌 차원의 엔드 투 엔드 컨설팅, 통합, 유지보수 및 관리형 서비스

글로벌 파트너 및 입지

풍부한 파트너 에코시스템

오늘날 모든 기업은 확장된 엔터프라이즈 접근 방식을 활용하여 취약점을 해결 및 제거합니다. 개방형 에코시스템의 장점은 업계를 선도하는 다른 벤더의 솔루션으로 강화할 수 있다는 것입니다.
따라서 슈나이더 일렉트릭은 글로벌 파트너와 협력하여 가능한 최고의 제품, 서비스, 솔루션을 제공합니다.

글로벌 범위

슈나이더 일렉트릭은 사이버 보안을 위한 강력한 글로벌 팀을 보유하고 있습니다. 슈나이더 일렉트릭은 강력한 IT 경험과 OT 세계에 대한 심층적인 지식을 활용하여 고객이 현재 갖고 있는 능력과 사이버 보안을 관리하는 데 있어서 가장 큰 격차가 있는 영역을 이해하도록 돕고 있습니다.

슈나이더 일렉트릭의 신속한 대응 팀이 사이버 공격이 발생할 경우 고객이 빠르게 조치를 취해 잠재적인 손상을 평가하고 복구하도록 지원할 준비가 되어 있습니다.

슈나이더 일렉트릭은 다음과 같은 보안 기관 및 협회의 소속입니다.

- ISA 글로벌 사이버 보안 연합
- 사이버 보안 연합
- 사이버 보안 기술 협정

팀 인증

산업 전반에서 사이버 보안 증가

어떤 산업이든지 관계없이 슈나이더 일렉트릭은 중대한 사이버 보안 솔루션을 구현하도록 지원할 수 있습니다. 슈나이더 일렉트릭은 식품 및 음료에서 오일 및 가스와 석유화학에 이르기까지 모든 산업에서 풍부한 경험을 갖고 있습니다.

SITE #1

(프랑스 – 선도적인 식품 생산 회사)

사이버 제품:

- IT/OT 통합
- DMZ 구현
- 보안 아키텍처 설계 및 구축
- 글로벌 사용자 관리 시스템, 네트워크 모니터링

성공 요인:

- 고객의 글로벌 영업 요구를 충족하는 맞춤형 솔루션
- 산업 및 국가 표준을 충족하는 중앙 집중화된 호스트 및 네트워크 솔루션

SITE #2

(카타르 – 중동의 LNG 리더)

사이버 제품:

- 사이버 보안 완충 지대(DMZ) 구현
- OT 네트워크의 CS 제어 현대화
- ICS를 위한 제3자 IT/OT 통합

성공 요인:

- ICS, OT 네트워크 + IT 인터페이스를 위해 제공된 맞춤형 시스템
- 관리형 멀티 벤더 OEM 시스템

사이버 보안 강화

강력한 사이버 보안은
비즈니스
요구사항입니다.

보안 데이터 수집 및 전송은 IoT의 이점을
활용할 때 매우
중요합니다.

슈나이더 일렉트릭은
사용자의 디지털
트랜스포메이션을
지원하기 위해 노력하고
있습니다.

Life Is On | Schneider Electric

웹사이트를 방문해 사이버 보안 위협으로부터
비즈니스를 보호하는 방법에 대해 자세히
알아보세요.

se.com/cybersecurity

SE 블로그

Schneider Electric
서울특별시 강서구 공항대로 248
DMC 타워 13~15층
전화: +82 1588 2630