SIEMENS
Ingenuity for life

플랜트 보안 서비스

고객의 자동화 자산을 보호하는 디지털 시대의 보안 기술

Innovation Tour Korea 2020

Innovation Tour Korea 2020 – Concept

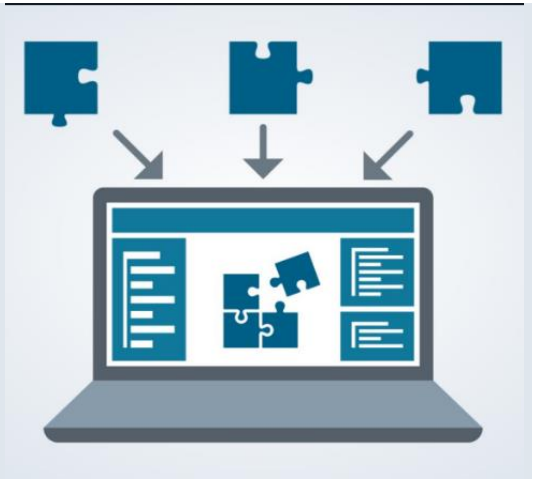
SIEMENS
Ingenuity for life

디지털 워크플로우

- 가상시운전
- SIMATIC Industrial Edge

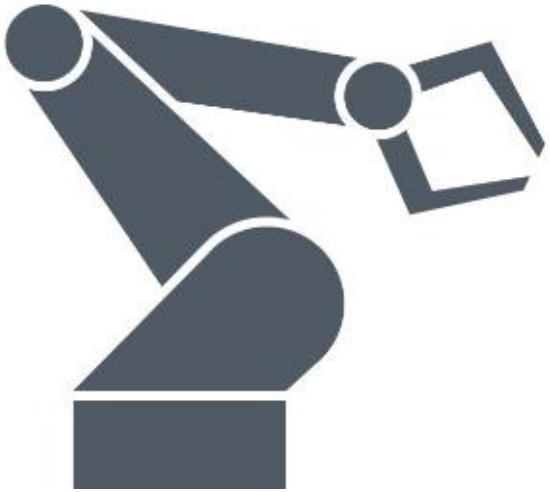
통합자동화

- SINAMICS Inverter
- SINAMICS Connect 300



운영 투명성

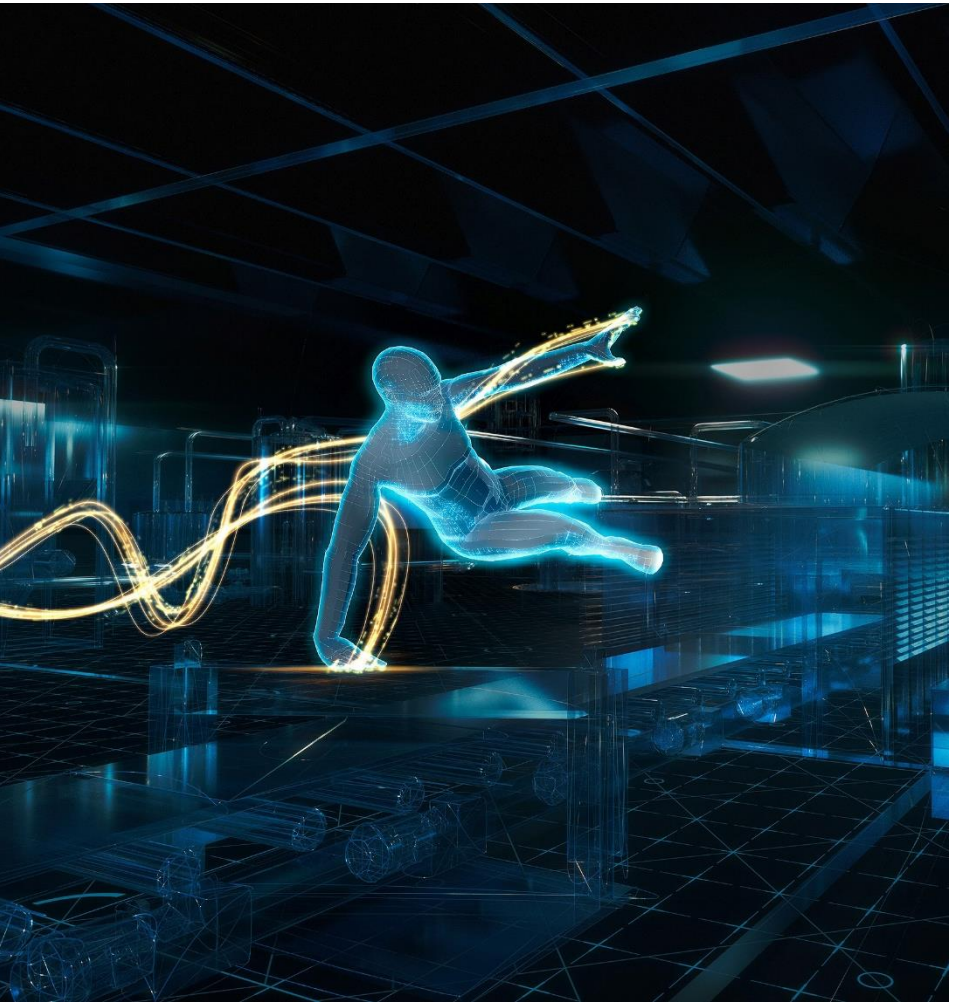
- WinCC Unified & Unified Panel
- 산업 네트워크 커뮤니케이션
- **플랜트 보안 서비스**



현장 사례

- SIMOCODE pro

목차



- 사이버 위협 환경
- 지멘스의 보안 솔루션
- 보안 컨설팅
- 보안 시스템 도입
- 보안 최적화

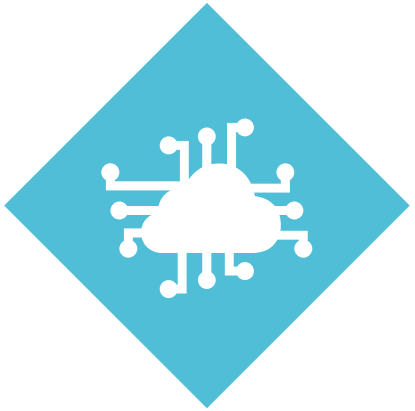
지속적으로 변화하는 위협 환경

SIEMENS
Ingenuity for life

전문적인
Hackers

디지털 환경에서의
보안 취약성

사물 인터넷
IoT



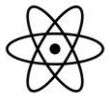
사이버 보안
법률 / 제도적 규제

Industrial Security Services
Actual Cases

SIEMENS
Ingenuity for life

2010
- 오하이오 핵발전소 공격으로 운영 중지 (웜) 2003

2011
- 이란 우라늄 농축시설 해킹 감염 (악성코드)



2012
- 사우디 아람코 정유 생산 마비 (악성코드)

- 카타르 LNG 생산시설 네트워크 마비 (악성코드)

2013
- 미국 뉴욕 댐 제어시스템 감염

- 벨기에 할만 컨테이너 제어시스템 해킹 (범죄목적)

2014
- 미국 의료기관 제어시스템 감염으로 혈액공급펌프 오작동 (악성코드)

- 미국 미시간 신호제어 시스템 감염(악성코드)

- 독일 제강공장 제어시스템 감염으로 운영중단 (악성코드)

2015
- 독일 제강 공장 용강로 손상 (악성코드)

- 우크라이나 전력청 감염으로 6시간 정전 (악성코드)

2017
- 미국 의약품 제조사 Merck 생산 중단 (랜섬웨어)

- 글로벌 해운사 머스크라인(Maersk) 시스템 운영중단 (랜섬웨어)

2018
- 사우디아라비아 석유화학 공장 전체 운영 중단 (ESD 목표 악성코드)

2019
- 알루미늄 공장 글로벌 운영중단 (랜섬웨어) : Norsk Hydro

취약성(Vulnerability)의 증가

SIEMENS
Ingenuity for life

90%

의 성공적인 사이버 공격은
이미 패치가 제공된 취약성(Vulnerabilities)에 기반하고 있음

55%

의 회사는 사이버 공격에서 복구하기 위해
최소 3시간 이상의 시간이 필요함

205 Days

은 2017년 기준 평균 시간으로
사이버 공격을 받은 사실을 확인하는데 소요함

44%

의 회사들은
사이버 공격의 원인 파악에 실패함

34%

의 자동화 제어 시스템을 보유한 회사들은
12개월 동안 최소한 2회 이상의 사이버 공격을 받음

위협은 유사하지만, 실제로는 IT 와 산업 (OT) 보안은 큰 차이가 있음

SIEMENS
Ingenuity for life

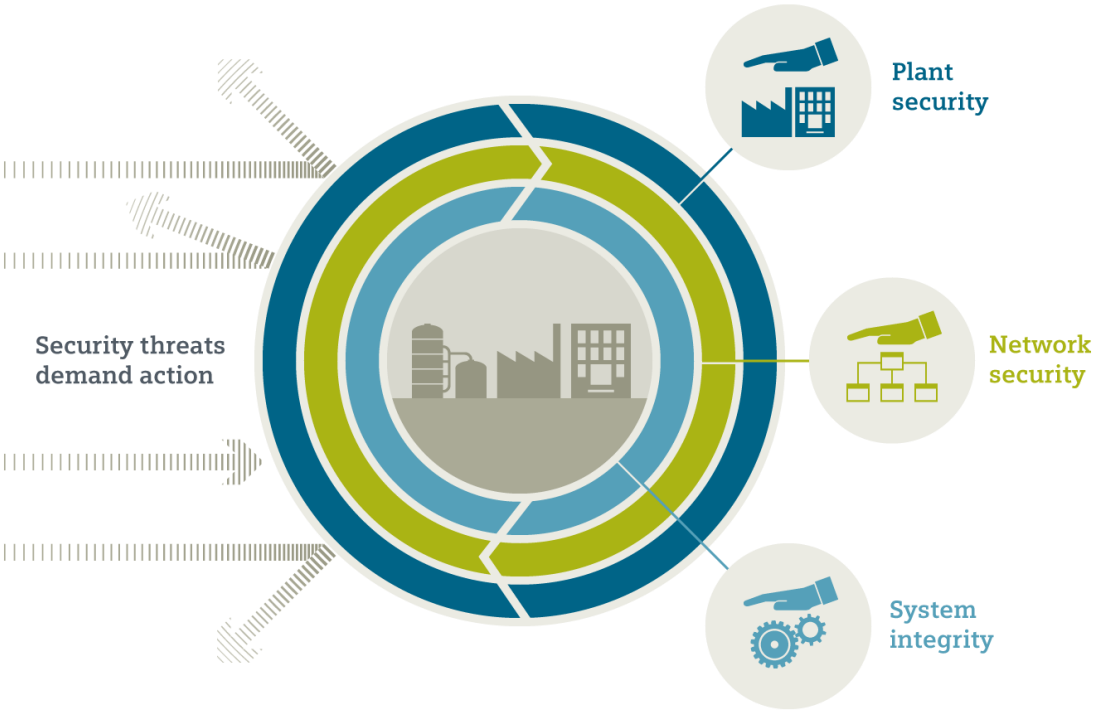
IT Security		Industrial Security
기밀유지		안정적인 운영
3-5 years	장비 사용연한	20-40 years
강제적인 Migration (예, PCs, smart phone)	소프트웨어 사용 연한	Usage as long as spare parts available
높다 (오피스 PC는 10 이상의 프로그램 실행)	보안 소프트웨어 추가 가능성	낮다 (여분의 성능이 없는 오래된 시스템)
낮다 (2개 세대 이하, Windows 7 and 10)	컴퓨터 환경의 불균질성	높다 (Windows 95 에서 10)
표준 기반 (보안 프로그램 및 강제 패치)	중요 보호 개념	상황과 위협 상황에 기반

- 산업 보안 시스템은 생산활동을 방해하지 않으면서도 효과적인 방어가 가능하도록, 최적화된 보안 시스템이 도입되어야 함

지멘스에서 제공하는 산업 보안

SIEMENS
Ingenuity for life

지멘스의 보안 전략 – “심층 방어”



지멘스 제품과 시스템으로 통합 보안을 제공

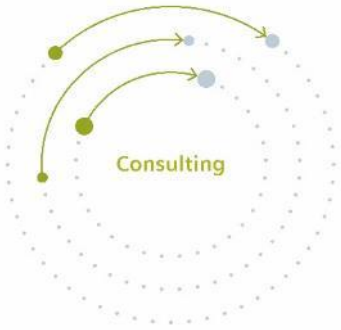
노하우 보호 및 복제 방비

사용자 인증 및 사용자 관리

방화벽과 VPN

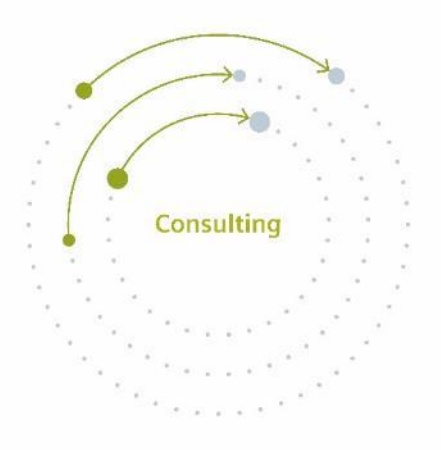
시스템 하드닝, 지속적인 모니터링 및 이상 검출

지멘스 산업 보안 서비스



산업 보안 서비스
End-to-end approach

SIEMENS
Ingenuity for life



Security Consulting

현재의 산업 보안 수준 및 산업 환경에 대한 평가

- 산업 보안 평가
- 스캐닝 서비스
- 산업 사이버 보안 컨설팅

Security Implementation

보안 관리 체계 도입을 통한 리스크 완화

- 보안 인식 교육
- 차세대 방화벽
- 산업 네트워크 이상동작 검출

Security Optimization

Managed 서비스를 통해 전반적인 보안 체계 도입

- 산업 보안상황 모니터링
- 원격 이상 조치
- 산업 네트워크 취약성 관리
- SIMATIC 보안 서비스 Packages

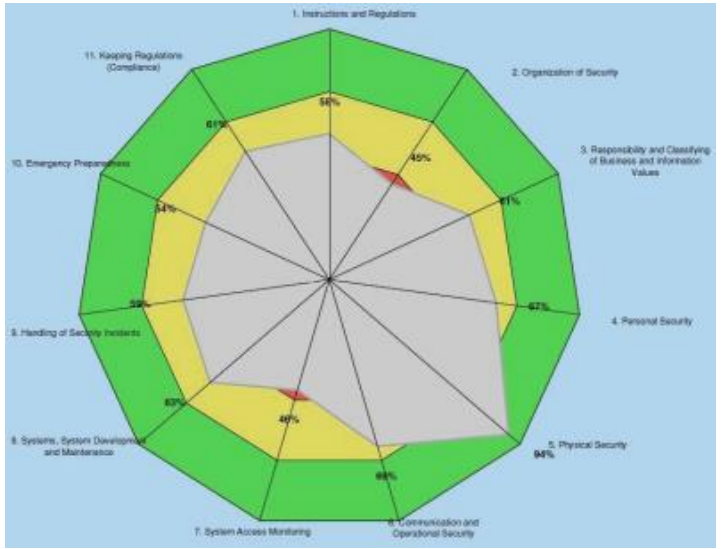
Security Consulting
IEC 62443 / ISO 27001 평가

SIEMENS
Ingenuity for life

국제 표준인 IEC 62443 또는 ISO 27001 국제 표준 에 적합한 간략한 형태의 보안 평가

- **IEC 62443** Parts 2-1에서 정의하는 “산업 자동화 시스템 및 보안 프로그램 구성” 와 Part 3-3 “산업 제어 시스템의 보안 **– 네트워크 및 시스템의 보안 체계**” 에서 정의한 내용을 기반으로 한 서비스
- **2 days** on-site
- **보안전문 컨설턴트, 보안 엔지니어**에 의해서 수행됨
- **지멘스** 및 **타사제품의 시스템에도 적용가능**
- **리스크 분석** 및 이에 대한 **대응 방안 리포트가 제공됨**

기업의 산업 보안 적용 방향을 수립하고, **현재의 단계에** 대한 **이해 및 발전 수준 평가**에 용이한 **컨설팅 서비스**

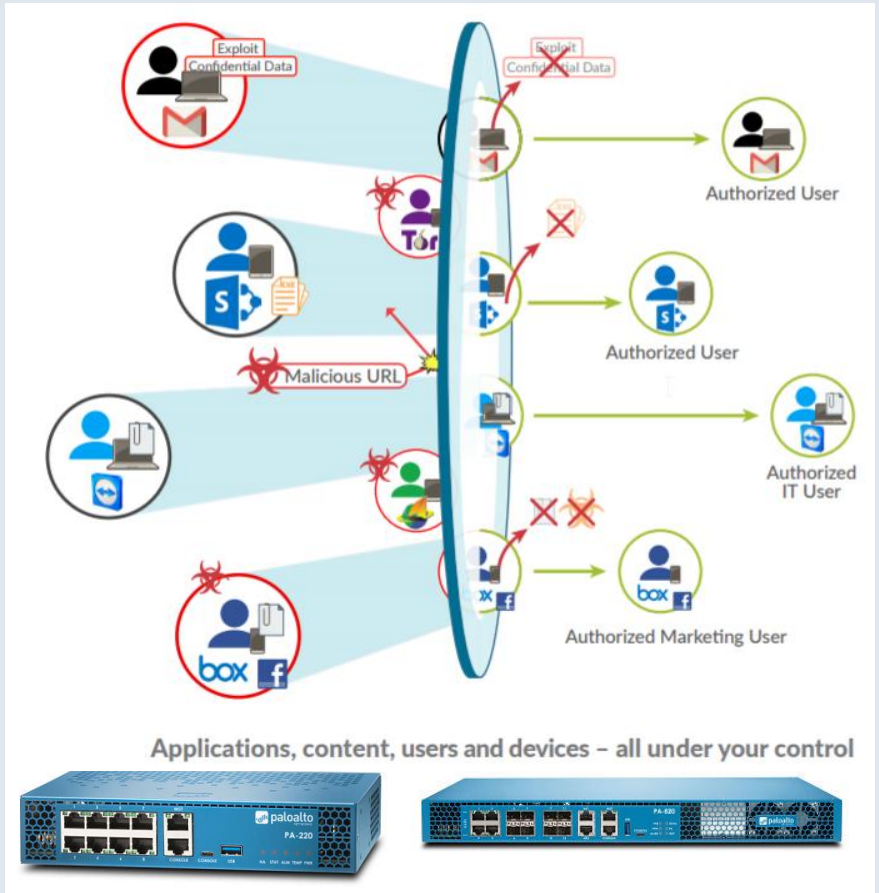


	Security Areas (Evaluation / Result)	Need for Action		Remarks (Priority)	
Management / Organisation	1. Instructions and Regulations	58%		1,0	
	2. Organization of Security	45%		1,0	
	3. Responsibility and Classifying of Business and Information Values	61%		1,0	
	4. Personal Security	67%		0,9	
Technique and Operation	5. Physical Security	94%		1,0	
	6. Communication and Operational Security	69%		0,9	
	7. System Access Monitoring	46%		0,9	
	8. Systems, System Development and Maintenance	63%		0,9	
	9. Handling of Security Incidents	59%		0,9	
	10. Emergency Preparedness	54%		0,9	
L / O	11. Keeping Regulations (Compliance)	61%		1,0	

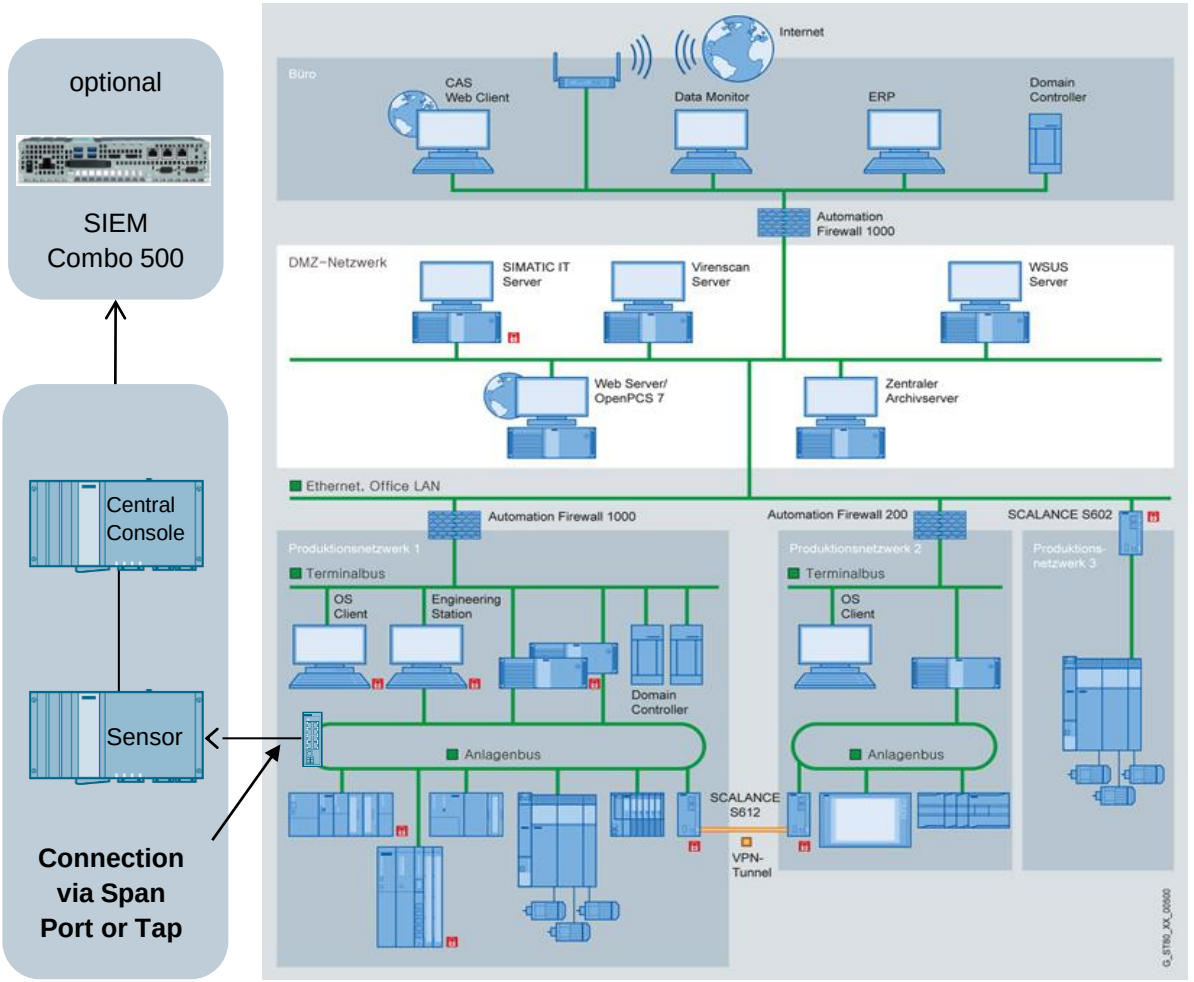
Security Implementation

SIEMENS
Ingenuity for life

자동화 시스템 방화벽 NG (Next-Generation)



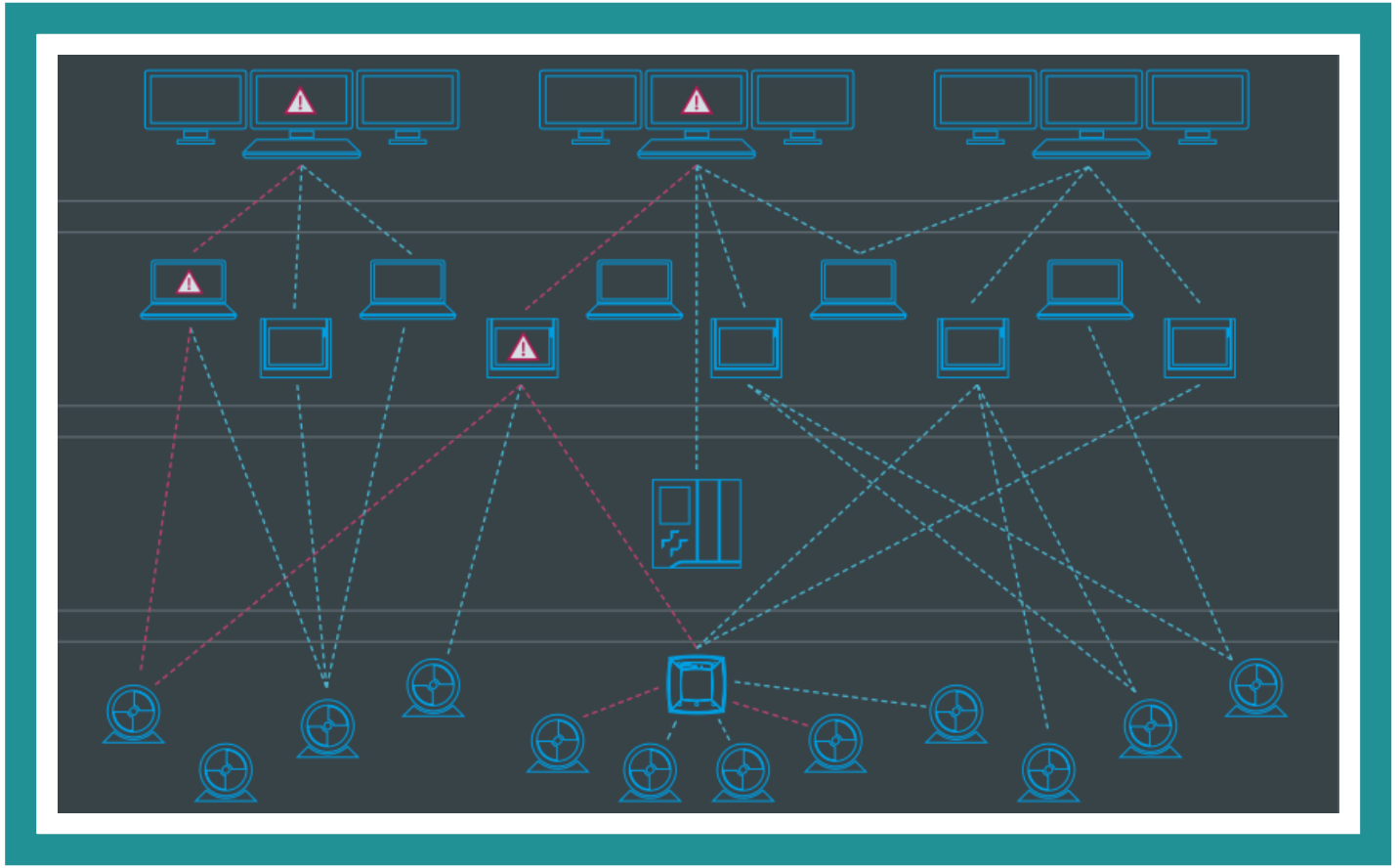
산업 네트워크 이상동작 진단



SIEMENS
Ingenuity for life

산업 네트워크 이상동작 진단 – 네트워크 뷰

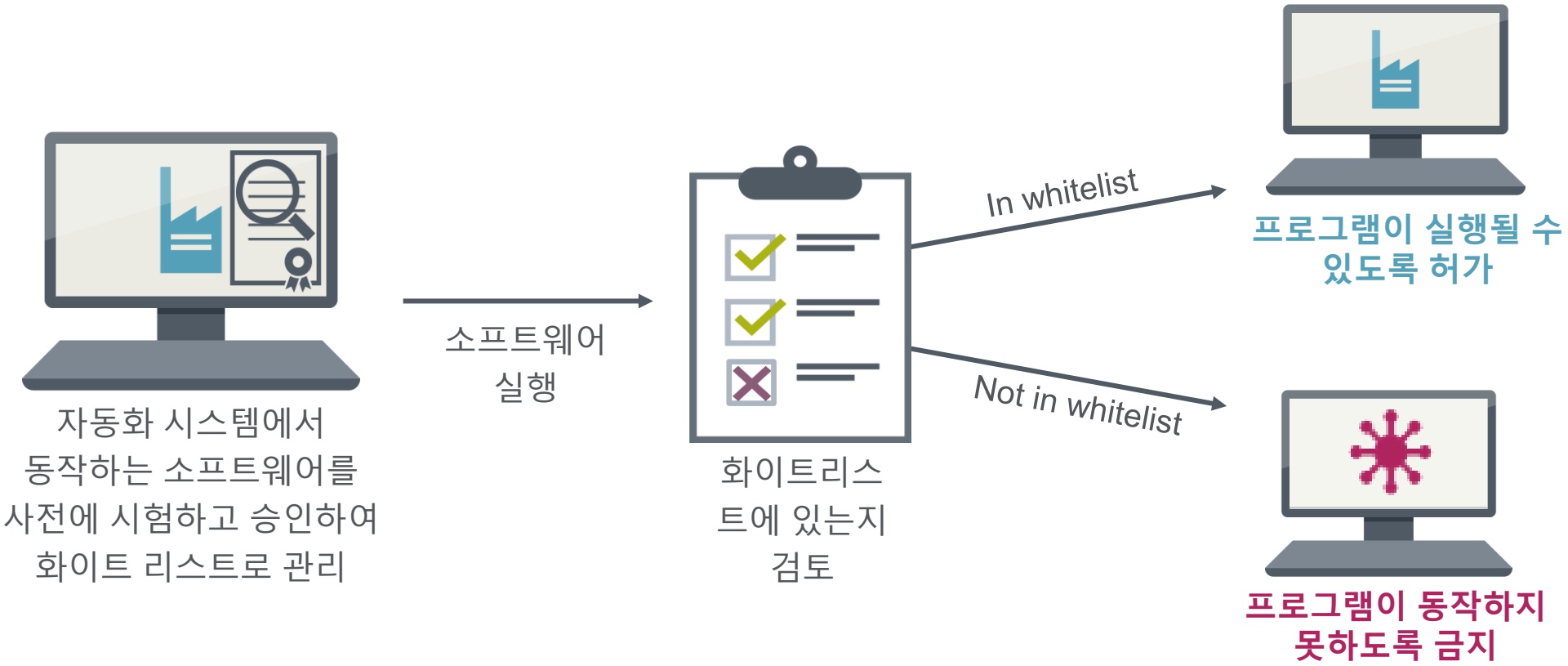
- 연결된 자산과 자산간의 통신 회선을 자동적으로 검출할 수 있음
- 효과적이고 손쉽게 구성할 수 있는 대쉬보드는 최소한의 구성만으로도 전체 Overview의 확인과 이벤트 관리가 용이함
- 취약점 정보도 시각화 가능함
- 지멘스 제품 뿐만 아니라 3rd Party 제품군에도 적용가능



Security Implementation
Whitelisting

SIEMENS
Ingenuity for life

화이트 리스팅은 어떤 원리로 동작하는가?



Security Optimization
Patch Management

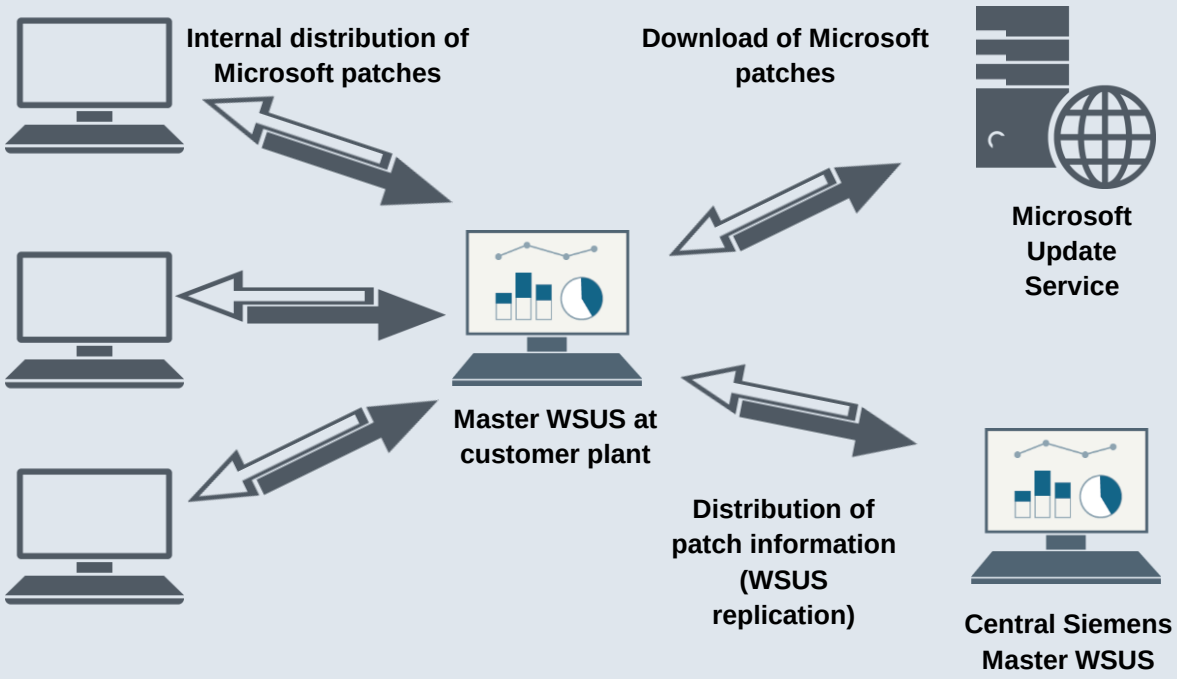
SIEMENS
Ingenuity for life

Our Solution

패치 & 취약점 관리 서비스로 사용자의 패치 서비스를 손쉽게 자동화함:

1. Microsoft 매월 제공되는 패치 서비스 (Patch Tuesday)
2. SIMATIC PCS 7 호환성 테스트
3. Siemens Master WSUS에서 제공되는 패치: 지멘스에서 업데이트 서버(WSUS)를 통해 PCS 7의 호환성 테스트가 끝난 패치의 Medata를 제공함
4. Medata 정보를 고객사로 제공하는 것은 완전히 자동화로 구성 가능
5. 고객이 새로운 패치가 있다는 통보를 받음
6. 고객사는 Microsoft로부터 패치를 직접 다운로드 받아 현장의 시스템에 설치함.

Solution Architecture

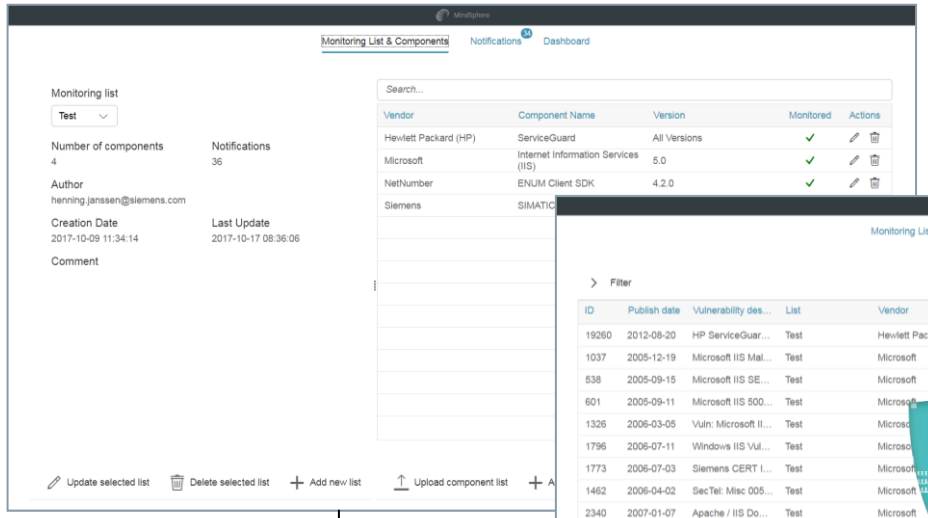


Security Optimization

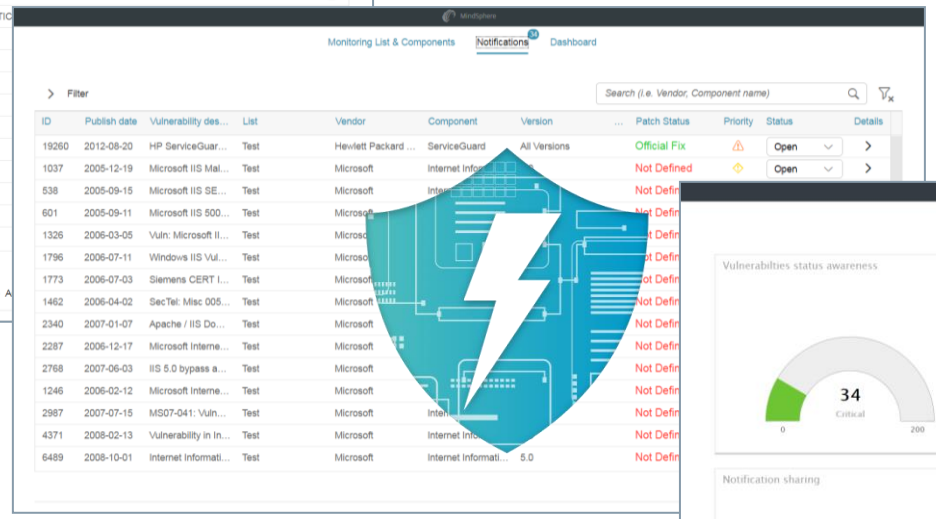
SIEMENS
Ingenuity for life

Mindsphere 기반의 보안 취약성 관리 시스템
(Security Vulnerability Information Management)

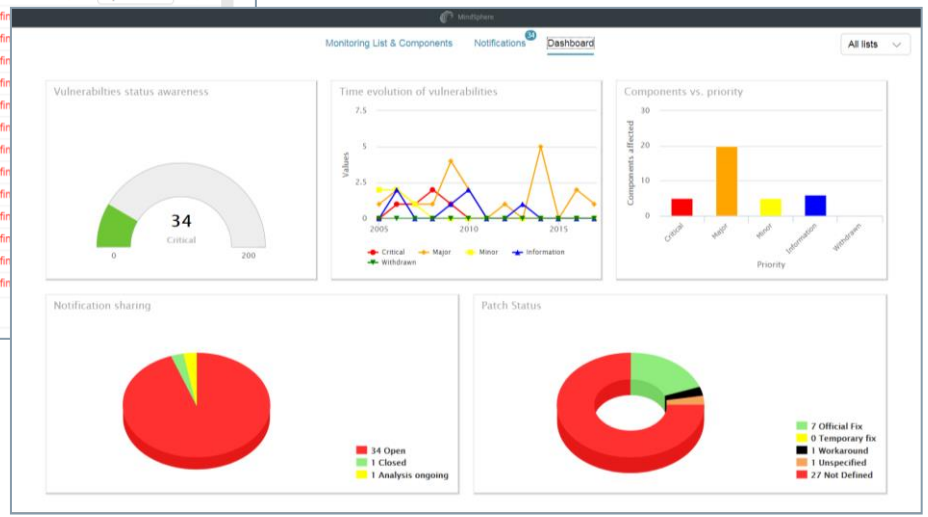
모니터링 대상 소프트웨어 선정

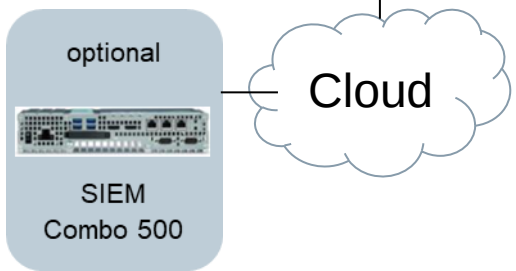


취약점이나 패치 소프트웨어를 감지하면 알림



리스크 기반의 취약점 관리

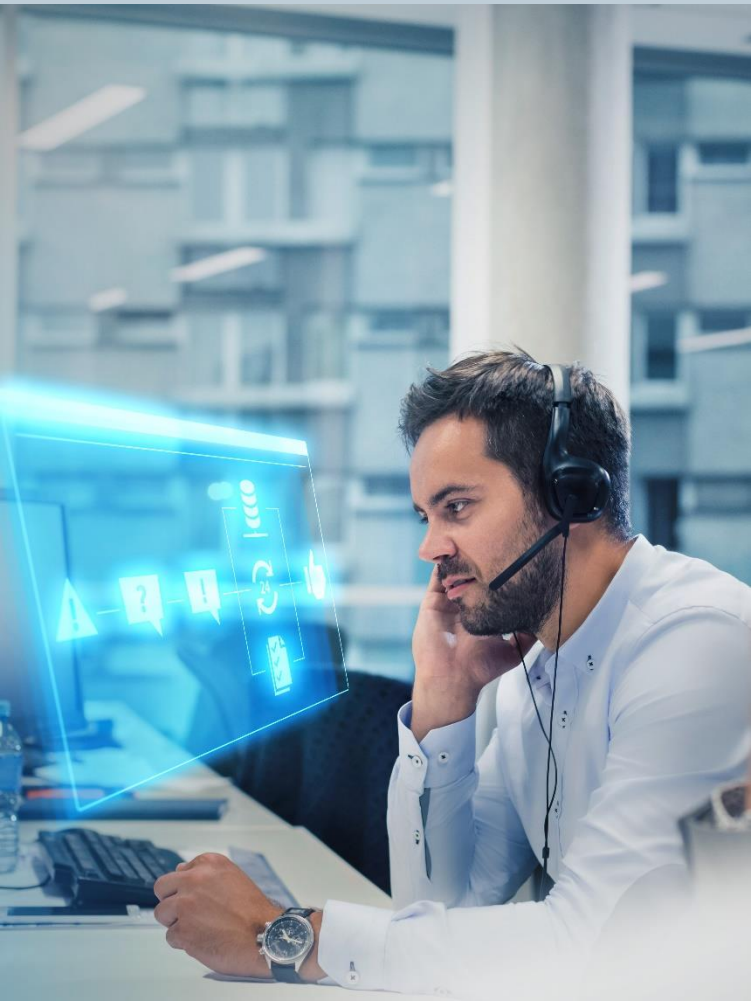




Security Optimization

SIEMENS
Ingenuity for life

원격 사고 처리를 통한 보안 사고에 대한 빠른 대응



Remote Incident Handling

- 보안 강화를 위해 가장 포괄적 인 대비를 구현해도 공격 및 보안 사고에 대한 100 % 보호를 보장하지는 않습니다. 보안 사고를 신속하고 목표에 맞게 정리함으로써 피해와 그 영향 최소화 가능
- 원격 사고 처리를 통한 보안 사고에 대한 빠른 대응
- 공장이 영향을 받는 경우 Siemens 산업 보안 전문가는 데이터 수집 및 분석부터 쉽고 빠른 대응 모델 제시까지 원격으로 지원

어떻게 동작하는가?

- 원격 사고 처리는 신속한 생산 복구에 중점

포렌식 정보 수집 ▶ 원인-결과 및 중요도에 따른 포괄적인 분석 ▶ 적절한 대응 전략 추천

주요 차별성

독일 보안 전문가 그룹의 직접적인 지원

생산 설비의 빠른 복구 지원

다운타임 비용의 최소화

Digitalization and security

SIEMENS
Ingenuity for life

디지털화는 분석된 데이터를 기반으로 **새로운 통찰력**을 가능하게 함

... 그렇지만, **사이버 공격**이라는 새로운 리스크도 있음.

지멘스는 안전한 Digitalization의 도입을 가능하게 하는 신뢰도 높은 파트너입니다.

- Digitalization에 대한 깊은 이해
- 산업에 대한 Kow-how
- 산업 네트워크 통신에 대한 깊은 이해
- 산업 보안 전영역에 대한 제품과 서비스 포트폴리오 보유
- 지멘스의 업무 프로세스와 제품의 성능은 산업 표준으로 인증됨

사이버 보안이 없는 Digitalization은 가능하지 않습니다.!

지멘스 Innovation Tour 2020 행사 요약

SIEMENS
Ingenuity for life

이제는 디지털화를 준비 해야 할 때 !

디지털화의 선두주자 지멘스가 제안하는
최적의 자동화 솔루션 라인업을 경험하십시오!

- ☑ 지멘스의 디지털화 기술을 통해 제품의 시장 출시 일정을 단축 할 수 있습니다.
- ☑ 지멘스의 최고의 디지털 솔루션으로 생산 라인을 최적화하고, 비용 절감, 생산성 및 유연성 향상을 동시에 달성할 수 있습니다.
- ☑ 디지털화를 통해 원격 모니터링과 조작 기술을 적용한다면, 모바일 작동 가능 시스템으로도 자동화 시대를 준비할 수 있습니다.
- ☑ 지멘스 디지털화 포트폴리오로 핵심 기술 역량을 개발 가능합니다. 이를 통해 인더스트리 4.0 시대에 경쟁력을 강화할 수 있습니다.

Contact

Joung, SoungMoon

DI CS DS
Consultant for Digital Service

Soungmoon.joung@siemens.com