CLAROTY COONTEC

생명과 안전을 지키는 ICS/OT 보안전략 수립 방안

Bridging the IT-OT Cybersecurity Gap

1부 : 정해식 책임 컨설턴트 | 클래로티코리아
2부 : 방혁준 대표 | 쿤텍

15th Oct, 2020

정해식 책임 컨설턴트 | ICS 사이버보안 | 클래로티코리아

[ICS/OT 보안 및 안전 관련 국제공인자격 보유]

- GICSP(국제산업사이버보안전문가) #1970 자격: SANS/GIAC | USA
- ISA/IEC 62443 CFS #20859114 자격 및 (현)사이버보안 표준위원회 활동, ISA(국제자동화협회) | USA
- FS(Functional Safety) Eng #17487/19 자격: IEC61508 & IEC61511, TÜV Rheinland | Germany
- GPEC SCADA Engineering #F161111-1003 자격: YHQ | Japan, Netherlands

[국내/외 100여개 이상의 ICS/OT 사이버보안 프로젝트 수행]

- ICS/OT Architect & FAT/SAT 수행 : 사이버보안 및 제어시스템(DCS/PLC/SCADA/OPC/PIMS/AMS 등)
- 글로벌 프로젝트 : 사우디아라비아, 알제리, 인도, 싱가폴, 인도네시아, 말레이시아, 베트남, 필리핀 등
- 프로젝트 수행 산업군 : 오일&가스 | 화공플랜트 | 제조업 | 발전소 | 식음료 | LNGC | 수처리 | BMS 등

[경력 사항]

- 2019~현재 : ICS/OT Cyber Security(사이버보안) Consultant, 클래로티코리아
- 2019~현재 : ISA/IEC 62443 - IACS(사이버보안) 표준위원회 회원, ISA(국제자동화협회)
- 2019~2019 : ICS/OT Cyber Security(사이버보안) Specialist, 한국하니웰
- 2011~2019 : ICS/OT Cyber Security(사이버보안) Specialist, 한국요꼬가와전기

1. ICS/OT 산업제어시스템
2. 생명과 산업을 위협하는 ICS/OT 위협 트렌드
3. 글로벌 가이드 및 표준에 따른 ICS/OT 보안
4. 클래로티·쿤텍 OT보안솔루션 도입 사례 소개

Bridging the IT-OT Cybersecurity Gap

1. ICS/OT 산업제어시스템

Bridging the IT-OT Cybersecurity Gap

CLAROTY

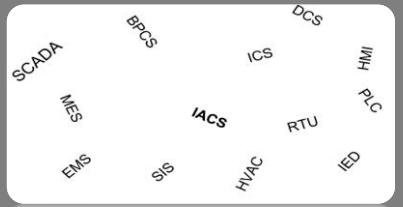
산업제어시스템

NIST 800.82

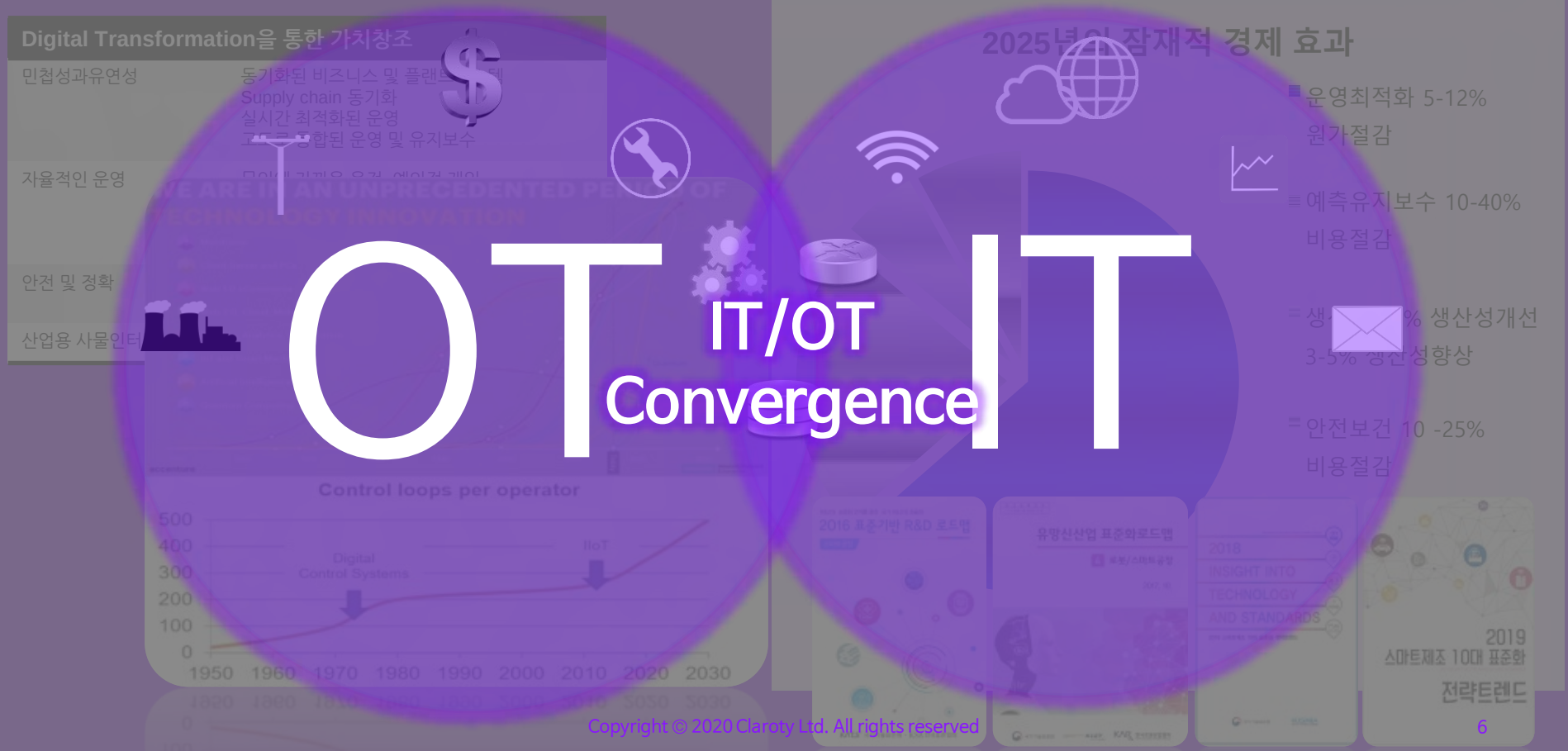
ICS의 형태

- PLC
- DCS
- SCADA
- BAS (BMCS)
- SIS

Et cetera



OT (Operational Technology | 운영기술)
ICS (Industrial Control System | 산업 제어 시스템)
OT ⊃ ICS ⊃ SCADA / DCS / PLC Et cetera



CLAROTY COONTEC

2. 생명과 산업을 위협하는 ICS/OT 위협 트렌드

Bridging the IT-OT Cybersecurity Gap

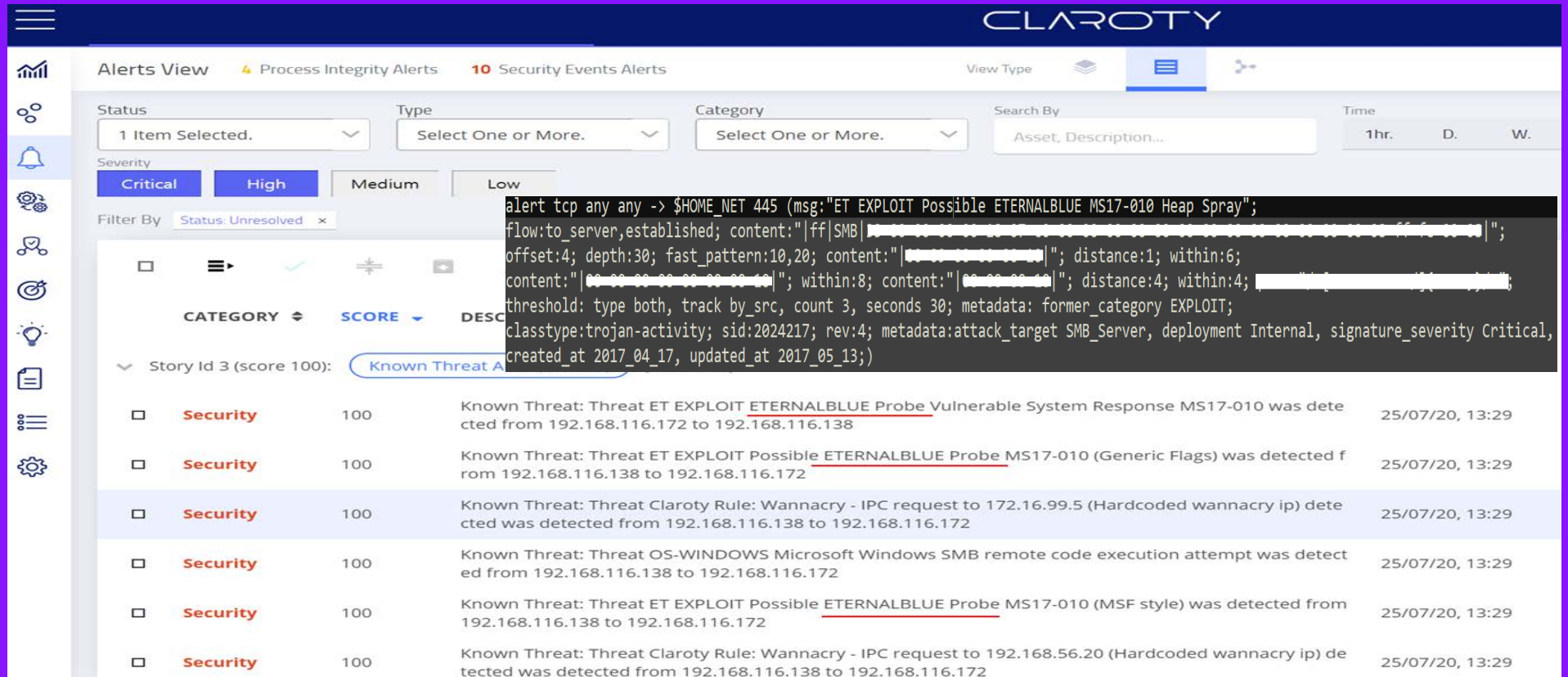
Case #01: NotPetya 랜섬웨어 3주년

CLAROTY

Case#01 NotPetya 랜섬웨어 공격 3 주년: 2020년 6월 27일

NotPetya 랜섬웨어에 악용되었던 “EternalBlue 취약점”에 대하여

사고 발생 2개월 전에 이미 발표된 패치를 적용을 했었을 경우 피해 방지 가능!



Case #02: 혼다 전세계 공장 셧다운

CLAROTY

Case#02 사이버 공격에의한 혼다 자동차 공장 셧다운: 2020년 6월9일

CLAROTY

Alerts View 4 Process Integrity Alerts 10 Sec

Status: 1 Item Selected. Type: Select One or

Severity: Critical | High | Medium | Low

Filter By: Status: Unresolved

```
# Wannacry signatures
alert tcp any any -> any 445 (msg:"Claroty Rule: Wannacry - IPC request to 192.168.56.20 (Hardcoded wannacry ip) detected";
flow:to_server,established; content:"[redacted]";
classtype:trojan-activity; sid:[redacted];)
alert tcp any any -> any 445 (msg:"Claroty Rule: Wannacry - IPC request to 172.16.99.5 (Hardcoded wannacry ip) detected";
flow:to_server,established; content:"[redacted]"; classtype:trojan-activity; sid:
```

RESULTS (4)

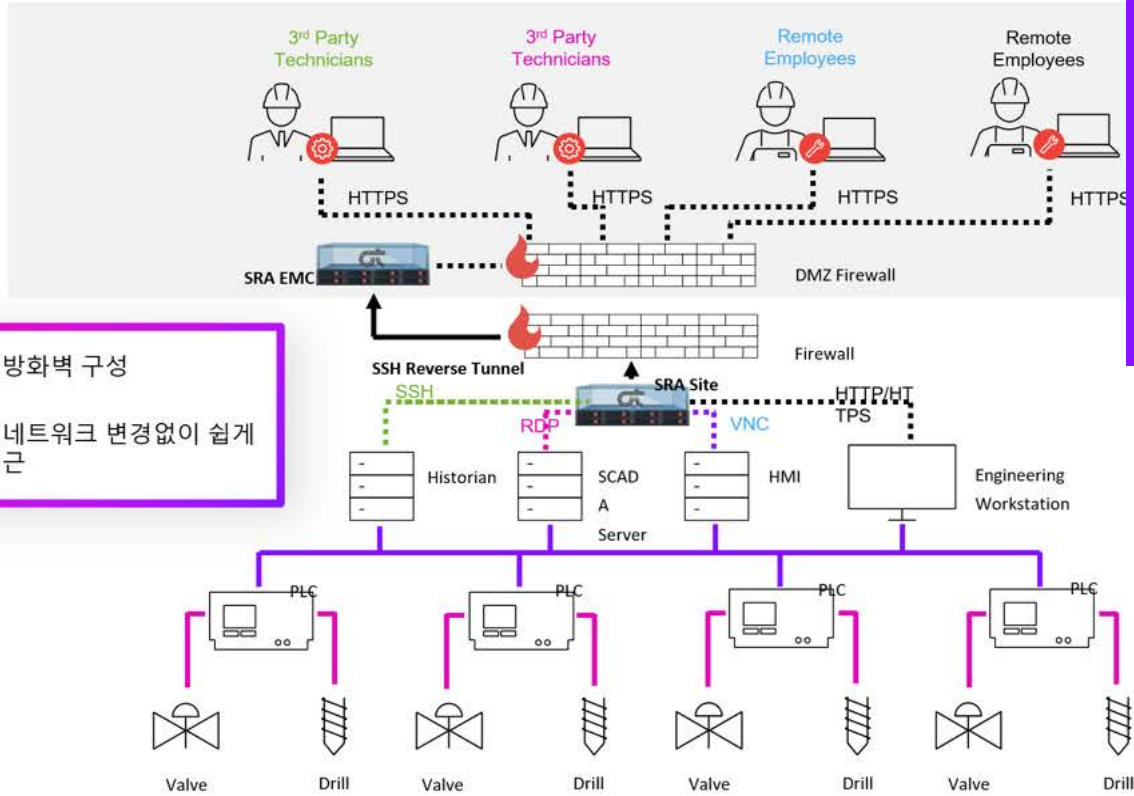
CATEGORY	SCORE	DESCRIPTION	DATE DETECTED
Story Id 3 (score 100): Known Threat Alert (6 alerts) (Total 6/6)			
Security	100	Known Threat: Threat ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010 was detected from 192.168.116.172 to 192.168.116.138	25/07/20, 13:29
Security	100	Known Threat: Threat ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags) was detected from 192.168.116.138 to 192.168.116.172	25/07/20, 13:29
Security	100	Known Threat: Threat Claroty Rule: Wannacry - IPC request to 172.16.99.5 (Hardcoded wannacry ip) detected was detected from 192.168.116.138 to 192.168.116.172	25/07/20, 13:29
Security	100	Known Threat: Threat OS-WINDOWS Microsoft Windows SMB remote code execution attempt was detected from 192.168.116.138 to 192.168.116.172	25/07/20, 13:29
Security	100	Known Threat: Threat ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style) was detected from 192.168.116.138 to 192.168.116.172	25/07/20, 13:29

Case #03: 이스라엘 수처리 공격 사례

CLAROTY

Case#03 이스라엘 수도 공급에 대한 주요 인프라 공격: 2020년 4월 24일

지리적으로 분산된 OT 환경에 시스템 공급 업체의 점검 등을 위한 원격 접근에 대한 Secure Remote Access를 배치 필요!!



간단한 방화벽 구성

비상시 네트워크 변경없이 쉽게 원격 접근

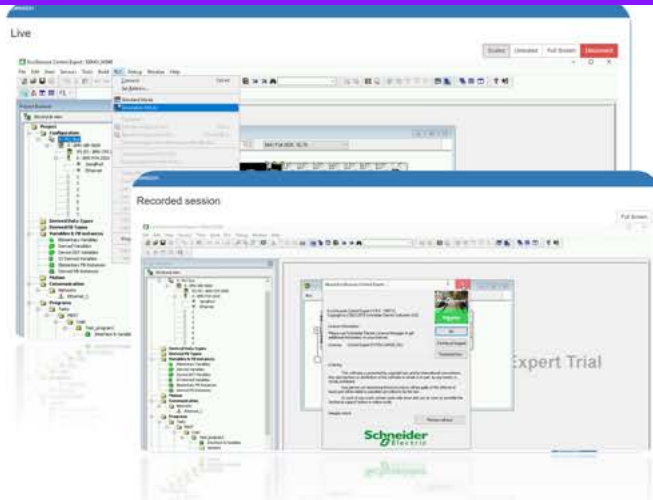
클래로티 SRA (Secure Remote Access)

세션 관리 (예약, 강제종료)

권한 관리 (최소 권한 부여)

증적 관리 (보안 에빈트 관리)

작업에 대한 자동 녹화 및 저장



Case #04: 사우디 정유사 공정 셧다운

CLAROTY

Case#04 Triton Malware 공격: 2017년 8월 4일

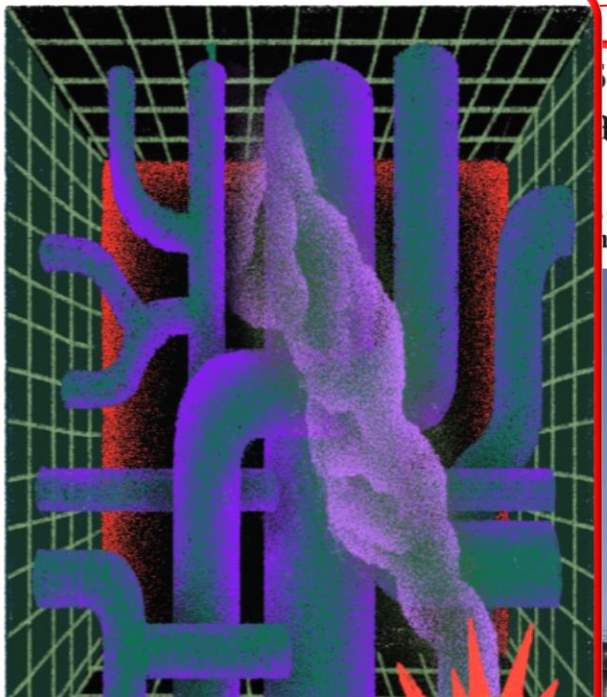
2017년 8월 4일 오후 7시 43분 사우디 아라비아의 Refinery Plant에서 ESD(비상 정지 시스템)이 가동 → 공정 셧다운
가스 누출과 치명적인 폭발을 방지하기 위해 설계되는 ESD로 인한 셧다운은 여러가지 원인이 밝혀지지만 이번엔 아님.

해커, OT망에 접근(2014) → 플랜트 1st 셧다운(2017년 6월) → 플랜트 2nd 셧다운(2017년 8월) → 사이버 공격(2017년 12월)

Computing / Cybersecurity

Triton is the world's most murderous malware, and it's spreading

The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of the world, too



take out safety systems attack on energy plant

operations at power station in
experts believe was state-sponsored

인명/산업 피해가 최종 목표였다면..?

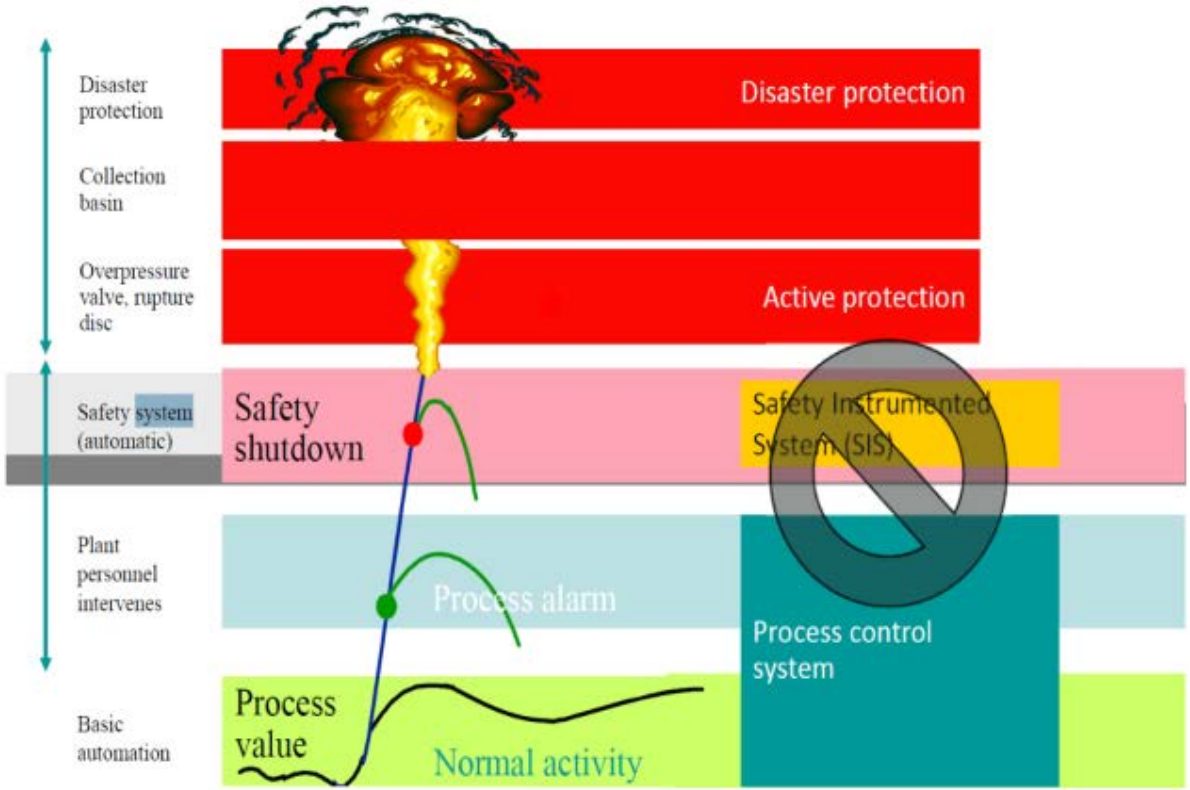
Bhopal 1984

CLAROTY

- Chernobyl Nuclear Power Plant (1986)
- Piper Alpha Platform (1988)
- Texas City BP Refinery (2005)
- Buncefield_Hemel_Hempstead (2005)
- Deepwater Horizon BP Oil rig (2010)
- Reynosa Gas Plant (2012)

18

오해 5: "우리 사이트의 SIS(안전계장시스템)가 있으니 괜찮아"



3. 글로벌 가이드 및 표준에 따른 ICS/OT 보안

Bridging the IT-OT Cybersecurity Gap

ICS 사이버 보안을 위한 요구 사항

Guide line & Regulation

Site Policy & Standard

Measures & Hardening

NERC(North American Electric Reliability Corporation)
NIST(National Institute of Standards and Technology)
IEC(International Electrotechnical Commission)
NEI(Nuclear Energy Institute)
⋮
*** 플랜트 사이버 보안
*** 해상 사이버 보안 기준
** SCADA & DCS 사이버 보안 표준
Saudi *** 산업 제어 시스템 보안
⋮

현장

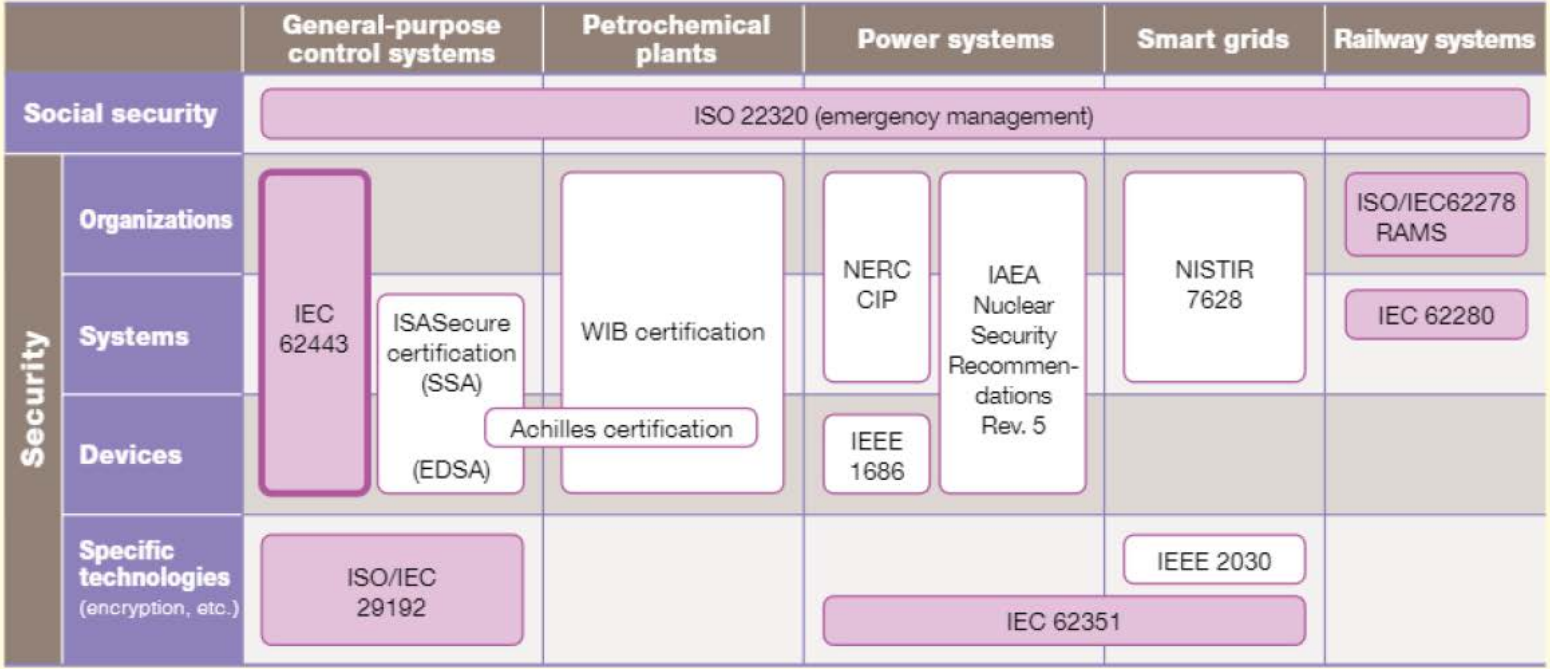
Design / 계획

Requirement to ICS/OT (보안) 전문 Vendors

적용 / 조치

유지 / 관리

제어분야 보안표준 관계도



ISA/IEC 62443 프레임워크 기반의 CSMS

- **ISA/IEC 62443**
  - 표준 제품군
  - ISA99위원회에서 시작 - IEC와 공동 개발
  - 산업 자동화 및 제어 시스템에서 현재 및 미래의 보안 취약성을 해결하고 완화하기위한 유연한 프레임 워크를 제공

- **ISA** (International Society of Automation)
  - IACS 제조사 및 유관 기업이 1945년에 설립한 비영리 기관
  - ANSI/ISA-62443를 기반으로 표준화 채택
- **ISA Security Compliance Institute (ISCI)**
  - ISA의 완전 소유 비영리 자회사
  - ISA / IEC 62334 표준에 대한 ISASecure 적합성 평가
- **International Electrotechnical Commission (IEC)**
  - 1906 년에 설립 된 세계 최고의
  - 모든 전기, 전자 및 관련 기술에 대한 국제 표준.
  - IEC 기술위원회 65 / Working Group 10에서 개발 된 ISA / IEC 62443

ISA/IEC 62443 Standards 구성

ISA/IEC 62443 Standards 구성

산업자동화제어시설

소유자

Operate

- ISA 62443-1-3: 시스템 준수사항
- ISA 62443-2-1: 보안 관리 요구사항
- ISA 62443-2-3: 패치 관리 요구사항

통합구축

설계/배포

- ISA 62443-2-4: 시스템 통합 요구사항

서브시스템1 | 서브시스템2 | 보완 구성 요소

- ISA 62443-3-3: 시스템 보안 요구사항

Products (off-the-shelf)

공급자

개발

- ISA 62443-4-1: 개발단계 보안 요구사항

어플리케이션 | 임베디드 디바이스 | 네트워크 장치 | 호스트 디바이스

- ISA 62443-3-3: 시스템 보안 요구사항
- ISA 62443-4-2: 구성요소 보안 요구사항

CLAROTY

KS 국가 표준 - ISA/IEC 62443

표준번호	표준명	개정/확인일	고시번호	적용범위
KS X IECTS62443-1-1	산업통신네트워크 - 네트워크 및 시스템 보안 - 제1-1부: 용어, 개념 및 모델	2020-04-08	2020-0064	이 표준은 한국산업표준(이하, "표준"이라 한다.)의 구성 및 표현형식에 대하여 규정하며 한국산업표준뿐만 아니라 단체표준, 회사표준 및 기술기준에도 적용이 가능하다. 한국산업표준은 국가표준으로서, 영문으로는 "Korean Standards"로 표기하며, 약칭은 "KS"로 한다.
KS X IEC62443-2-1	산업통신네트워크 - 네트워크 및 시스템 보안 - 제2-1부: 산업 자동화 및 제어 시스템 보안 프로그램 설정	2020-04-08	2020-0064	IEC 62443의 이 부분은 산업 자동화 및 제어 시스템 (IACS)을 위한 사이버보안 관리 시스템 (CSMS)을 구축하는 데 필요한 요소를 정의하고 그러한 요소를 개발하는 방법에 대한 지침을 제공합니다. 이 표준은 IEC/TS 62443-1-1에 기술된 IACS를 구성하는 것에 대한 광범위한 정의와 범위를 사용합니다. 이 표준에서 설명된 CSMS의 요소는 대부분 정책, 절차, 사례 및 인원 관련이며 조직의 최종 CSMS에 포함되거나 포함될 내용을 설명합니다.
KS X IEC62443-4-2	산업제어시스템 보안 제4-2부: 산업제어시스템 컴포넌트의 기술적 보안 요구사항	2020-04-08	2020-0064	IEC 62443의 이 부에서는 제어시스템 역량 보안등급 및 컴포넌트, SL-C(컴포넌트)의 요구사항 정의를 포함하여 IEC TS 62443-1-1에 서술된 7 가지 기본 요구사항(FR)과 관련된 상세한 기술적 제어시스템 컴포넌트 요구사항(CR)을 제공한다.

CSMS 프레임워크의 의미

1. 참조할 수 있는 OT 보안 베스트 프렉티스를 알고 있습니까?
2. 장기적인 OT 보안 로드맵을 계획하기 위한 지식체계가 있습니까?
3. OT 보안을 위해 효과적인 방법의 리스트를 갖고 있습니까?
4. OT분야의 주요 Player들이 준수(참조)하는 표준이 있습니까?
5. 최신 기술과 트렌드가 반영된 표준이 있습니까?
6. 구축된 IT(ISMS)보안과 유기적으로 적용할 수 있습니까?
7. 이미 다양한 분야에서 오랫동안 검증된 것입니까?

CSMS의 적용 개념

Asset Owner	System Integrator	Product Supplier
IACS	Automation Solution	Component/Control System

CSMS (IEC 62443)와 ISMS (IEC 27000) 비교

- IEC 62443-2- 1은 ISO / IEC 27001을 참조하여 개발됨
- ISMS는 정보의 유출에 초점을 맞추고 있으며 대부분의 경우 기밀성, 무결성 및 가용성 (CIA)을 순서대로 강조
- CSMS는 '작동 중지'를 가장 피해야하는 이벤트로 간주하며 가용성, 무결성 및 기밀성 (AIC)을 순서대로 강조
- HSE (Health & Safety Executive) 환경을 고려해야 함
- 제어시스템 가용성, 공장 보호, 공장 운용 (저하모드에서도) 및 시간-임계적 시스템 응답에 목표

속성	OT 중심	IT 중심
기밀성 / 개인 정보 보호	Low	High
메시지 무결성	Very High	Low - Medium
시스템 가용성	Very High	Low - Medium
입증	High	Medium - High
부인 방지	Low-medium	High
안전	Veri High	Low
시간 중요도	Critical	Delay 용인됨
시스템 다운 타임	Unacceptable	용인됨
기술 / 인식	Poor (부족)	Good
시스템 수명주기	15 - 25 년	3 - 5 년
상호 운용성	Critical	Not critical
컴퓨팅 리소스	Limited	(거의) Unlimited
기준	IEC 62443	IEC 27000

CSMS 특징

CSMS의 7가지 (FR, Foundational Requirements) 기본 요구사항

- 식별 및 인증(IAC, Identification and Authentication Control),
- 사용 통제(UC, Use Control),
- 시스템 무결성(SI, System Integrity),
- 데이터 기밀성(DC, Data Confidentiality),
- 데이터 흐름 제한(RDF, Restricted Data Flow),
- 이벤트 적시 대응(TRE, Timely Response to Events),
- 자원 가용성(RA, Resource Availability)

FR에서 도출한 시스템 요구사항 적용 대상

- 소프트웨어 애플리케이션 요구사항 (SAR, Software Application Requirements)
- 임베디드 장치 요구사항 (EDR, Embedded Device Requirements)
- 호스트 장치 요구사항 (HDR, Host Device Requirements)
- 네트워크 장치 요구사항 (NDR, Network Device Requirements)

보안레벨

- 총 4가지 단계로 구성 (보안 등급은 0~4까지 해당되는 값을 가짐)
- 0은 보안 요구사항이 없음

제어시설을 위한 사이버보안 관리 시스템(CSMS) 체계 구축

1단계	기존 시스템 평가
2단계	정책 및 절차 문서화
3단계	직원 및 계약자 교육 & 훈련 프로그램
4단계	제어 시스템 네트워크 분할
5단계	시스템에 대한 액세스 제어
6단계	시스템 구성 요소 식별 및 강화
7단계	모니터링 및 시스템 보안 유지

산업자동화제어시설 사이버보안 관리 시스템(CSMS) 프레임 워크

위협 분석

시스템 위험 평가

- 위험 평가 방법론 선택
- 위험 평가 배경 정보 제공
- 높은 수준 위험 평가 수행
- IACS 식별
- 단순 네트워크 다이어그램 개발
- 시스템 우선순위화
- 상세 취약성 평가
- 상세 위험 평가 방법론 식별
- 상세 위험 평가 수행
- 재평가 빈도 및 유발 기준 파악
- 물리적, HSE 및 사이버 보안 위험 평가 결과
- IACS 생명 주기 전반에 걸친 위험 평가 수행
- 위험 평가 문서화
- 취약성 평가 기록 유지

CSMS 구축 (위험 해결)

보안 정책, 조직 및 인식

- CSMS 범위 정의
- 범위 컨텐츠 정의
- 고위 경영진 지원받기
- 보안 조직 수립
- 조직 책임 정의
- 이해 관계자 팀 구성 정의
- 교육 프로그램 개발
- 절차 및 설비 교육 제공
- 지원 인력 교육 제공
- 교육 프로그램 유효성 검증
- 시간 경과에 따른 훈련 프로그램 개정
- 직원 교육 기록 유지
- 복구 목적 명시
- 각 시스템에 미치는 영향 및 결과 결정
- 사업 연속성 계획 개발 및 구현
- 사업 연속성 팀 구성
- 구체적인 역할과 책임 정의 및 전달
- 사업 연속성 계획을 지원하는 백업 절차 생성
- 사업 연속성 계획 테스트 및 업데이트
- 보안 정책 개발
- 보안 절차 개발
- 위험 관리 시스템 간 일관성 유지
- 사이버 보안 정책 및 절차 준수 요구사항 정의
- 조직의 위험 허용 수준 결정
- 정책 및 절차를 조직에 알림
- 사이버 보안 정책 및 절차 검토 및 업데이트
- 사이버 보안에 대한 선임 리더십 지원

보안대책

인적보안

- 인적 보안 정책 수립
- 초기 인사 스크린
- 인사 스크린 지속
- 보안 책임 해결
- 보안 기대 및 책임 문서화하고 전달
- 명확한 사이버 보안 용어 및 고용 조건
- 적절한 체크와 균형 을 유지하기 위한 임무 분리

엑세스제어 권한부여

- 액세스 계정은 권한 보안 정책을 구현
- 개인 식별
- 계정 액세스 권한 부여
- 액세스 계정 기록
- 불필요한 계정 중지 또는 제거
- 계정 권한 검토
- 기본 암호 변경
- 계정 관리 감사

네트워크 세분화

- 네트워크 세분화 아키텍처 개발
- 고위험도 IACS에서 고립 또는 세분화 사용
- 배리어 장치와의 필수적이지 않은 통신 차단

물리적 환경적 보안

- 보완적인 물리적 및 사이버 보안 정책 수립
- 물리적 보안 경계 설정
- 진입 제어 제공
- 환경 피해로부터 자산보호
- 직원들에게 보안 절차준수 요구
- 연결 보호
- 장치 자산 유지 보수
- 모니터링 및 경보 절차 수립
- 자산의 추가, 제거 및 폐기 절차 수립
- 중요 자산의 임시 보호 절차 수립

엑세스제어 계정관리

- 액세스 계정은 권한 보안 정책을 구현
- 개인 식별
- 계정 액세스 권한 부여
- 액세스 계정 기록
- 불필요한 계정 중지 또는 제거
- 계정 권한 검토
- 기본 암호 변경
- 계정 관리 감사

엑세스제어 인증

- 액세스 계정은 권한 보안 정책을 구현
- 개인 식별
- 계정 액세스 권한 부여
- 액세스 계정 기록
- 불필요한 계정 중지 또는 제거
- 계정 권한 검토
- 기본 암호 변경
- 계정 관리 감사

사고 계획 및 대응

- 침해사고 대응 계획 수립
- 사고 대응 계획 전달
- 비정상적인 활동 및 사건에 대한보고 절차 수립
- 사이버 보안 사고보고에 대해 직원 교육
- 적시에 사이버 보안 사고보고
- Identify and respond to incidents
- 사고 식별 및 대응
- 사건 세부 사항 문서화
- 사건 세부 정보 전달
- 발견 된 문제 해결 및 수정
- 훈련 실시

구현

위험관리 및 구현

- 지속적인 IACS 위험 관리
- 공통된 대책 채택

시스템 개발 및 유지보수

- 보안 정책 개발
- 보안 절차 개발
- 위험 관리 시스템 간 일관성 유지
- 사이버 보안 정책 및 절차 준수 요구사항정의
- 조직의 위험 허용 수준 결정
- 정책 및 절차를 조직에 알림
- 사이버 보안 정책 및 절차 검토 및 업데이트
- 바이러스 백신/악성 프로그램 관리 절차 수립 및 문서화
- 백업 및 복원 절차 수립

정보 및 문서 관리

- 보안 정책 개발
- 보안 절차 개발
- 위험 관리 시스템 간 일관성 유지
- 사이버 보안 정책 및 절차 준수 요구사항 정의
- 조직의 위험 허용 수준 결정
- 정책 및 절차를 조직에 알림
- 사이버 보안 정책 및 절차 검토 및 업데이트

모니터링 및 개선

CSMS 모니터링 개선

적합성

- 감사 프로세스 방법론 명시
- 정기 IACS 감사 실시
- 적합성 측정 기준 수립
- 문서 감사 추적 설정
- 미준수에 대한 징계 조치 정의
- 감사원 역량 보장

CSMS 검토, 개선 및 유지보수

- CSMS에 대한 변경사항을 관리 및 구현할 조직지정
- 주기적으로 CSMS 평가
- CSMS 평가를 위한 트리거 설정
- 시정 조치 및 예방 조치 식별 및 시행
- 위험 허용도 검토
- 산업 CSMS 전략 모니터링 및 평가
- 사이버 보안과 관련된 관련 법규 모니터링 및 평가
- 보안 제안에 대한 직원 피드백 요청 및 보고

CLAROTY

ICS Vendors

ABB, AVEVA, ALSTOM, BECKHOFF, BELDEN, CIMON, COGNEX, GE, EMERSON, Honeywell, KONGSBERG, LS, MITSUBISHI ELECTRIC, OMRON, Rockwell Automation, SIEMENS, Schneider Electric, Valmet, XINJI, YOKOGAWA

ICS 보안 전문 기업 "클래로티 with 쿤텍"

COONTEC

CLAROTY

Detect in Depth and..

*Reference to ISA/IEC 62443. NIST, NERC CIP 등

- 영역 전체에서 예상되는 트래픽의 일부가 아닌 트래픽을 식별하도록 방화벽 및 IDS를 구성필요
- 비정상적인 데이터 전송 패턴
- 새로운, 허용되지 않은 프로토콜
- 시간별 데이터 트래픽
- 고스트자산 존재 혹은 외부 MAC 또는 IP 주소와의 통신
- 활동 모니터링을 위한 로그 증적
- SYSLOG를 중앙 로깅 서버로 전송
- 새 자산 감지
- 누락된 자산 감지
- Secure Remote Access
- 패치 관리 / 안티 바이러스 / DRP
- 인증/식별/암호화, 시스템 보안 완화 방안

보안의 기본은 “Root of Trust”

IACS 환경에서 인증 암호 체계 구현의 어려움

Q. 안전한 키 저장 공금을 위해 Hardware Secure Element를 고려해야 합니까?

A. 하드웨어는 적용은 매우 제한적입니다. 화이트박스 암호는 소프트웨어 라이브러리로 적용이 용이 합니다.

Q. 기존에 구축된 시스템에는 어떻게 Key storage를 제공 합니까?

A. WhiteBox 암호로 라이브러리 형태로 쉽게 업데이트 가능합니다.

Q. 제어분야에는 매우 다양한 제조사와 다양한 소프트웨어 가 있습니다. 모두 지원이 가능한가요?

A. ANSI-C 기준으로 제공되어 모든 ANSI-C 표준을 따르는 소프트웨어를 지원 합니다.

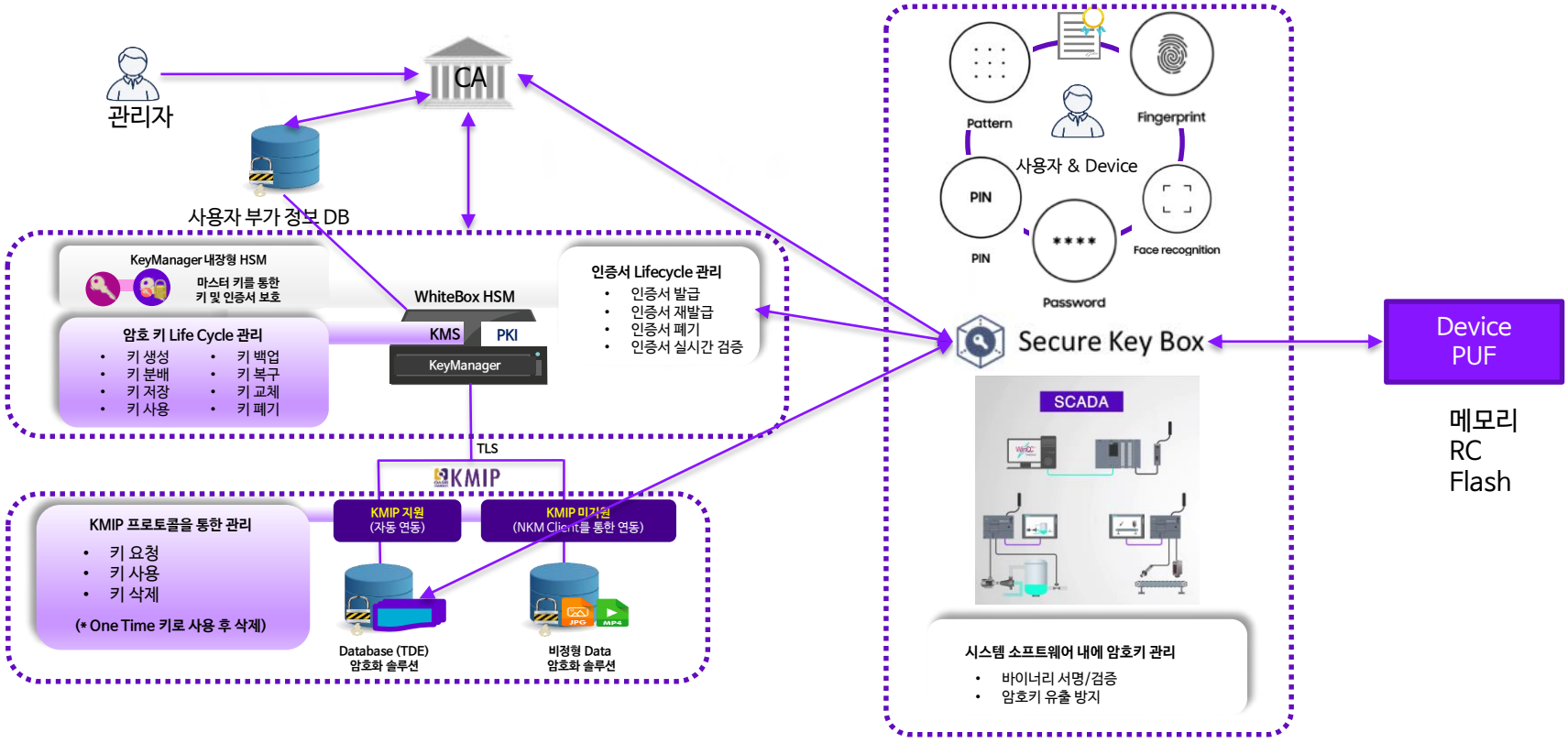
Q. 보안은 매우 중요하지만 모든 디바이스에 인증체계를 구현하면 많은 비용이 발생합니까?

A. 화이트박스 암호기반의 인증 체계는 소프트웨어로 비용에 매우 유리 합니다.

Q. 배포된 시스템의 안정성을 주기적으로 업데이트할 수 있습니까?

A. 네, 모든 것은 소프트웨어로 업데이트 가능합니다.

쿤텍 제어시스템 시큐리티 플랫폼



CSMS 환경에서의 Root of Trust 구현

쿤텍 제어시스템 시큐리티 플랫폼 (키매니저)

암호 키 **생성, 이용, 보관, 배포, 파기**에 대해 다음과 같은 항목이 포함된 **정책 및 절차를 수립하고 이행**하여야 한다.

1. 암호키 관리 담당자 지정

2. 암호키 생성, 보관 (소산 백업 등) 방법

3. 암호키 배포 대상자 정의 및 배포 방법 (복호화 권한 부여 포함)

4. 암호키 사용 유효기간 (변경 주기)

5. 복구 및 폐기 절차 및 방법 등

생성된 암호 키는 암호 키 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 **별도의 매체에 저장 후 안전한 장소에 보관 (소산 백업 포함)**

암호 키는 암호키를 이용하는 시스템에 저장할 수 있으나 **물리적으로 분리된 서버에 저장하는** 하는 것이 좋다.
- 암호 키는 하드코딩 방식으로 구현하면 안된다.

- 암호 키에 대한 **접근권한 부여는 최소화** 하여야 한다.

암호기술 구현시 **암호 키의 사용기간은 최대 2년, 유효기간은 최대 5년을 권고**

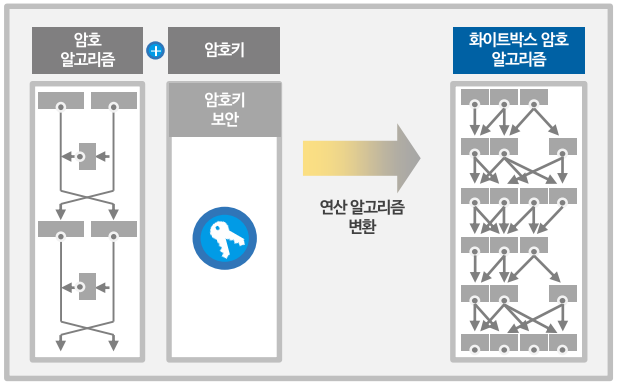
다만, **암호키 유출, 암호시스템 해킹이 의심되는 경우, 즉시 암호 키를 변경**하여야 한다.

KeyManager 로 모든 암호키 관리 요구 사항에 대한 대응 가능

쿤텍 ICS 시큐리티 플랫폼 (암호 보호, 화이트박스 암호)

WBC(White-Box Cryptography)

- 공격자가 접근 가능한 환경에서도 암호키에 대한 공격이 불가능한 암호 알고리즘
- 지속적인 암호 알고리즘 업데이트를 통해 보안성 강화 및 새로운 취약점에 대한 보완이 가능하여 **안전한 Time Resistance 확보**
- 물리적인 하드웨어 장치에 국한되지 않기 때문에 **암호 알고리즘과 암호 키 적용의 유연성을 보장**(HW의존성 탈피)



화이트박스 암호 기술

✓ 고급 수학 기술을 사용하여 비밀정보와 키를 보호

✓ 다양한 보안 기술 적용

- 디바이스바인딩, 일방향 함수 사용, 셔플, 마스킹, 인플리먼테이션, 랜덤 바이젝션 등

✓ 레드팀의 지속적인 보안 검증 필요(오픈소스 사례)

✓ 적용 시 안정적인 서비스를 보장하는 성능 확보 필요

최고 수준의 보안과 검증된 레퍼런스

쿤텍 ICS 시큐리티 플랫폼 (암호 보호, 화이트박스 암호)

화이트박스 암호로 세계 최고 수준의 안정성 입증

- 부채널 및 DBI 등 암호 공격 내성 평가 공개

키 관리

키 추가	• SKB 라이브러리나 KeyExportTool에서 Export 된 키를 추가 • SKB 내에서만 사용할 수 있는 키 생성 지원 • 키 교환 알고리즘을 통한 키 전달 • Wrapped (암호화) 된 키를 Unwrapping으로 추가
키 저장	• SKB에서만 지원하는 Export 방식으로 키 저장 • 다른 키를 이용하여 암호화하는 Wrapping 으로 키 저장 • 다른 시스템과 연동을 위해서는 Export가 아닌 Wrapping으로 저장하는 것을 추천

암호화 기술을 활용한 전자서명, 키 교환

전자서명

AES-CMAC (128, 192, 256 bit), Speck-CMAC (128, 64 bit),
RSA (1024, 2048 bit), ECC, HMAC, 3DES

전자서명 인증

AES-CMAC (128, 192, 256 bit), Speck-CMAC (128, 64 bit), HMAC, 3DES

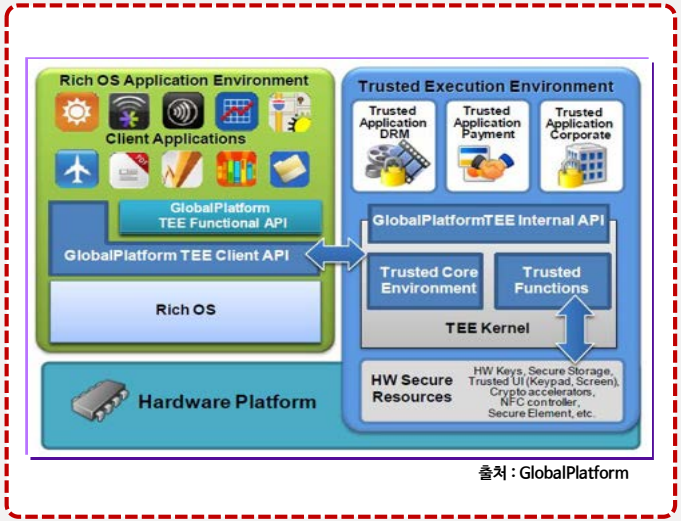
키 교환

Classical Diffie-Hellman, Elliptic curve Diffie-Hellman, Montgomery-X-coordinate DH

지원 가능한 해시 알고리즘	
MD5	SHA-256
SHA-1	SHA-384
SHA-224	SHA-512

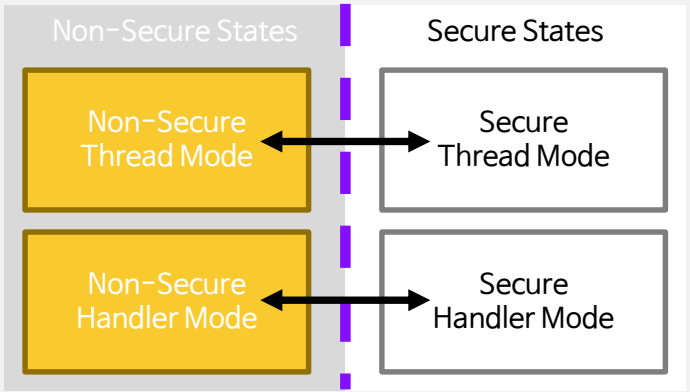
쿤텍 ICS 시큐리티 플랫폼 (HW 보안 TEE 기술)

- ARM社가 디바이스 보안을 보다 효율적이고 강화하기 위해 모바일 AP칩 내에 설계한 하드웨어 기술
- TrustZone 하드웨어와 TEE(보안 OS) 소프트웨어로 구성 → H/W와 S/W가 결합된 보안 기술



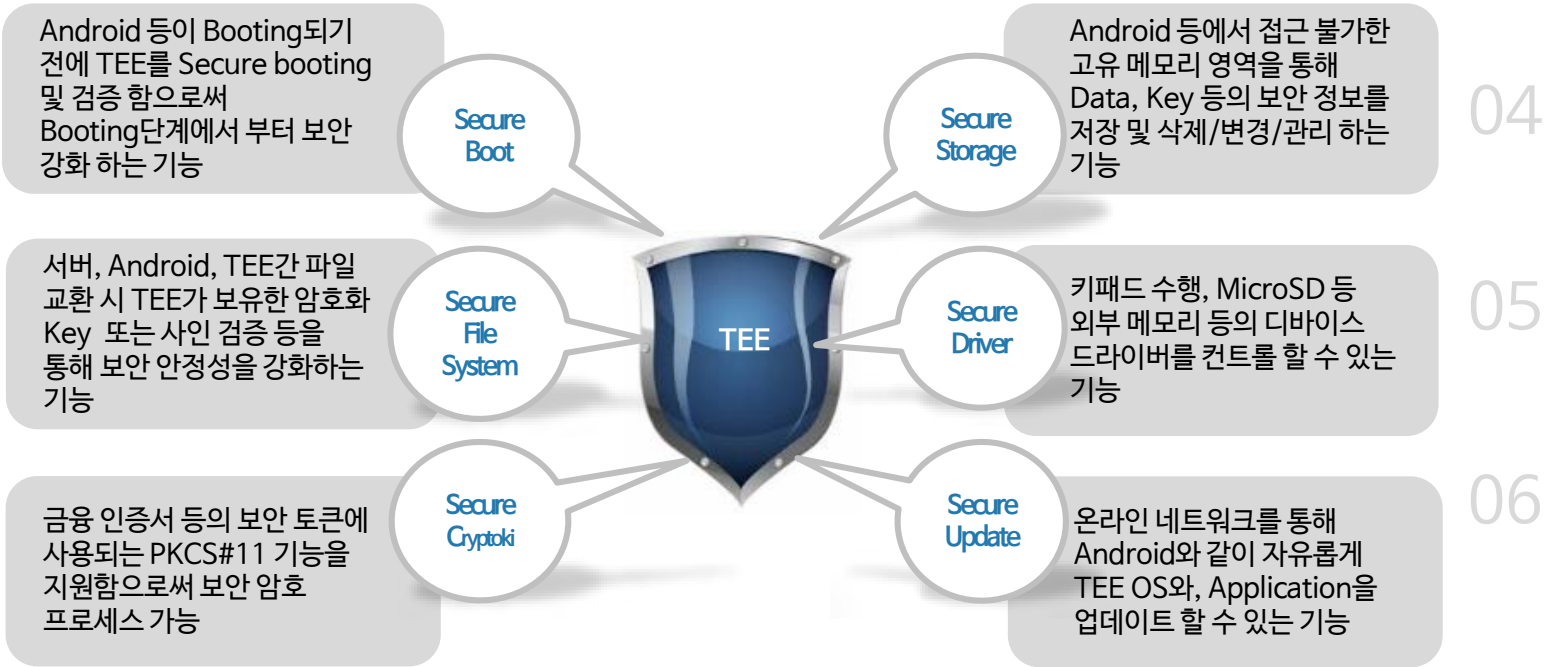
출처 : GlobalPlatform

[모바일 환경 TEE]



[IIoT 환경 TEE]

쿤텍 ICS 시큐리티 플랫폼 (HW 보안 TEE 기술)



쿤텍 & Claroty OT 보안 솔루션 & 서비스

쿤텍 솔루션 & 서비스	Asset Owner	System Integrator	Product Supplier
Claroty 통합 OT 보안 관제	○		
OT Security Platform (Key Manager, WBC)		○	
OT Security Platform (PUF, WBC)			○
OT 보안 교육 & 컨설팅	○	○	○

쿤텍 & 클래로티 OT 보안 솔루션 & 서비스

IEC 62443 전문 교육

4차 산업혁명으로 산업제어시스템(ICS, Industrial Control System)의 운영 환경에도 많은 변화가 생겼습니다. 산업제어시스템에 IT 기술이 도입되면서 스마트 팩토리, IIoT(Industrial Internet of Things)의 발전이 확대되고 있으며, 이에 따라 산업제어시스템을 대상으로 하는 사이버 보안 위협 역시 지속적으로 증가하고 있습니다.

융합 보안 전문 기업 **쿤텍**과 인증 서비스 시험인증기관 **TÜV-SÜD**는 산업제어시스템의 보안 역량 강화를 위하여 **'국제 산업제어시설 사이버 보안 표준 IEC 62443 전문가 과정'** 교육을 제공합니다.

본 교육은 국제 표준 위원회 참여를 통해 ICS 보안 동향에 대한 심도 깊은 이해도를 갖춘 전문 인력을 통해 진행되며, 산업용 사이버 보안과 IT 보안의 차이점, IEC 62443의 개념, IEC 62443의 적용 사례를 소개하고 산업제어망 사이버 보안의 개념과 산업제어망 침해사고 대응 방안을 제시합니다.

쿤텍 & 클래로티 OT 보안 솔루션 & 서비스

IEC 62443 전문 교육

교육내용

1. Overview of industrial cybersecurity
2. Introduction to IEC 62443
3. IEC 62443-4-1, IEC 62443-4-2
4. IEC 62443-2-3, IEC 62443-2-4
5. IEC 62443 Certification
6. Contd. IEC 62443-2-4
7. IEC 62443-3-2, IEC 62443-3-3
8. IEC 63069- Framework for functional safety and security
9. IEC 표준 모델 기반의 OT네트워크 보안 관제 및 침해대응 소개
10. 침해사고 발생 시 대응 절차
11. 사이버 보안 위협 기반 침해사고 대응 훈련 실습
12. 보안 위협 대응 완료 후 분석 교육 및 실습

4. 클래로티·쿤텍 OT보안솔루션 도입 사례 소개

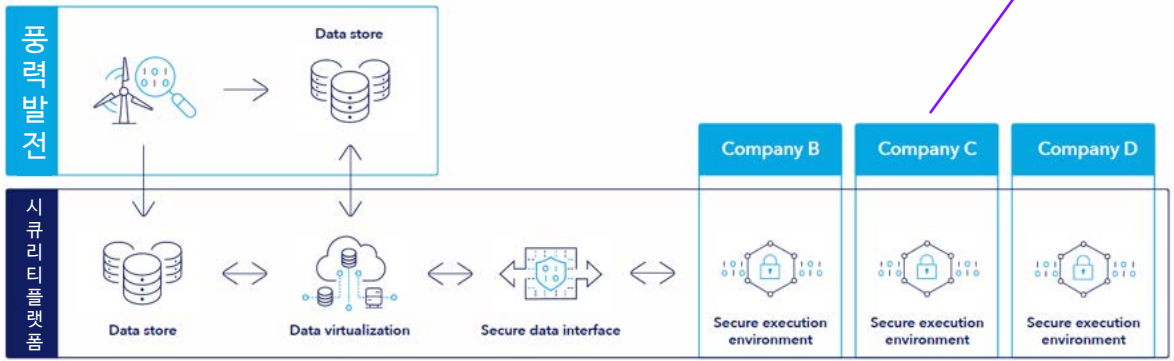
Bridging the IT-OT Cybersecurity Gap

쿤텍 OT 시큐리티 플랫폼 적용 사례

독일 해양 재생에너지 (RWE offshore renewables) 사례

- 해양 풍력 시스템은 다양하고 풍력이 있는 곳에 단지를 조성
- 지리적으로 매우 넓은 단위이며 이를 극복하여 운영의 효율성 및 성능을 개선 필요

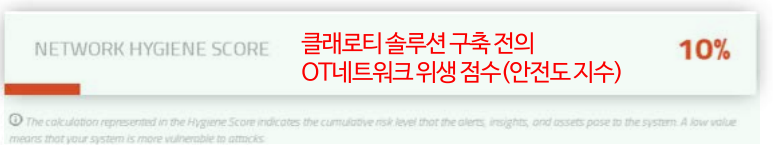
- 모든 데이터 시스템을 통합하여 데이터 소스를 하나로 공급 안전한 환경 구현
- 운영자를 위한 실시간 분석 의사 결정 시스템 제공
- 제 3 자와 함께 작업하기 위해 데이터 권한을 관리하는 기능 구현

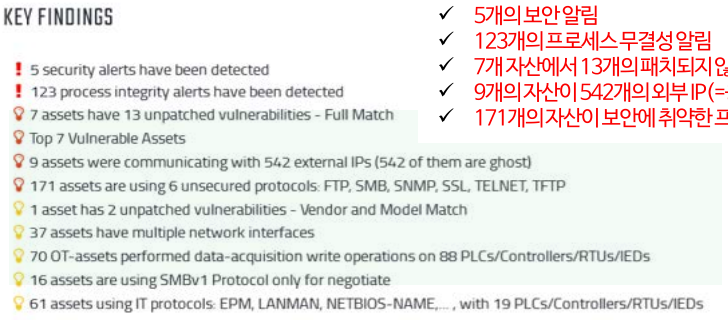


국내 A제조기업 클래로티 도입 이유

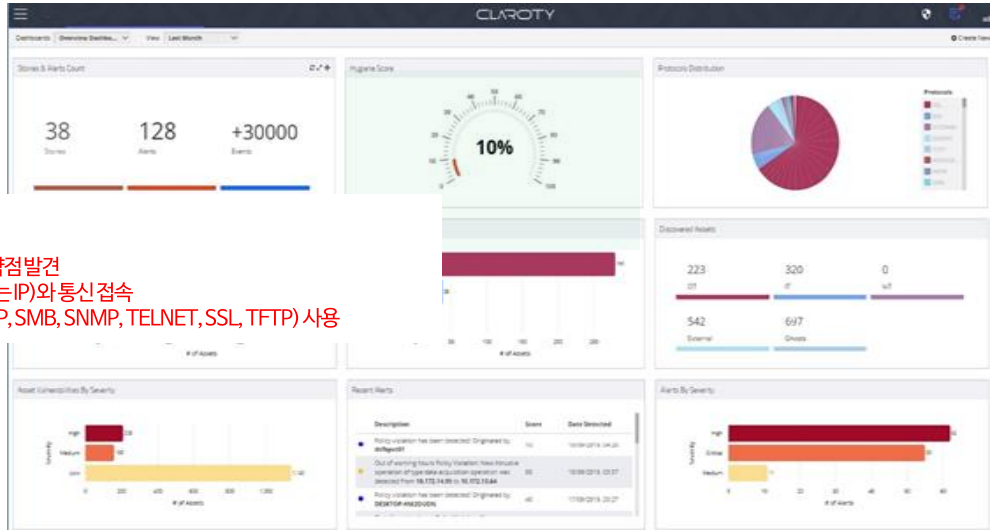
국내외 다양한 산업군 대상 ICS보안취약점 진단·컨설팅·솔루션 구축 경험을 바탕으로 한 성공적인 사업 수행 역량 보유

[국내 고객사 OO공장 – ICS보안취약점 진단/ OT보안컨설팅/구축 사례]





- ✓ 5개의 보안 알림
- ✓ 123개의 프로세스 무결성 알림
- ✓ 7개 자산에서 13개의 패치되지 않은 보안취약점 발견
- ✓ 9개의 자산이 542개의 외부 IP(=응답되지않는 IP)와 통신 접속
- ✓ 171개의 자산이 보안에 취약한 프로토콜(FTP, SMB, SNMP, TELNET, SSL, TFTP) 사용



제시된 개선 방향 (OT보안성숙도 단계 : "초기 단계" 에서 → "지속적으로 탐지/관리되는 단계" 로 개선 목표)

OT자산가시성 확보 및 OT보안솔루션 구축

- 보안경고 알림 가능 및 외부 IP 접속여부 탐지
- Unpatched 및 보안되지 않는 프로토콜 취약점 탐지
- OT Network Segmentation 정보 제공

OT 작업 행위에 대한 모니터링 및 변경관리

- OT 프로세스 수정 및 변경시 무결성 관리
- OT 운용환경의 비정상 행위 및 이상징후 지속 모니터링
- 보안사고 발생시 원인분석을 위한 OT보안솔루션 구축

OT운영 고도화 및 자동 진단을 통한 컴플라이언스 강화

- 실시간 OT 자산정보 관리, 사고 대응 및 복원시간 단축
- OT 인프라 위험요소 인지 및 OT 통신플로우/이벤트 상관분석
- OT 영역 보안평가를 위한 컴플라이언스 준수

국내 A제조기업 클래로티 도입 이유

OT보안가시성 솔루션 도입 및 ICS 이상징후 모니터링 체계 구축 후의 개선효과

OT보안가시성 솔루션 구축 전

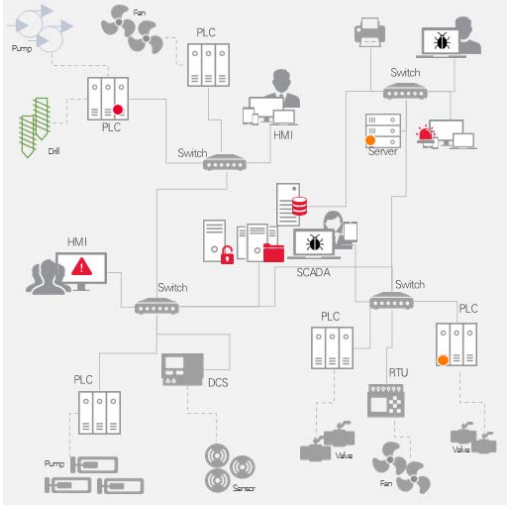
- ✓ ICS/OT/IoT 관련 제조사 프로토콜들에 대한 이해 부족
- ✓ 가시성이 결여된 상황에서 네트워크를 보호 및 보안사고에 즉각적인 대처 불가능
- ✓ 해당 환경의 실시간 보안/운영 가시성 결여로 복원력 상실

** OT 환경에 대한 완벽한 가시성 확보가 최우선 과제 **

OT보안가시성 솔루션 구축 후

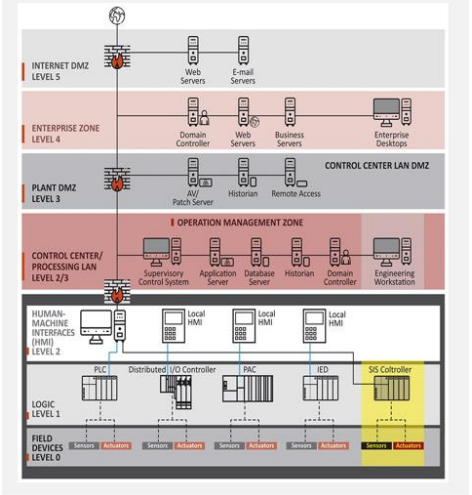
- ✓ 자동화 제어 시스템과 운영(OT) 네트워크의 가시성 확보로 안전성 및 신뢰성 향상
- ✓ OT사이버보안을 위해 퍼듀(Purdue) 모델 기반으로 OT보안 관리 및 ICS 이상징후 탐지/모니터링/대응
- ✓ OT네트워크 환경에 대한 사이버보안 강화 방안 제시로 보안규제 요구사항 준수 효과

As-Is (보안이 내재되어 있지 않은 OT네트워크 관리)



인벤토리 관리가 효율적으로 되지않고 있는 공장내의 OT자산/컨트롤러 등을 퍼듀 모델(Purdue Model) 기반으로 가시화하고 ICS 네트워크 토폴로지를 시각화하여 관리 가능토록 모니터링 방법론을 제시

To-Be (퍼듀 모델 기반 도식화 관리 가능)



IT+OT 융합 보안의 가까운 미래…

IT와 OT, 2년 이내에 완전 융합되어 전혀 새로운 세계가 도래할 것!

(하노버산업박람회 2019 기자회견 : 지멘스 스마트팩토리 오토메이션 BU CEO 랄프마이크 프란케 氏)

THANK YOU