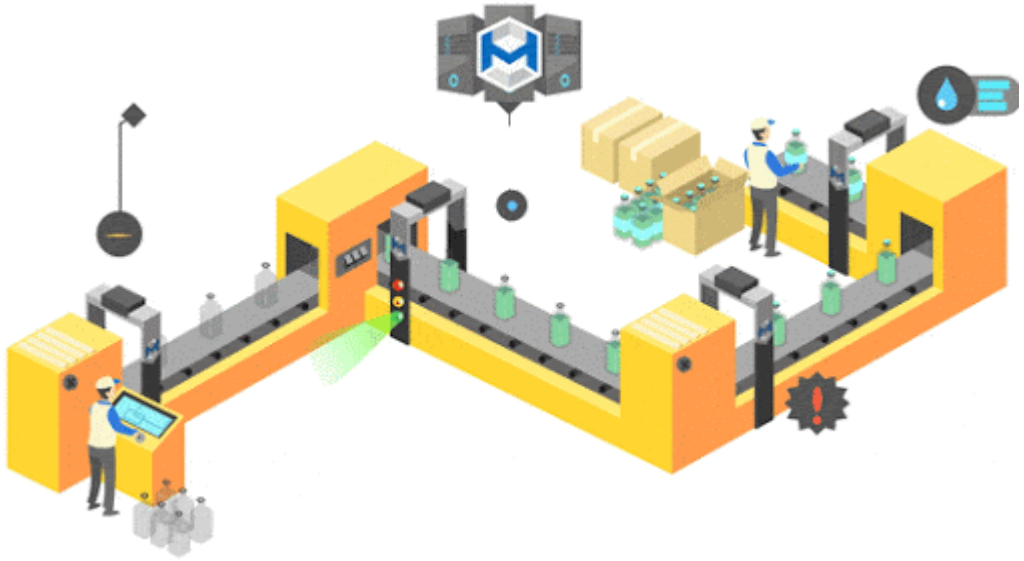
SK infosec

OT/ICS 기술동향 및 보안강화 방안

Industry 사업그룹 그룹장 문병기



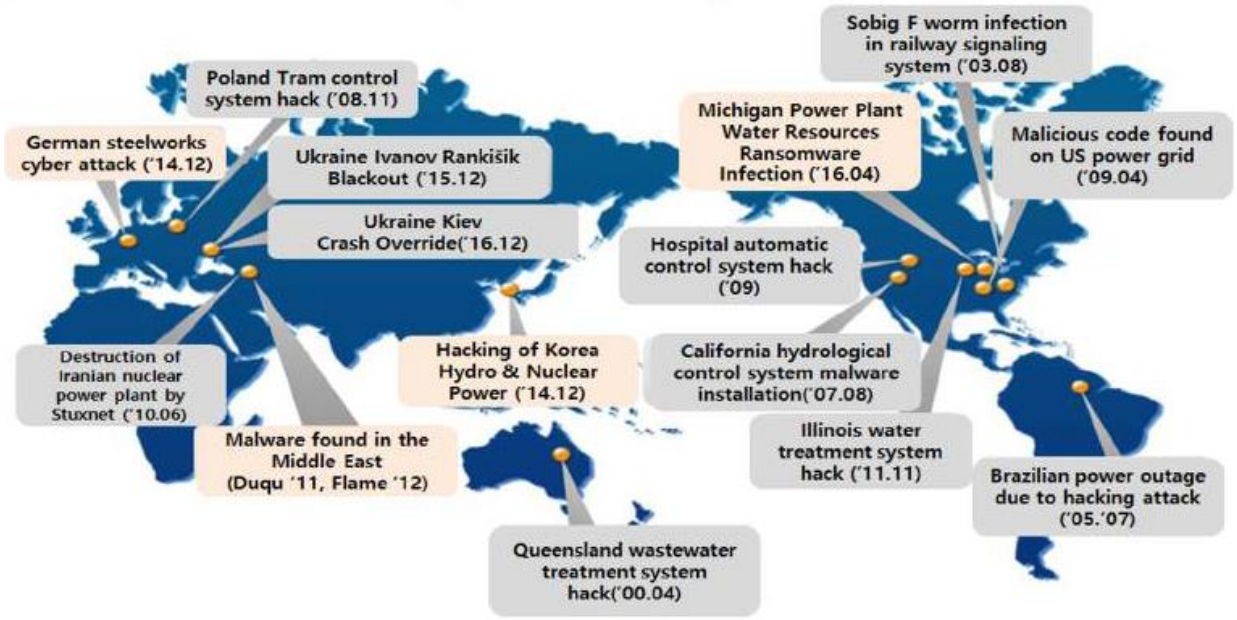
목차

Chapter 1
OT/ICS 최신 위협 동향

OT/ICS 보안 침해 사례

폐쇄 망으로 안전하다고 여겨진 OT/ICS의 보안사고가 지속적으로 발생하고 있음

OT/ICS 보안 침해 사례



(출처 : 포스코 ICT)

주요 침해 사례

2010

StuxNet(이란 핵 프로그램 중단)

우크라이나 전력망 공격

2015

2018

대만 TSMC 랜섬웨어 감염

Norsk Hydro 랜섬웨어 감염

2019

(출처 : Fortinet Security)

OT/ICS 보안 침해 사례

순번	시기	발생국	피해내용	비고
1	2010년	이란	스턱스넷 바이러스 원자력 발전소 제어시스템 침투, 1000여대 원심 분리기 파괴	
2	2011년	미국	일리노이 주 상수도 시설 시스템 침투, 펌프 작동 시스템 파괴	
3	2012년	미국	전력시설 터빈 제어시스템 악성코드 감염, 3주간 운영 중단	
4	2014년	독일	독일 청강회사의 용광로 제어시스템 장애 발생	
5	2015년	우크라이나	전력 발전소 내 악성코드 감염, 정전 발생(블랙에너지, 크래시 오버라이드 공격)	
6	2016년	미국	수처리 회사의 PLC를 임의 조작하여 화학물질 양을 조작	
7	2016년	독일	원자력 발전소 원료 적재 시스템 원격 조작을 통한 발전 중단	
8	2017년	우크라이나	낫페트야 랜섬웨어 활용 사회 기반 시설 대규모 공격	
9	2017년	미국	달라스 비상사이렌 제어시스템 해킹, 15시간 동안 비정상 가동 유발	
10	2017년	일본	혼다 모터스 사야마 공장, 워너크라이 랜섬웨어 감염으로 생산라인 정지	
11	2018년	대만	반도체 기업 TSMC 랜섬웨어 감염, 생산라인 일부 정지	
12	2019년	노르웨이	알루미늄 생산기업 노르스크 하이드로 랜섬웨어(록커고가) 감염, 생산중단	
13	2019년	베네수엘라	수력발전소 설비 고장으로 19개 주 전력 공급 차단	

(출처 : 포스코 ICT)

OT/ICS 보안 동향

35배

제조산업이 다른 분야에 비해 몸값을 지불할 가능성

22.3%

2019년 전체 사이버 공격 중 제조산업이 차지하는 비율 (전체 4위)

$22,000

생산라인 중단 시 시간당 평균 손실액 (2016년 예측)

13.9%

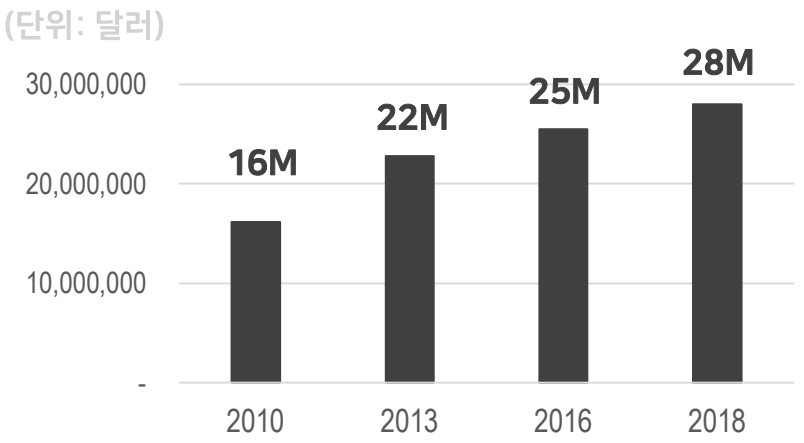
2019년 전체 랜섬웨어 공격 중 제조산업이 차지하는 비율 (전체 2위)

(출처 : Ponemon, Safety detectives)

OT/ICS 보안사고 특징

OT/ICS 분야에서 실제 보안 사고 발생 시, 전문기관 예측값보다 약 9배 큰 피해를 보임

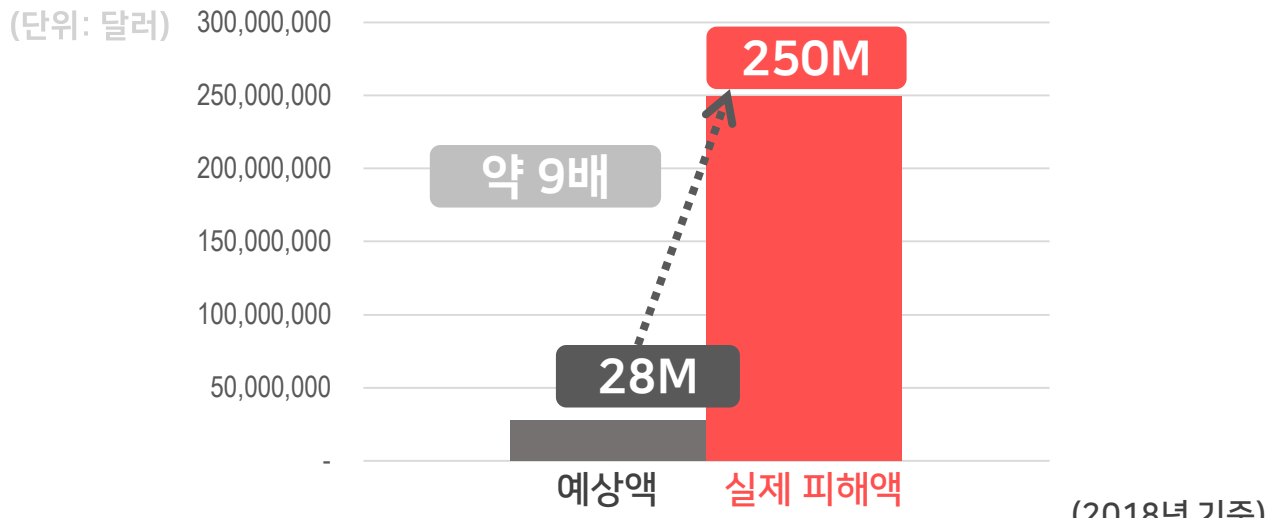
OT/ICS 보안 사고 1건 피해 예상액



OT/ICS 보안 사고 1건 피해 실제금액

2018년 대만 T반도체 랜섬웨어 사건 실제 피해액

$ 250,000,000 (250M)



(2018년 기준)

(출처 : Ponemon, 2016 Cost of data center outages)

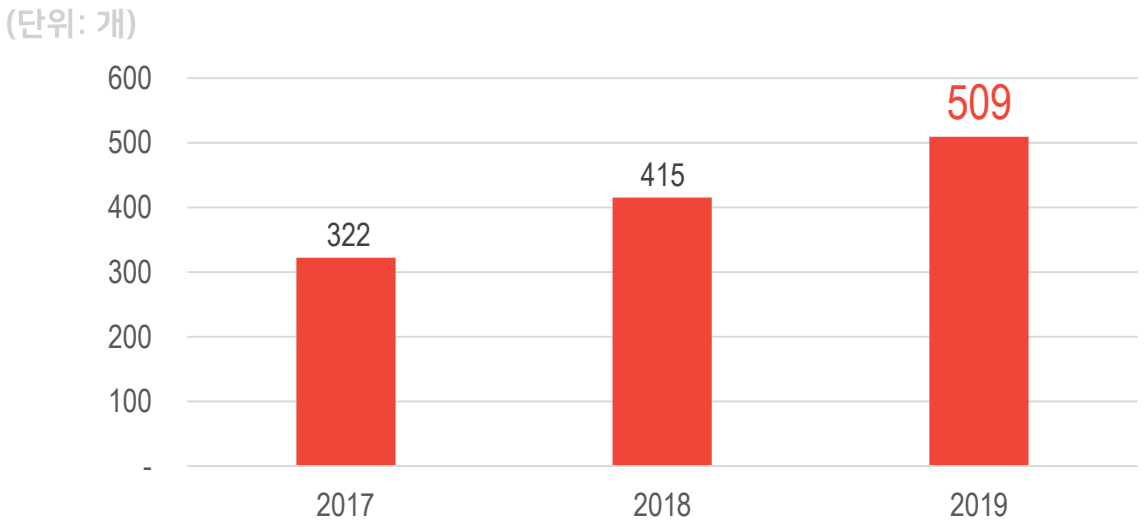
OT/ICS 보안사고 특징

OT/ICS는 높은 가용성을 요구하는 분야이므로 취약점에 즉시 대응이 어렵다는 특징이 있음

OT/ICS 보안 취약점 동향

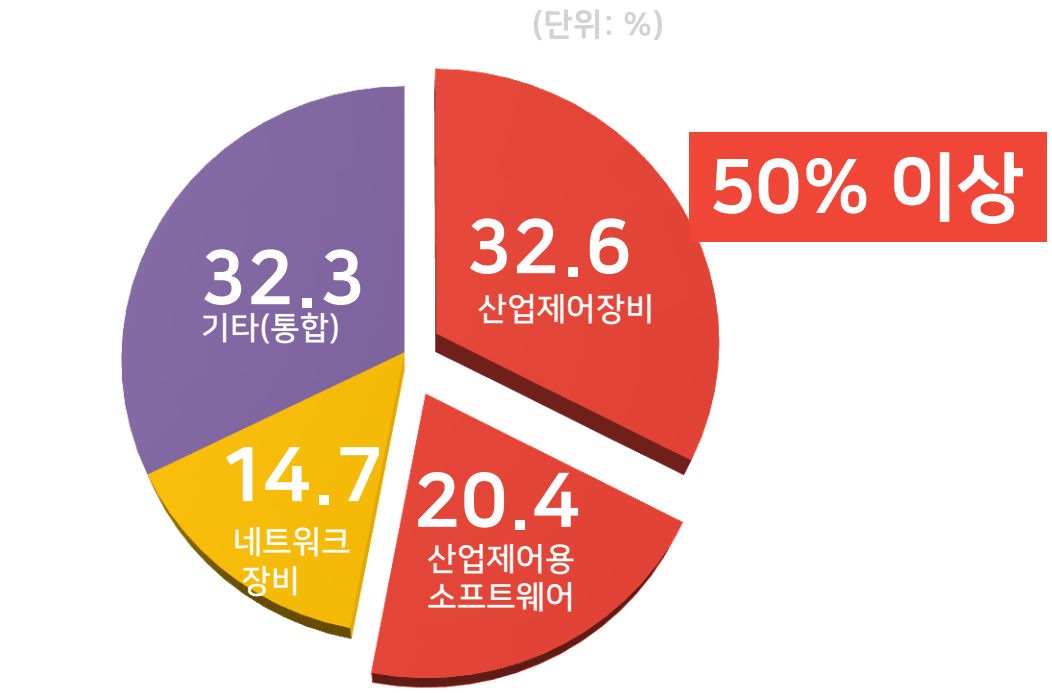
OT/ICS에서 발표된 취약점의 수

매년, 작년 대비 1.2배 이상의 신규 취약점이 OT/ICS 분야에서 나타나고 있음



(출처 : Kaspersky ICS CERT)

OT/ICS 보안 취약점 표적



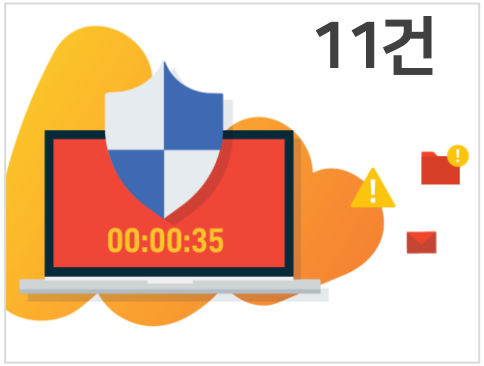
(출처 : Kaspersky ICS CERT)

OT/ICS 보안 위협 예측

IT 취약점을 이용한 OT 제어 시스템 정교화 공격 증가 예상

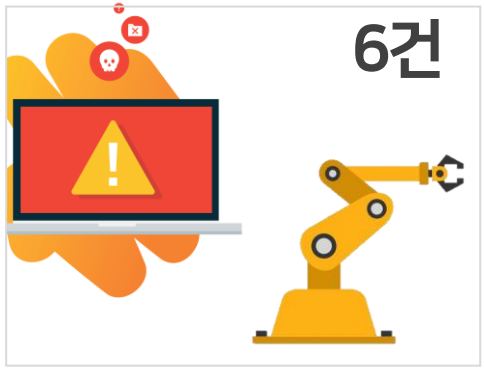
OT/ICS 보안 취약점 동향

랜섬웨어 및 악성코드



OS 및 응용 소프트웨어 취약점을 이용한 공격

ICS 시스템 전문화 공격



PLC, 제어시스템 공격 5건, 제어 시스템 안전 계측 1건

(출처 : MITRE ATT&CK 20.09 기준)

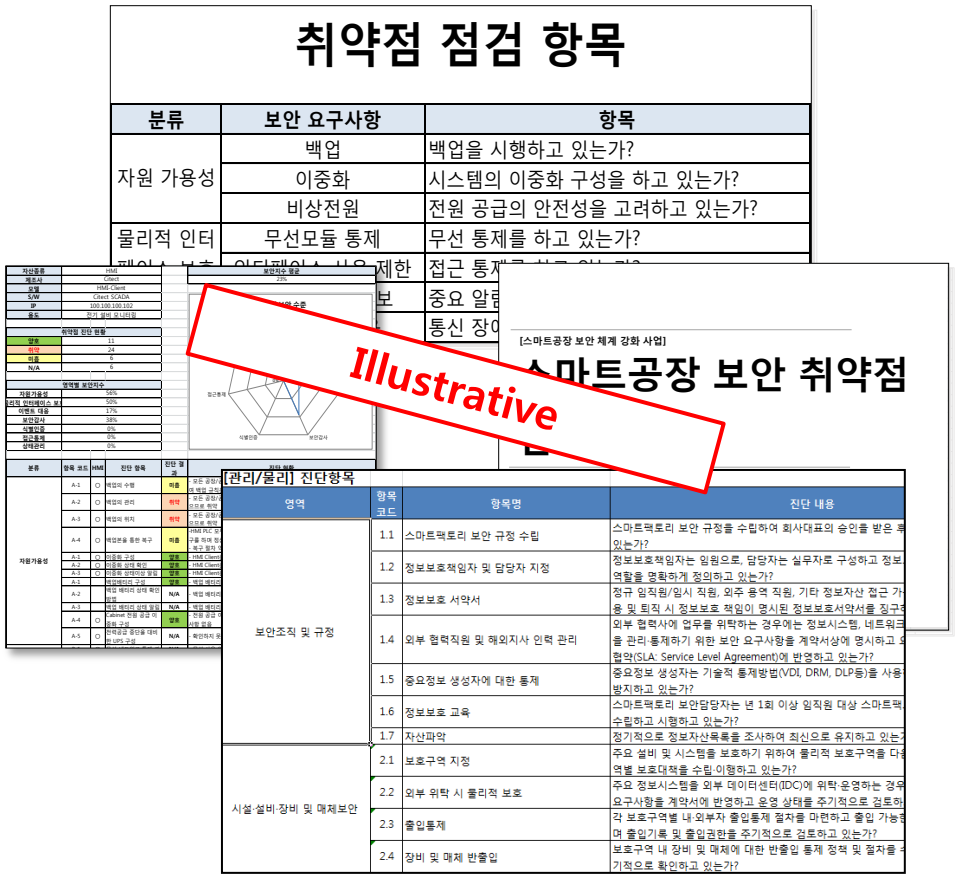
Chapter 2

고객사의 OT/ICS 보안 위협

OT보안자산 점검사례

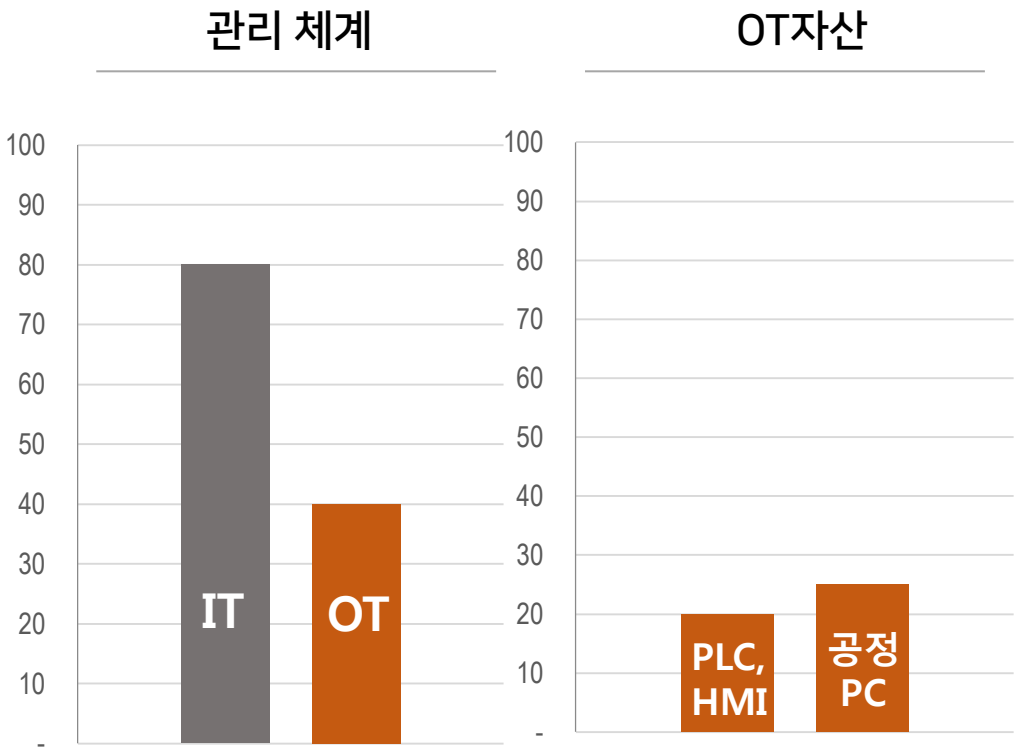
인포섹 OT자산 점검 체크리스트 및 가이드

- OT/ICS 취약점 점검 시 체크리스트 및 보안가이드 활용



OT보안 점검사례

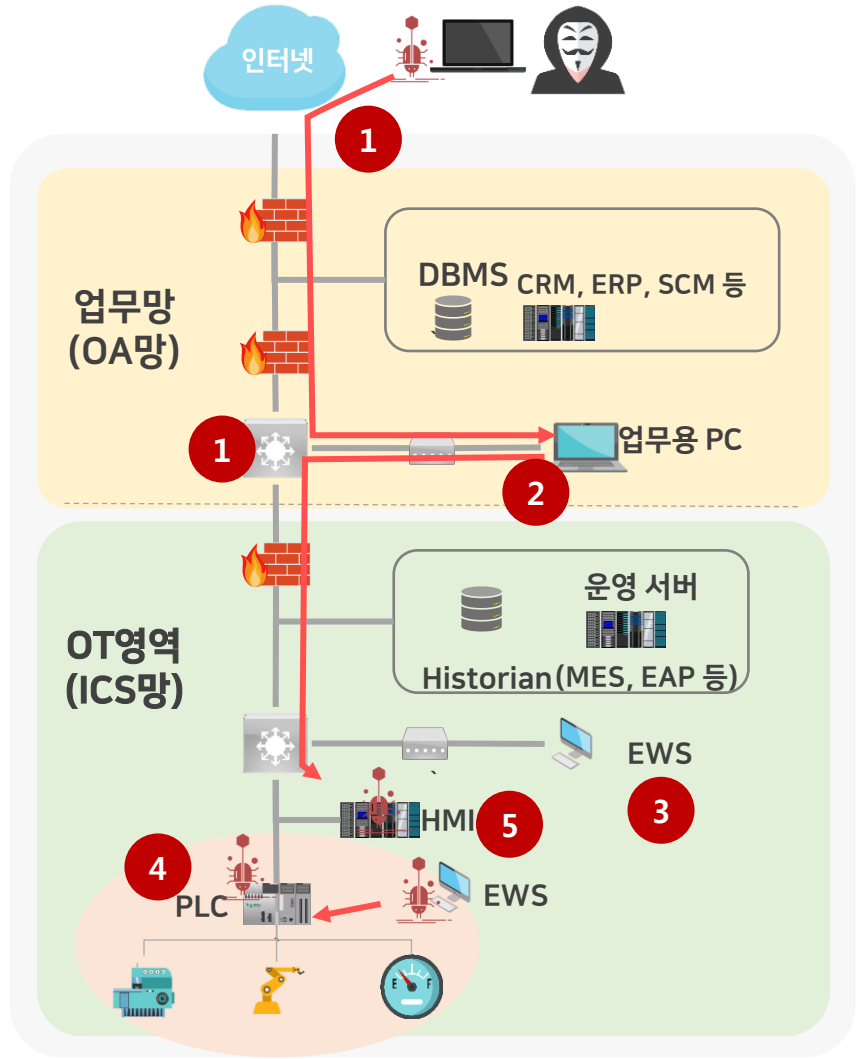
기존 IT보안 점검 점수 대비
2배 이상 낮은 OT보안 점수 확인



<대외중견 제조업체 평균>

사고사례 기반의 OT/ICS 보안 위협

OT/ICS 네트워크 구성도



OT/ICS 보안 위협

1 **네트워크 기반 악성코드 감염**

- IT / OT 망 접점
  - OA망을 통한 OT 장비 대상의 악성 코드 감염 및 전파

2 **OT 장비의 원격 조작 및 데이터 유출**

- OT 장비 유지 보수 및 관리
  - 관리 및 유지 보수 편리성을 위한 원격 조작 권한 위협

3 **내부자의 악의적인 행위**

- 악의 적인 행위 및 실수
  - 내부 운영 중요 데이터 유출 및 조작 실수

4 **OT 장비 및 소프트웨어 취약점**

- OT 장비 및 소프트웨어 취약점
  - 장비 및 소프트웨어 취약점 패치의 어려움으로 인한 악성 코드 공격

5 **OT 생산 장비 취약점**

- 노후 OS 취약점
  - OT 생산 장비의 노후 OS 사용에 따른 취약점 보유

OT/ICS 보안 위협 원인

OT 보안조직 부재

- 공장보안Ownership부재→ 공장보안사각지대

1

OT 보안기준 부재

- 공장보안적용을위한보안가이드부족

2

OT/ICS
보안 위협 원인

OT 자산관리 미흡

- 혼재된자산으로인한가시화미흡

3

보안이 고려되지 않은 네트워크 구성

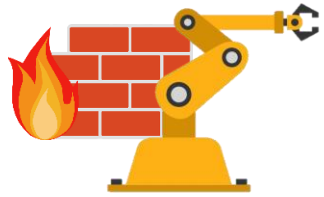
- 보안을고려하지않고시스템도입,네트워크구축

4

대응방안

전문 보안조직 구성
People

특화된 보안기준 수립
Process



전문 보안기술 확보
Technology

OT/ICS 보안 위협 대응

OT 사이버 보안 사고시 대응체계?

- OT 사고 대응 절차를 수립하여 가지고 있는가?
- OT 사고 조사 인력을 보유하고 있는가?
- 사고의 발생 원인을 분석하여 찾았는가?
- 발생 원인에 대한 조치 방안을 수립하였는가?
- 조치 내역을 확인하고 이력 관리를 별도로 하였는가?
- 재발 방지 대책을 수립하였는가?
- 위협 동향 분석 및 사전 보안 검토를 수행하고 있는가?

Case1 O

장비 장애 대응 매뉴얼 보유

생산에 따른 장비 장비 장애 발생 대응 매뉴얼 보유

장비의 유지 보수 관리 차원

Case2 X

사이버 장애 대응 매뉴얼 부재

IT 전산 시스템에 대한 사이버 보안 사고 매뉴얼 보유

OT 장비 시스템에 대한 전산 장애 대응 미흡

Case3 X

OT 보안 기준 및 가이드 부재

OT 취약점에 대한 내부 보안 기준 및 가이드 부재

생산 우선으로 인해 보안 의식 미흡으로 취약점 대응 미흡

People

- CISO 선임 및 역할통합 (IT-OT-물리)
- OT보안 전문 진단 및 대응 인력 확보

Process

- OT보안사고 대응체계
- OT장비 보안점검 체계(예방차원)

Technology

- OT장비 내 보안 기능 활성화
- OT보안 영역별 솔루션 도입 및 운영

OT/ICS 보안 위협 대응

내부자 악성 행위 및 실수 통제?

- OT 운영에 대한 변경에 대하여 경고를 제공하는가?
- OT 운영의 변경 내역을 로그로 남기고 해당 내용에 대하여 모니터링 하는가?
- OT 장비의 임계 값을 설정하여 통제하고 있는가?
- OT 장비에 대한 접근 및 변경에 대하여 모니터링 하고 있는가?

OT 장비 및 소프트웨어 취약점 대응?

- OT 장비 취약점 보고에 대하여 모니터링 하고 있는가?
- OT 장비의 취약점에 대하여 주기적 패치 계획 및 실행을 하는가?
- OT 소프트웨어 취약점 패치 계획 수립 및 실행을 하는가?

Case1 (O)

모니터링 및 장비 임계 값

- HMI를 통한 상태 모니터링 및 장비 내 임계 값 설정
- OT 장비 이벤트 모니터링 수행

Case2 (X)

보안 이벤트 모니터링

- 다양한 산업 프로토콜에 대한 네트워크 패킷 모니터링 방안 필요
- 이상 패킷 및 OT 운영 변경 프로젝트 파일 모니터링 방안 필요

Case3 (X)

OT 장비 패치 및 유지 보수

- OT 장비에 대한 취약점에 대하여 모니터링 및 대응 방안 수립 필요
- OT 장비 패치 어려움에 따른 대응 솔루션 검토 및 구축 필요

People

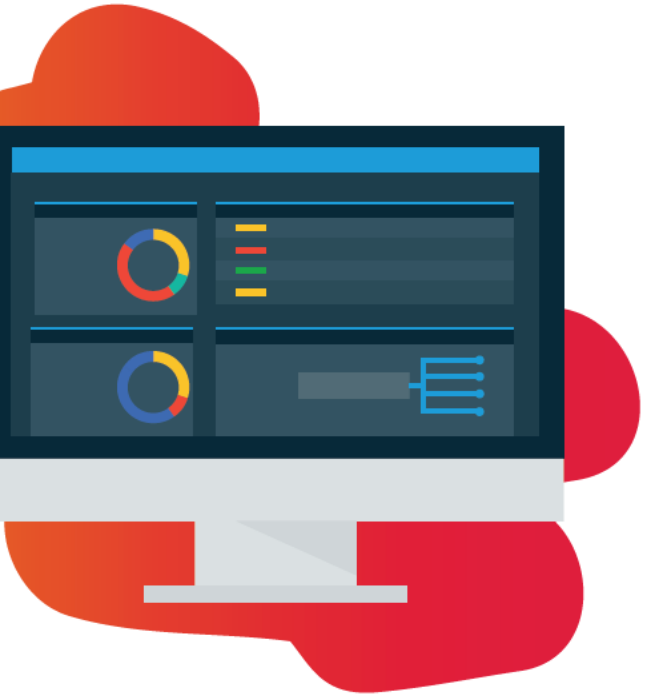
- OT보안조직 R&R 및 업무 프로세스 수립
- OT방역 전문 대응 조직 확보

Process

- OT장비의 통합이벤트 로그 수집/분석
- OT장비 패치/유지보수 보안관리체계

Technology

- OT 네트워크 가시성 확보(산업용 프로토콜)
- OT 장비 단종OS 대응방안 및 솔루션
- OT자산 통합관리 체계(방역 포탈)



Chapter 3
OT/ICS 심층보안 전략

OT/ICS 심층 보안전략

일차원적인 단일 보안 서비스가 아닌 다각도의 심층 보안전략 수립

SK 인포섹 OT/ICS 심층 보안전략

OT 보안 거버넌스 (OT RISK 분석 컨설팅)

- 관리적 보안으로 OT 보안 조직 및 정책을 수립
- OT의 보안 프로세스 및 점검 기준 확보
- OT 망 내 RISK 분석 및 진단

OT 물리보안

- 출입 및 OT 구역 접근 권한 관리
- OT 구역에 반/출입 전산 기기 관리 필요

기술적 보안

OT 네트워크

- OT 네트워크에 대한 견고성 확보를 위한 전략 수립 필요
- 다양한 산업용 프로토콜 분석 필요

OT 장비

- 다양한 제조사 별 장비 보안 정책 수립 필요
- 악성 코드 및 침해 사고에 대한 대응 방안 수립 필요

RISK 도출/분석

대응방안& 대응 시나리오 설계/구축

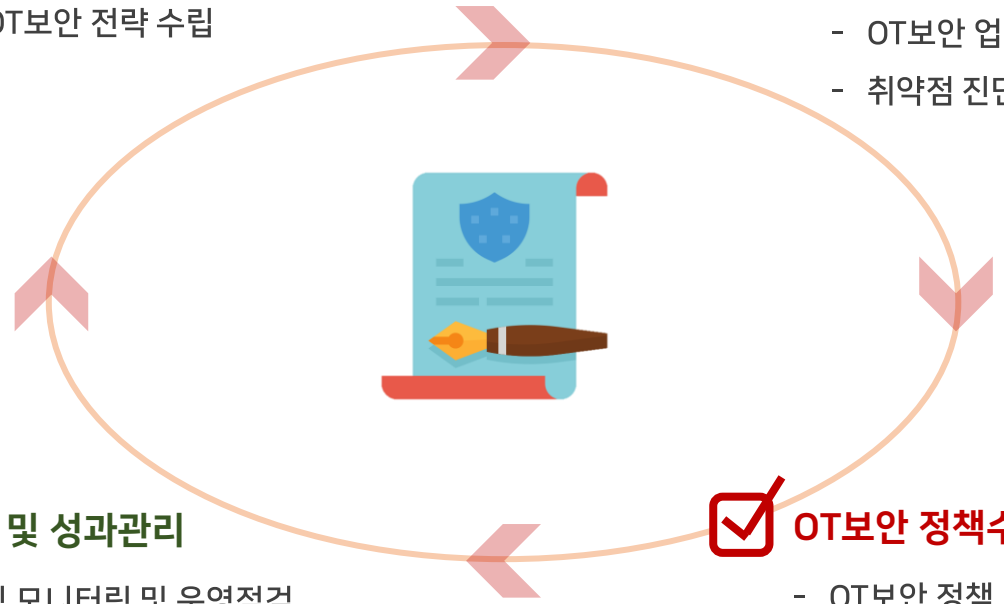
통합 모니터링 체계 수립

OT 보안 거버넌스 수립

컨설팅 수행을 통해서 OT 보안의 R&R을 수립하여 OT 보호 대상 및 보안 운영 방향 제시

OT기획 및 조직구성
- OT보안 전문인력 구성
- OT보안 전략 수립

OT/ICS 위험관리
- OT자산 관리범위 설정
- OT보안 업무/RISK 분석
- 취약점 진단 및 모의해킹



구현 및 성과관리
- 조직 모니터링 및 운영점검
- OT보안 아키텍처 구현
- OT보안설정 이행점검

OT보안 정책수립
- OT보안 정책 및 지침 수립
- OT보안 점검가이드라인
- OT보안 로드맵 수립

OT 거버넌스 수립 전

1	OT 보안 방안(대상 및 정책) 및 Ownership 부재
2	OT 사이버 보안 사고 시 대응 방안 부재
3	OT 보안 수행 및 관리 방안 부재

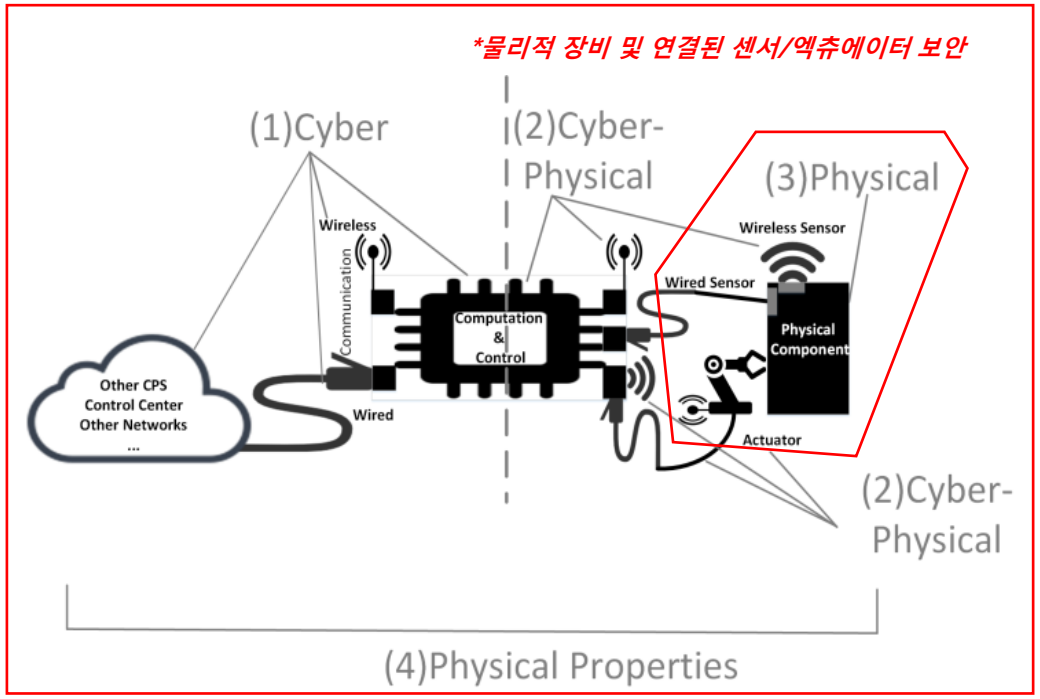
OT 거버넌스 수립 후

1	OT 보안 조직 수립 및 R&R 제시
2	OT 보안 대상 및 보안 정책 제공
3	OT 보안 수행 프로세스 수립 및 점검 방안 제공
4	OT 보안 취약점 점검을 통한 위험 관리 제공
5	OT 사이버 보안 사고 대응 절차 수립

OT물리보안

OT 장비 운영 및 보호를 위한 물리 보안 구성 및 운영

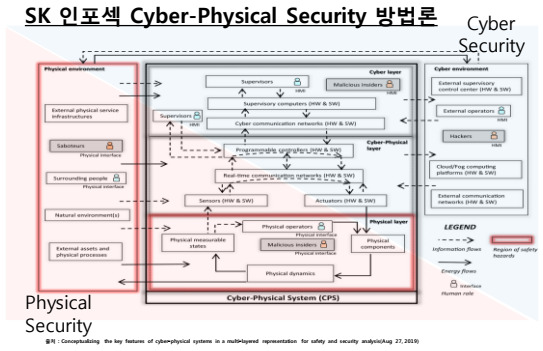
SK Infosec Cyber-Physical Security 체계수립



기밀 시설 출입 통제 및 관리

공장 모니터링 및 구역 경계

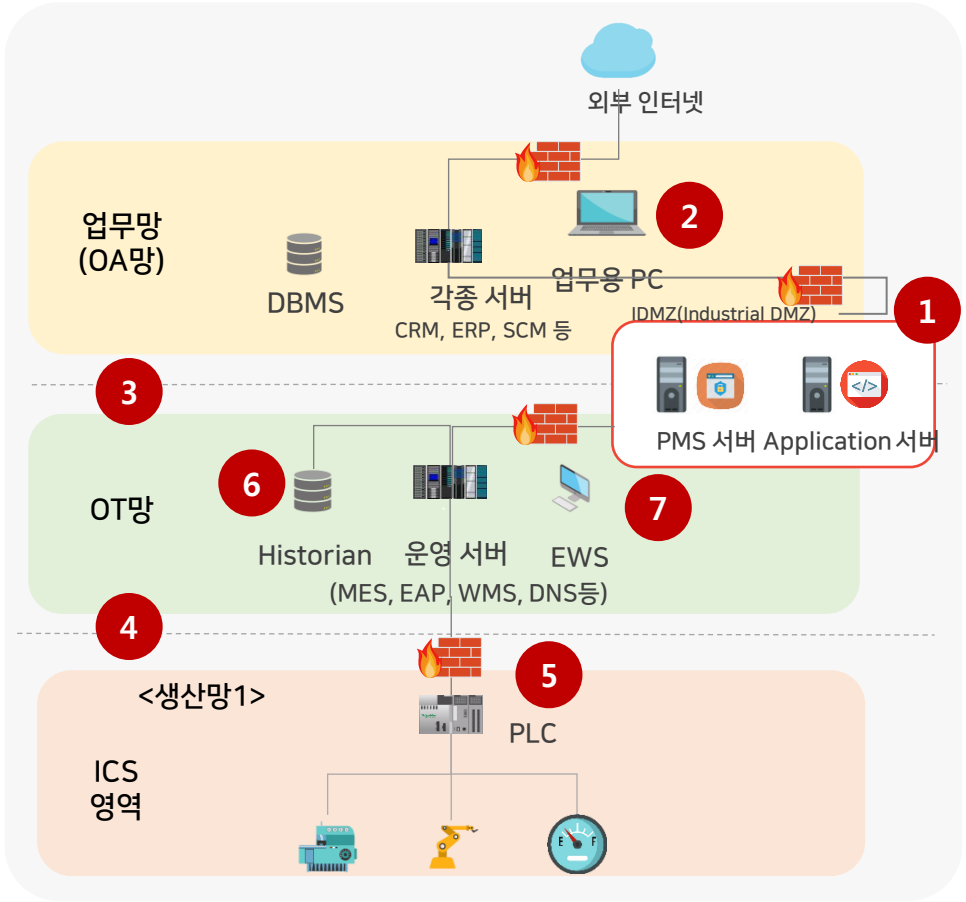
공장 내 OT 장비 운영 및 보호



(출처 : Cyber-Physical Systems Security–A Survey(The University of Kansas, Submitted on Jan 17, 2017)

OT네트워크 영역

OT/ICS 네트워크 세그멘테이션 및 견고성 제공에 대한 방안 제시



영역	보안구성	상세방안	비고
업무망 <-> OT망	IDMZ 구성	- 방화벽으로 분리된 산업전용 DMZ 구성	1
	원격접속 제어	- 네트워크 구성 / 방화벽 정책 확인 - 비정상접근/불필요 서비스 포트 차단 - 모의해킹을 통한 보안 Hole 확인	2
	네트워크 세그멘테이션	- OT망 ↔ IT 업무망 분리 (IDMZ 구축)	3
OT망 <-> ICS영역	OT보안 솔루션 구축	- ICS이상징후 탐지 솔루션 - 단방향 게이트웨이 등 맞춤 솔루션 도입	4
	네트워크 세그멘테이션	- 주요 생산/설비 네트워크 이중화	5
전체영역	네트워크 통합 모니터링	- 산업용 프로토콜 분석 및 모니터링	6
	ICS 이상징후 탐지	- 비정상 접근 / 비 인가자 접근탐지 및 차단 - 최신 제조산업 취약점 반영	7

OT 장비 보안

OT/ICS 자산 가시성 확보 부터 장비 별 보안 점검 관리 까지 심층 보안전략 수립

기존 공장 대응

신규 공장 대응

Security By Design

- 산업설비 도입 전 보안성 검토 진행
- 신규 구축 제조공장 보안시스템 설계 지원

장비 보안 취약점 분석

- 제조사별 장비 체크리스트 기반 취약점 점검
- OT장비 필수 보안설정 확인 및 적용

패치 및 취약점 관리

- 유지보수 PC 관리
- 설비 단말 최신 보안 패치
- EOS장비 관리

OT 장비보안 수립 전

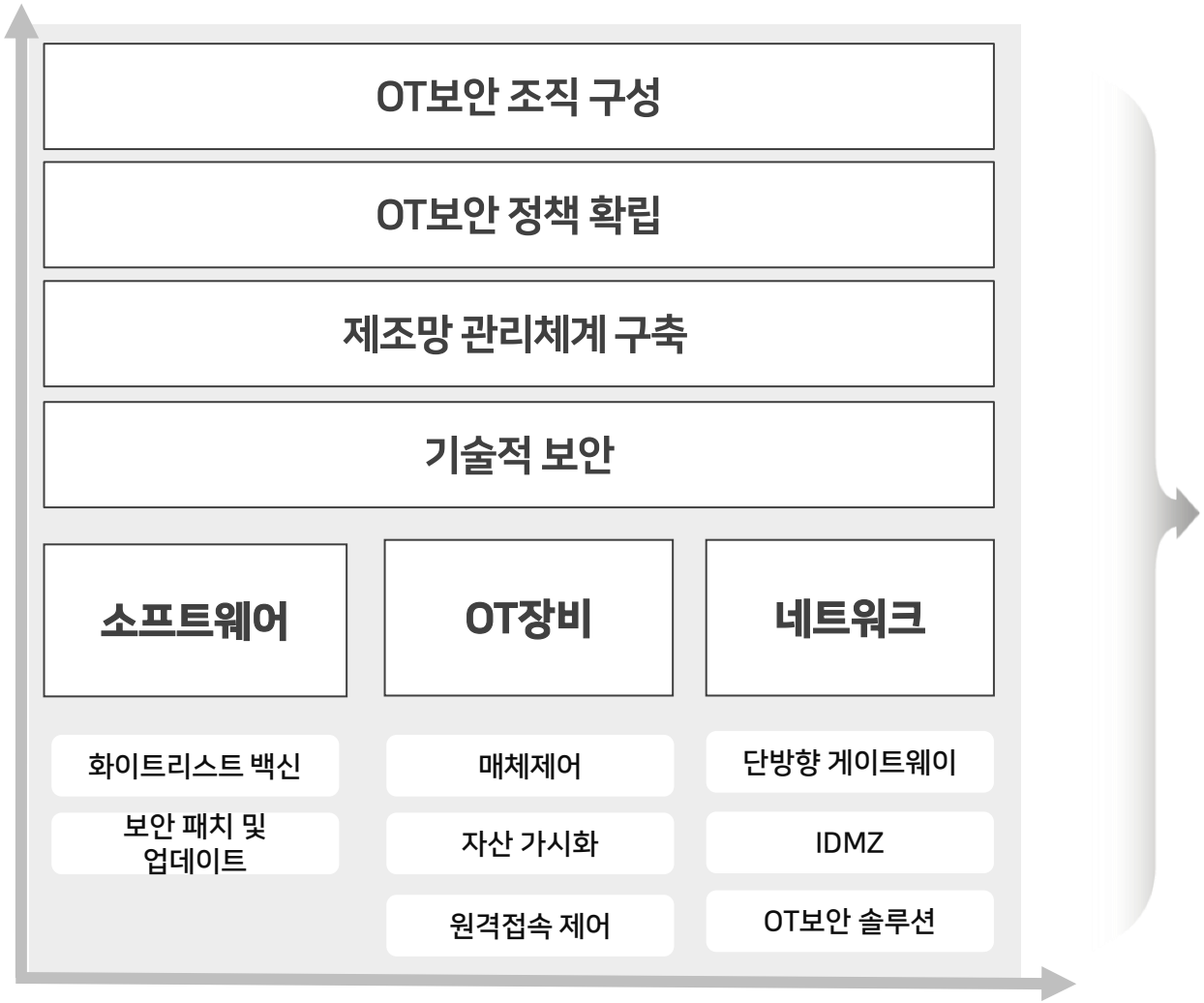
1	OT 자산 식별 및 보안 대상 구분 필요
2	OT 자산에 대한 보안 점검 방안 부재
3	OT 자산에 대한 보안 관리 방안 필요

OT 장비보안 수립 후

1	OT 장비 식별 및 대상 조사 진행 (가시성 보안 솔루션 구축)
2	OT 장비 보안 점검 항목 제공 (국내외 표준 기반의 OT장비 보안 요구사항)
3	OT 장비 별 보안 점검 가이드라인 제공 (제조사별 보안요건 분석)
4	OT 장비 취약점 보고서 및 이행 관리 제공

OT/ICS 심층보안 전략

SK 인포섹의 심층 보안전략의 구성은 관리, 물리, 기술적 보안 내용 및 대상으로 아래와 같이 정의하여 대응함



물리보안

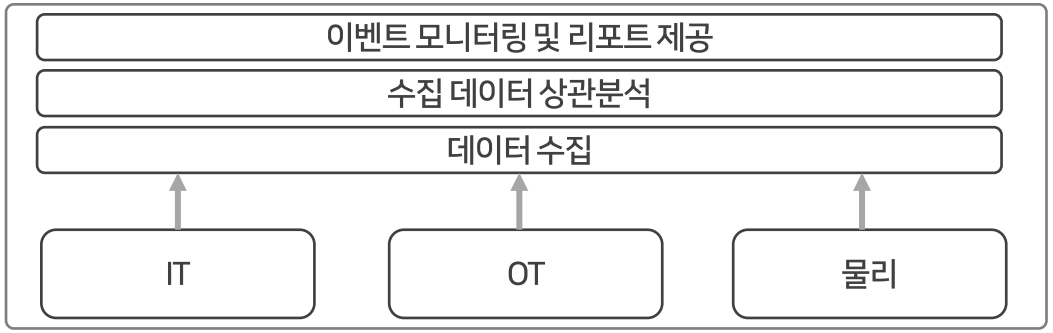
- 물리영역 관리
- 자산 접근제한
- 시설 접근제한

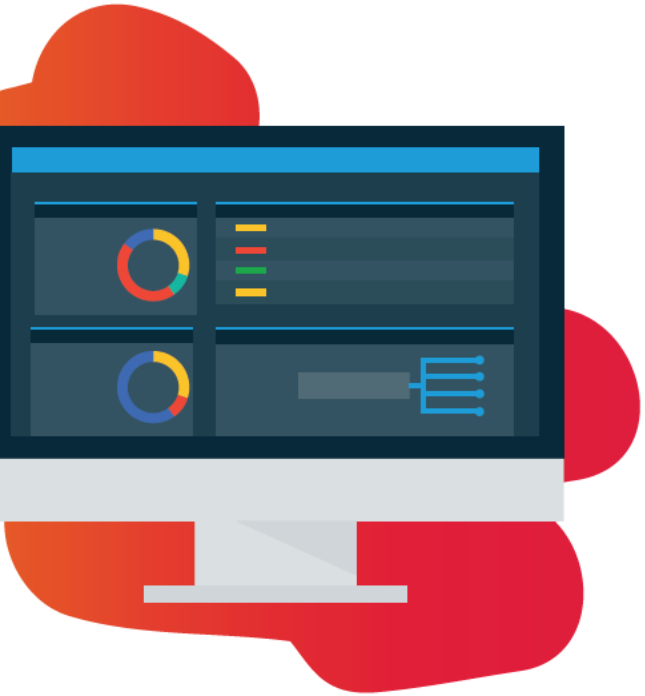
OT보안 거버넌스

- OT기획 및 조직구성
- OT/ICS 위험관리
- 보안적용 및 성과관리

통합보안관제

통합보안 관제플랫폼을 활용한 제조 전 공정 관제체계 수립 및 운영



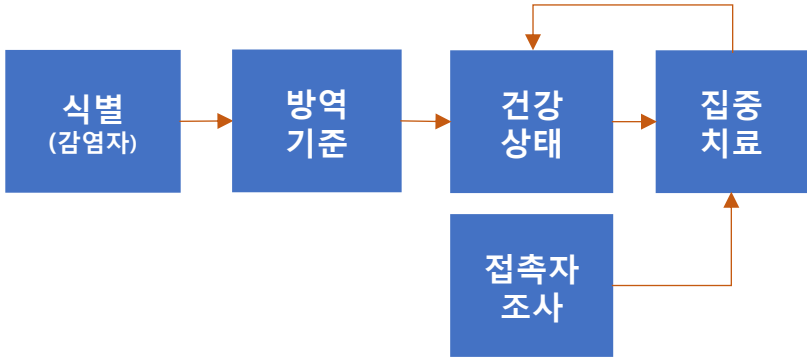


Chapter 4
SK 인포섹 OT 방역 서비스

방역이란?

COVID 방역

COVID-19 방역모델



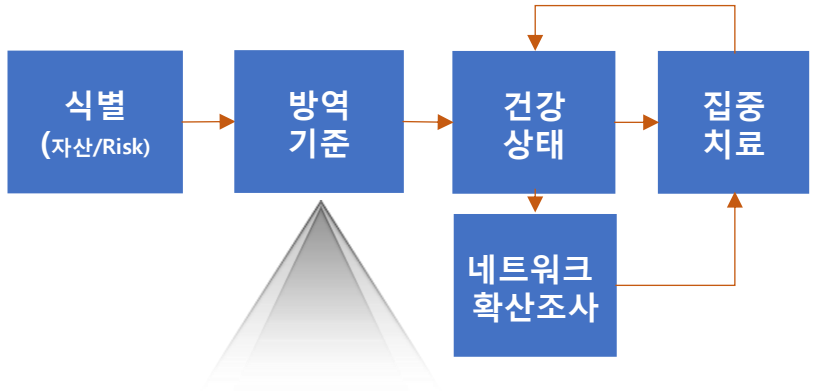
확진환자 발생 시 대응 프로세스

1 확진환자 역학조사	2 확진환자 관리	3 접촉자 역학조사	4 접촉자 관리
+ 추정감염원 조사 + 감염경로 재확인	+ 국가지정 입원치료 병상 입원 격리조치	+ 접촉자 재조사 + 접촉자 재분류	+ 접촉자 관리방법 계획 수립과 적용
◦ 증상 발생 14일 전 ◦ 방문지 및 상세이동경로 현지 의료기관 방문여부 의심·확진환자 접촉여부 기타 위험요인 확인	◦ 병상 배정 후 격리 조치 환자상태 일일현황보고 ◦ 검사결과 모니터링 ◦ 격리해제 전까지 관리	◦ 증상발생 1일 전부터의 방문지 및 상세 이동경로 파악 접촉자 명단 재작성 ◦ 접촉자 재분류 →격리/능동감시 ◦ 관리대상자 출국금지 ◦ 방역조치	◦ 접촉자 격리/능동감시 시행 ◦ 마지막 접촉일로부터 14일 동안 매일 2회 유선연락 ◦ 모니터링 결과 입력 ◦ 접촉자 모니터링 해제

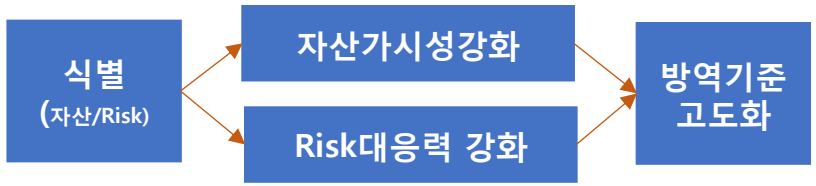
(출처 : 중앙방역대책본부COVID-19대응지침)

Smart Factory 방역

스마트팩토리 표준 사이버방역모델



OT/ICS 방역기준 고도화



OT 방역 서비스 라이프 사이클

OT보안 전문서비스

- 16년 부터 OT 보안 컨설팅 시작 4년간의 전문 노하우 보유 서비스
- 시큐디움을 통한 IT/OT 통합 관제 서비스
- OT 보안 솔루션 구축 및 운영 노하우 보유

연속된 서비스를 통한 효율성

- 컨설팅부터 관제 까지 토탈 서비스 제공 가능
- 한 번의 정보 제공으로 연속된 서비스 제공
- 각 단계의 연계성을 통한 효율적 관리 제공

IT/OT 융합 보안 제공

- 다년간 IT보안 관제 운영 노하우 보유
- IoT 및 OT 보안 융합 관제 서비스 솔루션 보유

SK인포섹 방역 체계와 심층 보안전략

심층 보안 전략

- OT보안 거버넌스
- OT물리보안
- 기술적 보안
  - OT네트워크
  - OT장비

OT 보안 방역 체계

OT 컨설팅	• 자체 방법론을 이용한 OT 보안 체계 수립 및 제공 • 리스크 및 모의 해킹 등을 통한 위협 분석 제공 • OT 보안 로드맵 및 향후 보안 방향성 제공
OT 보안 솔루션 구축	• OT 네트워크 및 장비 위협에 따른 보안 솔루션 검토 • 보안 솔루션 구축을 위한 OT 보안 아키텍처 수립 • 구축 수행 계획, 중간, 완료 보고서 및 정책서 작성 제공
OT 보안 솔루션 운영	• 보안 솔루션 정책 수립 및 보안 점검 결과 보고서 제공 • 보안 이벤트 로그 분석을 통한 OT 위협 분석 • OT 가시성 확보를 통한 자산 식별 및 산업 프로토콜 모니터링
OT 보안 관제	• OT 보안 솔루션 및 OT 장비 모니터링 이벤트 로그 수집 분석 • IT/OT 통합 관제 모니터링 수립

OT 보안 컨설팅

SK infosec

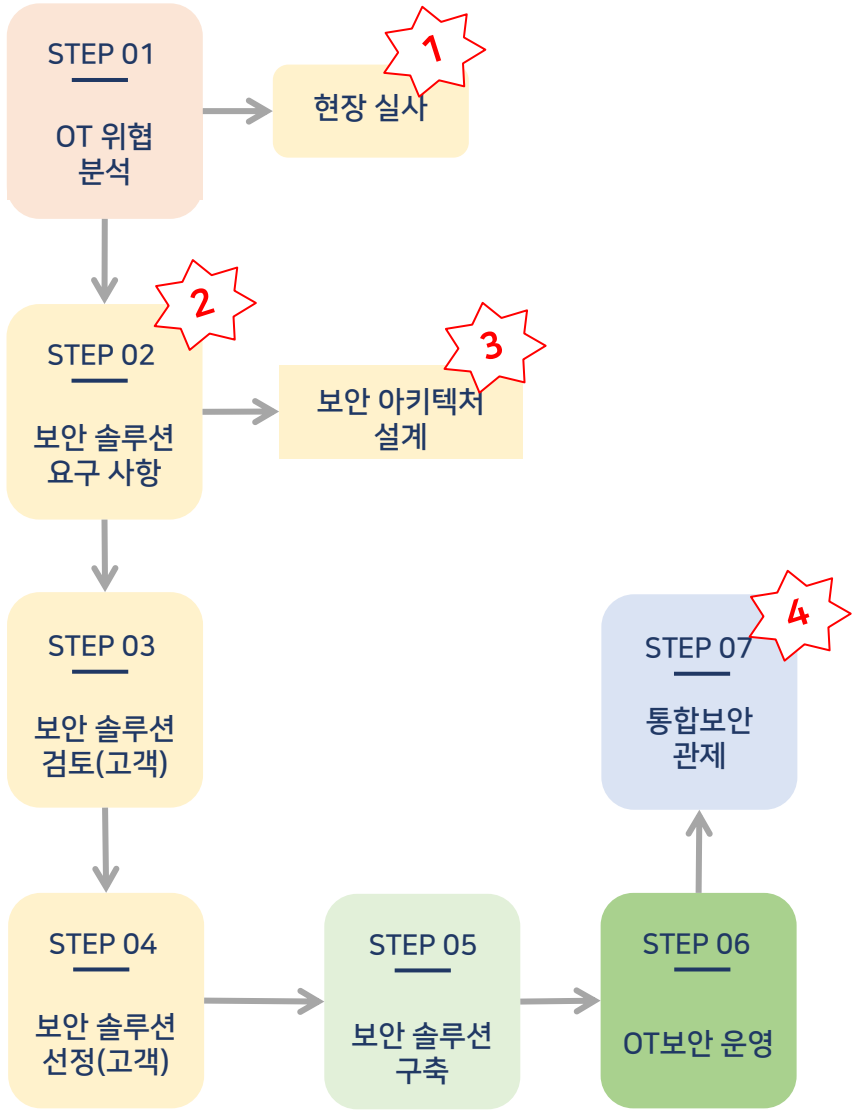
SK인포섹 OT보안 컨설팅 방법론(ISCM-OT)을 기반으로 다각도에서 OT보안RISK를 식별/분석하고 고객 맞춤형 OT보안 전략을 수립

다차원 OT보안 RISK분석 제공

현실적인 OT보안 체계 구축

고객 맞춤형 OT보안 전략수립

OT 보안 솔루션 구축, 운영 및 관제



OT 보안 솔루션 구축 시 고려사항

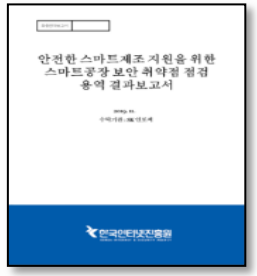
1 현장 실사	• OT 보안 위협에 대한 현장 점검 • OT/ICS 운영 환경에 대한 분석
2 보안 솔루션 요구 사항	• 현장 실사에 따른 산업용 프로토콜 지원 및 구축 제반 사항 • 소스코드 취약점 점검 및 보안 디자인 적용 여부 검토 • 도입 보안 솔루션의 OT/ICS 네트워크 및 장비 가용성 영향도 검토
3 보안 아키텍처 설계	• 보안 솔루션 도입으로 인한 OT/ICS 네트워크 및 보안 설계 • 표준 OT/ICS 보안 요구 사항에 따른 보안 솔루션 구성 제시
4 통합 보안 관제	• OT/ICS 보안 솔루션 이벤트 로그 수집 및 통합 모니터링 • OT/ICS 네트워크 패킷 분석을 통한 이상행위 모니터링 • IT / OT 통합 모니터링을 통한 융합 보안 제공

OT 보안 주요 수행역량

보안 취약점 점검

19년 KISA 스마트공장 보안 취약점 점검 사업 수행

- 2개 스마트공장 취약점 점검
- 스마트공장 보안 취약점 체크리스트 (44개 항목) 개발



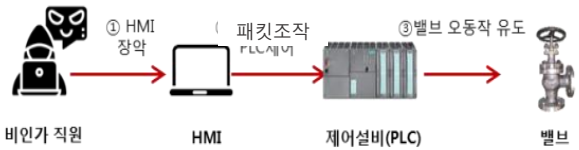
취약점 점검 용역 결과 보고서

OT/ICS 보안위협 테스트

SKXX ICS보안 사업에서 제어장비 보안 위협 테스트 시연

- 산업 제어 프로토콜 취약점을 이용한 제어장비(PLC) 오동작 시연

보안 위협 시연

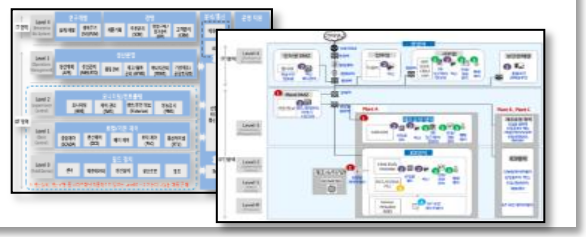


보안 모델 개발

SK C&C 스마트팩토리 보안체계 수립 컨설팅에서 스마트공장 보안모델 개발

- 스마트공장 모델 개발
- 스마트공장 보안 표준 모델, 선택 모델 개발

스마트공장 보안 모델 수립



SK infosec OT보안 레퍼런스

SK

SK 관계사

제조 120여 개 관계사 대상
OT방역체계 수행 및 제조 영역별
보안 점검방안 수립 중

KISA
Korea Internet & Security Agency

KISA 스마트 팩토리

19년,20년 스마트공장 보안모델
기준 수립 및 취약점 점검 수행

대외

대외사업

반도체 및 화학 전지계열
OT보안 수행