산업제어시스템(OT) 보안 트랜드와 대응 솔루션 소개 (PoShield)

2020. 9. 8

CONTENTS

산업제어시스템(OT) 보안 트랜드와 대응 솔루션

1. 산업제어시스템 보안 패러다임의 변화

Smart Factory 확산으로 설비제어 환경이 변화하고 있으며, 기존 정보시스템(IT) 보안과는 다른 방식으로 접근 필요

산업제어시스템 보안 현황

○ **폐쇄형 환경이라 안전하다는 인식 및 오해**

- 안전에 대한 인식은 높지만 보안 인식은 부족
  (예: USB 등을 통한 악성코드 감염, 유지보수 시 외부연결)

○ **오래된 설비와 수많은 프로토콜, 자산관리 미흡**

- 보안 적용이 힘든 오래된 기계설비 혼재
- 설비 제조사마다 각기 다른 전용 프로토콜과 OS 사용
- 전체 설비와 네트워크의 모니터링과 관리가 어려우며, 자산에 대한 가시성 및 식별에 어려움

○ **OT환경의 이해도가 높은 보안인력 부족**

- OT환경에 대한 지식이 높은 IT보안인력 (융합 전문가) 부족
- IT보안 전문기업도 동일한 현실, 전문 OT보안솔루션 부족

보안 패러다임의 변화

○ **경영 및 기술 환경의 변화로 기존 비즈니스(IT) 시스템과 통합되고, 개방형 시스템으로 표준화 진화 중**

- 폐쇄망(망 분리 환경) → 타 시스템과 연결점 발생 중

○ **Smart Factory, IoT 등의 확대로 외부 연결이 증가하면서 보안 경계 모호**

- IoT, Cloud, 5G 등 연결되는 기기 및 서비스의 증가
- 내부망으로 예상치 못한 접근을 사전 탐지 어려움

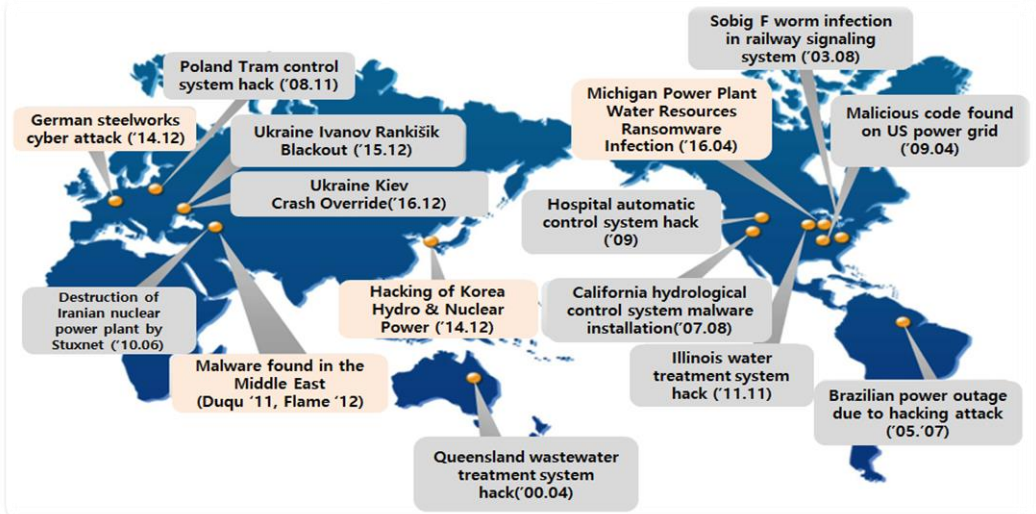
○ **단순 정보유출 → 시설 파괴, 서비스 중단 목적으로 변화**

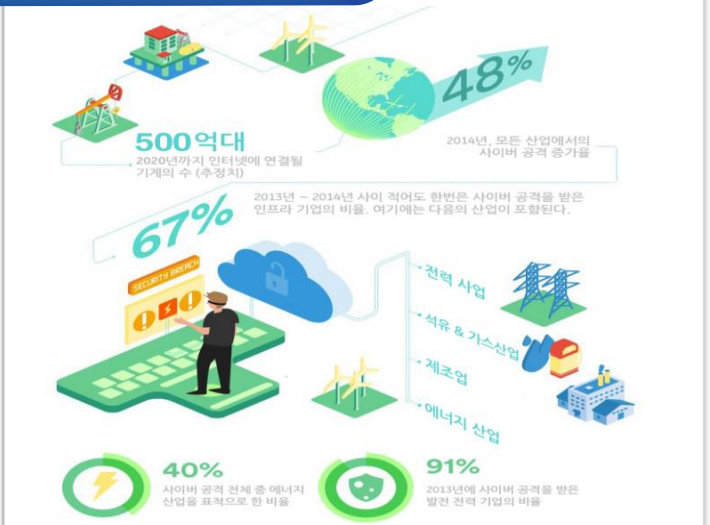
- 지능화된 공격으로 그 위험성과 파급력은 매우 큼

2. 산업제어시스템 보안 침해 사례

폐쇄망으로 안전하다 여겨진 산업제어시스템, 대형 보안사고는 빈번히 발생되고 있음

산업기반시설을 대상으로한 다양한 보안 침해 사례 발생





주요 산업제어시스템 보안 침해사고 피해 사고

독일 철강회사, 사이버공격으로 용광로 손상 ('14년)

"공장의 제어시스템을 파괴해 용광로를 차단하지 못하게 함으로, 물리적인 손상을 발생 엄청난 조업 피해 발생"

대만 TSMC (반도체) 조업중단 ('18년)

"소프트웨어 설치 과정 중 악성코드에 감염되어, 공장 가동이 이틀 동안 중단…"

노르웨이 알루미늄 공장 글로벌 운영중단 ('19년)

"랜섬웨어 감염으로 노르웨이 Norsk Hydro 생산공정 중단 생산량 감축으로 전 세계 알루미늄 가격 1.2% 상승"

베네수엘라 대정전 국가 96% 가 암흑사태 (19년)

수력발전소에 대한 해킹 (전자기 공격)으로 전국 23개주 중 19개주가 정전 피해 발생

[별첨] 산업제어시스템 피해 사례

No	시기	발생국	피해내용	비고
1	2010년	이란	- 스턱스넷 바이러스 원자력 발전소 제어시스템 침투, 이란 나탄즈 원자력발전소의 1000여대 원심분리기 파괴	
2	2011년	미국	- 일리노이 주 상수도 시설 시스템 침투, 펌프 작동시스템 파괴	
3	2012년	미국	- 전력시설 터빈 제어시스템 악성코드 감염, 3주간 운영 중단	
4	2014년	독일	- 독일 철강회사의 용광로 제어시스템 장애 발생	
5	2015년	우크라이나	- 전력 발전소에 악성코드를 통해 제어시스템 중단, 정전 유발 (블랙에너지, 크래시오버라이드 공격)	
6	2016년	미국	- 수처리 회사의 PLC를 임의 조작하여 수처리 관련 화학물질 양을 조작	
7	2016년	독일	- 원자력 발전소 원료 적재 시스템, 악성코드를 활용하여 원료 적재 시스템을 원격 조작하여 발전 중단	
8	2017년	우쿠라이나	- 우크라이나 등 다국가 대상 낫페트야 랜섬웨어 활용 사회 기반 시설 대규모 공격 - 러시아 로스네프트(Rosneft) 석유회사, 러시아 에브라즈(Evraz) 철강회사, 우크라이나 보리스필 국제 공항, 미국 머크(Merdk) 제약회사, 세르노빌 방사능 탐지 시스템 등 일시 마비	
9	2017년	미국	- 달라스 비상사이렌 제어시스템에 연결된 무선통신망 해킹, 비상사이렌 15시간 동안 비정상 가동	
10	2017년	일본	- 혼다 모터스 사야마 공장, 워너크라이 랜섬웨어 공격으로 엔진 생산 및 조립 라인의 P/C 정지	
11	2018년	대만	- 반도체 생산업체 TSMC, 제어시스템에 침투한 악성 코드로 생산 라인 일부가 멈춤. 3000억원의 손실	
12	2019년	노르웨이	- 알루미늄 생산기업 노르스크하이드로(Norsk Hydro), 랜섬웨어'록커고가(LockerGoga)'에 감염, 생산중단	
13	2019년	베네수엘라	- 국가 전력의 70% 이상을 공급하는 수력발전소 설비 고장으로 전국 23개 주 가운데 19개 주 전력공급 차단 . 일주일간 지속된 정전으로 민간 피해액은 4억달러 예상	

3. 산업제어시스템 보안에 대한 시장과 정부의 움직임

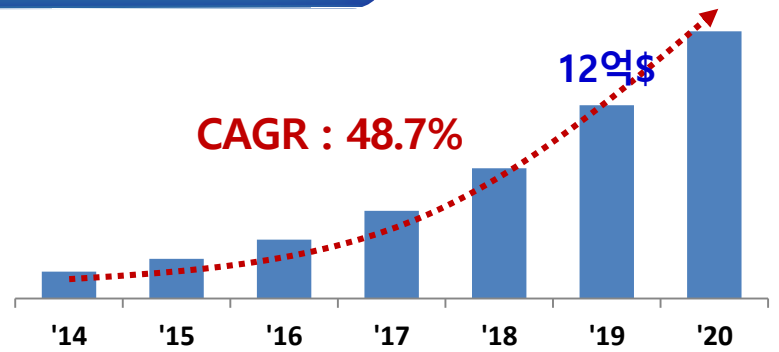
ICS보안 시장은 급격하게 성장하고 있으며, 중요성에 대한 인식도 변화하고 있음

아시아태평양 ICS보안 시장 규모는 '19년 12억$, CAGR 48.7%

아시아태평양의 산업제어시스템 보안 시장 전망

Market Overview

Market Stage	Market Revenue	Market Size for Last Year of Study Period	Compound Annual Growth Rate
Nascent	$162.9 M (2014)	$1,186.2 M (2019)	48.7% (CAGR, 2014-2019)

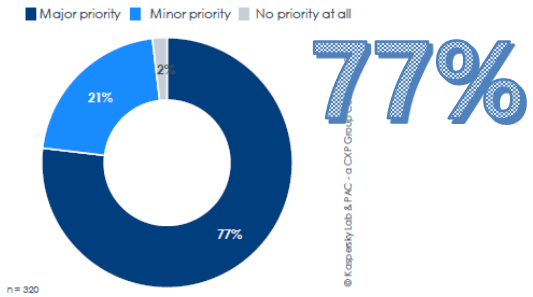


* 출처 : 프로스트앤설리번 `아시아·태평양 ICS 보안시장`, 2016.2

산업제어시스템 보안현황 Suvey (32개국 320명, CIO대상)

출처 : The State of Industrial Cybersecurity 2018, KASPERSKV

ICS 보안위협 증대 예상



- 지난 12개월동안 ICS에 대한 공격 경험 : 64%
  - 랜섬웨어 공격 30%, 내부직원의 실수 27%
- 보안침해 사건을 보고하지 않은 기업 : 16%
- ICS보안침해를 당한 기업 중 재정피해를 입은 기업 : 20%
- 산업 또는 정부규제 지침을 준수한 기업 : 23%

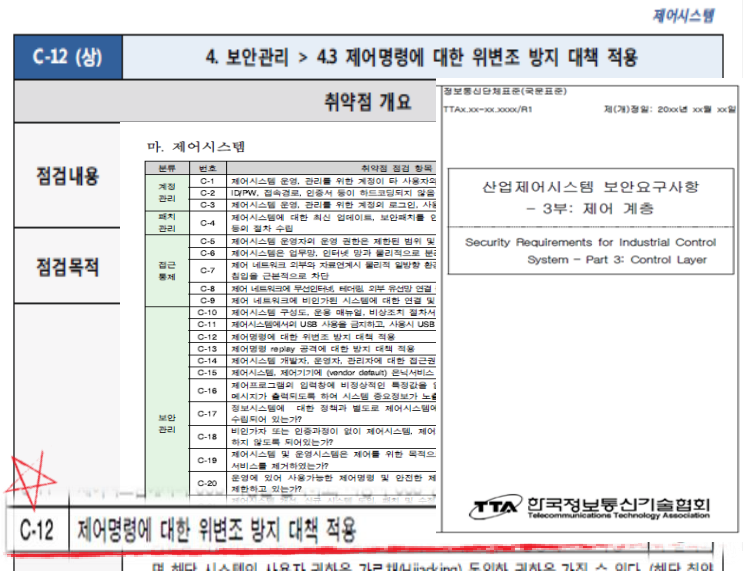
3. 산업제어시스템 보안에 대한 시장과 정부의 움직임

정부 주도로 산업기반시설에 대한 보안 가이드가 제시되고 보안준수에 대한 규제 움직임

해외에서는 ICS보안에 대한 제도 정비 및 전담기관을 설립하여 국가 차원의 산업제어시스템 보안을 강화

- **미국 : '18.6월 「산업제어시스템 기능 향상 법」**을 개정하여 산업제어시스템에 대한 연방 차원의 규제를 강화함
  - **국가사이버 보안 및 통합센터(NCCIC)는** 주요 산업시설에 대하여 **보안 점검 및 대응 권고에 대한 법적 권한 부여**
- **일본 : 제어시스템 보안검토위원회 설립, 사회기반시설의 보안 강화를 목적으로 ICS보안 인증 제도 추진**
- **중국 : 국가산업시설 및 민간 산업시설 전반의 보안강화를 위해 ICS보안 전담 정보안전사업연맹 설립**

국내 정부 움직임

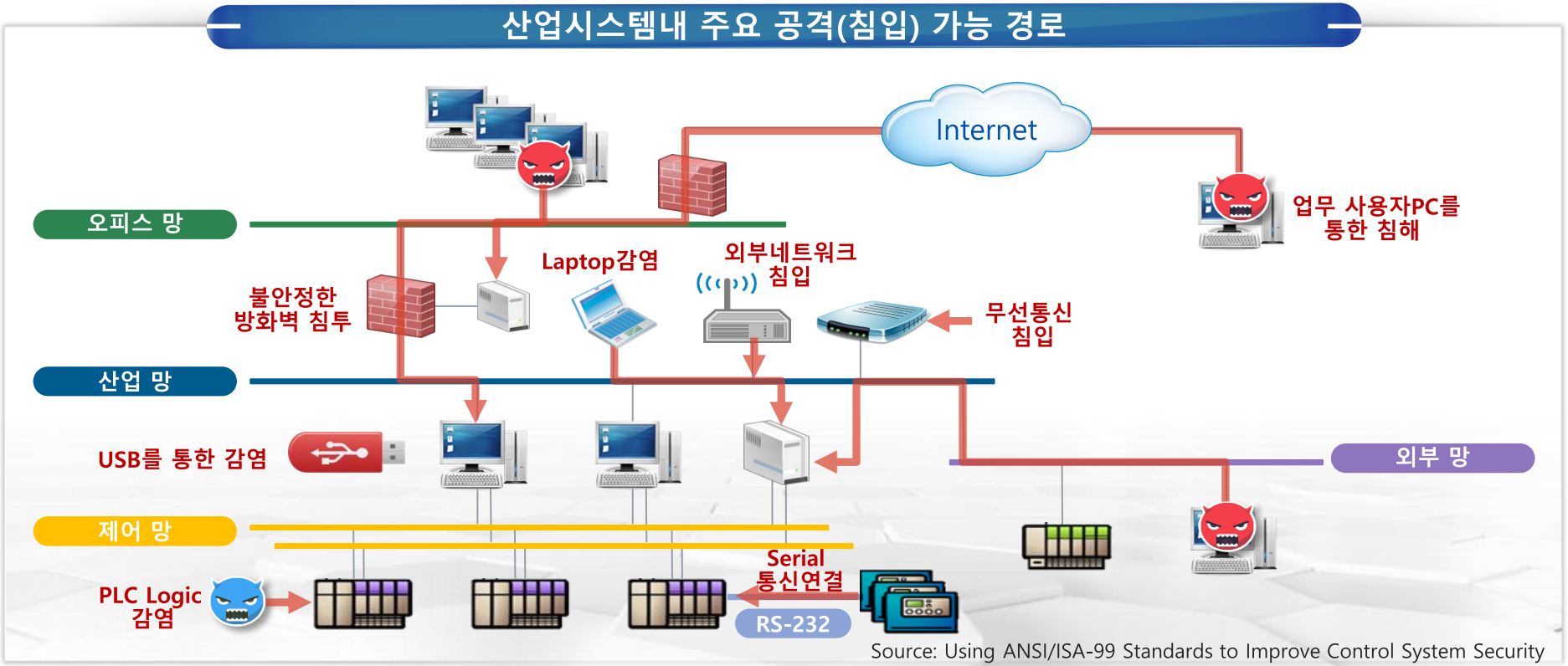


- **행정안전부와 KISA에서 주요정보통신기반시설대상 취약점 분석 및 평가 가이드 제시('14년)**
  - 정보통신기반보호법(제9조) 및 시행령(제17조)에 따라 매년 **주요 정보통신기반시설 대상 총 453개 항목의 취약점 분석 및 평가** 시행 **(ICS항목은 22개 → '20년 53개)**
- **국가정보원이 주도하여 산업제어시스템(ICS) 보안에 대한 KS국가표준을 제정('20.4.8)**
  - **산업제어시스템 컴포넌트의 기술적 보안 요구사항 표준번호 : KS X IEC62443-4-2**

정부 주도의 보안규제 및 법제화 예상

[별첨] 산업제어시스템 보안 침입 경로

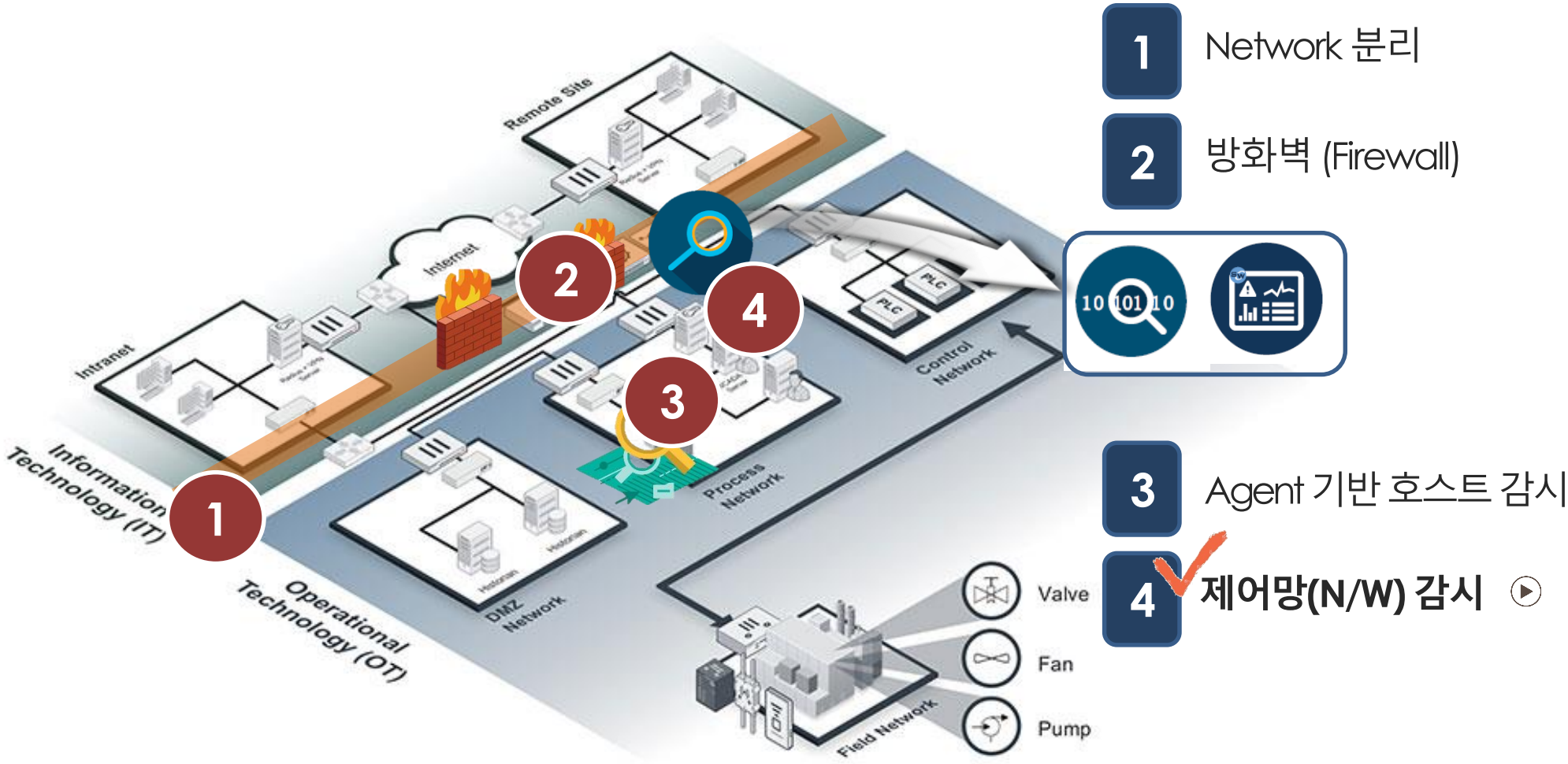
폐쇄망 환경에서 운영되는 산업제어시스템의 공격 경로는 매우 다양함



- 업무PC에서 원격접속시스템을 통해 현장내 HMI에 접속하는 경우 → **랜섬웨어 감염**
- 망분리 부재 및 불안정한 방화벽 설비 → **외부로부터 악성코드 침입**
- 시스템 업그레이드나 원격제어를 위해 무선 인터넷 환경에서 파일 전송 → **외부로부터의 악성코드 유입**
- 업무 편의를 위해 인터넷 망에서 다운로드 받은 파일을 USB를 이용해 폐쇄망 PC에 옮김 → **생산라인 접근 및 보안 유출 발생**
- Serial 포트 연결 → **연결 설비간 감염**

4. 산업제어시스템 보안 솔루션 유형

Network분리, 방화벽 등과 같은 전통적 보안 방식 외
제어 Data를 감시하고 이상징후를 탐지하는 제어망(N/W) 솔루션이 부각



4. 산업제어시스템 보안 솔루션 유형 _ 제어망 감시

제어망(N/W) 감시 유형의 솔루션은 제어 명령 위변조 탐지 솔루션과 제어 Data Traffic에 대한 이상탐지 솔루션이 있음

제어 명령 위변조 탐지

PLC, HMI, Process Computer 등 설비 제어시스템에서 자동화 설비로 통신(제어)하는 제어명령 Data Code 위변조 탐지

PLC 등 설비 제조사

제어망(N/W) 감시

제어 Data Traffic 이상탐지

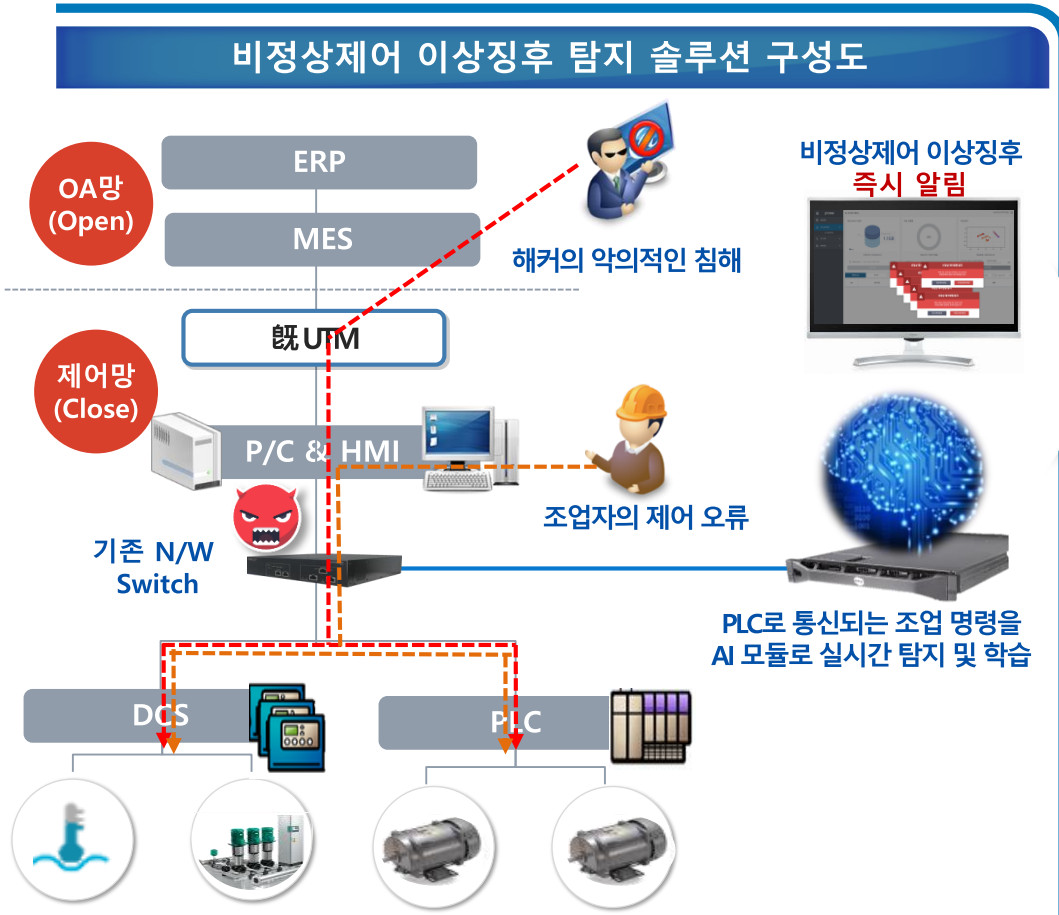
제어망 내 Data 흐름 (Traffic 양과 경로)에 대한 이상징후 탐지

통신 네트워크 장비업체

5. 솔루션 소개 _ 비정상 제어명령 탐지 솔루션『PoShield』

포스코ICT의『PoShield』는 제어 Data Code 위변조를 탐지하는 비정상제어명령 이상탐지 솔루션

주요 기능 및 구성도



주요 기능

01 ☑ 보안규칙 자동 생성(학습)
→ 정상 제어명령 데이터 수집 기반으로 머신러닝을 통해 보안규칙 자동 생성

02 ☑ 비정상 제어명령 탐지/알람
→ 학습으로 생성된 탐지 모델을 사용하여 비정상 제어명령을 탐지

03 ☑ N/W Topology 자동 생성
→ 수집된 IP 주소를 기반으로 연결 객체(설비) 대상 N/W Topology 자동 생성

04 ☑ 저장 데이터 암호화
→ 학습된 제어 명령 데이터, 사용자정보 등 암호화

05 ☑ 솔루션 환경 설정 및 자체 보안 기능
→ 사용자 관리(유저정보, 사용권한 등), 세션 관리, 접근관리 등 동작 상태 및 변경 내용을 주기적으로 체크

06 ☑ Dash Board
→ 각 모듈 동작 상태 및 H/W Resource 상태 정보 및 조업현황 모니터링 가능 (PLC 동작상태, 제어명령수)

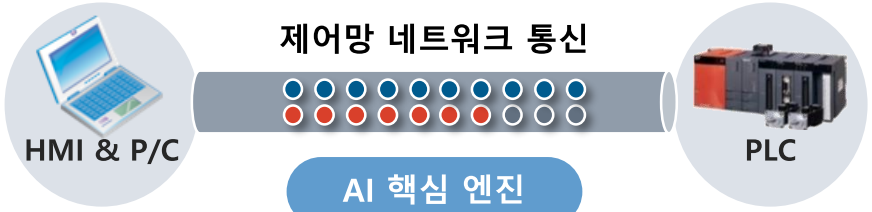
5. 솔루션 소개 _ 비정상 제어명령 탐지 솔루션『PoShield』

Heavy Industry의 특성을 반영한 Smart Factory 보안 솔루션입니다.

Heavy Industry 특징

01	02	03
기존 제어설비에 피해없이 무간섭한 솔루션 형태로 구현 가능	고객의 운영 Data 비밀을 최대한 유지시키며, 이상징후 탐지 해야함	다양한 프로토콜과 운영시스템을 수용할 수 있어야 함

비정상제어 이상징후 탐지 솔루션 "PoShield"



1. 산업 환경이 반영된 보안 규칙(White List) 생성
2. 작업자 운전환경을 고려한 지능적 Detection
3. 제어망 N/W 재구성이 없는 설치/운영
4. 다양한 PLC 통신 프로토콜 수용
5. 기존 ICS 설비에 무간섭 구성

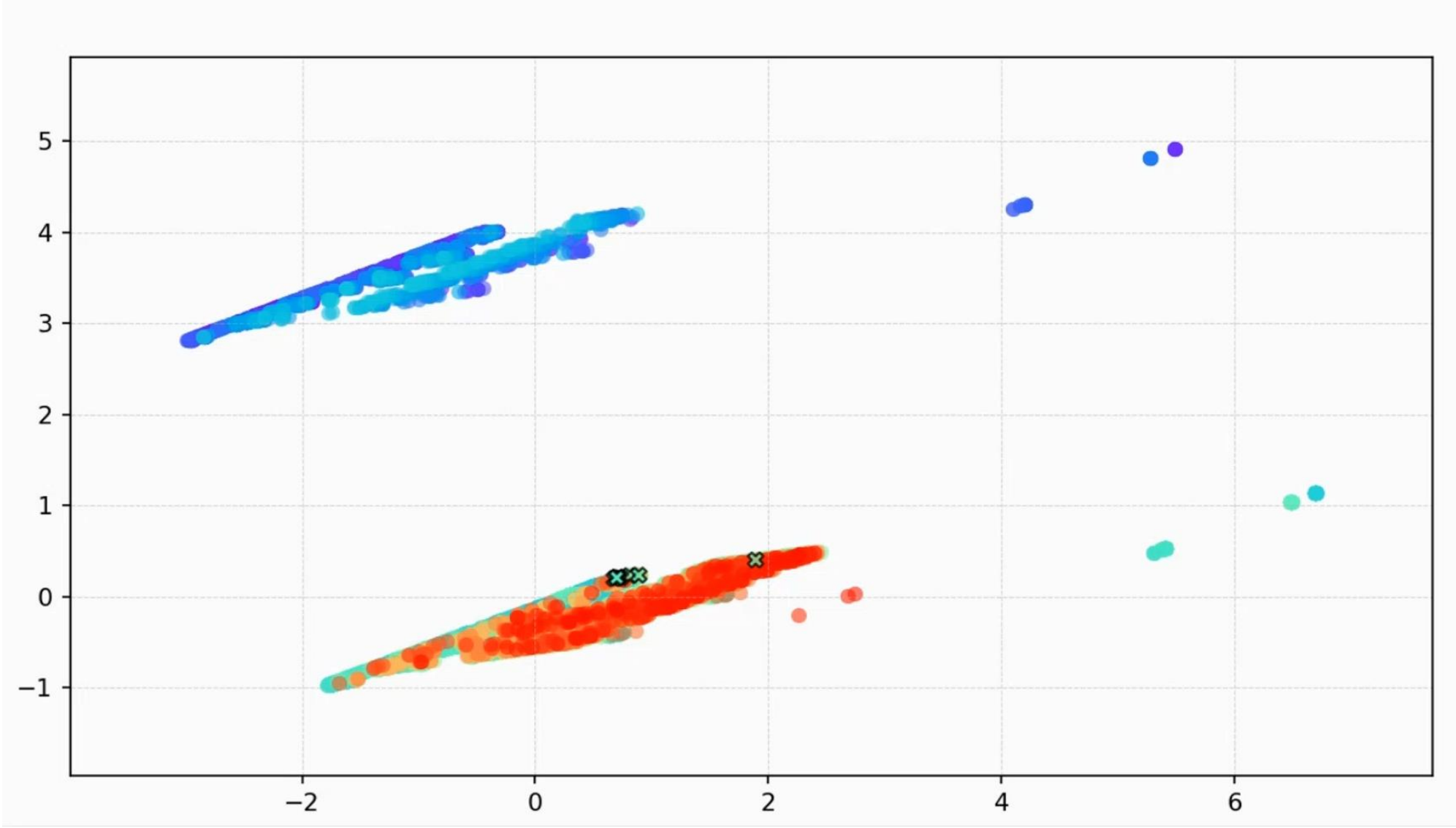
01 ☑ 생산, 운영 노하우의 외부 유출을 막는 높은 보안성
→ AI학습으로 보안규칙을 생성함으로써 제어명령 데이터가 보안사업자로 유출되는 위험성을 최소화

02 ☑ 산업별 특성을 고려한 탐지 오차범위 자동 설정
→ 비정상 제어명령 탐지 시 현장 작업 특성을 반영한 보안규칙 설정으로 탐지 정확도 및 신뢰성 향상

03 ☑ 기존 운영중인 네트워크/설비에 무간섭 작동
→ 기 설치된 N/W Switch의 미러링 기능 적용, 고객의 네트워크에 영향 및 재구성 없이 설치 운영

04 ☑ 다양한 PLC 통신프로토콜 적용 가능
→ TCP/IP, Modubus, OPC-UA, 지멘스 S7, YASKAWA, GMK, 멜섹, FATEK, HART 등

[별첨] PoShield 비정상제어명령 탐지 Logic



[별첨] PoShield 특허출원 내역

머신러닝 기반의 산업제어시스템 보안 장치 1건,
정상제어명령 패턴 추출 방법 1건외 다수 특허 및 인증 출원

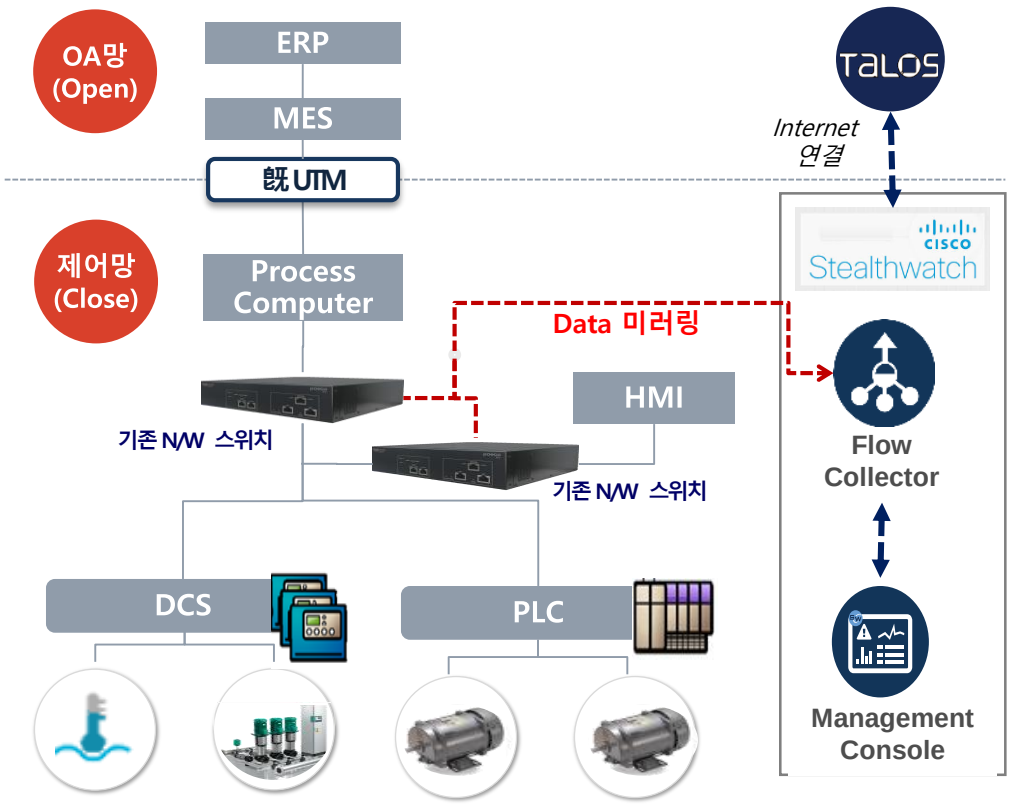
구분	명칭	출원일	지역	기타
특허	제어데이터의 정상 시퀀스 패턴 생성 시스템 및 방법	2017-12-28	국내	특허청
특허	비정상 제어데이터 탐지 시스템	2017-12-28	국내	특허청
인증	소프트웨어 품질 인증서 (GS인증)	2019-04-01	국내	한국정보통신기술협회
특허	제어데이터 이상 검출을 위한 시스템	2019-05-31	국내	특허청
특허	스위칭 장치를 이용하는 비정상 제어데이터 탐지시스템	2019-05-31	국내	특허청
특허	비정상 제어데이터 탐지시스템	2019-06-11	해외	특허청
인증	SW 저작권 등록증	2019-08-26	국내	한국저작권위원회

5. 솔루션 소개 _ 제어망 이상 트래픽 탐지『Stealthwatch』

Cisco의『Stealthwatch』는 제어망 내부의 N/W Traffic에 대한 모니터링과 이상징후 탐지 솔루션

주요 기능 및 구성도

NW Traffic 이상징후 탐지 솔루션 구성도



주요 기능

01 ☑ **NW Traffic 모니터링 (가시성 제공)**
- → 제어망 內 NW Traffic에 대하여 가시성 및 보안 위협 상황 제공
- → 전체 NW Traffic 상황 정보에 대한 실시간 정보 제공

02 ☑ **NW Traffic 흐름에 대한 이상징후 탐지**
- → 평상시와 다른 데이터 수집 또는 데이터 유출 행위 등 비정상적인 NW 접속/활용 탐지
- → 비정상적인 NW 및 서버 응답 속도 분석

03 ☑ **NW에 통신되는 위협 패킷 탐지**
- → Snort 기반의 알려진 위협 패킷 탐지
- → 위협 패킷 원본 데이터 보관
- → 탐지 이벤트 위험도 분류

04 ☑ **지속적인 멀웨어 분석**
- → 다양한 방식의 멀웨어 분석
- → 멀웨어 최초 유입경로 파악
- → 지속적 분석으로 이동경로 추적

6. Cisco와 협력

포스코ICT는 Cisco와 국내 OT보안 솔루션 사업의 선두 주자로 협력하고 있음

’19.1	’19.3	’19.6	’19.10	’20.2	’20.8~
Cooperation Discussion	MOU	양사 협력에 대한 글로벌 프로모션	Cisco 美 본사 및 Cisco APJ 협력	Cisco 美 본사 CDA Pjt 파트너 선정	포)전기강판 대상 양사 연계 솔루션 적용

MOU Signing Ceremony(‘19.3)

Cisco Digital Summit in Japan(‘19.6)

POSCO ICT

비정상 제어명령 이상 징후 탐지 솔루션

PoShield

+

Solution combination

CISCO

N/W Traffic 이상징후 탐지 솔루션

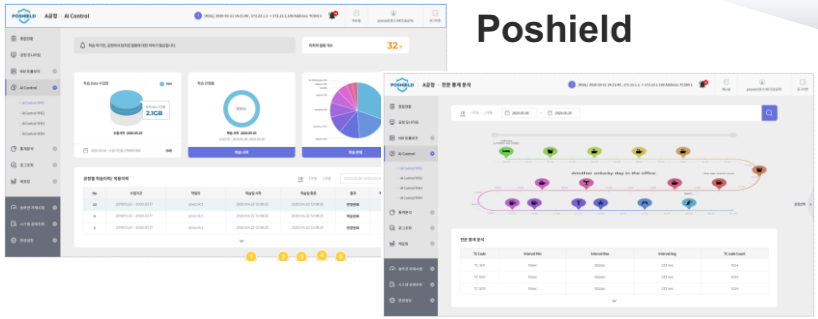
Stealthwatch

※『 **CDA**(Country Digital Acceleration) **Project** 』

- 전세계 각 국가별로 성장 가능성이 높은 사업에 **Cisco 본사가 사업기반 조성을 지원하는 프로그램**
  - ※ 전세계 Cisco 지역 법인에서 ‘국가 협력 사업’ 또는 ‘단일 사업 Item’을 제출 後, 심사를 거쳐 최종 선정
  - 전 세계 약 300개 프로젝트가 완료 및 추진 中에 있음
- 년 단일 사업 분야에서 포스코ICT가 Cisco korea와 협력하는 **『 Smart ICS 보안 사업 』이 국내 최초로 선정**
- CDA를 통해 전반적으로 Cisco와 연계 제품 개발 및 Co-Sales를 진행 (OT보안 시범사업 구축 협력 진행 中)

6. Cisco와 협력 _ PoShield + Stealth Watch 결합제품

제어명령 위변조 탐지



Poshield

N/W 트래픽 이상징후 탐지

Stealthwatch

ENCS

IE4000

Solution 결합

통합 구성도 및 화면

솔루션 통합 구성도

Stealthwatch + NetFlows + Database

PoShield + Data Mirroring + Database

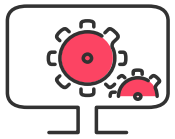
1) 두 솔루션의 고유 데이터를 활용, 상세 분석 가능
→ 비정상명령 상세 N/W 트래픽정보, 원인분석 가능

2) 통합 UI/UX를 통해 사용자 편의성 강화

[별첨] PoShield 통합 솔루션

보안 기능 강화 요구에 맞는 기능 통합으로 OT보안 솔루션 구성

❑ 통합 솔루션 기능 및 구성

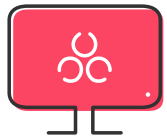


제어 명령 이상 탐지 POSHIELD

비정상 제어 명령의 실시간 감지로 신속한 대응 지원

- 해커의 악의적인 제어 명령 조작
- 조업자의 제어 오류 탐지
- 다양한 PLC 프로토콜 지원

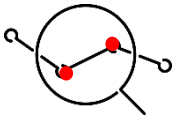
AhnLab 시그니처 기반의 취약점 탐지



시그니처 기반의 해킹 공격 예측

- 알려진 취약점 기반의 해킹 탐지
- 시그니처 / 행위 기반 공격 탐지

AI 기반 이상 행위 탐지

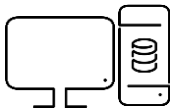


Traffic 이상 탐지 cisco

비정상 트래픽 자동 탐지로 위협의 조기 탐지

- 과다 세션 및 트래픽 Volume 발생 징후
- 비정상적인 Path로의 접속 증가
- 침입 이상징후에 대한 탐지

POSHIELD **제어망에 대한 유용한 정보**



제어 시스템의 제어명령 상황 및 N/W구성 등 모니터링

- 조업자에 포커싱된 제어설비 N/W 토플로지 제공
- 제어망 N/W Traffic의 상시 가시성 제공
- 제어시스템의 제어명령(공정) 상태(통계) 정도 제공

[별첨] OT보안 기능 커버리지 비교 자료

❑ NW트래픽 ~ 시그니처기반 위협 탐지 ~ 비정상메시지 탐지 범위까지 커버 가능한 Total 보안 솔루션 구성

	White List 기반 - Unknown 위협		Signature 기반- Known 위협		N/W Traffic 가시화(모니터링) & 제어시스템 N/W 토플로지	제어 명령 통계 모니터링
	비정상제어명령 이상징후 탐지	N/W Traffic 이상징후 탐지	악성코드 및 취약점 탐지	N/W 침입 탐지		
통합 연계 제품	◎	◎	◎	◎	◎	◎
포스코ICT	○				△	○
Cisco		○			○	
안랩			○	○	△	
Opshield	○		○		△	
Cyber-X	△	○	○	△		
클라로티	△	△	△		△	
가디언스	△	○	△		△	

[별첨] PoShield + Stealthwatch 결합제품 _ 화면예시


감사합니다