스마트팩토리를 위한 ICS/OT보안, 이젠 선택이 아닌 필수!

클래로티 코리아
김정수 지사장

2019-07-04

OT : Operational Technology (운영 기술) – 주요 구성 요소

SCADA / HMI

Analog I/O

Flow Meter
(유량계)

Pressure Transmitter
(증압기)

Temperature Transmitter
(온도 전송기)

Radar Level Transmitter
(레이더 레벨 전송기)

Valve Actuators
(밸브 작동기)

PLC

Digital I/O

VFD (Variable Frequency Drive)
(가변 주파수 드라이브)

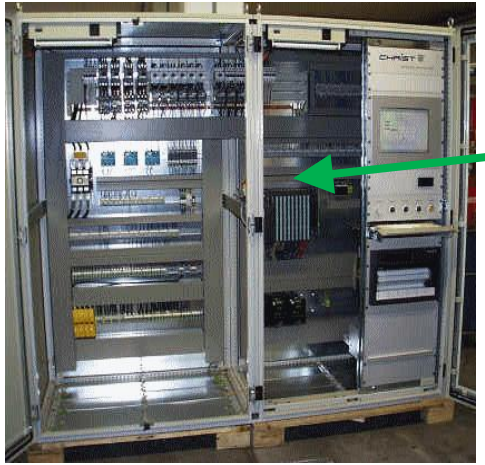
Motors
(모터)

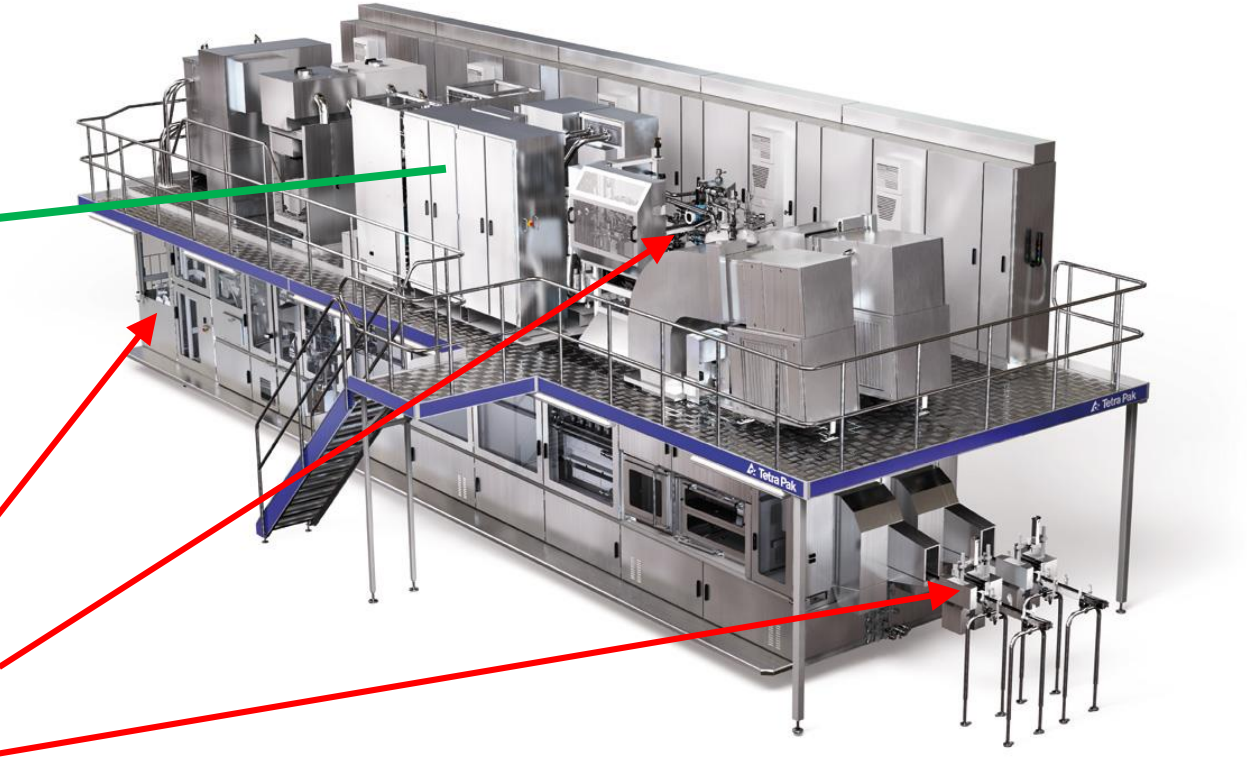
Pumps
(펌프)

Operational Technology (OT) – *the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc*.
(https://en.wikipedia.org/wiki/Operational_Technology)

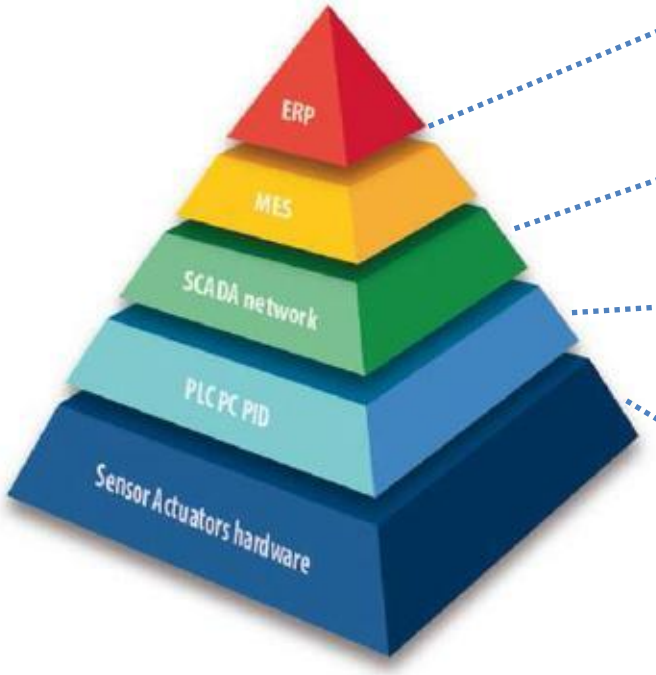
OT : Operational Technology (운영 기술) – 플랜트 개요

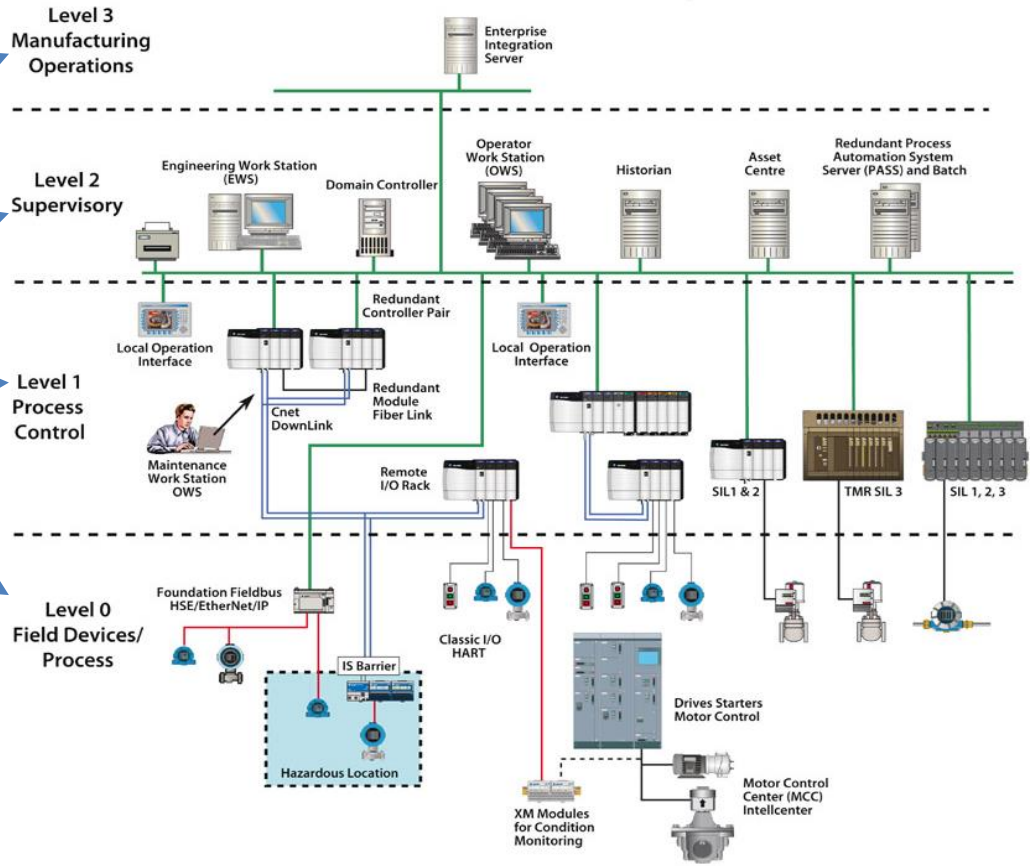
현장 제어 캐비넷





OT : Operational Technology (운영 기술) – ICS 기본 계층 구조





OT : Operational Technology (운영 기술) – ICS 주요 제조사

OT : Operational Technology (운영 기술) – ICS 제조사 주요 산업 영역

Life Is On Schneider Electric

Search

제품정보 솔루션 서비스

모든 솔루션 보기 »

파트너 ›
- Original Equipment Manufacturers
- System Integrators
- Service Providers
- Consultants, Designers & Engineers
- Connectivity Ecosystem
- Contractors
- 설치업체
- 전기장비제조업체
- SI
- Electricians
- 리셀러

For Your Business ›
- 자동차
- 클라우드 제공업체를 위한 솔루션
- 데이터센터 및 네트워크 시스템
- 전기 회사
- 해양
- 기계 제어
- 공정 자동화
- 스마트 시티
- 수처리
- 광산/철강
- 금속 산업
- 식음료 산업
- 오일 및 가스

For Your Systems ›
- 빌딩 시스템
- 전력 및 그리드 시스템
- 프로세스 시스템

EcoStruxure: Innovation At Every Level ›
- Building
- IT
- Grid
- Plant & Machine
- Power

Allen-Bradley | Rockwell Software

Rockwell Automation

산업 역량 제품 뉴스 행사 영업 및 파트너 지원

로크웰 오토메이션은 전 세계의 고객 요구에 맞춰진 산업 자동화 과제를 해결할 수 있는 전문성과 경험을 갖고 있습니다.

- 자동차
- 인프라
- 인쇄 및 출판
- 화학
- 생명 과학
- 펄프 및 제지
- 엔터테인먼트
- 선박
- 반도체
- 섬유 및 직물
- 광업, 광물, 시멘트
- 타이어 및 고무
- 식음료(F&B)
- 오일 & 가스
- 상하수도 및 폐수처리
- 가전용품 및 생활용품
- 발전

SIEMENS
Ingenuity for life

문의 Korea | 한국어

제품 및 서비스 산업별특화솔루션 한국지멘스

Search for ...

- 항공우주
- 오토모티브
- 배터리 산업
- 화학
- 시멘트
- 크레인
- 데이터센터
- 섬유산업
- 식음료
- 글래스
- 인트라 로지스틱스
- 기계 및 플랜트 건설
- 해양
- 채광
- 지역개발
- 석유&가스
- 판넬빌딩
- 제약
- 파워유틸리티
- 타이어 산업
- 운송 및 조달
- 수 처리
- 풍력 설비

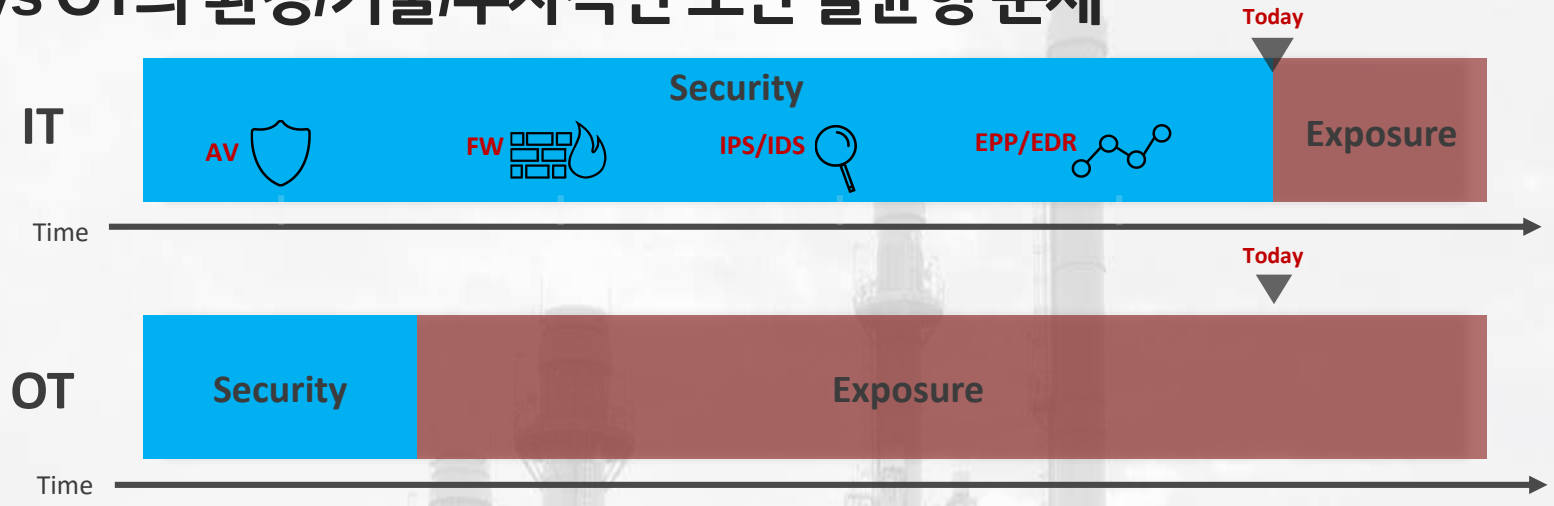
IT vs OT

IT는 CIA 우선순위
- **C**onfidentiality (기밀성)
- **I**ntegrity (무결성)
- **A**vailability (가용성)

OT는 AIC 우선순위
- **A**vailability (가용성)
- **I**ntegrity (무결성)
- **C**onfidentiality (기밀성)

항목	IT 시스템	산업제어시스템
하드웨어 및 소프트웨어	짧은 교체 주기 (3 ~ 5년)	장기간의 교체 주기 (15 ~ 20년)
	다양한 애플리케이션 및 범용 프로토콜 사용	전용 애플리케이션 및 비공개 전용 프로토콜(제어 프로토콜) 사용
	패치 등 유지·보수가 용이	패치 등 유지·보수가 어려움
	범용 OS 사용 (윈도우, 리눅스 등)	전용 OS/ 실시간 OS 사용
네트워크 성능 요구사항	전체 성능(throughput)에 초점	견고성 및 실시간 요구사항 중시
	응답의 신뢰성이 중요하며 일부 통신 지연 허용	응답 시간이 중요하며 통신 지연 불허
위험관리 목표	데이터의 무결성 중요	인간의 안전 및 시스템 가용성 중요
	일부 고장 및 장애 허용	운전 정지가 허용되지 않음
사고 영향	사고 발생 시 업무 불편 및 지연 등 상대적으로 미미한 경제적 피해 발생	사고 발생 시 산업현장 운영 중단으로 인한 인명 피해 및 대규모 물리적·경제적 피해

IT vs OT의 환경/기술/투자적인 보안 불균형 문제



초기 디자인 단계에서부터 보안/복원력을 고려하지 않았던 레거시 ICS/OT 인프라

(예 : 보안패치의 어려움)

점차적으로 연결되어가는 IT+OT 융합 환경

(예 : 생산성을 위한 공급망 통합)

지속적인 보안위협이 경고되는 크리티컬한 인프라

(예 : 전 국가적인 재난 발생 가능성)

OT 환경 피해 사례

Norsk Hydro

발생 일시: 2019. 03. 18
공격 유형: 램섬웨어(록커고가) 변종을 이용한 파일암호화
공격대상: 서버, PC 등 정보시스템
손실 비용: 약 4100만 달러 손실, 주가 3.4% 하락
영향: 전 세계 알루미늄 가격 1.3% 상승

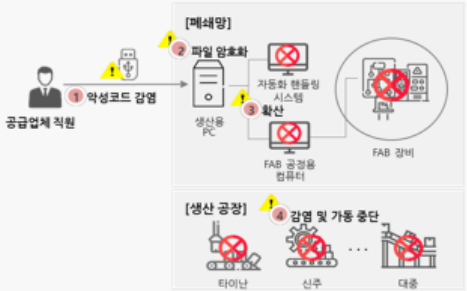
① **악성코드 감염** : 글로벌 IT 시스템 및 서버에서 이상행위가 탐지되었으며, 감염 경로는 파악 불가

② **확산** : 글로벌 네트워크를 통해 악성코드가 확산(SMB, Active Directory 이용)되었으며, 추가 확산을 막기 위해 모든 공장과 운영 네트워크를 글로벌 네트워크로부터 분리

③ **감염 및 가동 중단/수동 전환** : 감염된 시스템의 경우 백업 파일로 복구 진행, "금속 압출 공정" 가동 중단, 항시 작동되어야 하는 "전해조열 공정"의 수동 전환

TSMC

발생일시: 2018. 08. 04
공격유형: USB를 이용한 악성코드(워너크라이 변종) 유입
공격대상: 외부와 차단된 폐쇄망의 생산용 PC
손실비용: 약3000억원(연 매출 3%)
영향: 48시간 동안 공장 가동 중단으로 납품 지연 및 기업 신뢰도 ⇩



① **악성코드 감염** : 이동식 저장매체(USB)를 이용하여 바이러스 검사를 하지 않은 소프트웨어 설치, 랜섬웨어 감염

② **파일 암호화** : 랜섬웨어에 감염된 생산용 PC의 데이터 암호화/무결성 손상(읽기/쓰기/복원 불가)

③ **확산** : (회사)네트워크를 통해 급격히 확산

④ **감염 및 가동 중단** : 일부 생산 공장의 기기 1만대 이상 감염, 이틀 간 가동 중단

메드트로닉에서 만든 **인슐린 펌프에서 취약점 발견**돼 (2019.07.01)

산업용 IoT 플랫폼 솔루션에서 발견된 **7가지 제로데이 취약점** (2019.01.31)

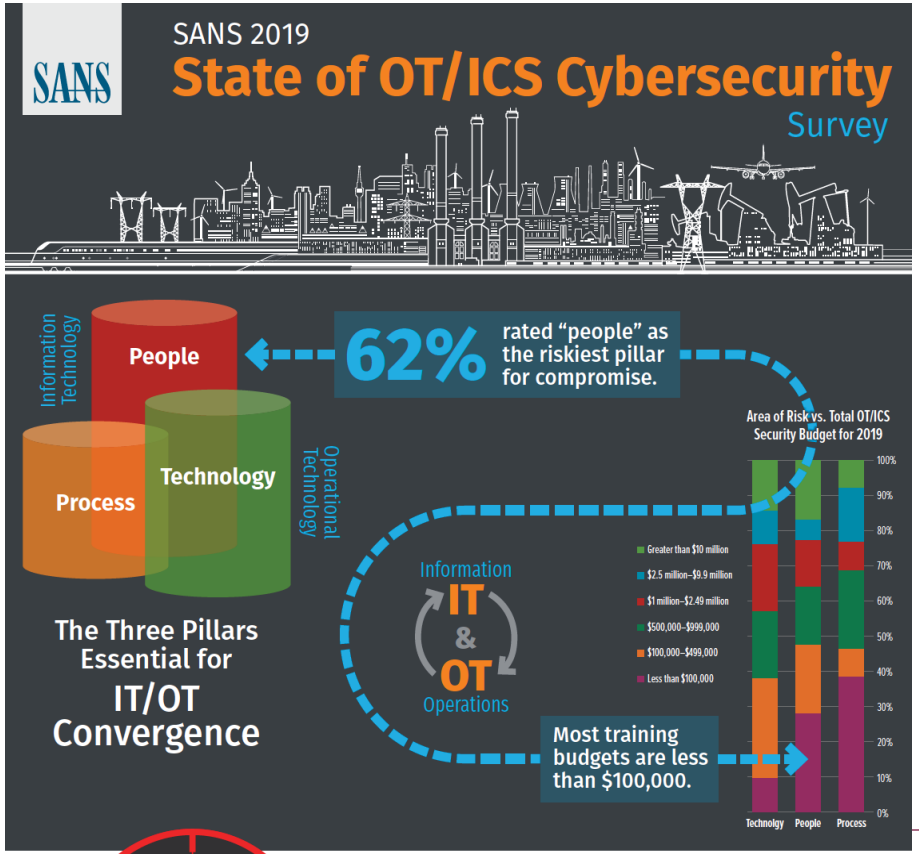
영국 브리스틀 공항, 랜섬웨어로 **부분적인 차질 생겨** (2018.09.18)

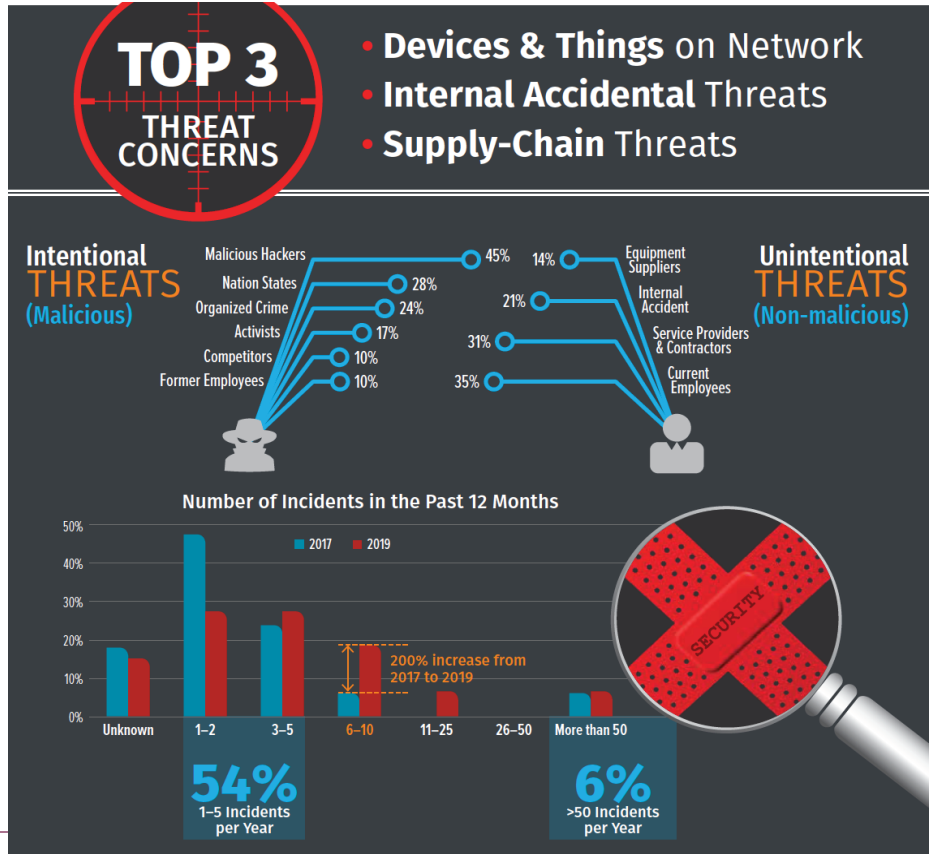
올해 상반기, **산업제어 시스템 PC 40% 이상 악성코드 감염** (2018.09.12)

정수·폐기물 처리시설 등 ICS 공격 심화되고 있다 (2018.04.24)

혼다도 당하고, 호주도 당하고...끝나지 않는 **워너크라이 랜섬웨어** (2017.06.23)

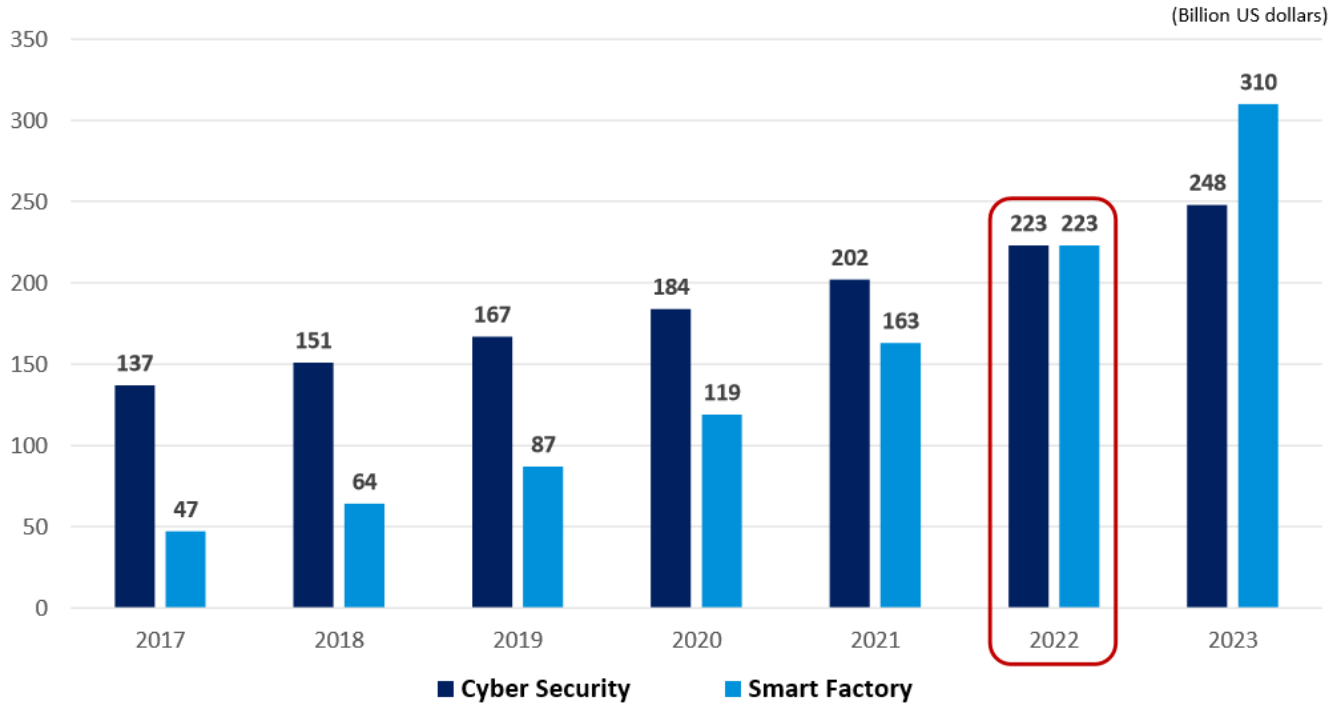
SANS 2019 – State of OT/ICS Cybersecurity Survery



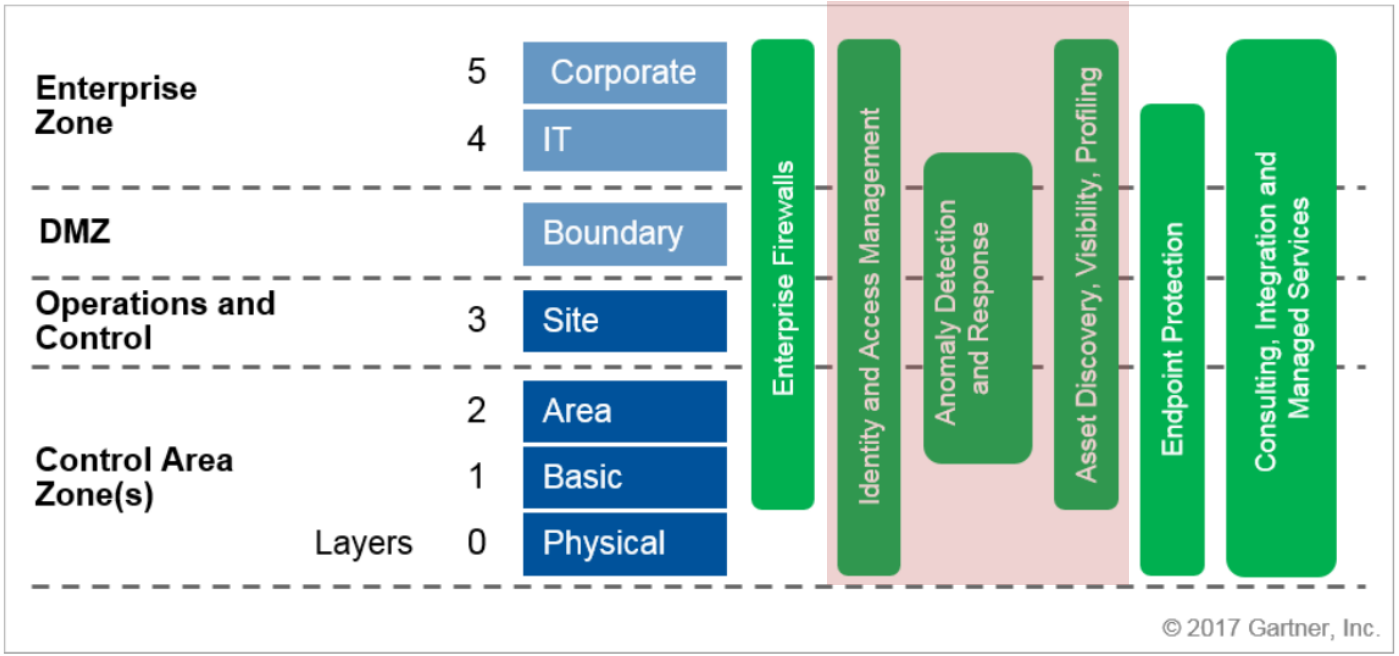


스마트팩토리 보안 시장 전망 : “New Blue Ocean”

스마트팩토리 시장은 아직 사이버 보안 시장에 비해 걸음마 단계에 불과하지만,
향후 확장성을 고려하였을 때, 스마트팩토리 보안 시장도 함께 성장할 것으로 전망



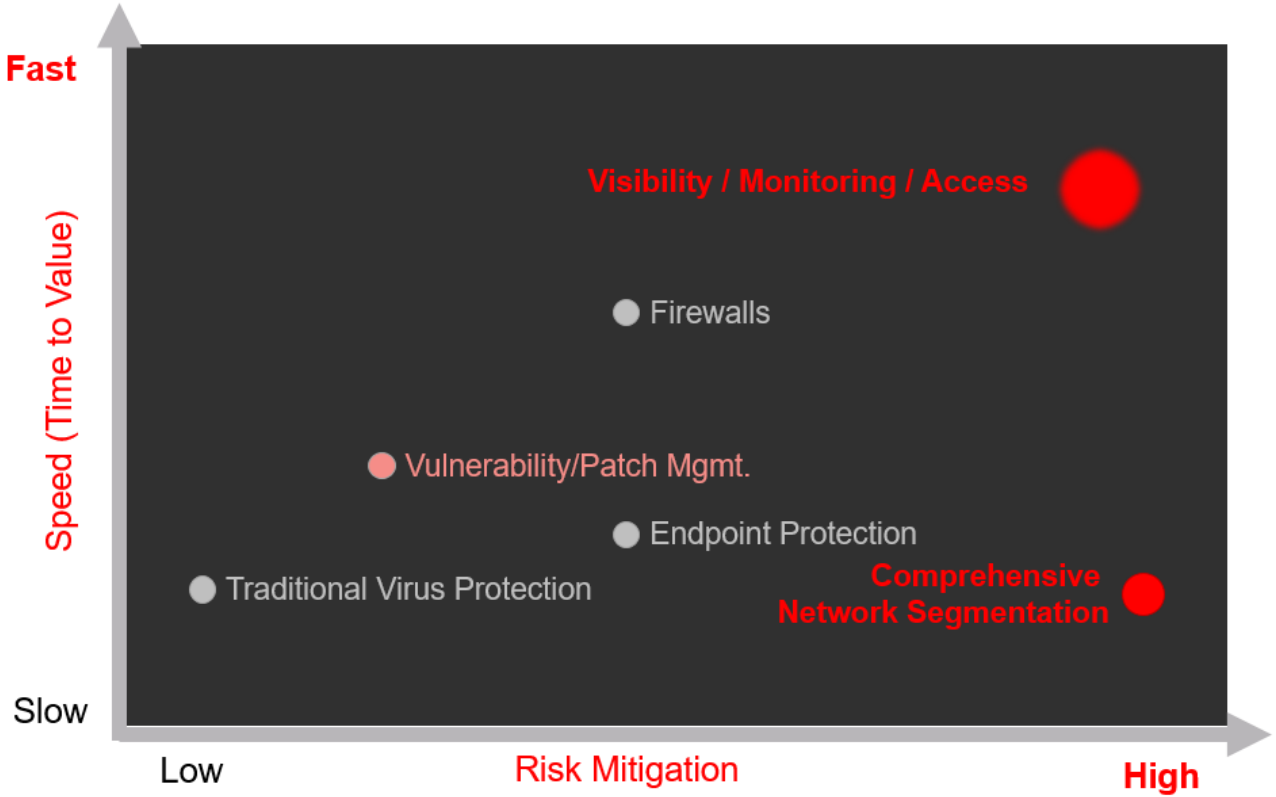
OT보안을 위해 무엇부터 먼저 해야 하는가?



DMZ = demilitarized zone; OT = operational technology

Source: Gartner (August 2017)

OT보안을 위해 무엇부터 먼저 해야 하는가? - 보안 효과가 크고 빠른 솔루션 우선 투자



OT보안을 위해 무엇부터 먼저 해야 하는가? - 보안 효과가 크고 빠른 솔루션 우선 투자

IT 영역

OT 영역

Level 4
Corporate Network

Level 3.5
IT/OT DMZ Zone

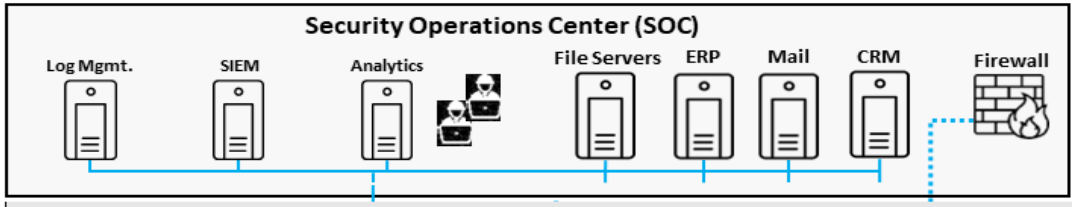
Level 3
Operations

Level 2
Process Network

Level 1
Control Network

Level 0
Field Devices I/O

Pump



- ICS/OT/IoT 관련 전문 프로토콜 이해 부족
- 해당 환경의 실시간 보안/운영 가시성 결여로 복원력 상실
- 예상 가능한 보안사고에 즉각적인 대처 불가능

"가시성이 없는 네트워크를 보호하는 것은 불가능하다"

OT 환경에 대한
완벽한 가시성 확보 필요

클래로티(Claroty) 회사 현황

- **ICS/OT 산업보안 전문회사로 2014년 설립 (본사 : 뉴욕)**

- **투자/펀딩 : 9천9백만 달러**
  경쟁사 대비 2~4배 많은 투자/펀딩 금액으로
  R&D 및 산업보안 전문솔루션 개발에 집중할 수 있는 건전한 투자구조

- **주요 투자사 현황** (ICS/OT 및 산업자동화 솔루션 메이저 제조사가 투자/펀딩)

BESSEMER VENTURE PARTNERS
TEMASEK
Rockwell Automation
Schneider Electric
SIEMENS
BMW i VENTURES
CLEARVISION VENTURES
ICV
TEKFEN
evergy ventures
INNOVATION ENDEAVORS
REdD OT
MITSUI
TEAM8 Rethinking Cyber

- **주요 수상 내역**

Gartner

Cool Vendors in Smart City Application Solutions 2016

RSAC Innovation Sandbox 2017 FINALIST

RSAC 2017 Innovation Sandbox Highlights
Top 10 Cyber Startups

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

Finalist in the Best Cybersecurity Startup

SA x18

Winner
ICS Threat Detection Challenge

WSJ Tech Companies to Watch 2018

Top 25 Tech Companies
to Watch 2019

FROST & SULLIVAN

2019 North American OT Network Protection Platform:
Entrepreneurial Company of the Year

클래로티(Claroty) 적용 주요 산업군

4차 산업혁명 및 디지털 트랜스포메이션을 위한 *시큐어* 스마트팩토리 / 스마트시티 / 스마트빌딩 등 다양한 산업군으로 확장 중

수자원 개발,
식수/폐수/수질 관리

오일/가스/에너지

광업/철강

농화학

해양 시추/플랜트

식음료(F&B)

제조

데이터센터/
빌딩관리시스템
(BMS)

전기/발전소

자동차/오토모티브

헬스케어/제약/바이오

풍력 발전/
친환경 에너지

정부/공공

유통/리테일/물류

글로벌 클래스의 ICS/OT 연구분석팀 보유

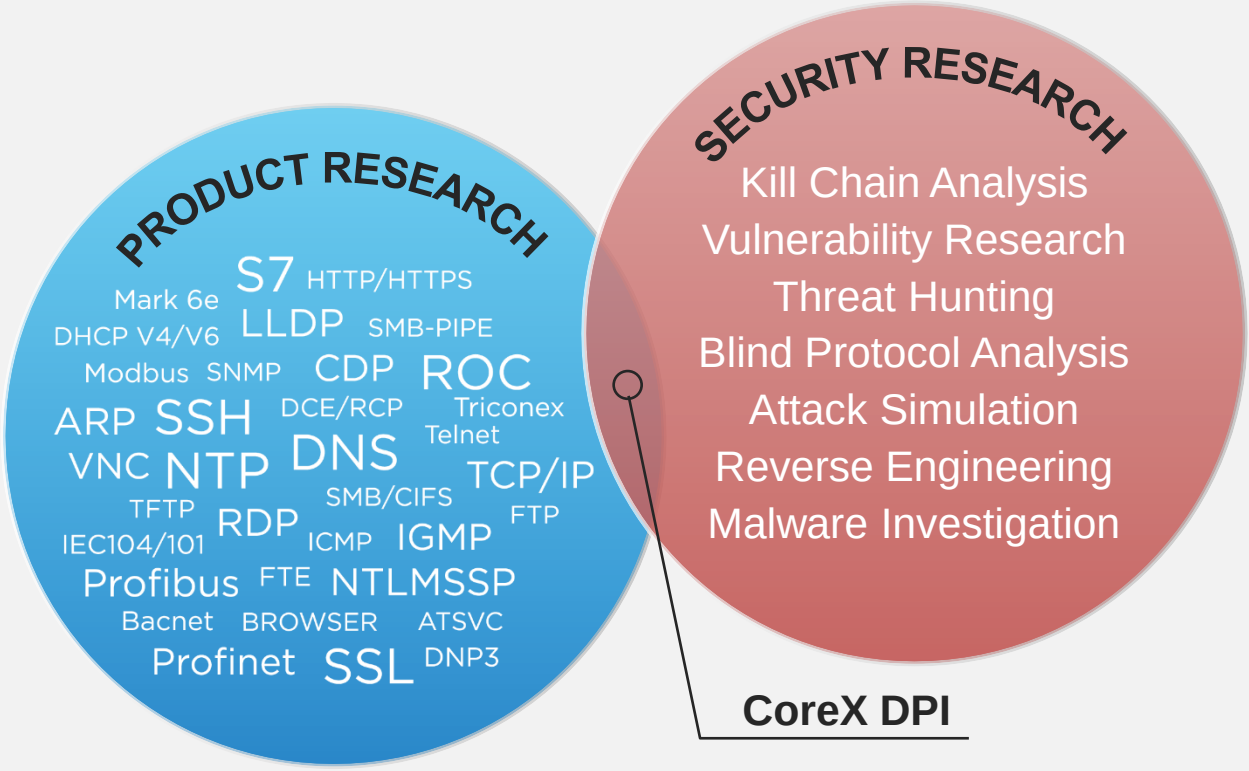
머신러닝 기반 CoreX DPI 기술을 통해 업계 가장 폭넓은 ICS/OT 프로토콜을 지원

TEAM 82

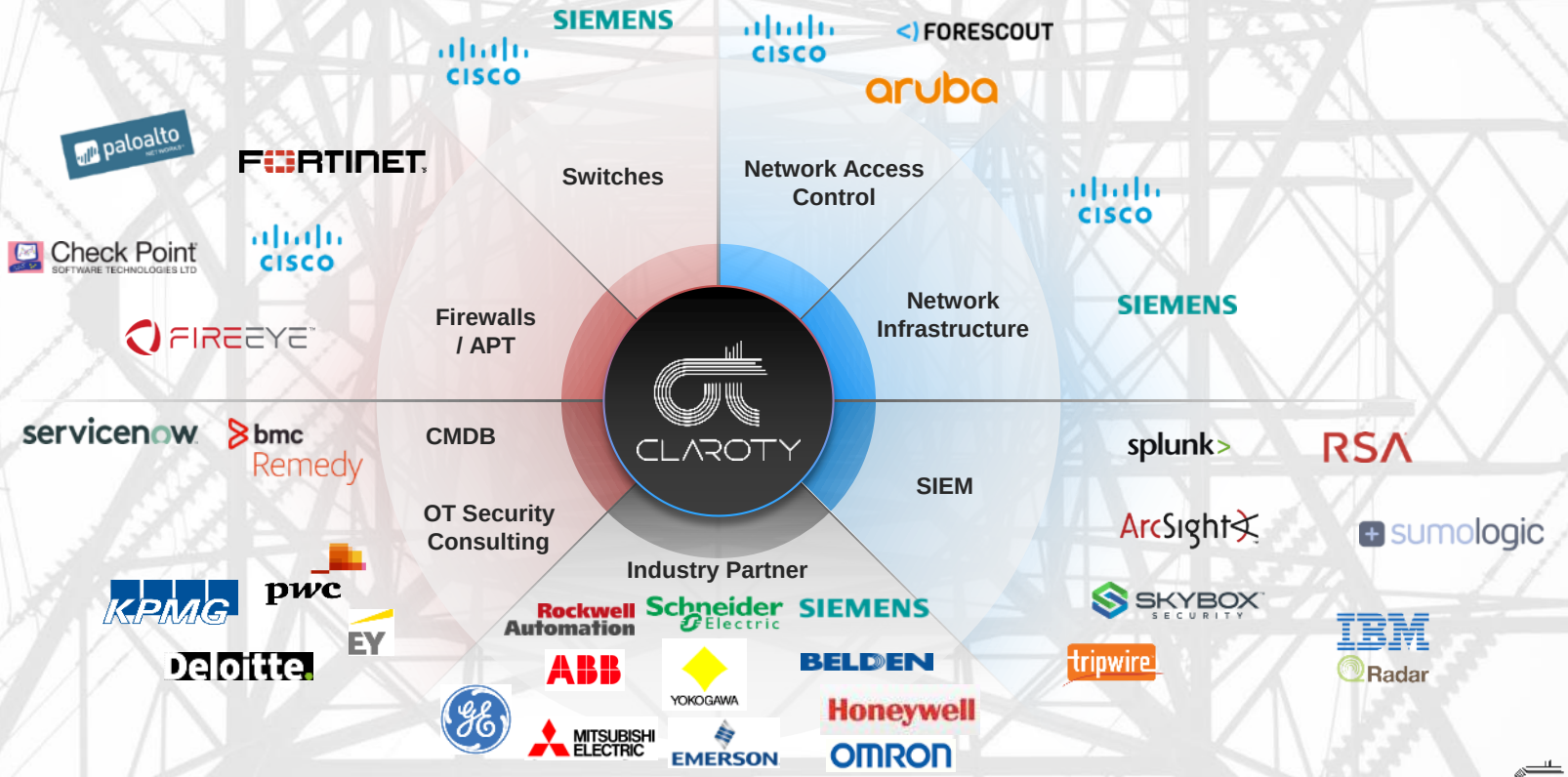
$5M
Research Lab

90+
Supported Protocols

50+
Researchers & Analysts



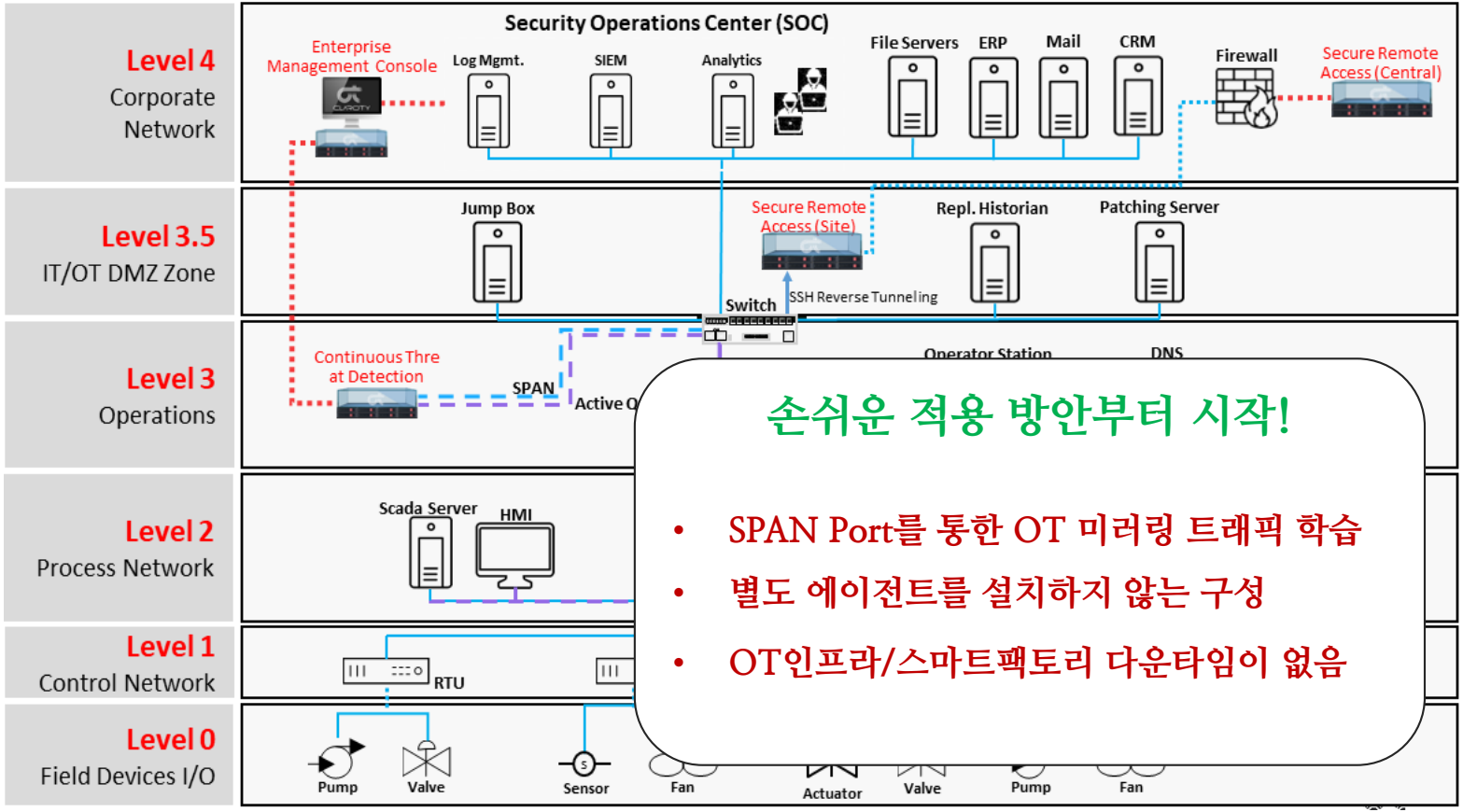
커넥티드 IT+OT 융합 환경의 통합보안을 위한 파트너 에코시스템



OT 환경의 가시성 확보를 위한 클래로티 적용 방안

IT 영역

OT 영역



손쉬운 적용 방안부터 시작!

- SPAN Port를 통한 OT 미러링 트래픽 학습
- 별도 에이전트를 설치하지 않는 구성
- OT인프라/스마트팩토리 다운타임이 없음

0. OT 구성요소의 계층별 연결관계 및 토폴로지 시각화

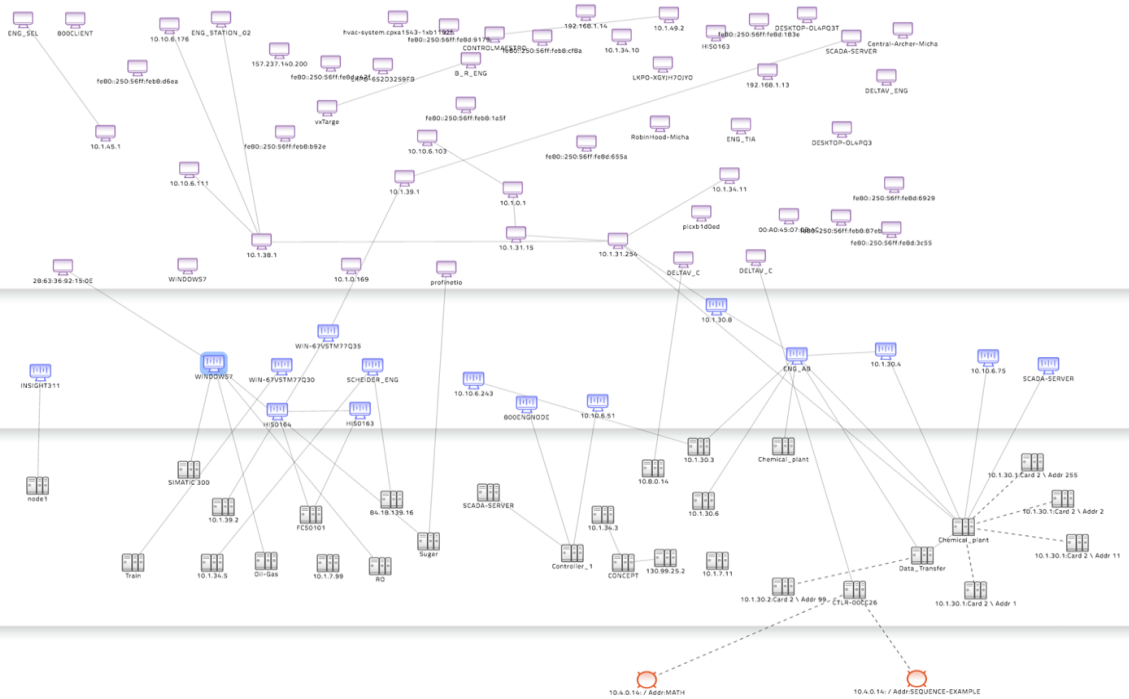
Level 4: Enterprise Zone (IT Domain)

Level 3: Site Manufacturing Operations & Control

Level 2: Supervisory Control DCS/SCADA

Level 1: Basic Control

Level 0: Process Device I/O



1. OT 구성요소의 Active한 자산정보 프로파일링

DEVICE INFORMATION

IP
10.2.0.1

MAC
00:50:56:B8:2E:7F
00:50:56:B8:DC:91

Network
Default

VLAN
N/A

Protocols
RPC

Hostname
DIGSI-ENG-04

Site
Default

Vendor
VMware, Inc.

OS
Windows 7/Server 2008 R2

OS Build
7601

Model
VMware Virtual Platform

Serial
VMware-42 38 19 24 b6 37 76 c6-c1 94 c5 2a 17 c1 df 87

MORE DETAILS

Type
ENGINEERING STATION

Criticality
MEDIUM

Information

Virtual Zone
Engineering Station: Other

Risk Level
Normal

Assigned Active Queries
WMI Digsi

Discovered By
Ping Sweep - SELs and Digsi

First Seen
05/02/19 20:13

Last Seen
05/02/19 20:13

Role
Siemens Engineering Station

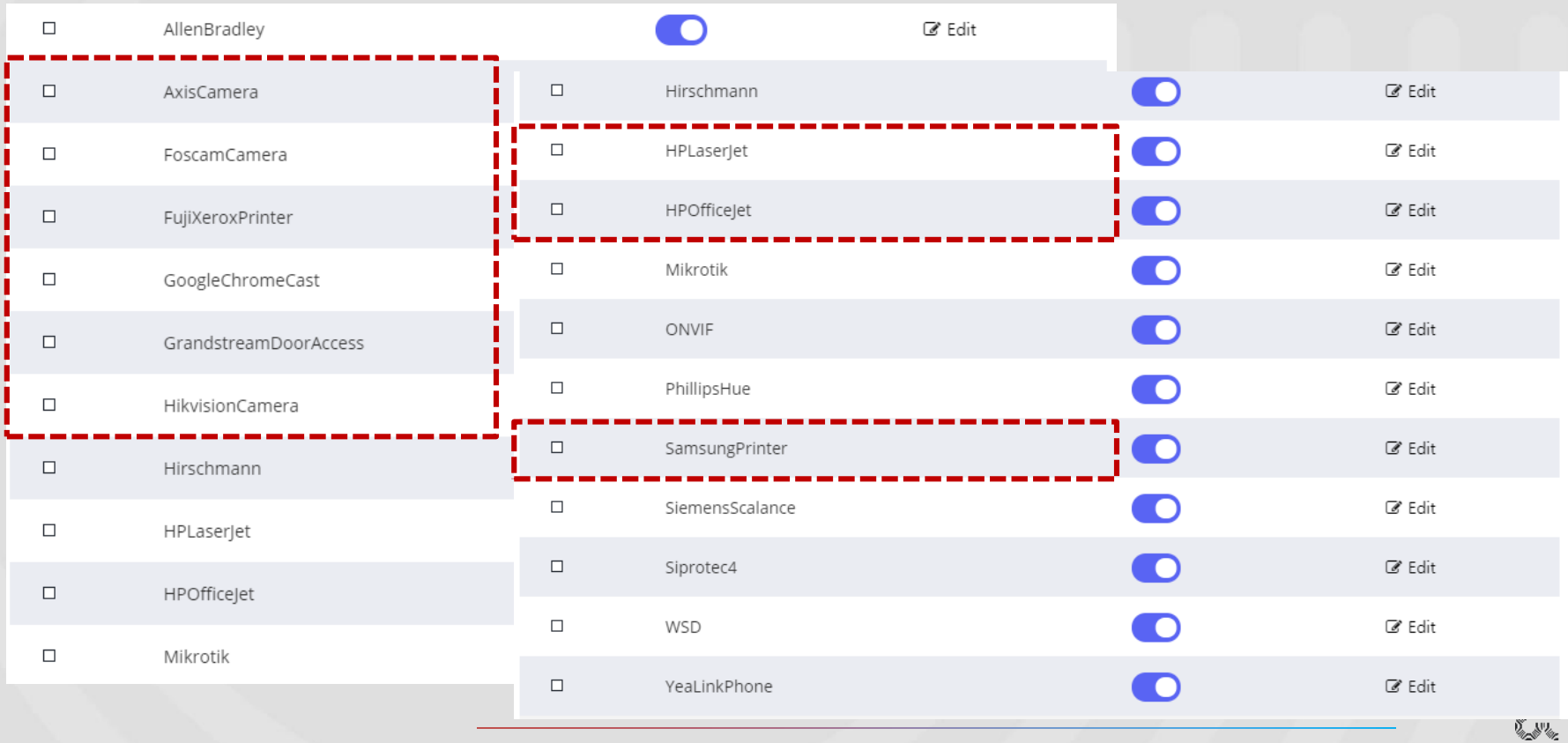
Last Program Installed Date
2019-02-03 (Google Update Helper)

Logged On User
DIGSI-ENG-04\User

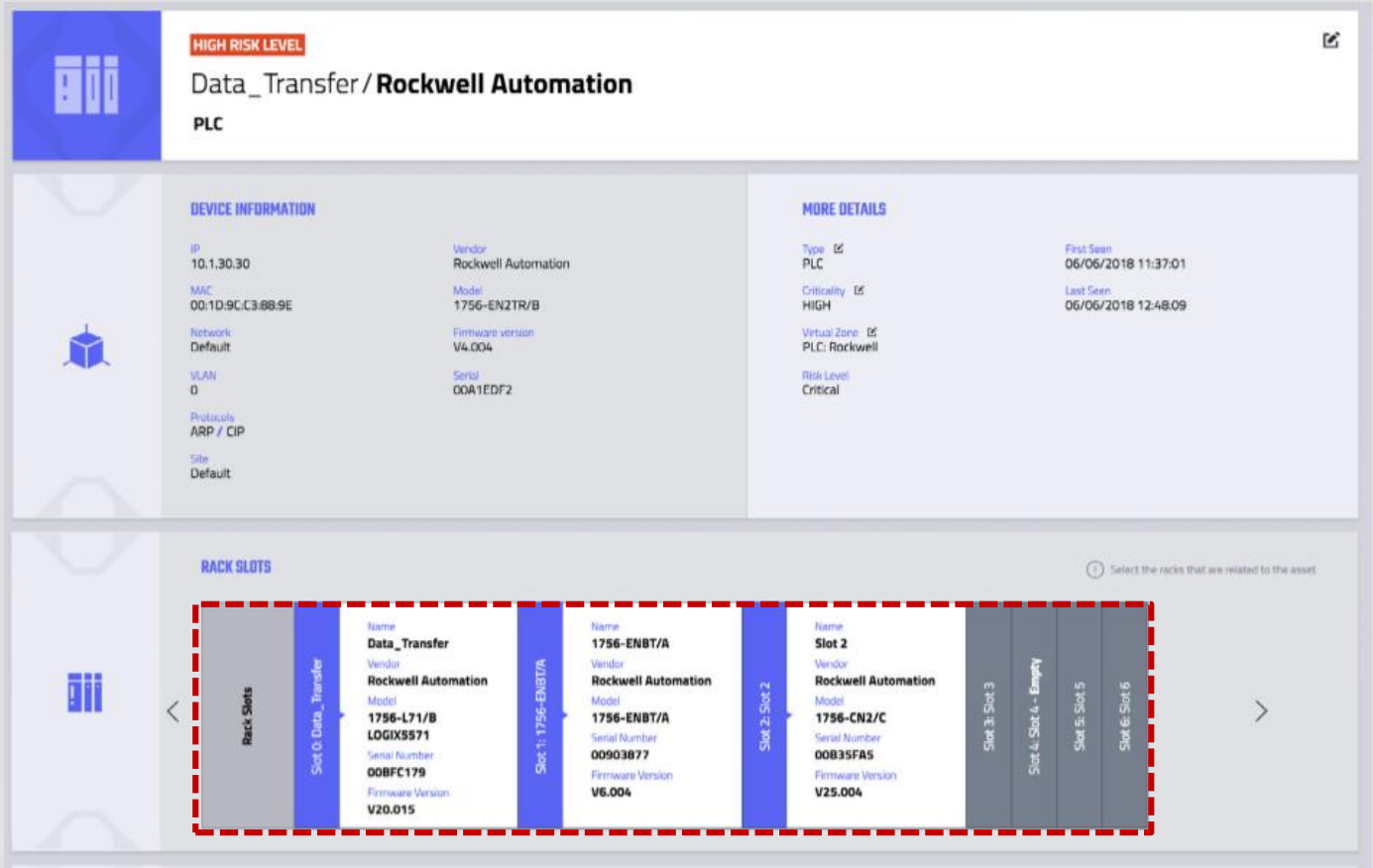
Windows Serial
00392-918-5000002-85968

Windows Edition
Microsoft Windows 7 Enterprise

2. IIoT(Industrial IoT) 장비에 대한 자산정보 및 이력 관리



3. 시리얼 I/O 통신 장비에 대해서도 자산정보 관리 및 가시성 제공



4. OT환경 위협 탐지를 위한 Yara Rule 및 Snort 기반 시그니처 지원

Active	Name	Time of Creation	System Rule	Options
☐	RANSOM_locdoor.yar	04/07/19 07:48	✓	
☐	ics_cert_hatman.yara			
☐	RANSOM_Anatova.yar			
☐	RANSOM_CTBLocker.yar			
☐	RANSOM_jeff_dev.yar			
☐	triton_claroty.yara			
☐	RANSOM_BadRabbit.yar			
☐	RANSOM_SamSam.yar			
☐	RANSOM_Shiva.yar			
☐	RANSOM_Ryuk.yar			

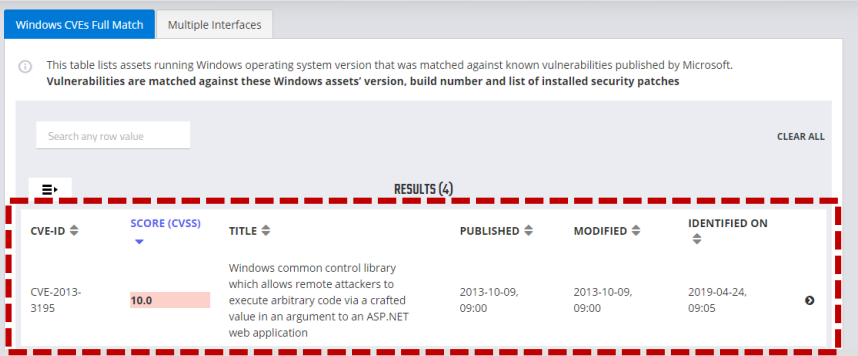
RESULTS (8,484)

Active	Name	Time of Creation	System Rule	Options
☐	ET CURRENT_EVENTS Bleeding Life 2 GPLed Exploit Pack payload download	19/05/19 19:50	✓	
☐	ET CURRENT_EVENTS Redkit Java Exploit request to /24842.jar	19/05/19 19:50	✓	
☐	ET CURRENT_EVENTS Fragus Exploit jar Download	19/05/19 19:50	✓	
☐	ET CURRENT_EVENTS Possible Sakura Exploit Kit Version 1.1 document.write Fake 404 - Landing Page	19/05/19 19:50	✓	
☐	ET CURRENT_EVENTS Sakura Exploit Kit Version 1.1 Applet Value lxxt	19/05/19 19:50	✓	
☐	ET CURRENT_EVENTS NuclearPack - JAR Naming Algorithm	19/05/19 19:50	✓	
☐	ET CURRENT_EVENTS NuclearPack - Landing Page Received - applet archive=32CharHex	19/05/19 19:50	✓	
☐	ET CURRENT_EVENTS DRIVEBY Incognito Landing Page Requested .php? showtopic=6digit	19/05/19 19:50	✓	

5. 최신 패치/펌웨어 적용 여부 및 설치된 애플리케이션/파일 감지

IOT 자산에
설치된 파일/프로그램 감지

OT 자산에 대한
보안취약점 인텔리전스 제공
(CVE 매칭)



OT 자산의
최신 보안패치 적용 여부 감지

6. 발견된 보안취약점을 기반으로 OT네트워크의 잠재적인 위협 시뮬레이션

ATTACK CHAIN

Gained control on selected Asset:

PLC 10.1.30.4:

- Is affected by Remote Code Execution CVEs published in the last 2 years.
- Is affected by multiple CVEs.

1 **Vulnerability used:**
ENG_AB has a Remote Code Execution vulnerability that can be exploited. Windows kernel in Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and RT 8.1, Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016, and Windows Server, version 1709 allows an attacker to log in and run a specially crafted application due to the Windows kernel improperly initializing a memory address

EngineeringStation ENG_AB:

- Uses the following unsecured protocols: SMB.
- Is affected by Remote Code Execution CVEs published in the last 2 years.
- Is affected by multiple CVEs.

2 **Vulnerability used:**
ENG_AB has executed privileged commands on Chemical_plant using CIP allowing full control over it.

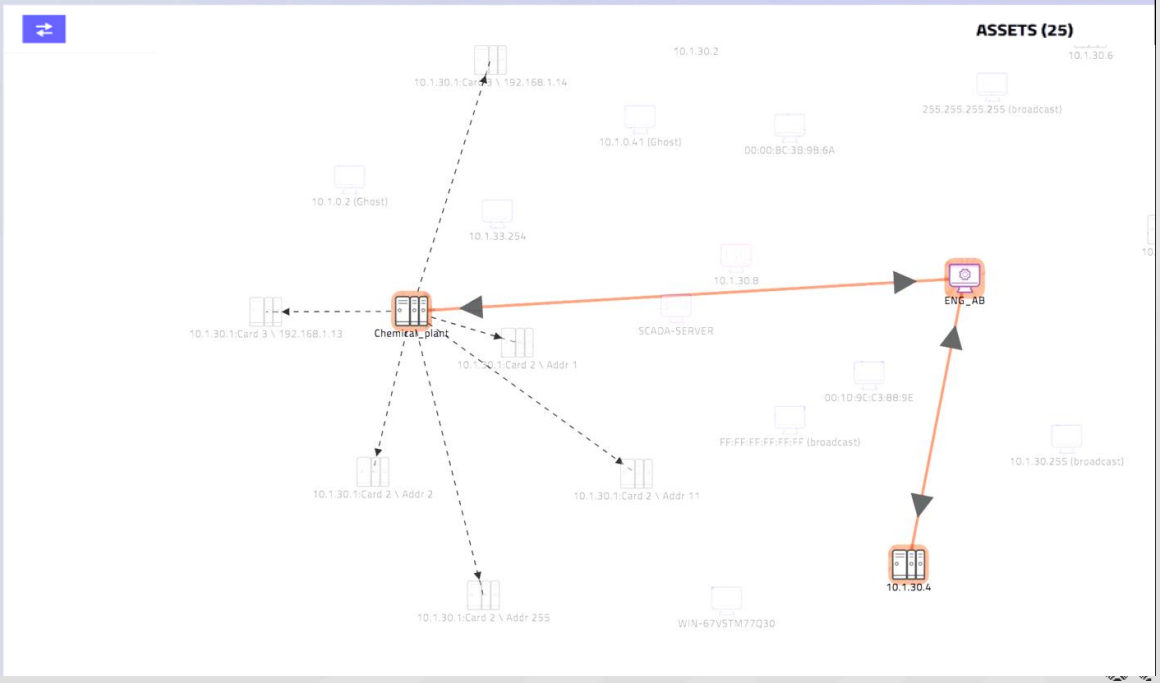
PLC Chemical_plant:

- Has privileged commands executed on it by 3 other assets other assets.
- Is affected by Remote Code Execution CVEs published in the last 2 years.
- Is affected by multiple CVEs.

ATTACK VECTOR

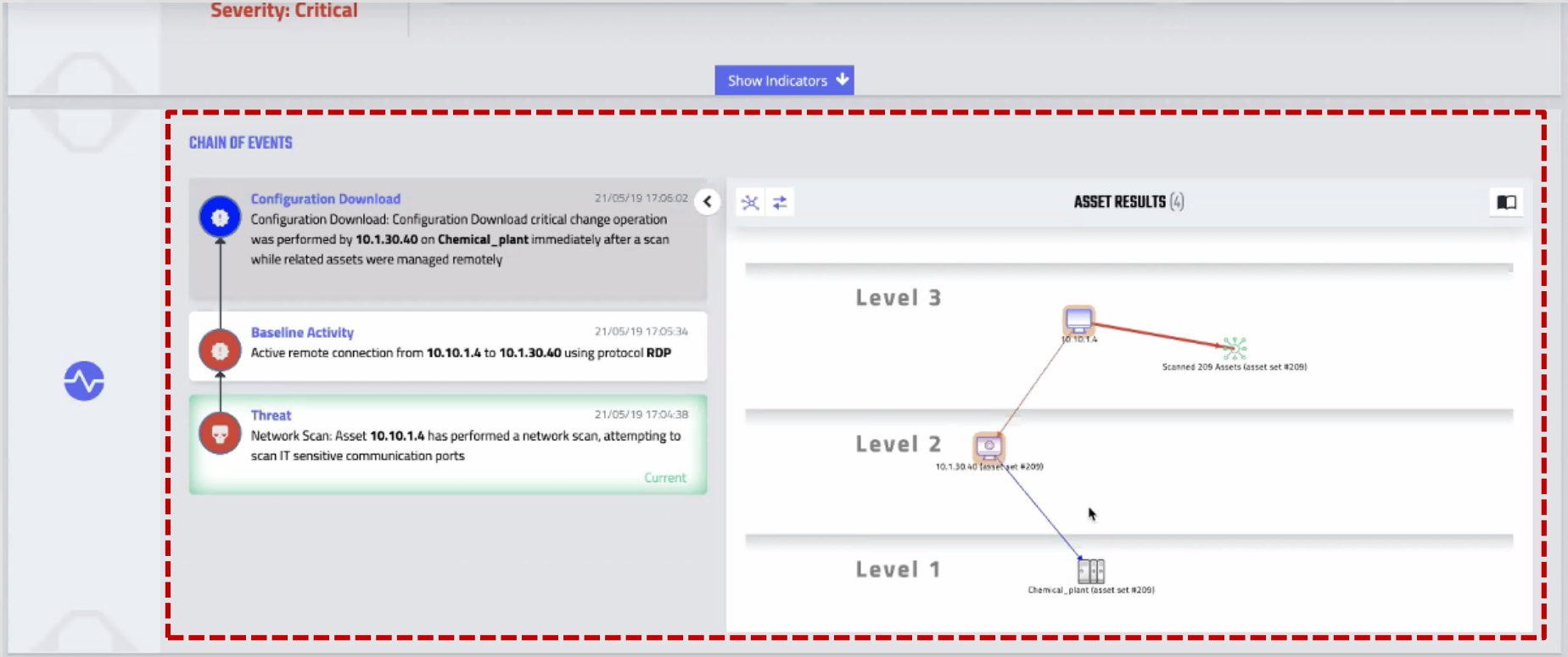
Source Asset: 10.1.30.4, E4:90:69:A7:70:0F

Destination Asset: Chemical_plant, 10.1.30.1, 00:1D:9C:C0:04:9D



7. 사이버 킬체인 방식의 Root Cause Analytics 지원

스토리보드 기반의 실시간 이상징후 포착, 선제적인 위협 헌팅 및 상관분석



8. OT구성요소간 데이터플로우 자동 분석을 통한 마이크로 세그멘테이션

- 베이스라인에 위배되는 이상징후/비정상 행위 감지
- OT환경을 위한 방화벽 정책 적용에 활용, Later Movement Attack 대응 가능

이상적인 OT네트워크 세분화 전략 제시

POLICY RULES

VIEW TYPE

7 Rules to validate

Source Zone: Select zone... | Destination Zone: Select zone | Protocols: Select protocol | Category: Select category | Access Type: Select access type | Search By: Search description, asset, action...

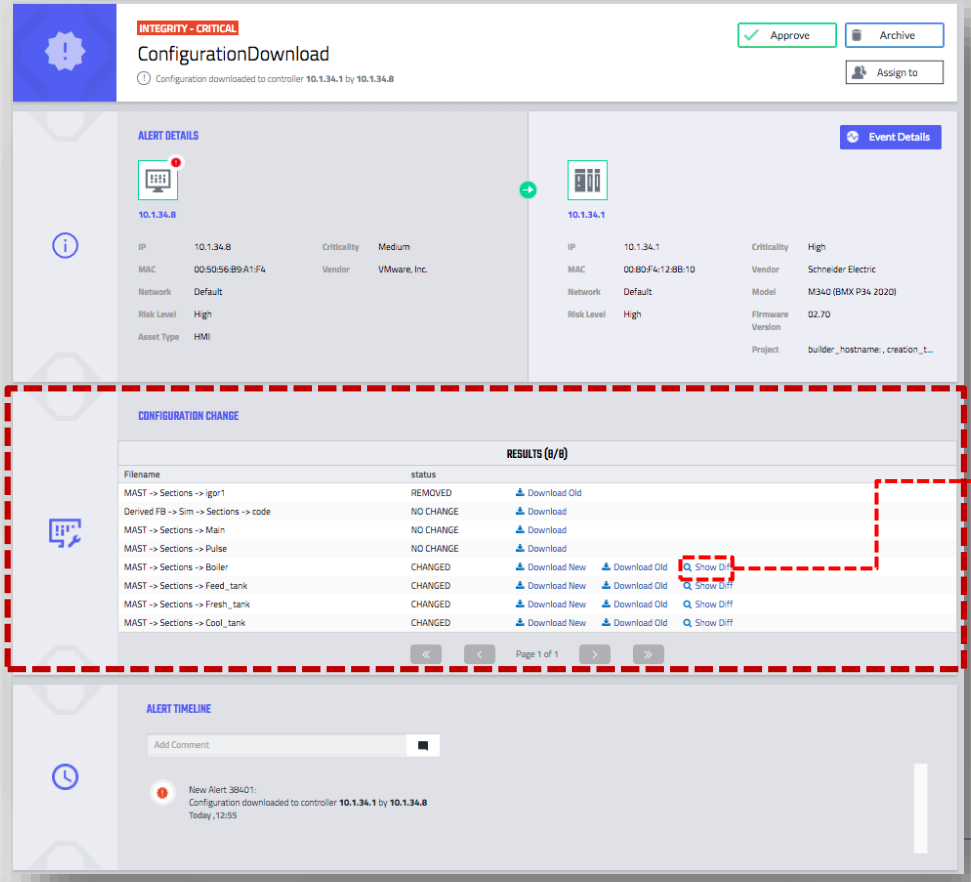
CLEAR ALL | QUERY VIEW | ADVANCED OPTIONS»

RESULTS (119)

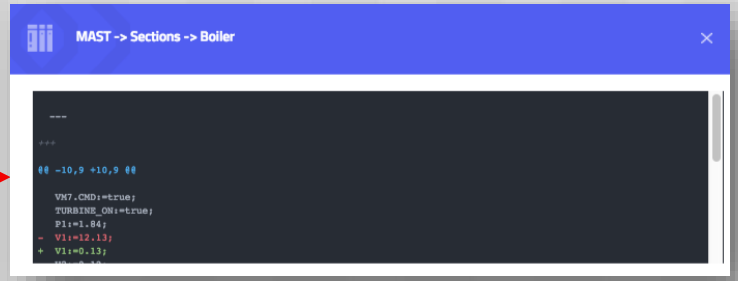
1 2 3

ID	ACTION	SOURCE ZONE	DESTINATION ZONE	PROTOCOLS	PORTS	CATEGORY	ACCESS	EXACT MATCH	DESCRIPTION	HIT COUNT	VALIDATED
35	Allow	SCADA Client: CITECT (1)	SCADA Server: CITECT (1)	CITECT	2080, 2082 ...	Data Acquisition, Alarm ...	Read	No	aaaa	42	Validated
36	Alert	SCADA Client: CITECT (1)	SCADA Server: CITECT (1)	CITECT	2082	Data Acquisition	Write	No		8	Validate
37	Allow	SCADA Server: CITECT (1)	SCADA Client: CITECT (1)	CITECT		Data Acquisition	Publish	No		47	Validated
67	Allow	Engineering Station: DELTA-V (1)	Controller: DELTA-V (1)	DELTA-V	18507	Protocol, Other	None	No		3	Validated
68	Allow	Controller: DELTA-V (1)	Engineering Station: DELTA-V (1)	DELTA-V		Other	None	No		1	Validated
69	Allow	Engineering Station: DELTA-V (1)	Controller: DELTA-V (1)	DELTA-V	18507	Data Acquisition, Programming ...	Read	No		4	Validated
70	Allow	Controller: DELTA-V (1)	Engineering Station: DELTA-V (1)	DELTA-V	18507	Alarm, Data Acquisition	Publish	No		5	Validated

9. OT 명령어/설정값 변경 인식 및 비교 관리



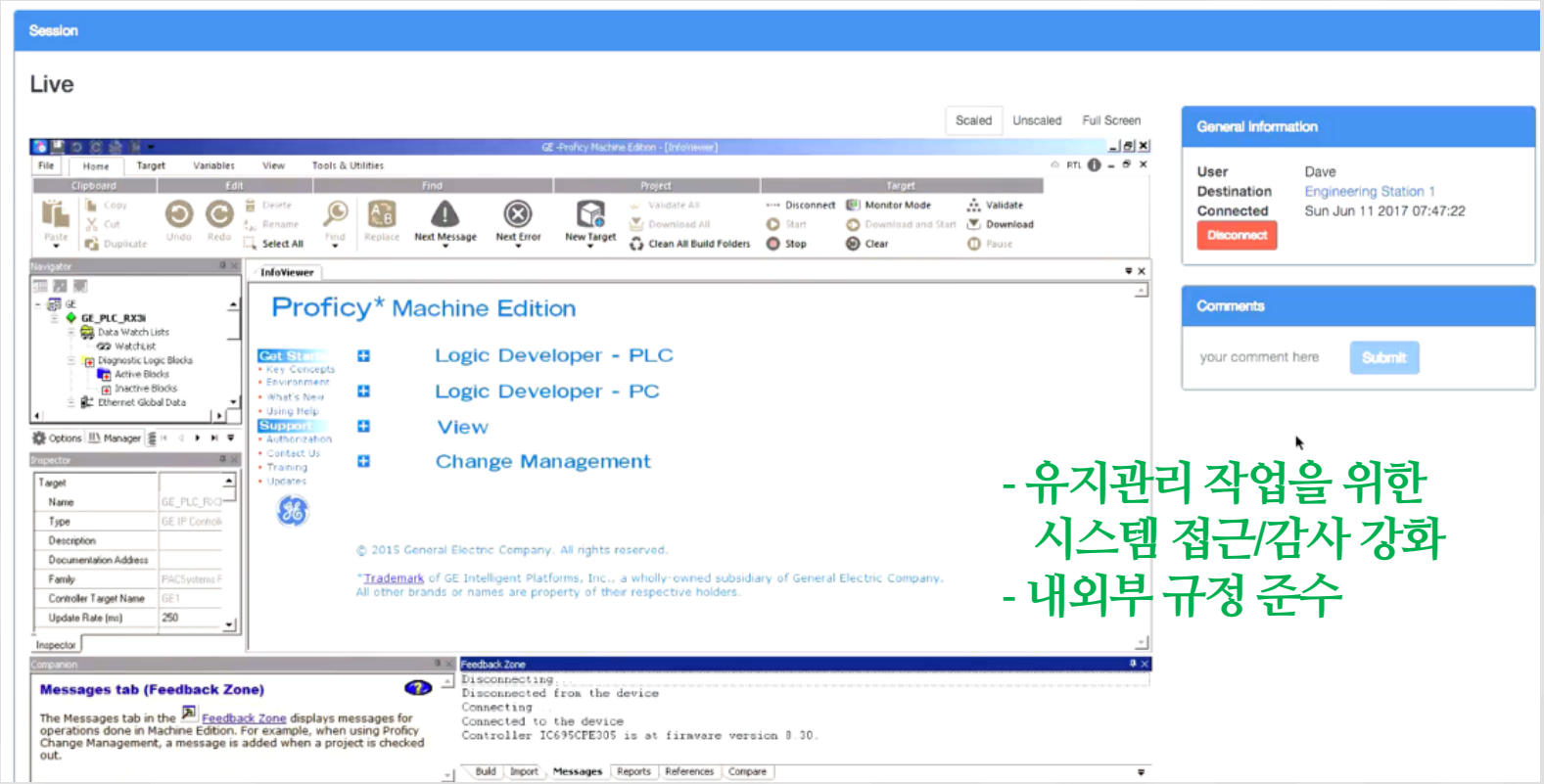
예) PLC의 설정값 변경 내역 제공
(변경 전/후 비교)



OT 운영 요소들의 실시간 상황 변화 인식을 기반으로 한 변경 관리

10. OT 인프라의 신속한 유지관리를 위한 안전한 원격 접속 제어

- 내부인원/관련부서 및 협력사를 통한 협업/유지관리 작업시, 위험 요소 제거
- 접속 작업 행위/내역에 대해서 동영상 녹화/저장 지원



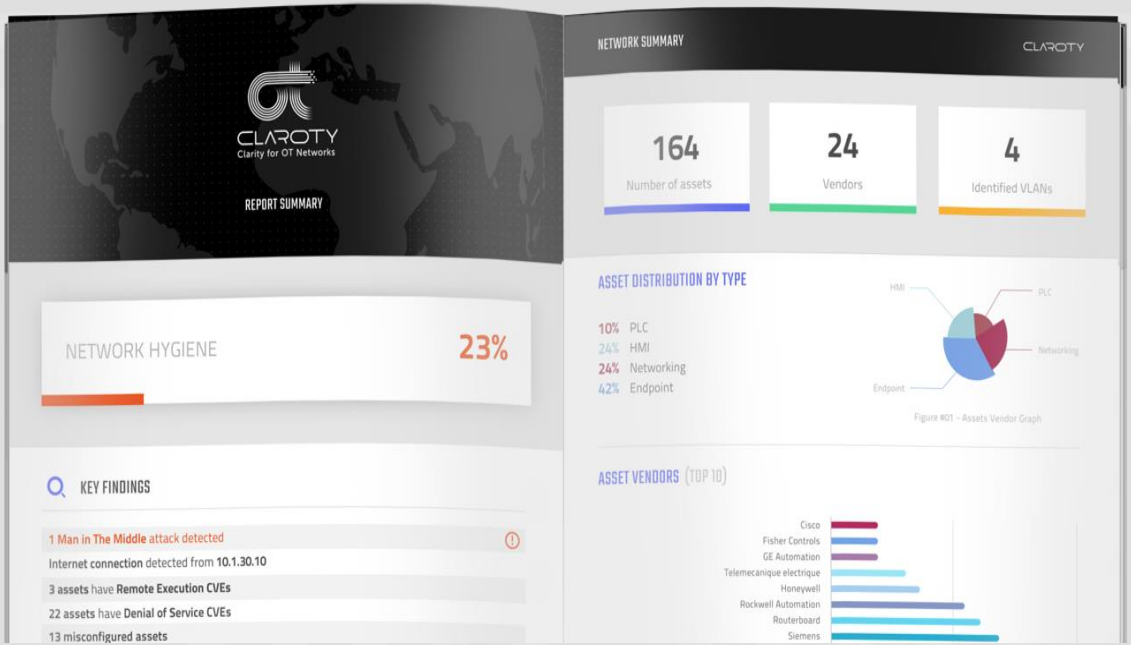
- 유지관리 작업을 위한 시스템 접근/감사 강화
- 내외부 규정 준수

OT 네트워크의 안전도 상태 점검 : 헬스체크 서비스

Security Posture Assessment for ICS/OT Network

- 현재 운영 중인 ICS/OT 자산 정보
- ICS/OT 구성 요소의 네트워크 분석
- 해당 자산 및 구성 요소들의 보안적인, 운영적인 취약점 분석
- ICS/OT 인프라의 안전도 상황 등

고객사 OT 구간의 PCAP 파일을 통해 클래로티(Claroty) 전문연구원이 분석 및 리포트



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)

CLAROTY

Bringing Clarity to OT Networks

감사합니다

클래로티 코리아
문의처 : daniel.k@claroty.com