포티넷 시큐리티 패브릭 기반의

OT/ICS/SCADA 인프라 보호 전략

Senior BDM / OT

문귀 전무 / NeoMoon@fortinet.com

AGENDA

1 OT & 보안 위협 동향

2 포티넷과 ICS 벤더사와 협업 사례

3 포티넷 OT 보안 아키텍처와 구축 예시

4 OT/ICS/SCADA 인프라 보호 제안

5 OT 보안 취약성 방어 데모

용어 설명 : OT/ICS/SCADA

OT : 운영 기술 (Operational Technology)

- 산업운영을 관리하는 컴퓨팅 시스템을 의미하며 IoT, 무선, 엣지컴퓨팅 등 생산관리, 운영통제 및 모니터링 포함

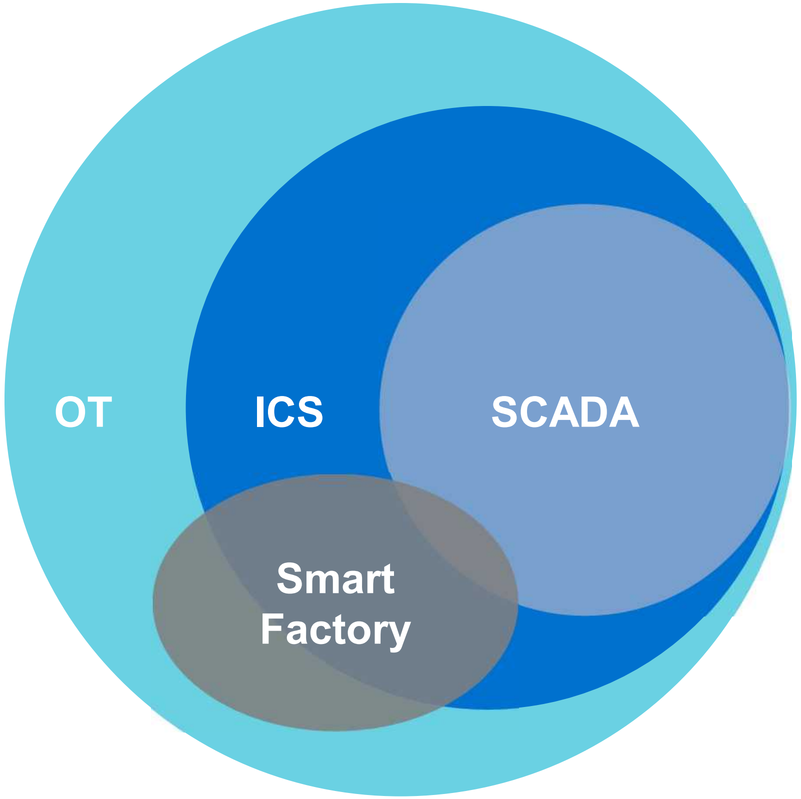
ICS : 산업 제어 시스템 (Industrial Control System)

- 산업 프로세스를 제어하는 운영기술 시스템으로 제조업의 생산 및 DCS, MES, ERP 와 기반시설 산업시스템 등 포함

SCADA : SCADA(Supervisory Control and Data Acquisition)

- 현장의 상태 및 정보를 PLC나 원격 접속장비로 수집하며, 원격지에서 모니터링, 분석, 제어하여 설비를 운용하는 시스템

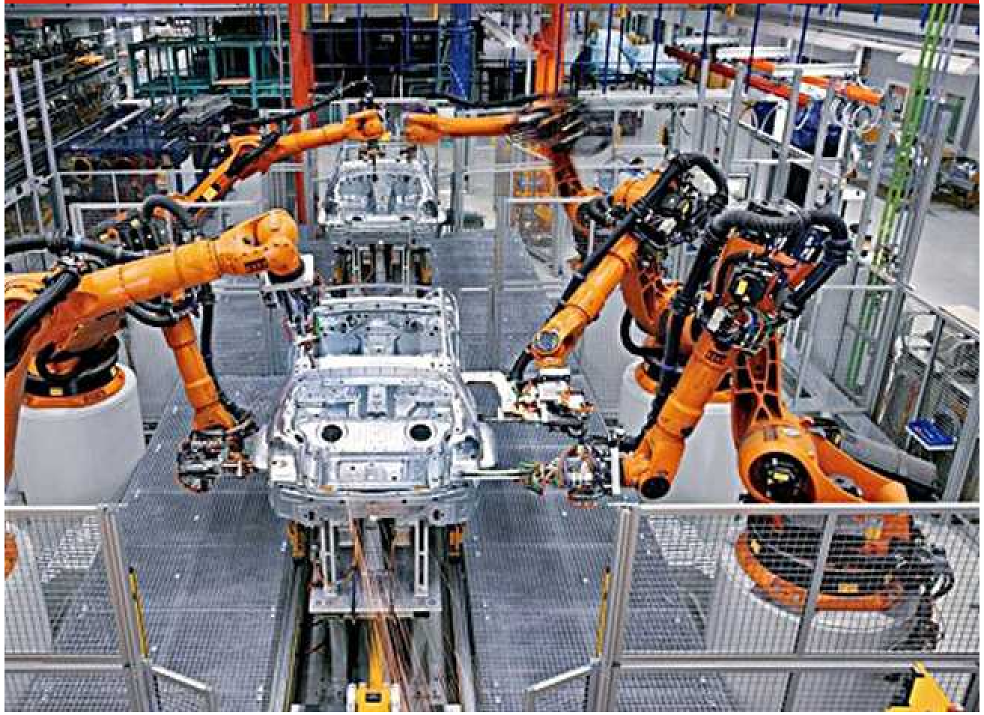
OT security is "*practices and technologies used to protect people, assets and information, monitor and/or control physical devices, processes and events, and initiate state changes to enterprise OT systems*" **-Gartner -**



Operational Technology (OT): Used For

감시, 제어, 운영

산업 자동화



FORTINET

© Fortinet Inc. All Rights Reserved.

Operational Technology (OT)

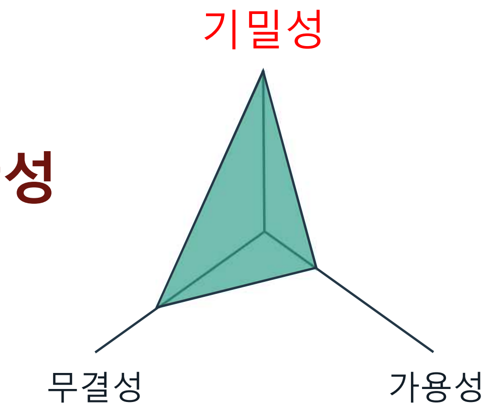
적용 분야

다양한 산업시설
기반시설, 스마트 펙토리 등에서 사용됨

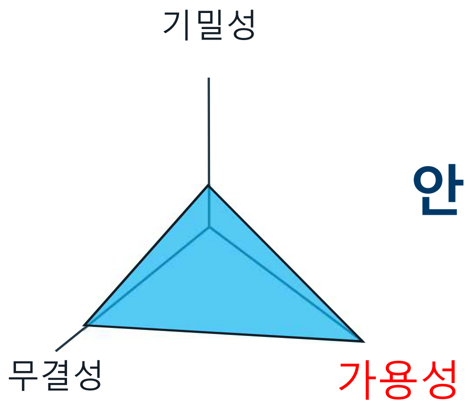
다양한 환경 조건에서 운영됨
가혹한 환경 (온도, 습도, 진동), 공장 & 데이타센터

IT 와 OT의 보안은 어떻게 다른가?

보안성



IT vs OT



안정성

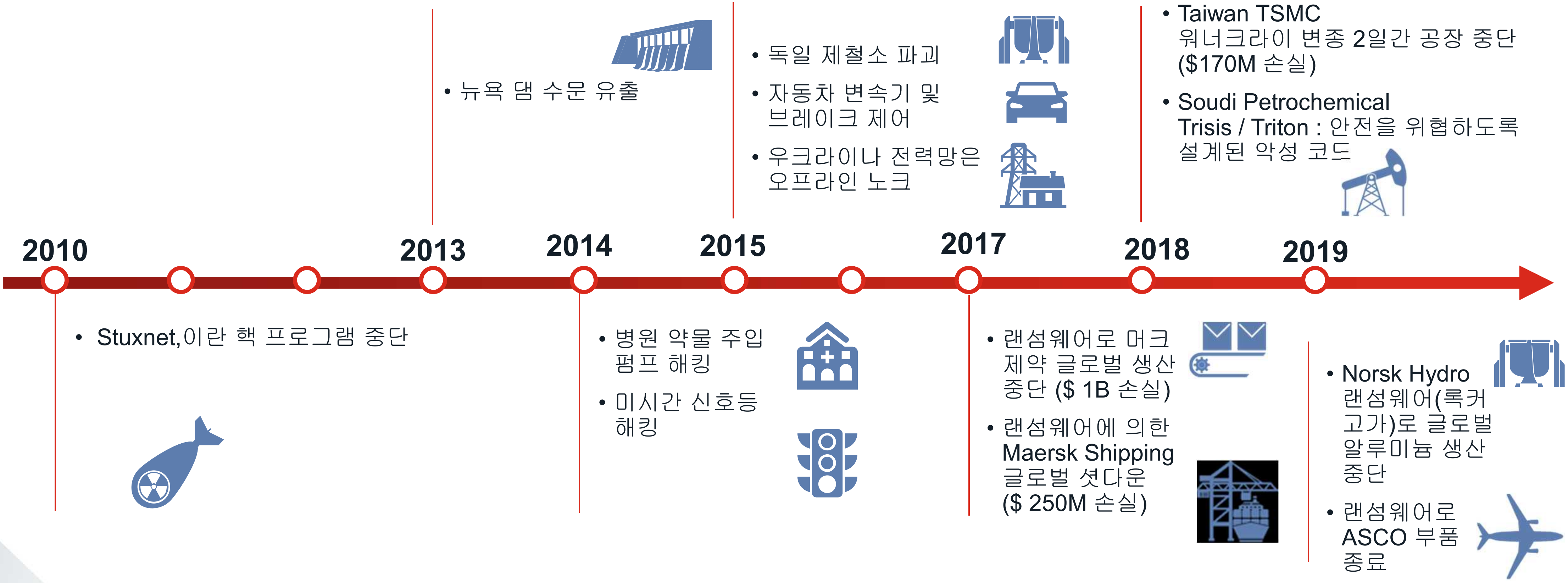
IT	보안 목표 우선 순위	OT
중간, 지연 가능	가용성 요구사항	매우 높음
지연 가능	실시간성 요구사항	크리티컬
약 5년	구성요소 라이프 사이클	20년 이상
정기적 / 필수적	패치 및 보안감사	상대적으로 가끔
높음 / 성숙	보안에 대한 인식	증가하고 있음
글로벌 표준	프로토콜	특수성

유지보수 종료, AV 미설치

은닉을 통한 보안 (Air Gap)

관리, 보안 고려사항 부족

OT 기간 산업 시설 공격 - 위험은 실제 상황



2010

- Stuxnet,이란 핵 프로그램 중단

2013

- 뉴욕 댐 수문 유출

2014

- 병원 약물 주입 펌프 해킹
- 미시간 신호등 해킹

2015

- 독일 제철소 파괴
- 자동차 변속기 및 브레이크 제어
- 우크라이나 전력망은 오프라인 노크

2017

- 랜섬웨어로 머크 제약 글로벌 생산 중단 ($ 1B 손실)
- 랜섬웨어에 의한 Maersk Shipping 글로벌 셧다운 ($ 250M 손실)

2018

- Taiwan TSMC
  워너크라이 변종 2일간 공장 중단 ($170M 손실)
- Soudi Petrochemical
  Trisis / Triton : 안전을 위협하도록 설계된 악성 코드

2019

- Norsk Hydro
  랜섬웨어(록커 고가)로 글로벌 알루미늄 생산 중단
- 랜섬웨어로 ASCO 부품 종료

포티넷 OT 산업 보안 위협 분석 보고서 요약

FORTINET

보고서

Fortinet 2019
운영 기술 보안 트렌드 보고서

ICS 및 SCADA 시스템에 대한 위협
동향 업데이트

인포그래픽: 주요 조사 결과

2018년에 거의 모든 ICS/SCADA 벤더에서 익스플로잇의 **출현 규모와 출현 빈도가 증가**했습니다.

범죄자들은 주기적으로 기존의 **IT 위협을 재활용**해 OT 시스템을 위협합니다.

85% 의 고유한 위협이 다음 프로토콜을 대상으로 함
OPC Classic
BACnet
Modbus

BACnet에 대한 공격은 **2018년 1월~4월** 최고치를 기록했고, 이는 Mirai 봇넷임

Moxa 313 취약점은 일본에 크게 집중되었습니다.

FORTINET

AGENDA

1 OT & 보안 위협 동향

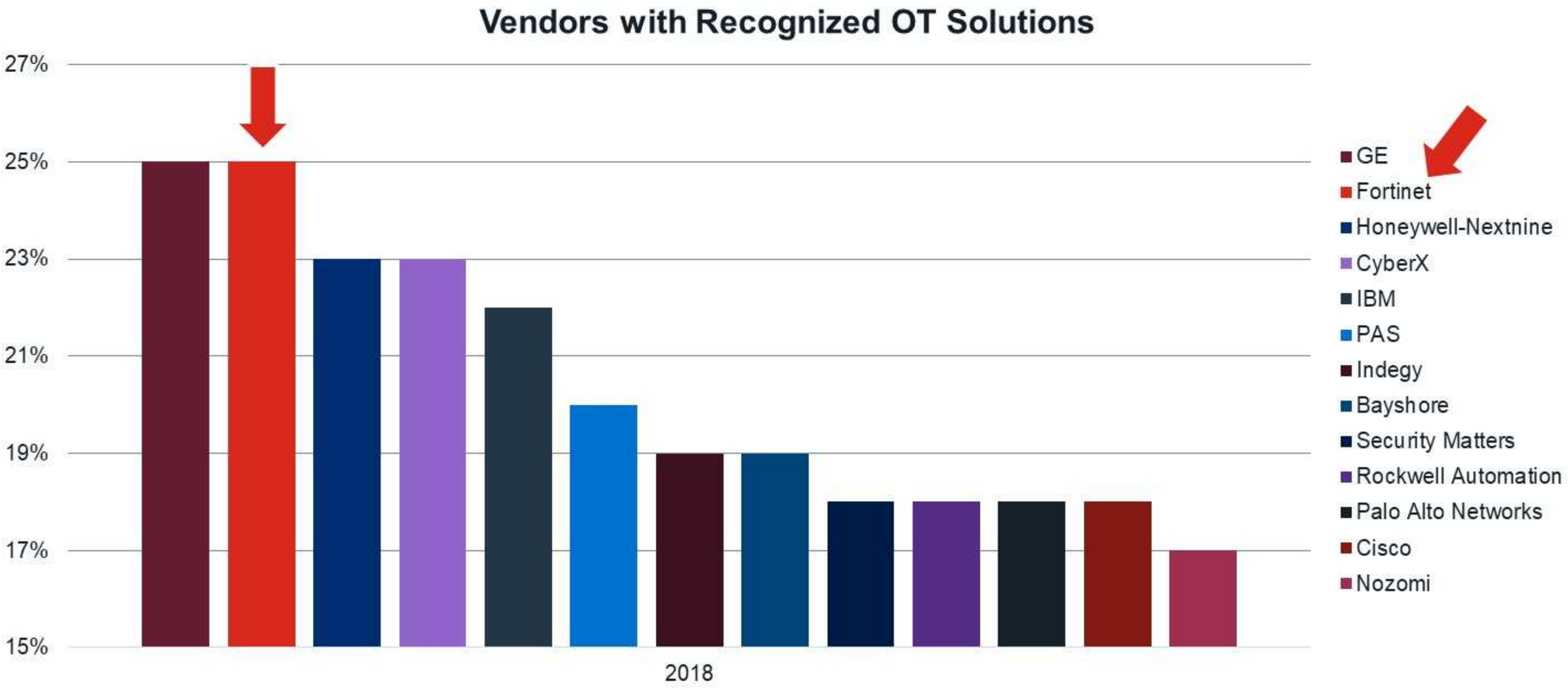
2 포티넷과 ICS 벤더사와 협업 사례

3 포티넷 OT 보안 아키텍처와 구축 예시

4 OT/ICS/SCADA 인프라 보호 제안

5 OT 보안 취약성 방어 데모

Fortinet : OT 산업 보안 분야의 리더



Source: Commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Fortinet (Nasdaq: FTNT)

$18B
Nasdaq: FTNT
Profitable

$2B+
Revenue
Fastest growing

450,000+
Customers
Massive sensor network

#1 Cybersecurity Company in the World

Leading Every Evolution of Cybersecurity

30%
Global Firewall Shipments
Huge scale

$200M+
Research & Development
Large investment

650+
Patents
Organic growth

Fortinet OT 보안 솔루션 도입 고객사

Utilities & Energy

- RWE The energy to lead
- enel
- Eidsiva
- energex
- Dominion Energy
- City of Burbank Water and Power Since 1913
- وقود WOQOD
- BS NETZ
- Yarra Valley Water
- NGCP
- HEDNO
- ontras Gastransport GmbH
- eDF
- Sydney Water
- AVANGRID
- Verbundnetz Gas AG
- VEOLIA
- Powercor Australia
- BarwonWater
- CELG
- AIK
- NBU New Braunfels Utilities
- SAM HOUSTON ELECTRIC COOPERATIVE
- City West Water
- RED ELÉCTRICA DE ESPAÑA
- هيئة كهرباء ومياه دبي Dubai Electricity & Water Authority

Manufacturing

- BMW
- Mercedes-Benz
- Volkswagen
- SANDVIK
- AIR LIQUIDE
- RHEINMETALL DEFENCE
- GLENCORE

Communications

- UNIGESTION
- EIDSIVA bredbånd
- DACAS
- CIVIQ SMARTSCAPES
- Claro
- orange

Government

- NASA
- City of Columbia, S.C.
- City and County of San Francisco
- UNDERGROUND
- BART

FORTINET

Fortinet : OT 얼라이언스 파트너쉽

FORTINET Fabric-Ready

OT TECHNOLOGY PARTNERS

Active Partners

SIEMENS RUGGEDCOM

WELOTEC

NOZOMI NETWORKS

CYBERX BATTLE-TESTED INDUSTRIAL CYBERSECURITY

Listed Partner

SCADAfence

Indegy

CLAROTY

DRAGOS

OWL Cyber Defense

BACKBOX

rubrik

Others

FORESCOUT

RAD

DARKTRACE

SOLUTION VENDORS AND SYSTEMS INTEGRATORS

Control Vendors

Schneider Electric

GE

ABB

SIEMENS

YOKOGAWA

GSIs

Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING

IBM

NTT

HCL

AtoS

Orange Cyberdefense

accenture

Others

T-Systems

Hewlett Packard Enterprise

Johnson Controls

Cognizant

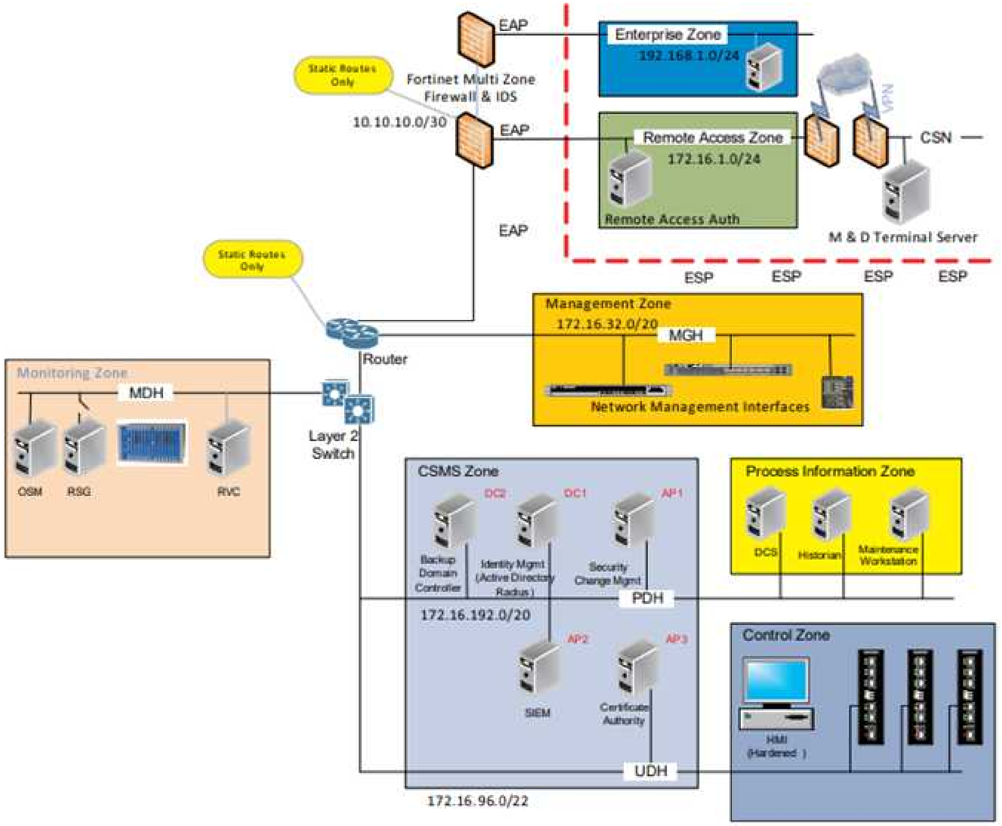
World Wide Technology, Inc.

FORTINET

ICS벤더사 협업모델 : GE

- Fortinet do business with GE Power as well as GE Renewables, GE energy and GE Grid (the old Alstom)
- Our FortiGate is their standard BOM for UTM/Firewalls.
- Typically they deploy out FortiGate 301E in pairs for high availability.

- GEH-6840G - NetworkST 3.1 / 4.0 for Mark* VIe Controls Application Guide, April 2019
- https://www.ge.com/content/dam/gepower-pgdp/global/en_US/documents/automation/GEH-6840.pdf



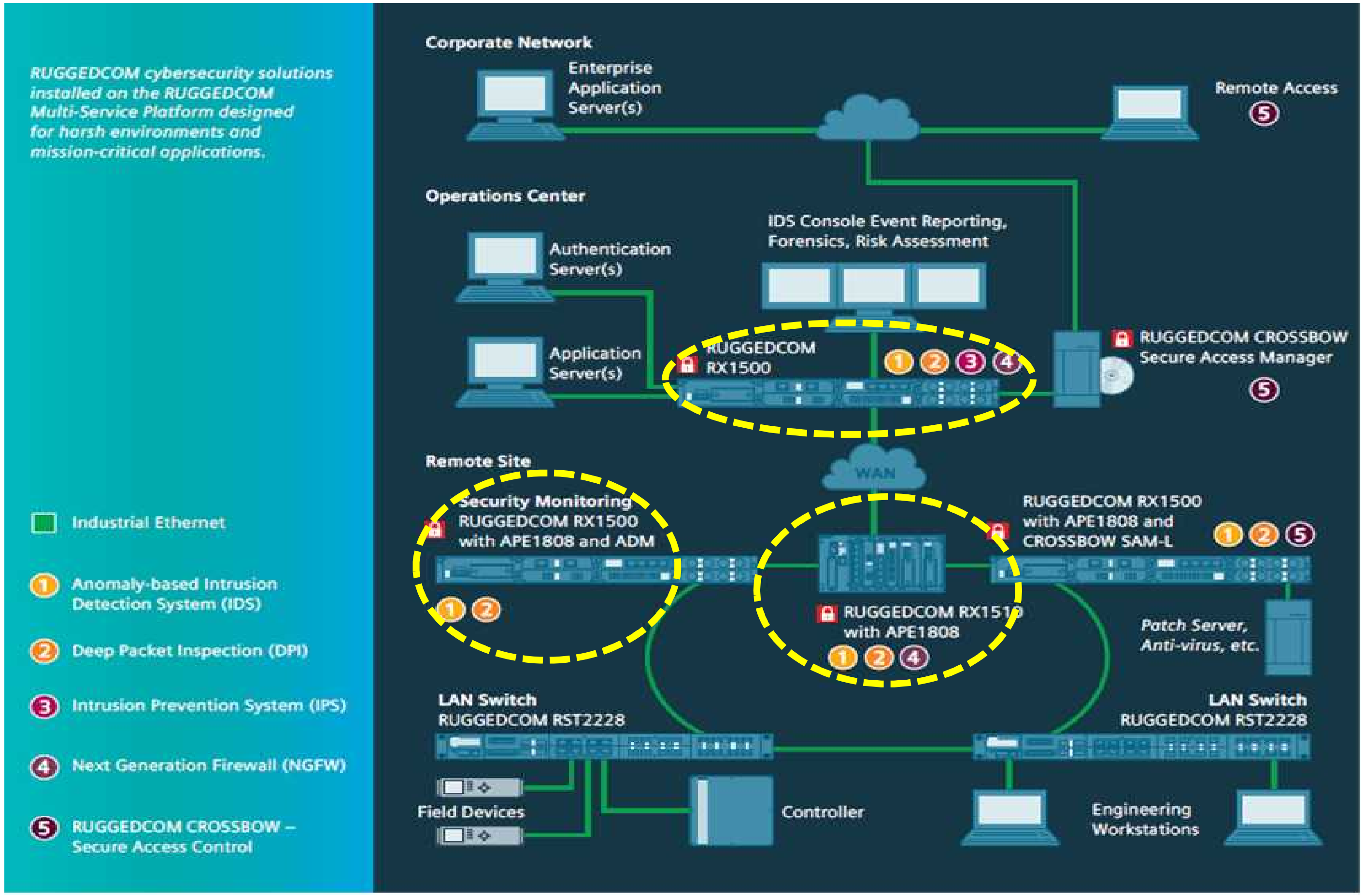
GE ICS Architecture Based on ISA 99 Zoning Model

ICS벤더사 협업모델 : Siemens

- Securing your critical infrastructure with RUGGEDCOM Cybersecurity Solutions.

  https://press.siemens.com/global/en/pressrelease/siemens-hosting-platform-solving-complex-cybersecurity-challenges

- Fortinet and Siemens Security Solutions : Industrial Switching Platform with Integrated FortiGate for Enhanced Security and Simplified Deployments



RUGGEDCOM cybersecurity solutions installed on the RUGGEDCOM Multi-Service Platform designed for harsh environments and mission-critical applications.

🟩 Industrial Ethernet

① Anomaly-based Intrusion Detection System (IDS)

② Deep Packet Inspection (DPI)

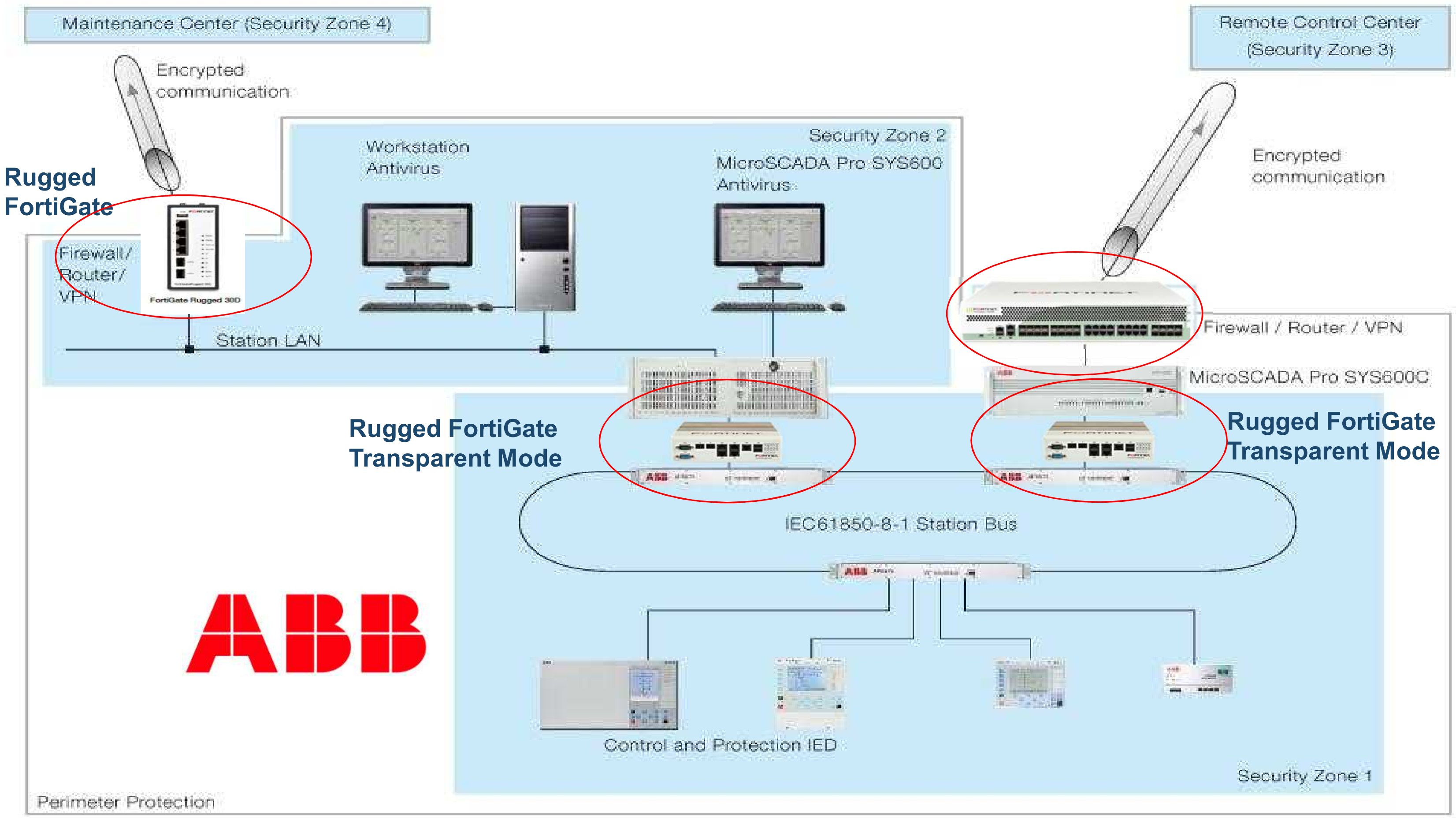
③ Intrusion Prevention System (IPS)

④ Next Generation Firewall (NGFW)

⑤ RUGGEDCOM CROSSBOW – Secure Access Control

Corporate Network
Enterprise Application Server(s)
Remote Access
⑤
Operations Center
IDS Console Event Reporting, Forensics, Risk Assessment
Authentication Server(s)
Application Server(s)
RUGGEDCOM RX1500
① ② ③ ④
RUGGEDCOM CROSSBOW Secure Access Manager
⑤
Remote Site
WAN
Security Monitoring RUGGEDCOM RX1500 with APE1808 and ADM
① ②
RUGGEDCOM RX1510 with APE1808
① ② ④
RUGGEDCOM RX1500 with APE1808 and CROSSBOW SAM-L
① ② ⑤
Patch Server, Anti-virus, etc.
LAN Switch RUGGEDCOM RST2228
LAN Switch RUGGEDCOM RST2228
Field Devices
Controller
Engineering Workstations

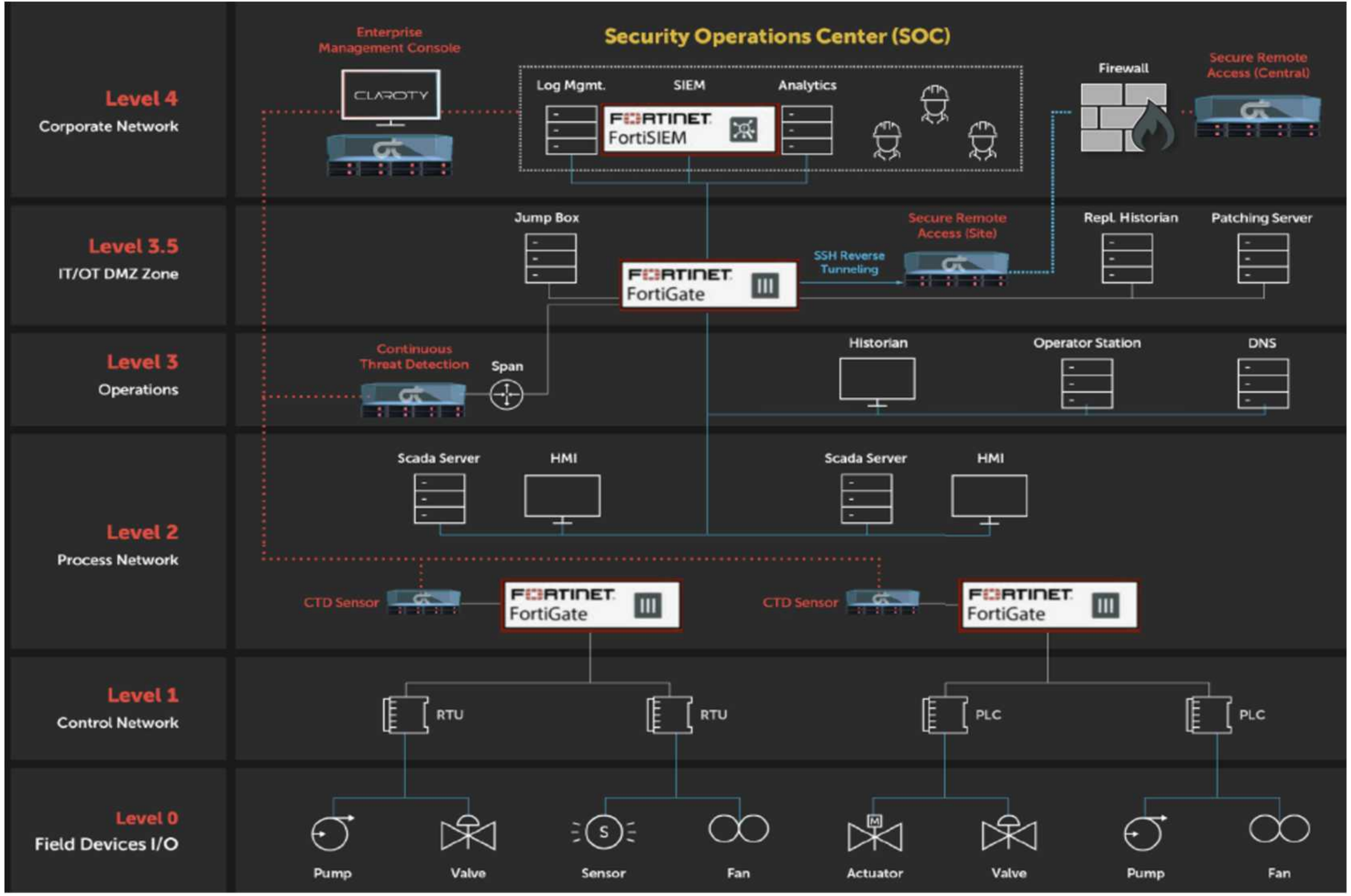
ICS벤더사 협업모델 : ABB



© Fortinet Inc. All Rights Reserved.

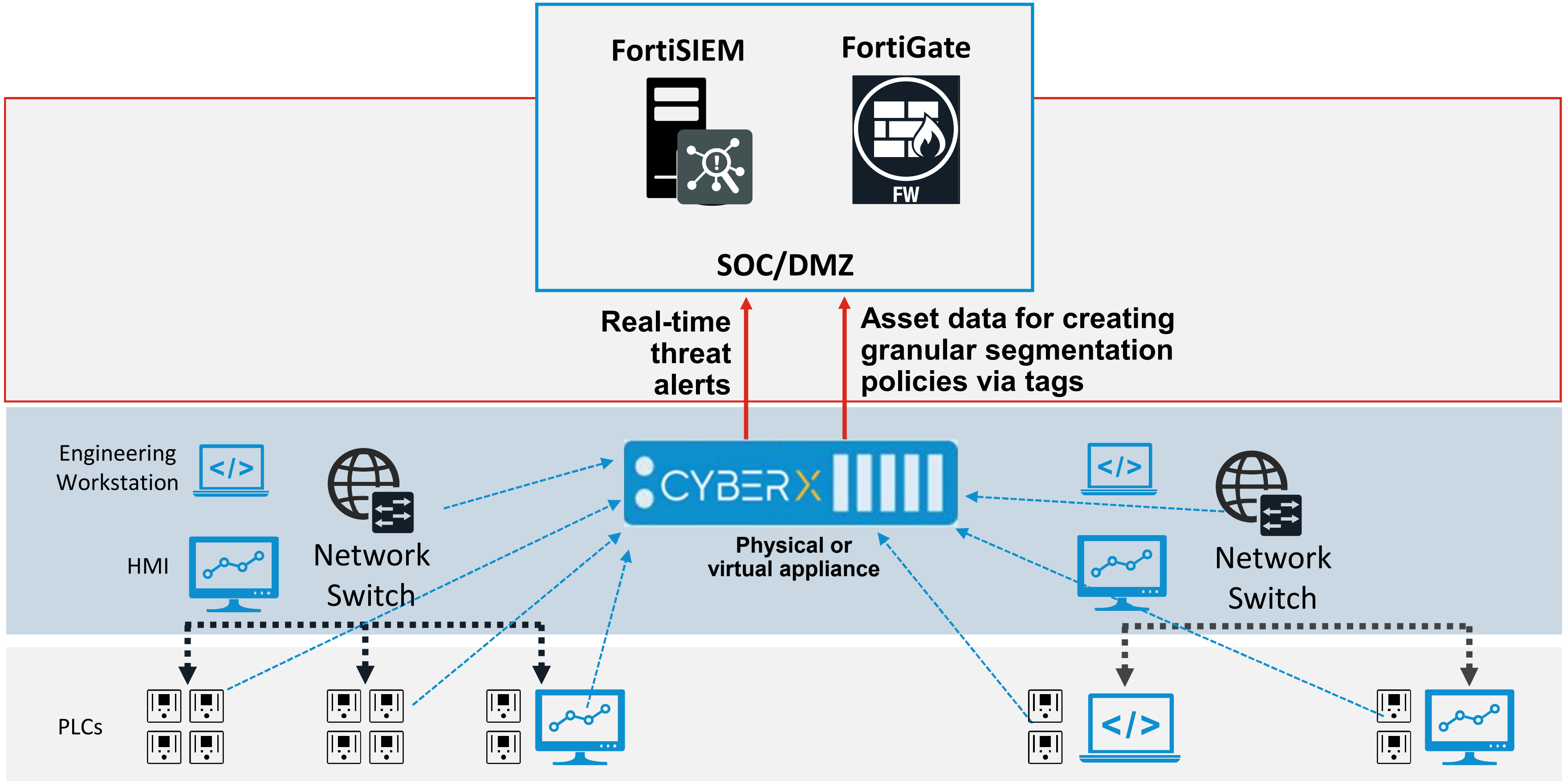
Visibility 벤더사 협업모델 : Claroty

FORTINET Fabric-Ready



FORTINET

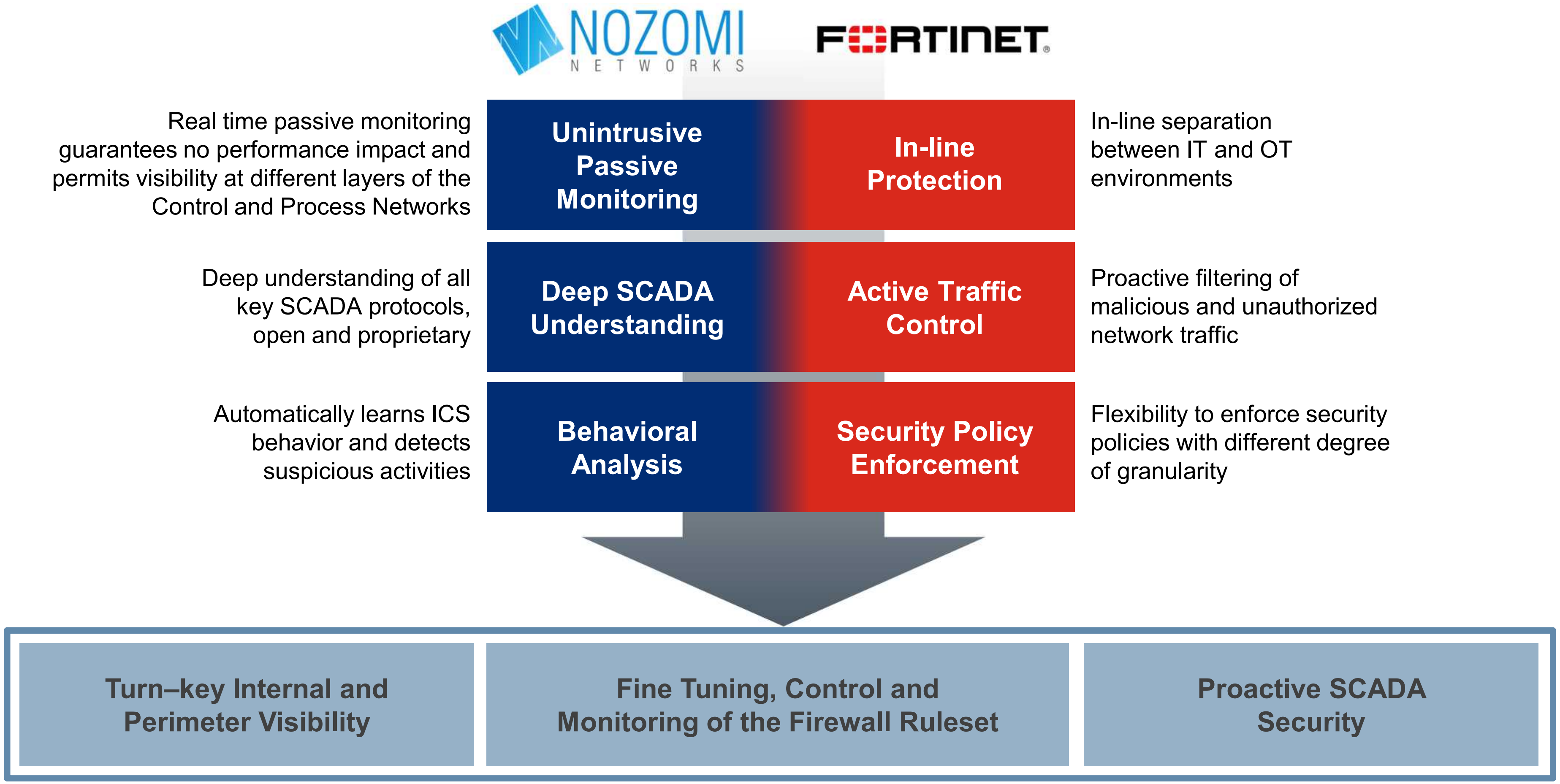
Visibility 벤더사 협업모델 : CyberX



FORTINET

Visibility 벤더사 협업모델 : Nozomi

Fabric-Ready



Real time passive monitoring guarantees no performance impact and permits visibility at different layers of the Control and Process Networks

Unintrusive Passive Monitoring

In-line Protection

In-line separation between IT and OT environments

Deep understanding of all key SCADA protocols, open and proprietary

Deep SCADA Understanding

Active Traffic Control

Proactive filtering of malicious and unauthorized network traffic

Automatically learns ICS behavior and detects suspicious activities

Behavioral Analysis

Security Policy Enforcement

Flexibility to enforce security policies with different degree of granularity

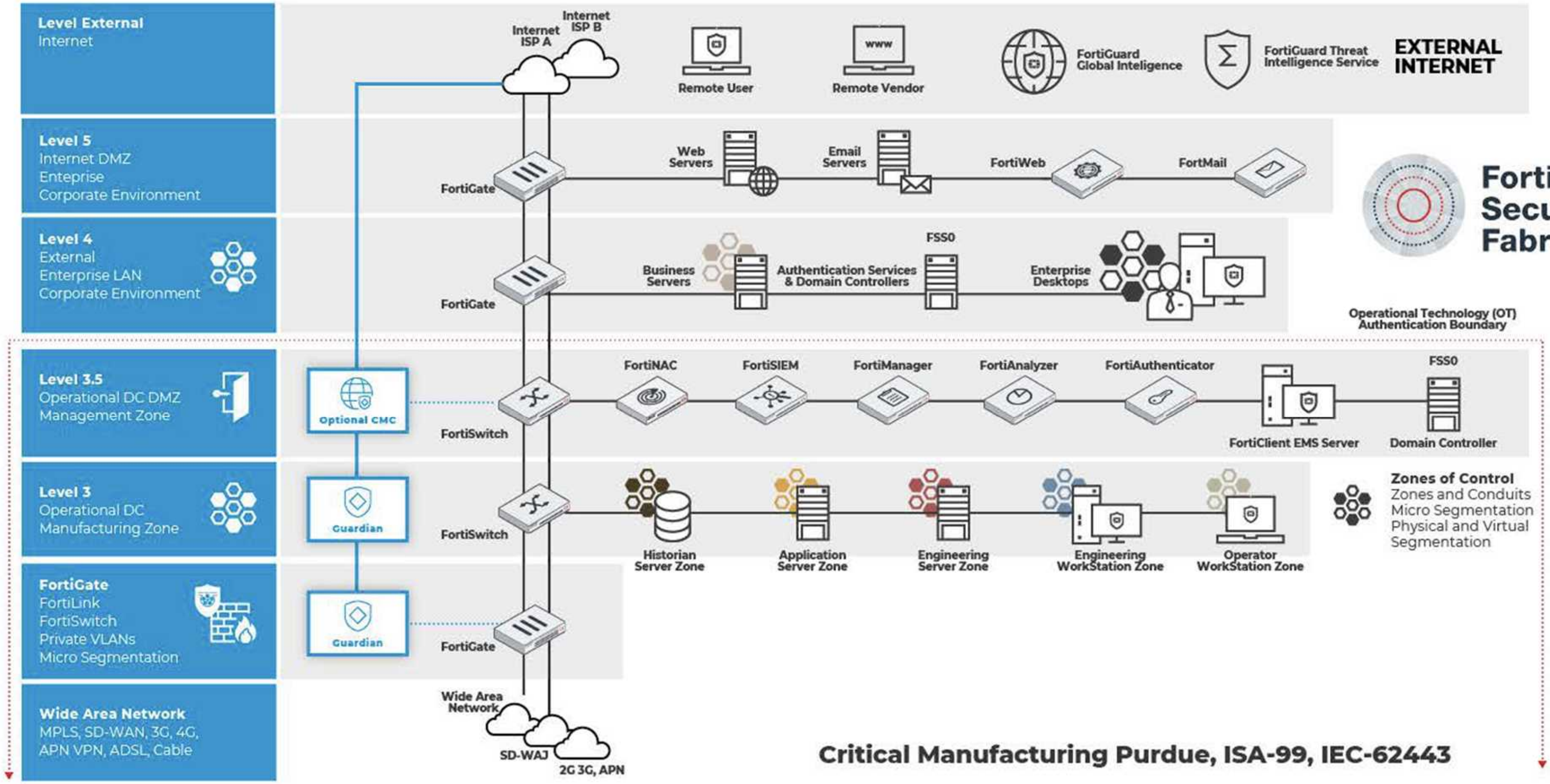
Turn–key Internal and Perimeter Visibility

Fine Tuning, Control and Monitoring of the Firewall Ruleset

Proactive SCADA Security

Visibility 벤더사 협업모델 : Nozomi

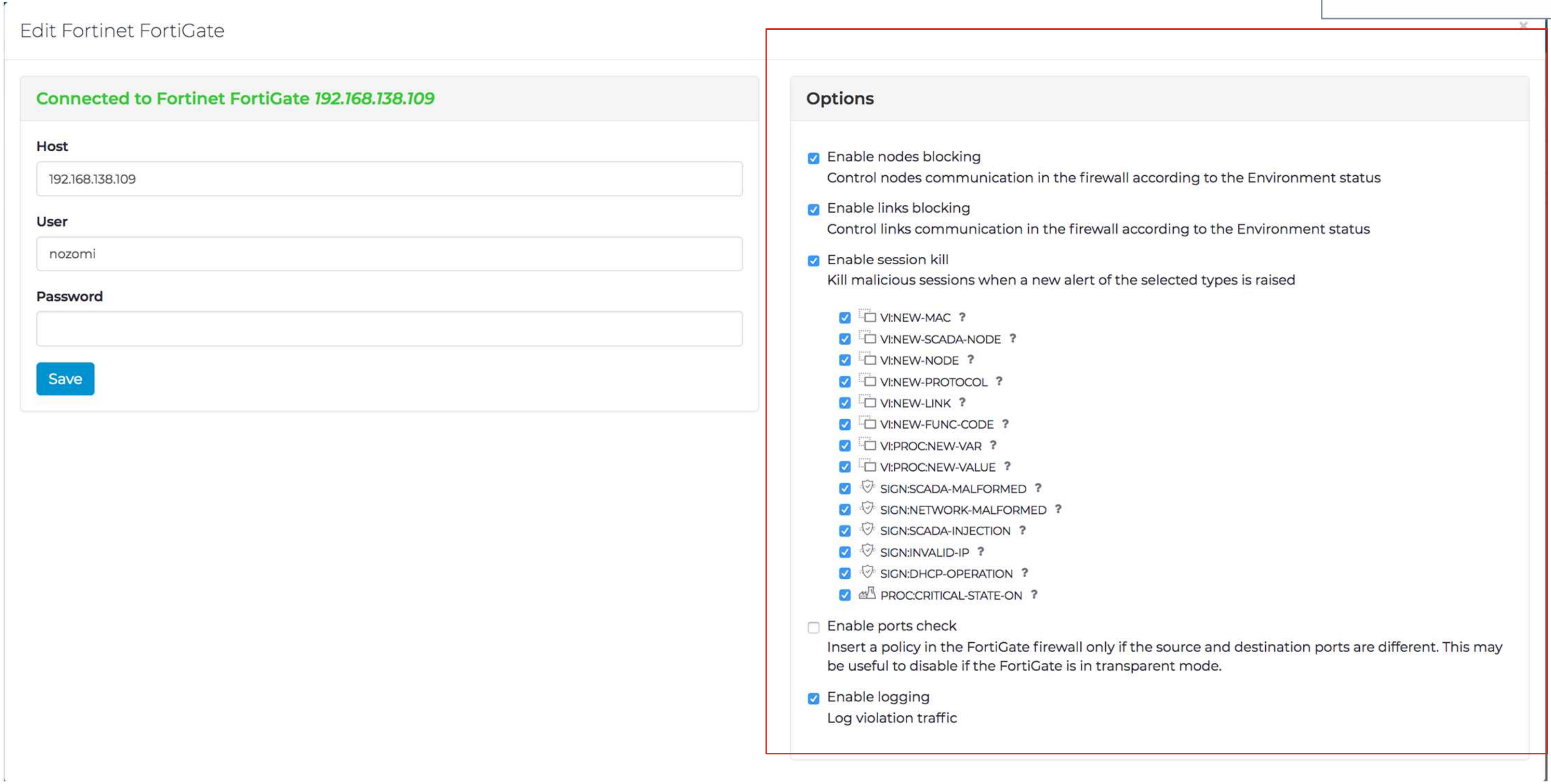
Fabric-Ready



Critical Manufacturing Purdue, ISA-99, IEC-62443

Visibility 벤더사 협업모델 : Nozomi

FORTINET Fabric-Ready



Edit Fortinet FortiGate

Connected to Fortinet FortiGate *192.168.138.109*

Host

192.168.138.109

User

nozomi

Password

Options

☑ Enable nodes blocking
Control nodes communication in the firewall according to the Environment status

☑ Enable links blocking
Control links communication in the firewall according to the Environment status

☑ Enable session kill
Kill malicious sessions when a new alert of the selected types is raised

- ☑ VI:NEW-MAC ?
- ☑ VI:NEW-SCADA-NODE ?
- ☑ VI:NEW-NODE ?
- ☑ VI:NEW-PROTOCOL ?
- ☑ VI:NEW-LINK ?
- ☑ VI:NEW-FUNC-CODE ?
- ☑ VI:PROC:NEW-VAR ?
- ☑ VI:PROC:NEW-VALUE ?
- ☑ SIGN:SCADA-MALFORMED ?
- ☑ SIGN:NETWORK-MALFORMED ?
- ☑ SIGN:SCADA-INJECTION ?
- ☑ SIGN:INVALID-IP ?
- ☑ SIGN:DHCP-OPERATION ?
- ☑ PROC:CRITICAL-STATE-ON ?

□ Enable ports check
Insert a policy in the FortiGate firewall only if the source and destination ports are different. This may be useful to disable if the FortiGate is in transparent mode.

☑ Enable logging
Log violation traffic

AGENDA

1 OT & 보안 위협 동향

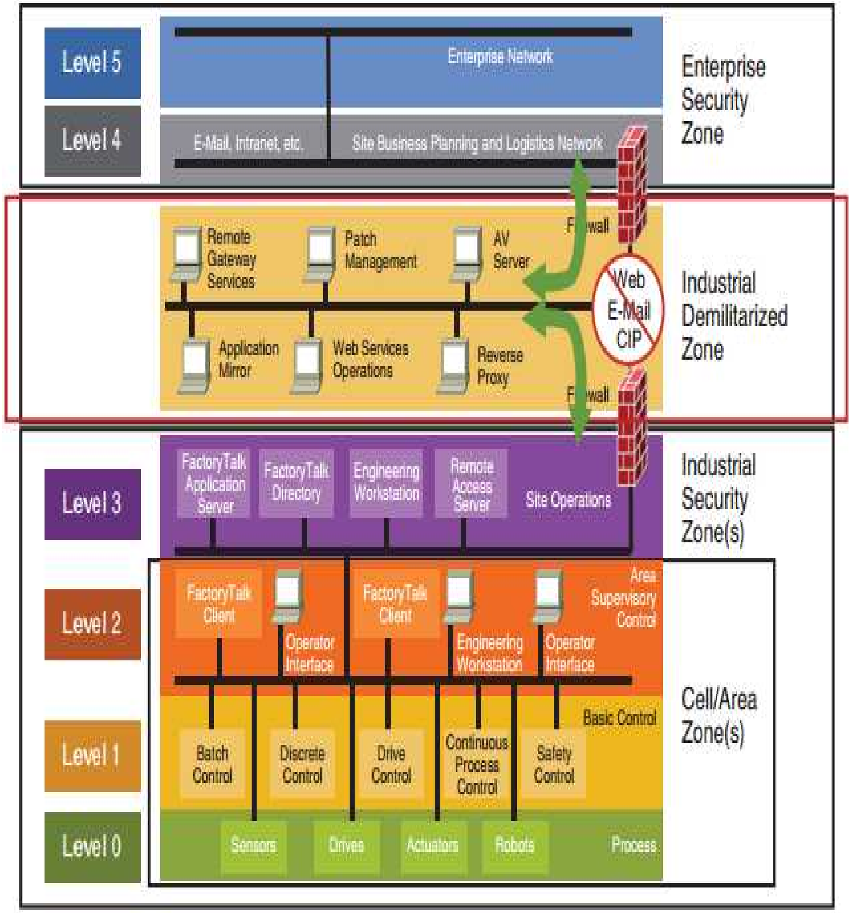
2 포티넷과 ICS 벤더사와 협업 사례

3 포티넷 OT 보안 아키텍처와 구축 예시

4 OT/ICS/SCADA 인프라 보호 제안

5 OT 보안 취약성 방어 데모

Purdue Enterprise Reference Architecture (ISA-99, IEC-62443) ICS 보안 레퍼런스

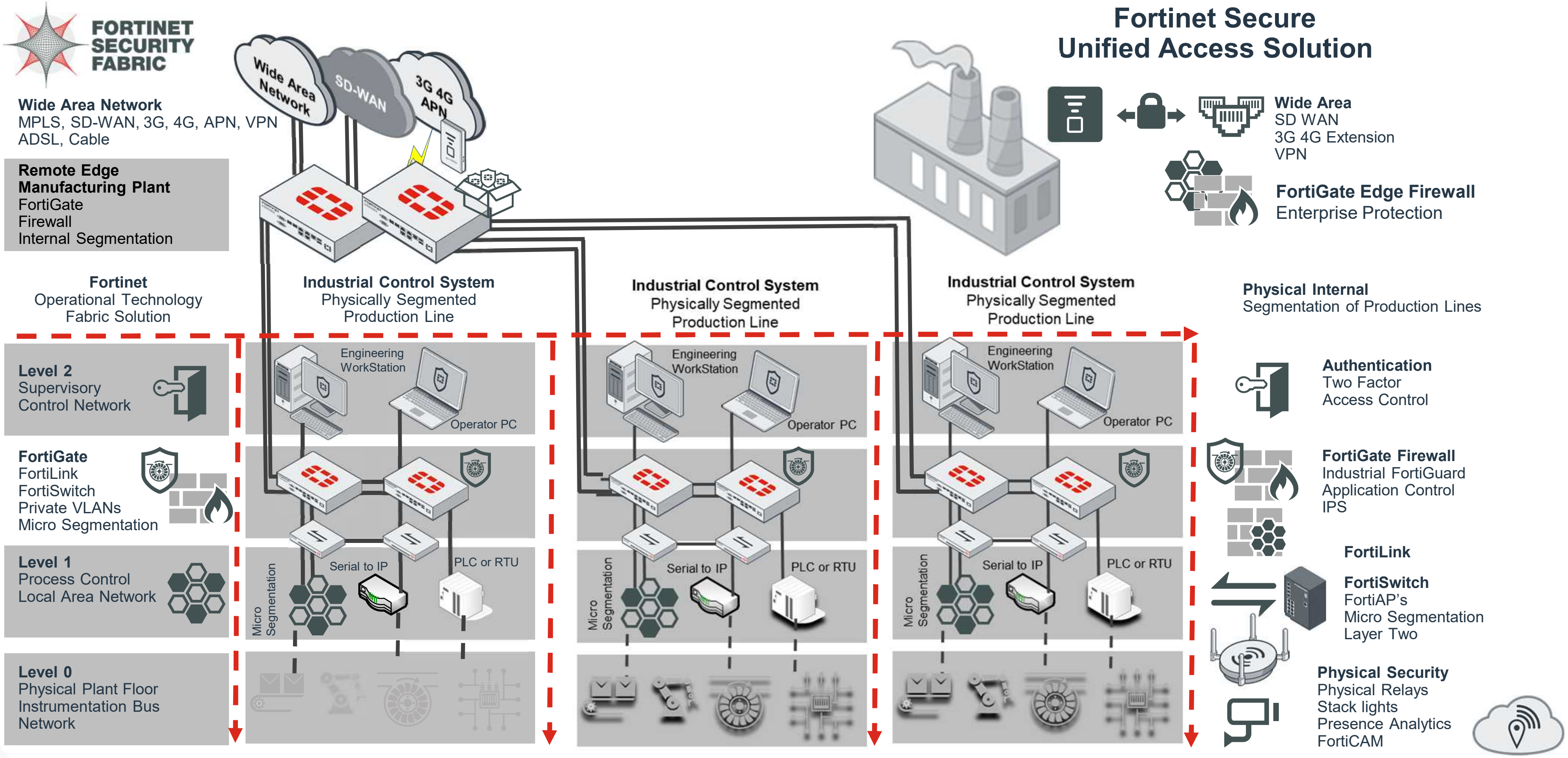


부문별 포티넷 OT 보안 솔루션 요약

- **OT 인프라 보안**
  (NGFW, UTM, IDS/IPS, L2 스위치, 비인가 자산 제어/NAC)
- **OT 인프라 가시성 & 통합관리**
  (ForgiGate, FortiSwitch, FortiManager, FortiAnalyzer)
- **OT SOC 통합관제**
  (FortiSIEM, SOAR)
- **OT 위협 탐지 & 방어**
  (IDS/IPS, Sandbox, AI)
- **OT 단말보안**
  (AV, EDR, NAC)
- **국제 & 국가 규정 준수**
  (Compliance)

포티넷 OT보안 레퍼런스 아키텍처 모델

Purdue, ISA-99, IEC-62443



FORTINET SECURITY FABRIC

Wide Area Network
MPLS, SD-WAN, 3G, 4G, APN, VPN
ADSL, Cable

Remote Edge
Manufacturing Plant
FortiGate
Firewall
Internal Segmentation

Fortinet
Operational Technology
Fabric Solution

Level 2
Supervisory
Control Network

FortiGate
FortiLink
FortiSwitch
Private VLANs
Micro Segmentation

Level 1
Process Control
Local Area Network

Level 0
Physical Plant Floor
Instrumentation Bus
Network

Fortinet Secure
Unified Access Solution

Wide Area
SD WAN
3G 4G Extension
VPN

FortiGate Edge Firewall
Enterprise Protection

Physical Internal
Segmentation of Production Lines

Authentication
Two Factor
Access Control

FortiGate Firewall
Industrial FortiGuard
Application Control
IPS

FortiLink

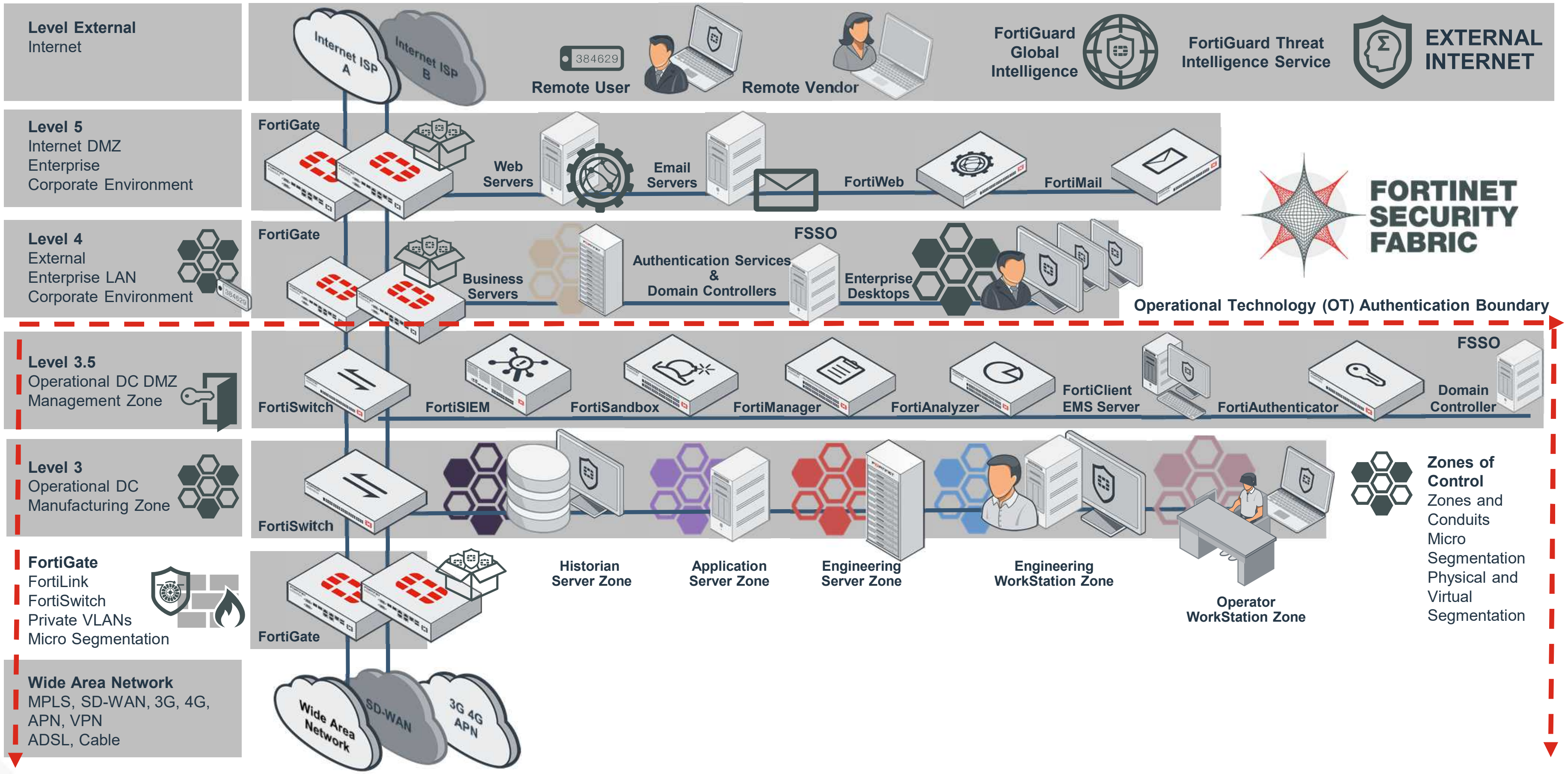
FortiSwitch
FortiAP's
Micro Segmentation
Layer Two

Physical Security
Physical Relays
Stack lights
Presence Analytics
FortiCAM

FORTINET

포티넷 OT보안 레퍼런스 아키텍처 모델

Purdue, ISA-99, IEC-62443



Level External
Internet

Internet ISP A
Internet ISP B
384629
Remote User
Remote Vendor
FortiGuard Global Intelligence
FortiGuard Threat Intelligence Service
EXTERNAL INTERNET

Level 5
Internet DMZ
Enterprise
Corporate Environment

FortiGate
Web Servers
Email Servers
FortiWeb
FortiMail

FORTINET SECURITY FABRIC

Level 4
External
Enterprise LAN
Corporate Environment

FortiGate
Business Servers
FSSO
Authentication Services & Domain Controllers
Enterprise Desktops

Operational Technology (OT) Authentication Boundary

Level 3.5
Operational DC DMZ
Management Zone

FortiSwitch
FortiSIEM
FortiSandbox
FortiManager
FortiAnalyzer
FortiClient EMS Server
FortiAuthenticator
FSSO
Domain Controller

Level 3
Operational DC
Manufacturing Zone

FortiSwitch
Historian Server Zone
Application Server Zone
Engineering Server Zone
Engineering WorkStation Zone
Operator WorkStation Zone

Zones of Control
Zones and Conduits
Micro Segmentation
Physical and Virtual Segmentation

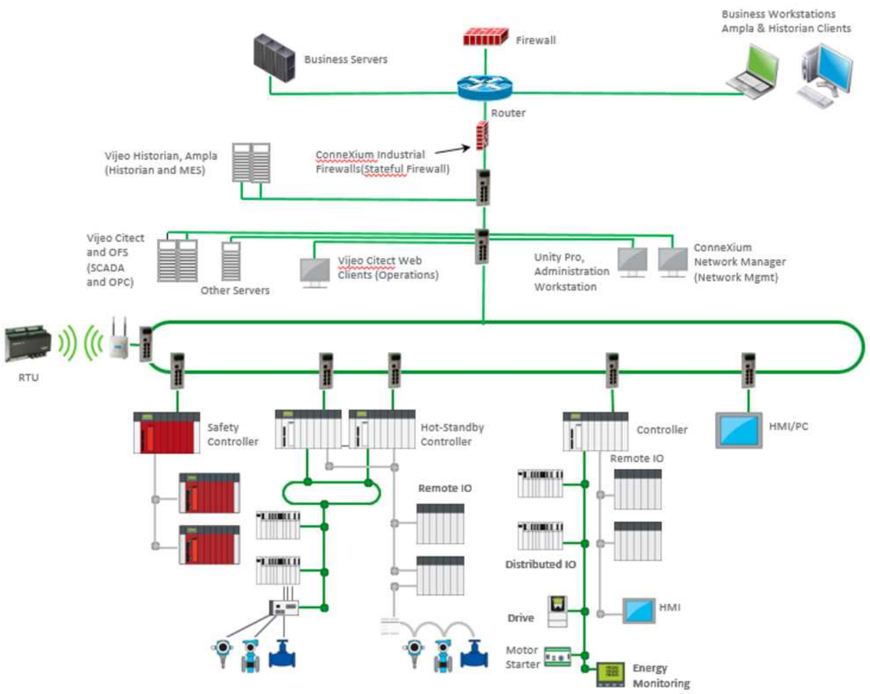
FortiGate
FortiLink
FortiSwitch
Private VLANs
Micro Segmentation

FortiGate

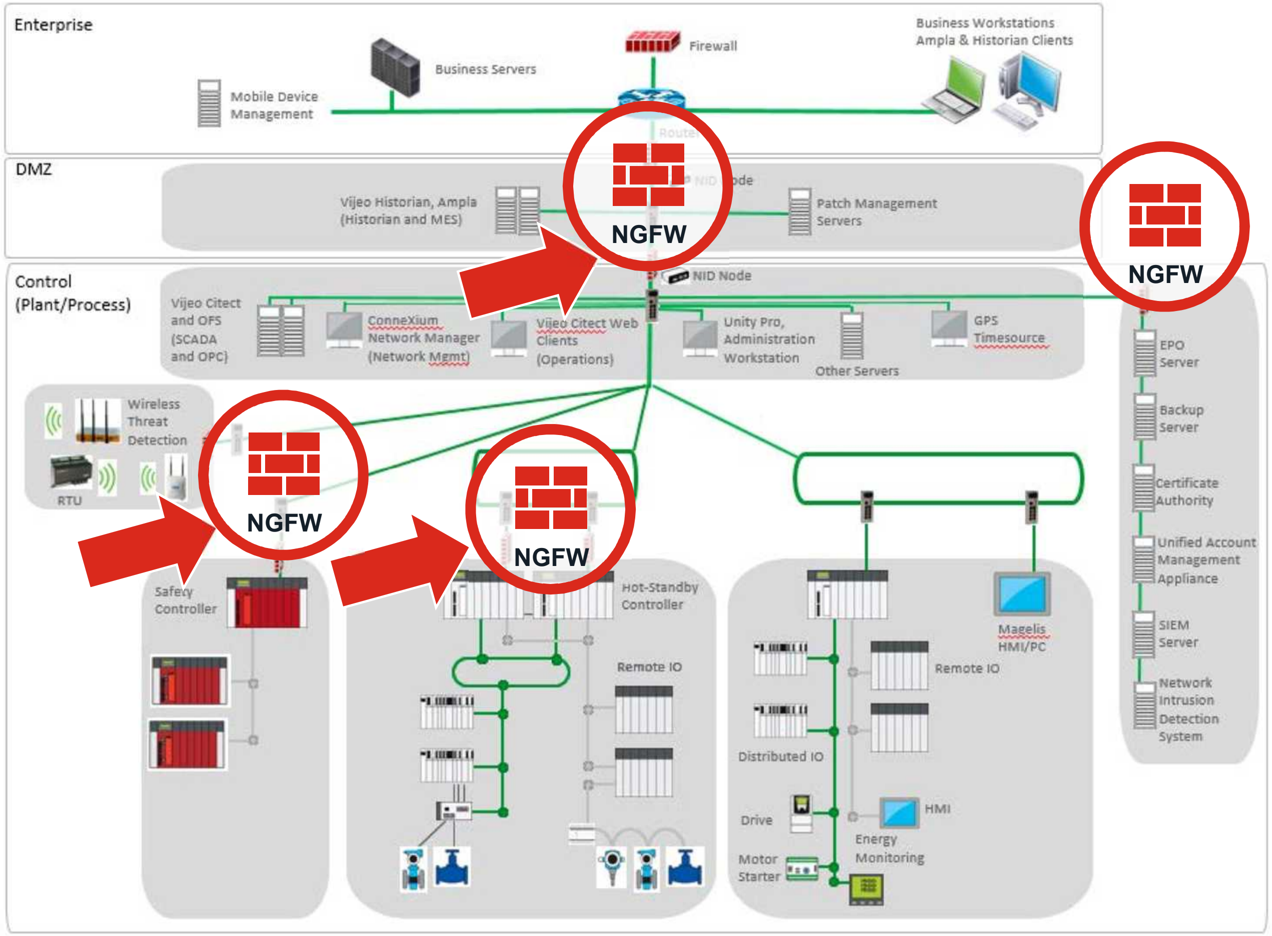
Wide Area Network
MPLS, SD-WAN, 3G, 4G,
APN, VPN
ADSL, Cable

Wide Area Network
SD-WAN
3G 4G APN

OT보안 구축 예시 : 네트워크 Zoning



Traditional

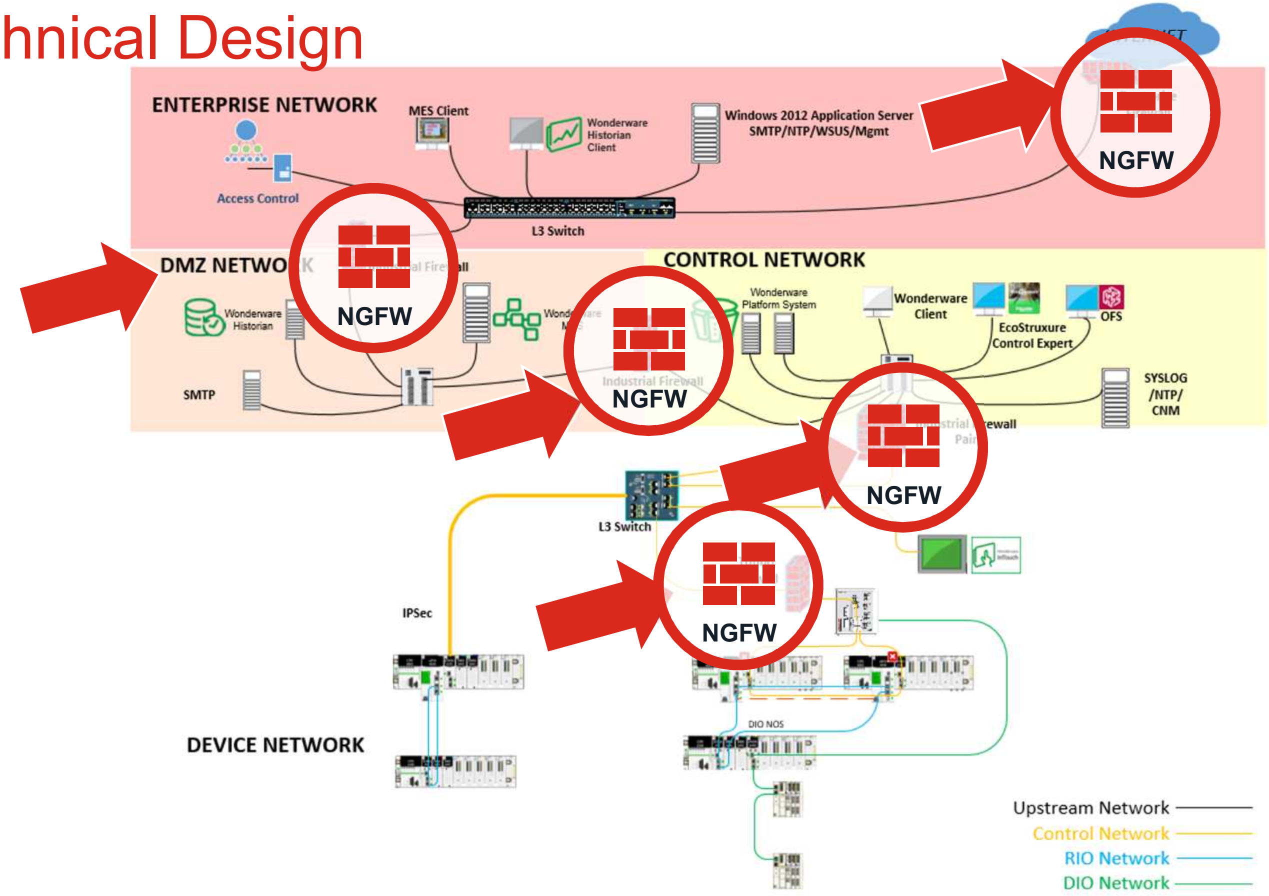


Sample Network with Zoning

OT보안 구축 예시 : 사이버보안 디자인

Cyber Security System Technical Design

- Plant Edge – FortiGate
- Purdue Zoning/Conduits - Rugged FortiGate
- Remote Access – FortiClient / FortiAuthenticator

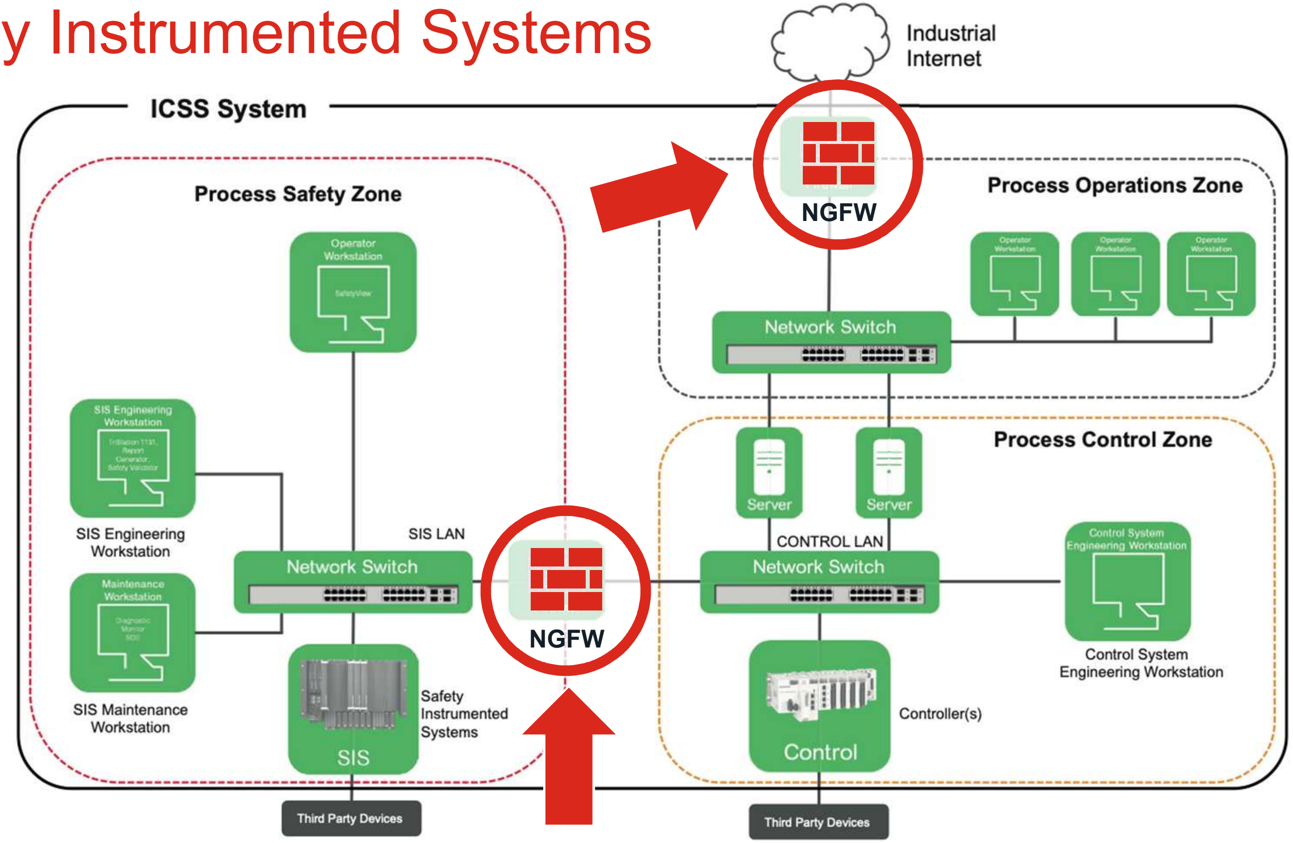


Cyber Security System Technical

OT보안 구축 예시 : 안전 계장 시스템 (SIS)

Schneider Triconex® Safety Instrumented Systems

- Plant Edge – FortiGate
- Purdue Zoning/Conduits for SIS LAN – **FortiGate**
- Remote Access – FortiClient / FortiAuthenticator 2FA

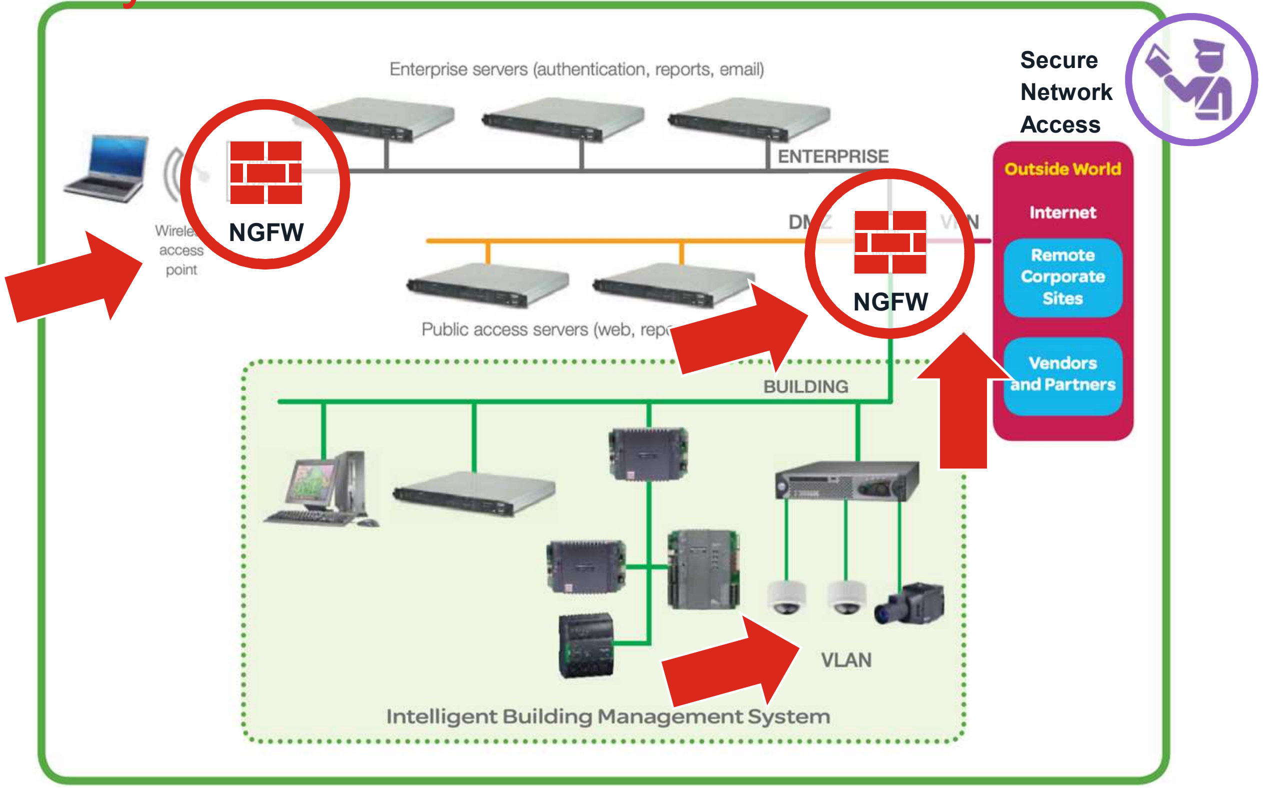


A practical guide to maximizing the resilience of your EcoStruxure Triconex Safety Systems against cyber threats.

OT보안 구축 예시 : Intelligent Building 보안

Intelligent Building Management Systems

- Plant Edge – FortiGate
- Purdue Zoning/Conduits – FortiGate
- Wireless Point – FortiAP



Best Practices for Securing an Intelligent Building Management System (iBMS)

AGENDA

1 OT & 보안 위협 동향

2 포티넷과 ICS 벤더사와 협업 사례

3 포티넷 OT 보안 아키텍처와 구축 예시

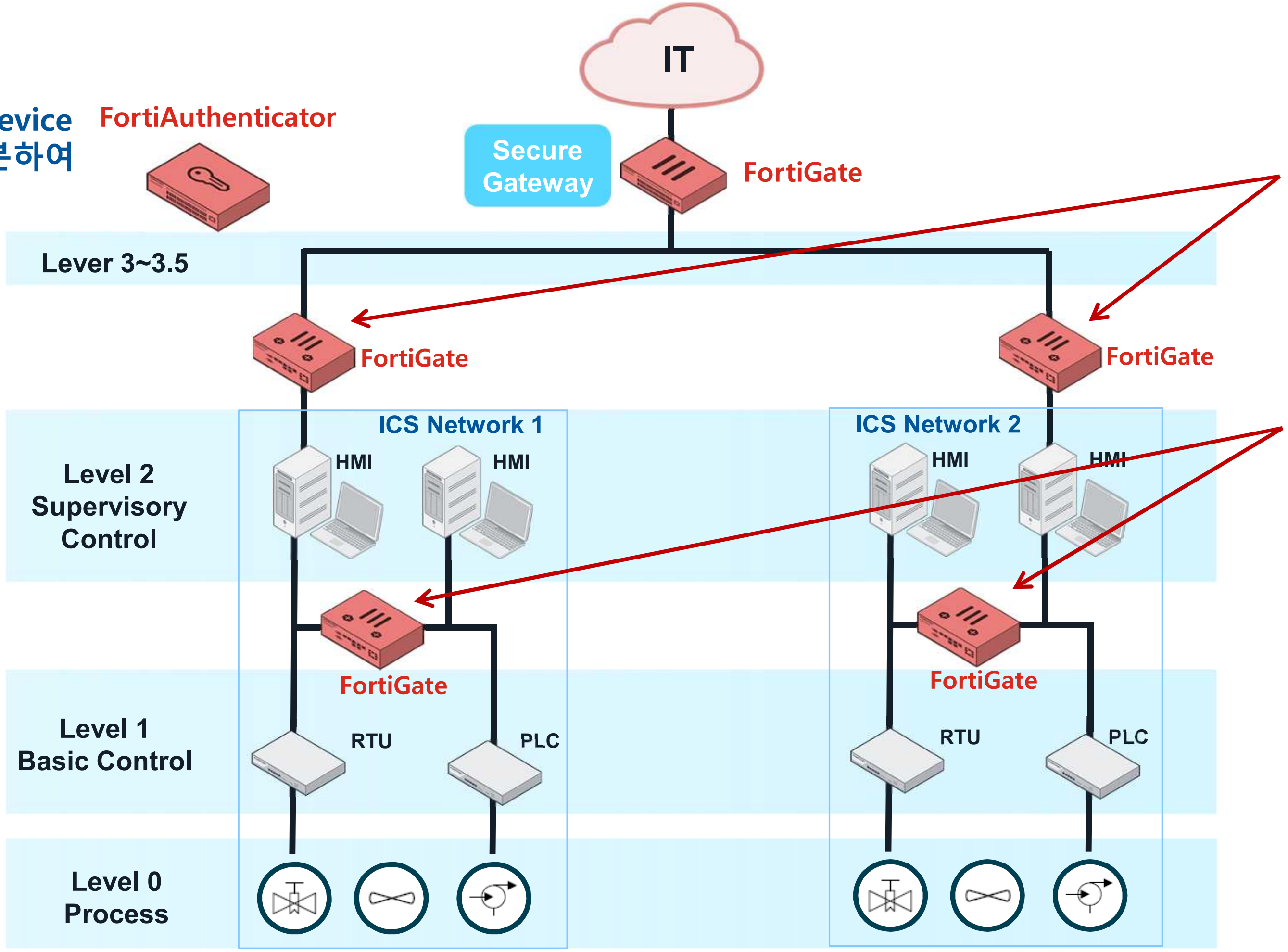
4 **OT/ICS/SCADA 인프라 보호 제안**

5 OT 보안 취약성 방어 데모

OT/ICS/SCADA 인프라 보호 제안

- 제안1 : Segmentation & 접근제어
- 제안2 : OT 보안 가시성
- 제안3 : OT 보안 관리 및 APT 탐지방어 기능

제안1 : Segmentation & 접근제어



User ID, Device 종류를 구분하여 접근제어

서로 다른 ICS 네트워크 사이의 접근 제어
- 미러링 모드 적용 가능
- Low latency

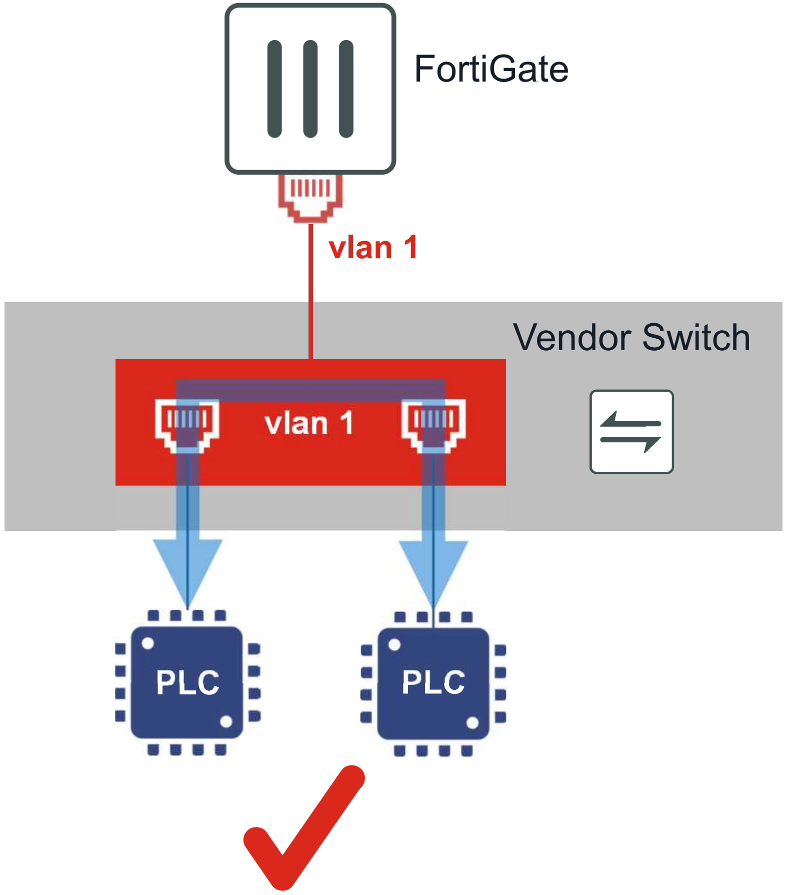
ICS 네트워크 내부의 세부 분할

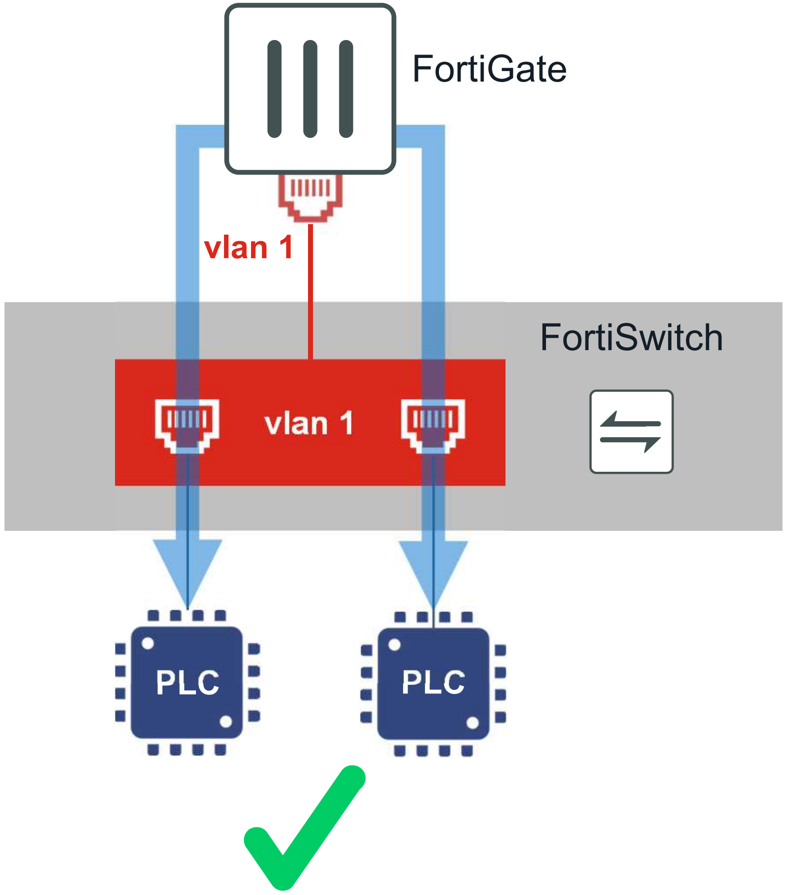
IEC 61850

EMI
Thermal
Vibration

Industrial Grade & Compliance Ready

Purdue Model Zoning – 마이크로 세그멘테이션

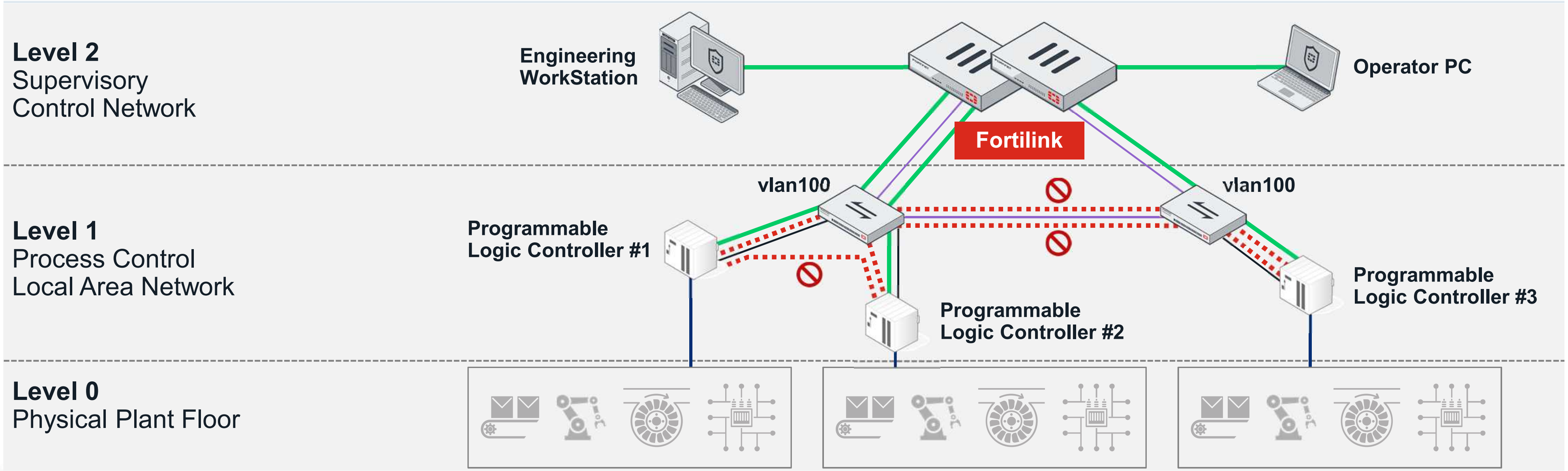




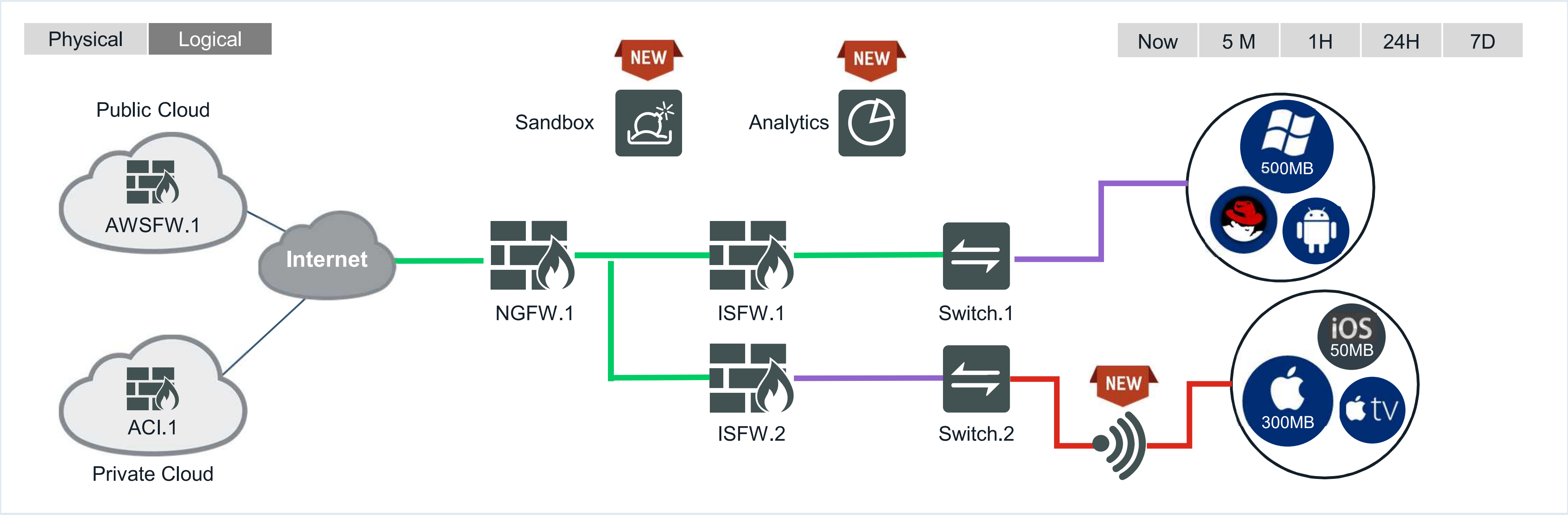
FORTINET

Purdue Model Zoning – 마이크로 세그멘테이션

- Process Layer의 추가적인 보안 적용 : VLAN 내의 트래픽 차단
  - 단말간에는 서로간에 보이지 않고,
  - 단말은 FortiGate를 통해서만 통신 가능
  - FortiGate는 필요한 단말간 또는 그룹간의 접근정책 만을 허용



제안2 : OT 네트워크 보안 가시성



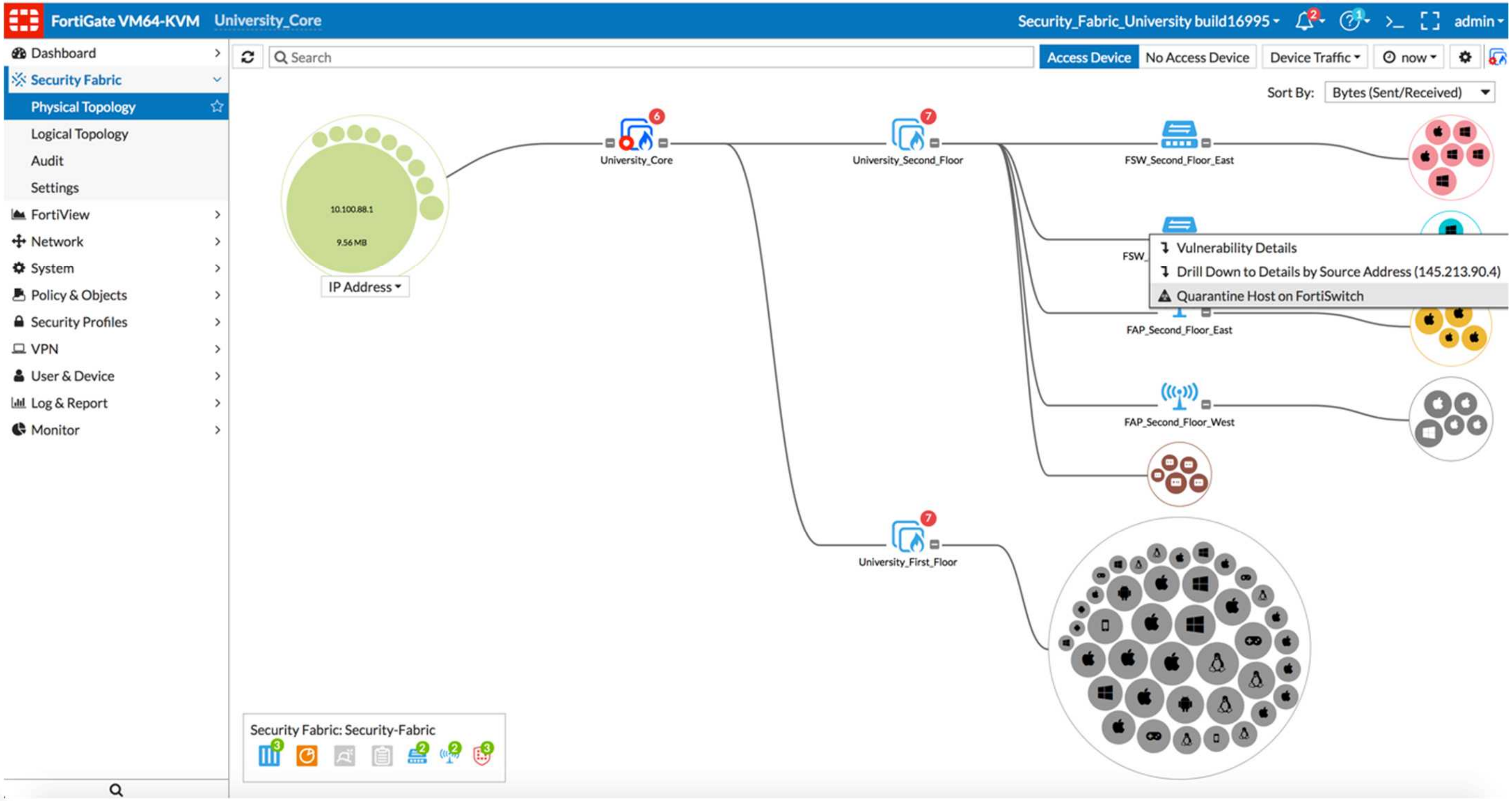
New Device and Status Visibility

New Historic Trending

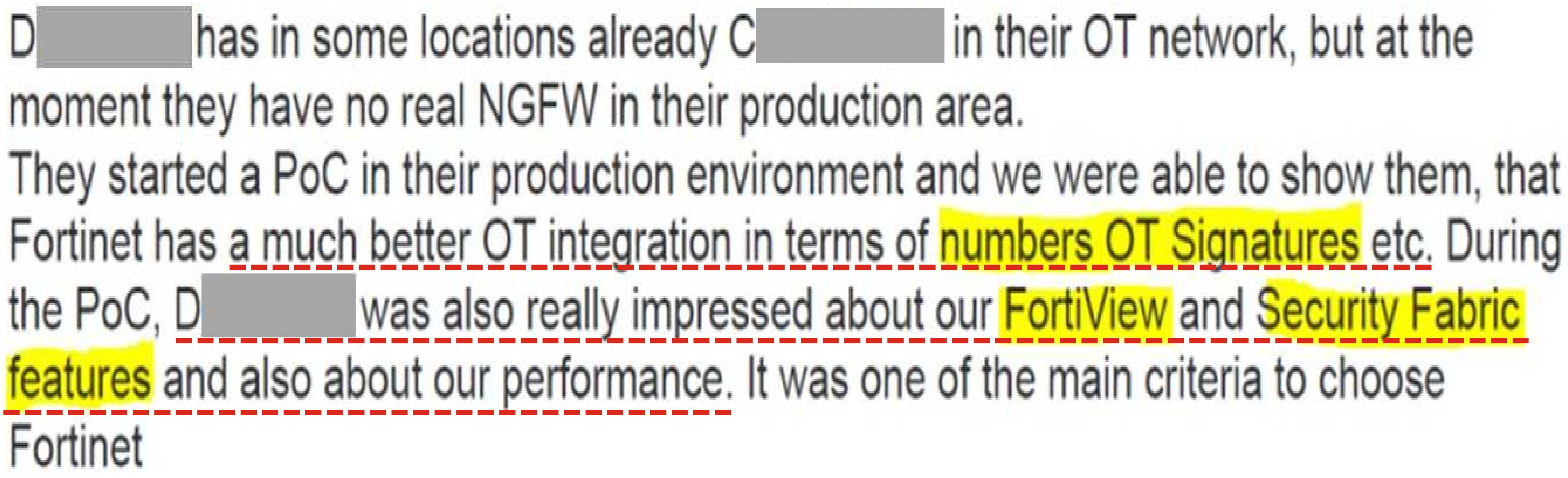
New Aggregate FortiGate View

New Downstream Device Quarantine

Security Fabric상의 네트워크 보안 가시성 확보



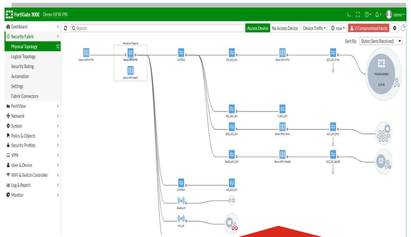
OT 네트워크 보안 가시성 - 해외 D그룹사 구축 사례



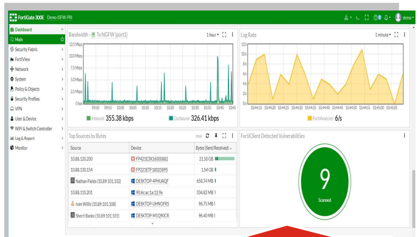
D[redacted] has in some locations already C[redacted] in their OT network, but at the moment they have no real NGFW in their production area.

They started a PoC in their production environment and we were able to show them, that Fortinet has a much better OT integration in terms of numbers OT Signatures etc. During the PoC, D[redacted] was also really impressed about our FortiView and Security Fabric features and also about our performance. It was one of the main criteria to choose Fortinet

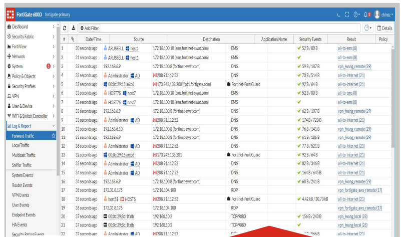
엔드투엔드 가시성



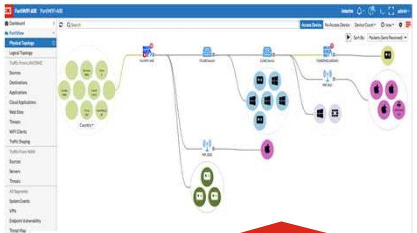
Connection Location



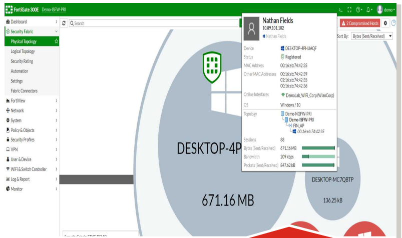
Network Usage



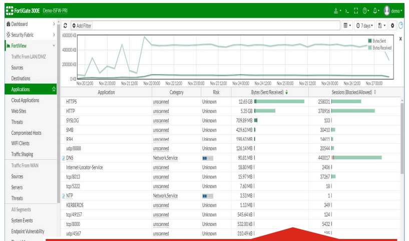
Traffic Type



Device Type

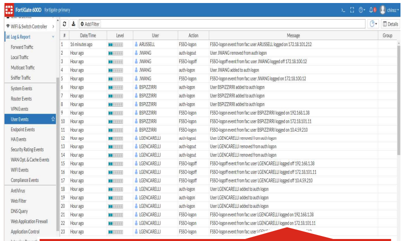


Device Information

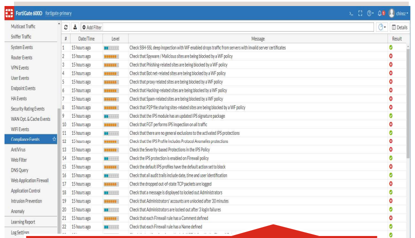


Applications

Security Threats



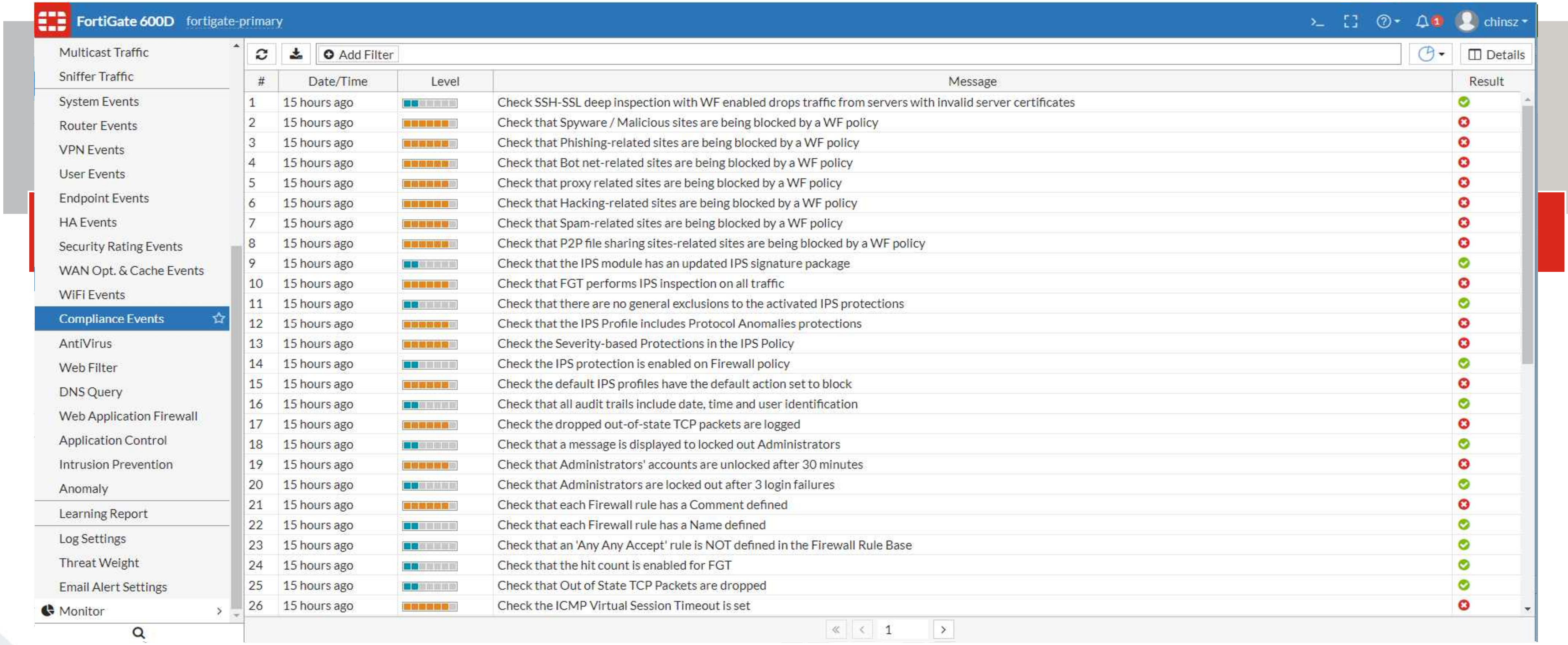
Actions Taken



Compliance

everything from connection level to applications and security

엔드투엔드 가시성



#	Date/Time	Level	Message	Result
1	15 hours ago	🟦	Check SSH-SSL deep inspection with WF enabled drops traffic from servers with invalid server certificates	✓
2	15 hours ago	🟧	Check that Spyware / Malicious sites are being blocked by a WF policy	✗
3	15 hours ago	🟧	Check that Phishing-related sites are being blocked by a WF policy	✗
4	15 hours ago	🟧	Check that Bot net-related sites are being blocked by a WF policy	✗
5	15 hours ago	🟧	Check that proxy related sites are being blocked by a WF policy	✗
6	15 hours ago	🟧	Check that Hacking-related sites are being blocked by a WF policy	✗
7	15 hours ago	🟧	Check that Spam-related sites are being blocked by a WF policy	✗
8	15 hours ago	🟧	Check that P2P file sharing sites-related sites are being blocked by a WF policy	✗
9	15 hours ago	🟦	Check that the IPS module has an updated IPS signature package	✓
10	15 hours ago	🟧	Check that FGT performs IPS inspection on all traffic	✗
11	15 hours ago	🟦	Check that there are no general exclusions to the activated IPS protections	✓
12	15 hours ago	🟧	Check that the IPS Profile includes Protocol Anomalies protections	✗
13	15 hours ago	🟧	Check the Severity-based Protections in the IPS Policy	✗
14	15 hours ago	🟦	Check the IPS protection is enabled on Firewall policy	✓
15	15 hours ago	🟧	Check the default IPS profiles have the default action set to block	✗
16	15 hours ago	🟦	Check that all audit trails include date, time and user identification	✓
17	15 hours ago	🟧	Check the dropped out-of-state TCP packets are logged	✗
18	15 hours ago	🟦	Check that a message is displayed to locked out Administrators	✓
19	15 hours ago	🟧	Check that Administrators' accounts are unlocked after 30 minutes	✗
20	15 hours ago	🟦	Check that Administrators are locked out after 3 login failures	✓
21	15 hours ago	🟧	Check that each Firewall rule has a Comment defined	✗
22	15 hours ago	🟦	Check that each Firewall rule has a Name defined	✓
23	15 hours ago	🟦	Check that an 'Any Any Accept' rule is NOT defined in the Firewall Rule Base	✓
24	15 hours ago	🟦	Check that the hit count is enabled for FGT	✓
25	15 hours ago	🟦	Check that Out of State TCP Packets are dropped	✓
26	15 hours ago	🟧	Check the ICMP Virtual Session Timeout is set	✗

everything from connection level to applications and security

산업 시스템을 위한 IPS / App-Control

지원 프로토콜

- BACnet
- DNP3
- Elcom
- EtherCAT
- EtherNet/IP
- HART
- IEC 60870-6 (TASE 2) /ICCP
- IEC 60870-5-104
- IEC 61850
- LONTalk
- MMS
- Modbus
- OPC
- Profinet
- S7
- SafetyNET
- Synchrophasor
- MMS

지원하는 어플리케이션 및 벤더

- 7 Technologies/ Schneider Electric
- ABB
- Advantech
- Broadwin
- CitectSCADA
- CoDeSys/3S-Smart
- Cogent
- DATAC
- Eaton
- GE
- Honeywell
- Iconics
- InduSoft
- IntelliCom
- Measuresoft
- Microsys
- MOXA
- PcVue
- Progea
- QNX
- RealFlex
- Rockwell
- RSLogix
- Siemens
- Sunway
- TeeChart
- VxWorks
- WellinTech
- Yokogawa

OT/ICS/SCADA 보안 – IPS 시그너쳐 제공

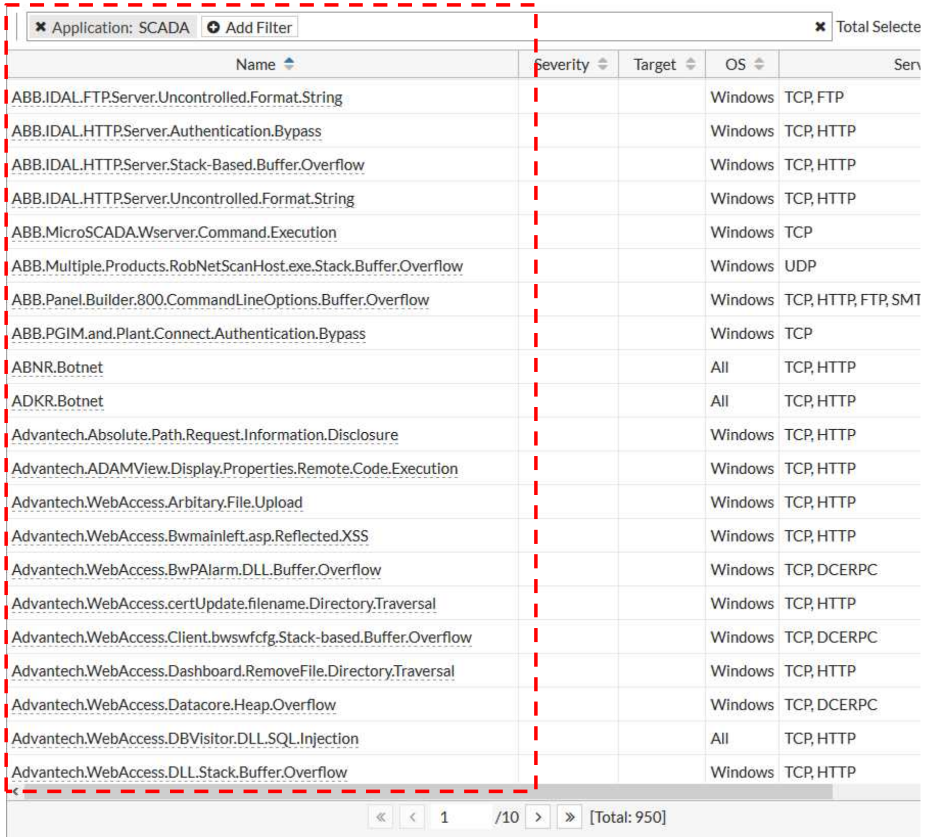
IPS 시그너쳐 제공 (Schneider Electric 예시)

- Schneider.ClearSCADA.OPF.File.Parsing.Out.of.Bounds.Array.Index (CVE-2014-0779)
- Schneider.ClearSCADA.Remote.Authentication.Bypass
- Schneider.Electric.Accutech.Manager.SQL.Injection
- Schneider.Electric.DTM.development.kit.Buffer.Overflow (CVE-2014-9200)
- Schneider.Electric.GP-Pro.EX.ParseAPI.Heap.Buffer.Overflow
- Schneider.Electric.InduSoftWebStudioAgent.Remote.Code.Execution (CVE-2015- 7374)
- Schneider.Electric.Interactive.Graphical.SCADA.Buffer.Overflow (CVE-2013-0657)
- Schneider.Electric.OSF.Configuration.File.Buffer.Overflow (CVE-2014-0774)
- Schneider.Electric.Pelco.DSNVs.Rvctl.RVControl.Buffer.Overflow (CVE-2015-0982)
- Schneider.Electric.ProClima.Atx45.ocx.ActiveX.Access (CVE-2014-8511, CVE-2014-8512)
- Schneider.Electric.ProClima.MDraw30.ocx.ActiveX.Access (CVE-2014-8513, CVE-2014-9188)
- Schneider.Electric.ProClima.MetaDraw.Buffer.Overflow (CVE-2014-8514)
- Schneider.Electric.SCADA.Expert.ClearSCADA.XSS (CVE-2014-5411)
- Schneider.Electric.VAMPSET.CFG.File.Handling.Buffer.Overflow (CVE-2014-8390)
- Schneider.Modicon.M340.Password.Buffer.Overflow (CVE-2015-7937)
- Schneider.Quantum.Module.Backdoor.Access (CVE-2011-4859)
- Schneider.SCADA.Expert.ClearSCADA.Authentication.Bypass (CVE-2014-5412)
- SchneiderElectric.ProClima.F1BookView.Memory.Corruption (CVE-2015-7918, CVE-2015-8561)
- SearchBlox.File.Exfiltration (CVE-2015-7919)
- Sielco.Sistemi.Winlog.File.Access.Directory.Traversal (CVE-2012-4356)
- Siemens.0day.40142
- Siemens.ALM.almaxcx.dll.ActiveX.Arbitrary.File.Overwrite (CVE-2011-4532)
- Siemens.Automation.License.Manager.DoS (CVE-2011-4529, CVE-2011-4531)
- Siemens.S7300.Hardcoded.Credentials.Security.Bypass
- Siemens.Simatic.WinCC.Default.Password (CVE-2010-2772)
- Siemens.SIMATIC.WinCC.Flexible.HmiLoad.Multiple.Vulnerabilities (CVE-2011-4877)
- Siemens.SIMATIC.WinCC.Flexible.miniweb.DoS (CVE-2011-4879)
- Siemens.Tecnomatix.FactoryLink.Multiple.Vulnerabilities

OT/ICS/SCADA 보안 – 버추얼 보안 패치

- SCADA 보안 침입방어 시그니처 내장
  - » 대부분의 OT 프로토콜을 식별하여 위협 트래픽 패턴을 탐지
  - » OT 제품의 취약점을 직접 패치하지 않더라도 산업 보안 시그니처를 통해 OT용 차세대 방화벽에서 통제

버추얼 보안 패치



Name	Severity	Target	OS	Serv
ABB.IDAL.FTP.Server.Uncontrolled.Format.String			Windows	TCP, FTP
ABB.IDAL.HTTP.Server.Authentication.Bypass			Windows	TCP, HTTP
ABB.IDAL.HTTP.Server.Stack-Based.Buffer.Overflow			Windows	TCP, HTTP
ABB.IDAL.HTTP.Server.Uncontrolled.Format.String			Windows	TCP, HTTP
ABB.MicroSCADA.Wserver.Command.Execution			Windows	TCP
ABB.Multiple.Products.RobNetScanHost.exe.Stack.Buffer.Overflow			Windows	UDP
ABB.Panel.Builder.800.CommandLineOptions.Buffer.Overflow			Windows	TCP, HTTP, FTP, SMT
ABB.PGIM.and.Plant.Connect.Authentication.Bypass			Windows	TCP
ABNR.Botnet			All	TCP, HTTP
ADKR.Botnet			All	TCP, HTTP
Advantech.Absolute.Path.Request.Information.Disclosure			Windows	TCP, HTTP
Advantech.ADAMView.Display.Properties.Remote.Code.Execution			Windows	TCP, HTTP
Advantech.WebAccess.Arbitary.File.Upload			Windows	TCP, HTTP
Advantech.WebAccess.Bwmainleft.asp.Reflected.XSS			Windows	TCP, HTTP
Advantech.WebAccess.BwPAlarm.DLL.Buffer.Overflow			Windows	TCP, DCERPC
Advantech.WebAccess.certUpdate.filename.Directory.Traversal			Windows	TCP, HTTP
Advantech.WebAccess.Client.bwswfcfg.Stack-based.Buffer.Overflow			Windows	TCP, DCERPC
Advantech.WebAccess.Dashboard.RemoveFile.Directory.Traversal			Windows	TCP, HTTP
Advantech.WebAccess.Datacore.Heap.Overflow			Windows	TCP, DCERPC
Advantech.WebAccess.DBVisitor.DLL.SQL.Injection			All	TCP, HTTP
Advantech.WebAccess.DLL.Stack.Buffer.Overflow			Windows	TCP, HTTP

« ‹ 1 /10 › » [Total: 950]

※ 포티넷은 산업 네트워크 보호를 위한 시그니처 개발에 지속적인 투자와 관심을 기울이고 있습니다.

OT/ICS/SCADA 보안 – 어플리케이션 제어

섬세한 OT 어플리케이션 제어 (DNP3 예시)

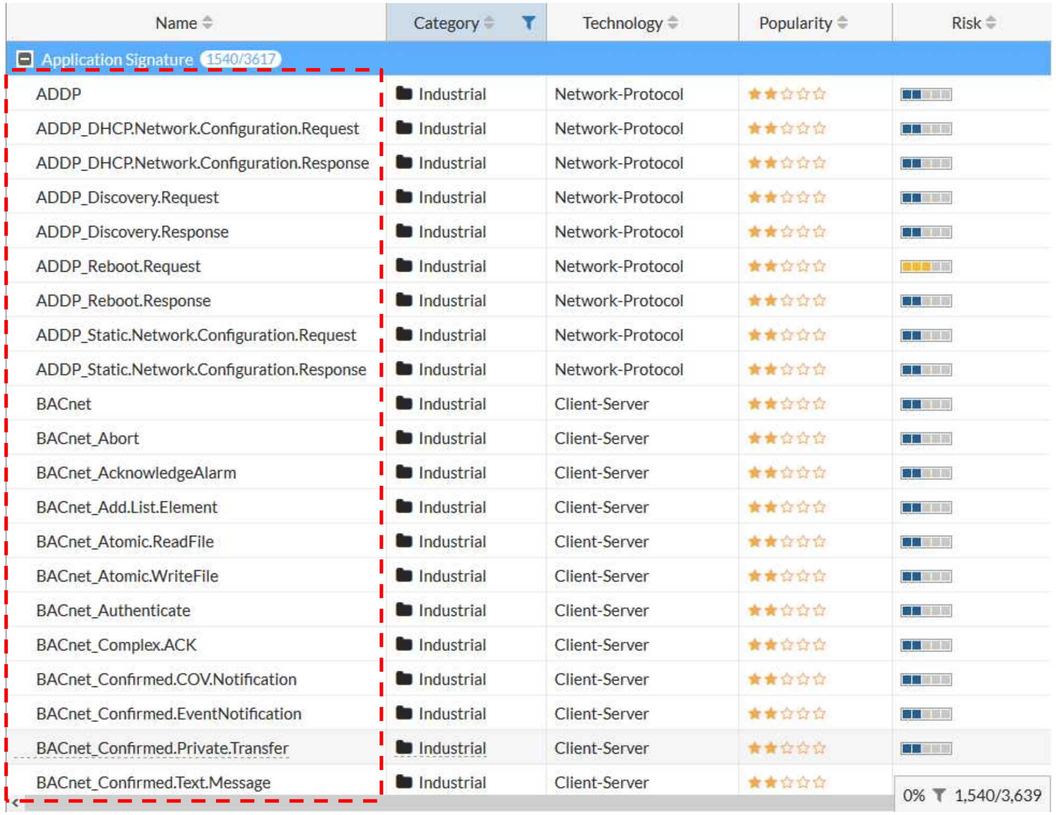
- DNP3
- DNP3_Assign.Class
- DNP3_Cold.Restart
- DNP3_Confirm
- DNP3_Delay.Measurement
- DNP3_Direct.Operate
- DNP3_Direct.Operate.Without.Ack
- DNP3_Disable.Spontaneous.Messages
- DNP3_Enable.Spontaneous.Messages
- DNP3_Freeze.And.Clear
- DNP3_Freeze.And.Clear.Without.Ack
- DNP3_Freeze.With.Time
- DNP3_Freeze.With.Time.Without.Ack
- DNP3_Immediate.Freeze
- DNP3_Immediate.Freeze.Without.Ack
- DNP3_Initialize.Application
- DNP3_Initialize.Data
- DNP3_Operate
- DNP3_Read
- DNP3_Response
- DNP3_Save.Configuration
- DNP3_Select
- DNP3_Start.Application
- DNP3_Stop.Application
- DNP3_Unsolicited.Message
- DNP3_Warm.Restart
- DNP3_Write

OT/ICS/SCADA 보안 -- 어플리케이션 제어

- 산업 네트워크 어플리케이션 시그니처 내장
  - » 산업 현장에서 사용되는 프로토콜의 상세 Action 단위로 제어
  - » 현장에서 꼭 필요하거나 사용중인 액션만 허용하고 불필요한 패턴은 탐지 또는 차단 가능

OT 어플리케이션 제어

※ 포티넷은 산업 네트워크 보호를 위한 시그니처 개발에 지속적인 투자와 관심을 기울이고 있습니다.

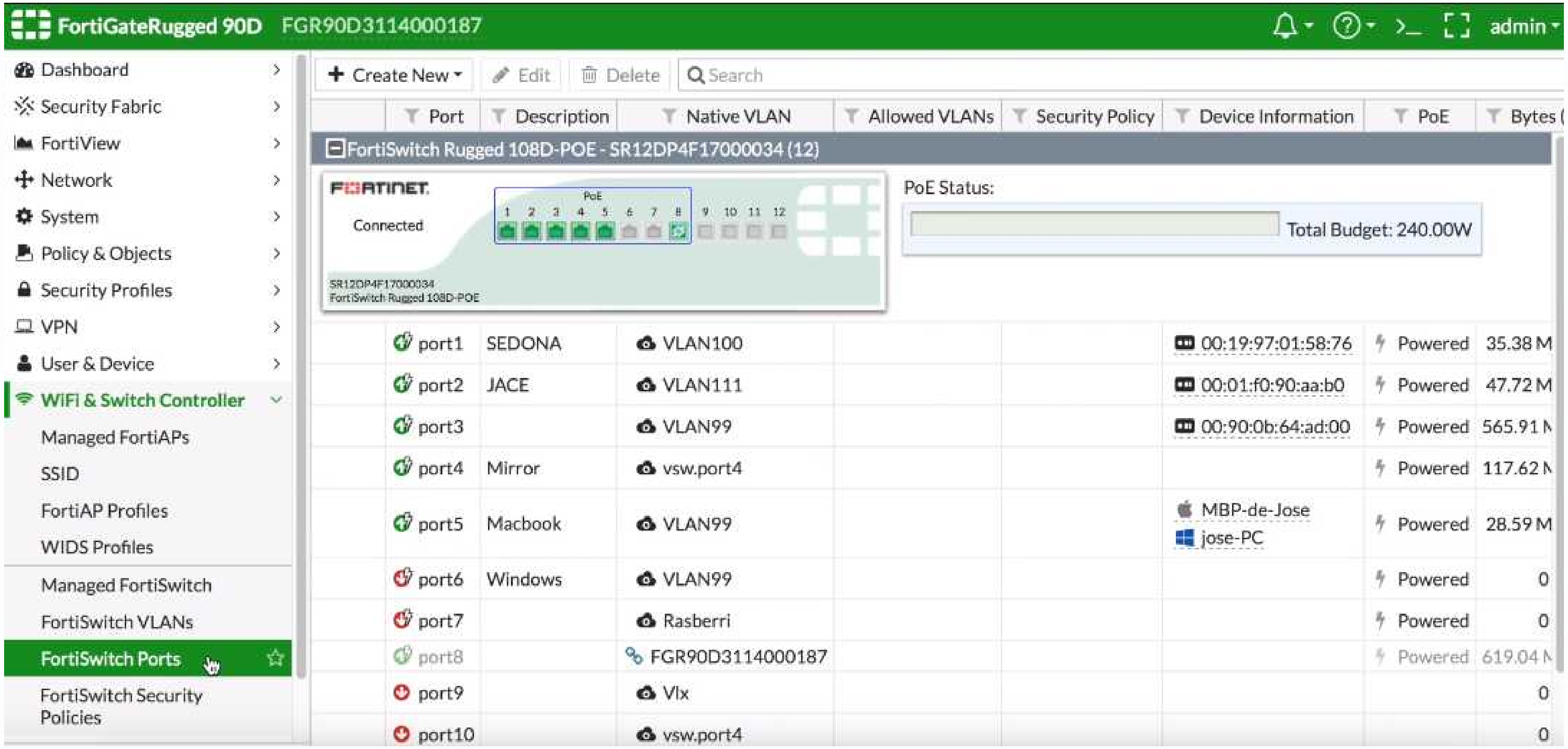


Name	Category	Technology	Popularity	Risk
Application Signature 1540/3617				
ADDP	Industrial	Network-Protocol	★★☆☆☆	■■□□□
ADDP_DHCP.Network.Configuration.Request	Industrial	Network-Protocol	★★☆☆☆	■■□□□
ADDP_DHCP.Network.Configuration.Response	Industrial	Network-Protocol	★★☆☆☆	■■□□□
ADDP_Discovery.Request	Industrial	Network-Protocol	★★☆☆☆	■■□□□
ADDP_Discovery.Response	Industrial	Network-Protocol	★★☆☆☆	■■□□□
ADDP_Reboot.Request	Industrial	Network-Protocol	★★☆☆☆	■■■□□
ADDP_Reboot.Response	Industrial	Network-Protocol	★★☆☆☆	■■□□□
ADDP_Static.Network.Configuration.Request	Industrial	Network-Protocol	★★☆☆☆	■■□□□
ADDP_Static.Network.Configuration.Response	Industrial	Network-Protocol	★★☆☆☆	■■□□□
BACnet	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Abort	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_AcknowledgeAlarm	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Add.List.Element	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Atomic.ReadFile	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Atomic.WriteFile	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Authenticate	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Complex.ACK	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Confirmed.COV.Notification	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Confirmed.EventNotification	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Confirmed.Private.Transfer	Industrial	Client-Server	★★☆☆☆	■■□□□
BACnet_Confirmed.Text.Message	Industrial	Client-Server	★★☆☆☆	0% 1,540/3,639

FORTINET

OT 네트워크 보안 구성 : 유무선 통합관리

스위치 통합관리



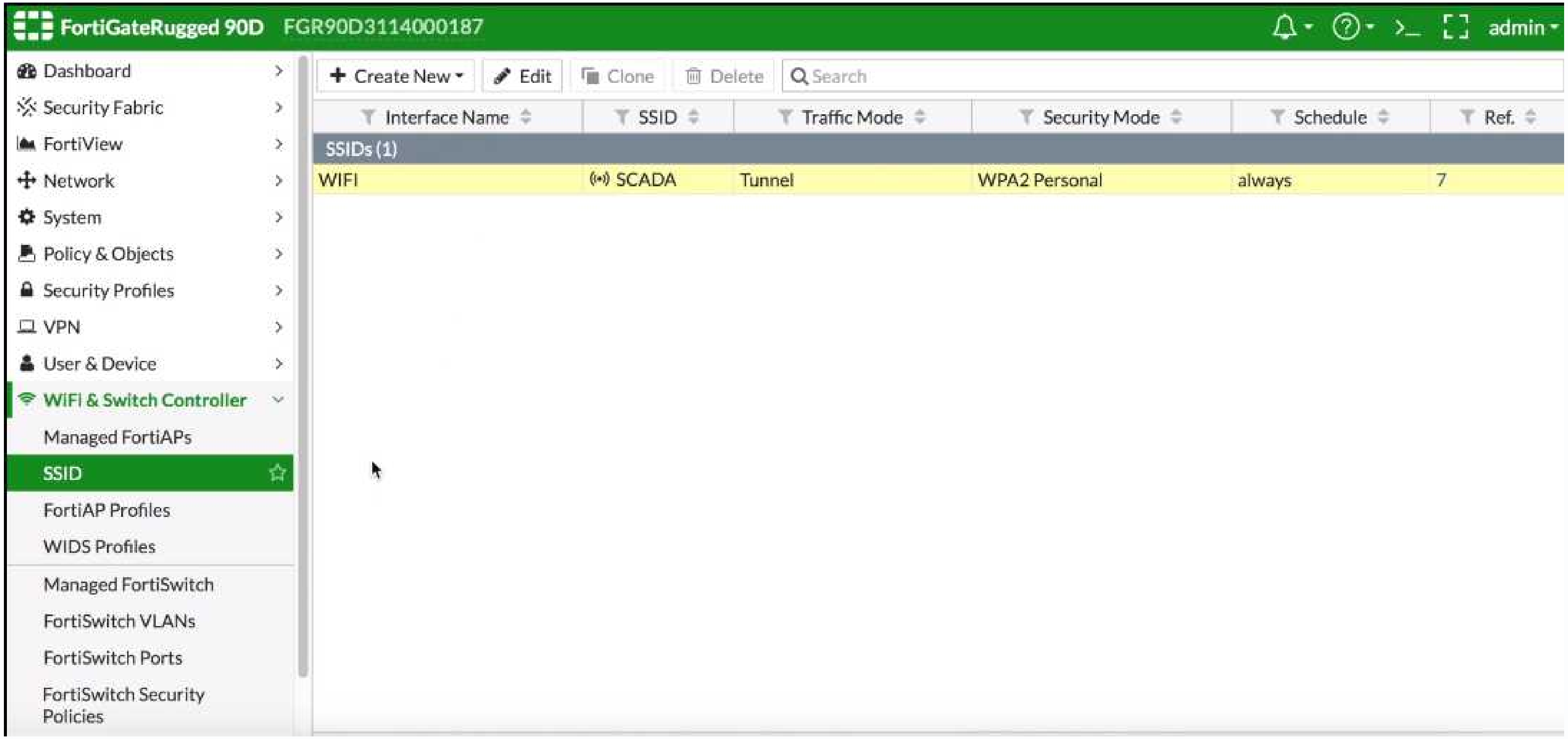
FortiSwitch Rugged 108D-POE - SR12DP4F17000034 (12)

PoE Status: Total Budget: 240.00W

Port	Description	Native VLAN	Allowed VLANs	Security Policy	Device Information	PoE	Bytes (
port1	SEDONA	VLAN100			00:19:97:01:58:76	Powered	35.38 M
port2	JACE	VLAN111			00:01:f0:90:aa:b0	Powered	47.72 M
port3		VLAN99			00:90:0b:64:ad:00	Powered	565.91 N
port4	Mirror	vsw.port4				Powered	117.62 N
port5	Macbook	VLAN99			MBP-de-Jose jose-PC	Powered	28.59 M
port6	Windows	VLAN99				Powered	0
port7		Rasberri				Powered	0
port8		FGR90D3114000187				Powered	619.04 N
port9		Vlx					0
port10		vsw.port4					0

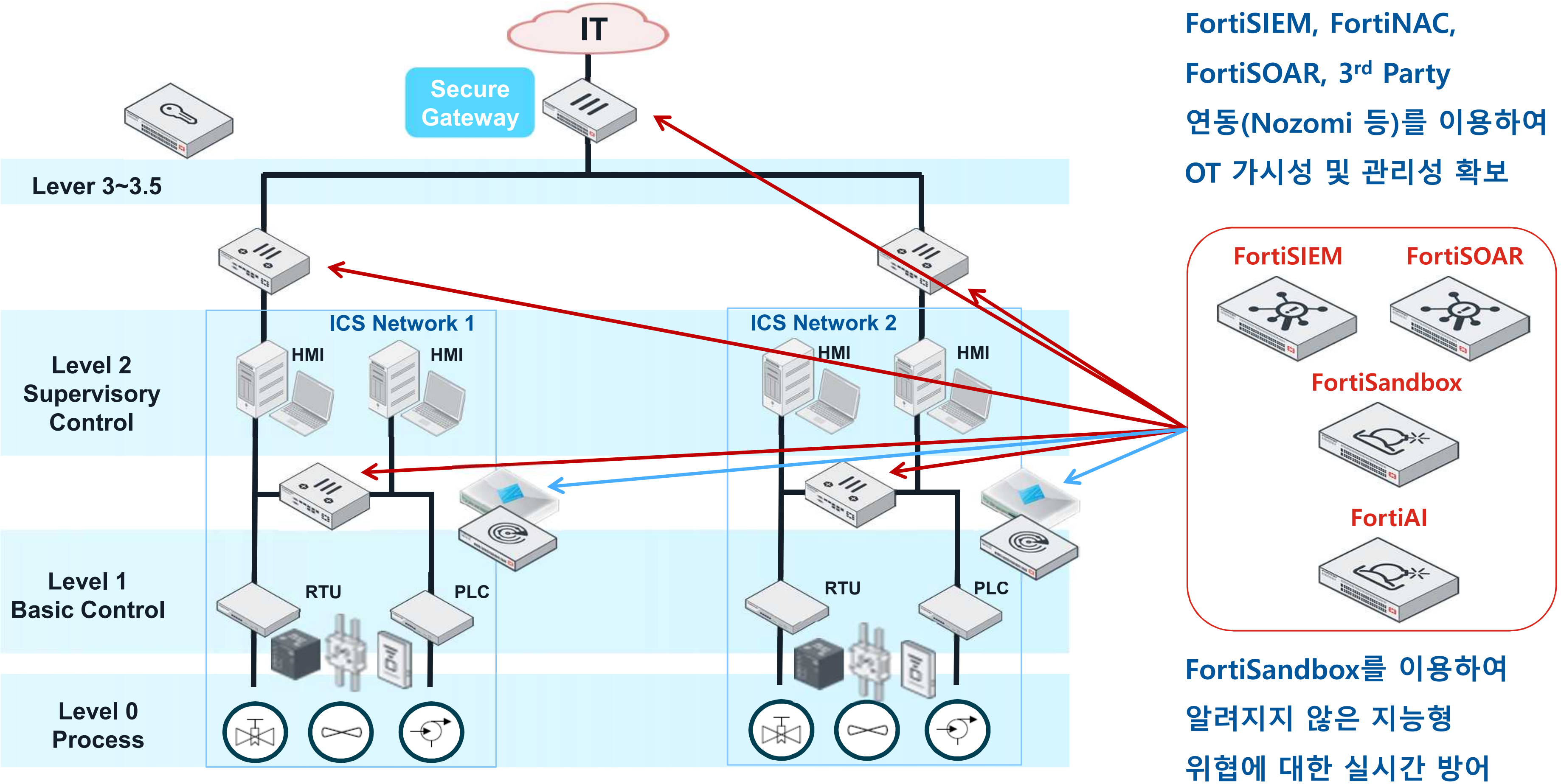
OT 네트워크 보안 구성 : 유무선 통합관리

무선AP 통합 관리 (FortiAP)



Interface Name	SSID	Traffic Mode	Security Mode	Schedule	Ref.
SSIDs (1)					
WIFI	SCADA	Tunnel	WPA2 Personal	always	7

제안3 : OT 보안 관리 및 APT 탐지방어 기능



FortiSIEM, FortiNAC, FortiSOAR, 3rd Party 연동(Nozomi 등)를 이용하여 OT 가시성 및 관리성 확보

FortiSandbox를 이용하여 알려지지 않은 지능형 위협에 대한 실시간 방어

※ OT VMS : Visibility, Management, Security
(OT 가시성, 관리성, 보안성)

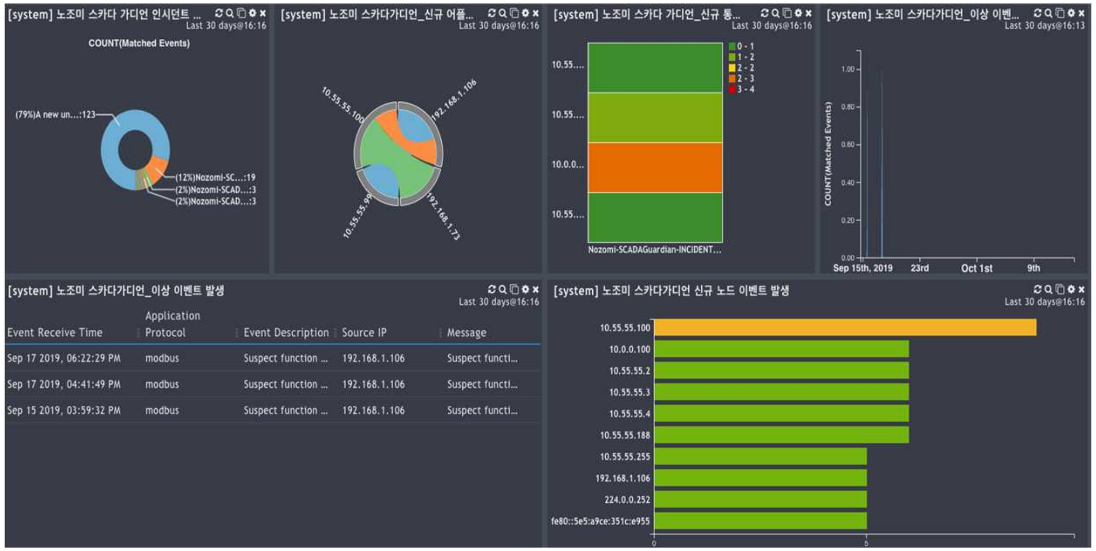
OT-VMS (가시성, 관리성, 보안성) 제공

FortiSIEM

- 사전 정의된 Report, 대시보드, Log Parser
- 다양한 글로벌 벤더 제품과도 빠르고 손쉽게 연동 및 운영 가능
- 비정상 행위 발생시 이에 대한 방어 액션 스크립트를 자동으로 전달

Nozomi ScadaGuardian

- OT 전문 가시성 및 관리 솔루션
- 특정 단말 차단 필요시 자동으로 방화벽 정책을 생성하여 FortiGate에게 전달
- FortiSIEM, FortiNAC 과 연동



[system] 노조미 스카다 가디언 인시던트 ... Last 30 days@16:16

[system] 노조미 스카다가디언_신규 어플... Last 30 days@16:16

[system] 노조미 스카다 가디언_신규 통... Last 30 days@16:16

[system] 노조미 스카다가디언_이상 이벤... Last 30 days@16:13

[system] 노조미 스카다가디언_이상 이벤트 발생 Last 30 days@16:16

Event Receive Time	Application Protocol	Event Description	Source IP	Message
Sep 17 2019, 06:22:29 PM	modbus	Suspect function ...	192.168.1.106	Suspect functi...
Sep 17 2019, 04:41:49 PM	modbus	Suspect function ...	192.168.1.106	Suspect functi...
Sep 15 2019, 03:59:32 PM	modbus	Suspect function ...	192.168.1.106	Suspect functi...

[system] 노조미 스카다가디언 신규 노드 이벤트 발생 Last 30 days@16:16

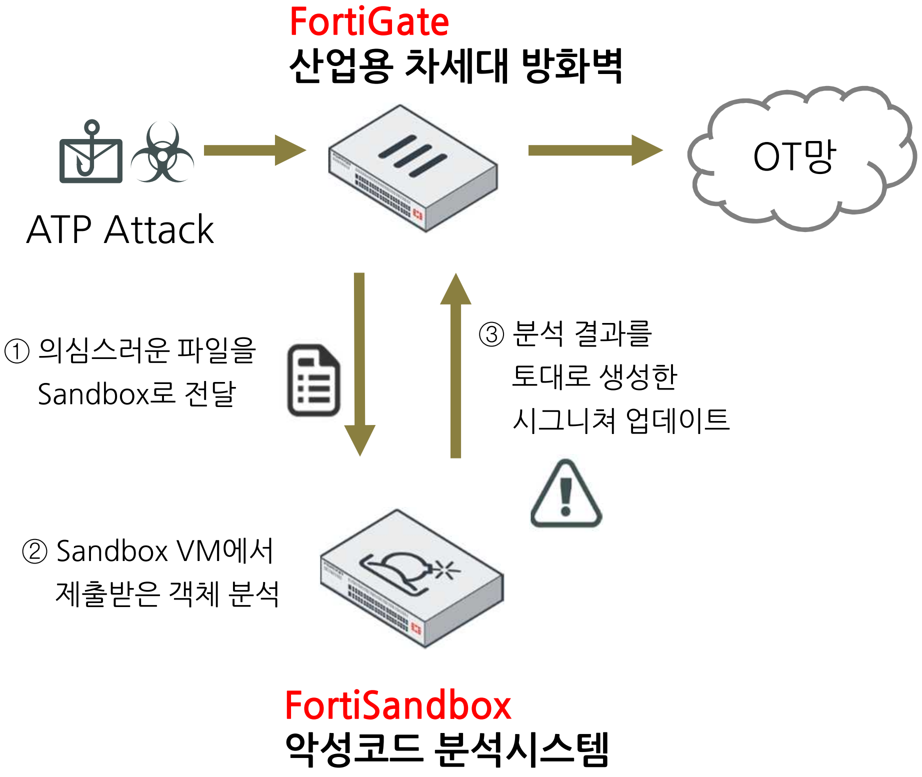
APT 탐지방어 기능 : 제로데이 악성코드/멀웨어 탐지

FortiGate (산업용 차세대 방화벽)

- 1차 보안 필터링(AV, IPS, WF, SSL, AC, DoS…)
- CDR (문서 무해화) 기능
- 샌드박스 분석 결과를 로컬 DB 업데이트 후 자동 차단

FortiSandbox (악성코드 분석시스템)

- FortiGate에서 객체 수신
- 모든실행파일 및 URL접속 행위분석
- 위험등급 지정 및 결과값 반환
- 위협 인텔리전스 동적 생성 및 배포(AV DB)
- 타 보안 장비와 연동 가능한 표준 위협 공유 지원 (STIX/IOC)


FortiGate
산업용 차세대 방화벽
ATP Attack
OT망
① 의심스러운 파일을 Sandbox로 전달
② Sandbox VM에서 제출받은 객체 분석
③ 분석 결과를 토대로 생성한 시그니쳐 업데이트
FortiSandbox
악성코드 분석시스템

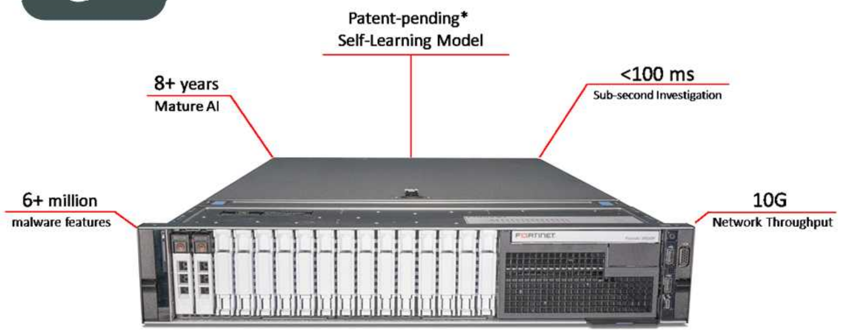
F⠿RTINET

FortiAI: 가상 보안 분석가™

업계 최초 온프레미스 딥 러닝 AI 모델

가상 보안 분석가™ **심층 신경망**을 통해 위협을 식별 및 분류하고 **1초** 안에 멀웨어를 탐지함.

FortiAI
가상 보안 분석가™



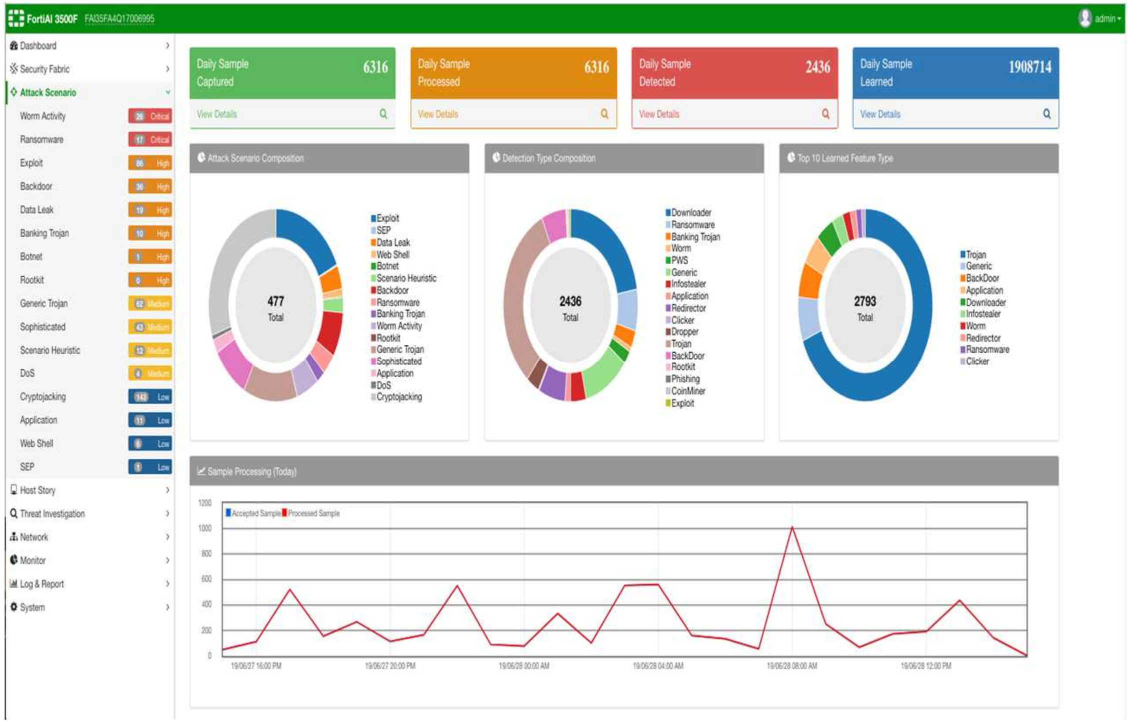
Patent-pending*
Self-Learning Model

8+ years
Mature AI

<100 ms
Sub-second Investigation

6+ million
malware features

10G
Network Throughput



FortiAI 3500F FAI35FA4Q17006995

admin ▾

- Dashboard ›
- Security Fabric ›
- Attack Scenario ⌄

Worm Activity	26	Critical
Ransomware	17	Critical
Exploit	86	High
Backdoor	36	High
Data Leak	19	High
Banking Trojan	10	High
Botnet	1	High
Rootkit	0	High
Generic Trojan	62	Medium
Sophisticated	43	Medium
Scenario Heuristic	12	Medium
DoS	4	Medium
Cryptojacking	143	Low
Application	11	Low
Web Shell	6	Low
SEP	1	Low

- Host Story ›
- Threat Investigation ›
- Network ›
- Monitor ›
- Log & Report ›
- System ›

Daily Sample Captured	6316
Daily Sample Processed	6316
Daily Sample Detected	2436
Daily Sample Learned	1908714

AGENDA

1 OT & 보안 위협 동향

2 포티넷과 ICS 벤더사와 협업 사례

3 포티넷 OT 보안 아키텍처와 구축 예시

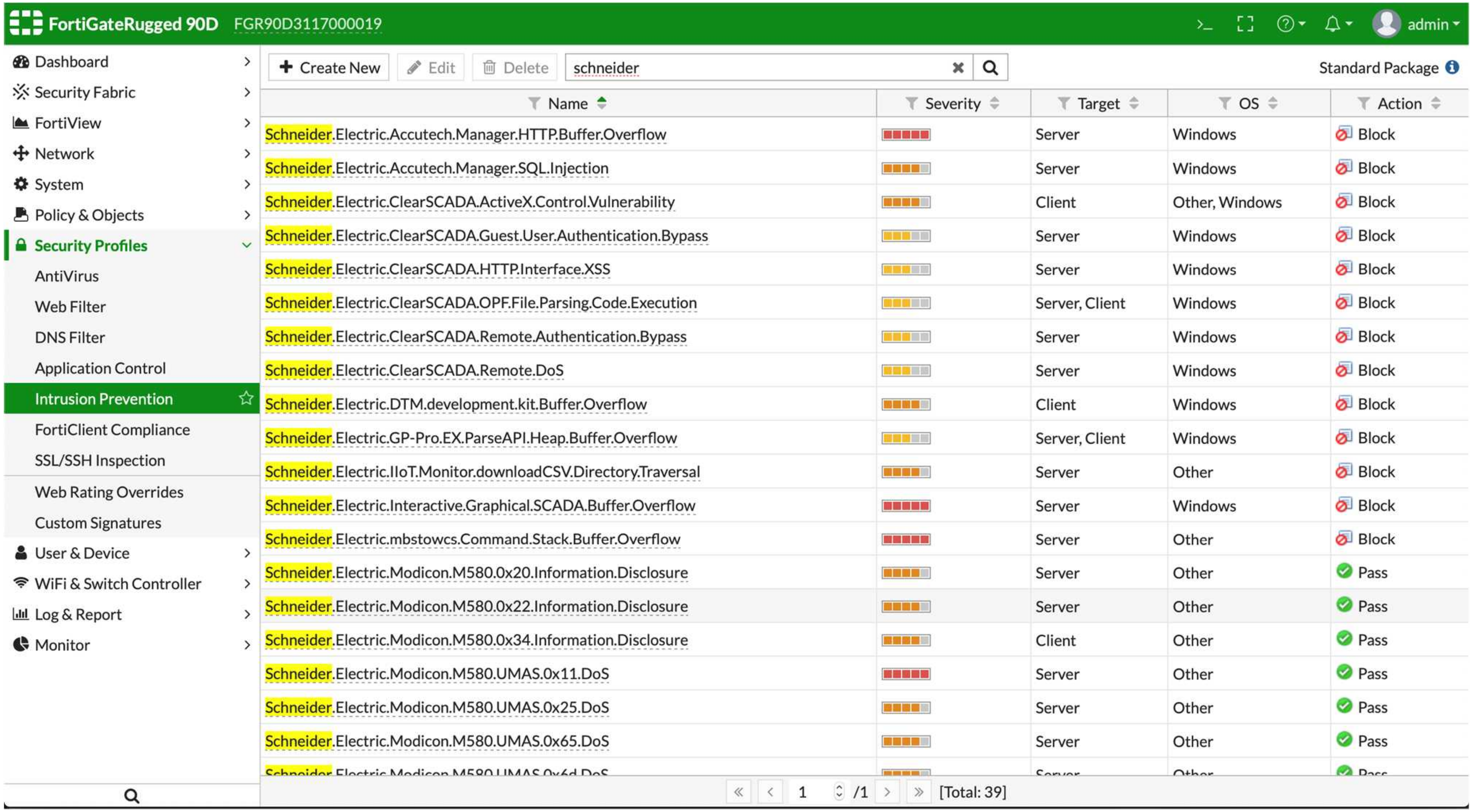
4 OT/ICS/SCADA 인프라 보호 제안

5 **OT 보안 취약성 방어 데모**

데모1. IDP/IPS Signature Virtual Patching

- **CVE 2017-7575: Schneider Electric Modicon** TM221CE16R 1.3.3.3 devices
- Allow remote attackers to **discover** the application-protection **password** via a *\x00\x01\x00\x00\x00\x05\x01\x5a\x00\x03\x00* request to the Modbus port (502/tcp).
- Subsequently the application may be arbitrarily downloaded, **modified**, and uploaded.

데모1. IDP/IPS Signature Virtual Patching



schneider

Name	Severity	Target	OS	Action
Schneider.Electric.Accutech.Manager.HTTP.Buffer.Overflow	■■■■■	Server	Windows	Block
Schneider.Electric.Accutech.Manager.SQL.Injection	■■■■□	Server	Windows	Block
Schneider.Electric.ClearSCADA.ActiveX.Control.Vulnerability	■■■■□	Client	Other, Windows	Block
Schneider.Electric.ClearSCADA.Guest.User.Authentication.Bypass	■■■□□	Server	Windows	Block
Schneider.Electric.ClearSCADA.HTTP.Interface.XSS	■■■□□	Server	Windows	Block
Schneider.Electric.ClearSCADA.OPF.File.Parsing.Code.Execution	■■■□□	Server, Client	Windows	Block
Schneider.Electric.ClearSCADA.Remote.Authentication.Bypass	■■■□□	Server	Windows	Block
Schneider.Electric.ClearSCADA.Remote.DoS	■■■□□	Server	Windows	Block
Schneider.Electric.DTM.development.kit.Buffer.Overflow	■■■■□	Client	Windows	Block
Schneider.Electric.GP-Pro.EX.ParseAPI.Heap.Buffer.Overflow	■■■□□	Server, Client	Windows	Block
Schneider.Electric.IIoT.Monitor.downloadCSV.Directory.Traversal	■■■■□	Server	Other	Block
Schneider.Electric.Interactive.Graphical.SCADA.Buffer.Overflow	■■■■■	Server	Windows	Block
Schneider.Electric.mbstowcs.Command.Stack.Buffer.Overflow	■■■■■	Server	Other	Block
Schneider.Electric.Modicon.M580.0x20.Information.Disclosure	■■■■□	Server	Other	✓ Pass
Schneider.Electric.Modicon.M580.0x22.Information.Disclosure	■■■■□	Server	Other	✓ Pass
Schneider.Electric.Modicon.M580.0x34.Information.Disclosure	■■■■□	Client	Other	✓ Pass
Schneider.Electric.Modicon.M580.UMAS.0x11.DoS	■■■■■	Server	Other	✓ Pass
Schneider.Electric.Modicon.M580.UMAS.0x25.DoS	■■■■□	Server	Other	✓ Pass
Schneider.Electric.Modicon.M580.UMAS.0x65.DoS	■■■■□	Server	Other	✓ Pass
Schneider.Electric.Modicon.M580.UMAS.0x4d.DoS	■■■■□	Server	Other	✓ Pass

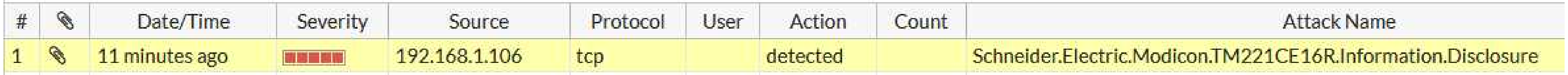
1 /1 [Total: 39]

FORTINET

데모1. IDP/IPS Signature Virtual Patching

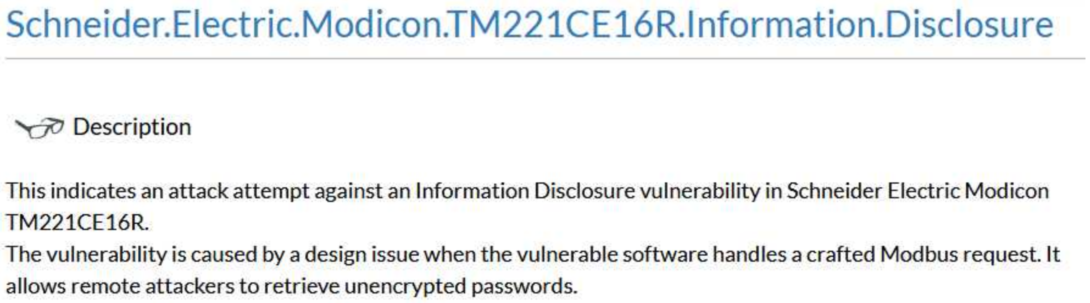
해커 Linux에서 다음 명령 수행

```
echo -n -e '₩x00₩x01₩x00₩x00₩x00₩x05₩x01₩x5a₩x00₩x03₩x00' | nc 10.55.55.99 502
echo -n -e '₩x00₩x01₩x00₩x00₩x00₩x05₩x01₩x5a₩x00₩x03₩x00' | nc 10.55.55.100 502
```



#	📎	Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1	📎	11 minutes ago	■■■■■	192.168.1.106	tcp		detected		Schneider.Electric.Modicon.TM221CE16R.Information.Disclosure

https://fortiguard.com/encyclopedia/ips/44293



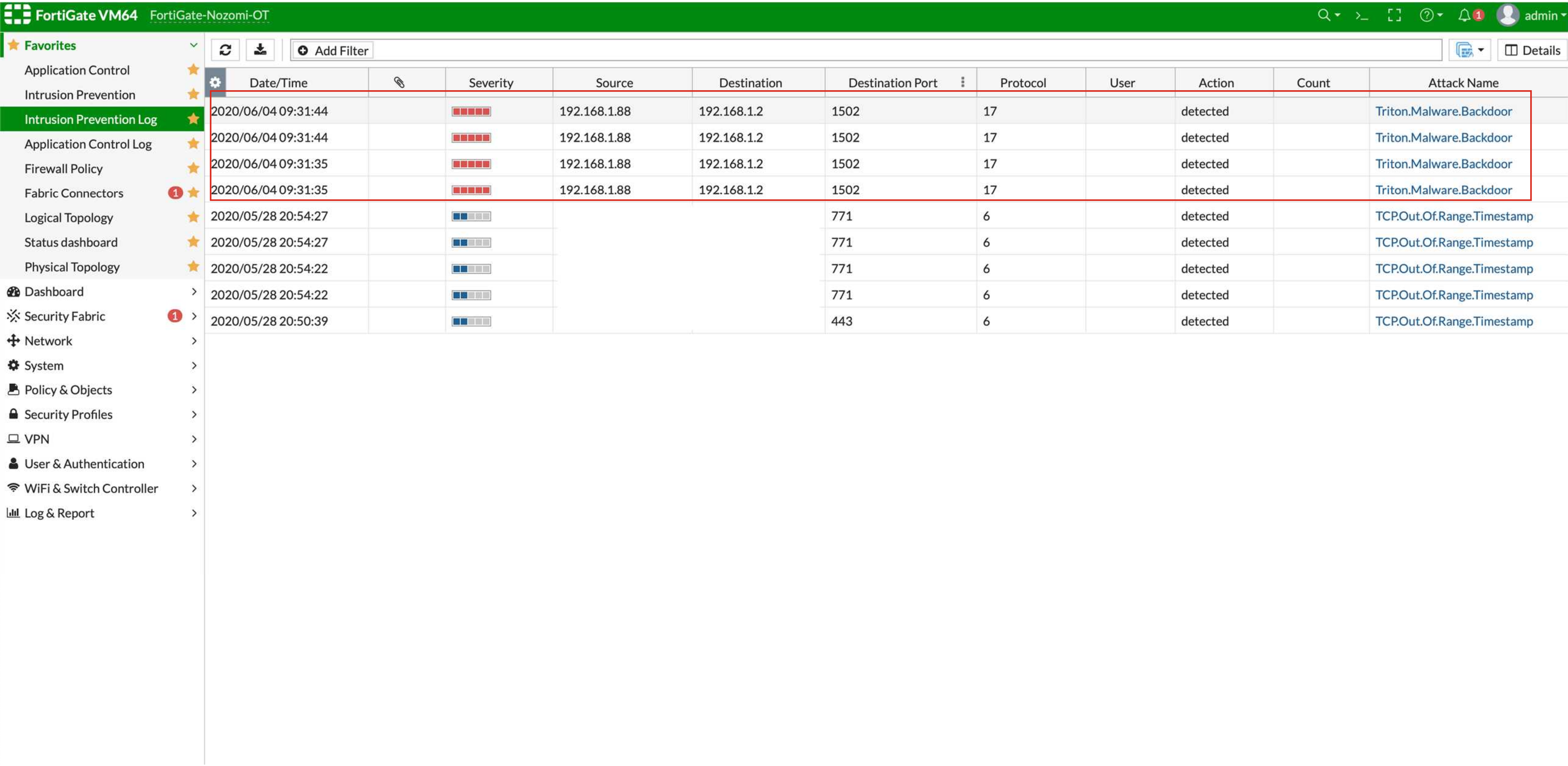
Schneider.Electric.Modicon.TM221CE16R.Information.Disclosure

Description

This indicates an attack attempt against an Information Disclosure vulnerability in Schneider Electric Modicon TM221CE16R.
The vulnerability is caused by a design issue when the vulnerable software handles a crafted Modbus request. It allows remote attackers to retrieve unencrypted passwords.

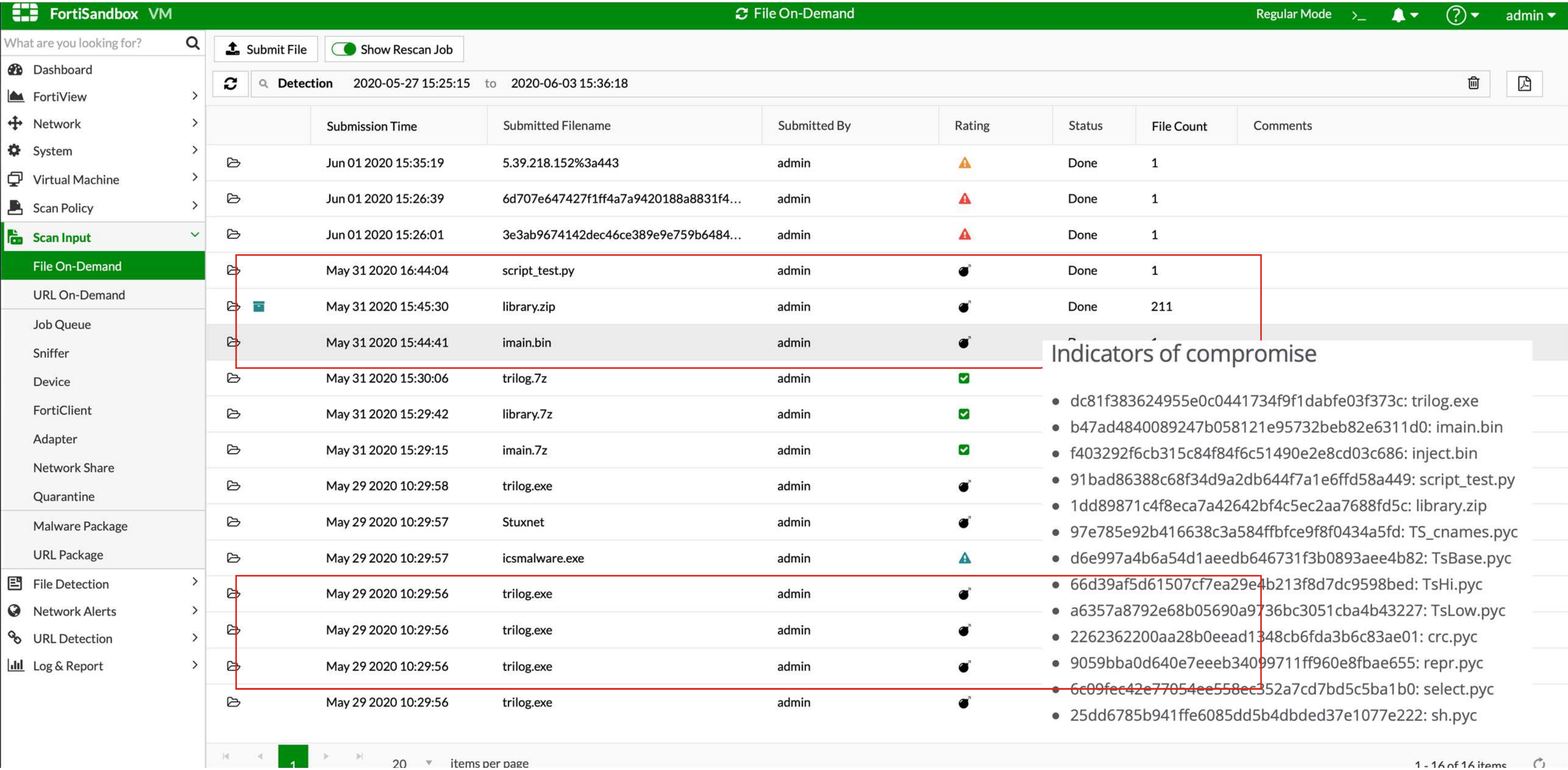
데모1. FortiGate – Triton Malware

"Triton.Malware.Backdoor" Industrial DB v15.00856



Date/Time		Severity	Source	Destination	Destination Port	Protocol	User	Action	Count	Attack Name
2020/06/04 09:31:44		🟥🟥🟥🟥🟥	192.168.1.88	192.168.1.2	1502	17		detected		Triton.Malware.Backdoor
2020/06/04 09:31:44		🟥🟥🟥🟥🟥	192.168.1.88	192.168.1.2	1502	17		detected		Triton.Malware.Backdoor
2020/06/04 09:31:35		🟥🟥🟥🟥🟥	192.168.1.88	192.168.1.2	1502	17		detected		Triton.Malware.Backdoor
2020/06/04 09:31:35		🟥🟥🟥🟥🟥	192.168.1.88	192.168.1.2	1502	17		detected		Triton.Malware.Backdoor
2020/05/28 20:54:27		🟦🟦⬜⬜⬜			771	6		detected		TCP.Out.Of.Range.Timestamp
2020/05/28 20:54:27		🟦🟦⬜⬜⬜			771	6		detected		TCP.Out.Of.Range.Timestamp
2020/05/28 20:54:22		🟦🟦⬜⬜⬜			771	6		detected		TCP.Out.Of.Range.Timestamp
2020/05/28 20:54:22		🟦🟦⬜⬜⬜			771	6		detected		TCP.Out.Of.Range.Timestamp
2020/05/28 20:50:39		🟦🟦⬜⬜⬜			443	6		detected		TCP.Out.Of.Range.Timestamp

데모1. FortiSandbox – Triton Malware



Detection 2020-05-27 15:25:15 to 2020-06-03 15:36:18

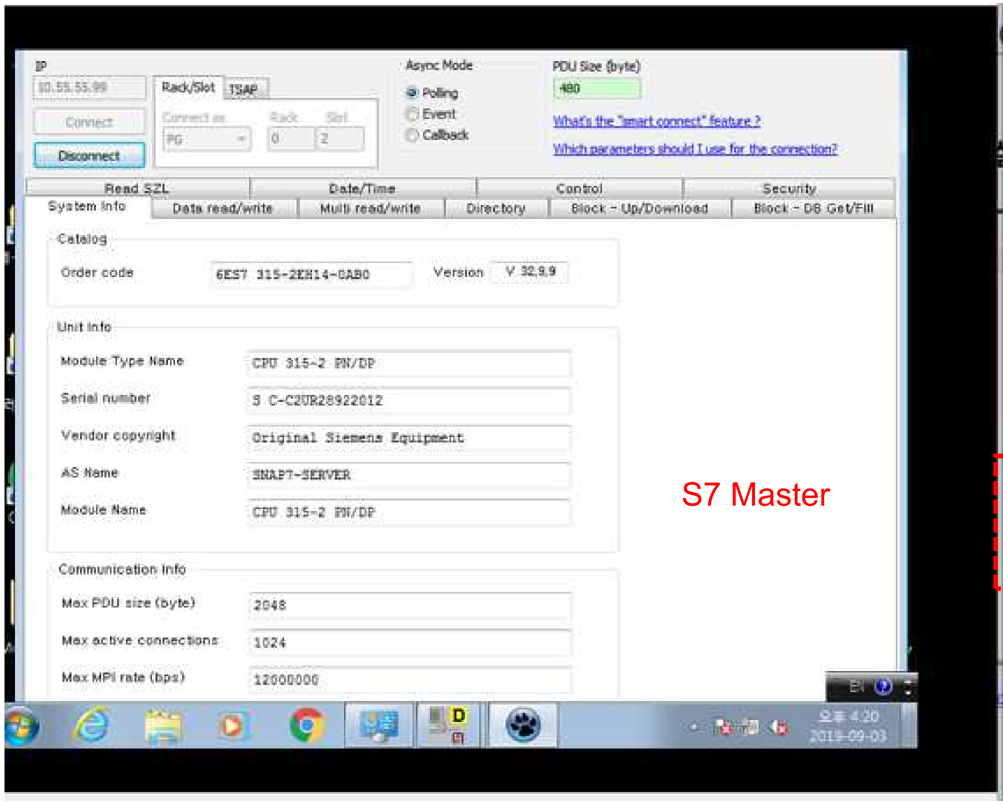
Submission Time	Submitted Filename	Submitted By	Rating	Status	File Count	Comments
Jun 01 2020 15:35:19	5.39.218.152%3a443	admin	⚠	Done	1	
Jun 01 2020 15:26:39	6d707e647427f1ff4a7a9420188a8831f4…	admin	⚠	Done	1	
Jun 01 2020 15:26:01	3e3ab9674142dec46ce389e9e759b6484…	admin	⚠	Done	1	
May 31 2020 16:44:04	script_test.py	admin	💣	Done	1	
May 31 2020 15:45:30	library.zip	admin	💣	Done	211	
May 31 2020 15:44:41	imain.bin	admin	💣			
May 31 2020 15:30:06	trilog.7z	admin	☑			
May 31 2020 15:29:42	library.7z	admin	☑			
May 31 2020 15:29:15	imain.7z	admin	☑			
May 29 2020 10:29:58	trilog.exe	admin	💣			
May 29 2020 10:29:57	Stuxnet	admin	💣			
May 29 2020 10:29:57	icsmalware.exe	admin	⚠			
May 29 2020 10:29:56	trilog.exe	admin	💣			
May 29 2020 10:29:56	trilog.exe	admin	💣			
May 29 2020 10:29:56	trilog.exe	admin	💣			
May 29 2020 10:29:56	trilog.exe	admin	💣			

Indicators of compromise

- dc81f383624955e0c0441734f9f1dabfe03f373c: trilog.exe
- b47ad4840089247b058121e95732beb82e6311d0: imain.bin
- f403292f6cb315c84f84f6c51490e2e8cd03c686: inject.bin
- 91bad86388c68f34d9a2db644f7a1e6ffd58a449: script_test.py
- 1dd89871c4f8eca7a42642bf4c5ec2aa7688fd5c: library.zip
- 97e785e92b416638c3a584ffbfce9f8f0434a5fd: TS_cnames.pyc
- d6e997a4b6a54d1aeedb646731f3b0893aee4b82: TsBase.pyc
- 66d39af5d61507cf7ea29e4b213f8d7dc9598bed: TsHi.pyc
- a6357a8792e68b05690a9736bc3051cba4b43227: TsLow.pyc
- 2262362200aa28b0eead1348cb6fda3b6c83ae01: crc.pyc
- 9059bba0d640e7eeeb34099711ff960e8fbae655: repr.pyc
- 6c09fec42e77054ee558ec352a7cd7bd5c5ba1b0: select.pyc
- 25dd6785b941ffe6085dd5b4dbded37e1077e222: sh.pyc

데모2. PLC 스캔 차단

Simens S7 PLC : Windows에서 S7 PLC 에뮬레이터 실행



IP: 10.55.55.99

Rack/Slot | TSAP — Connect as: PG, Rack: 0, Slot: 2

Async Mode: ● Polling ○ Event ○ Callback

PDU Size (byte): 480

What's the "smart connect" feature ?

Which parameters should I use for the connection?

Catalog

Order code: 6ES7 315-2EH14-0AB0 Version: V 32.9.9

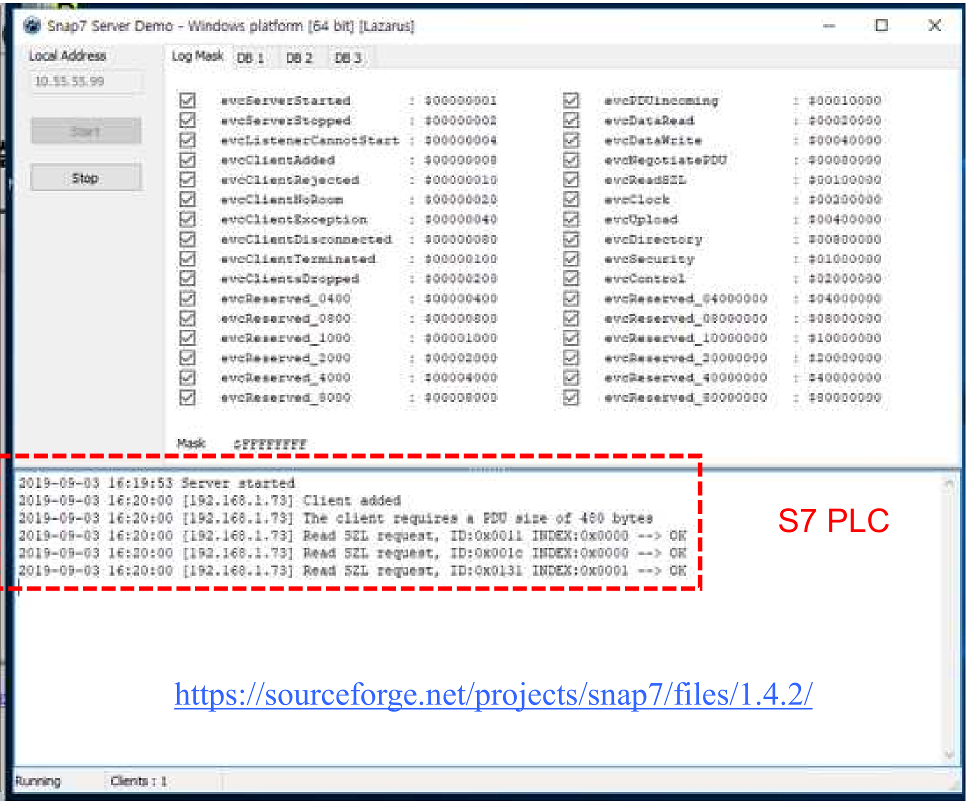
Unit info

Module Type Name	CPU 315-2 PN/DP
Serial number	S C-C2UR28922012
Vendor copyright	Original Siemens Equipment
AS Name	SNAP7-SERVER
Module Name	CPU 315-2 PN/DP

Communication info

Max PDU size (byte)	2048
Max active connections	1024
Max MPI rate (bps)	12000000

S7 Master



Snap7 Server Demo - Windows platform [64 bit] [Lazarus]

Local Address: 10.55.55.99

```
☑ evcServerStarted         : $00000001    ☑ evcPDUincoming           : $00010000
☑ evcServerStopped         : $00000002    ☑ evcDataRead              : $00020000
☑ evcListenerCannotStart   : $00000004    ☑ evcDataWrite             : $00040000
☑ evcClientAdded           : $00000008    ☑ evcNegotiatePDU          : $00080000
☑ evcClientRejected        : $00000010    ☑ evcReadSZL               : $00100000
☑ evcClientNoRoom          : $00000020    ☑ evcClock                 : $00200000
☑ evcClientException       : $00000040    ☑ evcUpload                : $00400000
☑ evcClientDisconnected    : $00000080    ☑ evcDirectory             : $00800000
☑ evcClientTerminated      : $00000100    ☑ evcSecurity              : $01000000
☑ evcClientsDropped        : $00000200    ☑ evcControl               : $02000000
☑ evcReserved_0400         : $00000400    ☑ evcReserved_04000000     : $04000000
☑ evcReserved_0800         : $00000800    ☑ evcReserved_08000000     : $08000000
☑ evcReserved_1000         : $00001000    ☑ evcReserved_10000000     : $10000000
☑ evcReserved_2000         : $00002000    ☑ evcReserved_20000000     : $20000000
☑ evcReserved_4000         : $00004000    ☑ evcReserved_40000000     : $40000000
☑ evcReserved_8000         : $00008000    ☑ evcReserved_80000000     : $80000000

Mask    $FFFFFFFF
```

```
2019-09-03 16:19:53 Server started
2019-09-03 16:20:00 [192.168.1.73] Client added
2019-09-03 16:20:00 [192.168.1.73] The client requires a PDU size of 480 bytes
2019-09-03 16:20:00 [192.168.1.73] Read SZL request, ID:0x0011 INDEX:0x0000 --> OK
2019-09-03 16:20:00 [192.168.1.73] Read SZL request, ID:0x001c INDEX:0x0000 --> OK
2019-09-03 16:20:00 [192.168.1.73] Read SZL request, ID:0x0131 INDEX:0x0001 --> OK
```

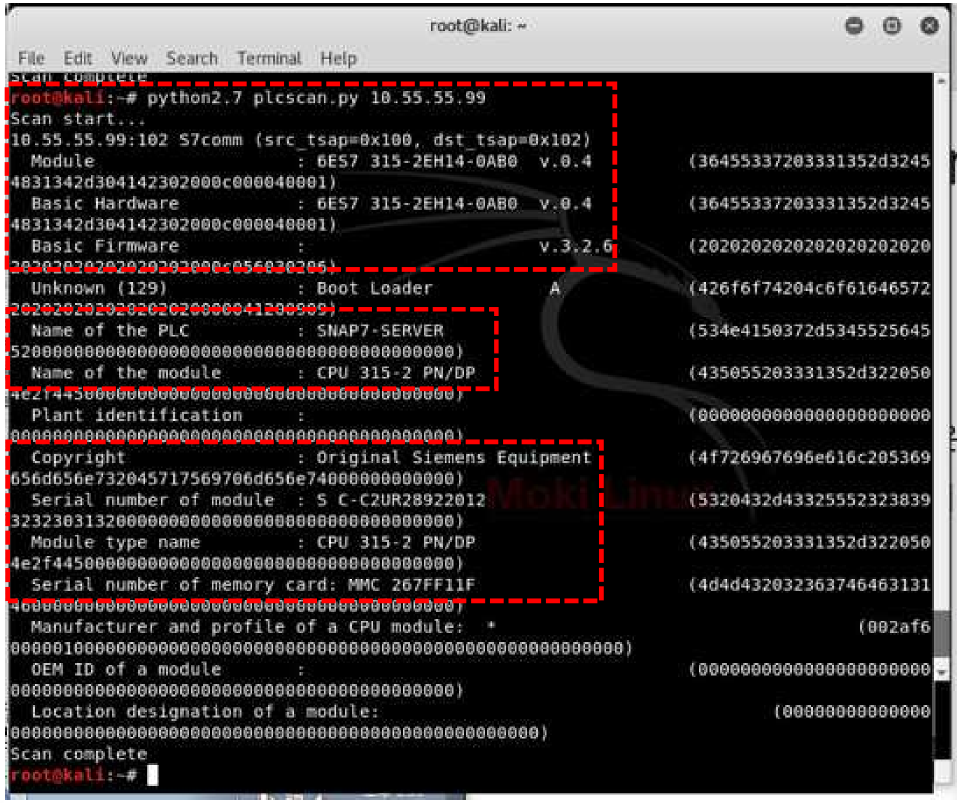
Running   Clients : 1

S7 PLC

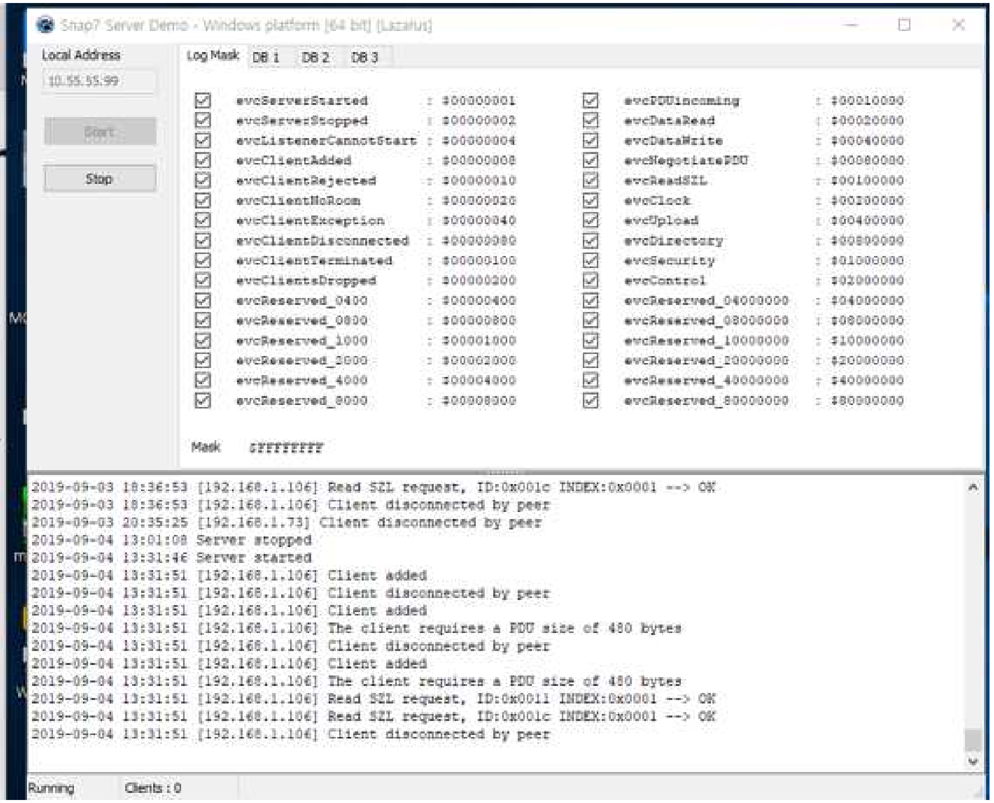
https://sourceforge.net/projects/snap7/files/1.4.2/

데모2. PLC 스캔 차단

해커 : Moki 툴을 이용하여 PLC 정보 스캔



```
Scan complete
root@kali:~# python2.7 plcscan.py 10.55.55.99
Scan start...
10.55.55.99:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                   : 6ES7 315-2EH14-0AB0  v.0.4        (36455337203331352d3245
4831342d304142302000c000040001)
  Basic Hardware           : 6ES7 315-2EH14-0AB0  v.0.4        (36455337203331352d3245
4831342d304142302000c000040001)
  Basic Firmware           :                      v.3.2.6      (20202020202020202020
2020202020202020202000c056030206)
  Unknown (129)            : Boot Loader             A         (426f6f74204c6f61646572
2020202020202020202000000041200909)
  Name of the PLC          : SNAP7-SERVER                      (534e4150372d5345525645
5200000000000000000000000000000000000000)
  Name of the module       : CPU 315-2 PN/DP                   (435055203331352d322050
4e2f445000000000000000000000000000000000)
  Plant identification     :                                   (0000000000000000000000
0000000000000000000000000000000000000000)
  Copyright                : Original Siemens Equipment        (4f726967696e616c205369
656d656e73204571756970606d656e74000000000000)
  Serial number of module  : S C-C2UR28922012                  (5320432d43325552323839
3232303132000000000000000000000000000000)
  Module type name         : CPU 315-2 PN/DP                   (435055203331352d322050
4e2f445000000000000000000000000000000000)
  Serial number of memory card: MMC 267FF11F                   (4d4d4320323637464631311
4600000000000000000000000000000000000000)
  Manufacturer and profile of a CPU module:  *                          (002af6
000001000000000000000000000000000000000000000000000000000000)
  OEM ID of a module       :                                   (0000000000000000000000
0000000000000000000000000000000000000000)
  Location designation of a module:                                     (00000000000000
00000000000000000000000000000000000000000000000000)
Scan complete
root@kali:~# 
```



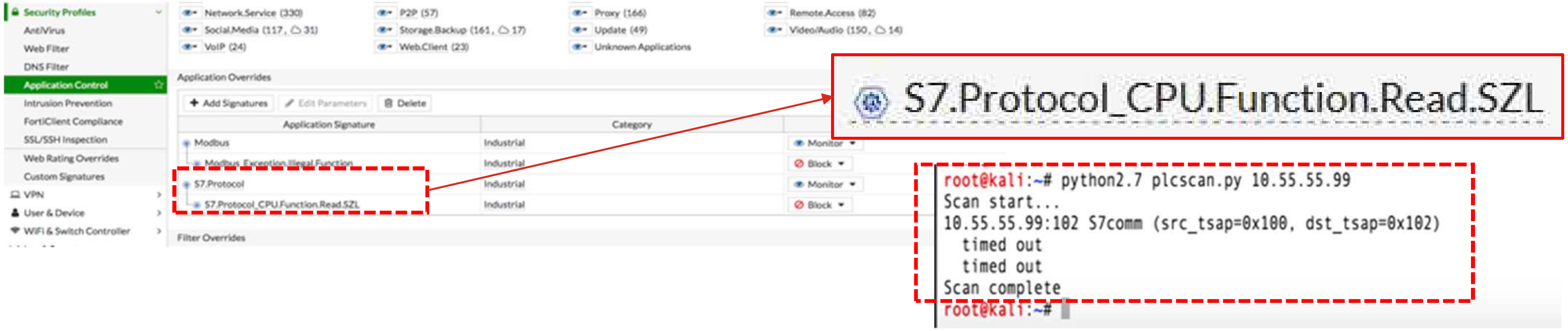
```
☑ evcServerStarted         : $00000001     ☑ evcPDUincoming            : $00010000
☑ evcServerStopped         : $00000002     ☑ evcDataRead               : $00020000
☑ evcListenerCannotStart   : $00000004     ☑ evcDataWrite              : $00040000
☑ evcClientAdded           : $00000008     ☑ evcNegotiatePDU           : $00080000
☑ evcClientRejected        : $00000010     ☑ evcReadSZL                : $00100000
☑ evcClientNoRoom          : $00000020     ☑ evcClock                  : $00200000
☑ evcClientException       : $00000040     ☑ evcUpload                 : $00400000
☑ evcClientDisconnected    : $00000080     ☑ evcDirectory              : $00800000
☑ evcClientTerminated      : $00000100     ☑ evcSecurity               : $01000000
☑ evcClientsDropped        : $00000200     ☑ evcControl                : $02000000
☑ evcReserved_0400         : $00000400     ☑ evcReserved_04000000      : $04000000
☑ evcReserved_0800         : $00000800     ☑ evcReserved_08000000      : $08000000
☑ evcReserved_1000         : $00001000     ☑ evcReserved_10000000      : $10000000
☑ evcReserved_2000         : $00002000     ☑ evcReserved_20000000      : $20000000
☑ evcReserved_4000         : $00004000     ☑ evcReserved_40000000      : $40000000
☑ evcReserved_8000         : $00008000     ☑ evcReserved_80000000      : $80000000

Mask    $FFFFFFFF
```

```
2019-09-03 18:36:53 [192.168.1.106] Read SZL request, ID:0x001c INDEX:0x0001 --> OK
2019-09-03 18:36:53 [192.168.1.106] Client disconnected by peer
2019-09-03 20:35:25 [192.168.1.73] Client disconnected by peer
2019-09-04 13:01:08 Server stopped
2019-09-04 13:31:46 Server started
2019-09-04 13:31:51 [192.168.1.106] Client added
2019-09-04 13:31:51 [192.168.1.106] Client disconnected by peer
2019-09-04 13:31:51 [192.168.1.106] Client added
2019-09-04 13:31:51 [192.168.1.106] The client requires a PDU size of 480 bytes
2019-09-04 13:31:51 [192.168.1.106] Client disconnected by peer
2019-09-04 13:31:51 [192.168.1.106] Client added
2019-09-04 13:31:51 [192.168.1.106] The client requires a PDU size of 480 bytes
2019-09-04 13:31:51 [192.168.1.106] Read SZL request, ID:0x0011 INDEX:0x0001 --> OK
2019-09-04 13:31:51 [192.168.1.106] Read SZL request, ID:0x001c INDEX:0x0001 --> OK
2019-09-04 13:31:51 [192.168.1.106] Client disconnected by peer
```

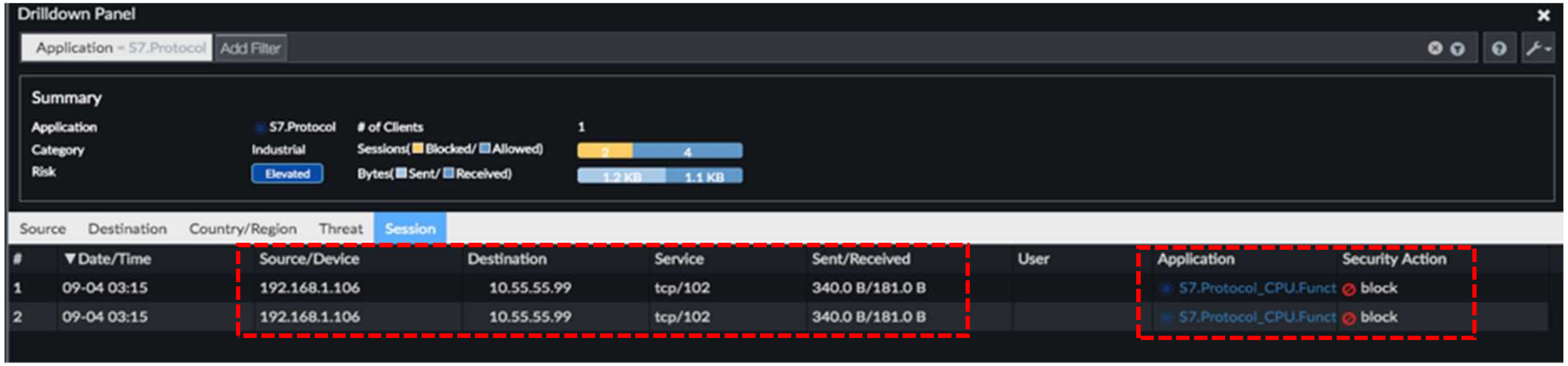
데모2. PLC 스캔 차단

네트워크 보안 방화벽(FortiGate)이용 : PLC 정보 SCAN 차단



Application Signature	Category	
Modbus	Industrial	Monitor
Modbus_Exception.Illegal.Function	Industrial	Block
S7.Protocol	Industrial	Monitor
S7.Protocol_CPU.Function.Read.SZL	Industrial	Block

```
root@kali:~# python2.7 plcscan.py 10.55.55.99
Scan start...
10.55.55.99:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  timed out
  timed out
Scan complete
root@kali:~#
```



Summary

Application	S7.Protocol	# of Clients	1
Category	Industrial	Sessions(Blocked/Allowed)	2 / 4
Risk	Elevated	Bytes(Sent/Received)	1.2 KB / 1.1 KB

#	▼Date/Time	Source/Device	Destination	Service	Sent/Received	User	Application	Security Action
1	09-04 03:15	192.168.1.106	10.55.55.99	tcp/102	340.0 B/181.0 B		S7.Protocol_CPU.Funct	block
2	09-04 03:15	192.168.1.106	10.55.55.99	tcp/102	340.0 B/181.0 B		S7.Protocol_CPU.Funct	block

FORTINET CBC
(CUSTOMER BRIEFING CENTER)

포티넷 CBC (고객 솔루션 체험센터)가
새로운 모습으로 여러분을 찾아갑니다.

포티넷 CBC (고객 솔루션 체험센터)가 국내 최초로 OT 보안 데모 시설을 갖추고
새로이 오픈을 합니다.

클라우드 보안부터 다양한 사이버 보안 솔루션과 보안 패브릭을 직접 시연하고
귀사의 비즈니스와 IT 요구사항에 맞춤화된 1:1 기술 컨설팅을 받으실 수 있습니다.

VISIT TODAY

포티넷 CBC 문은 언제나 열려있습니다.
방문을 원하시는 고객분들은
언제든지 연락 주시기 바랍니다.

FORTINET®