OT 산업보안 세션 :

1) OT 보안 레퍼런스 모델과 국제규정, 아키텍처 구성 소개 (20min)

- 포티넷 문귀 전무 / OT BDM

2) OT 보안 구축사례 및 단계별 구축전략 소개 (20min)

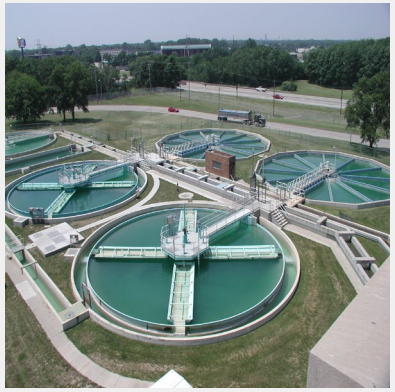
- 포티넷 유종웅 과장 / OT SE

OT 보안 레퍼런스 모델과 국제규정, 아키텍처 구성 소개

문귀 전무 (Neo Moon)
Senior OT Business Development Manager

Operational Technology (OT)

적용 분야




다양한 산업시설
기반시설, 스마트 펙토리 등에서 사용됨




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

OT 산업의 특징

IT / OT 융합

"과거에는 별개로 여겨지던 OT 환경이 이제는 완전히 분리된 존재가 아니게 되었습니다. 즉 OT 환경이 비즈니스, OEM은 물론 여타 제삼자와도 직결되어 있습니다."

Gartner, Reduce Risk to Human Life by Implementing This OT Security Control Framework, 2021년 6월 17일 공개

긴 수명

"프로세스 자동화 시스템에서 자동화 하드웨어는 20~30년을 사용할 수 있는 경우가 많습니다."

Automation's Life Cycle Management of Processing Automation Control Systems, 2021년 4월 공개

보안사고의 불충분한 신고

"설문조사 대상 응답자의 15%가 작년에 보안 사고로 인해 운영 또는 미션 크리티컬 시스템이 중단된 경험이 있었습니다."

Gartner, Emerging Technologies: Critical Insights for Operational Technology Security, 2021년 11월 10일 공개

IT 해킹으로 인한 ICS/OT 사고 증가

"설문조사 참가자는 IT에서 해킹이 발생하여 ICS/OT 제어 네트워크로 위협이 유입되는 것이 제어 시스템 사고와 관련된 가장 큰 위협 벡터라고 언급했습니다."

SANS 2022 Survey: OT/ICS Cybersecurity, 2022년 10월 공개

기존 기술과 최신 기술의 혼합

"OT 기술과 프로세스를 보호하는 데 큰 문제는 기존의 노후한 OT 기술을 최신 IT 시스템과 기술적으로 통합하는 것입니다."

SANS 2022 Survey: OT/ICS Cybersecurity, 2022년 10월 공개

랜섬웨어가 가장 큰 위협

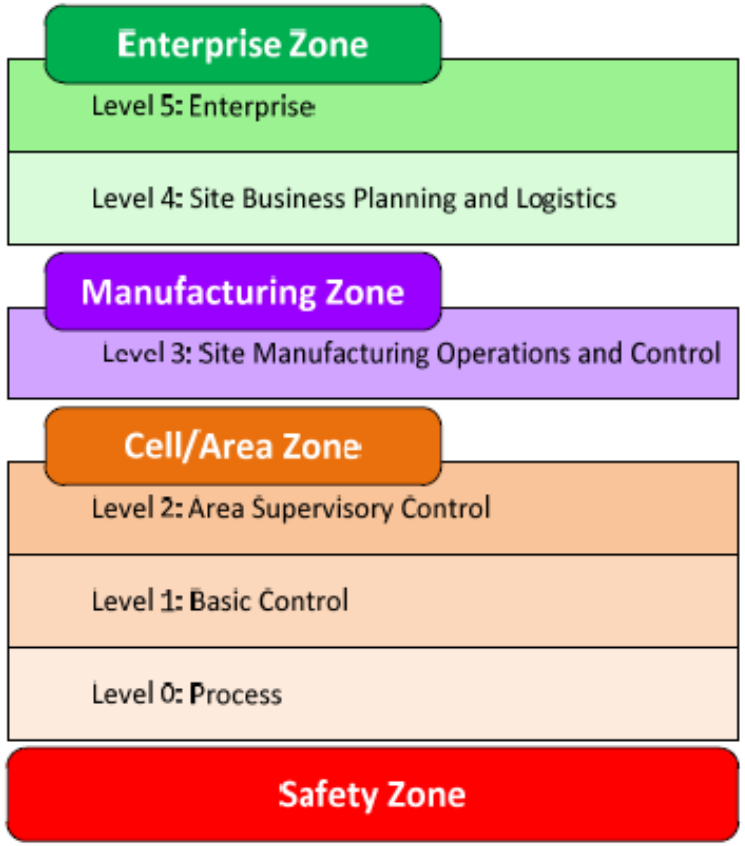
"랜섬웨어, 갈취 또는 금전을 목적으로 한 범죄가 우려되는 위협 벡터 중 1위로 떠올랐습니다."

SANS 2022 Survey: OT/ICS Cybersecurity, 2022년 10월 공개

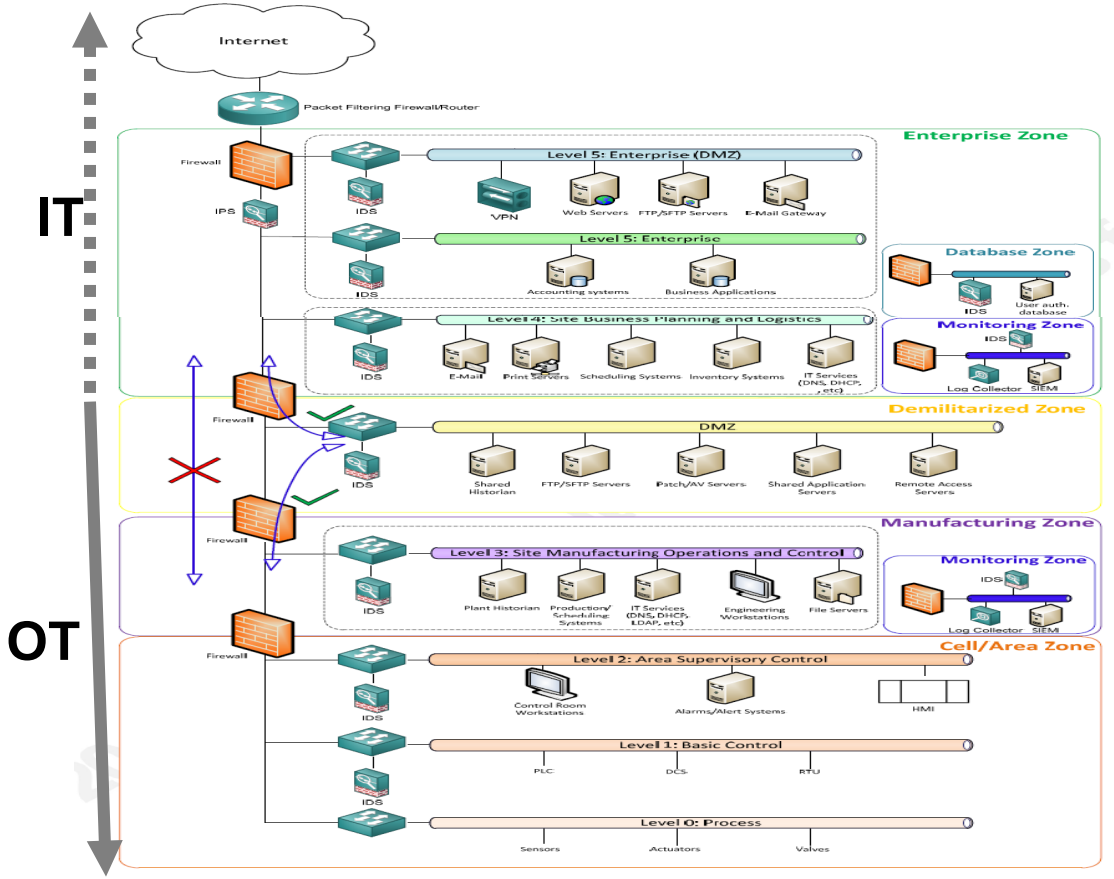
OT 레퍼런스 모델 & 국제 규정

OT 보안 기본 요건

NIST SP 800-82 / IEC-62443 기반 기본 보안요건



Purdue Model for Control Hierarchy logical framework

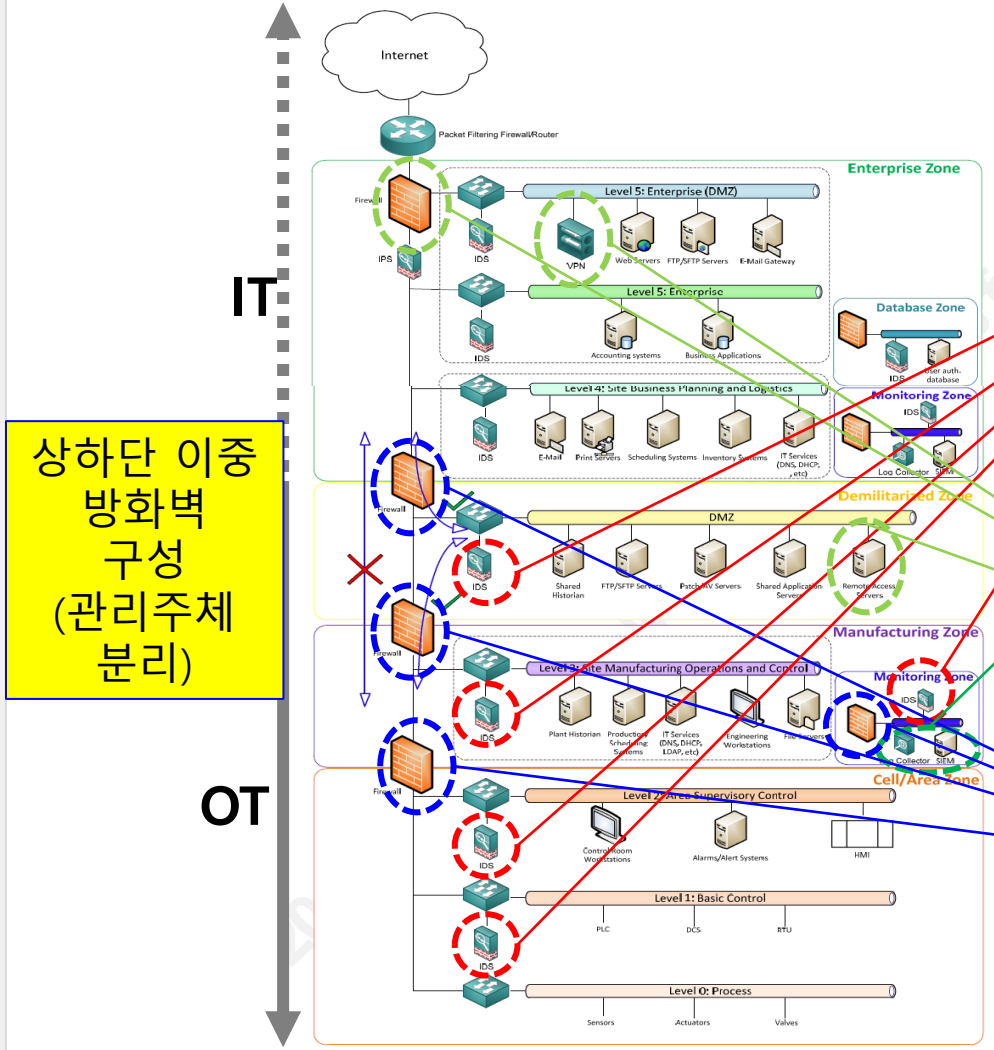


Modified Purdue Model for Control Hierarchy Architecture (NIST SP 800-82)

출처 : SANS Institute - Secure Architecture for Industrial Control Systems
https://www.sans.org/white-papers/36327/

OT 보안 기본 요건

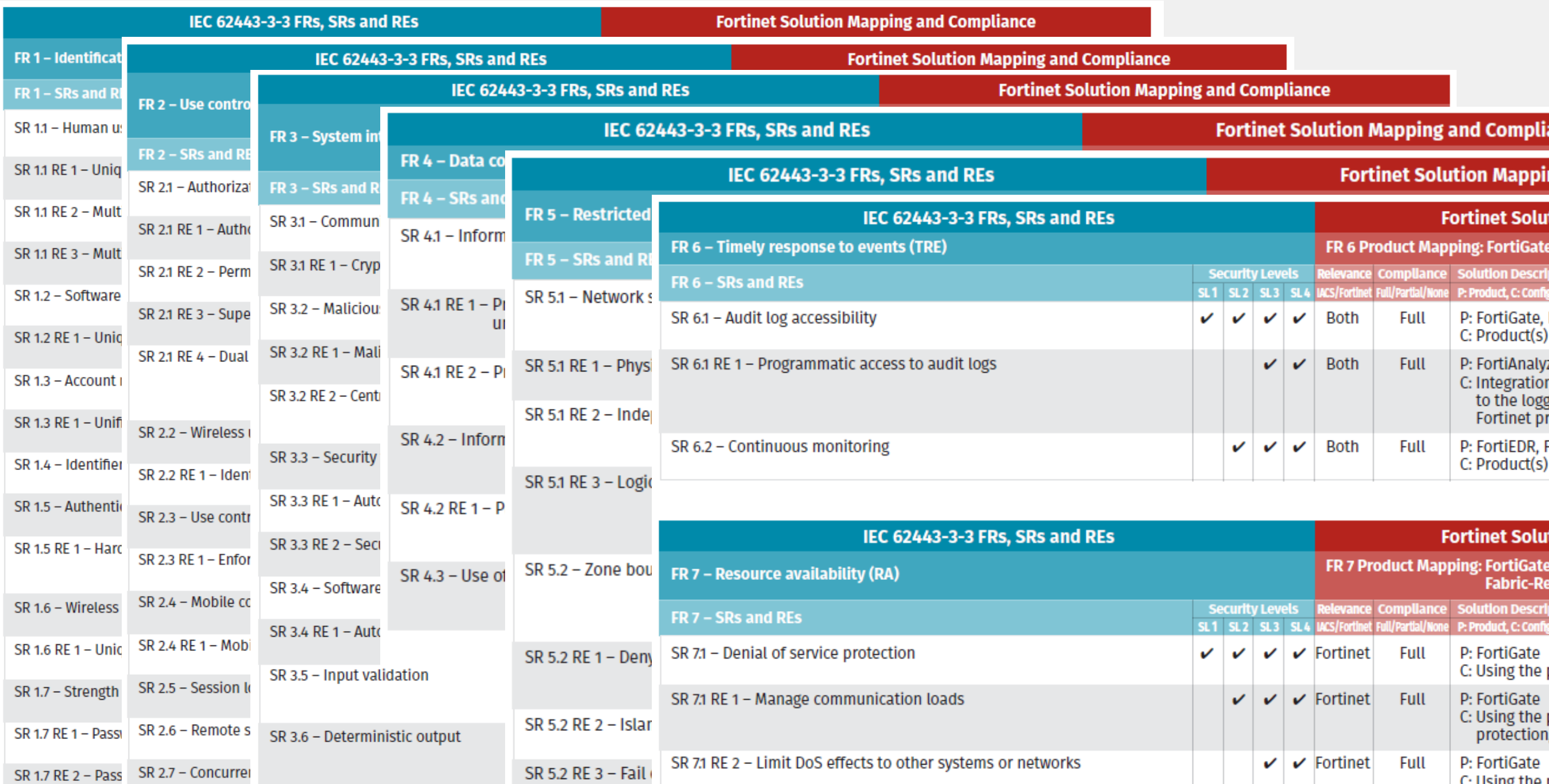
NIST SP 800-82 / IEC-62443 기반 기본 보안요건



OT망 기본 보안요건	포티넷 솔루션
1) 미러링 모드 OT IDS • Network IDS (mirror모드) • AI/ML 랜섬웨어/멀웨어 탐지	**1) 미러링 모드 OT IDS** • FortiGate IDS • IDS Manager (FortiAnalyzer) • FortiAI(NDR) / FortiSandbox
2) 통합로깅 및 로그수집 • SIEM & Log Collector	**2) 통합로깅 및 로그수집** • FortiSIEM & SIEM Collector
3) 외부 Remote Maintenance • NGFW • VPN • Remote Access Server	**3) 외부 Remote Maintenance** • FortiGate NGFW • FortiGate VPN / FortiClient • **FortiPAM(SRA)**
4) 사용자 정책 기반 NGFW • NGFW(산업용 UTM) • (User ID 정책)	**4) 사용자 정책 기반 NGFW** • NGFW(산업용 UTM) • FortiAuthenticator/FortiToken

출처 : SANS Institute - Secure Architecture for Industrial Control Systems
https://www.sans.org/white-papers/36327/

IEC 62443 FR & Mapping Solutions



IEC 62443-3-3 FRs, SRs and REs | Fortinet Solution Mapping and Compliance

FR 1 – Identificat
FR 1 – SRs and R
SR 1.1 – Human u
SR 1.1 RE 1 – Uniq
SR 1.1 RE 2 – Mult
SR 1.1 RE 3 – Mult
SR 1.2 – Software
SR 1.2 RE 1 – Uniq
SR 1.3 – Account
SR 1.3 RE 1 – Unif
SR 1.4 – Identifier
SR 1.5 – Authenti
SR 1.5 RE 1 – Hard
SR 1.6 – Wireless
SR 1.6 RE 1 – Unic
SR 1.7 – Strength
SR 1.7 RE 1 – Passv
SR 1.7 RE 2 – Pass

IEC 62443-3-3 FRs, SRs and REs | Fortinet Solution Mapping and Compliance

FR 2 – Use contro
FR 2 – SRs and RE
SR 2.1 – Authorizat
SR 2.1 RE 1 – Autho
SR 2.1 RE 2 – Perm
SR 2.1 RE 3 – Supe
SR 2.1 RE 4 – Dual
SR 2.2 – Wireless
SR 2.2 RE 1 – Ident
SR 2.3 – Use contr
SR 2.3 RE 1 – Enfor
SR 2.4 – Mobile co
SR 2.4 RE 1 – Mobi
SR 2.5 – Session l
SR 2.6 – Remote s
SR 2.7 – Concurre

IEC 62443-3-3 FRs, SRs and REs | Fortinet Solution Mapping and Compliance

FR 3 – System int
FR 3 – SRs and R
SR 3.1 – Commun
SR 3.1 RE 1 – Cryp
SR 3.2 – Maliciou
SR 3.2 RE 1 – Mali
SR 3.2 RE 2 – Centr
SR 3.3 – Security
SR 3.3 RE 1 – Autc
SR 3.3 RE 2 – Secu
SR 3.4 – Software
SR 3.4 RE 1 – Autc
SR 3.5 – Input validation
SR 3.6 – Deterministic output

IEC 62443-3-3 FRs, SRs and REs | Fortinet Solution Mapping and Compli

FR 4 – Data co
FR 4 – SRs and
SR 4.1 – Inform
SR 4.1 RE 1 – Pr
SR 4.1 RE 2 – Pr
SR 4.2 – Inform
SR 4.2 RE 1 – P
SR 4.3 – Use of

IEC 62443-3-3 FRs, SRs and REs | Fortinet Solution Mappi

FR 5 – Restricted
FR 5 – SRs and R
SR 5.1 – Network s
SR 5.1 RE 1 – Physi
SR 5.1 RE 2 – Indep
SR 5.1 RE 3 – Logic
SR 5.2 – Zone bou
SR 5.2 RE 1 – Deny
SR 5.2 RE 2 – Islar
SR 5.2 RE 3 – Fail

IEC 62443-3-3 FRs, SRs and REs | Fortinet Solu

FR 6 – Timely response to events (TRE) | FR 6 Product Mapping: FortiGate

FR 6 – SRs and REs	Security Levels SL 1	SL 2	SL 3	SL 4	Relevance IACS/Fortinet	Compliance Full/Partial/None	Solution Descri P: Product, C: Config
SR 6.1 – Audit log accessibility	✔	✔	✔	✔	Both	Full	P: FortiGate, C: Product(s)
SR 6.1 RE 1 – Programmatic access to audit logs			✔	✔	Both	Full	P: FortiAnaly C: Integration to the logg Fortinet pr
SR 6.2 – Continuous monitoring		✔	✔	✔	Both	Full	P: FortiEDR, C: Product(s)

IEC 62443-3-3 FRs, SRs and REs | Fortinet Solu

FR 7 – Resource availability (RA) | FR 7 Product Mapping: FortiGate Fabric-Re

FR 7 – SRs and REs	Security Levels SL 1	SL 2	SL 3	SL 4	Relevance IACS/Fortinet	Compliance Full/Partial/None	Solution Descri P: Product, C: Config
SR 7.1 – Denial of service protection	✔	✔	✔	✔	Fortinet	Full	P: FortiGate C: Using the
SR 7.1 RE 1 – Manage communication loads		✔	✔	✔	Fortinet	Full	P: FortiGate C: Using the protection
SR 7.1 RE 2 – Limit DoS effects to other systems or networks			✔	✔	Fortinet	Full	P: FortiGate

NIST CSF (Cyber Security Framework)

중요 인프라 시스템의 사이버보안 부문 강화를 위한 프레임워크이며, 사이버사고의 예방, 탐지 및 대응할 수 있는 능력을 평가하고 향상시킬 수 있게 한다.

※ NIST : 미국표준기술연구소

NIST CSF의 5가지 기능

4.1 식별 (Identity)

- 4.1.1 시스템 및 네트워크 목록(Inventory)

4.2 보호 (Protect)

- 4.2.1 보안 구역(Security Zones)
- 4.2.2 네트워크 보호 안전장치(Safeguard)
- 4.2.3 안티바이러스, 안티멀웨어, 안티스팸 및 악성코드로부터 보호
- 4.2.4 접근 통제(Access control)
- 4.2.5 무선 통신(Wireless Communication)
- 4.2.6 원격 접근 통제 및 신뢰할 수 없는 네트워크 에서 통신
- 4.2.7 모바일 및 휴대용 장치의 사용

4.3 탐지 (Detect)

- 4.3.1 네트워크 운영 모니터링
- 4.3.2 CBS 및 네트워크의 진단 기능

4.4 대응 (Respond)

- 4.4.1 사고 대응 계획 (Incident response plan)
- 4.4.2 로컬, 독립 또는 수동 운전 지원
- 4.4.3 네트워크 격리 (Network isolation)
- 4.4.4 최소 위험 조건으로의 복귀

4.5 복구 (Recover)

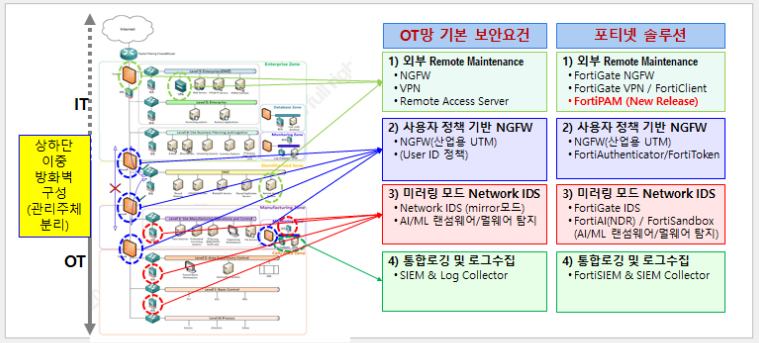
- 4.5.1 복구 계획
- 4.5.2 백업 및 복구 기능 (Backup and restore capability)
- 4.5.3 제어된 종료, 리셋, 롤백 및 재시작

OT 아키텍처 모델 정립 및 벤더사 최적화 필요

❑ 국제 규정 준수 = 10~20개의 OT 보안 솔루션 필요

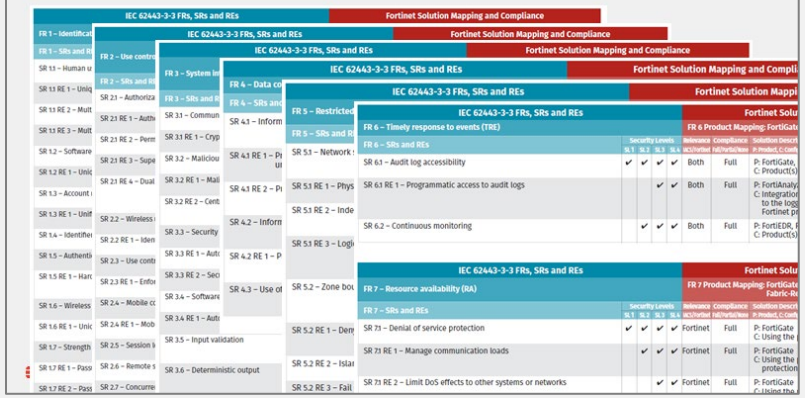
OT 보안 기본 요건 (기존망 / 신규망 공통)

❑ Enhanced Purdue Model / NIST SP 800-82 / IEC-62443 기반



OT망 기본 보안요건	포티넷 솔루션
1) 외부 Remote Maintenance • NGFW • VPN • Remote Access Server	1) 외부 Remote Maintenance • FortiGate NGFW • FortiGate VPN / FortiClient • FortiPAM (New Release)
2) 사용자 정책 기반 NGFW • NGFW(산업용 UTM) • (User ID 정책)	2) 사용자 정책 기반 NGFW • NGFW(산업용 UTM) • FortiAuthenticator/FortiToken
3) 미러링 모드 Network IDS • Network IDS (mirror모드) • AI/ML 탠섬웨어/멀웨어 탐지	3) 미러링 모드 Network IDS • FortiGate IDS • FortiAI(NDR) / FortiSandbox (AI/ML 탠섬웨어/멀웨어 탐지)
4) 통합로깅 및 로그수집 • SIEM & Log Collector	4) 통합로깅 및 로그수집 • FortiSIEM & SIEM Collector

IEC 62443 FR & Mapping Solutions



NIST CSF (Cyber Security Framework)

중요 인프라 시스템의 사이버보안 부문 강화를 위한 프레임워크이며, 사이버사고의 예방, 탐지 및 대응할 수 있는 능력을 평가하고 향상시킬 수 있게 한다.

※NIST : 미국표준기술연구소

NIST CSF의 5가지 기능

- 4.1 식별 (Identity)
  - 4.1.1 시스템 및 네트워크 목록(Inventory)
- 4.2 보호 (Protect)
  - 4.2.1 보안 구역(Security Zones)
  - 4.2.2 네트워크 보호 안전장치(Safeguard)
  - 4.2.3 안티바이러스, 안티멀웨어, 안티스팸 및 악성코드로부터 보호
  - 4.2.4 접근 통제(Access control)
  - 4.2.5 무선 통신(Wireless Communication)
  - 4.2.6 원격 접근 통제 및 신뢰할 수 있는 네트워크 에서 통신
  - 4.2.7 모바일 및 휴대용 장치의 사용
- 4.3 탐지 (Detect)
  - 4.3.1 네트워크 운영 모니터링
  - 4.3.2 CBS 및 네트워크의 진단 기능
- 4.4 대응 (Respond)
  - 4.4.1 사고 대응 계획 (Incident response plan)
  - 4.4.2 프린, 통합 또는 수동 운전 지원
  - 4.4.3 네트워크 격리 (Network isolation)
  - 4.4.4 최소 위험 조건으로의 복귀
- 4.5 복구 (Recover)
  - 4.5.1 복구 계획
  - 4.5.2 백업 및 복구 기능 (Backup and restore capability)
  - 4.5.3 제어된 종료, 리셋, 롤백 및 재시작

NERC CIP : North American Electric Reliability Corporation, Critical Infrastructure Protection

북미 지역 전기망 시설을 소유하거나 관리하는 단체에 적용되는 의무적인 보안기준

Standard - Version	Standard Name
CIP-002-5.1	BES Cyber System Categorization
CIP-003-8	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-6	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-3	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection
CIP-012-1	Communications Between Control Centers
CIP-013-1	Supply Chain Risk Management
CIP-014-2	Physical Security

* As of July 2020

※BES : Bulk Electric System

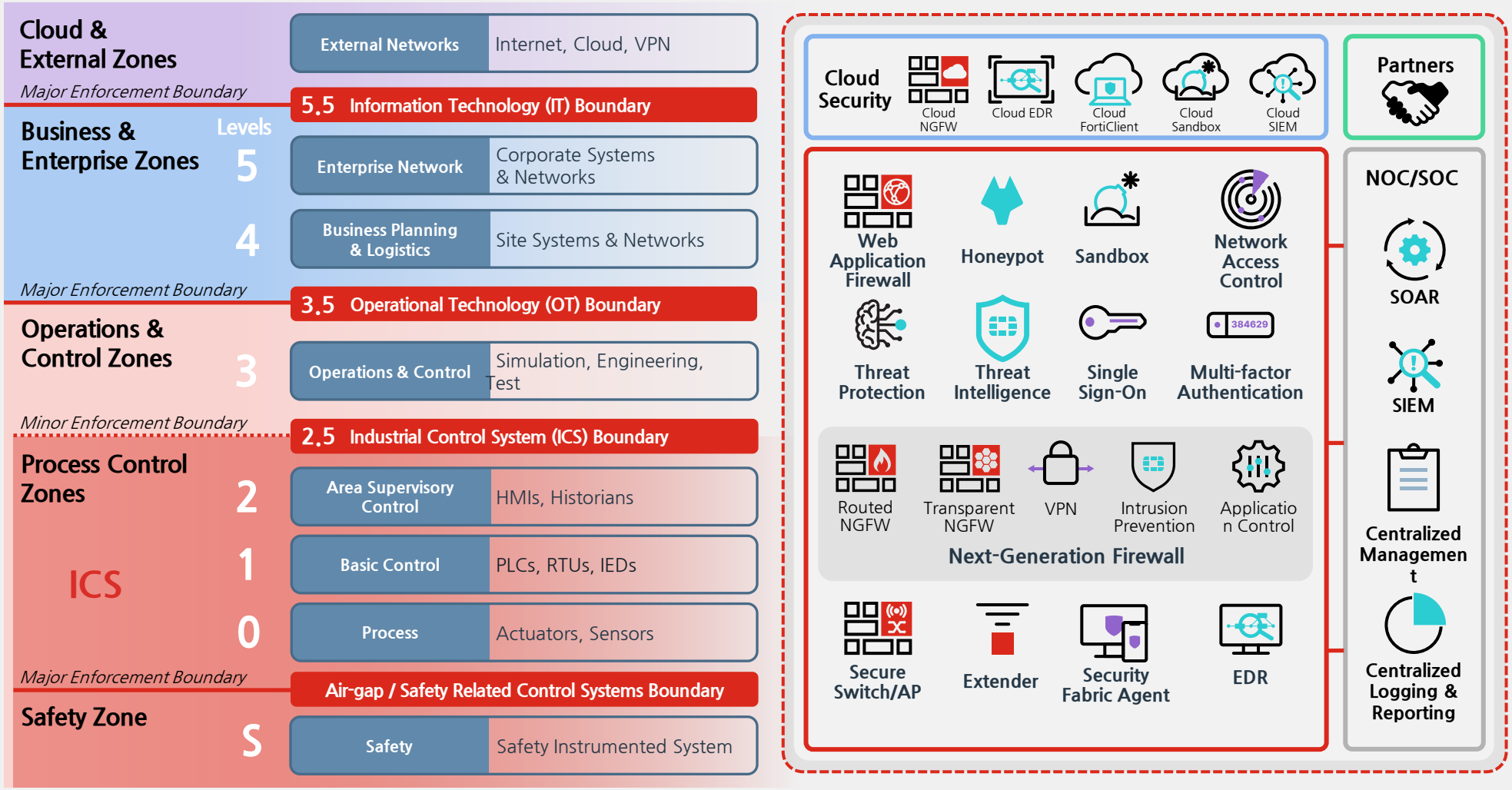
- 10~20개의 OT 보안 솔루션 필요
- Best of Breed 도입 : 10개 이상 벤더사에서 각각의 솔루션 도입은 비현실적 (비용↑, 인력부하↑, 관리↑)
- OT 아키텍처 모델 정립 및 벤더사 최적화 필요

강력한 OT 사이버 보안 플랫폼

포티넷 시큐리티 패브릭

Boundary: *Demilitarized Zone (DMZ), Security Conduit*
Zones: *Security Zones*
IPS: *Intrusion Prevention System*
SIEM: *Security Information and Event Management*
SOAR: *Security Orchestration, Automation and Response*

- NOC/SOC 통합관제
- 제로 트러스트
- 구역 및 통신경로 보안
- 위협 및 취약성 관리
- 엔드포인트 보안
- 전문 산업 솔루션 (Rugged 제품군)

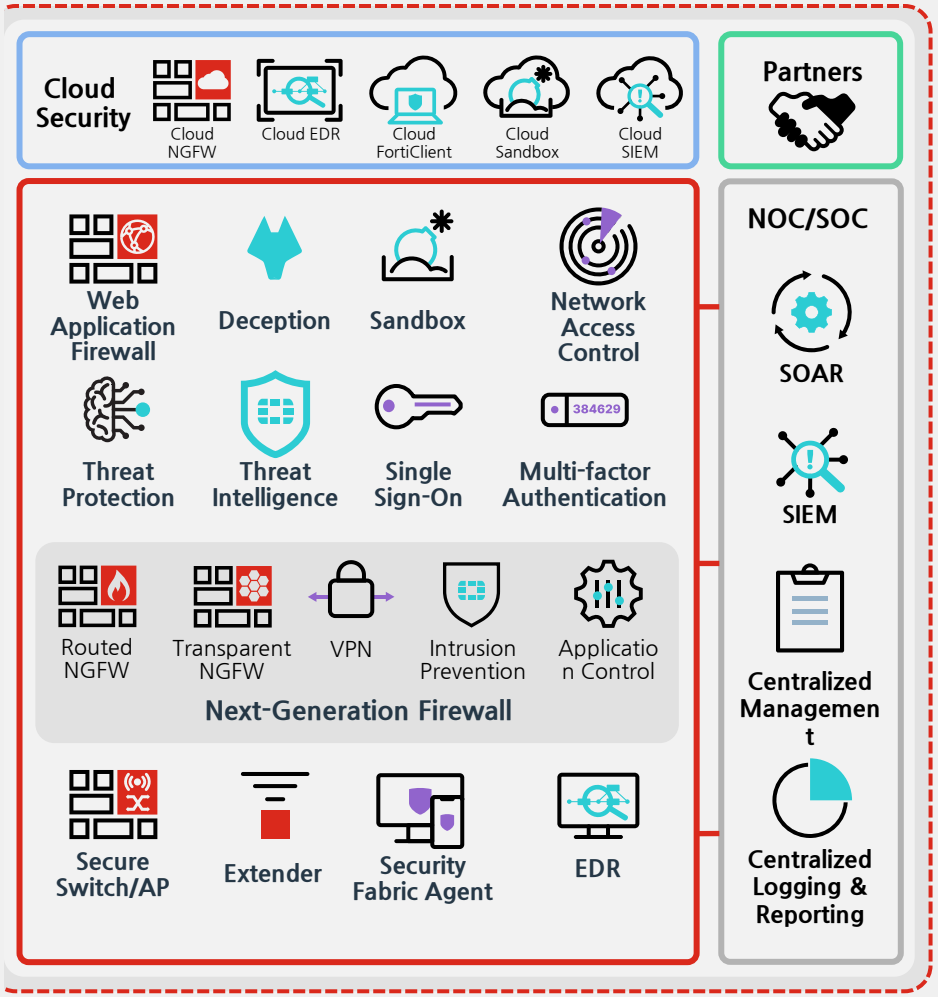


강력한 OT 사이버 보안 플랫폼

포티넷 시큐리티 패브릭

Boundary: *Demilitarized Zone (DMZ), Security Conduit*
Zones: *Security Zones*
IPS: *Intrusion Prevention System*
SIEM: *Security Information and Event Management*
SOAR: *Security Orchestration, Automation and Response*

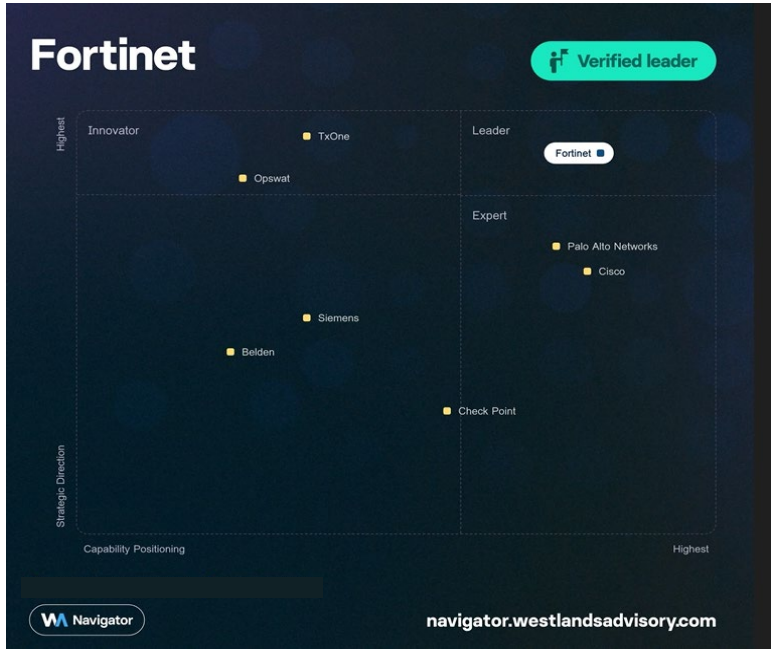
- NOC/SOC 통합관제
- 제로 트러스트
- 구역 및 도관 보안
- 위협 및 취약성 관리
- 엔드포인트 보안
- 전문 산업 솔루션 (Rugged 제품군)



포티넷 IT/OT Platforms Leader

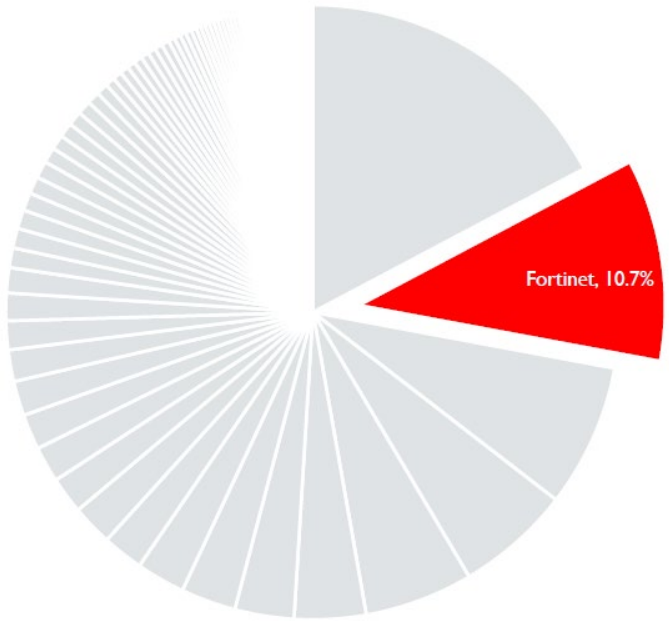
IT/OT 네트워크 보안 플랫폼 내비게이터 2023의 유일한 리더 선정

IT/OT Network Security Platform Navigator 2023



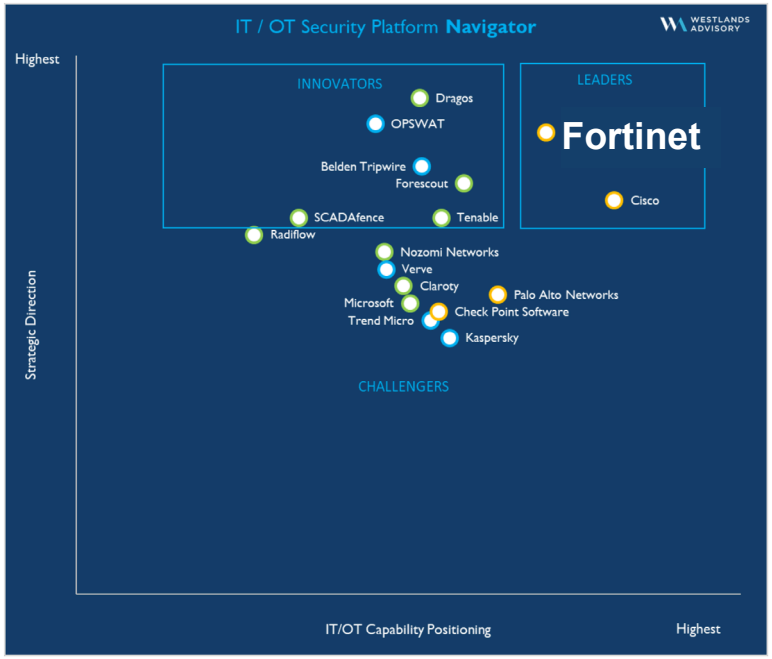
WESTLANDS ADVISORY

Market Share Profile
IT/OT Convergence TAM, 2022



WESTLANDS ADVISORY

IT/OT Security Platform Navigator 2022



Primarily NGFW & Zero Trust
Mixed Capabilities
Primarily Vulnerability Management & Threat Detection

WESTLANDS ADVISORY

Fortinet Championship PGA Tour

Silverado Country Club, Napa, California

FORTINET CHAMPIONSHIP

CHECK BACK SOON FOR NEXT YEAR'S TOURNAMENT DATE.

SILVERADO RESORT & SPA, NAPA VALLEY

Congratulations to 2023 winner **Sahith Theegala.**

Thanks to everyone year!

포티넷 챔피언십

순위	선수	홀	금일	타수
1	Sahith Theegala	F	-4	-21
2	김성현	F	-4	-19
3	Cam Davis	F	-2	-17

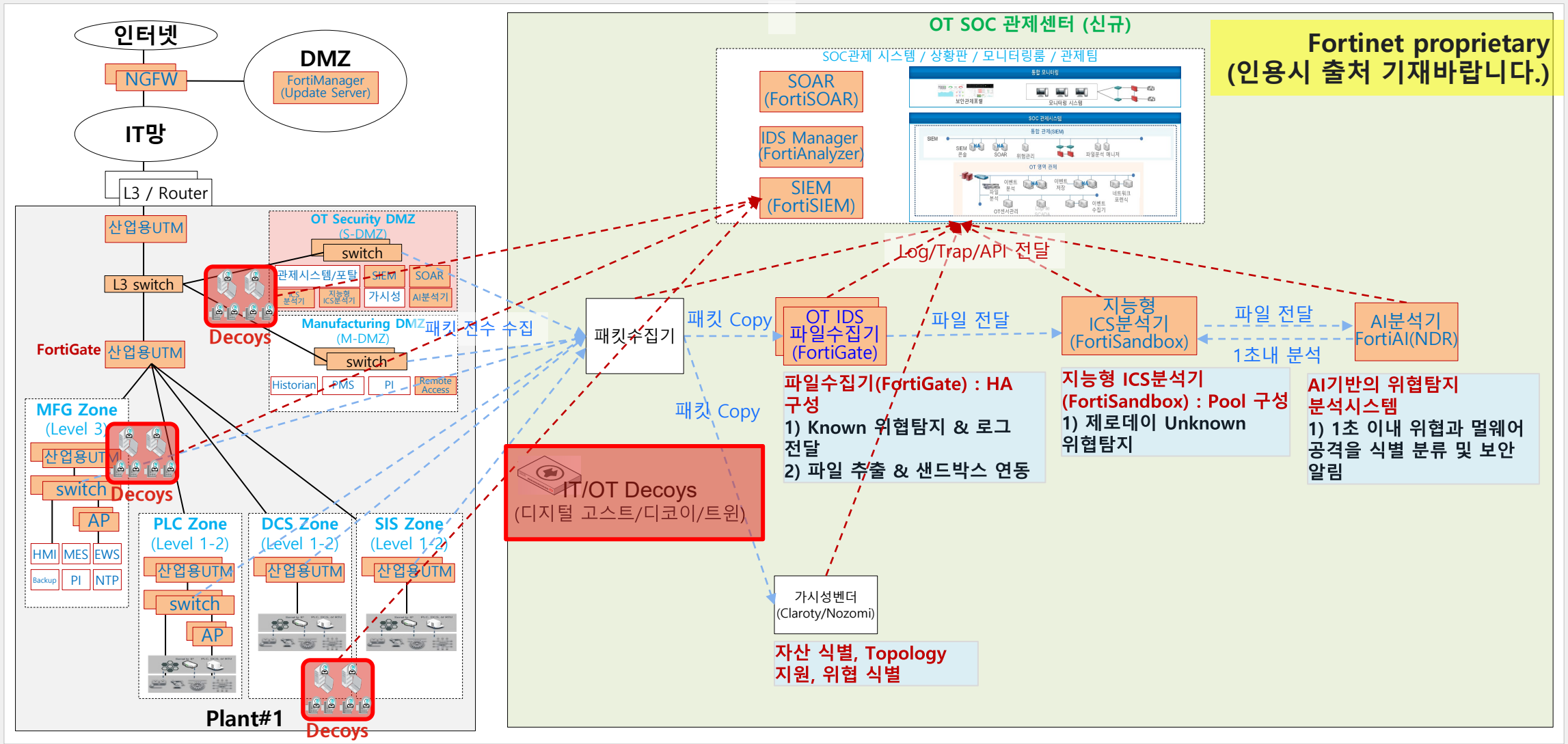
OT보안 아키텍처 모델

OT SOC 통합관제 설계

OT 인프라 아키텍처 설계 (신규망)

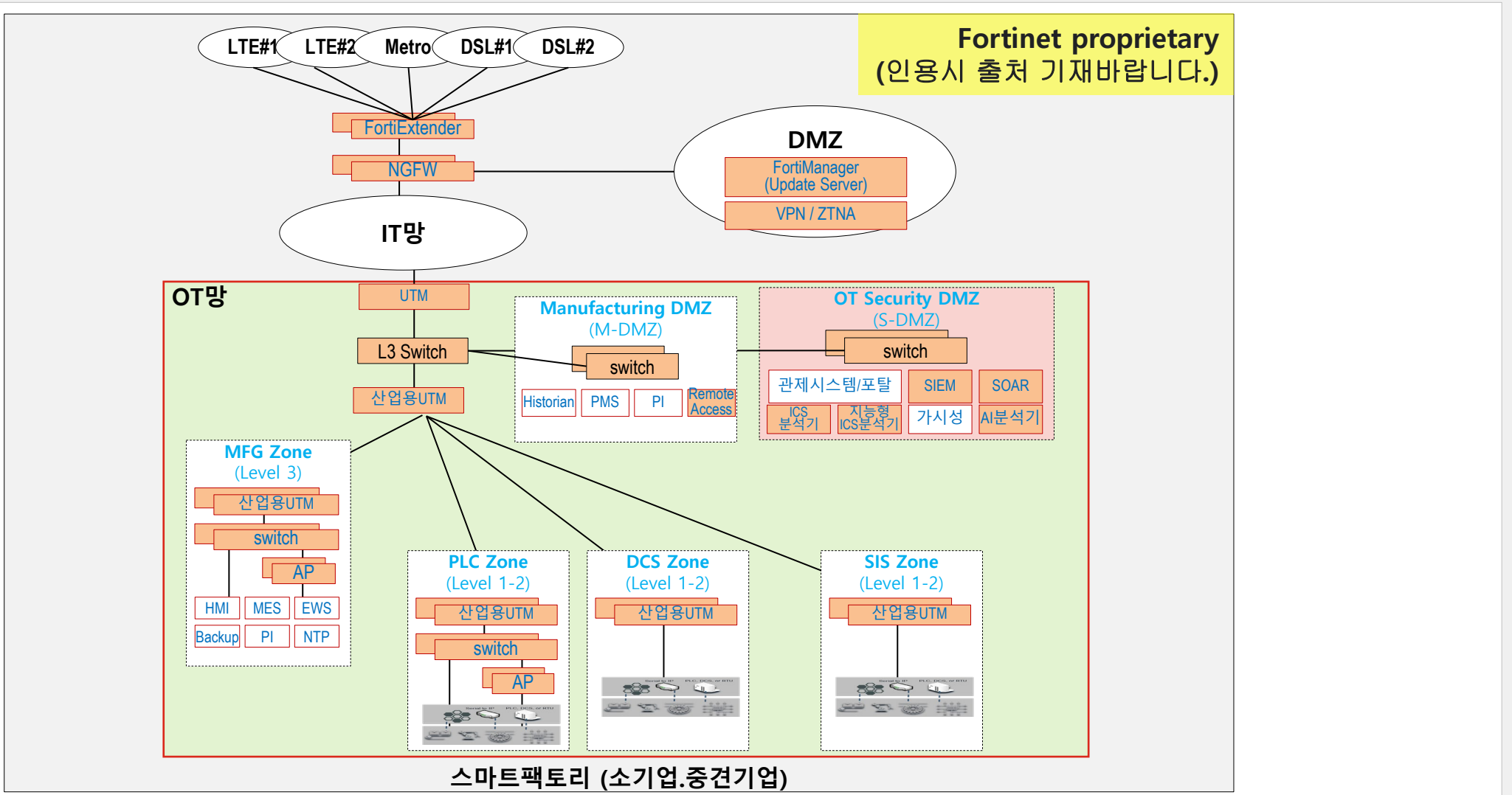
OT SOC 통합관제 설계 (신규망 / 기존망 공통)

❑ 패시브 모니터링 방식의 OT SOC 통합관제 설계 – 구성 개념도



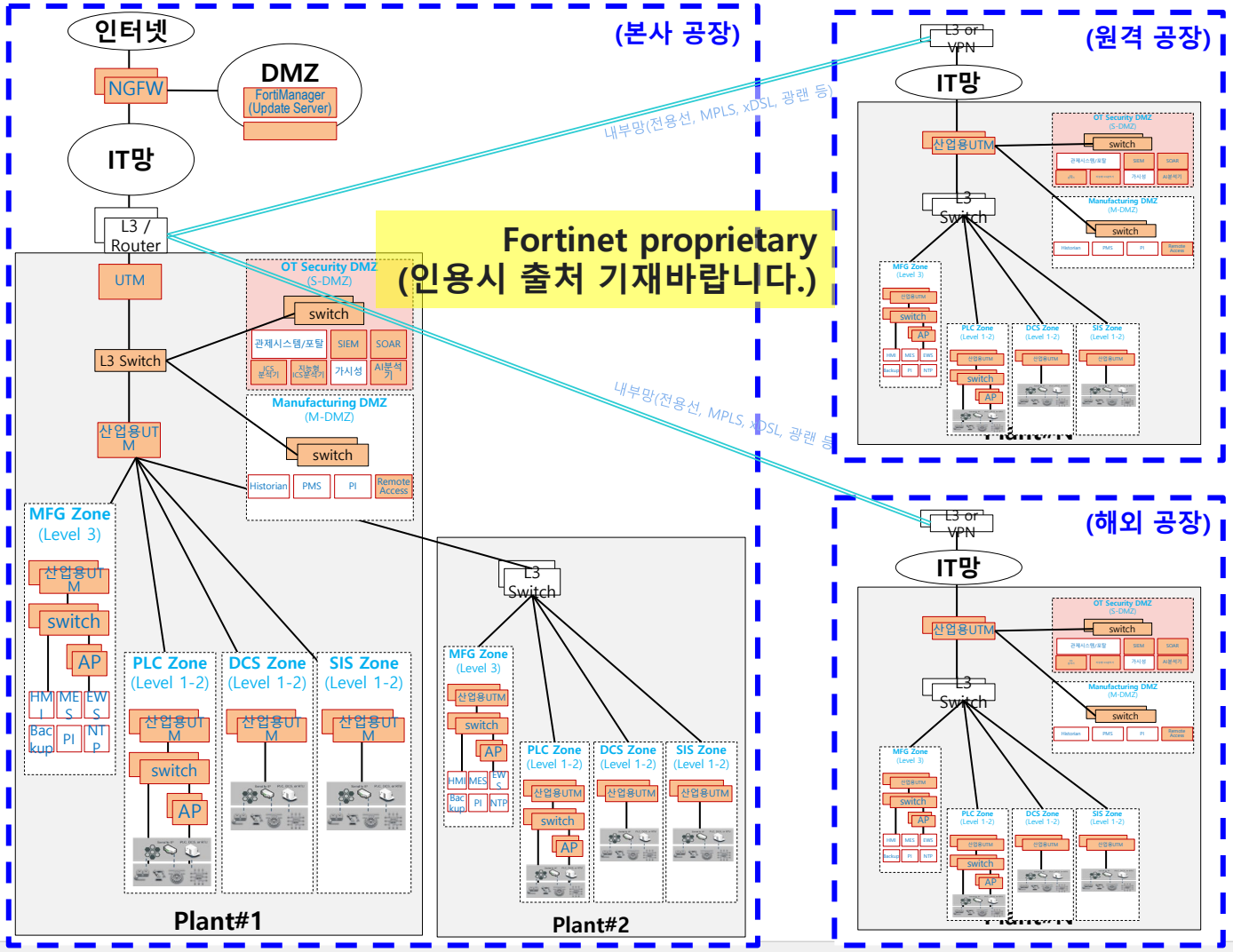
OT 인프라 아키텍처 설계 (신규망)

❑ 소기업.중견기업 스마트팩토리 아키텍처 설계 – 구성 개념도



OT 인프라 아키텍처 설계 (신규망)

❑ 중견기업.대기업 스마트팩토리 아키텍처 설계 – 솔루션 내역



멀티클라우드 보안 솔루션 :

- Forti VMs : All appliance models.
- FortiCASB : SaaS applications 관리
- FortiCWP : 멀티클라우드 보안 관리

SOC/NOC 솔루션 :

- FortiSIEM : SOC 통합관제, 로깅/리포팅
- FortiSOAR : 오케스트레이션 자동화
- FortiAuthenticator / FortiToken : 통합인증 / 2FA (2차 인증)
- FortiDeceptor : OT Honeypot 솔루션
- FortiManager : FortiGate 정책관리
- FortiAnalyzer : 통합 로깅/리포팅(포티넷 전용)

네트워크 보안 솔루션 : (소기업.중견기업과 동일)

- FortiExtender, FortiGate, FortiSwitch, FortiAP , FortiManager, FortiAnalyzer

단말 보안 솔루션 : (소기업.중견기업과 동일)

- FortiEDR, FortiClient, FortiESM, FortiAuthenticator/FortiToken, FortiNAC

권고 사항

❑ 랜섬웨어와 내부자 위협에 대한 방어 (공격 동인은 Money=Bitcoin)

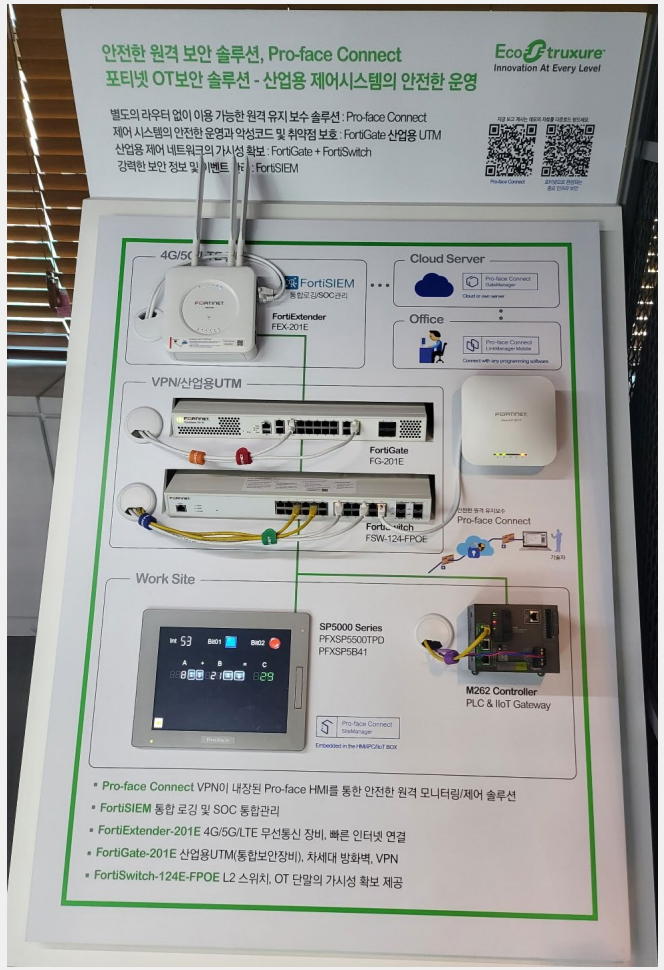
- EDR : OT 단말(HMI, EWS, SCADA서버, Historians 등) 보호
- ATP : OT 경계망 및 내부 주요 구간에서 랜섬웨어 등 능동적 악성코드 탐지/방어 체계 구축
- Deception : 내부자 위협에 대한 선제적 탐지 및 모니터링을 위한 OT SOC 구축

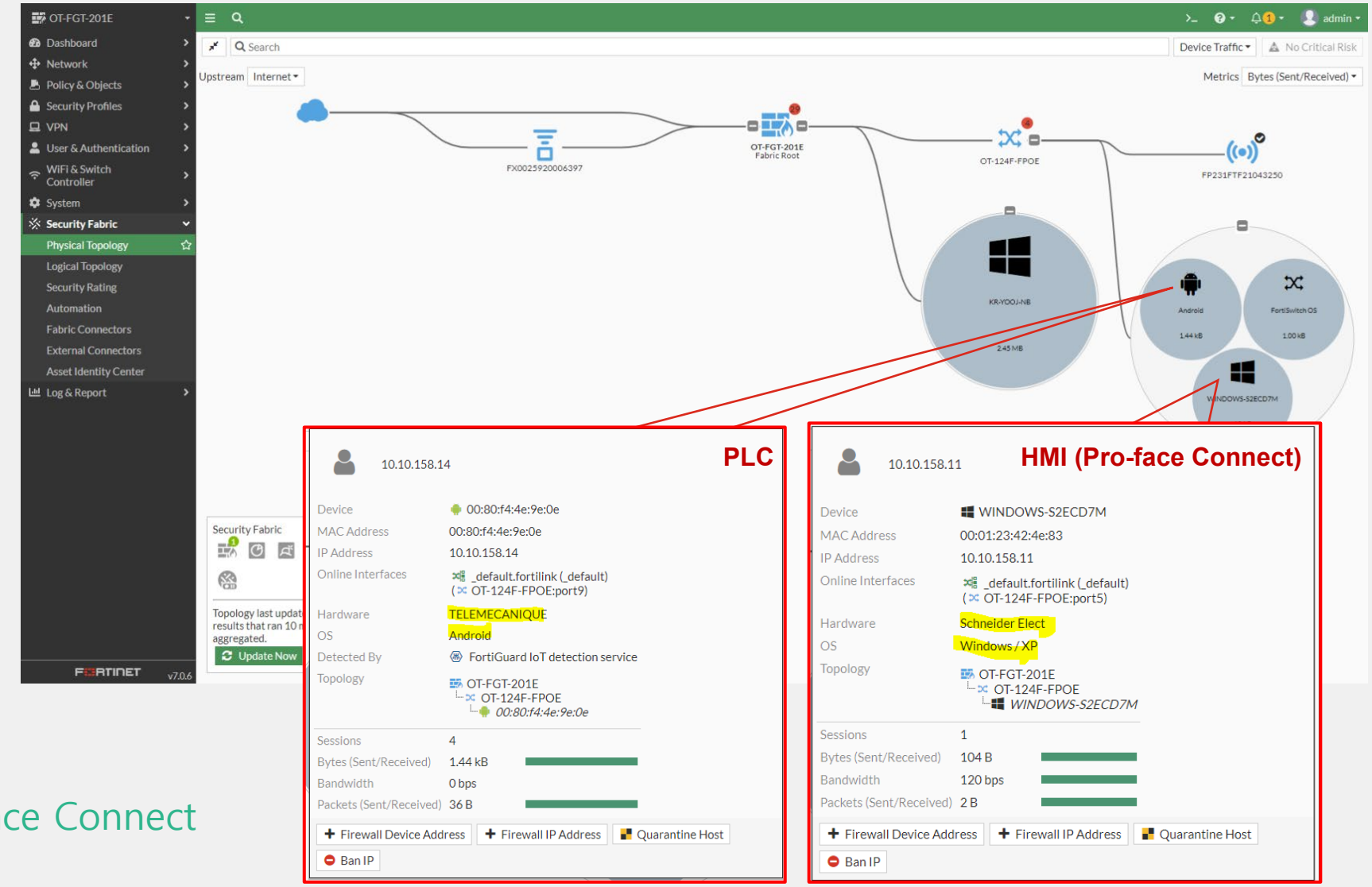
❑ OT 사이버 보안 플랫폼 정립

- OT 영역 필수 솔루션 정의 (국제표준, 구축사례, 타 제소사 표준제품 등 참고)
- OT영역 표준 솔루션을 2~4개 벤더사로 최적화 (해외 지원, Supply Chain 최적화 고려)
- 고객사 환경에 최적화된 OT 사이버 보안 플랫폼 정립 권고

포티넷 데모 부스 & CBC 초청

포티넷 데모 부스 - Secure SD-Branch





Secure Remote Access Pro-face Connect

FORTINET

Customer Briefing Center

포티넷 CBC 고객 솔루션 체험 센터

전세계 TOP3 사이버 보안 벤더인 포티넷에서 국내 고객 분들을 위해 마련한 솔루션 체험 센터로 방문하시는 고객분들의 요구사항에 따라 맞춤화된 컨설팅을 제공합니다.

보안 중심 네트워크 | 다이나믹 클라우드 보안 | AI 기반 보안 관제 | 제로 트러스트 엑세스

☑ 포티넷CBC에 방문해야 하는 이유?

- 디지털 트랜스포메이션에 필요한 IT보안 요구 사항을 알아보고 최적의 해결 방안을 제시합니다.
- 고객의 비즈니스 목표에 맞추어 당사 기술 전문가와 1:1 맞춤 컨설팅이 가능합니다.
- 축적된 수많은 레퍼런스로 고객의 다양한 상황에 맞는 완벽한 보안 솔루션을 제공합니다.
- 보안 솔루션을 시각적으로 확인할 수 있는 라이브 데모를 직접 체험할 수 있습니다.

포티넷 CBC는 언제나 여러분께 열려있습니다. 지금 방문 신청해주세요!

www.fortinet-vcbc.com www.fortinet.com/kr/corporate/cbc

CBC 방문 신청하기

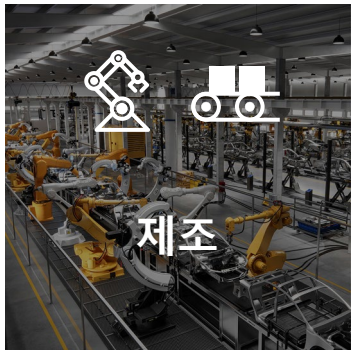
Virtual CBC 바로가기

OT 보안 구축사례 및 단계별 구축전략 소개

유종웅 과장 / Systems Engineer(OT)

광범위한 산업 인프라 시설

운영기술 영역



OT보안 고객 성공 사례

BMW
Mercedes-Benz
Volkswagen
AIR LIQUIDE
EDF
ENGIE
enel
SANDVIK
بلدية مدينة أبوظبي
ABU DHABI CITY MUNICIPALITY
SHIPSERV
Find. Connect. Trade.
Petrol Ofisi
WM
WASTE MANAGEMENT
MASERGY
SCHILLER
The Art of Saving Lives
telenor
SIEMENS
Ingenuity for life
BT
NEXUS OCEAN
orange Business Services
NTT WEST
IndiGo
Falu Energi & Vatten
SULLAIR
ARGENTINA
UNITED ARAB EMIRATES
MINISTRY OF HEALTH & PREVENTION
Telefónica
BALEARIA
مجموعة المطار الدولي
Airport International Group
NORDLAKS

OT 보안 구축 사례

- 52,000곳 이상의 고객사
- OT 산업 보안 솔루션
- 글로벌, 로컬, 원격
- 업종
  - 제조
  - 에너지
  - 오일 및 가스
  - 채굴
  - 상하수
  - 교통
  - 헬스케어
  - 스마트 건물

North American Pulp and Paper Manufacturer

Protecting OT in wake of Ransomware Outbreak

COMPELLING EVENT
- Ransomware Outbreak in early 2020 resulted in operational downtime
- Significant remediation costs

CUSTOMER NEEDS
- Endpoint / device protection
- Network segmentation to separate OT from IT environment.
- Network Access Control
- Mail Protection
- Ease of Configuration and Deployment
- OT and IT Security Domain Expertise

FORTINET SOLUTION
- FortiEDR
- FortiGate
- FortiNAC
- FortiMail
- Advanced Threat Protection
- Intrusion Protection System

 33

Global Automotive Manufacturer

18 Production Sites Globally, 180 Production Halls

COMPELLING EVENT
- Modernization of Security
- Executive concerns about security effectiveness
- OT Domain Expertise brought into Information Technology Security
- Concerns of Operational Impact

CUSTOMER NEEDS
- Visibility, Auditability
- Logical business need Segmentation, Physical Network Segmentation
- Complete network controls, Wired and Wireless
- Ease of Configuration and Deployment
- OT and IT Security Domain Expertise

FORTINET SOLUTION
- Pre-sales consulting to alleviate customer concerns
- Consulting toward people, process, cultural shifts
- Assessment of existing environment
- Solution Consulting to establish future vision
- Executive Engagement
- Customer engagement ensured systemic solution acceptance

 26

ECHOENERGIA WIND

1.2 GW, 484 Wind Turbines in 12 Brazilian wind farms

COMPELLING EVENT
- Rapid expansion within the first couple years of operation
- High industry standards to meet
- Ensure safe use of innovative energy solutions

CUSTOMER NEEDS
- Fulfill industry compliance requirements
- Intelligent and fast management
- Inclusion of IT infrastructure to provide high availability communication
- Avoid redundancies
- Increased security

FORTINET SOLUTION
- Fortinet's solutions help meet industry requirements and overcome geographical challenges
  - FortiSwitch
  - FortiGate
  - FortiAP
  - FortiAuthenticator
  - FortiToken

https://www.fortinet.com/customers/echoenergia

 5

RH Marine

Dutch Maritime Systems Integrator Fortifies Operations With New Integrated Security Architecture

COMPELLING EVENT
- Exploring innovative new technologies that will create a more efficient, greener, and safer future
- Compliance with the International Maritime Organization (IMO) regarding safety and security
- Desire to converge IT and OT environment

CUSTOMER NEEDS
- Comply with numerous cybersecurity requirements
- Regular software updates
- Improve the performance, efficiency, and security

FORTINET SOLUTION
- Clear advantages in licensing, features, and integration through Fortinet Security Fabric
- Provides broad visibility and control over the digital attack surface
- Products:
  - FortiGate, FortiGate Next Generation Firewall, FortiClient, FortiToken, FortiNAC, FortiAP, FortiSandbox, FortiManager, FortiAnalyzer, FortiSIEM

https://www.fortinet.com/customers/rh-marine

 40

북미 펄프 및 제지 제조업체

랜섬웨어 발생 후 OT 보호

사이버 보안 검토 동기

- 2020년 초 랜섬웨어 발생으로 운영 중단 시간 발생
- 상당한 수리 비용

고객 요구 사항

- 엔드포인트/기기 보호
- IT 환경에서 OT를 분리하기 위한 네트워크 세분화
- 네트워크 액세스 제어
- 메일 보호
- 손쉬운 구성 및 배포
- OT 및 IT 보안 도메인 전문성

포티넷 솔루션

- FortiMail
- Advanced Threat Protection
- FortiEDR
- FortiGate
- FortiNAC
- Intrusion Protection System

독일 글로벌 자동차 제조 그룹

장기적인 EDR PoC를 진행하여 OT영역 전반에 강력한 엔드포인트 보안 구축

사이버 보안 검토 동기

- 기존 엔드포인트 솔루션(Symantec & Sophos)의 지원 종료(EoS)

고객 요구 사항

- 소규모 설치와 고성능 collector agent 요건
- 레거시 OS(예: Windows XP)을 포함한 다양한 OS 유형 지원
- 하이브리드 온프레미스 배포 아키텍처
- 배포와 관리의 단순성
- Siemens, Schneider Electric, Rockwell, ABB, Kuka 등 산업용 제어 공급업체와의 입증된 호환성 (HMI, EWS, SCADA서버, Historians, etc)
- 도입 결정의 핵심요소는 PoC를 통한 성공적인 개념 증명

포티넷 솔루션

- 전세계 20개 자동차 생산 공장을 커버하는 솔루션 (6만개 단말)
- FortiEDR은 FortiGate NGFW & SIEM와의 통합 계획 예정

[redacted] claimed that FortiEDR provided one of the broadest OS coverage models they had seen. Fortinet was able to support [redacted] needs for twelve on-premises central managers to manage the EDR solution.

The PoC ran for almost a year. During this time, [redacted] intensively tested the compatibility of the collector on most of the production systems that they use. Performance impacts and useability was tested during this phase. FortiEDR was the only suitable OT on-prem solution in the market. One of our technical key advantages were that we support legacy Microsoft OS (Windows XP).

The endpoint security software had to be able to run on their automation and control systems such as HMIs, engineering workstations, jump and SCADA servers, workstations and historians.

ECHOENERGIA WIND (브라질 / 풍력발전)

12개의 브라질 풍력 발전 단지에 1.2GW, 484개의 풍력 터빈

사이버 보안 검토 동기

- 운영 초기 몇년 이내에 급속한 사업 확장 지원
- 충족해야 하는 높은 수준의 산업 표준
- 혁신적인 에너지 솔루션의 안전한 사용 보장

고객 요구 사항

- 업계 규정 준수
- 요구 사항 충족
- 지능적이고 빠른 관리
- 고가용성 통신을 제공하기 위한 IT 인프라 제공
- 과투자 방지
- 보안 강화

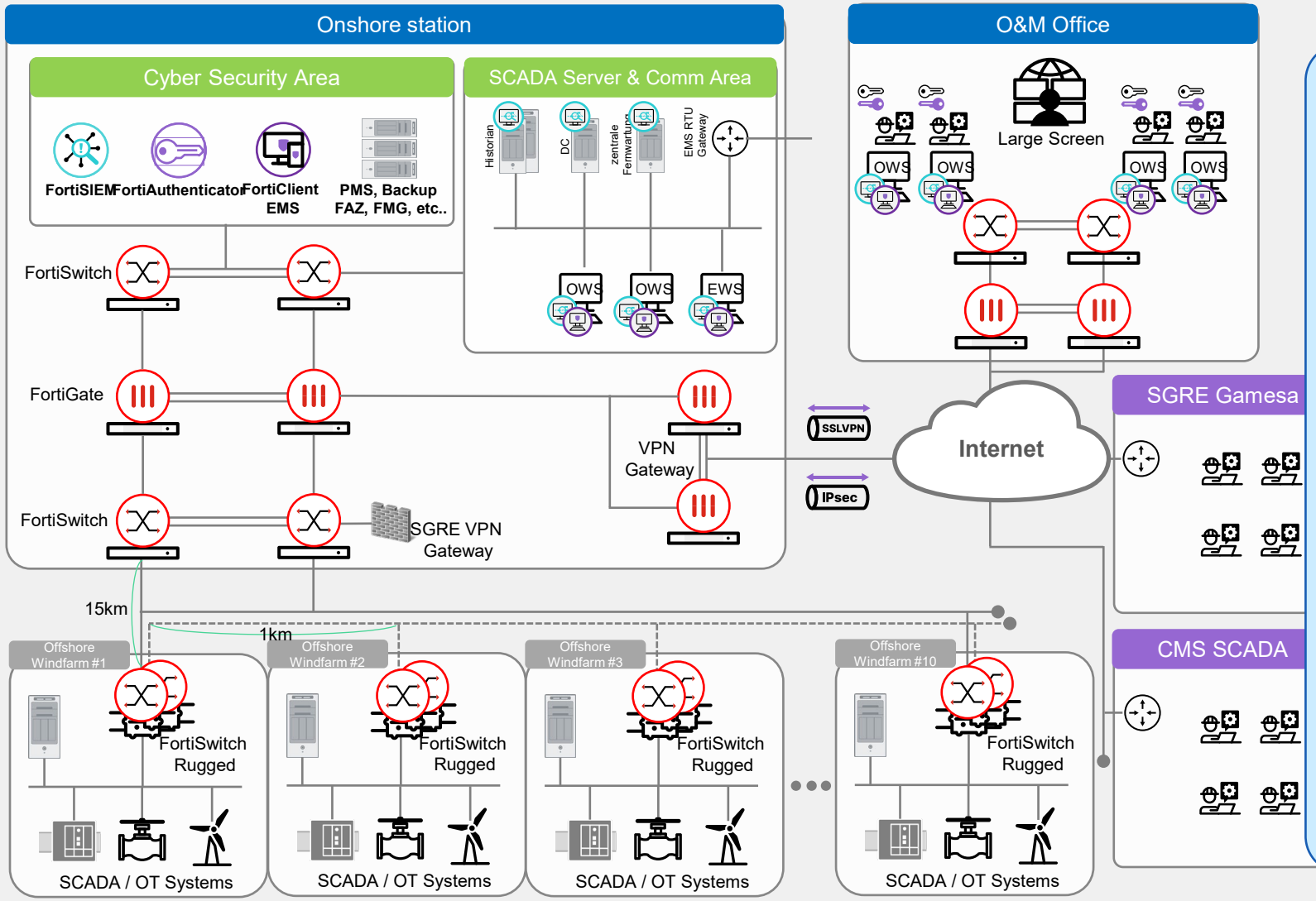
포티넷 솔루션

- Fortinet의 솔루션은 산업 요구 사항을 충족하고 지리적 문제를 극복하는 데 도움을 주었다.
  - FortiGate & FortiGate Rugged
  - FortiSwitch & FortiSwitch Rugged
  - FortiAP
  - FortiAuthenticator
  - FortiToken

https://www.fortinet.com/customers/echoenergia

국내 풍력발전 OT보안 구축사례

IEC-62443, NERC CIP, NIST CSF 준수



1. 풍력발전 OT Security 구축 사례

- 해상에 설치되는 총 10개의 WTG와, 무인도에 구축될 Onshore station의 네트워크/보안 인프라
- FortiGate와 FortiSwitch 구성을 통한 네트워크 트래픽 가시성 확보
- FortiEDR과 FortiClient로 멀웨어/랜섬웨어 대응
- FortiSIEM을 통한 Onshore/Offshore 모니터링 제공
- FortiClient VPN을 통한 외부 유지보수 업체 접근 / FortiAuthenticator로 FSSO 지원
- FortiAuthenticator/FortiToken으로 2FA 지원

2. 납품 솔루션

- Fortigate, Fortiswitch, Fortiswitch Rugged, FortiSIEM, FortiAuthenticator, FortiEDR/MDR, FortiClient, FortiManager, FortiAnalyzer

단계별 OT보안 구축 전략(안)

공격 표면의 증가와, 각종 신규 보안 규정

잘 공유되지 않으나, 증가되고 있는 OT/ICS 보안사고를 줄이기 위해 개정되는 보안 규정들

2018

- TSMC **WannerCry** 변종 멜웨어 공격으로 공장 2일간 중단

2019

- **랜섬웨어**로 인해 Norsk Hydro 공장 운영 중단
- **랜섬웨어**로 인해 ASCO 부품 가동 중단

2020

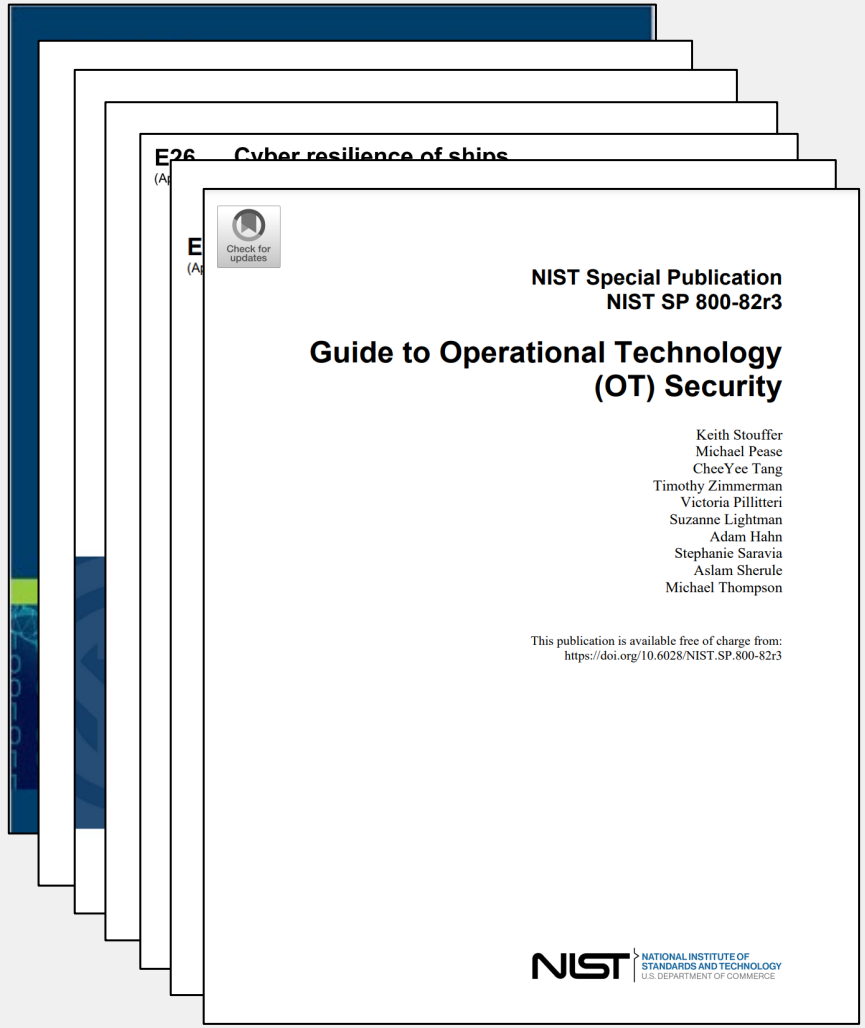
- Honda에 **EKANS/SNAKE 랜섬웨어** 공격
- SolarWinds Orion- Sunburst Malware 공급망 공격

2021

- 플로리다 Oldsmar **TeamView/RDP** 취약점을 통한 수도 공급 해킹
- JBS USA 육가공업체 **랜섬웨어 공격** (비트코인 122억 지급)
- 대형 양조회사 Molson Coors의 랜섬웨어 공격으로 생산 중단
- 미국 콜로니얼 파이프라인 해킹 **랜섬웨어 공격** (비트코인 50억원 지급)

2022

- 미국 트랙터 제조업체 ACGO 랜섬웨어 공격으로 생산 중단
- Toyota 부품 공급업체에 **랜섬웨어** 공격으로 28개 조립라인 중단
- 우크라이나 전력망 멜웨어 공격 사건



단계별 OT 보안 구축전략(안)

NIST CSF (Cyber Security Framework)

※ NIST : 미국표준기술연구소

4.1 식별 (Identity)

4.1.1 선내 CBS 및 네트워크 목록(Inventory)

4.2 보호 (Protect)

4.2.1 보안 구역(Security Zones)
4.2.2 네트워크 보호 안전장치(Safeguard)
4.2.3 안티바이러스, 안티멀웨어, 안티스팸 및 악성코드로부터 보호
4.2.4 접근 통제(Access control)
4.2.5 무선 통신(Wireless Communication)
4.2.6 원격 접근 통제 및 신뢰할 수 없는 네트워크 에서 통신
4.2.7 모바일 및 휴대용 장치의 사용

4.3 탐지 (Detect)

4.3.1 네트워크 운영 모니터링
4.3.2 CBS 및 네트워크의 진단 기능

4.4 대응 (Respond)

4.4.1 사고 대응 계획 (Incident response plan)
4.4.2 로컬, 독립 또는 수동 운전 지원
4.4.3 네트워크 격리 (Network isolation)
4.4.4 최소 위험 조건으로의 복귀

4.5 복구 (Recover)

4.5.1 복구 계획
4.5.2 백업 및 복구 기능 (Backup and restore capability)
4.5.3 제어된 종료, 리셋, 롤백 및 재시작

단계별 OT 보안 구축전략(안)

난이도 + 비용

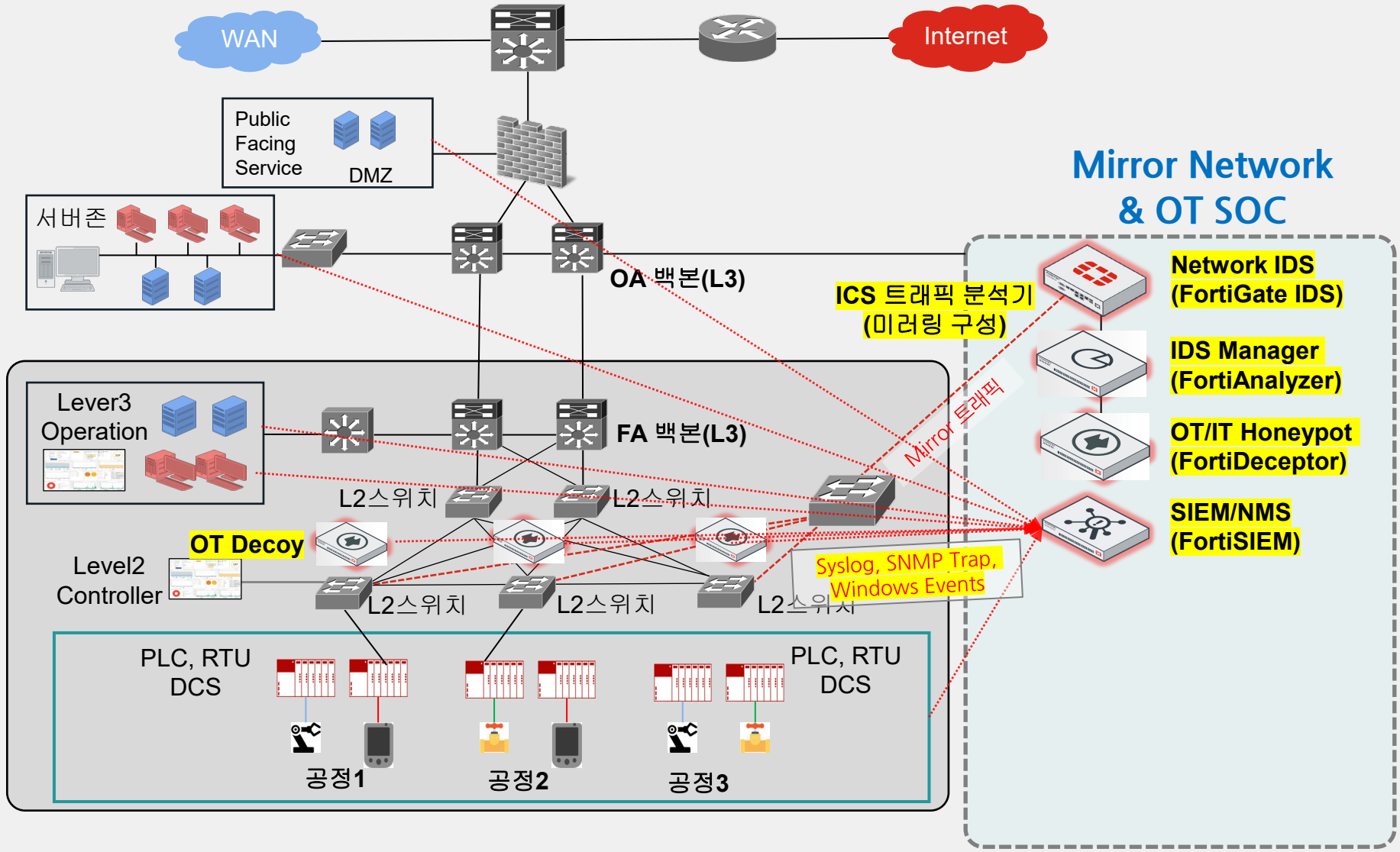
	1단계	2단계	3단계	4단계
Identify (식별)	OT Network IDS	Secure LAN-Edge	User Authenticate	3rd party (Asset Inventory)
Protect (보호)	OT/IT Deception 3rd Party (USB/UTP Port Lock)			OT Protocol DPI
Detect (탐지)	SIEM+NMS	Endpoint Protection	Secure Remote Access	ATP Solution
Respond (대응)	IDS Manager		3rd party (OS Backup & Recovery, Patch Management)	
Recover (복원)				Network Config Managing (FortiManager)

산업 환경에서 단계별 OT보안 구축 전략

1단계. 운영중인 산업 환경에서의 보안

- **Network IDS (FortiGate IDS + FAZ)**
  - 미러링 모드로 구축
  - 최소한의 위협 탐지를 위함
  - FortiGate IDS의 리포트 자동 출력
  - 최소한의 위협 모니터링 / 관리를 위함
- **OT/IT Honeypot(FortiDeceptor)**
  - 운영 환경 내부의 위협 탐지 및 자산 가시성
- **SIEM/NMS (FortiSIEM)**
  - 이기종 로그 수집, 네트워크 모니터링
  - 인시던트 알림 및 OT 대시보드 활용

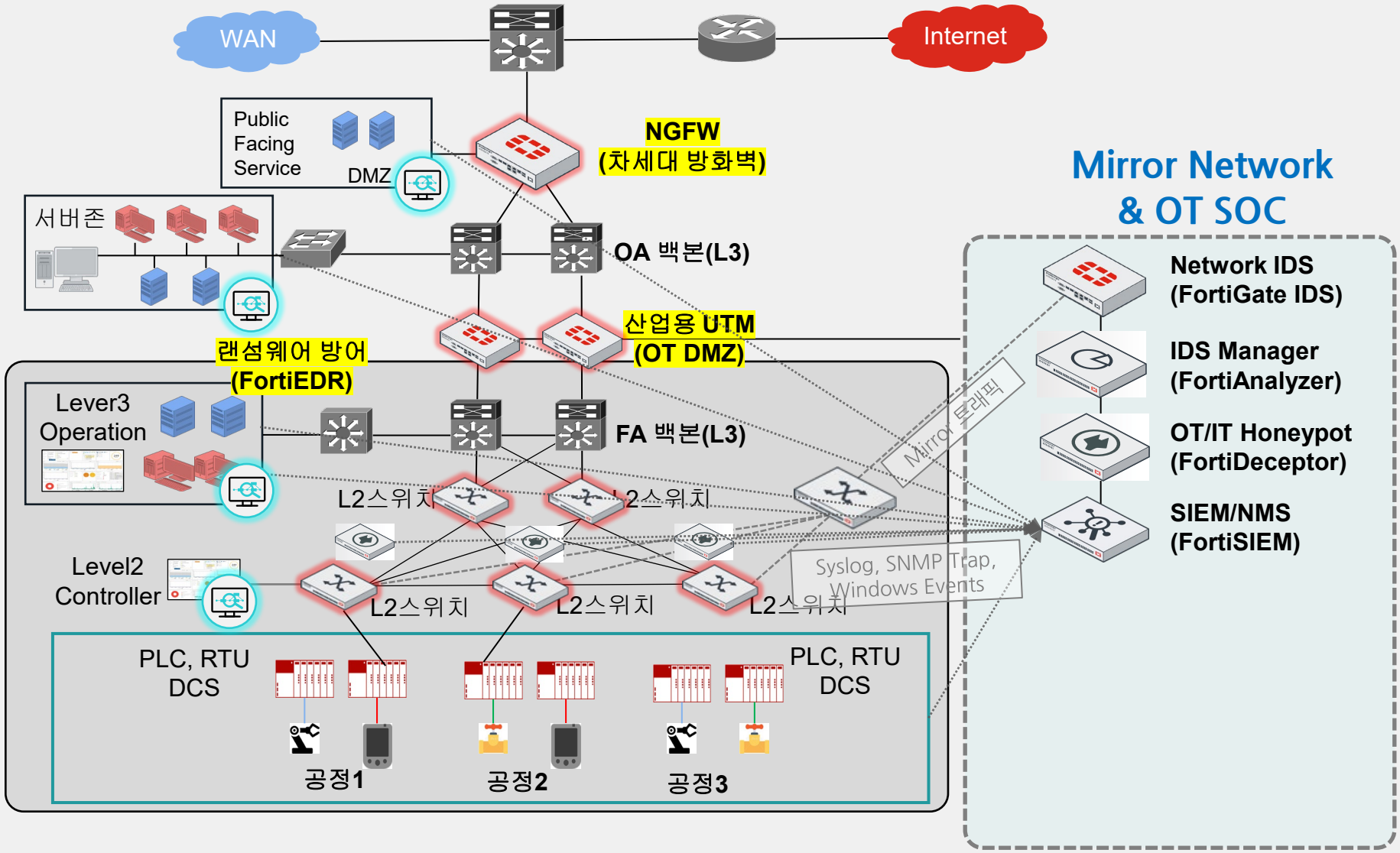
- 3rd Party(USB/UTP PortLock)
  - 내부 시스템의 물리적 포트 Lock



산업 환경에서 단계별 OT보안 구축 전략

2단계. 신규 산업 환경에서의 보안

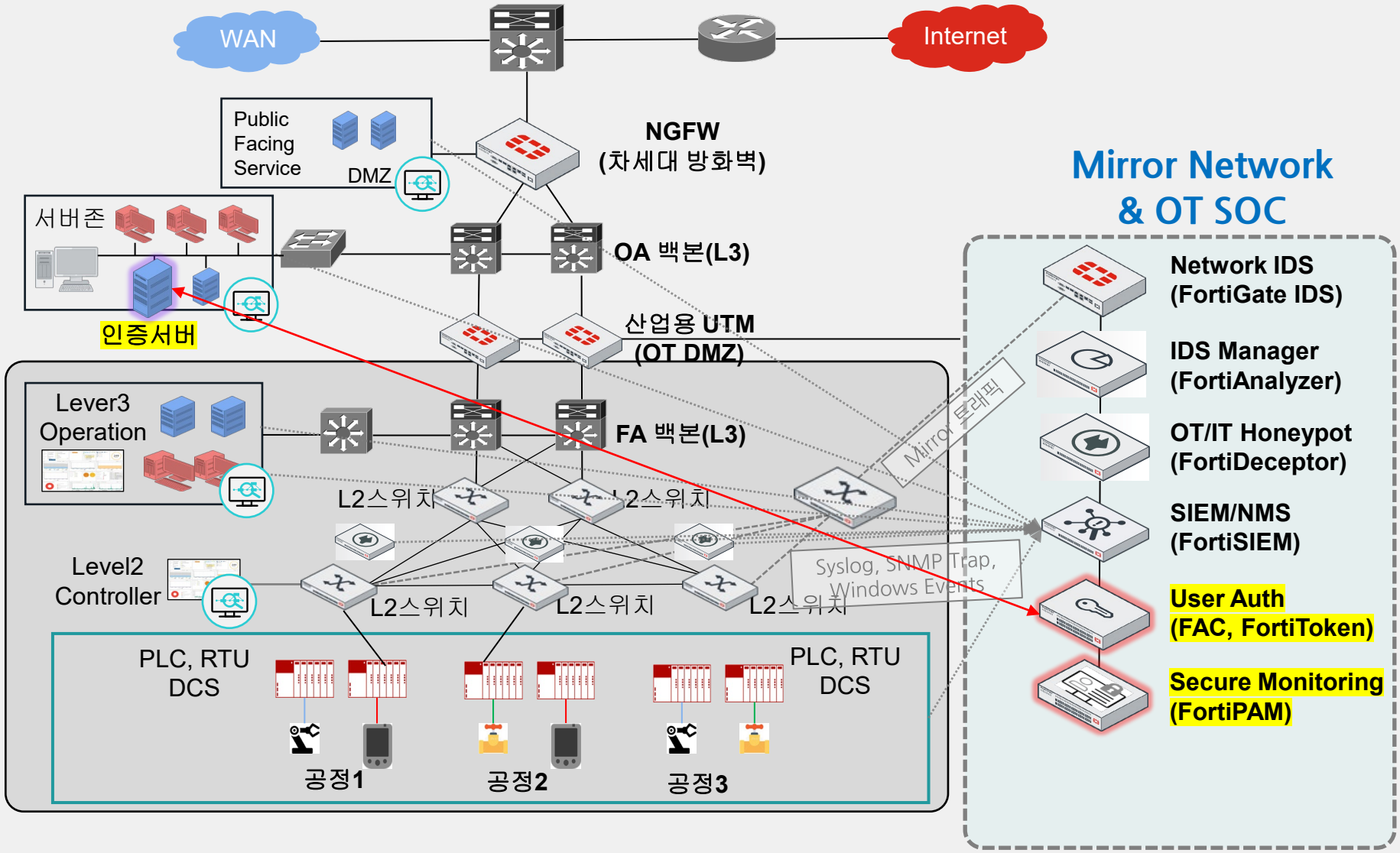
- **FortiGate NGFW**
  - 차세대방화벽, IT/OT & 공정별 망분리,
  - VDOM 기능 활용 TCO 절감 효과
- **FortiSwitch(Managed FortiGate)**
  - 네트워크 가시성, 스위치 통합관리,
  - Micro-Segmentation, FortiGate NAC 등 보안기능 활용
- **Endpoint 보호 (FortiEDR)**
  - Application Whitelisting, Anti-Virus, Media Control(USB 차단 등)
  - 행위/코드기반 분석 활용 랜섬웨어 대응



산업 환경에서 단계별 OT보안 구축 전략

3단계. 산업 환경 보안 고도화

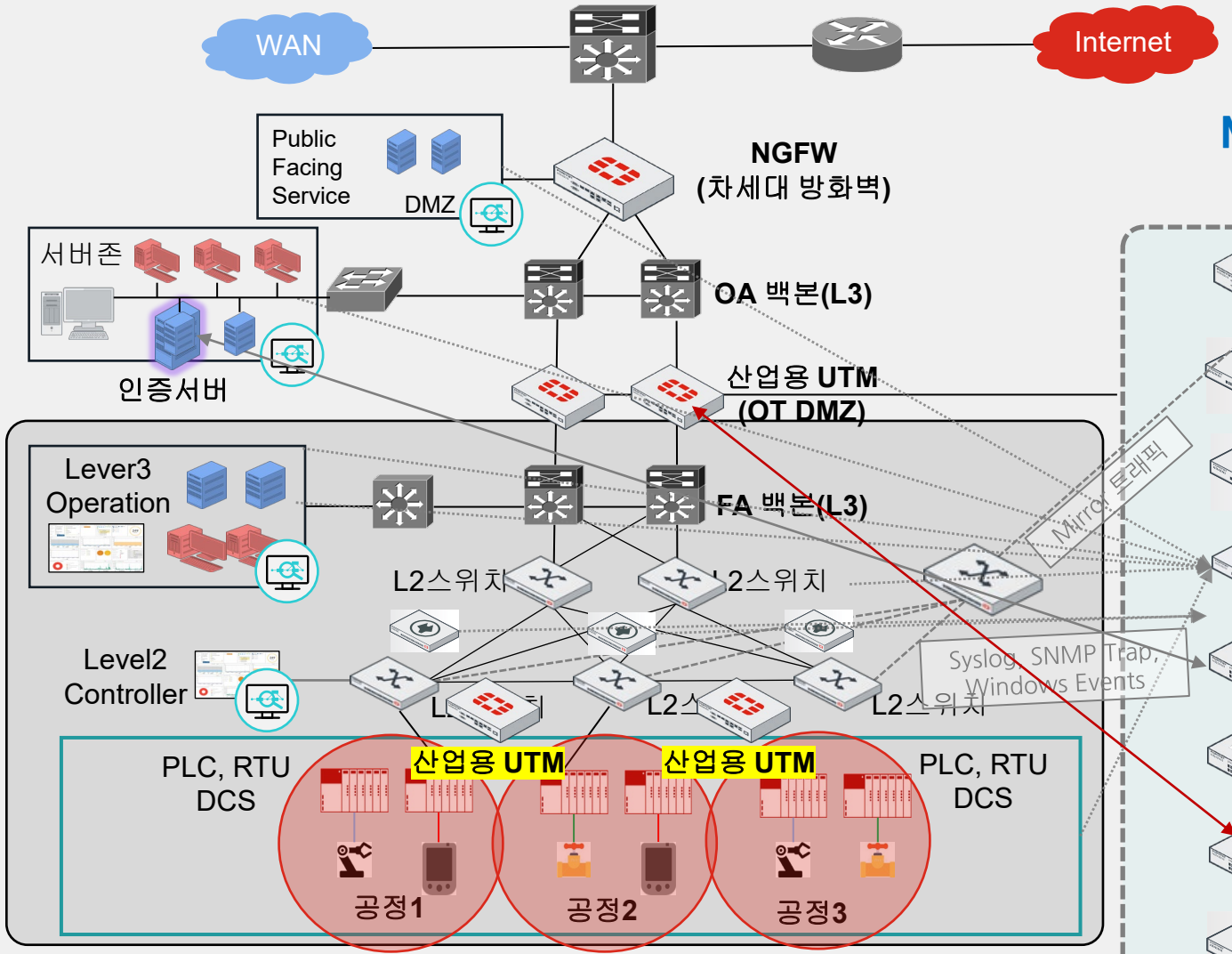
- **Secure Monitoring(FortiPAM)**
  - OT 시스템의 안전한 원격 접근 관리
  - 세션 로깅 및 녹화, 커멘드 제어, 감사
- **User Authenticate(FAC/FortiToken)**
  - 인증서버 연동을 통한 사용자 접근관리
  - FortiToken(Mobile or Device)로 2FA 구현
- 3rd Party(Backup & Recovery)
  - 내부 Windows/Linux 시스템의 백업관리 솔루션
- 3rd Party(Patch Management)
  - 내부 Windows OS의 최신 업데이트 패치관리



산업 환경에서 단계별 OT보안 구축 전략

4단계. 산업 환경의 심층적인 보안

- **OT Protocol DPI(FortiGate+Industrial)**
  - 공정 내 중요 자산에 대한 파라미터 제어
  - 인가된 시스템의 허용된 제어 명령만 시스템에 입력하도록 함
- **Network Config Managing (FortiManager)**
  - FortiGate 네트워크/보안 정책 백업관리
  - 시그니처 업데이트 중앙관리
- **ATP Solution (FortiSandbox)**
  - IT와 OT 환경에서 파일이 자주 이동하는 경우 Network ATP 고려
- 3rd Party(Asset Inventory)
  - 자산 인벤토리 관리, 이상징후 탐지



Mirror Network & OT SOC

- Network IDS (FortiGate IDS)
- IDS Manager (FortiAnalyzer)
- OT/IT Honeypot (FortiDeceptor)
- SIEM/NMS (FortiSIEM)
- User Auth (FAC, FortiToken)
- Secure Monitoring (FortiPAM)
- **ATP Solution (FortiSandbox)**
- **Network Managing (FortiManager)**

산업 환경에서의 단계별 OT보안 구축 전략(안)

1단계. 운영중인 산업 환경에서의 보안

- **Network IDS (FortiGate IDS + FAZ)**
  - 미러링 모드로 구축
  - 최소한의 위협 탐지를 위함
  - FortiGate IDS의 리포트 자동 출력
  - 최소한의 위협 모니터링 / 관리를 위함
- **OT/IT Deception(FortiDeceptor)**
  - 운영 환경 내부의 위협 탐지 및 자산 가시성
- **SIEM/NMS (FortiSIEM)**
  - 이기종 로그 수집, 네트워크 모니터링
  - 인시던트 알림 및 OT 대시보드 활용

- 3rd Party(USB/UTP PortLock)
  - 내부 시스템의 물리적 포트 Lock

2단계. 신규 산업 환경에서의 보안

- **FortiGate NGFW**
  - 차세대방화벽, IT/OT & 공정별 망분리,
  - VDOM 기능 활용 TCO 절감 효과
- **FortiSwitch(Managed FortiGate)**
  - 네트워크 가시성, 스위치 통합관리,
  - Micro-Segmentation, FortiGate NAC 등 보안기능 활용
- **Endpoint 보호 (FortiEDR)**
  - Application Whitelisting, Anti-Virus, Media Control(USB 차단 등)
  - 행위/코드기반 분석 활용 랜섬웨어 대응

3단계. 산업 환경 보안 고도화

- **Secure Monitoring(FortiPAM)**
  - OT 시스템의 안전한 원격 접근 관리
  - 세션 로깅 및 녹화, 커멘드 제어, 감사
- **User Authenticate(FAC/FortiToken)**
  - 인증서버 연동을 통한 사용자 접근관리
  - FortiToken(Mobile or Device)로 2FA 구현

- 3rd Party(Backup & Recovery)
  - 내부 Windows/Linux 시스템의 백업관리 솔루션
- 3rd Party(Patch Management)
  - 내부 Windows OS의 최신 업데이트 패치관리

4단계. 산업 환경의 심층적인 보안

- **OT Protocol DPI(FortiGate+Industrial)**
  - 공정 내 중요 자산에 대한 파라미터 제어
  - 인가된 시스템의 허용된 제어 명령만 시스템에 입력하도록 함
- **Network Config Managing (FortiManager)**
  - FortiGate 네트워크/보안 정책 백업관리
  - 시그니처 업데이트 중앙관리
- **ATP Solution (FortiSandbox)**
  - IT와 OT 환경에서 파일이 자주 이동하는 경우 Network ATP 고려
- 3rd Party(Asset Inventory)
  - 자산 인벤토리 관리, 이상징후 탐지

난이도 + 비용

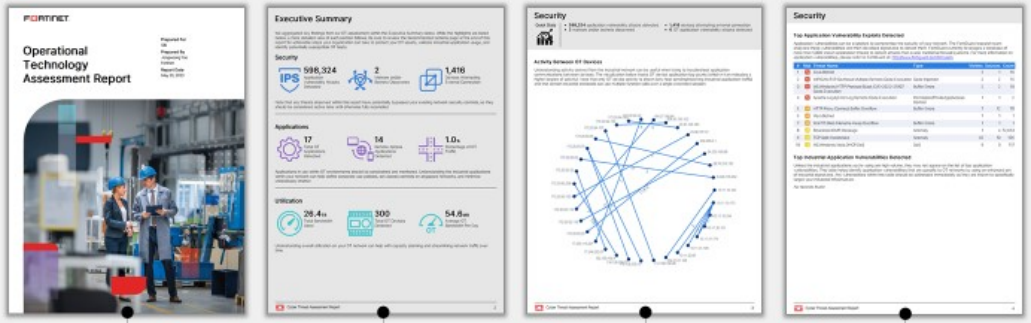
플랫폼 기반의 보안 솔루션을 단계적으로 적용하여
고객 환경에 맞는 OT 보안 전략 수립 및 최적화 수행

OT/ICS를 위한 보안 플랫폼 구축 프로젝트 제안 (예시)

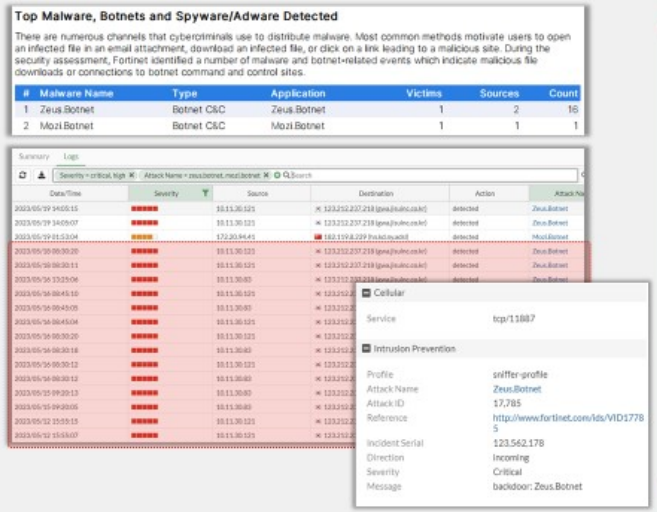
OT 보안 플랫폼 구축 전략 – OT IDS

FortiGate(IDS)/FortiAnalyzer(IDS Manager) + FortiSIEM : 운영 중단없는 OT망 침입탐지

OT Report 제공 사항



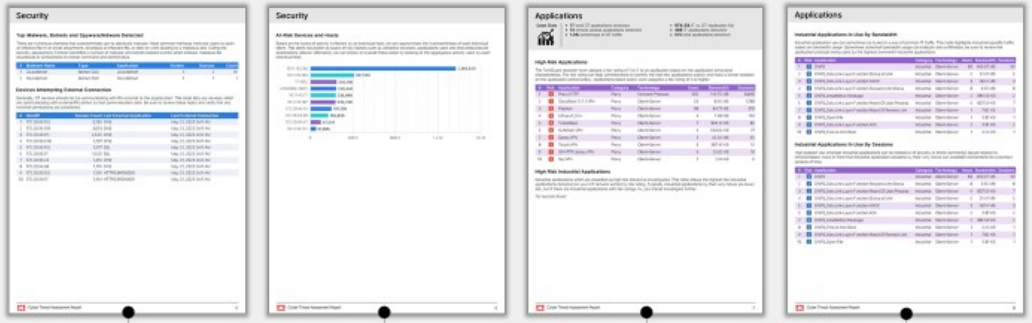
멀웨어 감염 정보



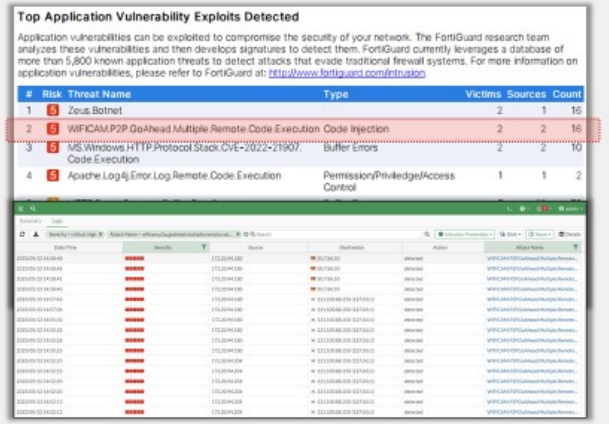
Botnet 활동 탐지

- **Severity – 5(Critical)**
- **Threat Name** –Zeus.Botnet
- **Type** – Botnet C&C
- **Count** – 16
- Zeus Botnet은 웹사이트를 감염시켜 사용자의 개인정보나 금융정보를 탈취하는 악성코드 봇넷(Botnet).
- Zeus Botnet은 2007년부터 활동을 시작하여, 금융 기관 등을 대상으로 한 APT 공격 툴로 수행되었고 감염된 컴퓨터들을 제어하고, 탈취한 정보를 분석하여 금융 사기 등을 수행.
- PCAP이 남아있지 않으나, Backdoor 메시지로 보아 이미 감염된 자산이 내부에 있는 가능성이 있음

OT Report 제공 사항



IT/OT Application 취약점 탐지 정보



P2P 취약점 탐지

- **Severity – 5(Critical)**
- **Threat Name** – WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution
- **Type** – Code Injection
- **Count** – 16
- GoAhead 웹 서버의 취약점을 이용하여 원격에서 코드 실행이 가능해지는 취약점. 이 취약점은 WIFICAM P2P 카메라 및 기타 다른 브랜드의 카메라에서 발견되었고, GoAhead 웹 서버의 버전 업그레이드로 해결할 수 있음. 사용자는 업그레이드를 진행하거나, 방화벽 등의 보안 장치를 통해 외부 침입을 차단할 필요가 있습니다.
- 이 취약점을 이용하면, 공격자는 인증되지 않은 원격 코드를 실행하여 원격 카메라를 제어할 수 있습니다.

OT 보안 플랫폼 구축 전략 – Digital Ghost

FortiDeceptor + any SIEM : OT망에 특화된 기만 솔루션

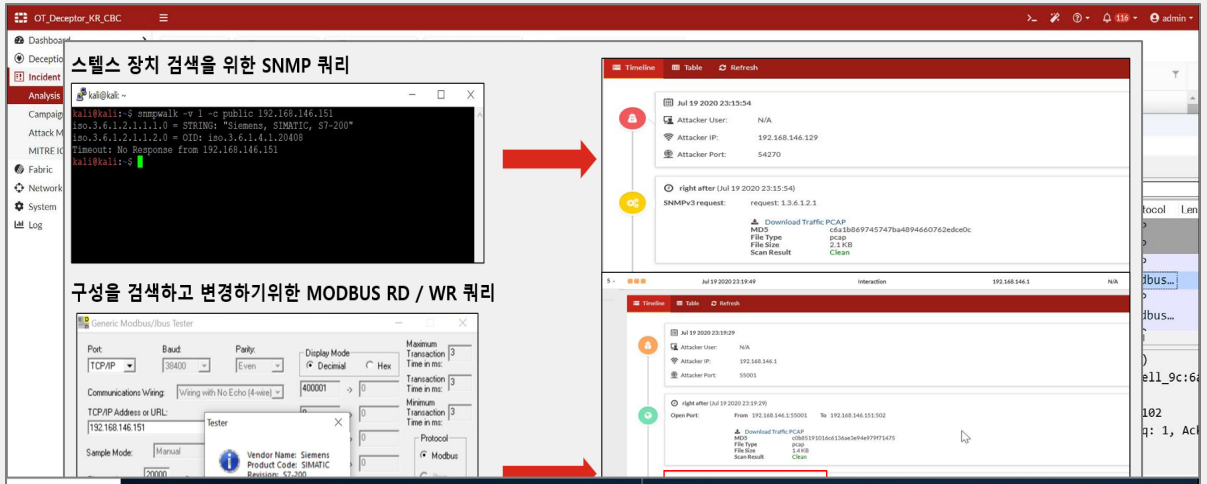
공격자를 가짜 자산인 디지털 고스트로 유인하여 기업의 실제 자산을 보호

Decoy (유인 시스템)
실제 네트워크에 연결되어 작동하는 가상 자산 및 네트워크 장치, 가상 애플리케이션

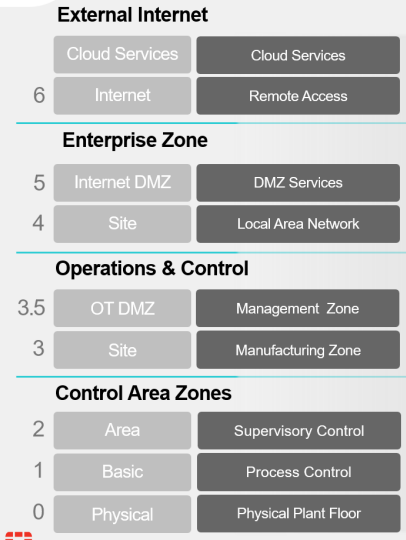
Lure (미끼)
Decoy를 통해 탐지하고자 하는 서비스

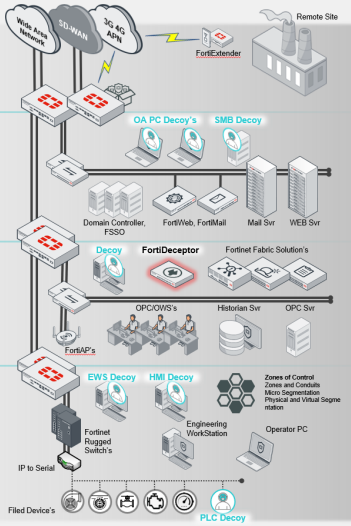
Network Traffic
공격자를 유인하기 위한 Fake Network Traffic beaconing (SMB, CDP, UPnP, etc…)

Breadcrumbs(Token)



퍼듀모델 기반의 디지털 고스트 구축





- IT DMZ에 웹 서비스를 모방하는 디코이를 배포하거나, Fake VPN Gateway를 디코이로 배포하여 SSL VPN을 서비스로 오픈해 둡니다.
- OA PC들, ERP/POS/DB/WEB 서버 등 중요 앱을 디코이로 배포합니다.
- RDP, SMB 등의 서버에서 사용하는 서비스를 Lure로 오픈해 둡니다.
- 시스템 데이터 및 IT/OT 장비를 모방하는 디셉션 시스템을 구축하여 SCADA 관리 HMI, App, IT 데스크톱 및 업무용 파일서버를 디코이로 구축합니다.
- 디셉션 시스템을 고객사 환경에서 사용중인 ICS 벤더사의 PLC, HMI, IoT센서(예: Siemens, Rockwell, Schneider) 및 Windows XP, 7과 같은 OT 자산을 고객사의 "원본 이미지" 로 배포합니다.

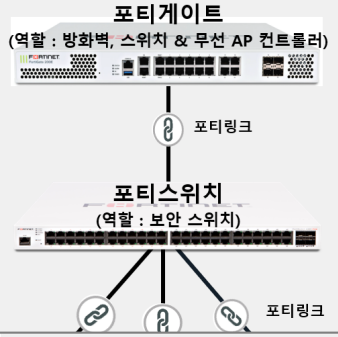
우리는 왜 OT환경에서 Deception 기술을 검토해야 할까요?

OT 보안 플랫폼 구축 전략- 유무선 통합관리

본사 유무선 LAN-Edge와 해외 거점을 위한 Secure SD-Branch

FortiSwitch / FortiAP

네트워크와 보안 컨버전스의 핵심 솔루션



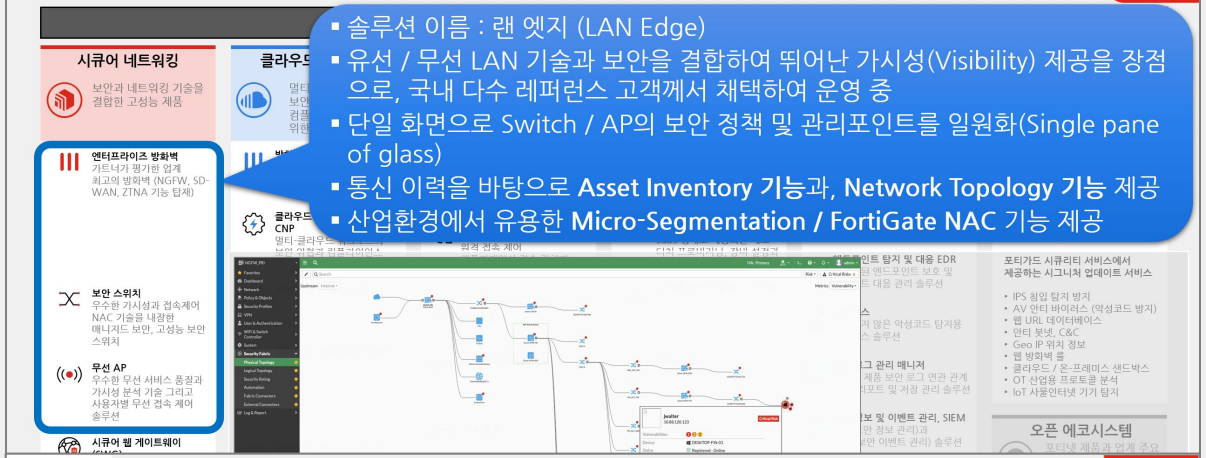
1 포티게이트(FortiGate)

포티게이트의 시큐어 유/무선 컨트롤러를 통해 유선 및 무선 네트워킹 서비스를 통합한 가장 이상적인 솔루션을 제공합니다. 엔터프라이즈급 무선-랜 보안 뿐 아니라, 유선 네트워크에 대한 보안까지 하나의 통합 플랫폼에서 제공하는 고성능 엔터프라이즈 유/무선 네트워크 솔루션입니다.

2 포티스위치 (FortiSwitch)

매니지드 스위치 구축을 위한 별도의 장비 설정 등이 필요없이 UTP 케이블과 전원만 연결하면, 포티게이트와 자동으로 인지하고 연동합니다. 이로 인해 네트워크 구축 시간이 단축이 되며, 네트워크 확장도 용이합니다.

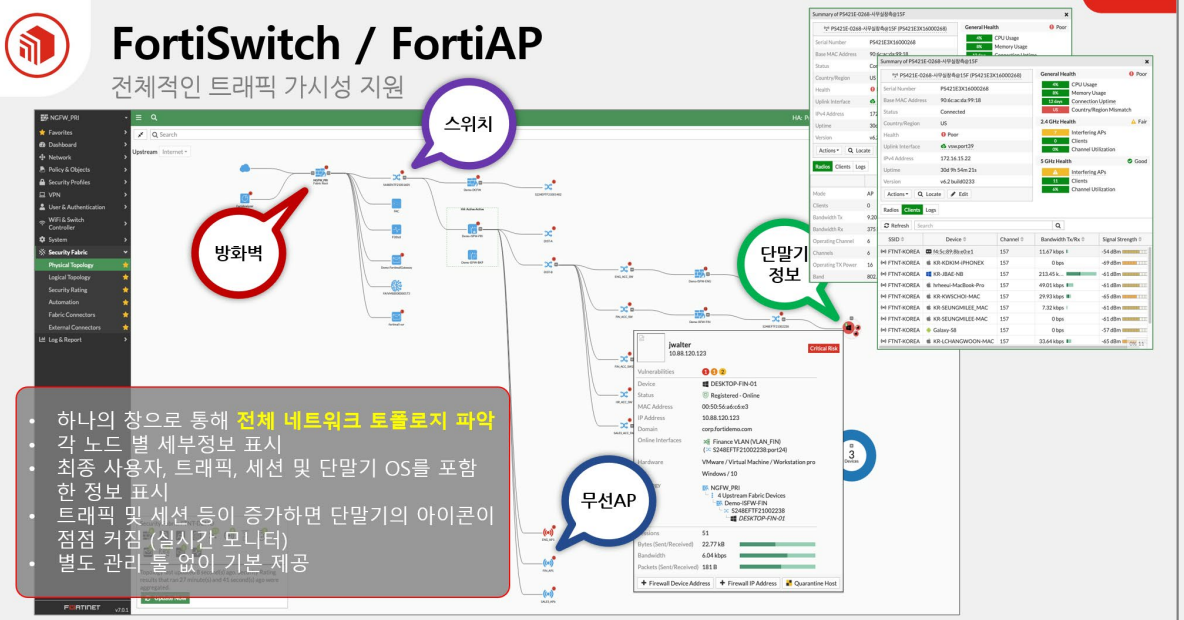
3 포티AP(FortiAP)



- 솔루션 이름 : 랜 엣지 (LAN Edge)
- 유선 / 무선 LAN 기술과 보안을 결합하여 뛰어난 가시성(Visibility) 제공을 장점으로, 국내 다수 레퍼런스 고객께서 채택하여 운영 중
- 단일 화면으로 Switch / AP의 보안 정책 및 관리포인트를 일원화(Single pane of glass)
- 통신 이력을 바탕으로 **Asset Inventory 기능**과, **Network Topology 기능** 제공
- 산업환경에서 유용한 **Micro-Segmentation / FortiGate NAC** 기능 제공

FortiSwitch / FortiAP

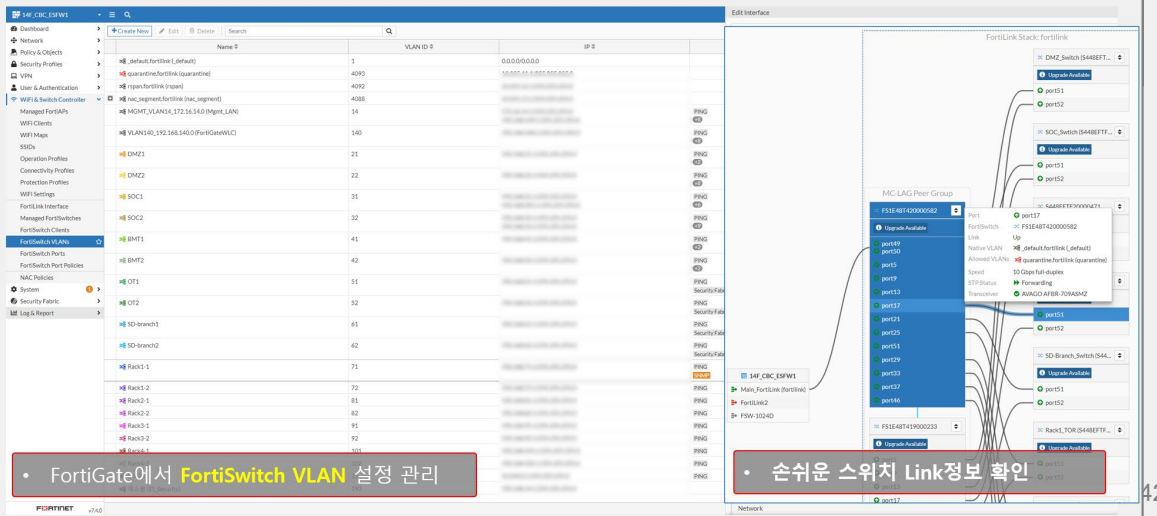
전체적인 트래픽 가시성 지원



- 하나의 창으로 통해 **전체 네트워크 토폴로지 파악**
- 각 노드 별 세부정보 표시
- 최종 사용자, 트래픽, 세션 및 단말기 OS를 포함한 정보 표시
- 트래픽 및 세션 등이 증가하면 단말기의 아이콘이 점점 커짐 (실시간 모니터)
- 별도 관리 툴 없이 기본 제공

FortiSwitch / FortiAP

하나의 **단일 관리창**(Single Pain of Glass)으로 네트워크 인프라 / 유무선 통합관리



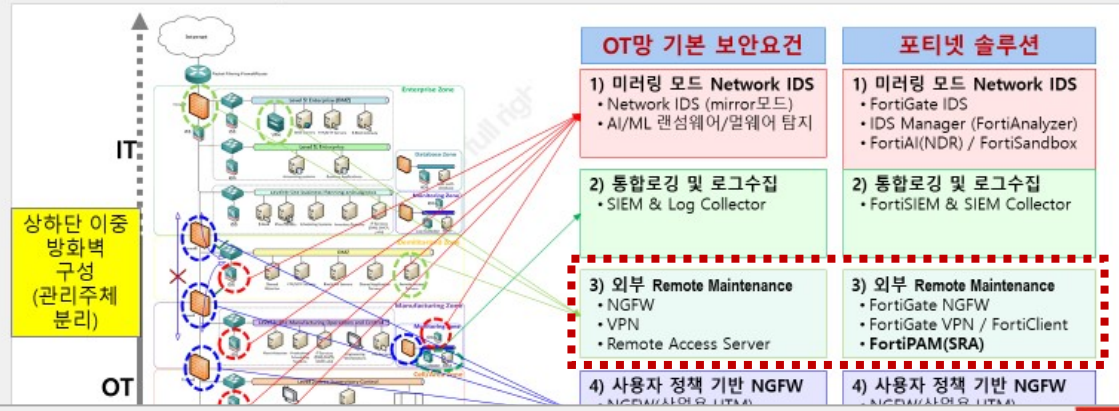
- FortiGate에서 **FortiSwitch VLAN** 설정 관리
- **손쉬운 스위치 Link정보 확인**

OT 보안 플랫폼 구축 전략- Secure Remote Access

Remote Maintenance 보안 : FortiPAM(SRA) + VPN

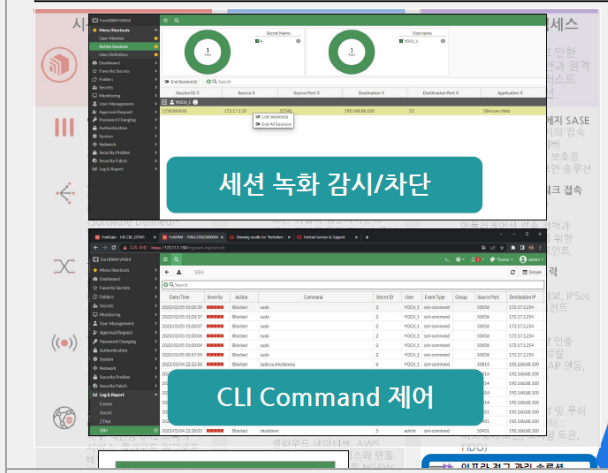
OT 보안 기본 요건

NIST SP 800-82 / IEC-62443 기반 기본 보안요건



OT망 기본 보안요건	포티넷 솔루션
1) 미러링 모드 Network IDS • Network IDS (mirror모드) • AI/ML 랜섬웨어/멀웨어 탐지	1) 미러링 모드 Network IDS • FortiGate IDS • IDS Manager (FortiAnalyzer) • FortiAI(NDR) / FortiSandbox
2) 통합로깅 및 로그수집 • SIEM & Log Collector	2) 통합로깅 및 로그수집 • FortiSIEM & SIEM Collector
3) 외부 Remote Maintenance • NGFW • VPN • Remote Access Server	3) 외부 Remote Maintenance • FortiGate NGFW • FortiGate VPN / FortiClient • **FortiPAM(SRA)**
4) 사용자 정책 기반 NGFW	4) 사용자 정책 기반 NGFW

포티넷 코리아 주력 솔루션과 제품 2023



NOC 패브릭 관리 센터

포티넷 제품 보안 정책과 개체 관리 및 다양한 관리 업무를 수행하는 중앙 관리 솔루션

SOC 패브릭 관리 센터

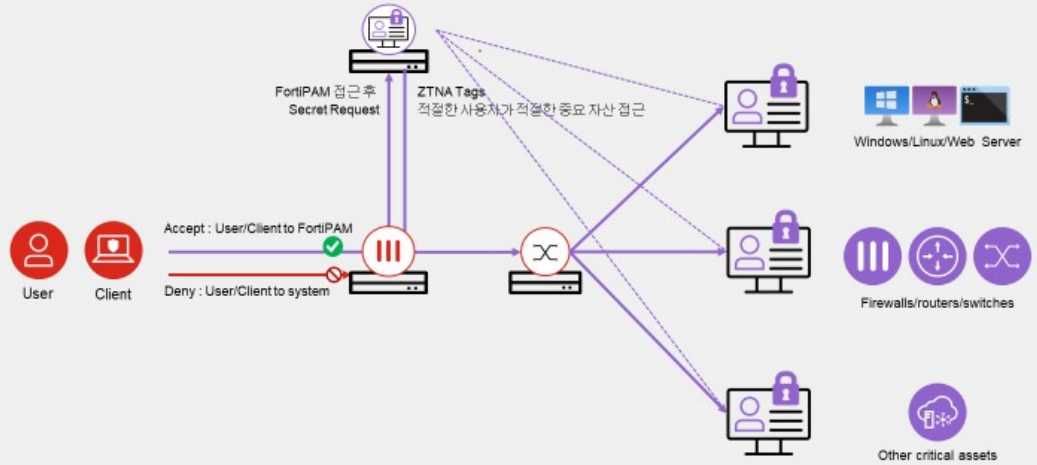
보안 이벤트 연관 관계 분석과 같이 다양한 보안 관제 업무 영역에 필요한 솔루션

보안 위협 인텔리전스

포티넷 제품에 탑재되는 보안 시그니처 서비스를 제공하는 글로벌 위협 인텔리전스 서비스

- 솔루션 : 원격 유지보수 서비스(FortiSRA)
- 원격 접속을 활용하여 업무를 수행하는 산업 환경을 위한 신제품
  - VNC, RDP 등의 세션 녹화 / 감시 / 차단기능
  - TELNET, SSH 등의 CLI 접근 Command 제어 / 차단기능
  - 사용자 세션 모니터링 및 이상징후 탐지 시 세션 차단 기능

FortiPAM 유스케이스 – 안전한 원격접속 보안

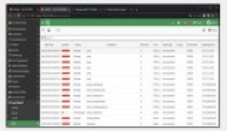


FortiPAM 기능

FortiPAM 기능 소개

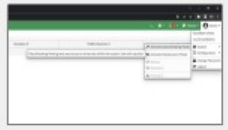

사용자 별 Secrets(PAM Security Policy)


Critical Assets 접근 관리 기능


SSH Commend 제한 및 모니터링


패스워드 변경 자동화 기능


세션 감시 및 차단 기능


'유리 깨기' 모드와 '관리' 모드


ZTNA Tag를 이용한 시스템 접근제어


세션 녹화 / 감시 기능

Fortinet 시큐리티 패브릭 - OT

안전한 네트워크
- 네트워크 세그멘테이션
- 네트워크 마이크로 세그멘테이션
- LAN Edge - OT환경의 네트워크 가시성
- DPI를 통한 파라미터 변조 보호

제로 트러스트 액세스
- 네트워크 액세스 제어
- 권한/역할 기반 액세스 제어
- OT환경 내의 보안 원격 액세스

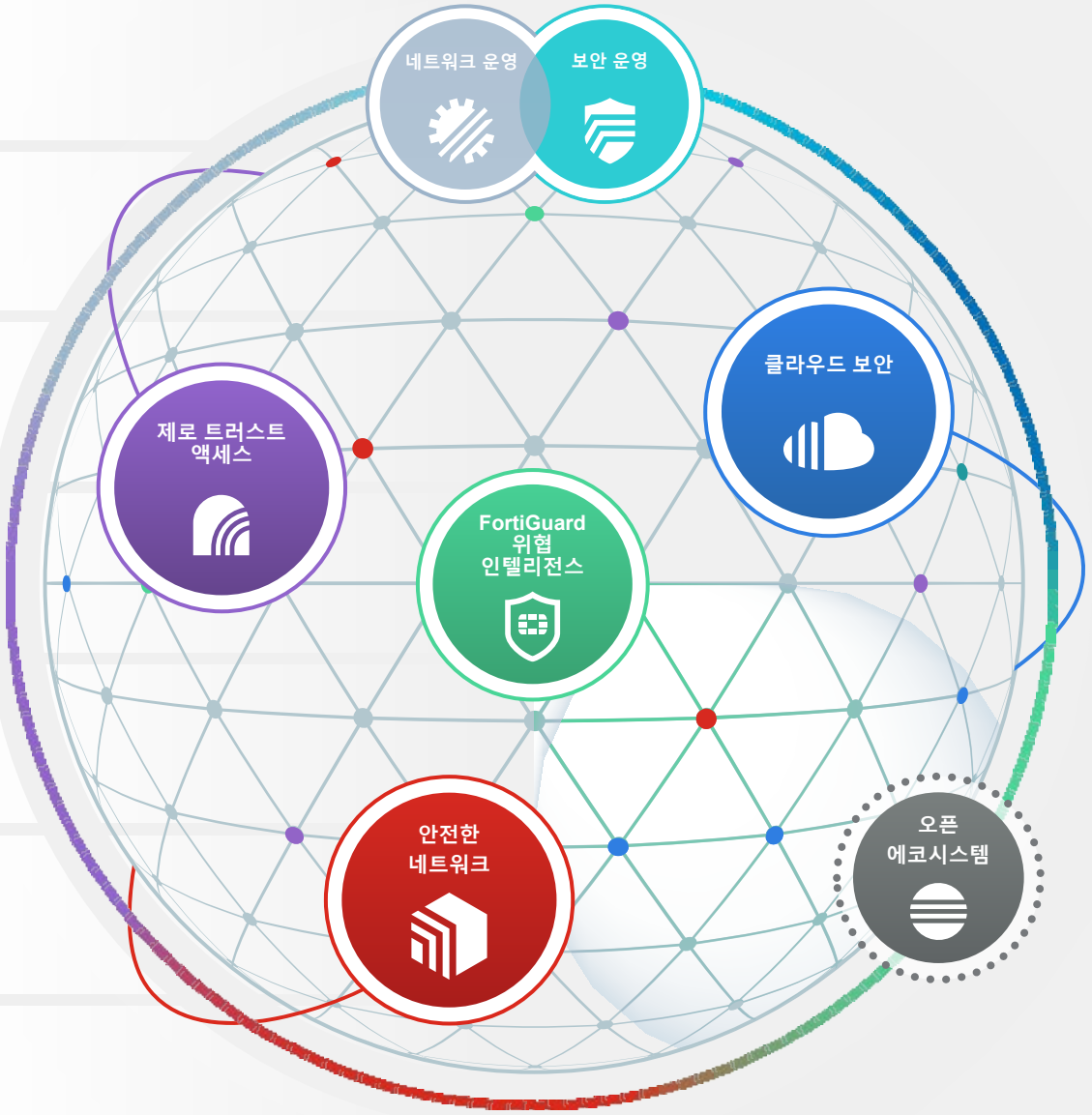
네트워크 운영
- 트래픽 로깅, 모니터링
- 네트워크 운영 센터 대시보드

보안 관제/운영
- MITRE ATT&CK for ICS 대시보드
- OT/ICS Deception / Lure
- 이·기종 이벤트 로깅, 모니터링

글로벌 위협 인텔리전스
- 엔드포인트 탐지 및 대응
- 글로벌 지능형 위협 보호
- Industrial Security 서비스
- OT 보안 진단 프로그램

오픈 에코시스템
- 패브릭 지원 파트너(with ICS Vendor)
- OT/ICS 보안 파트너(with Visibility Vendor)
- 국제 시스템 통합업체(with HCL, Infosys..)

전문 산업용 솔루션
- 산업환경 특화 하드웨어 제품(Rugged)
- 다양한 보안 제품의 가상 머신 제품
- SD-WAN기능과 3G/4G 무선 제품



어플라이언스
가상
호스팅
클라우드
Agent
컨테이너

SUMMARY

- Key 위협 요소 : 랜섬웨어 & 내부자 위협 with 비트코인(Money) 동인
- OT 보안 기본 요건 : 1) OT IDS, 2) 통합 로깅, 3) Remote Maintenance, 4) 사용자 정책 기반 NGFW
- OT 레퍼런스 모델 & 국제 규정, OT 보안 구축 사례 제시
- 스마트팩토리 아키텍처 모델 제시
- 산업 환경에서 단계별 OT보안 구축 전략(안) 제시
- 고객사를 위한 포티넷 OT보안 협업 제안 (5가지)


FORTINET