24. dubna 2024

Seyfor

If you want something to digitize,

Just sey it!

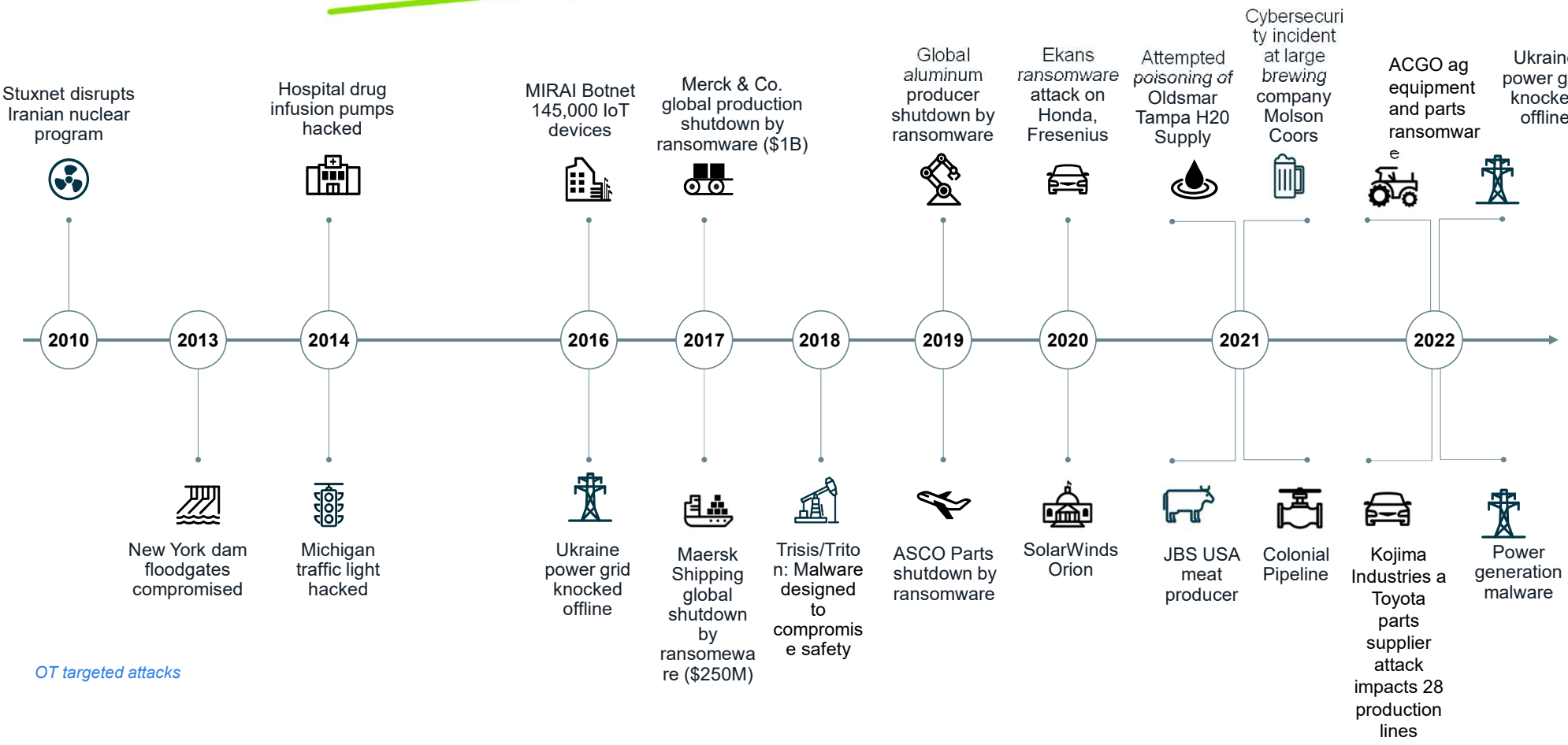
Fortinet Security Fabric

Komplexní ochrana OT sítí

Jan Nguyen, Cyber Security Consultant

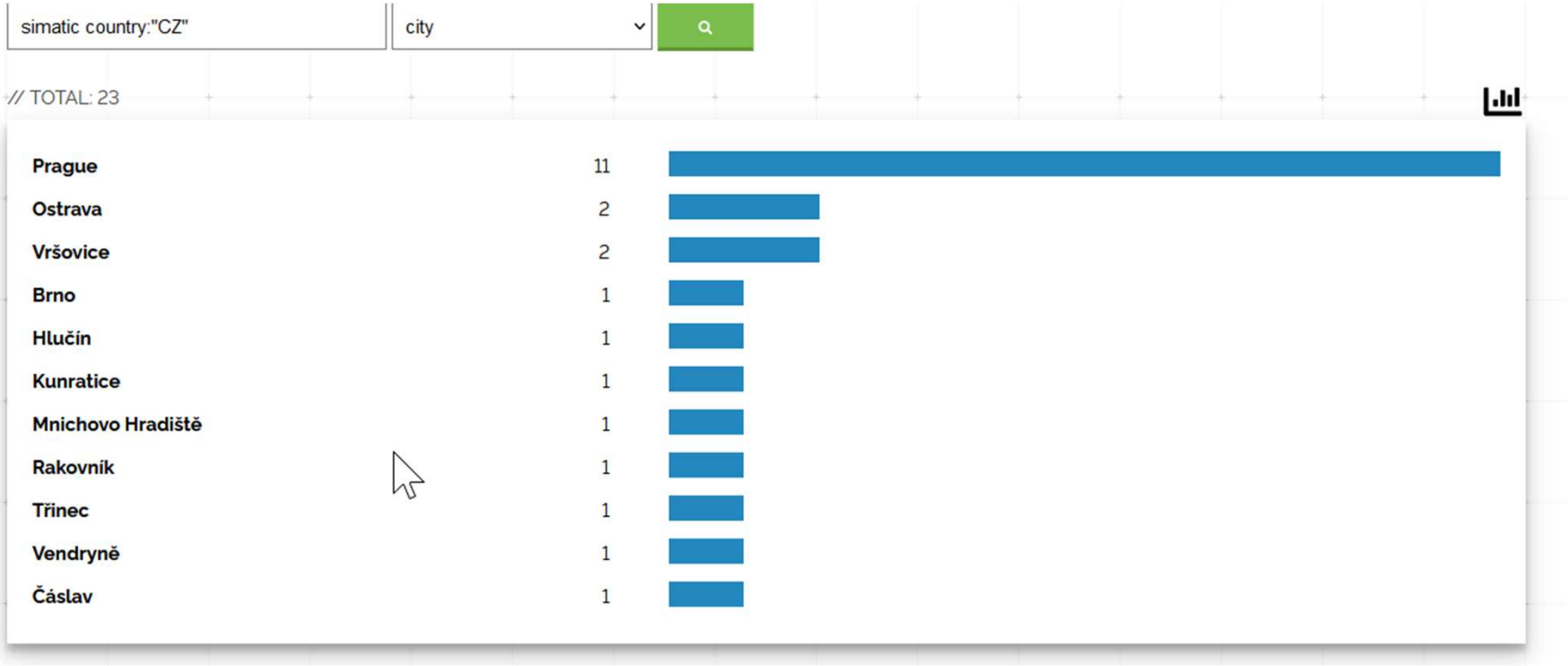
2024

Útoky na OT infrastrukturu



OT targeted attacks

Shodan.io



Shodan.io

TOTAL RESULTS

11

TOP PORTS

102	7
161	4

TOP ORGANIZATIONS

[redacted]	3
	2
	2
	1
	1

More...

View Report View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

[redacted]

Czechia, Prague

ICS

```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 315-2 PN/DP
Unknown (129): Boot Loader          A
Module: 6ES7 315-2EH14-0AB0  v.0.3
Basic Firmware: v.3.2.3
Module name: CPU 315-2PN/DP
Serial number of module: S C-B5TK54402011
Plant identification:
Basic Hardware...
```

[redacted]

Czechia, Prague

ICS

```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 314C-2 PN/DP
Unknown (129): Boot Loader          A
Module: 6ES7 314-6EH04-0AB0  v.0.2
Basic Firmware: v.3.3.6
Module name: CPU 314C-2 PN/DP
Serial number of module: S C-C6V833152012
Plant identification:
Basic Hardw...
```

[redacted]

Czechia, Prague

ICS

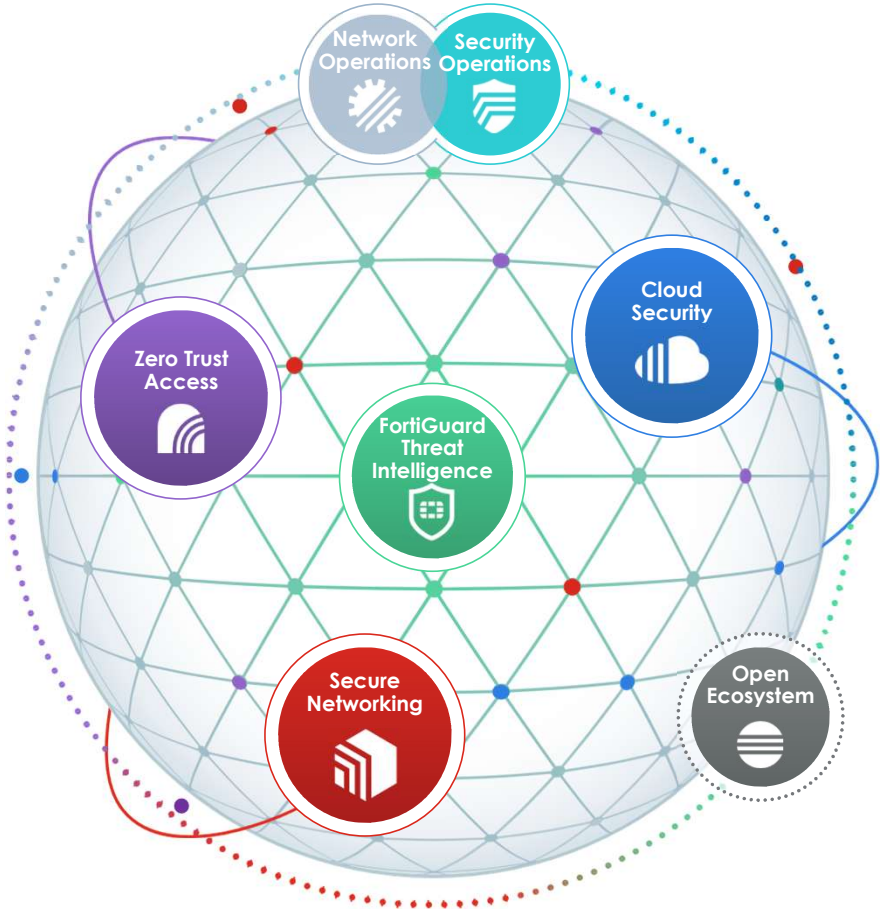
```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 315-2 PN/DP
Unknown (129): Boot Loader          A
Module: 6ES7 315-2EH13-0AB0  v.0.4
Basic Firmware: v.2.6.7
Module name: CPU 315-2 PN/DP
Serial number of module: S C-WNUC89052008
Plant identification:
Basic Hardwar...
```

Fortinet Security Fabric

Široký záběr
- Vhled a ochrana provozu od uživatele, přístupovou vrstvu, NGFW až po samotnou aplikaci či cloud

Integrace
- Možnost propojení s řadou produktů od společnosti Fortinet či jiných výrobců

Automatizace
- Zrychluje odezvu od detekce bezpečnostního incidentu po jeho mitigaci
- Využívá prvky umělé inteligence (AI) a strojového učení (ML)

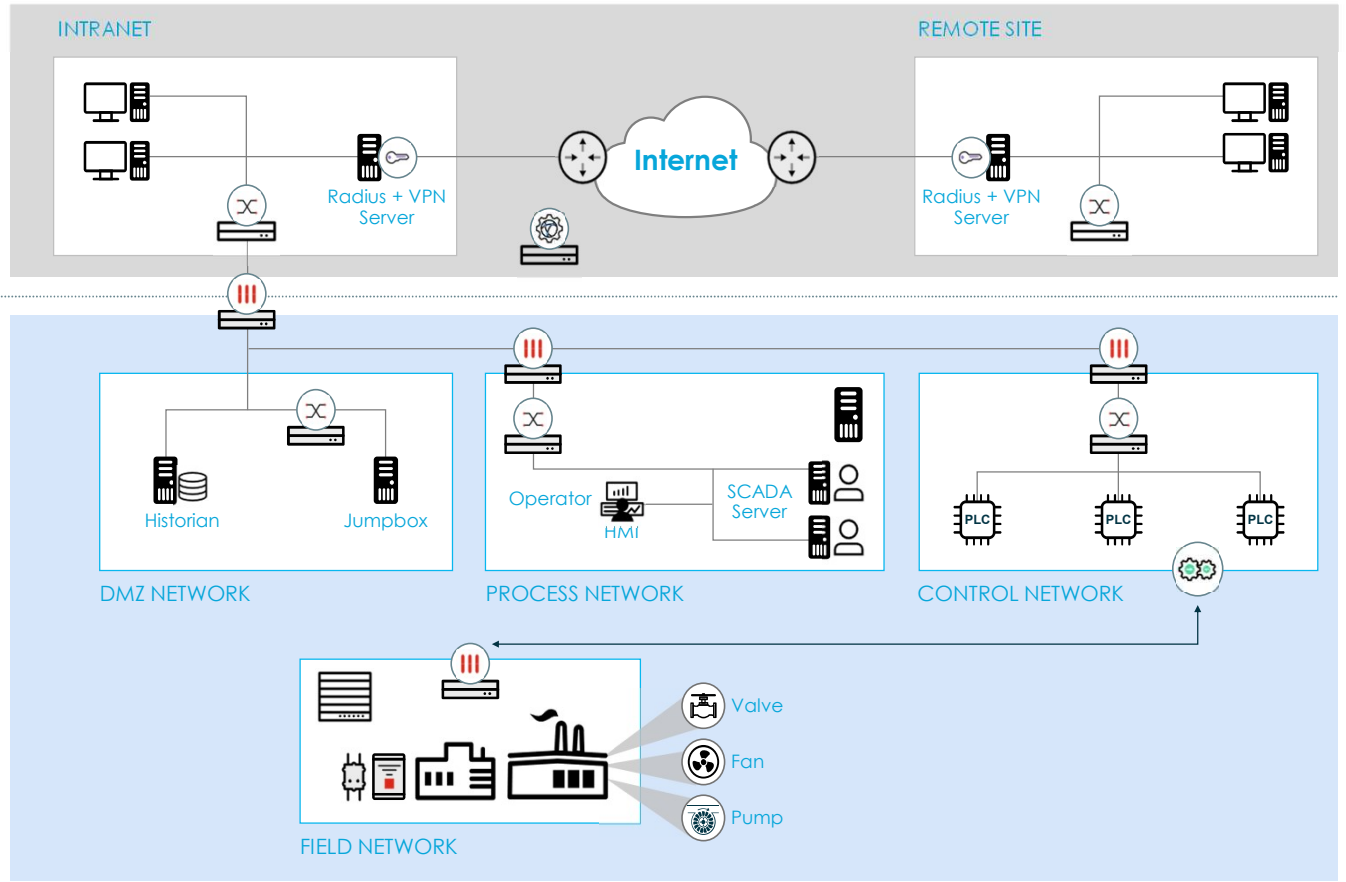


Fortinet Rugged Solution for ICS/OT

Fortinet's Security Fabric Protects OT&IT

Information Technology (IT)

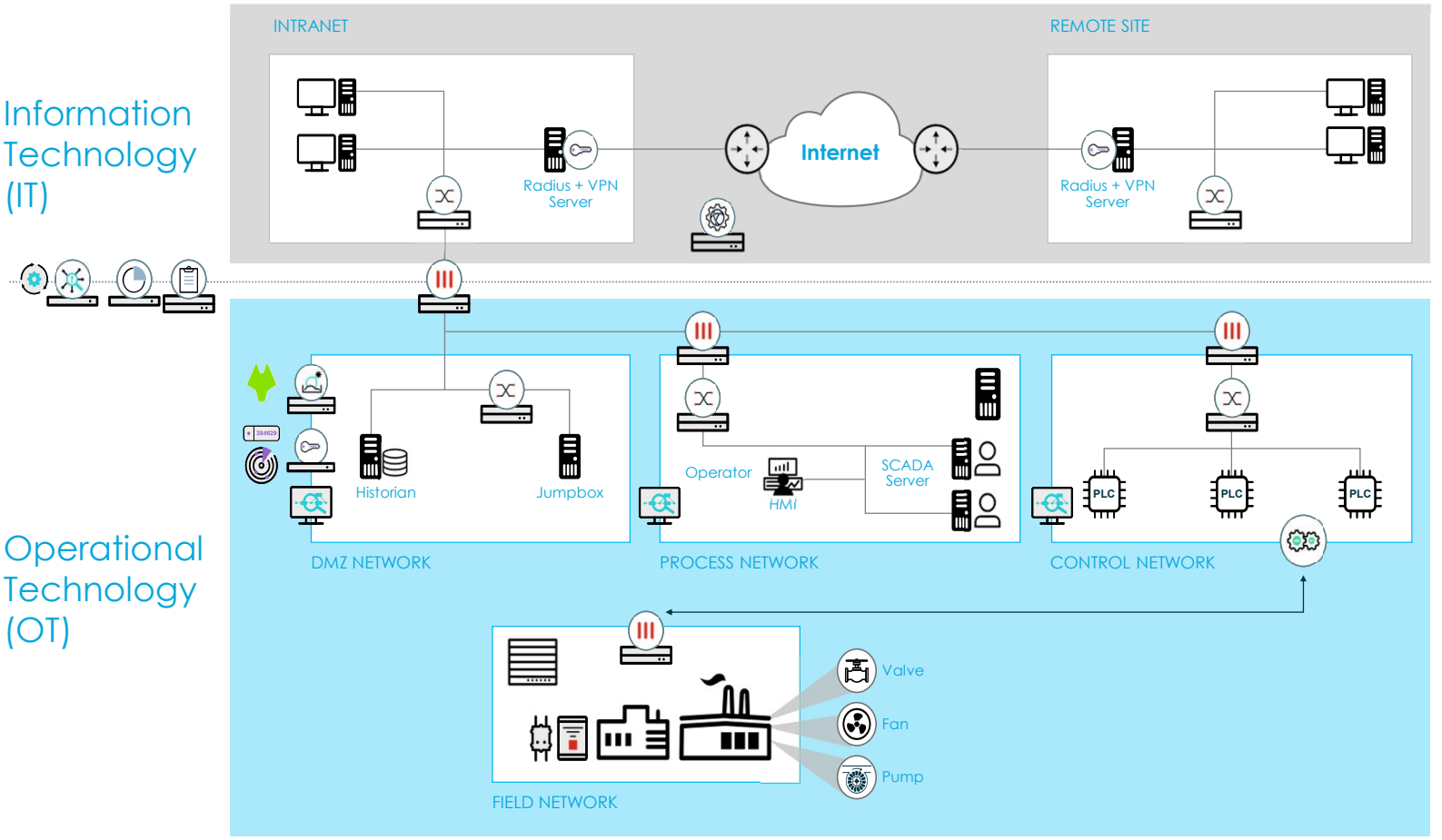
Operational Technology (OT)



Addressing Critical Use Cases Integrating OT & IT

Information Technology (IT)

Operational Technology (OT)



- Zones and Conduits
- Secure Remote Connectivity
- Deep OT Visibility
- Role-based Access Control
- Securing Critical End Point
- Centralize Security Management
- Advanced Persistent Threat

Securing Operational Technology

- Network Segmentation
- Network Microsegmentation
- Network Access Control
- Web Services Security
- Secure Remote Access
- Threat Protection
- Application Control
- Endpoint Security
- Honeypot
- Sandbox
- NOC/SOC

Cloud & External Zones

External Networks	Internet, Cloud, VPN

Major Enforcement Boundary

5.5 Information Technology (IT) Boundary

Business & Enterprise Zones — Levels

5 Enterprise Network	Corporate Systems & Networks
4 Business Plannng & Logistics	Site Systems & Networks

Major Enforcement Boundary

3.5 Operational Technology (OT) Boundary

Operations & Control Zones

3 Operations & Control	Simulation, Engineering, Test

Minor Enforcement Boundary

2.5Industrial Control System (ICS) Boundary

Process Control Zones

2 Area Supervisory Control	HMIs, Historians
1 Basic Control	PLCs, RTUs, IEDs
0 Process	Actuators, Sensors

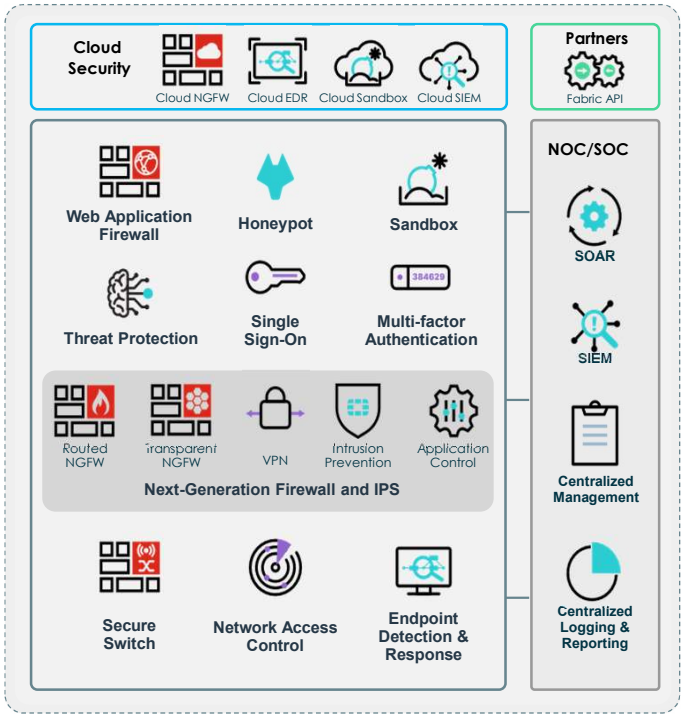
Major Enforcement Boundary

Air-gap / Safety Related Control Systems Boundary

Safety Zone

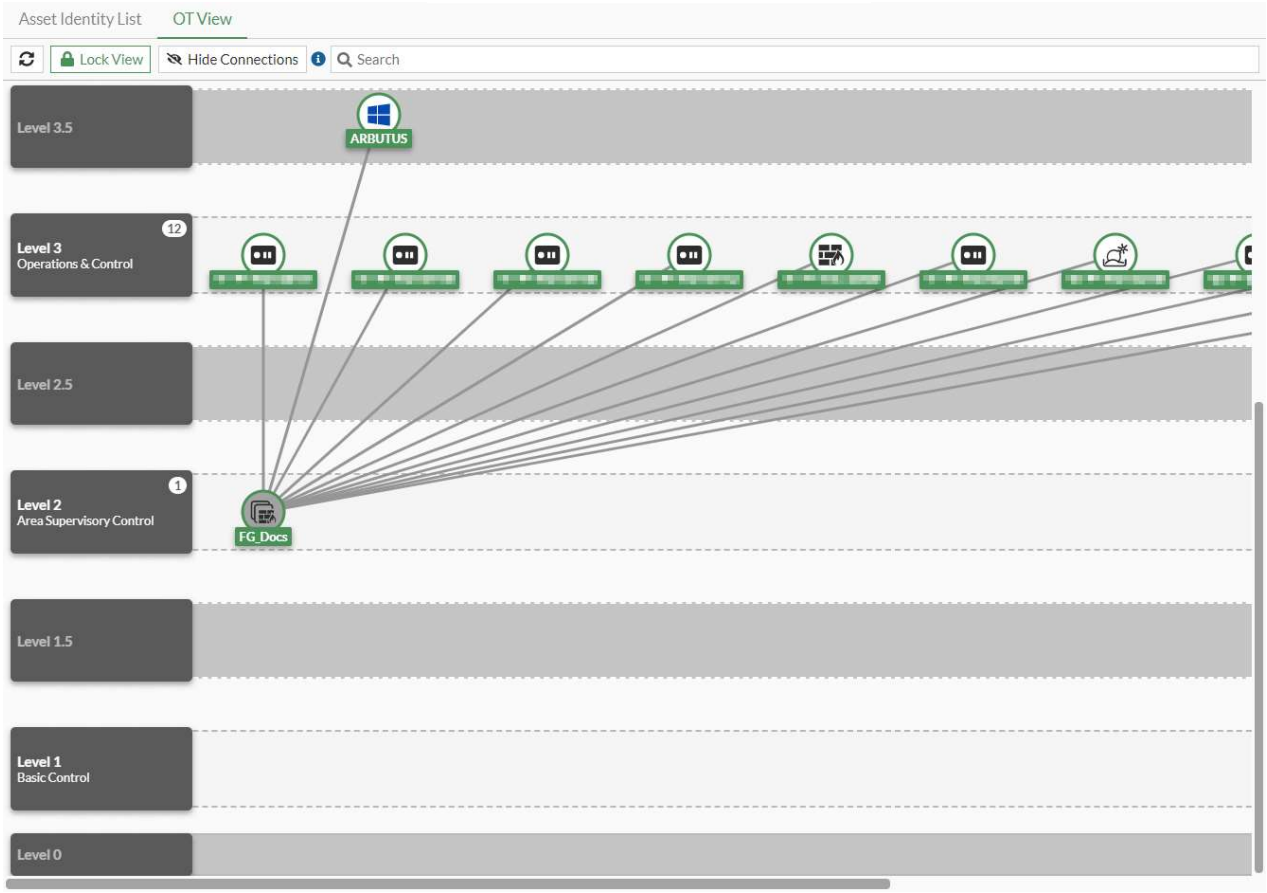
S Safety	Safety Instrumented System

Fortinet Security Fabric



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

FortiGate



FortiNAC

Healthcare and IoMT

MEDIGATE

asimily

Cynerio

CyberMDX
A FORESCOUT COMPANY

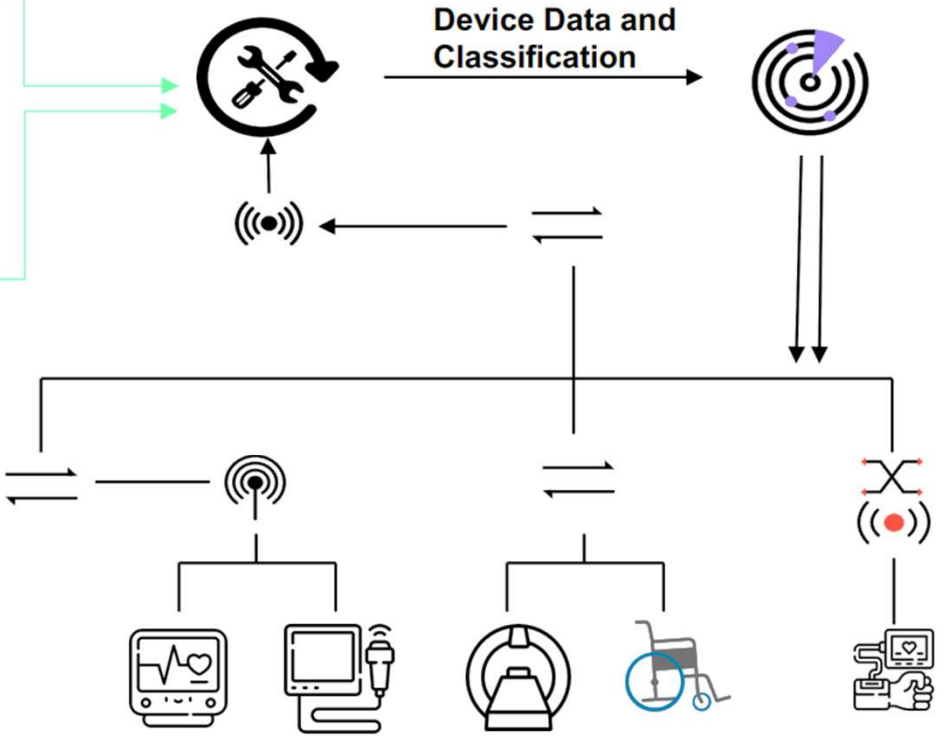
IoT/OT

CLAROTY

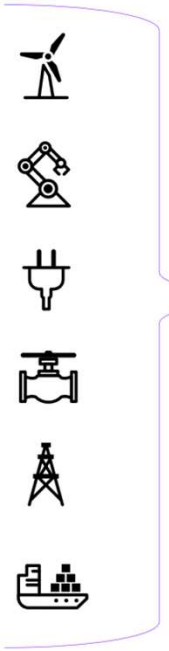
NOZOMI NETWORKS

DRAGOS

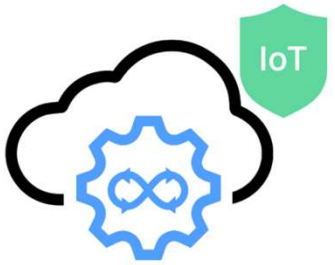
ordr



FortiNAC



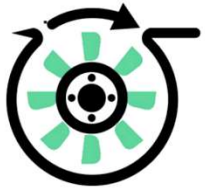
Enhanced Visibility and Control



FortiGuard IoT Detection Service

300M+
IoT devices

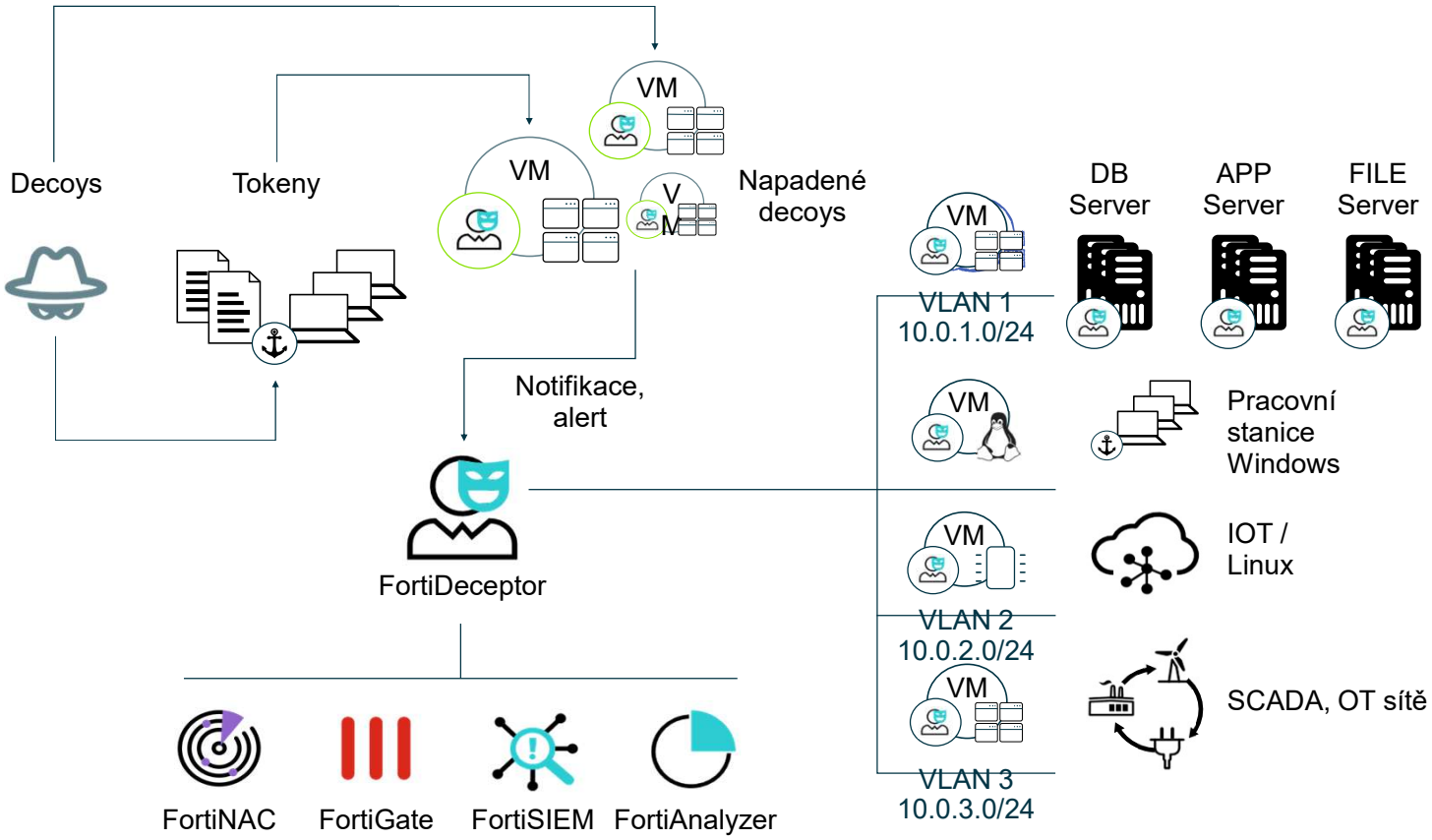
Granular classification of OT devices



FortiGuard Industrial Security Service

3000+
Industrial Protocols and applications supported

FortiDeceptor



FortiDeceptor

Local Windows Decoys
- Windows 7
- Windows 10

Custom Windows Decoys
- Windows 7
- Windows 10
- Windows Server 2016
- Windows Server 2019

Windows Lure / Token
- SMB
- RDP
- TCP Port Listener
- SQL (MS-Server)
- Cache Credentials
- Fake Network Connection
- SQL ODBC
- SAP Connector
- FTP
- HoneyDocs (Office & PDF & Excel)

VPN Decoys
- FortiOS

VPN Lures
- SSLVPN

Linux Decoy
- Ubuntu 16.0.4
- Ubuntu 18.0.4
- CentOS
- Outbreak Alerts

Linux Lure / Token
- ESXi
- ELK
- MySQL
- Tomcat

Cloud Decoys
- AWS
- AZURE
- GCP

IoT Decoys
- Cisco Router
- IP Camera
- Printers (HP,Lexmark,Brother)
- UPS

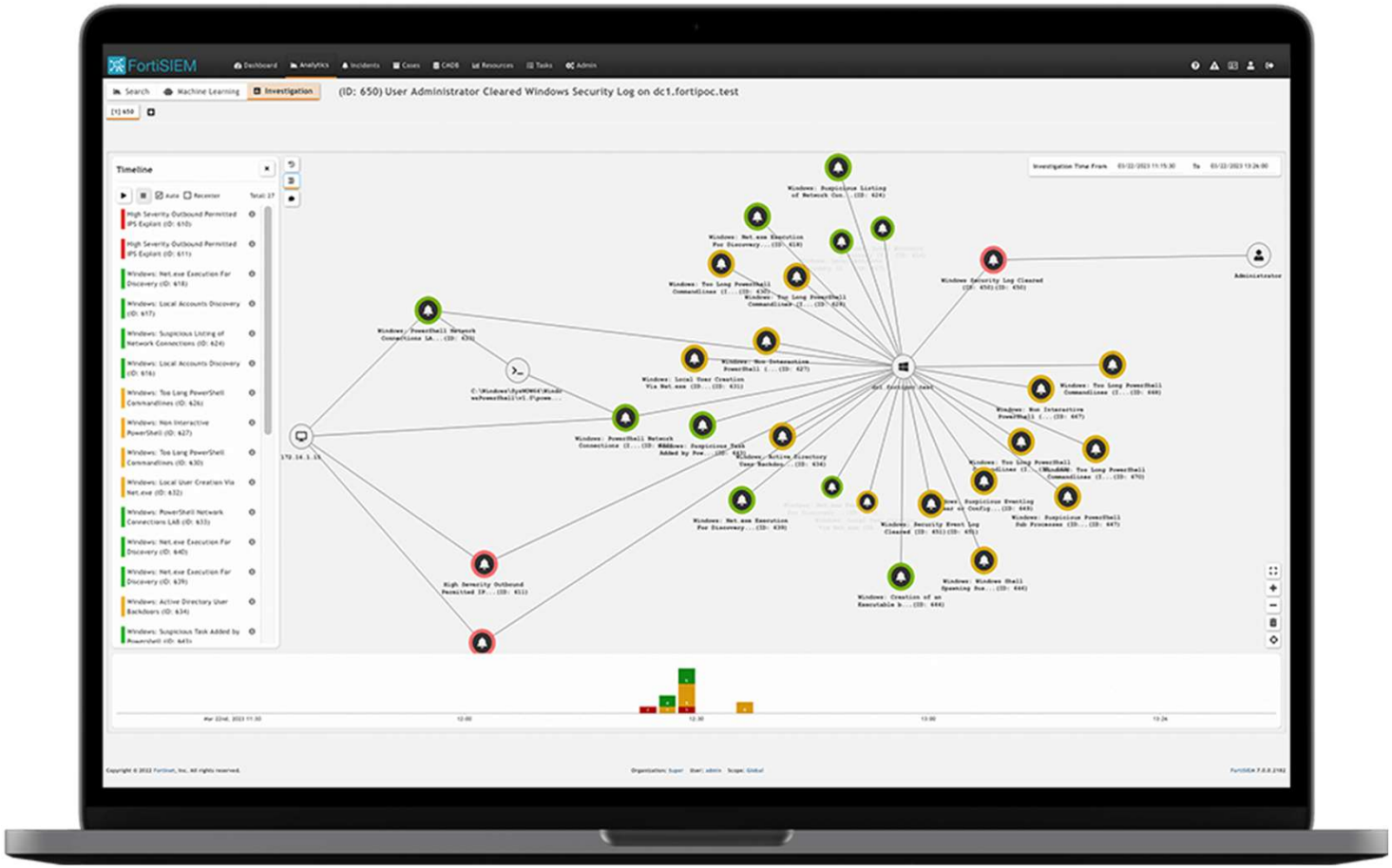
VoIP Decoys
- SIP
- XMPP
- MQTT

Application Decoys
- SAP
- ERP
- POS
- GIT

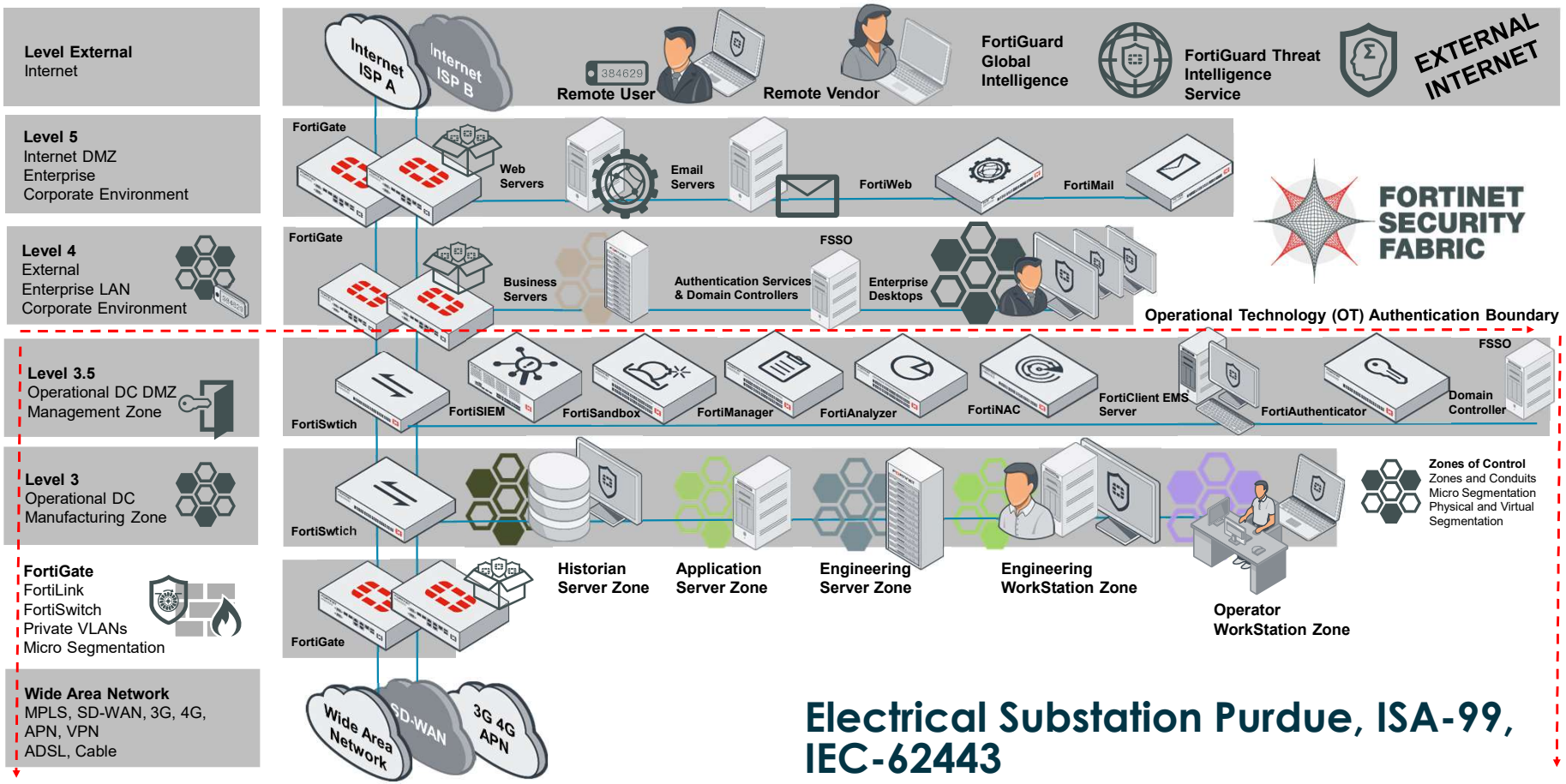
Medical Decoys
- PACS
- DICOM
- Infusion Pump

SCADA Decoys
- HTTP
- FTP
- TFTP
- MODBUS
- S7COMM (Siemens)
- BACNET
- IPMI
- TRICONEX (Schneider)
- GUARDIAN-AST
- IEC 60870-5-104
- EtherNet/IP (Rockwell)
- DNP3
- SRTP (GE IP Series 90-30)
- MOXA (NPORT)
- SCADABR (MGMT)

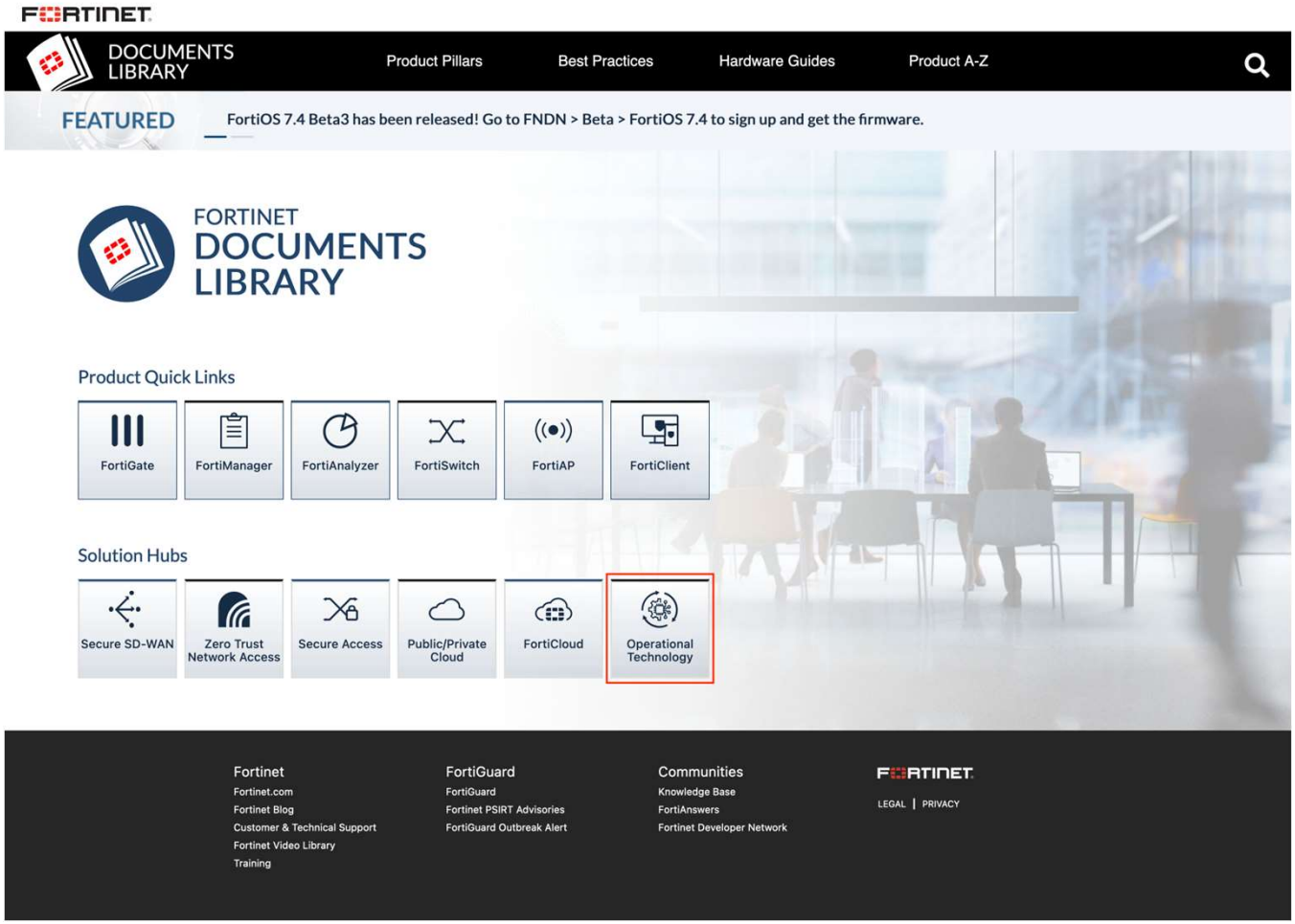
FortiSIEM a FortiSOAR



Applying Fortinet's Reference Architecture to Purdue



OT Security Solution Hub



Thank you for your attention.

Seyfor