IoT Security

IoT/OT Security Conference
7. März 2023 in Cham

iCB Infosec Community Builder

FORTINET

Industrial Security Fabric für Operational Technology (OT)

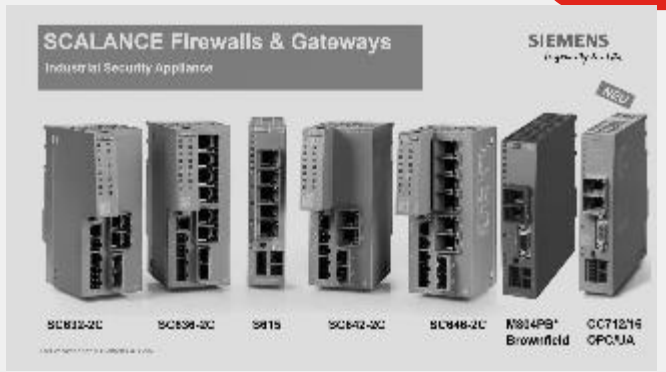
Mit intelligenter Security wird Safety & Availability durch Sichtbarkeit & Segmentierung sichergestellt

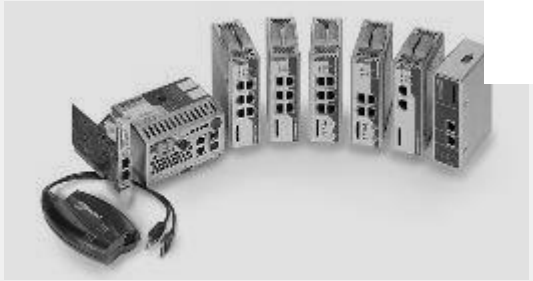
Mirco Kloss
Manager Business Development | Operational Technology D-A-CH

Sichtbarkeit
Segmentierung
Sicherer Zugang

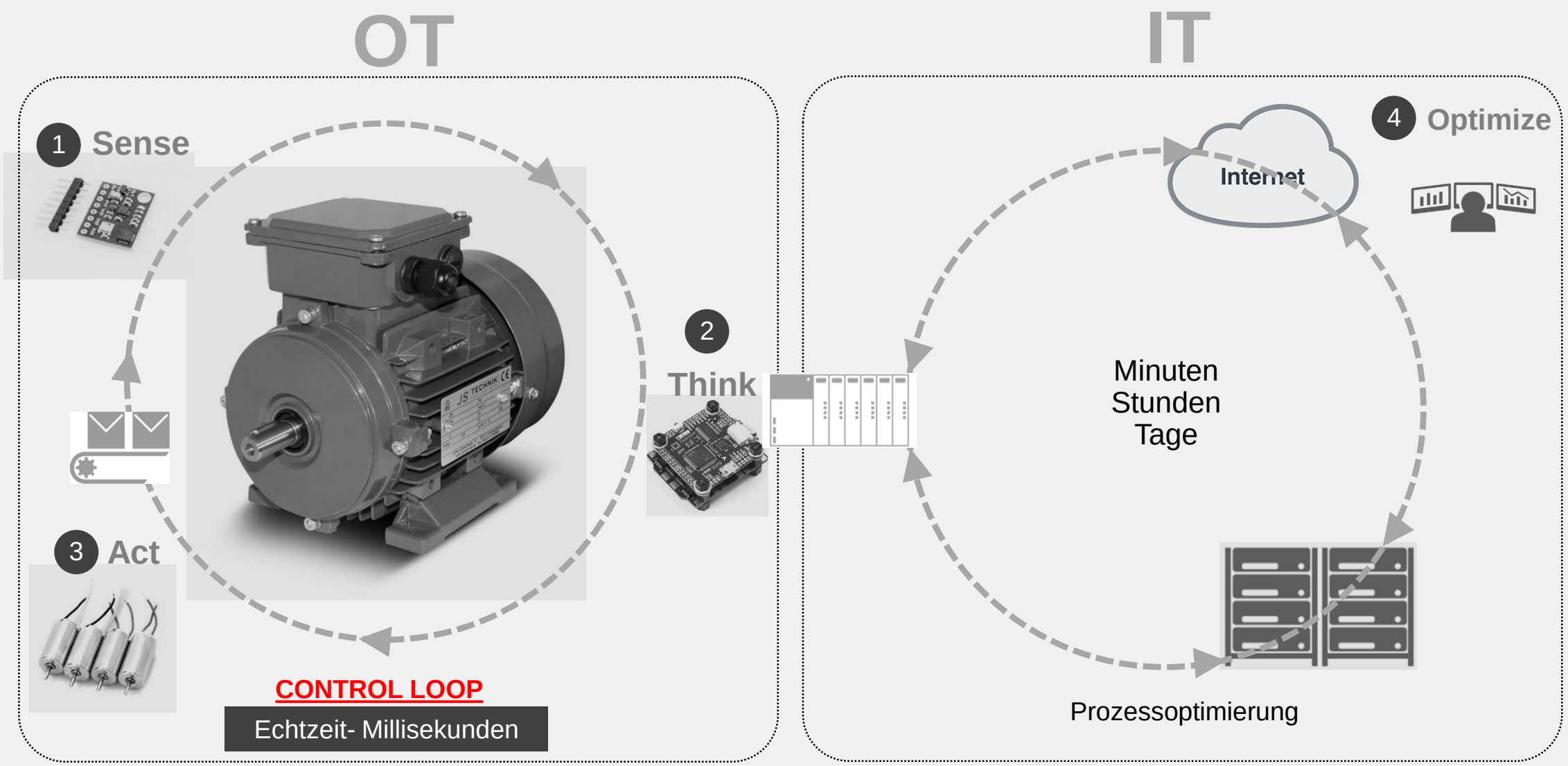
Einleitung

IT vs OT





OT und IT – unterschiedliche Welten vereinen sich



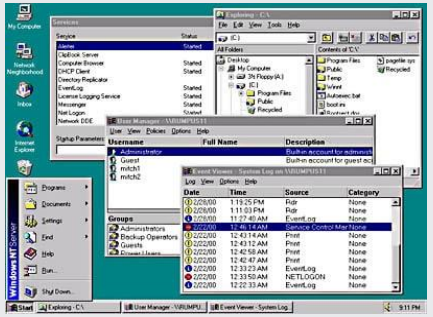
Security Herausforderungen

SAFETY IS PARAMOUNT

Da Safety für ICS-Kunden von größter Bedeutung ist, betrachtet man die zielgerichtete polymorphe Malware Triton seit 2018 mit größter Sorge

SECURITY NOT DESIGNED

Security ist für ICS Endpoints, Controller und deren Kommunikations-protokolle nicht vorgesehen



OUTDATED LEGACY OPERATING SYSTEMS

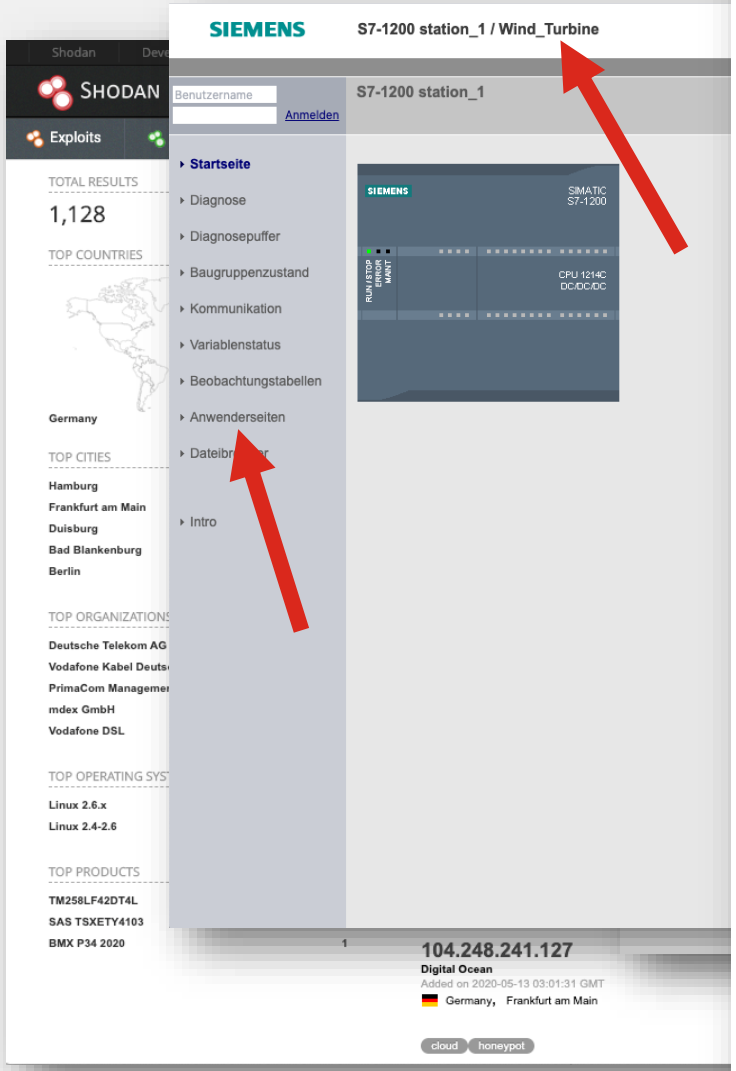
ICS Geräte führen sehr häufig veraltete Legacy Betriebssysteme aus

VISIBILITY

fehlende Sicht

mangelnde Kontrolle

Shodan



WIND TURBINE STATUS AND CONTROL

Power Meter		
Ua = 239.9 V	**Ub** = 239.6 V	**Uc** = 238.7 V
Ia = 58.9 A	**Ib** = 54.3 A	**Ic** = 60.5 A
P = 39.8947 kW		
S = 40.4147 kVA		
Q = -6.4619 kVAr		
PF = 0.99		
ImpWh = 41907.41 kWh		
ExpWh = 633.256 kWh		
ImpVArh = 647.736 kVArh		
ExpVArh = 40804.05 kVArh		

Turbine Parameters	
Wind Speed = 8.19	**Wind Direction** = 176
Motor RPM = 1001.77	**Main Shaft** = 45.22
Motor Temp = 13	
Bearing Temp = 37.7	
Brake Temp = 30.2	
Ambient Temp = 8	
Multiplicator Temp = 31.2	

Faults

Step = 5

Fault Code = 0 RESET

Turbine

START

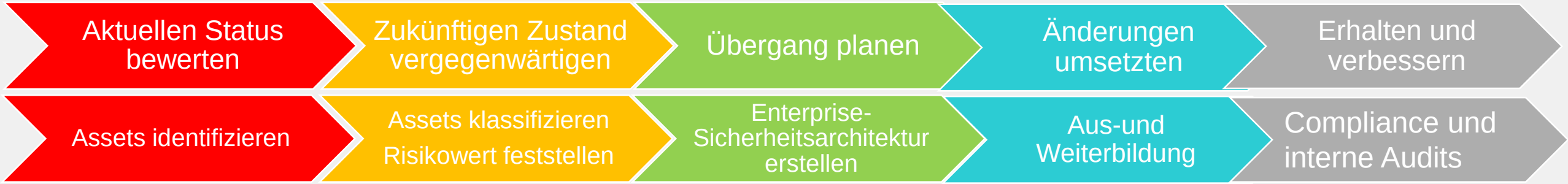
STOP START

MAN START

Rotation

CCW STOP CW

Cyber-Physische-Sicherheit



Sichtbarkeit erhalten

Assetes erkennen, wo sie sich befinden, was sie tun. Dieser Schritt ist entscheidend, um zu ermitteln, was zu schützen ist und welches Risiko mit den Assets verbunden ist, um eine effektive Sicherheitslage zu gewährleisten

Risiken verstehen

Risiken verstehen, die mit den Assets verbunden sind, was dies bedeutet, und um einen Angriff zu verhindern

Architektur bereitstellen

Beginnen mit bekannten Framework, z.B. IEC-62443. Anpassen des Sicherheits-Blueprint an die Umgebung.Implementieren, verwalten und unterstützen der Lösung, um eine kontinuierliche Verbesserung, Berichterstellung und Überprüfung sicherzustellen

NIS Directive 2.0 (EC 2016/1148)

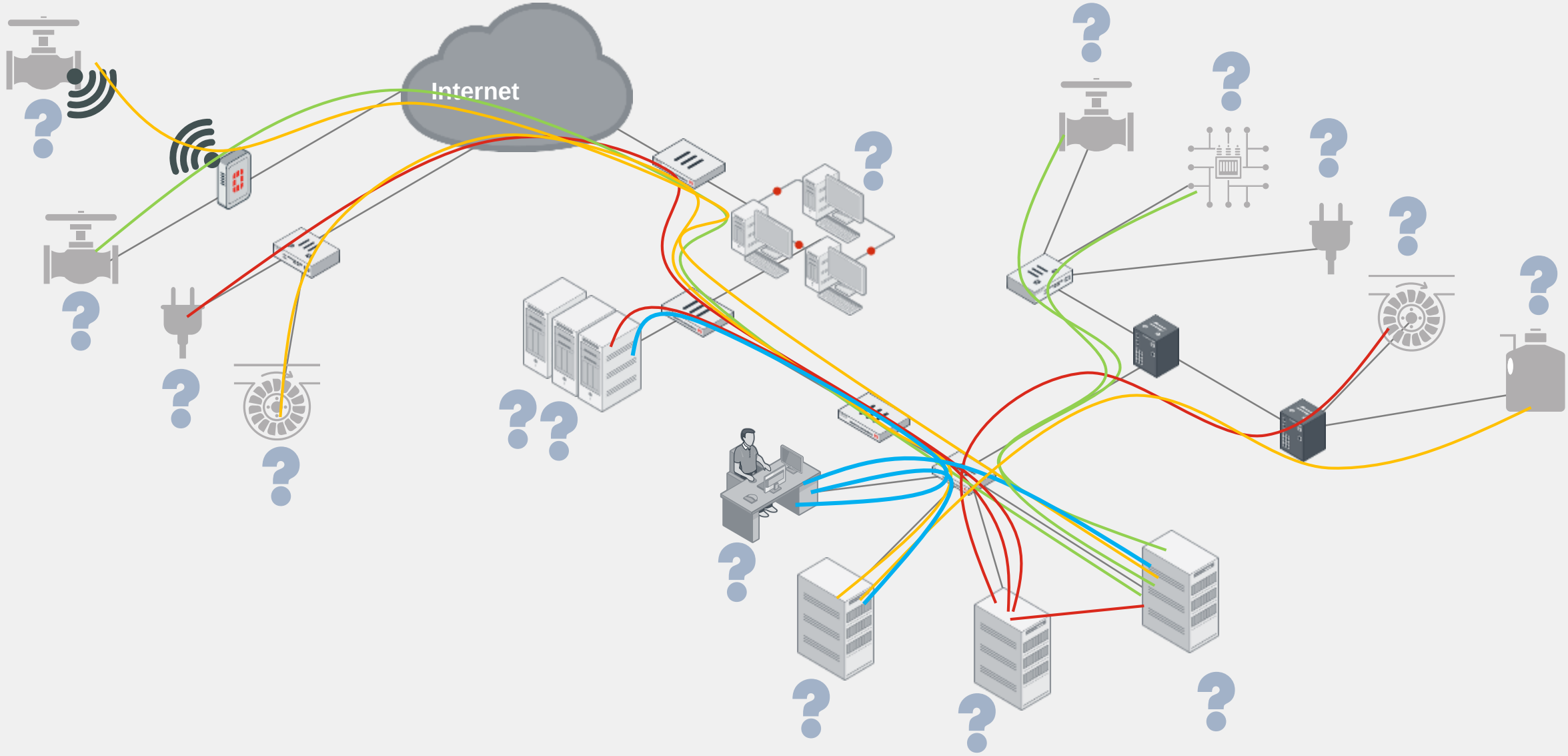
EU NIS2 ist der europäische Rahmen für Betreiber Kritischer Infrastrukturen und legt Cyber Security Mindeststandards in der EU fest. NIS2 (EU 2022/2555) erweitert die Betroffenheit und Pflichten deutlich – ab 2024 müssen viele Unternehmen in 18 Sektoren ab 50 Mitarbeitern und 10 Mio. EUR Umsatz Cyber Security umsetzen.

Kategorie	Sektoren
Essential	Energie, Transport, Banken, Finanzmärkte, Gesundheit, Trinkwasser, Abwasser, Digitale Infrastruktur, ICT Service Management, Öffentliche Verwaltung, Raumfahrt
Important	Post und Kurier, Abfallwirtschaft, Chemikalien, Ernährung, Industrie, Digitale Dienste, Forschung

Quellen: https://www.openkritis.de/it-sicherheitsgesetz/index.html
https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html

OT Security Best Practices

Schritt 1: Sichtbarkeit



OT Cyber Threat Assessment

FORTINET

OT Overview

Report Date: June 2, 2019 13:19
Data Range: 2019-06-02 00:00 2019-06-02 13:19 CEST (FAZ local)

Table of Contents

FG140D3G13801859
FGR30D-104-Demo
FGR90D-OTDemo

Executive Summary

This report provides findings of application risk analysis that Fortinet conducted for your organization. Fortinet next generation firewall is used for the analysis. This document begins with a summary of these findings, followed by details of the applications, types of content found and closes with a set of recommended actions.

Below is a summary of the critical and high risk security events detected:
Application Visibility & Control

No matching log data for this report

Threats Detection & Prevention

Critical & High Intrusion Attack	43

Application Categories

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application management. For application category details, see: http://www.fortiguard.com/appcontrol

The following section shows the application category breakdown of all the applications on the network, sorted by bandwidth. Thi information helps network administrators to identify where the bandwidth is used, and how many applications use it. Armed wit this information, the administrators can effectively prioritize the applications based on the business needs: for example, allow business applications but traffic shape the applications for personal use.

Industrial	92.68%
Email	6.59%
Web.Client	0.68%
Network.Service	0.05%

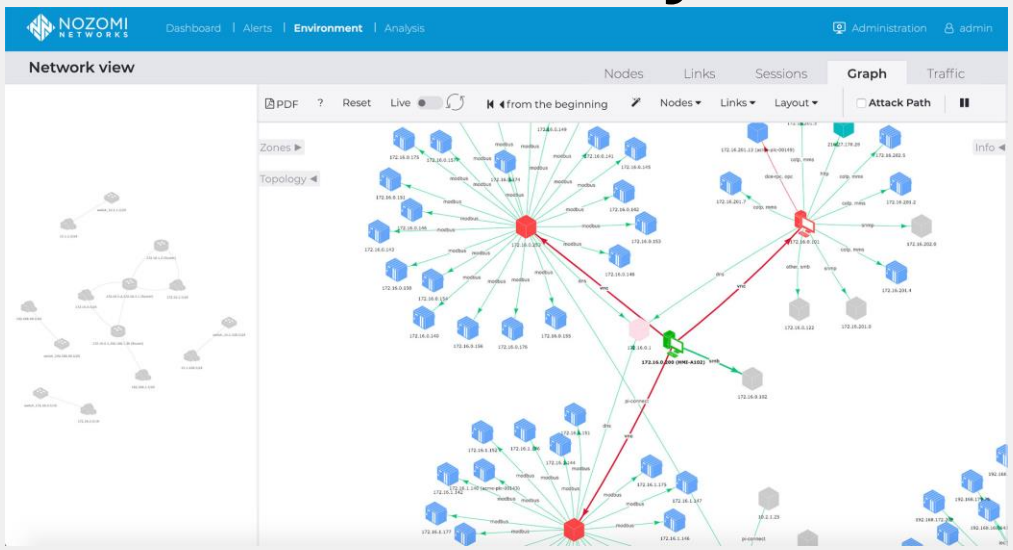
Figure 5: Top 10 application categories by bandwidth usage

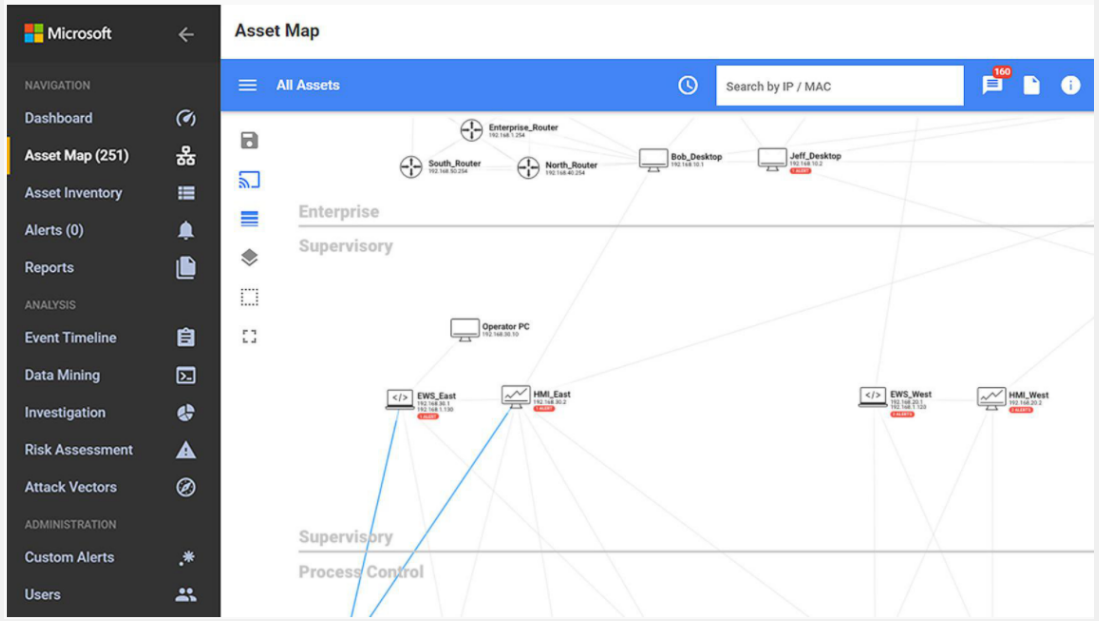
FORTINET

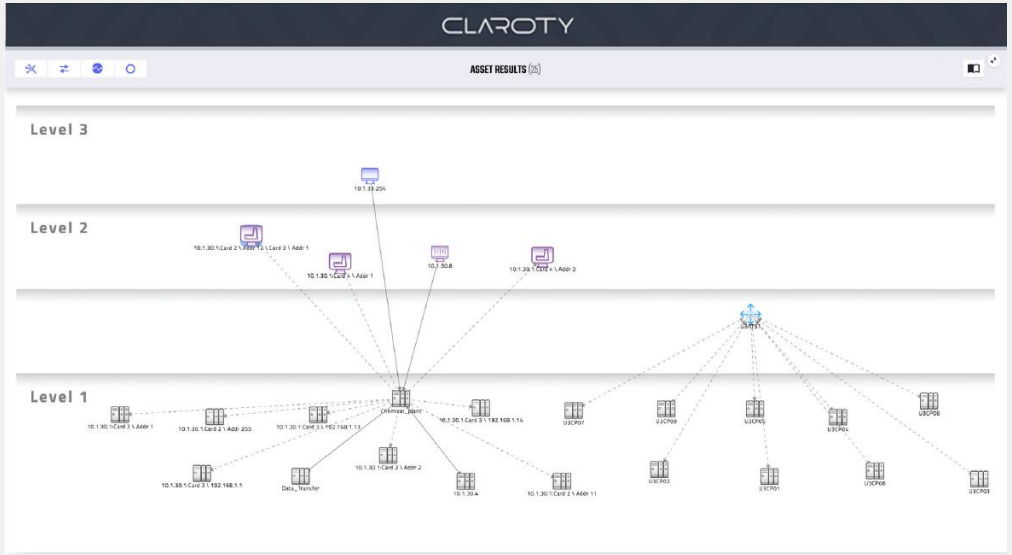
#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	2	PROFINET.IO_DeviceInterface	Industrial	Client-Server	5	428.43 KB	1,899
2	2	BACnet_Time.Synchronization	Industrial	Client-Server	5	266.07 KB	9
3	2	BACnet_Atomic.WriteFile	Industrial	Client-Server	5	177.78 KB	6
4	2	BACnet_Who.Is	Industrial	Client-Server	4	149.60 KB	5
5	2	EtherNet.IP_Unregister.Session	Industrial	Client-Server	5	134.34 KB	800
6	3	SMTP	Email	Network-Protocol	5	132.49 KB	8
7	2	OPC.UA_Get.Endpoints.Request	Industrial	Client-Server	5	119.90 KB	824
8	2	IEC.61850_GetAllDataValues	Industrial	Client-Server	5	113.47 KB	421
9	2	IEC.61850	Industrial	Client-Server	5	109.43 KB	406
10	2	OPC.UA_Close.Secure.ChannelRequest	Industrial	Client-Server	5	92.97 KB	68
11	2	BACnet_Who.Has	Industrial	Client-Server	2	90.26 KB	3
12	2	BACnet_Atomic.ReadFile	Industrial	Client-Server	2	60.04 KB	2
13	2	DNP3_Read	Industrial	Client-Server	5	36.55 KB	1,425
14	2	Modbus_Write.Multiple.Registers	Industrial	Client-Server	5	26.66 KB	260
15	2	DNP3_Write	Industrial	Client-Server	5	26.43 KB	660
16	2	DNP3	Industrial	Client-Server	5	10.57 KB	984
17	3	HTTP.BROWSER_IE	Web.Client	Browser-Based	5	6.62 KB	34
18	2	Modbus_Write.Single.Coil	Industrial	Client-Server	5	6.30 KB	496
19	2	Modbus_Read.FIFO.Queue	Industrial	Client-Server	5	5.37 KB	500
20	2	IEC.60870.5.104_Control.Functions.TESTFR.ACT	Industrial	Client-Server	5	3.62 KB	529
21	3	HTTP.BROWSER	Web.Client	Browser-Based	4	3.60 KB	7
22	2	IEC.60870.5.104_Control.Functions.STOPDT.CON	Industrial	Client-Server	5	3.27 KB	478
23	2	Google.Bot	Web.Client	Client-Server	1	1.28 KB	1
24	2	Modbus_Read.Coils	Industrial	Client-Server	2	1.24 KB	2
25	2	File.Upload.HTTP	Network.Service	Browser-Based	1	961 B	1
26	2	HTTP.BROWSER_Safari	Web.Client	Browser-Based	2	865 B	2
27	2	HTTP.BROWSER_Opera	Web.Client	Browser-Based	1	539 B	1
28	2	HTTP.BROWSER_Firefox	Web.Client	Browser-Based	1	452 B	1
29	2	HTTP.BROWSER_Chrome	Web.Client	Browser-Based	1	264 B	1

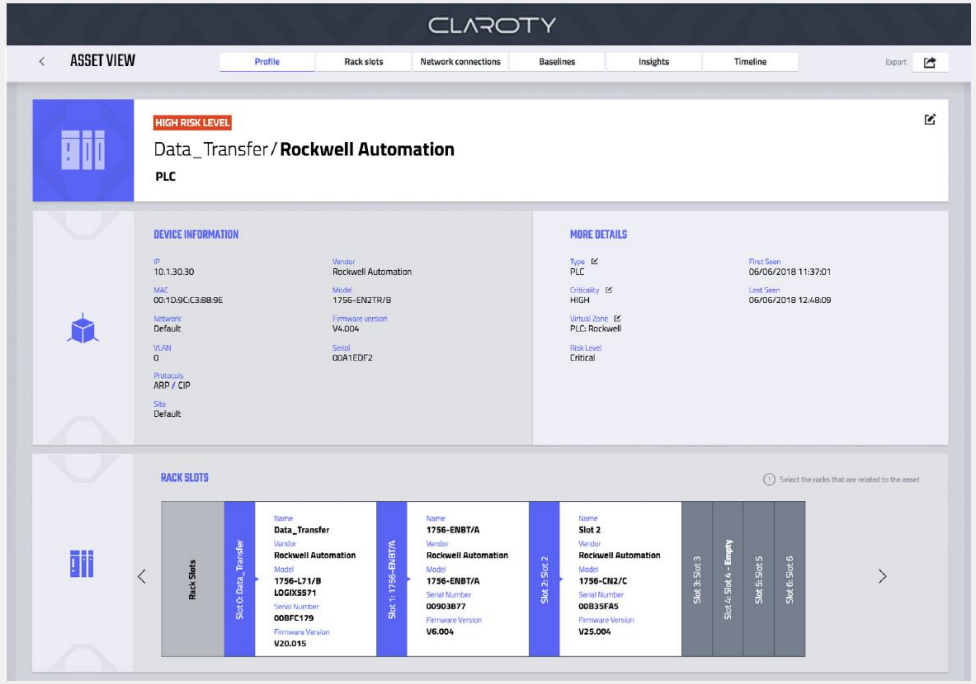
Figure 4: Top applications that are consuming the most bandwidth, sorted by category and technology

Asset Inventory (examples)

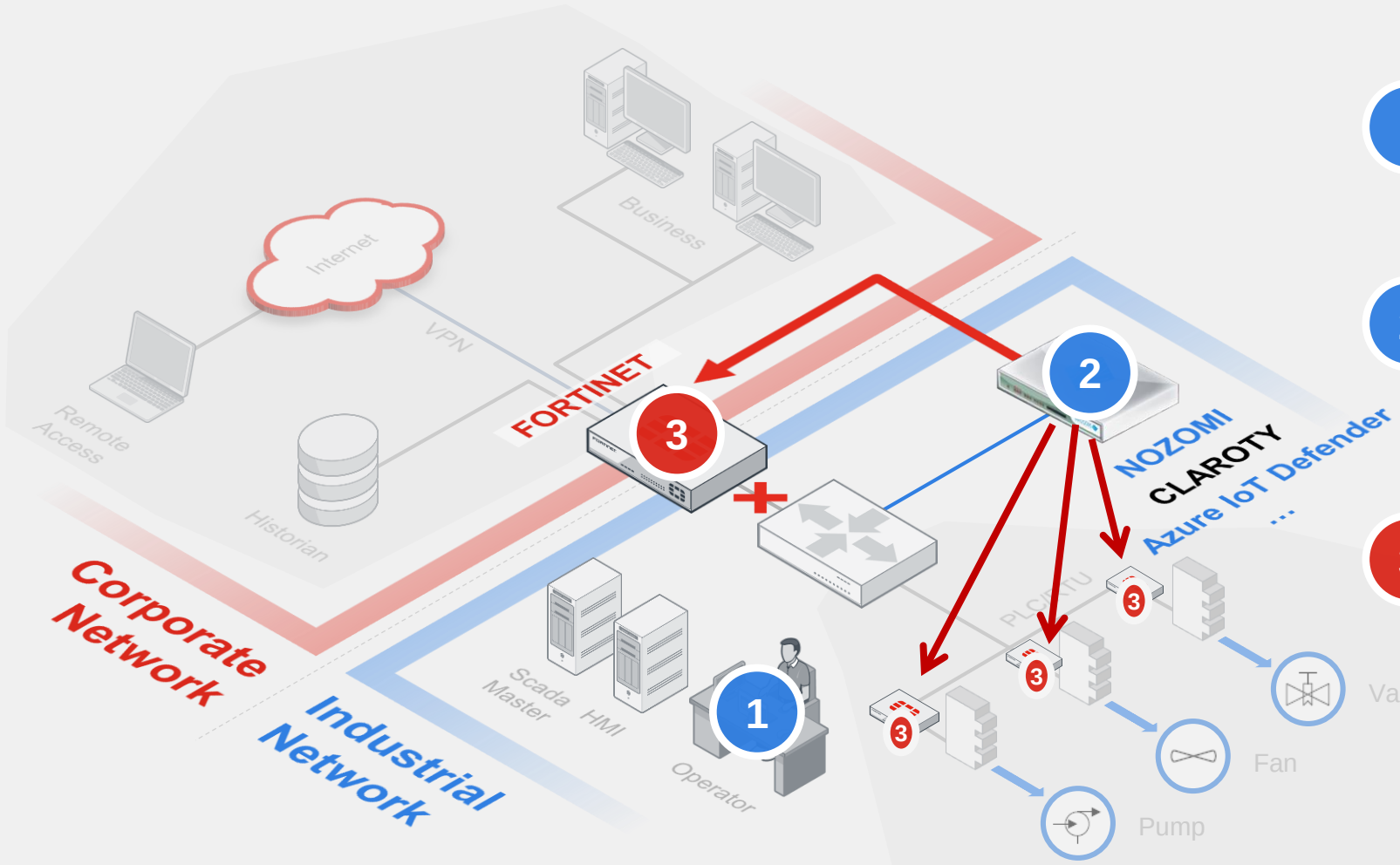








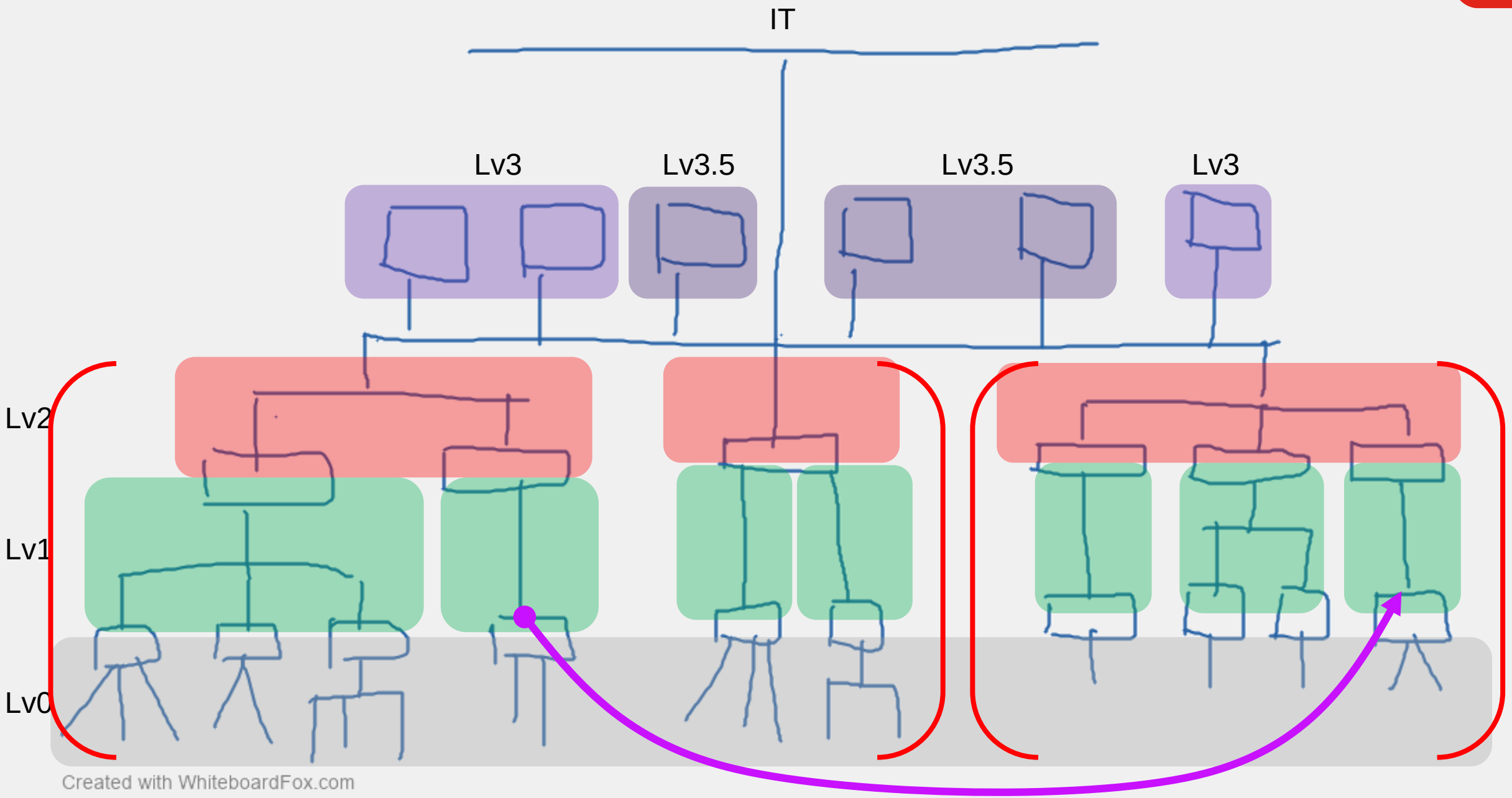
Responding to Threats in Real Time



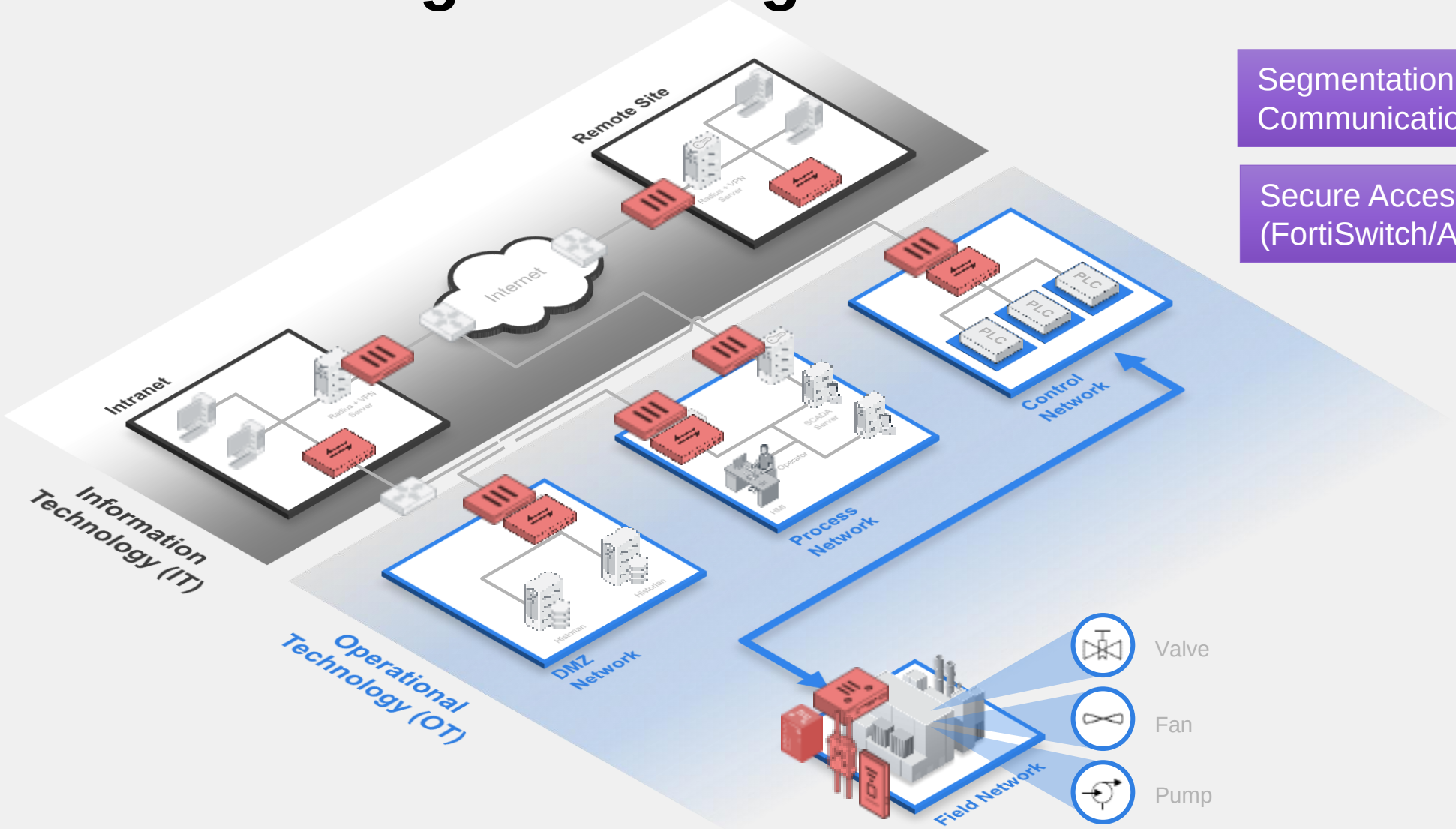
1 Monitor
A threat is detected and an alert is generated

2 Detect
User-defined policies are examined and the appropriate corresponding action is triggered

3 Protect
FortiGate responds according to the user-configured action (Node Blocking, Link Blocking, or Kill Session) in order to mitigate the issue

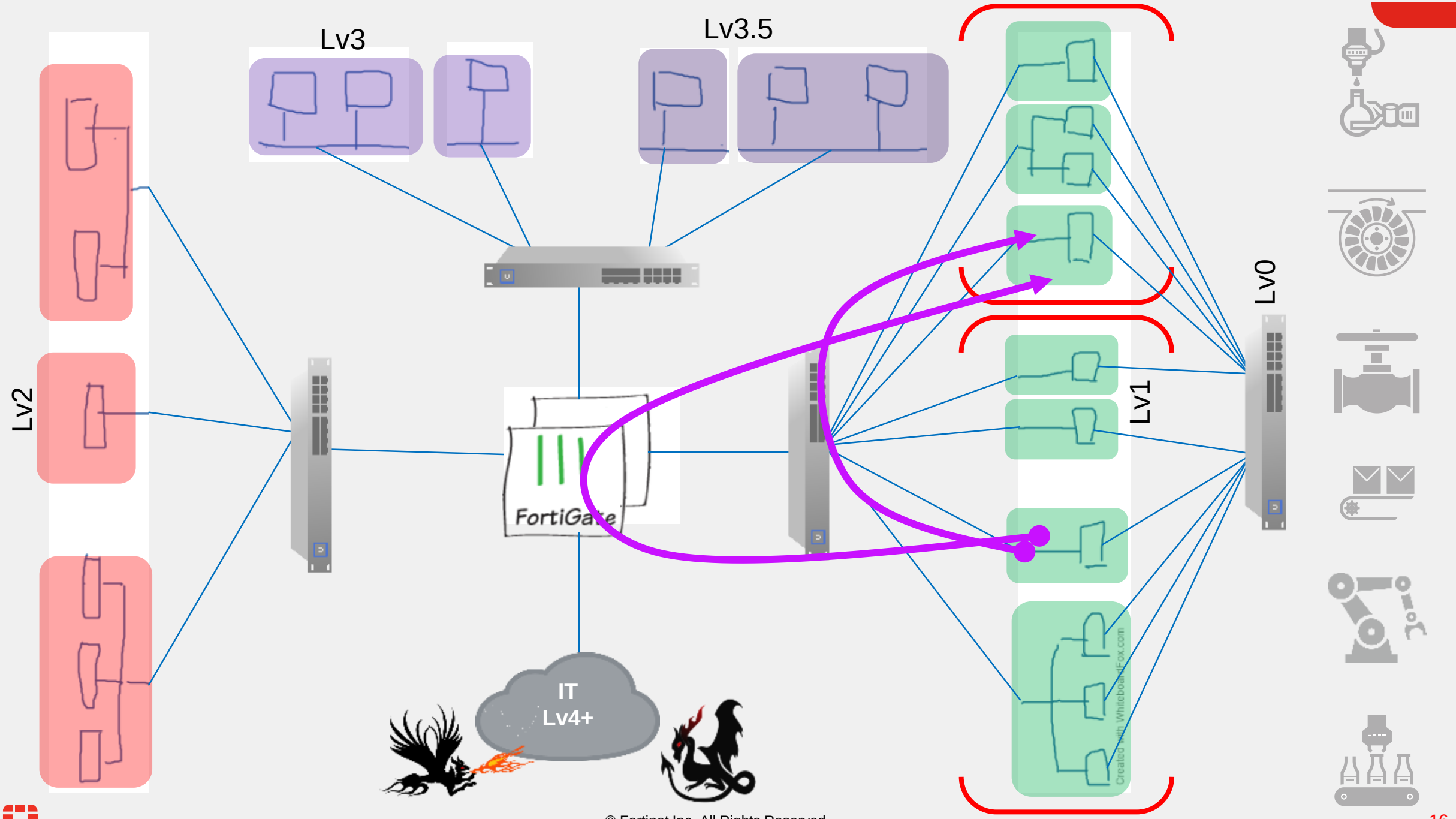


Schritt 2: Segmentierung

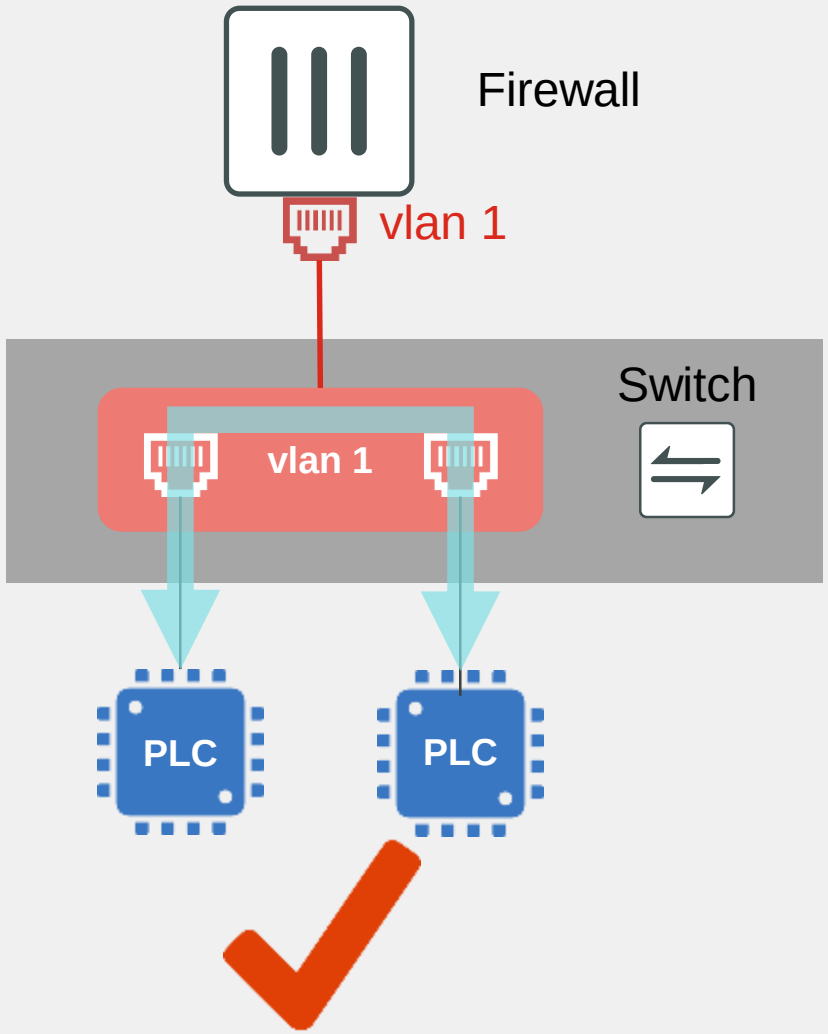


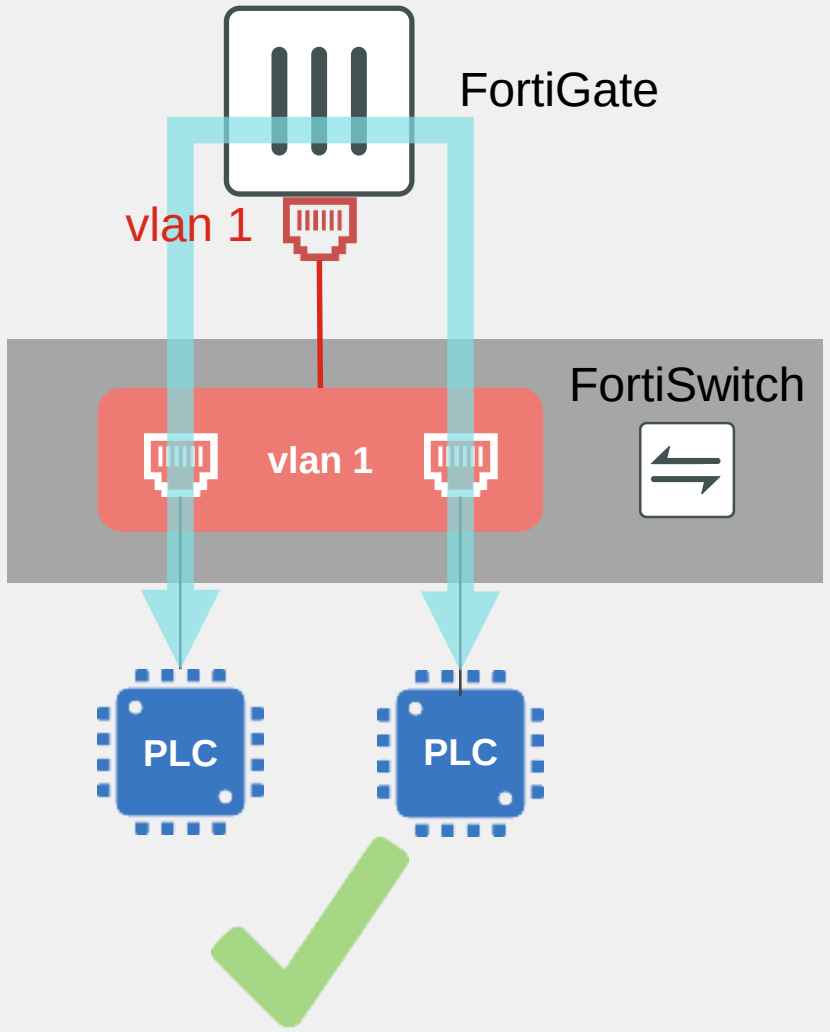
Segmentation / Encrypted Communication / IDS/IPS (FortiGate)

Secure Access (FortiSwitch/AP/Extender/NAC)

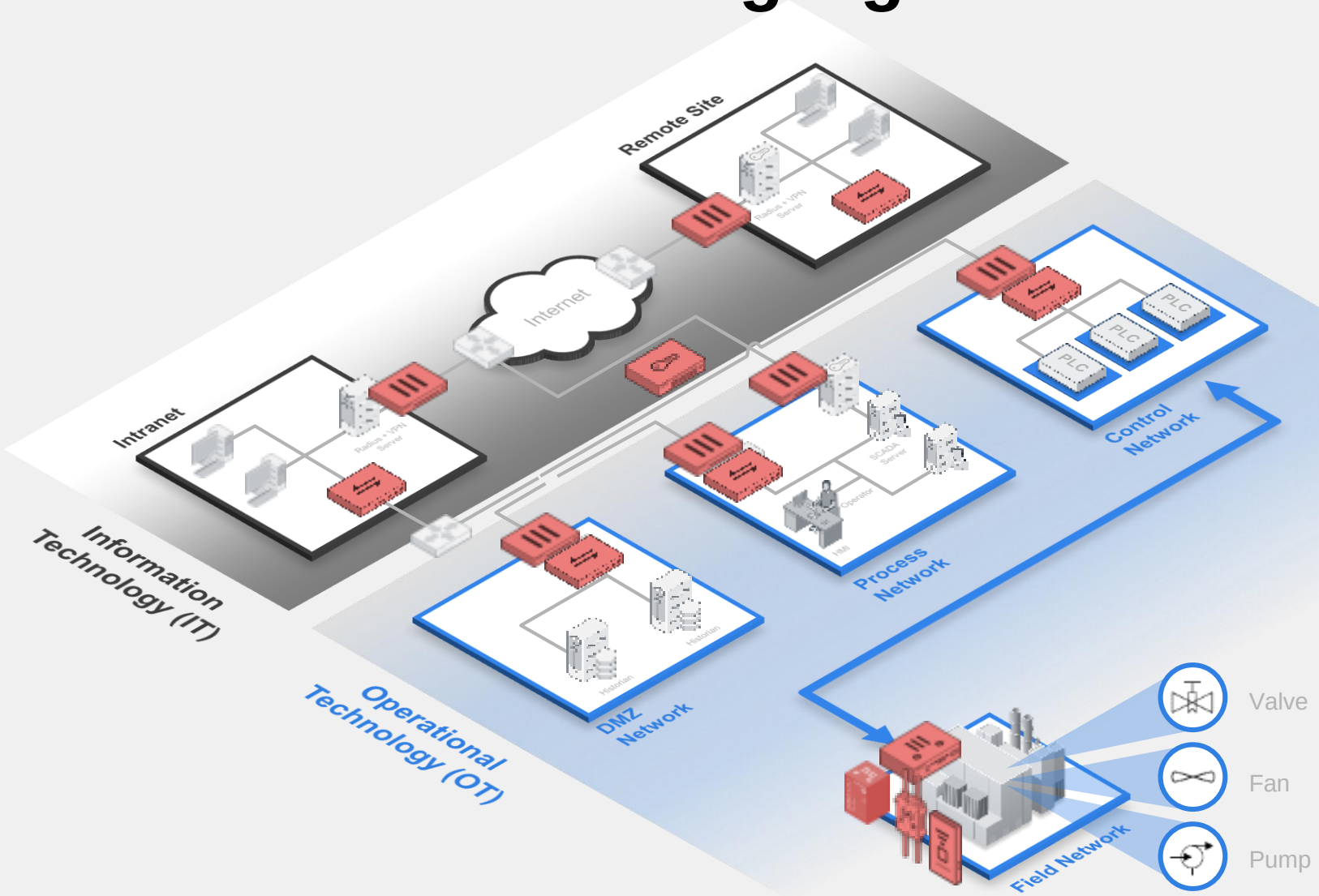


VLAN Routing vs. Micro-Segmentierung





Schritt 3: Sicherer Zugang



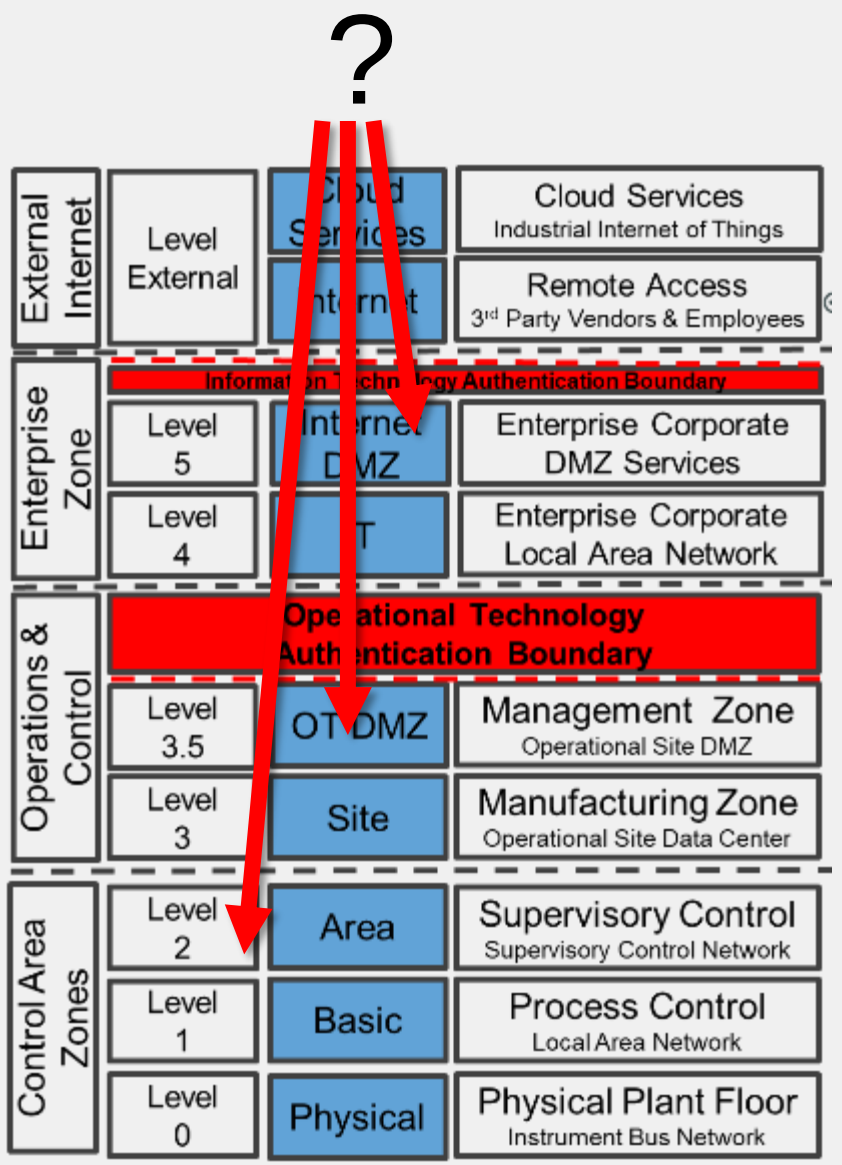
Segmentation / Encrypted Communication / IDS/IPS (FortiGate)

Secure Access (FortiSwitch/AP/Extender/NAC)

Access Control – Users, Devices, Applications and Protocols (FortiGate and FortiAuthenticator)

Schwachstelle: Remote-Zugänge

- „Honey Pot“ für Angreifer
- Oft ungesicherter Zugang zur Anlage
- Im Internet sichtbar, meist länger als Arbeiten dauern
- Unbeobachteter Datentransfer in die Anlage und aus der Anlage
- Unsicherer Umgang mit Login-Daten



SSL-VPN Portal

Launch FortiClient | Download FortiClient

Bookmarks

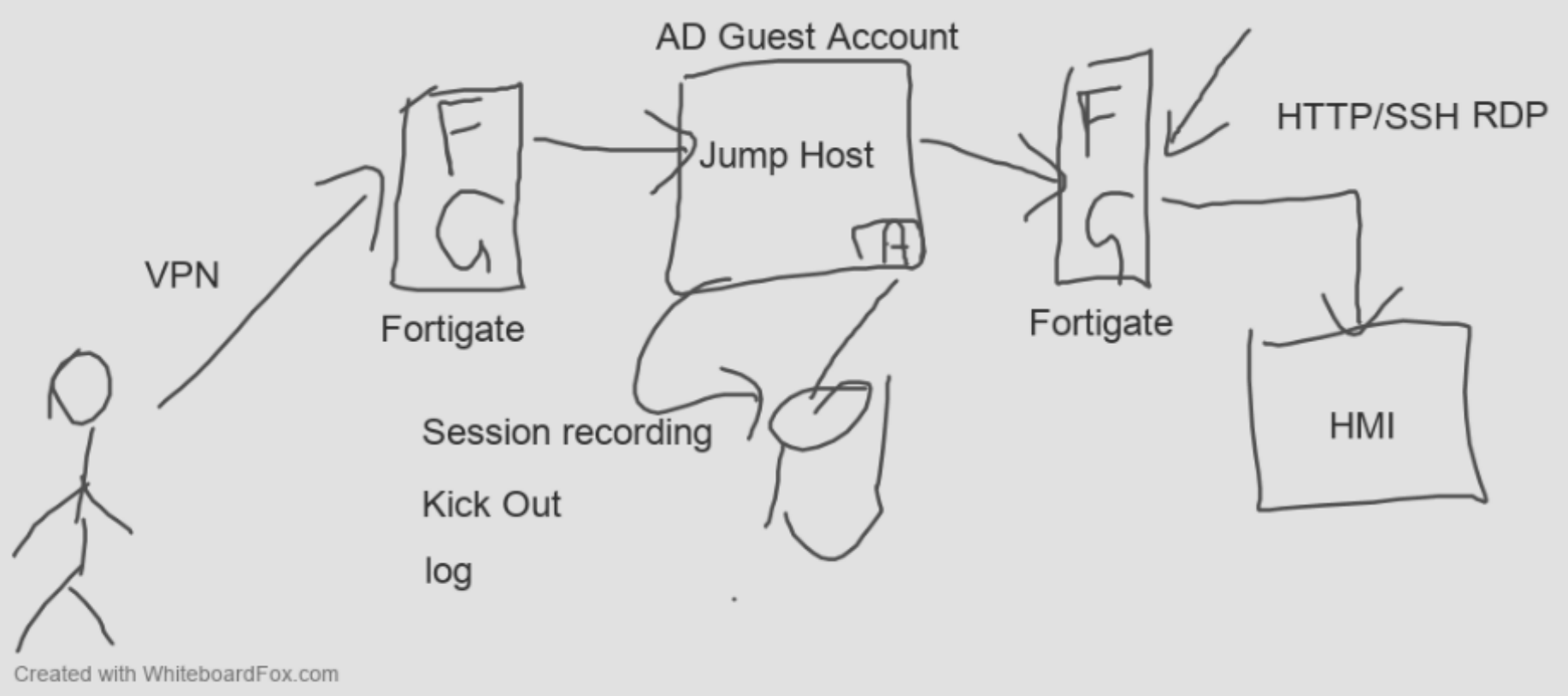
Engineering Station1

Fileshare Engineering Station1

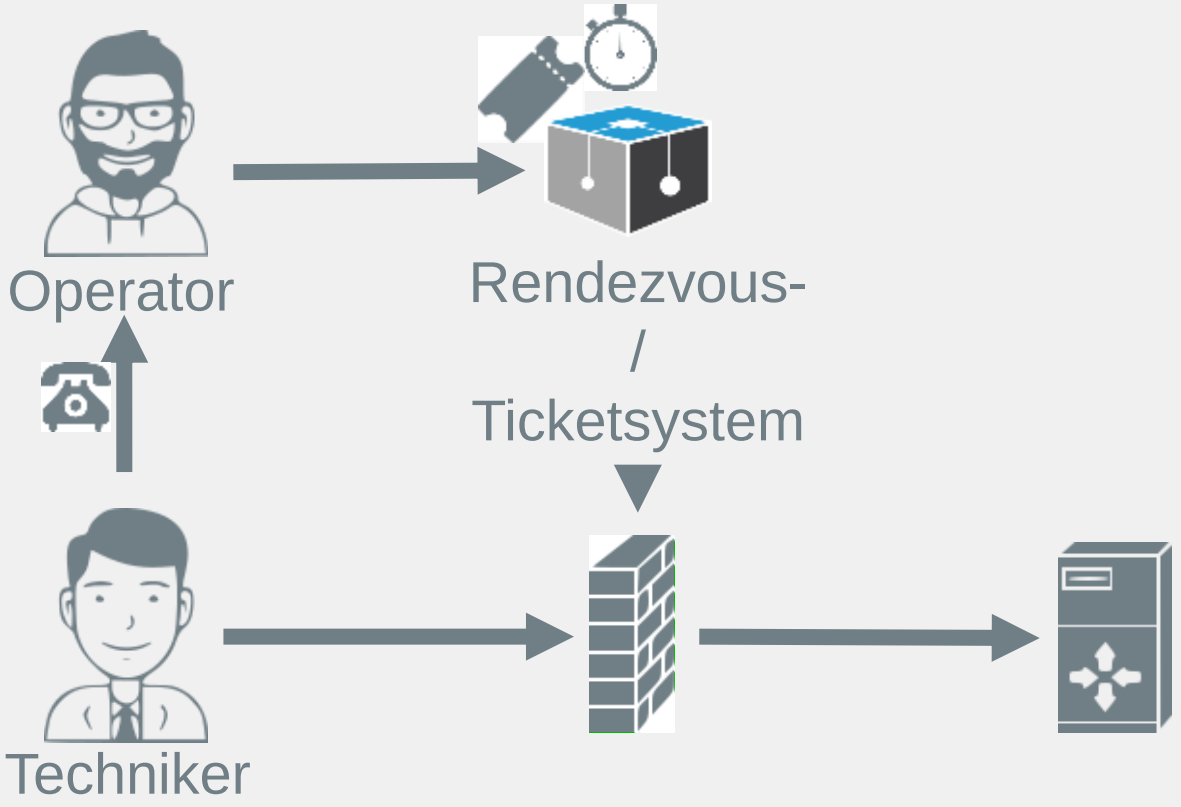
Quick Connection | New Bookmark

History

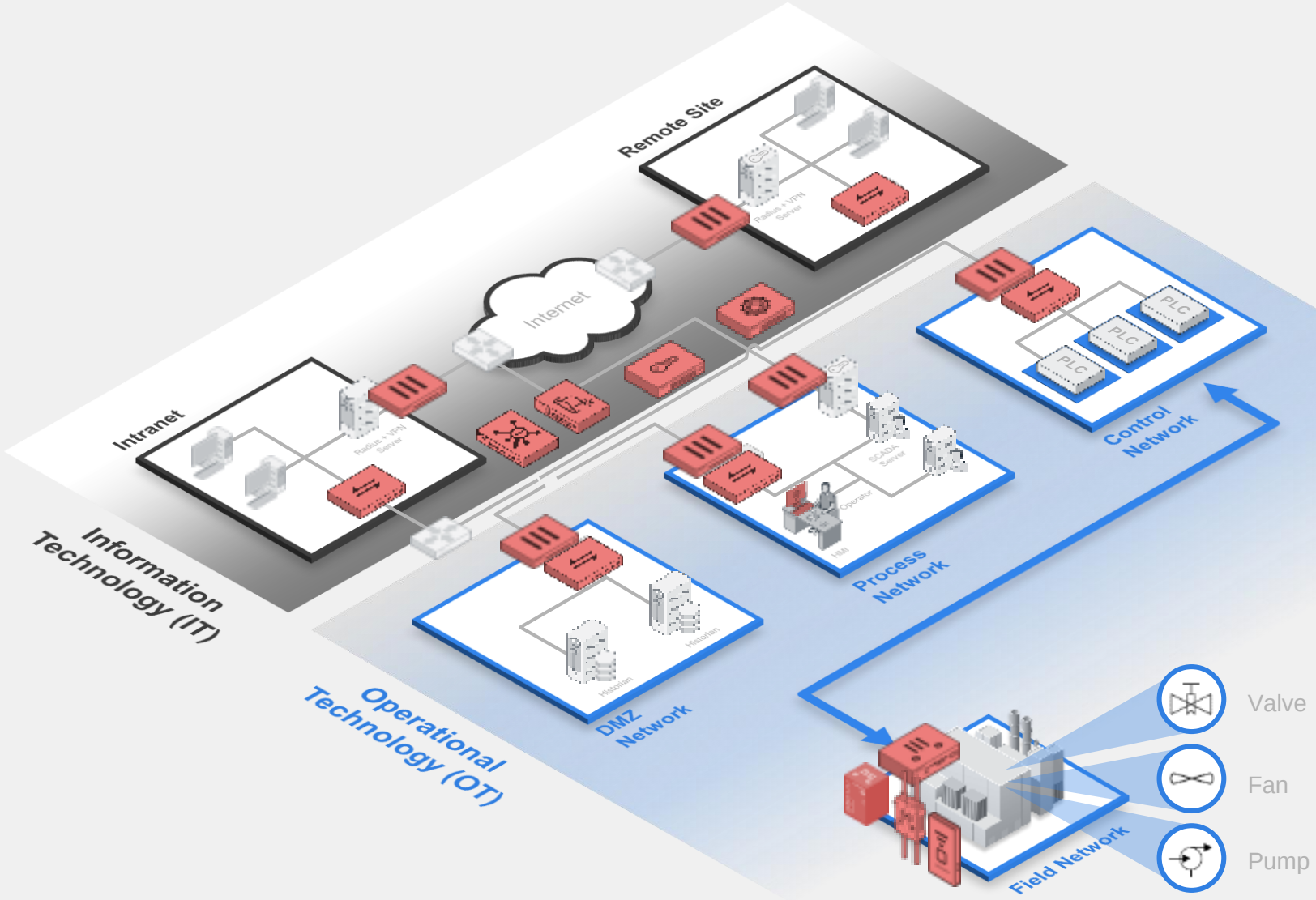
Use Case Fernwartung über Jump Host



Use Case Fernwartung über Ticketsystem

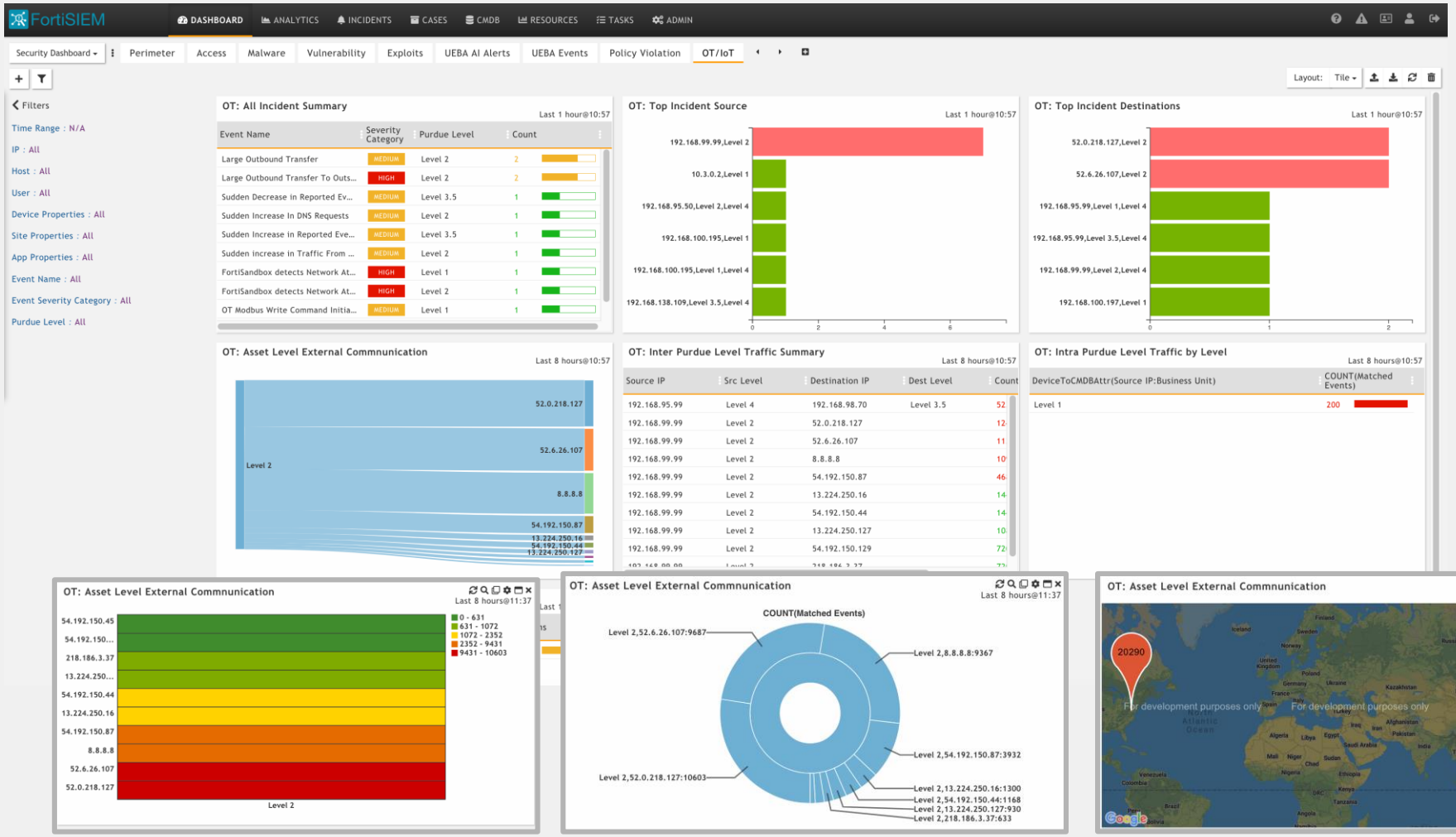


Weitere Schritte



- Segmentation / Encrypted Communication / IDS/IPS (FortiGate)
- Access Control – Users, Devices, Applications and Protocols (FortiGate and FortiAuthenticator)
- Secure Access (FortiSwitch/AP/Extender/NAC)
- Vulnerability and Patch Management (FortiWeb/FortiClient/FortiEDR/FortiGate)
- Unknown Samples Analysis (FortiSandbox via FortiGate, FortiMail, FortiWeb, FortiClient & FortiEDR)
- Log Collection for Correlation and Security Auditing (FortiSIEM/FortiSOAR)

OT related Dashboard

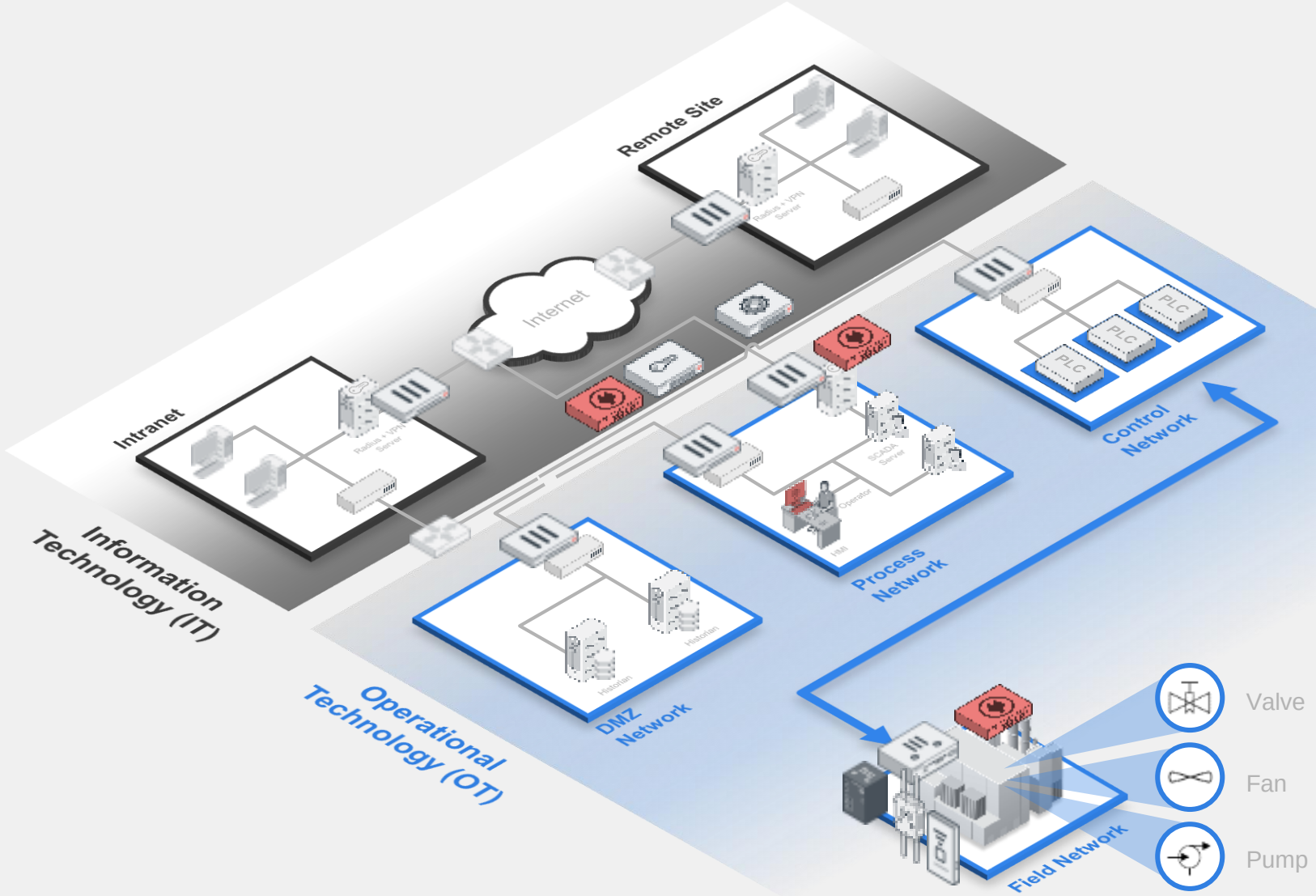


Ot-the-box OT related dashboard

Customize for use case:

- Widget Types
- Widget Reports
- Widget Time Scales

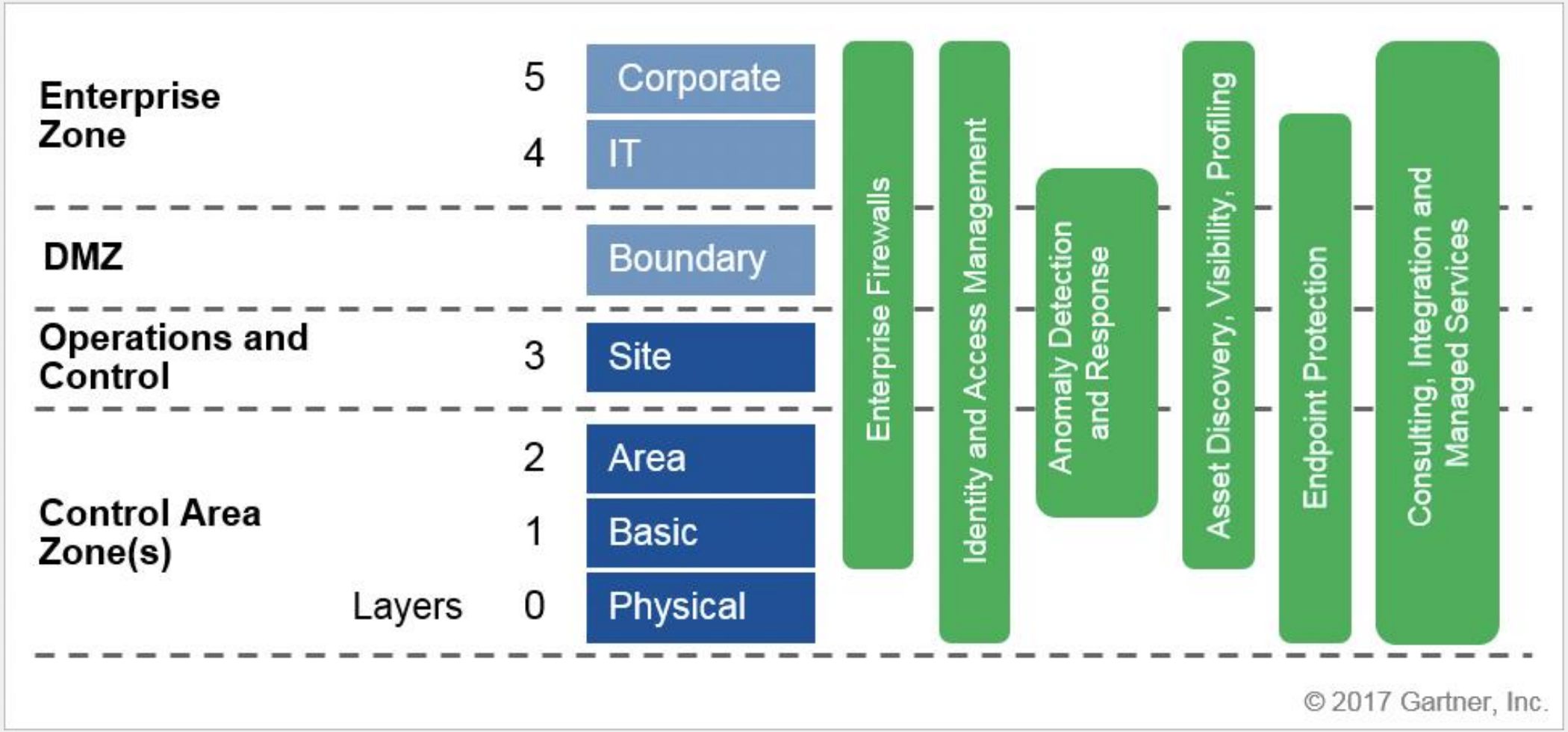
Automated Detection and Response



Automated Deception and Response (FortiDeceptor)

Zusammenfassung

It´s a Journey



Fortinet Security Fabric

Umfassend

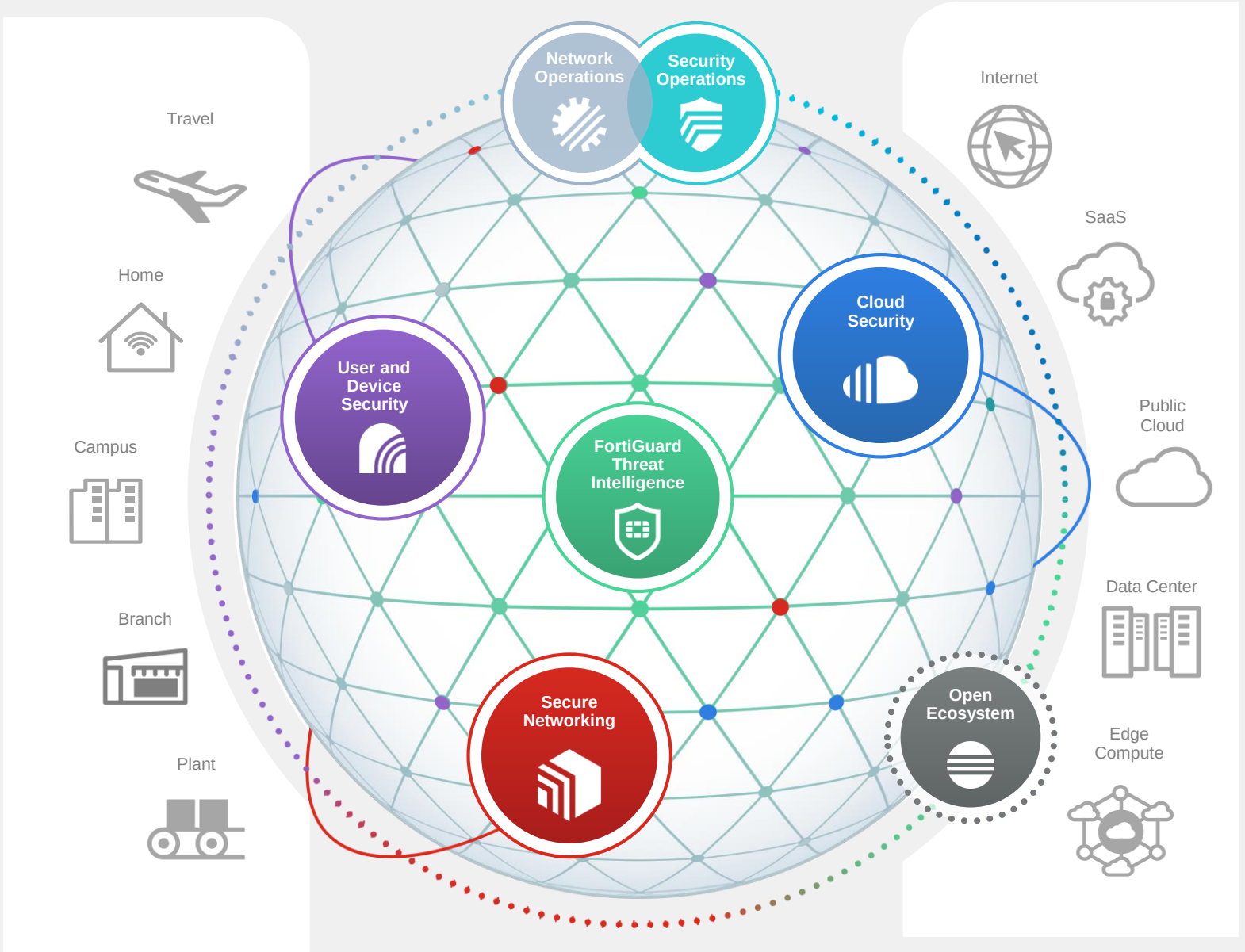
Sichtbarkeit und Schutz der gesamten digitalen Angriffsfläche, um das Risiko besser bewerten zu können

Integriert

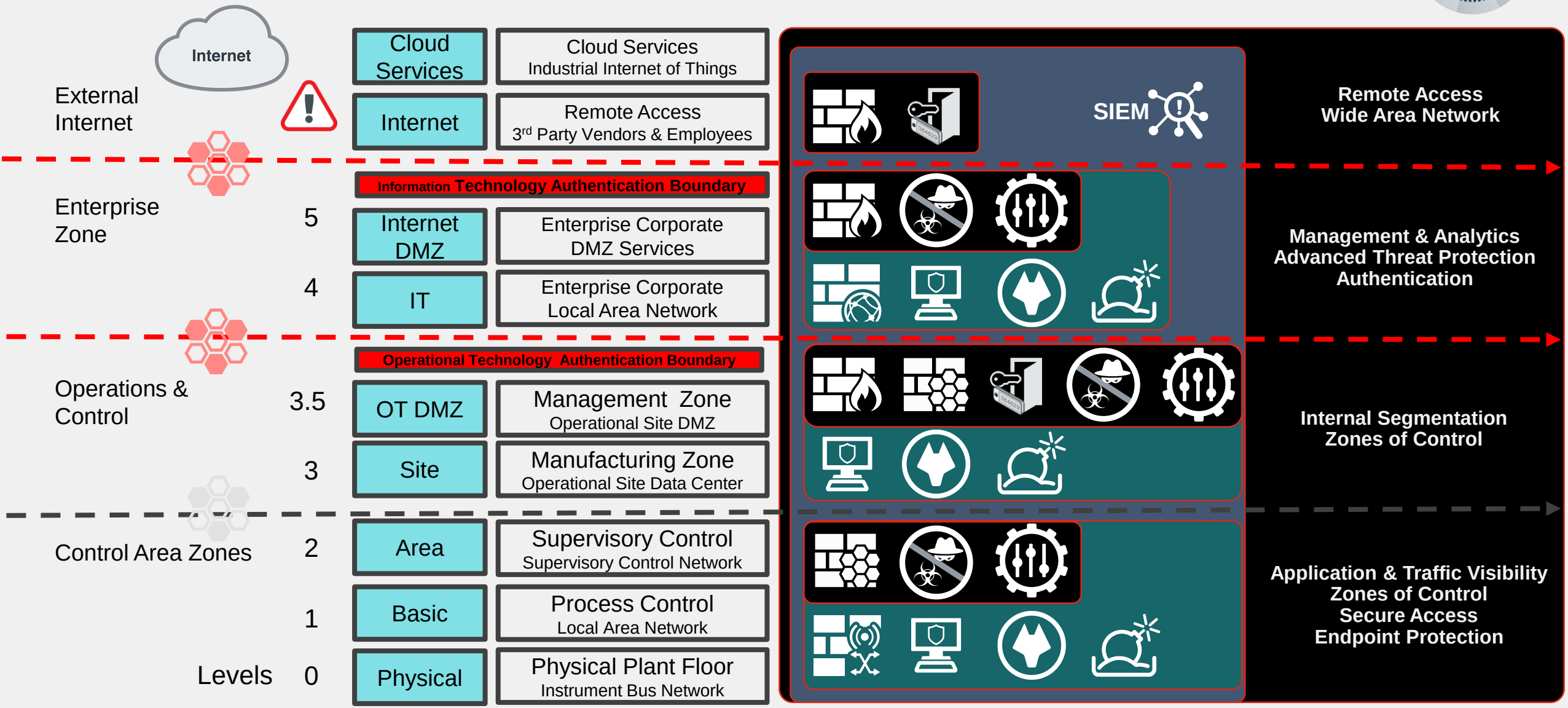
Der Management-Aufwand und die Komplexität werden reduziert, Informationen zwischen den Bausteinen ausgetauscht

Automatisiert

Selbstheilende Netzwerke mit KI-Komponenten, um Security-Vorfälle schnell und effektiv behandeln zu können



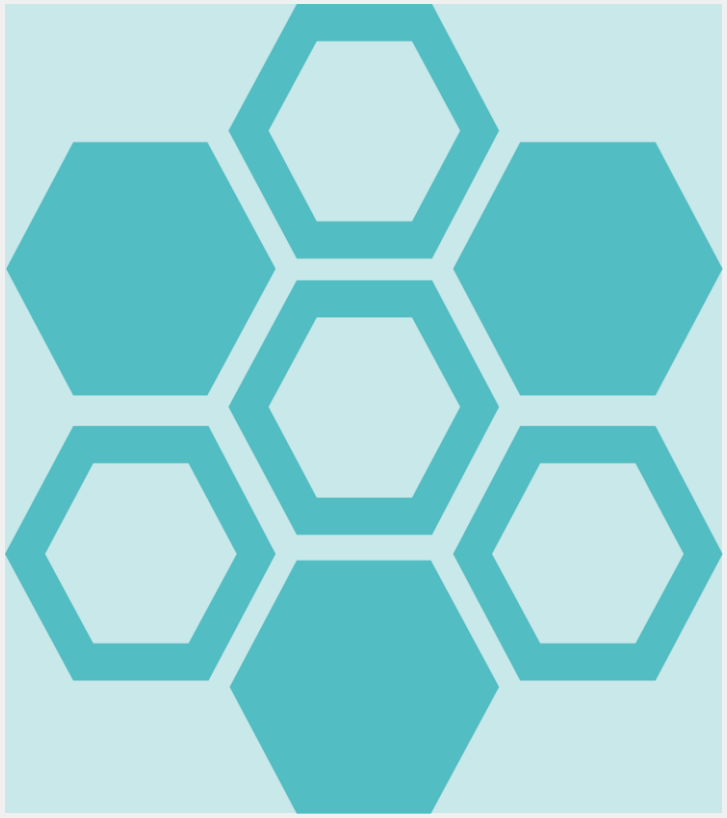
Industrial Security Fabric für Operational Technology



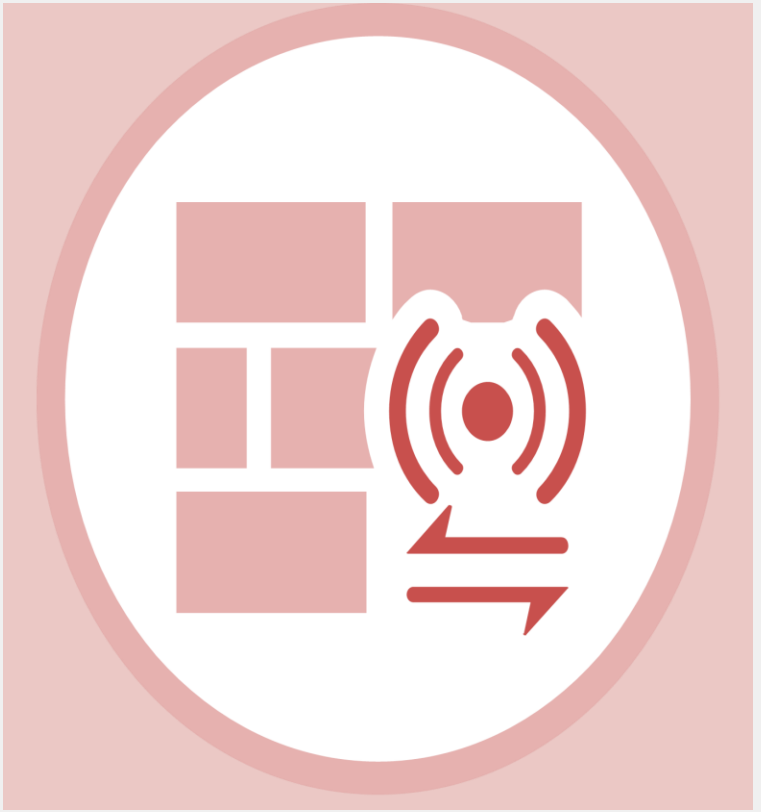
Kontrolle und sichere OT Netze durch

SICHTBARKEIT

SEGMENTIERUNG



SICHERER ZUGANG



IoT Security

IoT/OT Security Conference
7. März 2023 in Cham

ICB Infosec Community Builder

Aufzeichnung Fortinet OT Security:
https://attendee.gotowebinar.com/recording/6941221731356603137

Sichtbarkeit
Segmentierung
Sicherer Zugang

FORTINET®

Mirco Kloss
Manager Business Development
Operational Technology D-A-CH
+49 173 41 31 705
mkloss@fortinet.com
LinkedIn
https://ready.fortinet.com/ot
https://www.fortinet.com/industrydemo