

Hoe krijgt IT meer grip op security in het productienetwerk ?



Paul van Ruiten
Business Development
Digital Enterprise



Ruud Welschen
Product Manager
Digital Enterprise Services

Strategy

- Business drivers & goals
- Business opportunities and threats
- Initiate security program
- Budget, roles, responsibilities

INDUSTRIAL CYBER SECURITY

Identify

- Assess actual risk level
- Connected Assets & Software
- Architecture
- Implementation plan & change management

INDUSTRIAL CYBER SECURITY

Protect

- Training & awareness
- Authorization & access control
- Ringfencing, Defense in Depth
- Security Cells (firewalls)
- Patching & AntiVirus

INDUSTRIAL CYBER SECURITY

Detect

- Continuous Network monitoring
- Anomaly Detection

INDUSTRIAL CYBER SECURITY

Respond

- Event & incident response
- Continuity plan
- Network segmentation

INDUSTRIAL CYBER SECURITY

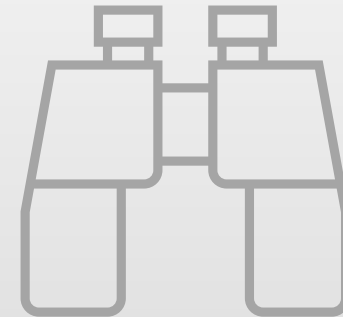
Recover

- Back-up & Restore
- Recovery plan

INDUSTRIAL CYBER SECURITY

Strategy

- Business drivers & goals
- Business opportunities and threats
- Initiate security program
- Budget, roles, responsibilities



Business drivers & goals



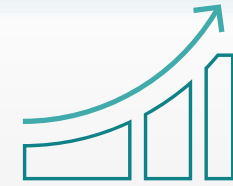
Speed



Flexibility



Quality



Efficiency



New business models



Security

Business opportunities and threats

- Digitalization

- Process optimization
- Predictive maintenance
- Customer intimacy
- Digital Twins
- Industrial IoT
- ...

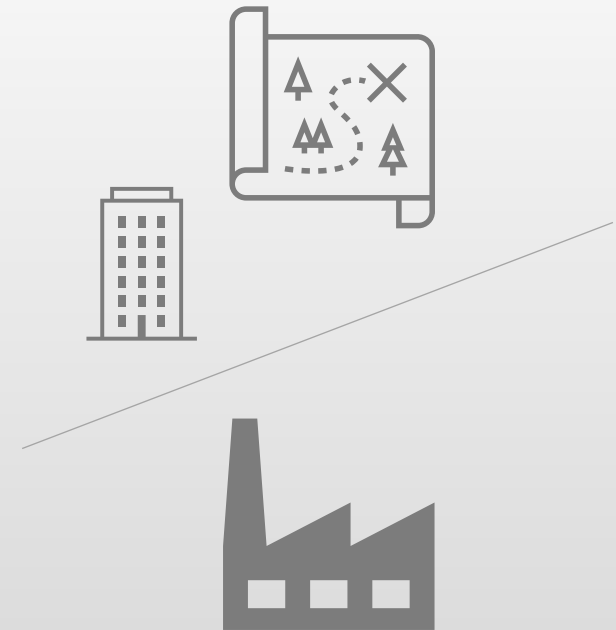
INVEST

- Airgap > Connectivity

INSURE

Initiate security program

- Usually focused on Information Security.
- Managed by consultancy company.
- Production facilities as “black box”.
- IT-OT convergence drives OT Security.



Strategy

- Business drivers & goals
- Business opportunities and threats
- Initiate security program
- Budget, roles, responsibilities

INDUSTRIAL CYBER SECURITY

Identify

- Assess actual risk level
- Connected Assets & Software
- Architecture
- Implementation plan & change management

INDUSTRIAL CYBER SECURITY

Protect

- Training & awareness
- Authorization & access control
- Ringfencing, Defense in Depth
- Security Cells (firewalls)
- Patching & AntiVirus

INDUSTRIAL CYBER SECURITY

Detect

- Continuous Network monitoring
- Anomaly Detection

INDUSTRIAL CYBER SECURITY

Respond

- Event & incident response
- Continuity plan
- Network segmentation

INDUSTRIAL CYBER SECURITY

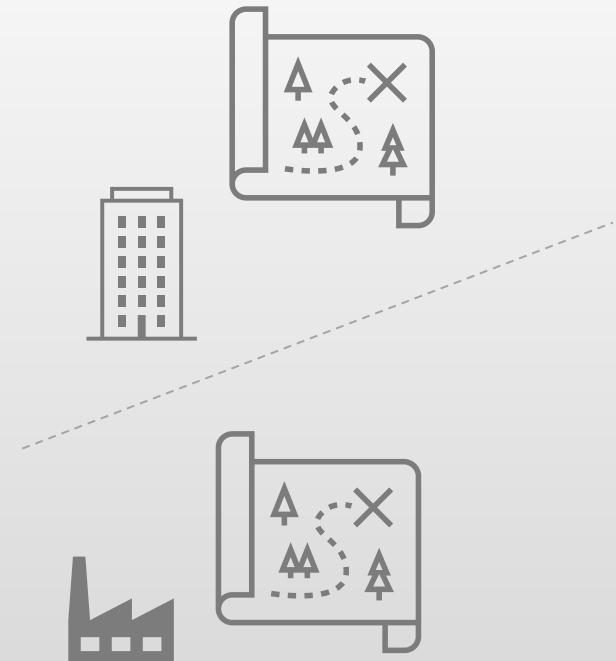
Recover

- Back-up & Restore
- Recovery plan

INDUSTRIAL CYBER SECURITY

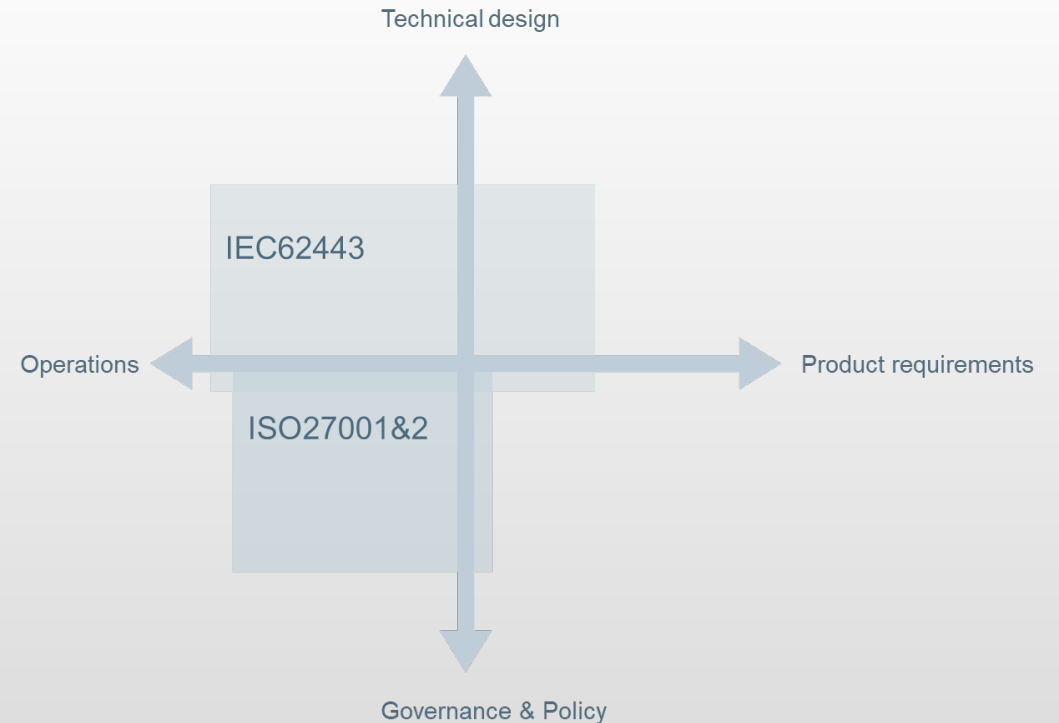
Identify

- Assess actual risk level
- Connected Assets & Software
- Architecture
- Implementation plan & change management



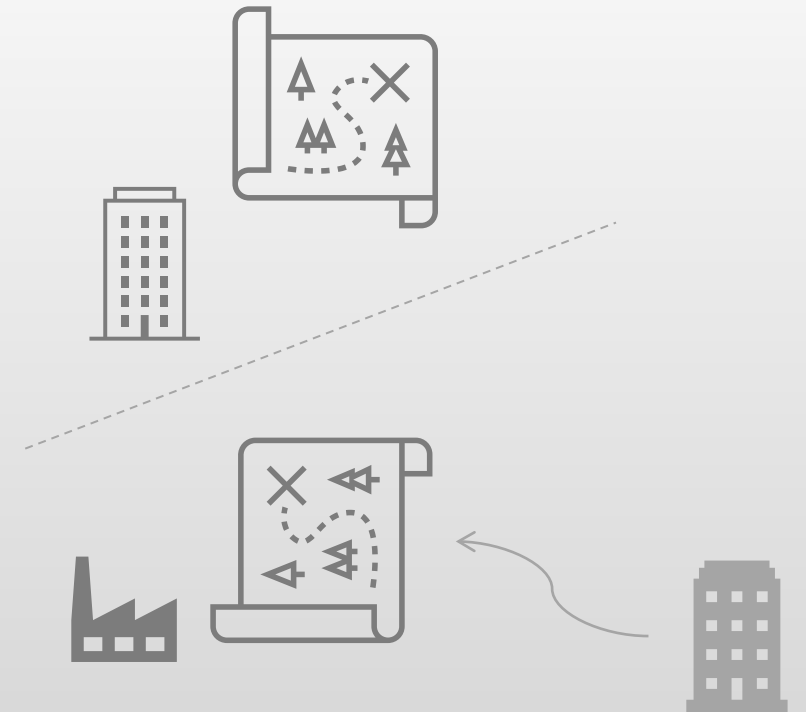
Assess actual risk level

- Use IEC62443 instead of ISO27001
- By OT specialist
- Processes, people & technology
- Define action list priorities



Connected Assets & Software

- OT focus on mechanical assets, not on connected assets
- Connectivity on several media & protocols
- Extreme lifecycle for hardware
- Backdoors common practice



Connected Assets & Software

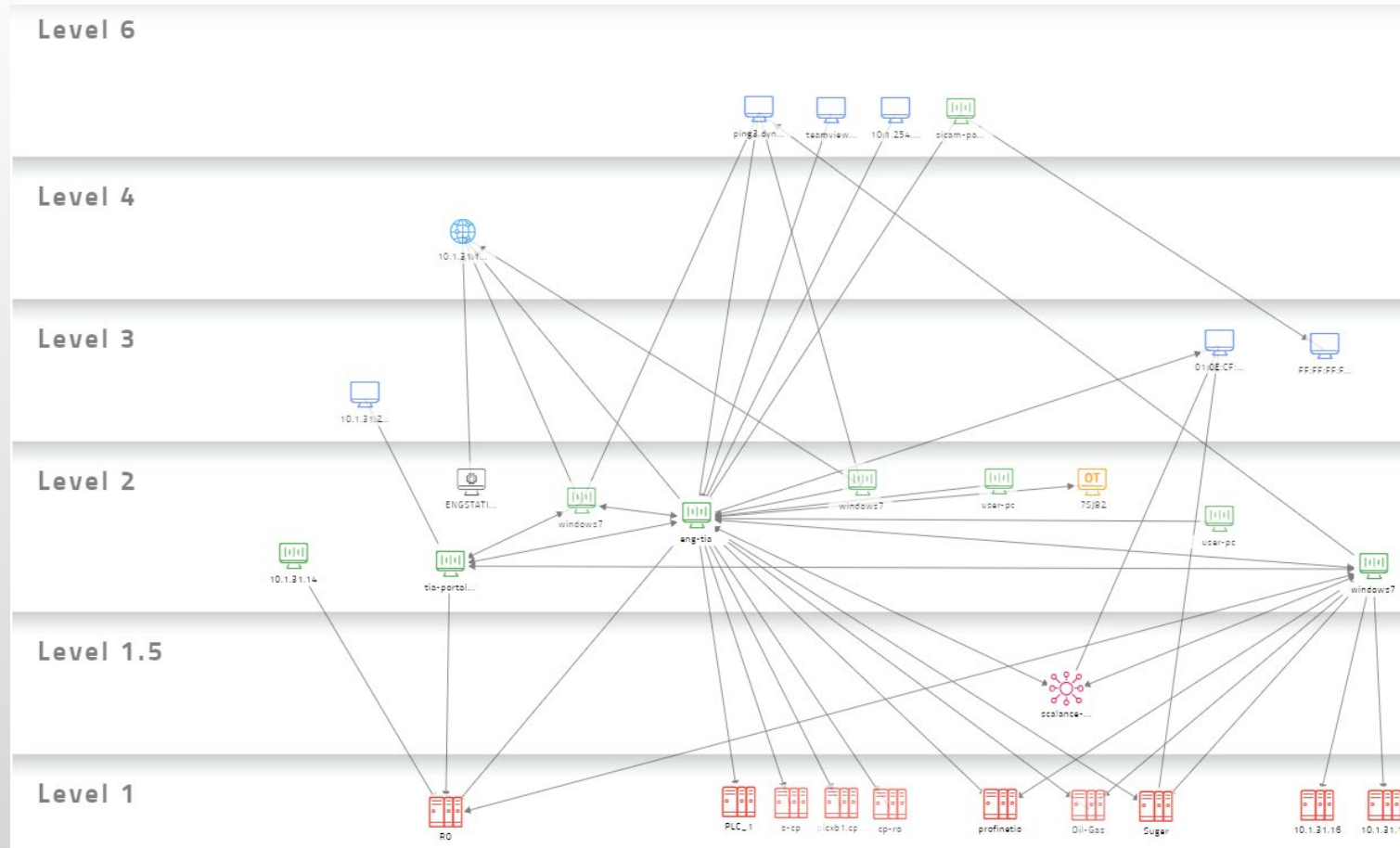
- Limited toolbased options available
- Mostly vendor specific
- Dedicated network monitoring tools available



Claroty passive scan – asset list

RESULTS (15)											<< < 1 > >>
<input type="checkbox"/>	RO	10.1.31.1	28:63:36:26:F0:74	OT	PLC	High	Medium	Siemens	Default	26/10/20, 07:05	
<input type="checkbox"/>	10.1.31.16	10.1.31.16	08:00:06:93:8C:DA	OT	PLC	High	Medium	Siemens	Default	26/10/20, 04:06	
<input type="checkbox"/>	10.1.31.17	10.1.31.17	08:00:06:93:8C:B7	OT	PLC	High	Medium	Siemens	Default	26/10/20, 04:06	
<input type="checkbox"/>	scalance-x200	10.1.0.180, 10.1.31.10	00:0E:8C:98:E3:50	IT	Networking	Medium	Low	Siemens	Default	26/10/20, 05:12	
<input type="checkbox"/>	PLC_1	10.1.0.50, 10.1.31.6	28:63:36:88:F7:AE	OT	PLC	High	High	Siemens	Default	26/10/20, 04:06	
<input type="checkbox"/>	profinetio	10.1.31.11	28:63:36:09:42:23	OT	PLC	High	Medium	Siemens	Default	26/10/20, 04:06	
<input type="checkbox"/>	windows7	10.1.31.219, 10.1.31.241, 10.10.9.65	00:50:56:8D:DF:B8	OT	HMI	Medium	Medium	Siemens	Default	26/10/20, 14:16	
<input type="checkbox"/>	eng-tia	10.1.31.15, 192.168.0.253	00:50:56:8D:27:66	OT	HMI	High	Medium	Siemens	Default	26/10/20, 14:22	
<input type="checkbox"/>	tia-portal-15-e	10.1.31.116	00:50:56:B8:C8:3E	OT	HMI	Medium	Low	Siemens	Default	26/10/20, 07:05	
<input type="checkbox"/>	10.1.31.14	10.1.31.14	00:50:56:8D:DA:F7	OT	HMI	Medium	Low	VMware	Default	26/10/20, 04:06	
<input type="checkbox"/>	lkpo-xgyjh7ojyo	169.254.114.2	00:50:56:8D:2E:17	IT	Endpoint	Low	Low	VMware	Default	26/10/20, 03:46	
<input type="checkbox"/>	DESKTOP-OL4PQ3T	169.254.116.246	00:50:56:8D:FE:3C	IT	Endpoint	Low	Medium	VMware	Default	26/10/20, 03:46	
<input type="checkbox"/>	172.31.28.5	172.31.28.5		OT	HMI	Medium	Low		Default	26/10/20, 05:05	
<input type="checkbox"/>	172.31.28.8	172.31.28.8		OT	HMI	Medium	Low		Default	26/10/20, 05:05	

Clarity network view



Clarity device information

DEVICE INFORMATION

NETWORK

IP
10.1.31.11

MAC
28:63:36:09:42:23

Host name
profinetio

Purdue Level
Level 1 [🔗](#)

First Seen
26/10/20, 04:06

Class
OT

Protocols
ARP, EPM, PROFI...

HARDWARE

Vendor
Siemens

Serial
S C-E4VU761220...

Model
IM155-6PN HF

Family
SIMATIC S7

Firmware
V3.3.0

Hardware Revision
0

Order Number (MLFB)
6ES7 155-6AU00...

SOFTWARE

Parsed Asset
No

COMPLIANCE

Default Passwords
Yes

OTHER

Description
Siemens, SIMATI...

RACK SLOTS

Slot 0 - Slot 0	Name Slot 0 Vendor Siemens Model IM 155-6 PN HF V3.3 Serial Number S C-E4VU76122014 Firmware Version V3.3.0
Slot 1 - Slot 1	Name Slot 1 Vendor Siemens Model DI 8x24VDC BA Serial Number S C-F3VM29382015 Firmware Version V1.0.0
Slot 2 - Slot 2	Name Slot 2 Vendor Siemens Model DQ 8x24VDC/0.5A ST V1.1 Serial Number S C-F4UC01392015 Firmware Version V1.1.0
Slot 3 - Slot 3	Name Slot 3 Vendor Siemens Model AI 4xU/I 2-wire ST V1.1 Serial Number S C-F4UX04882015 Firmware Version V1.1.0
Slot 4 - Slot 4	Name Slot 4 Vendor Siemens Model AQ 4xU/I ST V1.1 Serial Number S C-F4VL81612015 Firmware Version V1.1.0
Slot 5 - Slot 5	Name Slot 5 Vendor Siemens Model Server module V1.1 (IM 155-6 PN ST V1.0) Serial Number S C-C6UV84042012 Firmware Version V1.0.0

Claroty OT audit report

Asset Name: Search by asset name | Tag Name: Search by tag name | Protocols: Select Protocol | Last Access Type: Select Access Type | Time: 1hr. D.

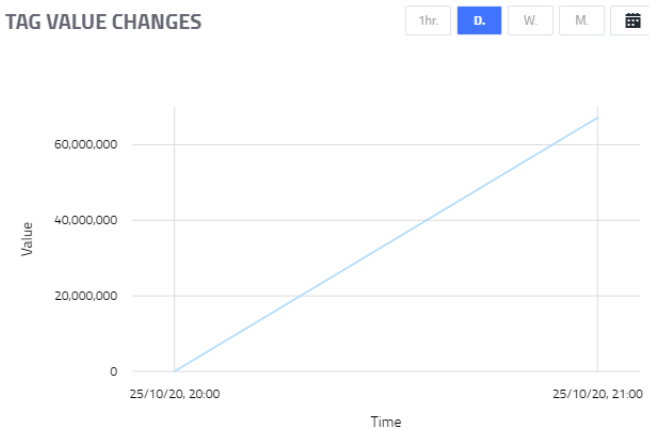
RESULTS (109)

ID	ASSET NAME	PROTOCOL	TAG NAME	LAST VALUE	LAST ACCESS TYPE	LAST FUNCTION CODE
108	RO	S7COMM	DB1.DBX328.0 Size:DINT Length:1	67165600.0	Write	Write Var
50	Controller_1	MMS	SIPV13p1_5051OC3phase1: IL_PTOC1\$ST\$Beh\$stVal	100.0	Read	read
4	Controller_1	MMS	SIPDc3: CSW11\$CF\$Pos.2	10000.0	Read	read
6	Controller_1	MMS	SIPDc2: CSW11\$CF\$Pos.0	4.0	Read	read
7	Controller_1	MMS	SIPDc2: CSW11\$CF\$Pos.1	30000.0	Read	read
8	Controller_1	MMS	SIPDc2: CSW11\$CF\$Pos.2	10000.0	Read	read
10	Controller_1	MMS	SIPDc1: CSW11\$CF\$Pos.1	30000.0	Read	read
18	Controller_1	MMS	SIPV13p1_5051NOCgndB1: ND_PTOC2\$ST\$Beh\$stVal	5.0	Read	read
11	Controller_1	MMS	SIPDc1: CSW11\$CF\$Pos.2	10000.0	Read	read
12	Controller_1	MMS	SIPApplication: LLN0\$CF\$LocSta.0	1.0	Read	read
13	Controller_1	MMS	SIPCB1: CSW11\$CF\$Pos.0	4.0	Read	read
14	Controller_1	MMS	SIPCB1: CSW11\$CF\$Pos.1	30000.0	Read	read

TAG INFORMATION

Tag name	Asset Name	Protocol	Last Value
DB1.DBX328.0 Si...	RO	S7COMM	67165600.0
Write Count	Read Count	Last Function Code	Min Value
7	12	Write Var	0
Max Value	Variance Between Values	Abnormal changes	
67165600	14996315.38	1	

TAG VALUE CHANGES



Strategy

- Business drivers & goals
- Business opportunities and threats
- Initiate security program
- Budget, roles, responsibilities

INDUSTRIAL CYBER SECURITY

Identify

- Assess actual risk level
- Connected Assets & Software
- Architecture
- Implementation plan & change management

INDUSTRIAL CYBER SECURITY

Protect

- Training & awareness
- Authorization & access control
- Ringfencing, Defense in Depth
- Security Cells (firewalls)
- Patching & AntiVirus

INDUSTRIAL CYBER SECURITY

Detect

- Continuous Network monitoring
- Anomaly Detection

INDUSTRIAL CYBER SECURITY

Respond

- Event & incident response
- Continuity plan
- Network segmentation

INDUSTRIAL CYBER SECURITY

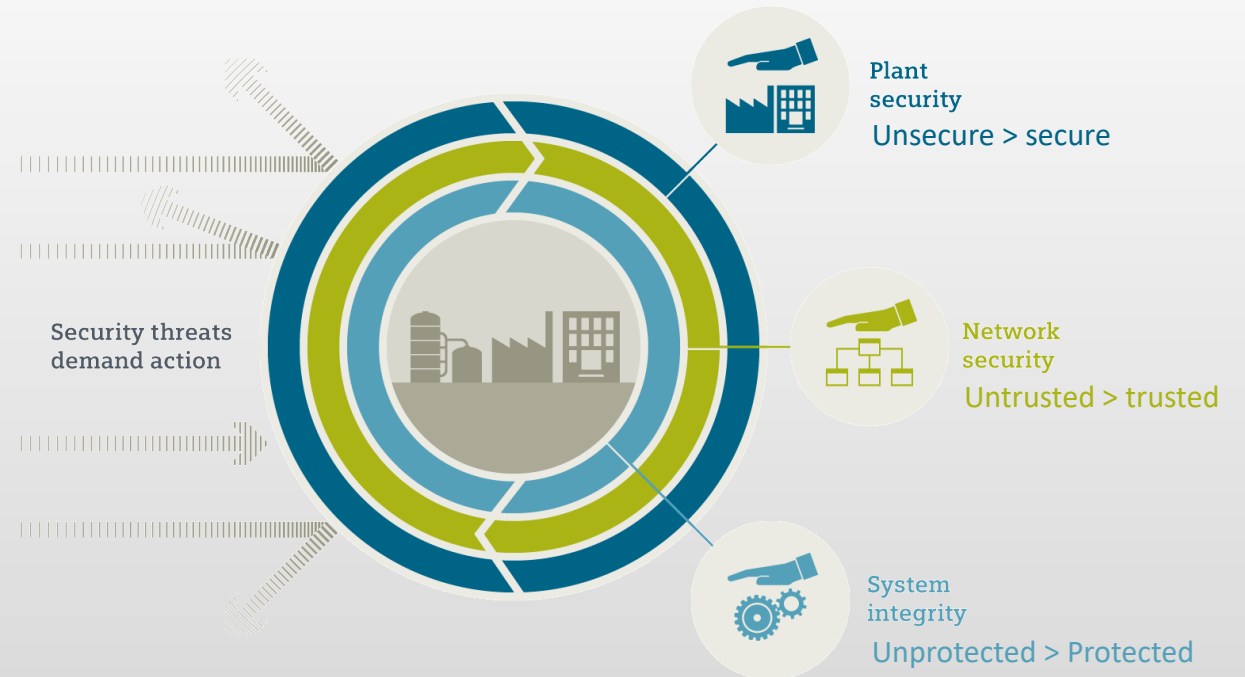
Recover

- Back-up & Restore
- Recovery plan

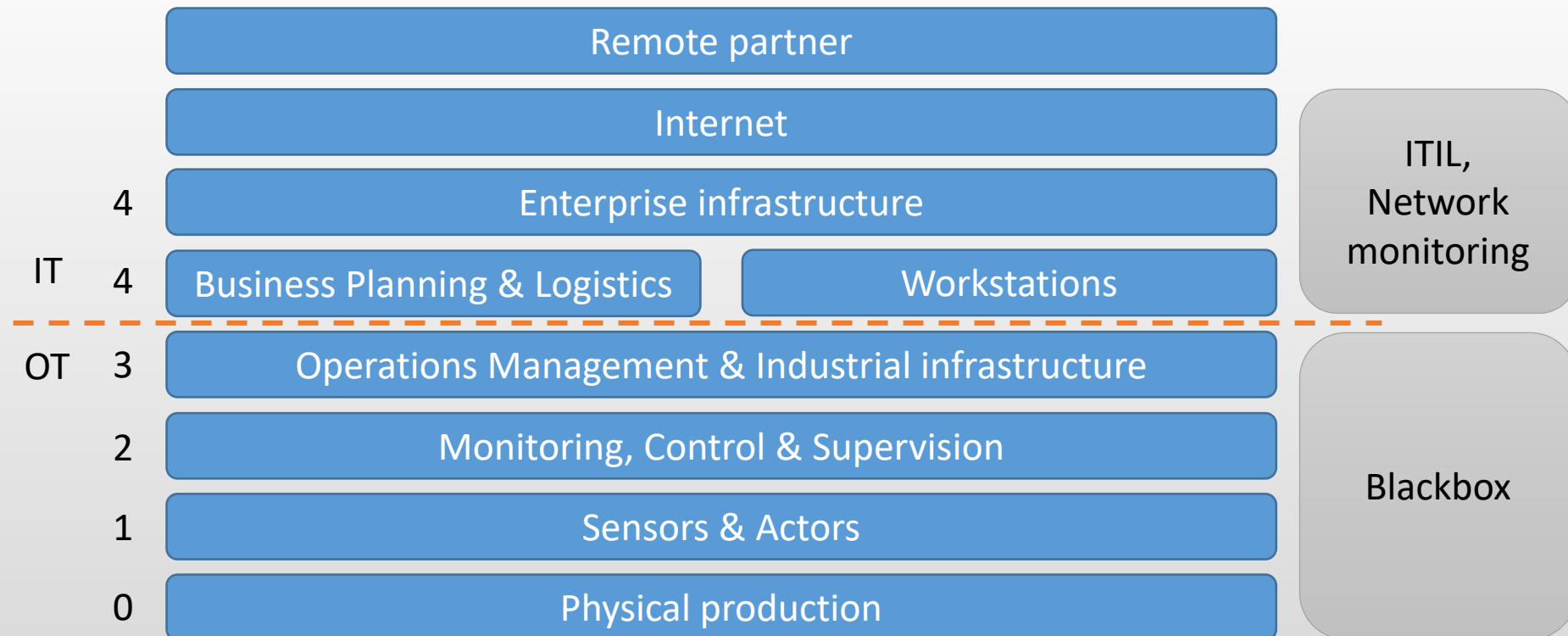
INDUSTRIAL CYBER SECURITY

Protect

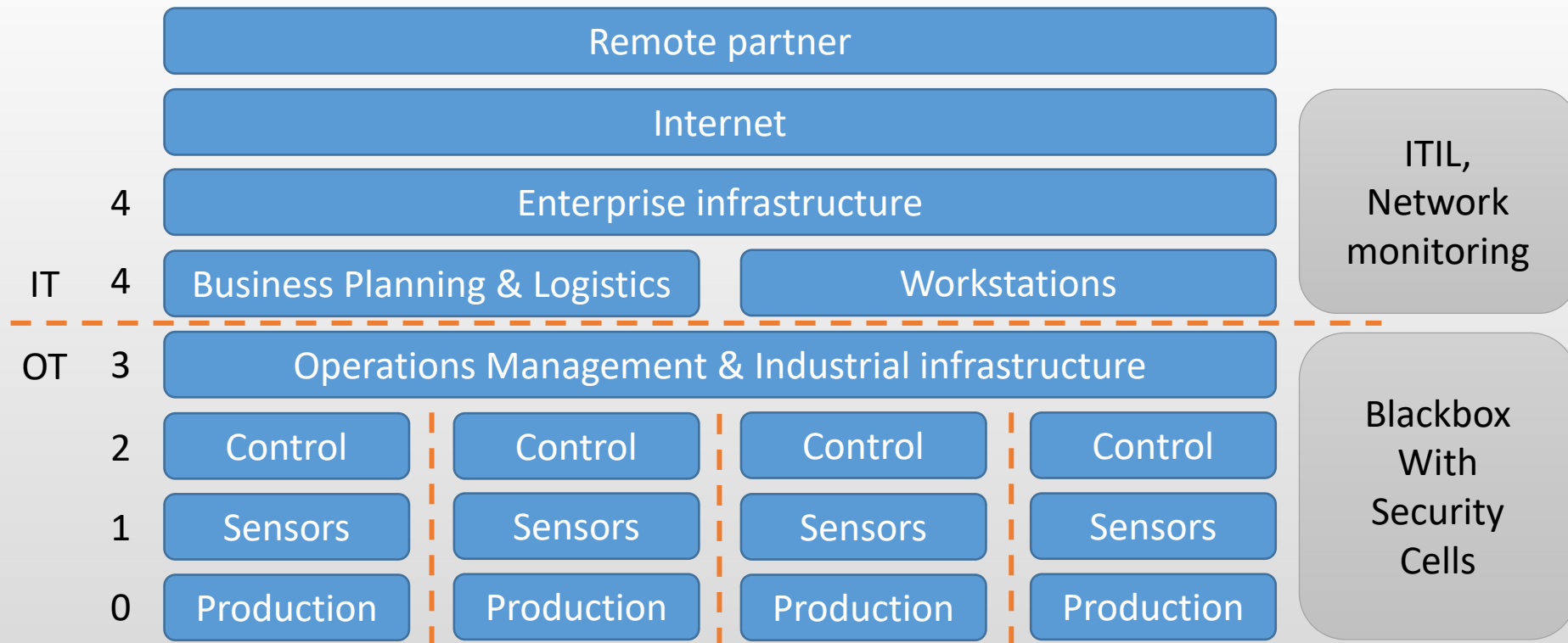
- Training & awareness
- Authorization & access control
- Ringfencing, Defense in Depth
- Security Cells (firewalls)
- Patching & AntiVirus



Functional levels



Security Cells



Strategy

- Business drivers & goals
- Business opportunities and threats
- Initiate security program
- Budget, roles, responsibilities

INDUSTRIAL CYBER SECURITY

Identify

- Assess actual risk level
- Connected Assets & Software
- Architecture
- Implementation plan & change management

INDUSTRIAL CYBER SECURITY

Protect

- Training & awareness
- Authorization & access control
- Ringfencing, Defense in Depth
- Security Cells (firewalls)
- Patching & AntiVirus

INDUSTRIAL CYBER SECURITY

Detect

- Continuous Network monitoring
- Anomaly Detection

INDUSTRIAL CYBER SECURITY

Respond

- Event & incident response
- Continuity plan
- Network segmentation

INDUSTRIAL CYBER SECURITY

Recover

- Back-up & Restore
- Recovery plan

INDUSTRIAL CYBER SECURITY


Detect

- Continuous Network monitoring
- Anomaly Detection

Anomaly detection

- Available for both IT and OT
- Passive listening to network traffic
- Understands OT protocols
- Detects deviations from baseline
- Builds threat level overview of the company

Clarity anomaly detection alert




Configuration Download

Out of working hours Configuration Download: Configuration Download critical change operation was performed for the first time by 10.1.30.40 on 10.1.30.1 while related assets were managed remotely


What does this mean?
An attacker may want to interfere with normal critical infrastructure activity by changing a PLC code. If the PLC is running and as a result stops functioning, it may cause a significant production loss.

ALERT SCORE




Severity: Critical


Significant Indicators



Event occurred out of working hours.



Connected assets were previously accessed via Remote Connection



Critical Change Operation.

Indicator	Match	Score Points
● Event occurred out of working hours.	✓	+ 10
● This OT operation was previously approved in the system, but never between these zones/assets	✓	+ 80
● Critical Change Operation.	✓	+ 20
● A new code section was added	✗	0
● A large code section was changed	✗	0
● Connected assets were previously accessed via Remote Connection	✓	+ 10
● Event is related to previous alerts in the system.	✓	+ 10
Total Score	<i>Alert score is capped at 100.</i>	130
Alert Score		100

Clarity risk insights

INSIGHTS (25)	
🔦	Top 7 Risky Assets
🔦	17 assets are using 4 unsecured protocols: , SMB, SNMP
🔦	1 asset has 149 unpatched vulnerabilities - Windows Full Match
🔦	11 assets were communicating with 9 external IPs (2 of them are ghost)
🔦	34 assets have 183 unpatched vulnerabilities - Full Match
🔦	9 assets are using default passwords
🔦	4 assets using IT protocols: EPM, PHYSICAL, RDP , with 10 PLCs/Controllers/RTUs/IEDs
🔦	5 OT-assets performed privileged OT operations on 3 PLCs/Controllers/RTUs/IEDs
🔦	1 asset managed 1 asset remotely using protocol: RDP
🔦	12 assets have 98 unpatched vulnerabilities - Vendor and Model Match
🔦	12 assets have multiple network interfaces
🔦	11 OT-assets performed data-acquisition write operations on 8 PLCs/Controllers/RTUs/IEDs
🔦	1 asset has 29 vulnerabilities in its installed programs
🔦	1 asset is using SMBv1 Protocol only for negotiation

Clarity potential attack chain

ATTACK CHAIN

1 External Endpoint

teamviewer.com (external) in zone Endpoint: Other - External

Communicating in SSL protocol

The attacker can leverage the asset's connection to the external network to enter the internal network.

with:

2 HMI

eng-tia in zone HMI: Profibus,S7

performing OT commands via PROFINET-IO protocol

With access to the OT network, the attacker can leverage OT protocols for malicious purposes, such as changing register values, shutting down controllers or changing configurations

to:

3 PLC

profinetio in zone PLC: Profibus
SSA-880233 ⓘ

Attack Vector

Target Zone

PLC: Profibus

ASSET RESULTS (3)

Level 6



teamview...

Level 2



eng-tia

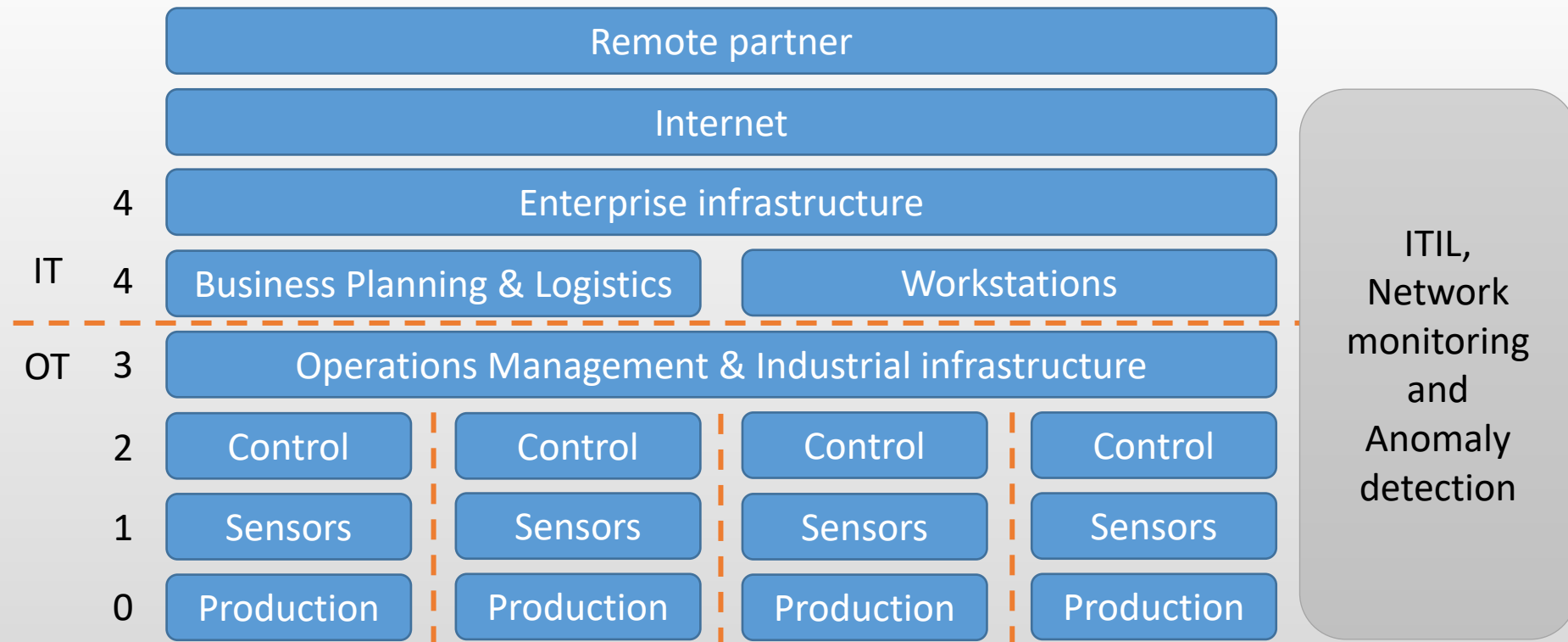
Level 1



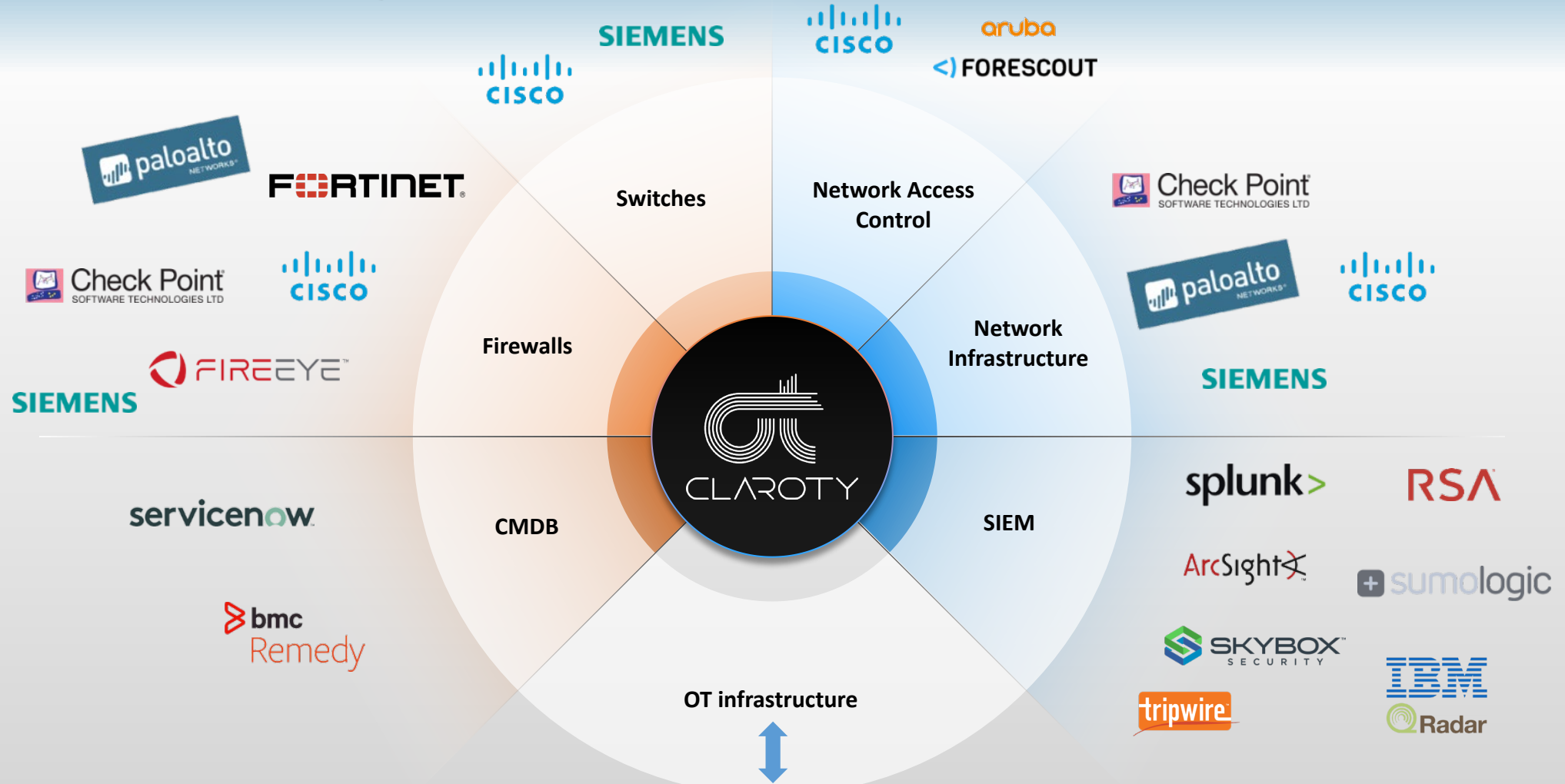
profinetio



IT – OT convergence



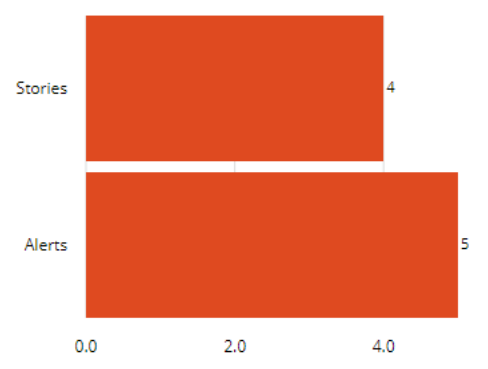
IT – OT integration





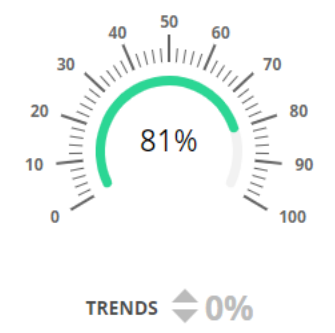
THREAT DETECTION

ALERT STATUS



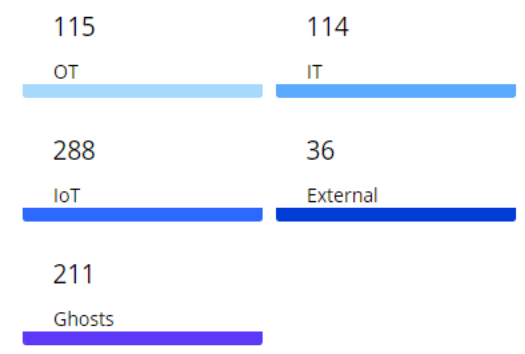
RISK & VULNERABILITIES

HYGIENE SCORE



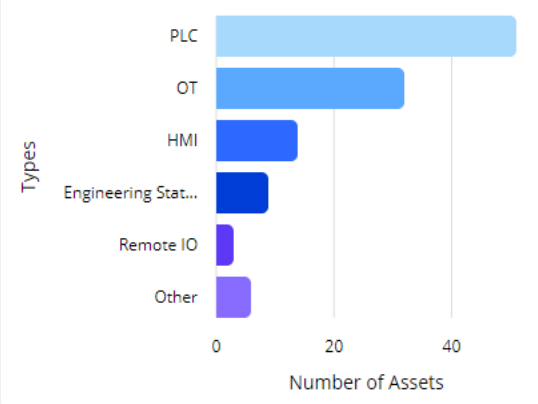
VISIBILITY

DISCOVERED ASSETS



OT / ASSET INVENTORY

OT ASSETS DISTRIBUTION



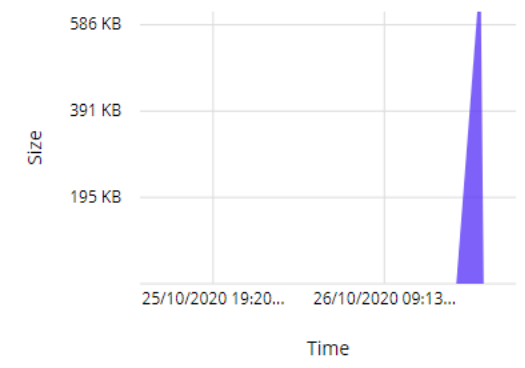
TOP ALERTED ZONES

Zone	Criticality	Alerts
Endpoint: Oth...	● Low	2
Endpoint: Oth...	● Low	2
Engineering S...	● Medium	2
PLC:	● High	2
Broadcast / M...	● Low	1
Camera: Other	● Low	1

TOP INSIGHTS

- 34 assets have 183 unpatched vulnerabilities - Full Match
 - Top 7 Risky Assets
 - 1 asset has 149 unpatched vulnerabilities - Windows Full Match
- [Show More](#)

NETWORK ANALYTICS



SUMMARY

OT Assets	115
OT Operations	31
Write and Execute OT Operations	54

Summary

- OT security is an enabler for Digitalization
- Use NCSC model as approach
- Refer to IEC62443 for OT security
- Request OT specialist for assessment
- Adopt Anomaly Detection for IT-OT convergence

Thank you

Digitalization and cybersecurity go hand in hand:

<http://siemens.com/industrialsecurityservices>

Download from the site: E-book Primer for Cybersecurity in Industrial Automation

The International Society of Automation (ISA) and Siemens team up to bring you an in-depth e-book as a guide to facilitate the access to the standard IEC 62443 – including main concepts and basic principles to design and deploy security concepts for industrial plants.



Paul van Ruiten

Business Development
Digital Enterprise
Paul.vanruiten@siemens.com
06-83572745



Ruud Welschen

Product Manager
Digital Enterprise Services
Ruud.Welschen@siemens.com
06-55844911