



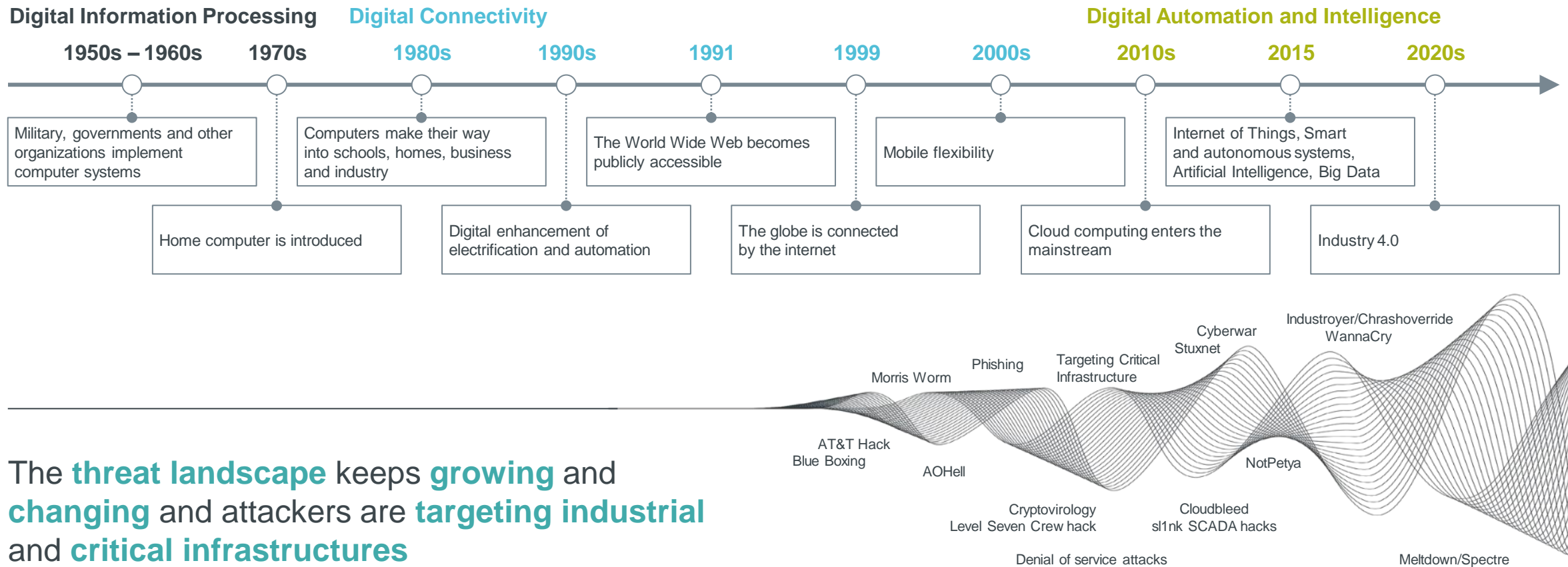
**SIEMENS**  
*Ingenuity for life*

# Cybersecurity for OT

© Siemens 2020

[www.siemens.com/industrial-security-services](http://www.siemens.com/industrial-security-services)

# Evolution of the cyber threat landscape



The **threat landscape** keeps **growing** and **changing** and attackers are **targeting industrial** and **critical infrastructures**

# Challenges are similar but reality is very different in IT and Industrial (OT) Security

## IT Security

Confidentiality

3-5 years

Forced migration (e.g. PCs, smart phone)

High (> 10 “agents” on office PCs)

Low (mainly Windows 10)

Standards based (agents & forced patching)

Asset lifecycle

Software lifecycle

Options to add security SW

Heterogeneity

Main protection concept

## Industrial Security

Availability and Safety

20-40 years

Usage as long as spare parts available

Low (old systems w/o “free” performance)

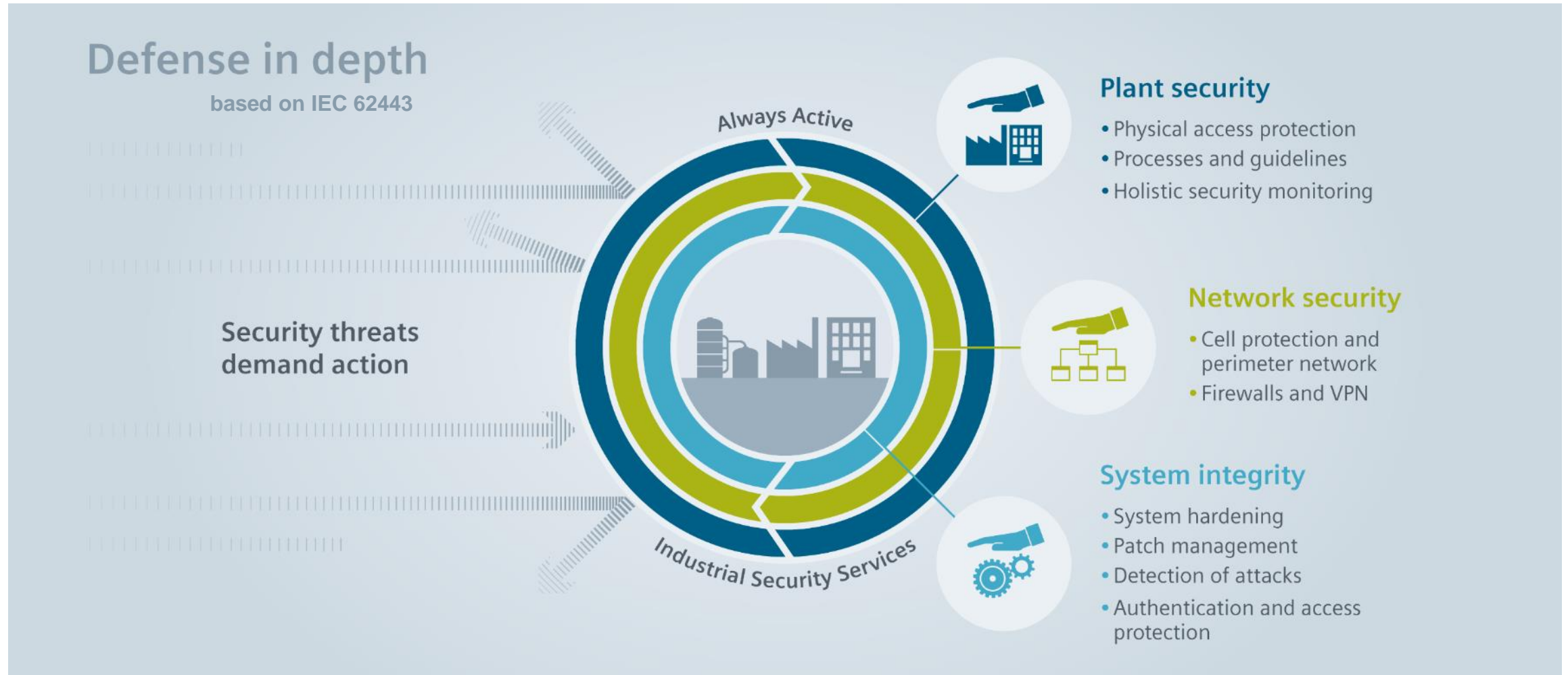
High (from Windows 95 up to 10)

Case and risk based



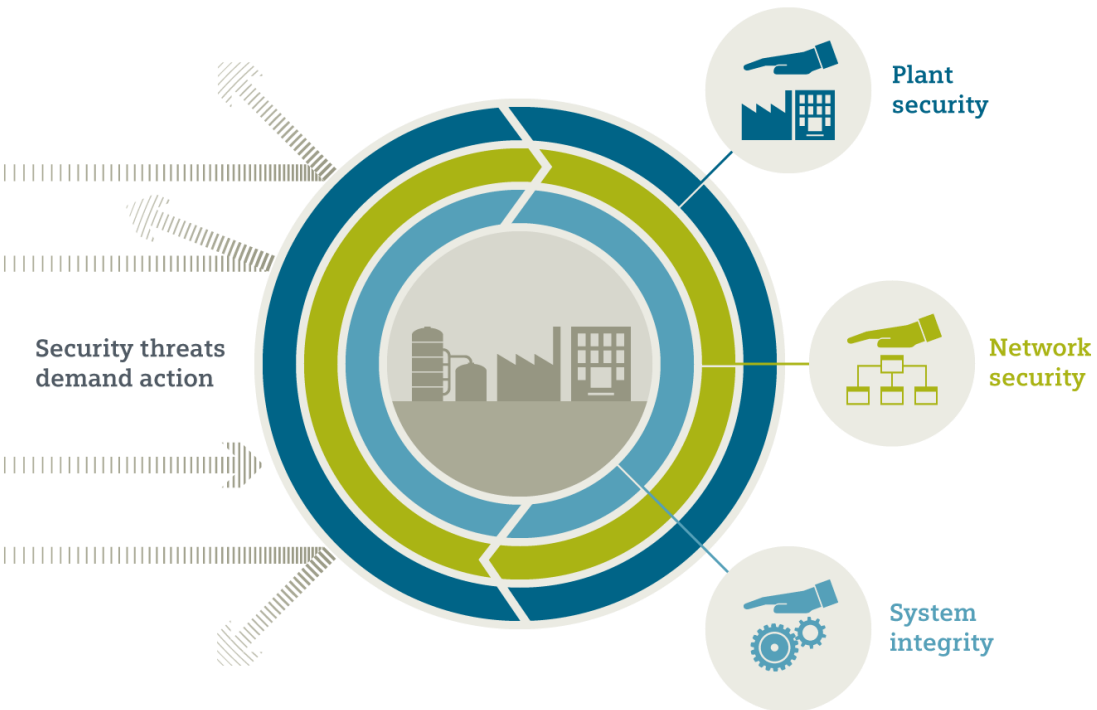
# Industrial Security concept

## Defense in depth – based on IEC 62443



# Industrial Security concept

## The security concept – “Defense in depth”



## Products and systems offer integrated security



Know-how and copy protection



Authentication and user management



Firewall and VPN

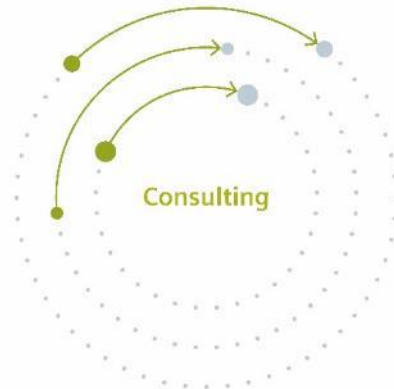


System hardening, continuous monitoring and anomaly detection

## Siemens Industrial Security Services



# Industrial Security Services End-to-end approach



## Security Consulting (Planning)

*Evaluation of the current security status of an industrial environment*

- Security Assessments
- Scanning Services
- Industrial Security Consulting

## Security Implementation

*Risk mitigation through implementation of security measures*

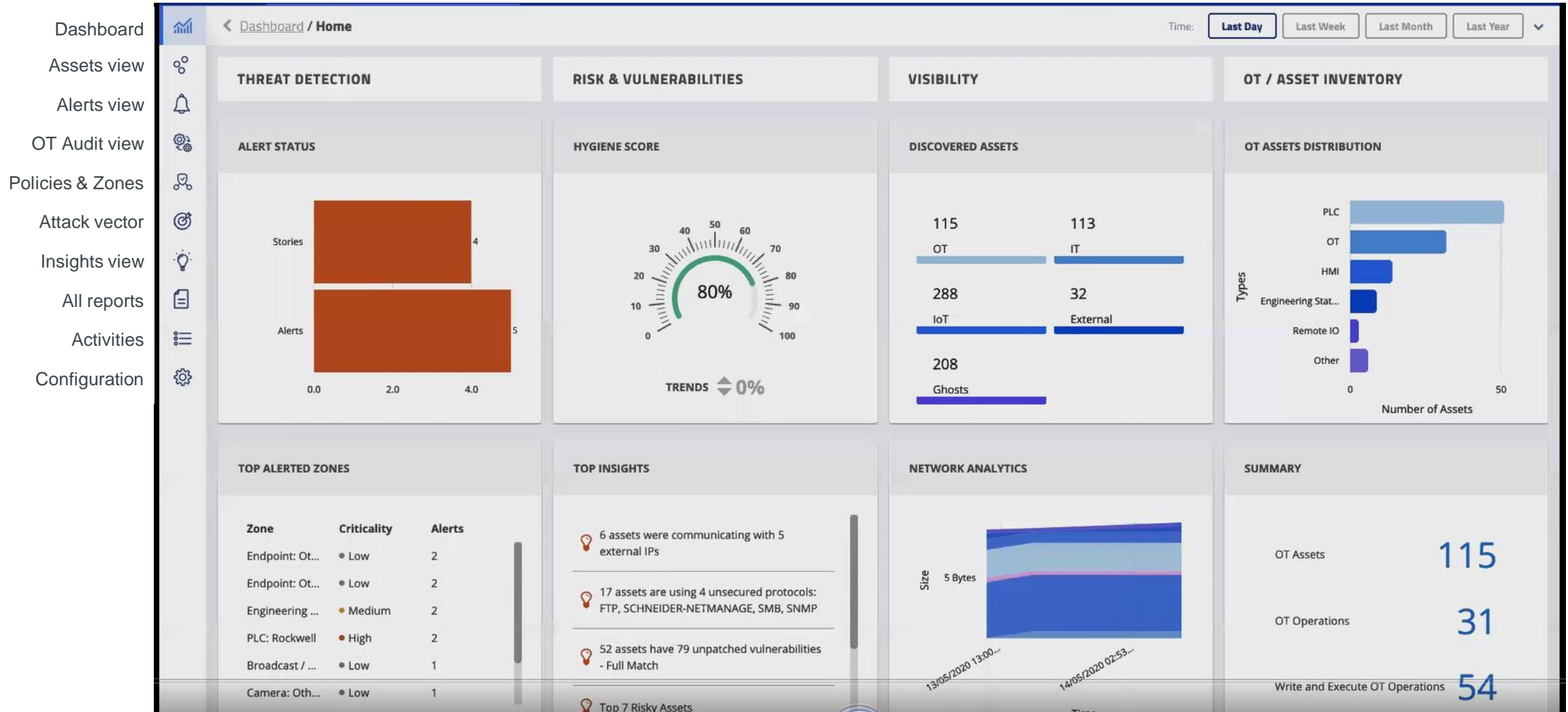
- Security Awareness Training
- Automation Firewall
- Endpoint Protection

## Security Optimization (Monitoring)

*Comprehensive security through managed services*

- Industrial Anomaly Detection
- Industrial Security Monitoring
- Remote Incident Handling
- Industrial Vulnerability Manager
- Patch Management

# Industrial Anomaly Detection Dashboard



# Industrial Anomaly Detection

## Assets view / Network Graph



Viewing: Default

CLAROTY



admin



Network View

View Type



Presets

Custom



Reset

Class  
1 Item Selected.

Type  
Select Type...

Vendor  
1 Item Selected.

Protocol  
Select Protocol...

Criticality  
Select Criticality...

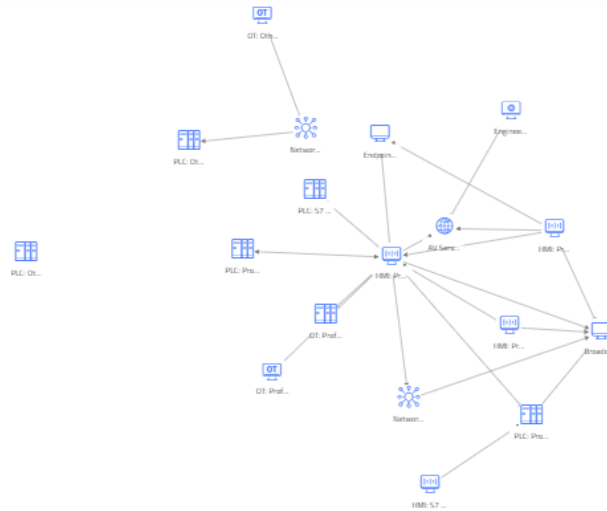
Search By  
Name, IP, Version, Model, Mac ...

Filter By Class: OT Vendor: Siemens

[CLEAR ALL](#) | [QUERY VIEW](#) | [ADVANCED OPTIONS»](#) | [GRAPH OPTIONS»](#)



ASSET RESULTS (18)





# Industrial Anomaly Detection Alerts view

Alerts View 1 Process Integrity Alerts 4 Security Events Alerts

View Type



Events

Uncollapse Alerts by Story

Status

1 Item Selected. ▼

Type

Select One or More. ▼

Category

Select One or More. ▼

Search By

Asset, Description...

Time

1hr.

D.

W.

M.



Severity

Critical

High

Medium

Low

Filter By

Status: Unresolved ×

CLEAR ALL | QUERY VIEW | ADVANCED OPTIONS»



RESULTS (4)



ID	SCORE	TYPE	DESCRIPTION	DATE DETECTED	CATEGORY	NETWORK	STATUS	ASSIGNED TO
Story Id 26 (score 100):		Configuration Download (2 alerts)	Host Scan (1 alert)	(Total 2)				
Story Id 19 (score 100):		Known Threat Alert (1 alert)	(Total 1)					
				1938 100	Configuration Download: Configuration Download critical change operation was performed for the first time by 10.1.30.40 with user: ENG_ABAAdministrator on 10.1.30.1 while related assets were managed remotely	17/01/21, 21:56	Integrity	Default Unresolved
Story Id 18 (score 100):		Known Threat Alert (1 alert)	(Total 1)					
Story Id 16 (score 100):		Known Threat Alert (1 alert)	(Total 1)					

# Industrial Anomaly Detection Insights view

Insights View View Type ☰ 🔗 💡 ↔️ 🌐 DNS Presets Custom ☰ ☁️ Reset

Class 1 Item Selected. Type Select Type... Vendor 1 Item Selected. Protocol Select Protocol... Criticality Select Criticality... Search By Name, IP, Version, Model, Mac ... 📈

Filter By Class: OT Vendor: Siemens CLEAR ALL QUERY VIEW ADVANCED OPTIONS» INSIGHTS OPTIONS»

**INSIGHTS (19)**

- 💡 Top 2 Risky Assets
- 💡 1 asset has 149 unpatched vulnerabilities - Windows Full Match
- 💡 4 assets were communicating with 3 external IPs (2 of them are ghost)
- 💡 1 asset is using 1 unsecured protocol: SNMP
- 💡 14 assets have 41 unpatched vulnerabilities - Full Match
- 💡 1 OT-asset performed privileged OT operations on 1 PLC/Controller/RTU/IED

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	AFFECTED ASSETS	ACTIONS
CVE-2019-1182	9.8	Remote Desktop Services Remote Code Execution Vulnerability	12/08/19 21:00	12/08/19 21:00	1 asset - click to filter	<ul style="list-style-type: none"> <li>✓ Mark All as Completed</li> <li>☑️</li> </ul>
CVE-2017-8589	9.8	Windows Search Remote Code Execution Vulnerability	10/07/17 21:00	10/07/17 21:00	1 asset - click to filter	<ul style="list-style-type: none"> <li>✓ Mark All as Completed</li> <li>☑️</li> </ul>

## Contact Information



### Carlos Campos

Digital Portfolio Specialist

RC-BR DI DES

Industry Lifecycle Services

[campos.carlos@siemens.com](mailto:campos.carlos@siemens.com)

Phone: + 55 11 99653-6482

