

NIS2 for Real Estate and Smart Infrastructure

Cybersecurity



**Cybersecurity:
A major concern for different
industries**

Building automation giant Johnson Controls hit by ransomware attack

By Lawrence Abrams

September 27, 2023 03:48 PM 1



REUTERS®

World ▾

Business ▾

Markets ▾

Sustainability ▾

Legal ▾

Breakingviews

Technology ▾

Investigative

Autos & Transportation

Toyota to suspend packaging line after cyberattack on Japan port

Reuters

July 6, 2023 10:23 AM GMT+2 · Updated 5 months ago



TOKYO, July 6 (Reuters) - Toyota Motor ([7203.T](#)) plans to suspend operations at a packaging line for export-bound components on Friday, the automaker said on Thursday, after a cyberattack at Japan's biggest port triggered a system glitch and stalled work for more than two days.

The port of Nagoya in central Japan, where Toyota exports most of its cars, was hit by a ransomware attack on Tuesday morning and was unable to load and unload containers from trailers.

Slovenia's largest power provider HSE hit by ransomware attack

By Bill Toulas

November 27, 2023 11:16 AM 0



U.S. NEWS

MGM Resorts computers back up after 10 days as analysts eye effects of

SIEMENS

Vulnerability exploitation

In among the main attack vectors

Cybercriminals

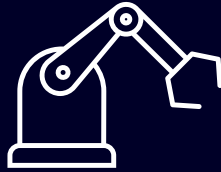
were responsible for

>95%

of attacks worldwide



Targeting **Manufacturing** sector in growing two digits y-o-y since **2019**,



...followed by

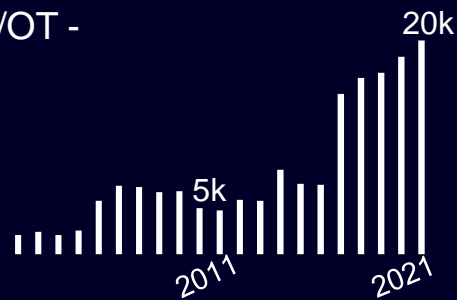


Ransomware and server-access accounted for

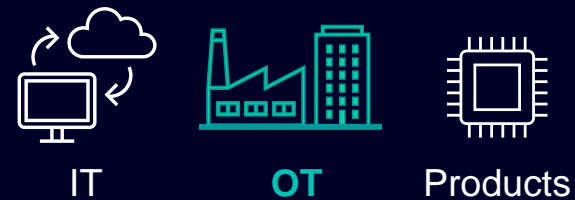
>85% of cases



Published vulnerabilities
- IT/OT -



Vulnerabilities are **everywhere**



Vulnerability exploitation

In among the main attack vectors

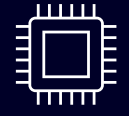
Vulnerabilities are everywhere



IT



OT



Products

Why we make a difference particularly in OT

Complexity: unthreads of vendors, 3rd party (software, automation, network, IIoT...)

Requirement: Quality of data, trusted information, combined information

Results: Reduced time to fix | mitigate

A threat landscape that is constantly changing and digitalization requires sustainable investments and tighter regulations

Increasing Digitalization

- Digital business models
- Digital Infrastructure

Changing Threat Landscape

- Threat Actors
- Digital Infrastructure

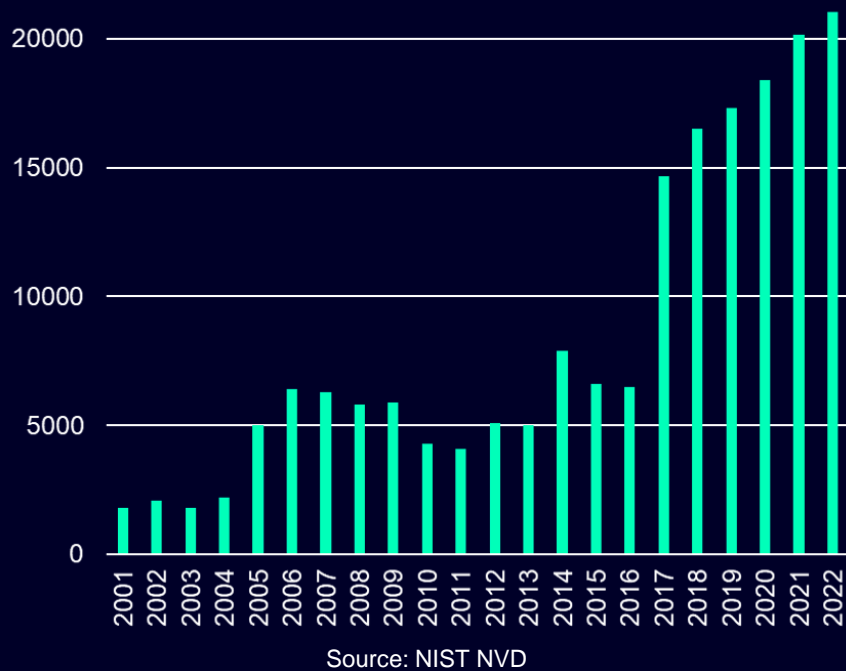
Increasing Regulations

- Products
- Critical Infrastructure

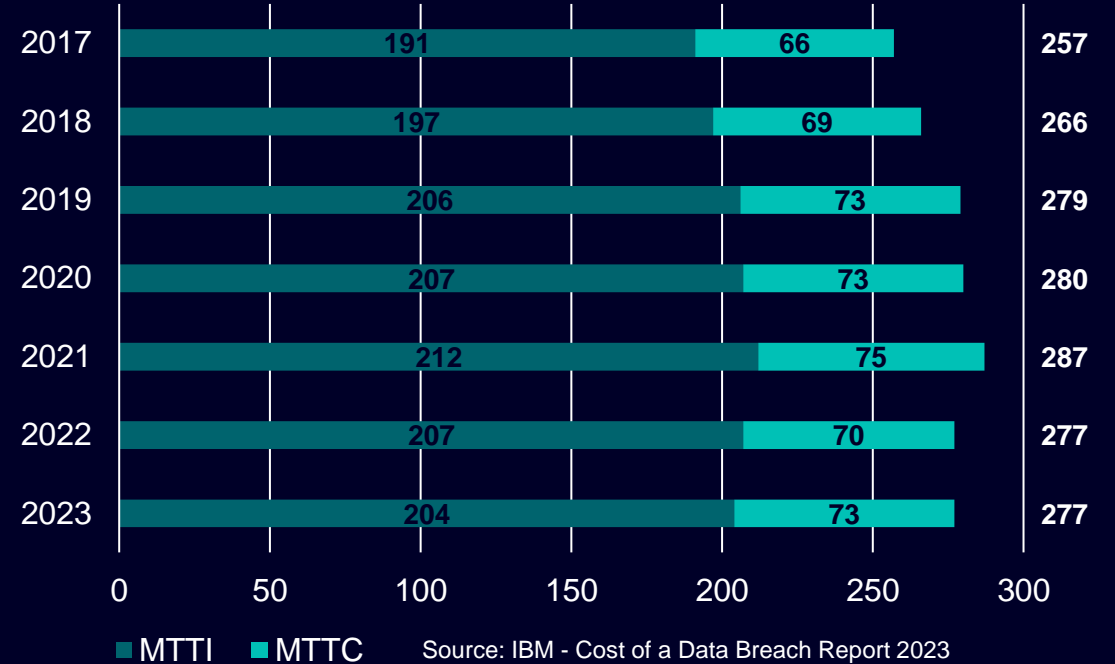
Threat Landscape and Drivers

Number of vulnerabilities and time to detect attacks are increasing

Growing number of vulnerabilities



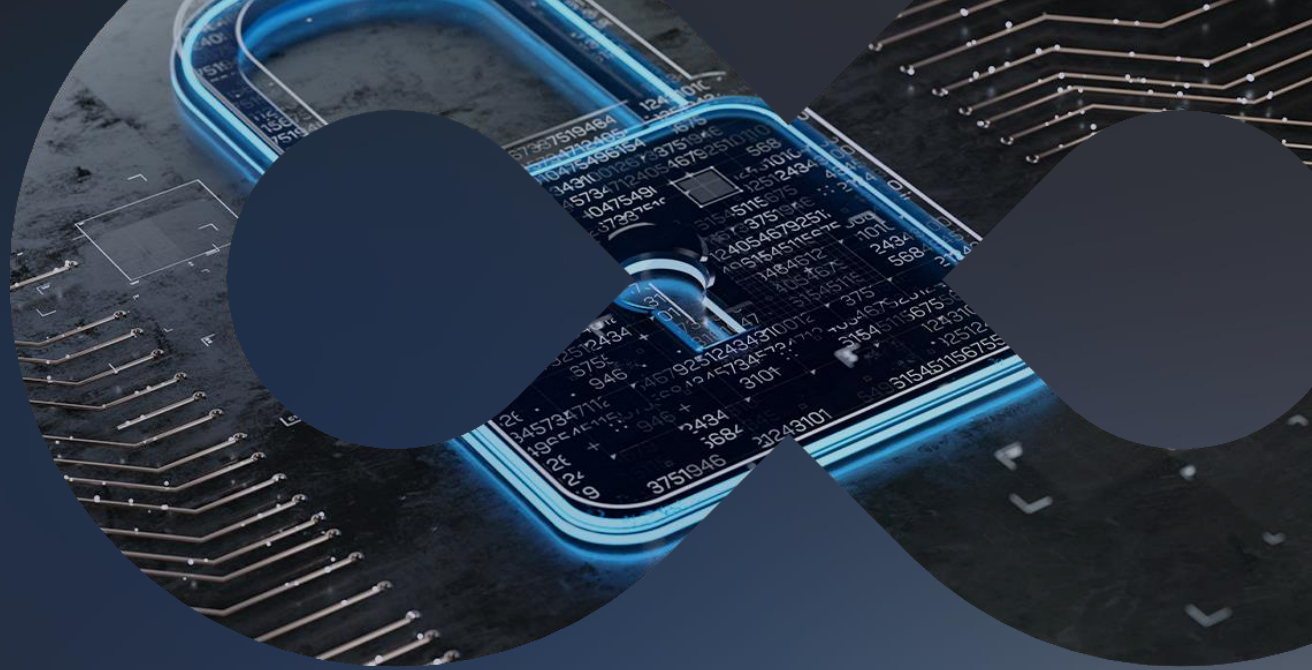
Time to identify and contain in days



+25k New vulnerabilities reported in 2022

+200 Days cyberattacks remain unnoticed

+70 Days to stop and contain a cyberattack



NIS2 regulations and their consequences

The world is changing...



NIS2

New legislation is happening



CIRCA and **SEC**-rules in **USA** will change the requirements on companies.

Cybersecurity in **Europa** – NIS 2 directive

Major changes in legislation with tougher requirements in **south east asia** with a start in 2022

Entities

Essential entities

(Sectors of High Criticality)

Included in Annex I
+ Annual turnover >€50 m

Fines:

Max. **€10 m up to 2%**
total worldwide annual turnover



On-site inspections and off-site supervision,
including random checks, and regular audits

Important entities

(Other Critical Sectors)

Included in Annex II
+ Annual turnover >€50 m

Fines:


Max. **€7 m up to 1.4%**
total worldwide annual turnover



On-site inspections and off-site ex post
supervision

Essential entities

Annex II¹

 **Energy** (electricity, remote heating and cooling, oil and gas)

 **Transport** (Air, rail, boat and road)

 Financial market infrastructure

 Banking


 Health including production of **pharmaceutical** products and vaccines

 **Drinking water**


Waste water 

New

New

 Digital infrastructure

New

Space 

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e32-143-1>

Important entities

Annex I¹

New



Postal- and courier services

New



Waste

New



Chemicals

New



Food



Manufacturing of **medical devices**, computers and electronics,

machine equipment, **motor vehicles**

New

Supplier of digital services

New



Research

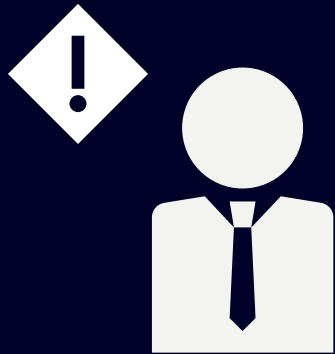


¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e32-143-1>

Management responsibilities

Management members

can be made personal responsible for damages



The **top management** of essential and important entities **must approve risk management** for cyber security, **must check compliance** and will be **responsible for insufficient compliance.**

Management must routinely complete specific training!

Cybersecurity risk management (CRM) obligations

Article 21 - Cybersecurity risk management measures

Measures shall at least
cover*

* Technical measures and other requirements will be defined by local regulators



Reporting obligations

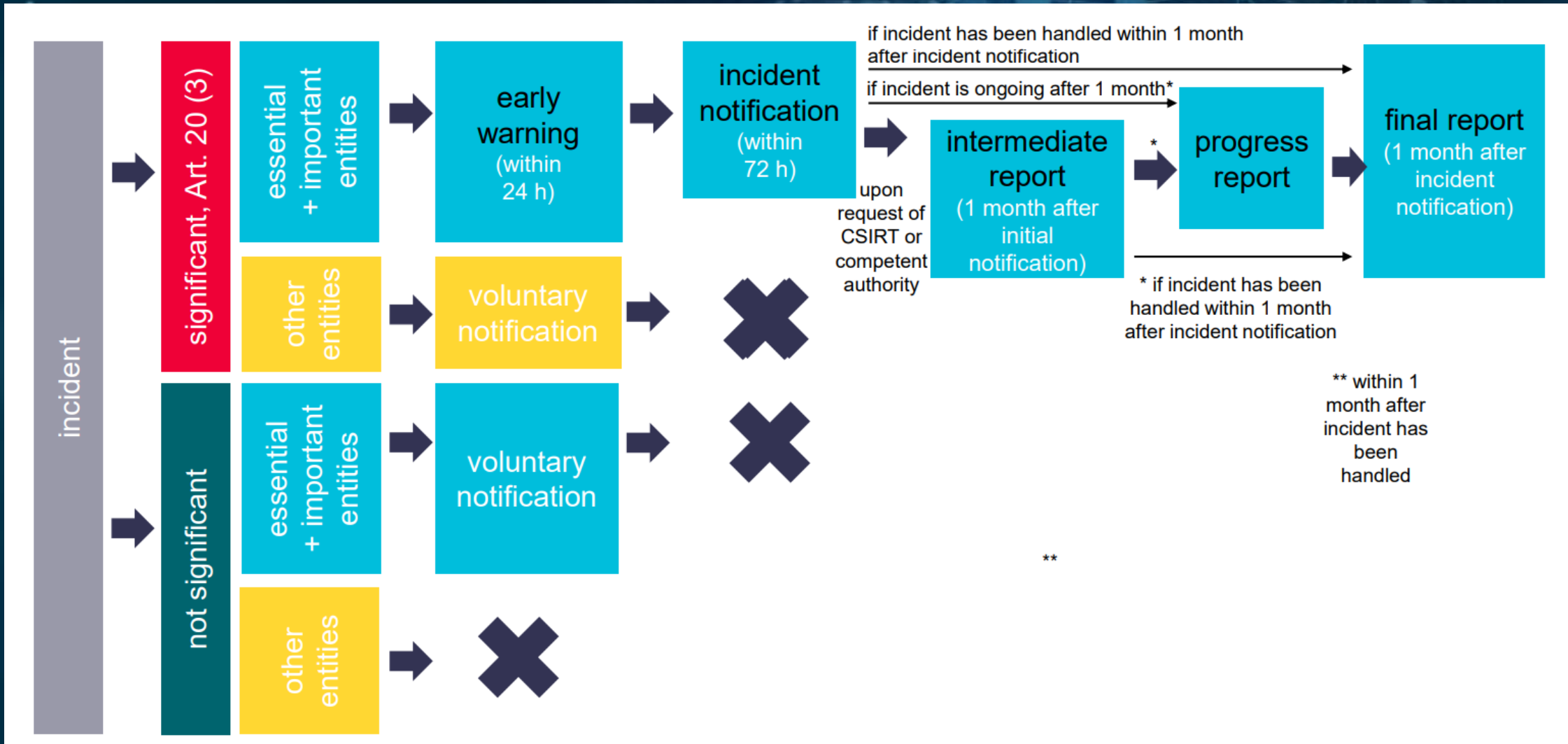
- Essential / important entities must **notify significant incidents** to the CSIRT / competent authority (in Germany: BSI) as follows:

	By when?	Content
early warning	without undue delay , in any event within 24 h after having become aware of the incident	information whether the significant incident is presumably caused by unlawful / malicious action or could have a cross-border impact
incident notification	without undue delay , in any event within 72 h after having become aware of the incident	<ul style="list-style-type: none">❖ update of the information of the early warning❖ initial assessment of the incident, its severity + impact, and, where available, the indicators of compromise
intermediate report	upon request of CSIRT / competent authority	relevant status updates
final report	not later than 1 month after incident notification	<ul style="list-style-type: none">❖ detailed description of the incident, its severity + impact;❖ type of threat / root cause that likely triggered the incident;❖ applied + ongoing mitigation measures;❖ where applicable, the cross-border impact of the incident

In cases of **ongoing incidents** at the time of the submission of the final report:

➔ **progress report** at that time + **final report within 1 month after the incident has been handled.**

Incident reporting



Remote Access

Asset
Inventory
Scan

Assessment

Firewalls

End Point
Protection

Risk
Awareness

How can we
support you

Whitelisting

DMZ

Patch
Management

Anomaly
Detection

Network
Monitoring & Management

Network
Segmentation

Cybersecurity step by step

Phases of the Journey

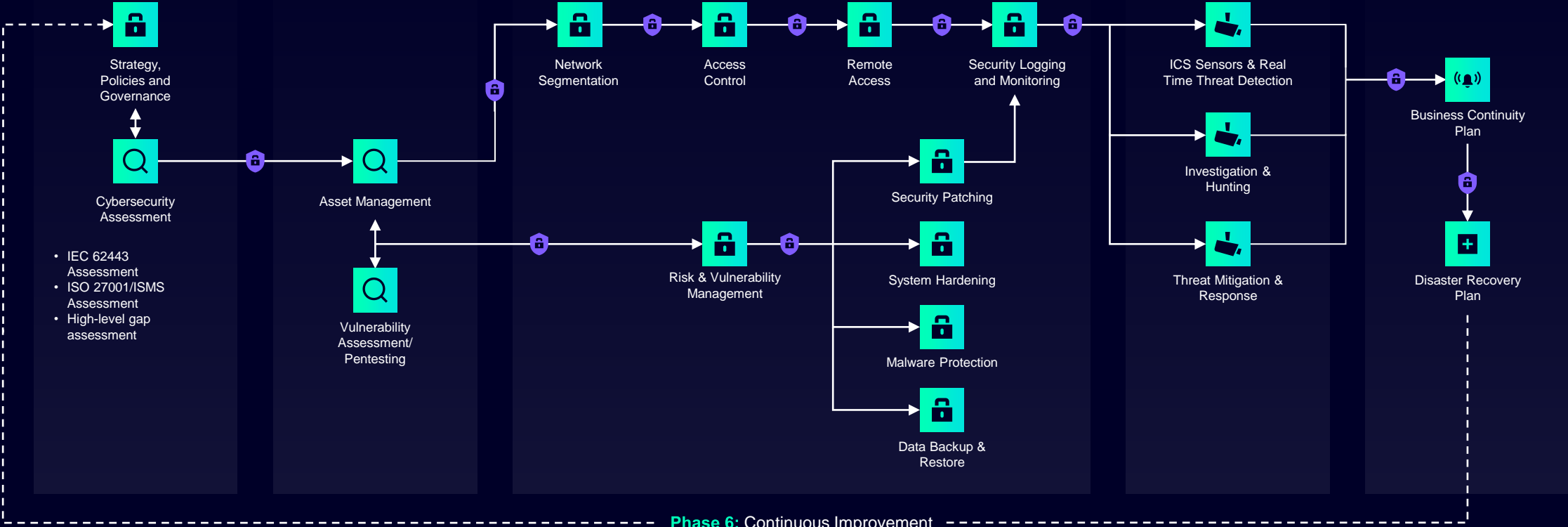
Phase 1
Where do I stand?
Where do I want to go?

Phase 2
Where do I start?
Which are my critical assets?

Phase 3
How can I protect my critical assets?
How do I secure my overall environment?

Phase 4
How do I know if my security controls are working?

Phase 5
What do I do in case of a cyber attack?



🔍 Identify
🔒 Protect
📡 Detect
🛡️ Defense
🛠️ Recover
🧠 Training, Simulations and Awareness

Proactive way of working



With our own **Cyber Emergency Response Team (CERT)**, we can uphold the highest possible level of protection for our own factories and our customers factories and sites





Operational Guidelines for Industrial Security

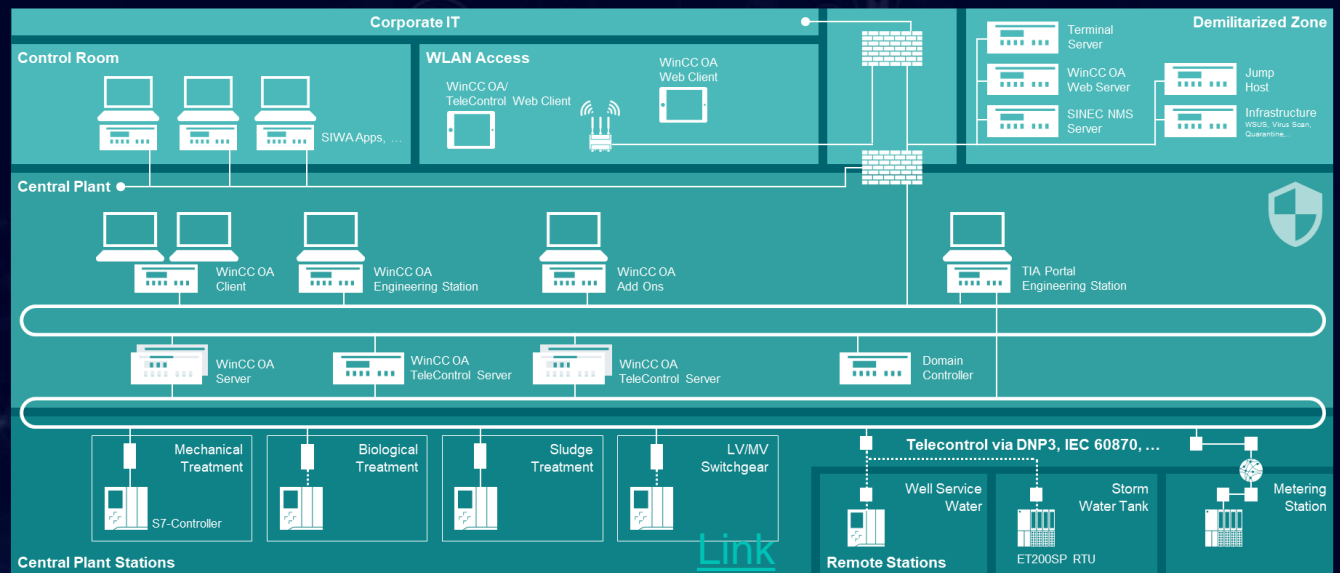
© Siemens 2020 Version 2.1



Industrial Edge Security Guidelines

A comprehensive guide to secure your Edge solution

Unrestricted | © Siemens 2021



SIEMENS

Security information 1

Preface 2

SIMATIC

What's new? 3

Process Control System PCS 7 Compendium Part F - Industrial Security (V9.1)

Security strategies 4

Configuration Manual

Network security 5

System hardening 6

User Administration and Operator Permissions 7

Patch management 8

Protection against malware using virus scanners 9

Backing up and restoring data 10

Disposal of systems and components 11

Remote access 12

Definitions and Abbreviations 13

Service and support 14

PCS7 Compendium F

Valid for PCS 7 V9.1



Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices



SIMATIC WinCC Unified V16
SIMATIC HMI Unified Comfort Panels

<https://support.industry.siemens.com/cs/ww/en/view/109481300>

Siemens Industry Online Support







Available reference architecture



Secure Reference Architecture

Discrete Manufacturing Network

<https://support.industry.siemens.com/cs/ww/en/view/109802750>





Security Blueprint for a Food and Beverage Production Plant


Application Example for a Bakery Plant

Guideline for Secure Configuration V1.0

<https://support.industry.siemens.com/cs/ww/en/view/109816864>




Ingenueity for Life




PCS 7 Blueprint for a Waste Water Treatment / Water Treatment / Desalination Plant

Guideline for Secure Configuration





Ingenueity for Life



Network concepts for factory automation

SIMATIC S7, SCALANCE X/M/S, SIMATIC HMI

<https://support.industry.siemens.com/cs/ww/en/view/109802750>





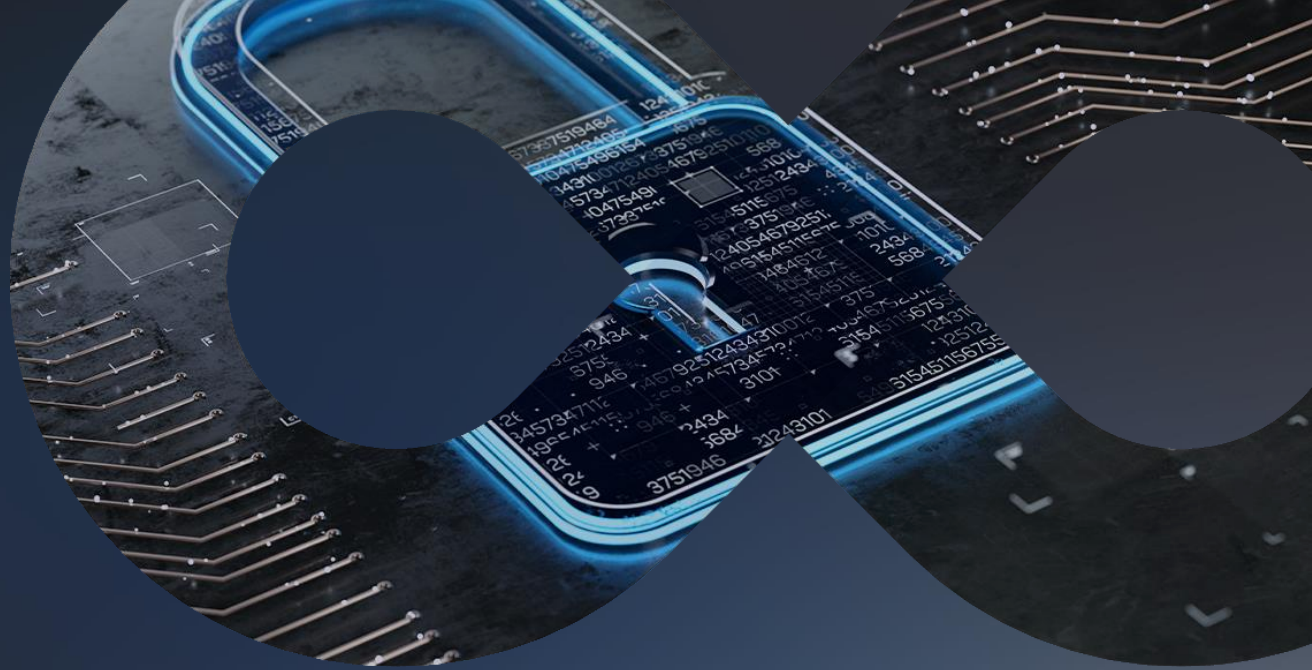
If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you.

Stephane Nappo

Global Head Information Security for
Société Générale International Banking pole



SIEMENS



NIS2 experiences and concrete steps ahead

A holistic Cybersecurity approach is guided by three main pillars People, Technology and Processes



A holistic security protection concept has to include technology, processes and people

What is needed to do?

1. Identify your critical infrastructure

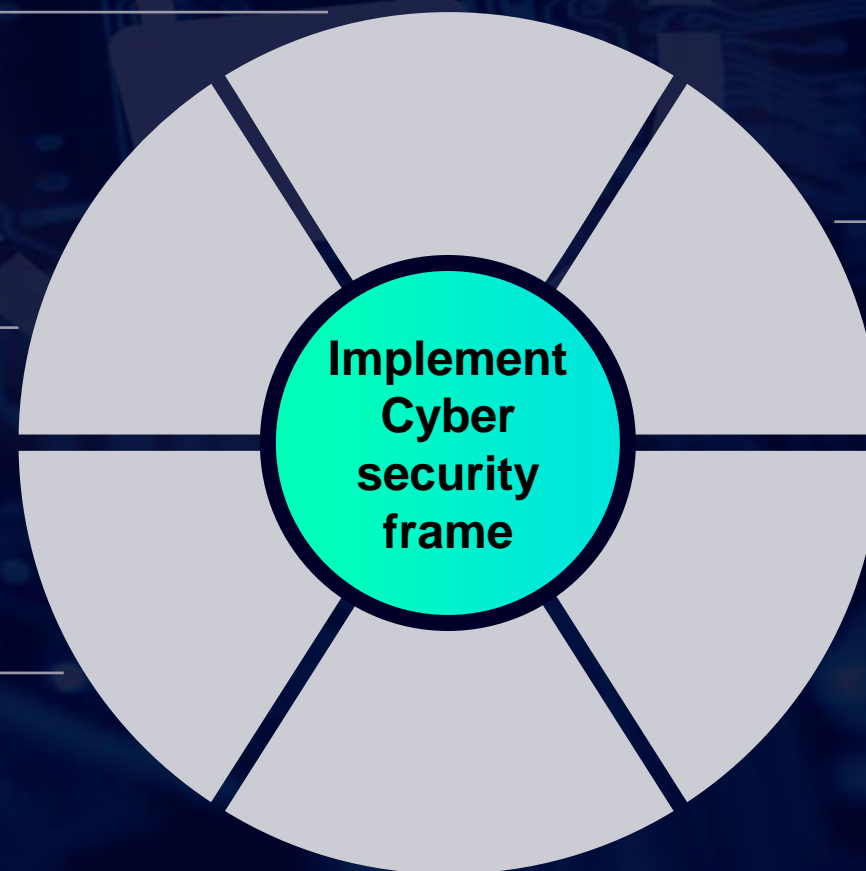
2. Develop an incident response & disaster recovery plan

3. Conduct regular security assessments

4. Keep your software up to date

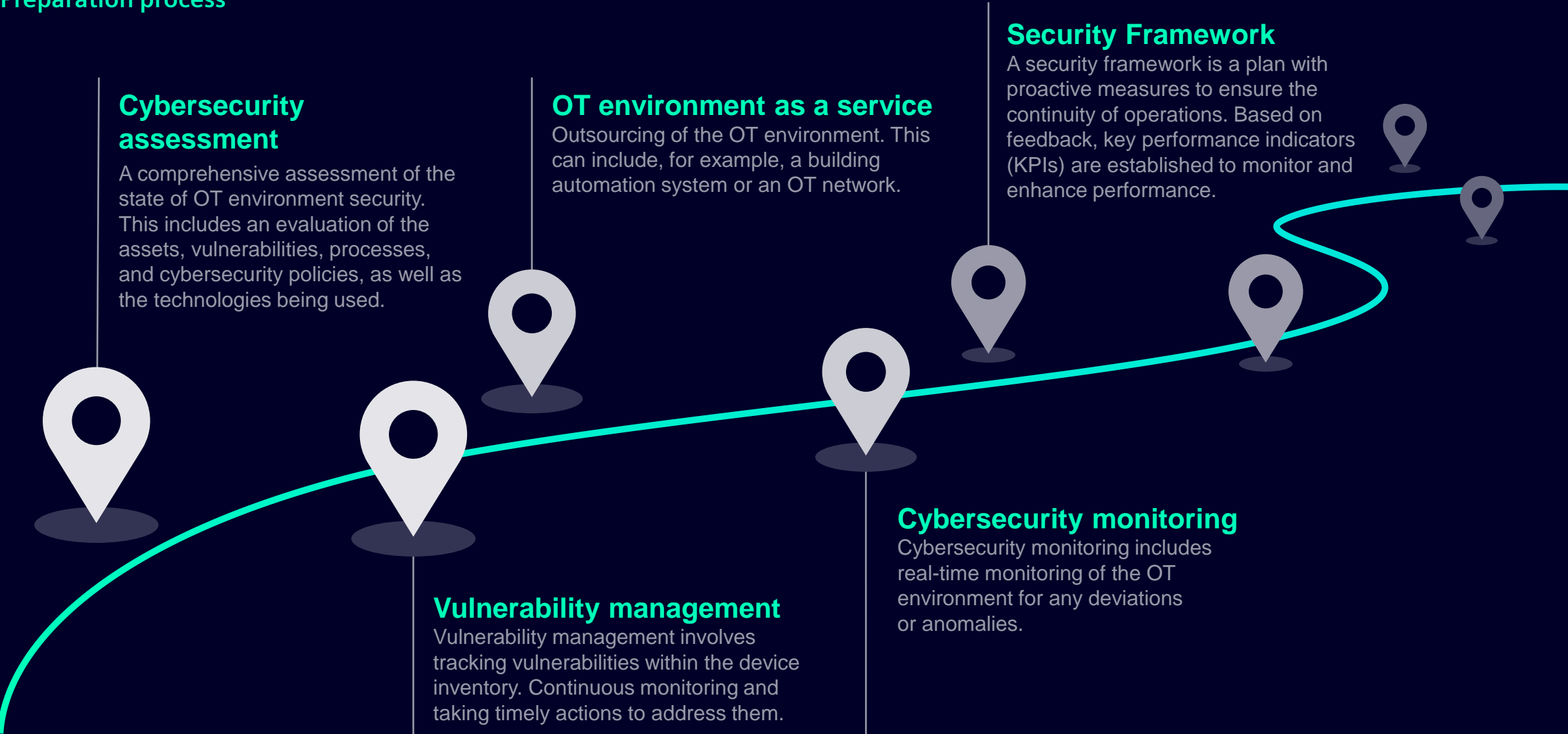
5. Train your employees

6. Monitor your network for anomalies:



The OT security customer journey

Preparation process



Cyber Security assesment steps

Define coverage

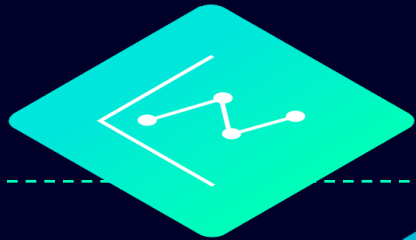
Define coverage of the assessment.

Visual inspection

Site visit with short tour around facility.

Thread and Risk Analysis

Analyze findings and compare the status of the environment to NIS2, ISO27001, IEC62443.



Interview

Interview for the personnel working daily in the OT environment.

Tool assisted inspection

OT-network scanning to have a accurate view on assets connected and possible vulnerabilities.

Report and improvement measures

Report of the state of environment and possible improvement mesures.

What shortcomings have we discovered?

Commonly known passwords

Passwords that are commonly used in the past.

Cyber Security awereness

Missing training and attitude towards topic.

Windows server never being updated

WLAN reachable outside of the building

No knowledge of assets in OT-environment

Service relations

Unclear responsibilities.

Contact



Jani Hämäläinen

Head of IT and Digital services,
Smart buildings
Siemens Finland

 [LinkedIn](#)




Mobile +358 504695066

E-mail jani.hamalainen@siemens.com



Michael Dufva

Chief information and Security officer
Siemens Nordic

 [LinkedIn](#)



Mobile +46 707281628

E-mail michael.dufva@siemens.com



Mithra Pakdaman Kiasat

Branch Manager
Smart Infrastructure
Siemens Sweden

 [LinkedIn](#)



Mobile +46 702198807

E-mail mithra.kiasat@siemens.com

THANK YOU