Cybersecurity Becomes Law, Are You Ready?

- Lesson learned from the most destructive cyberattack
- What is NIS2 and how will it affect you?
- What should you do?
- Phoenix Contact as an example

Jiunn-Jer Sun

Network & Cybersecurity

Approved specialist by TÜV Rheinland Cyber Security training program with 20-year experience in industrial networking.

jsun@phoenixcontact.com

PHOENIX CONTACT
INSPIRING INNOVATIONS

Story: The Most Devastating Cyberattack

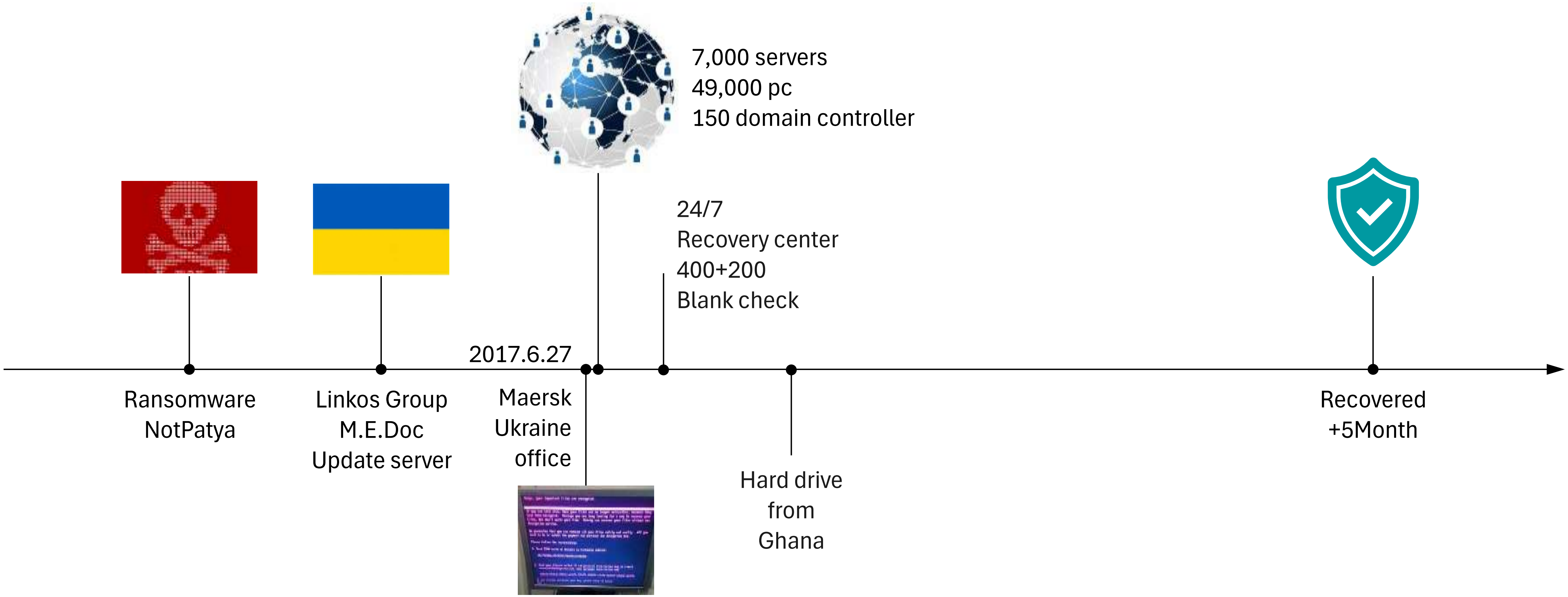
The Global Shipping and Logistics Giant

MAERSK

- Shipping, port operation, supply chain management and warehousing
- Copenhagen Danmark
- > 130 countries
- > 900 subsidiaries
- >105K employees
- > 51 Billion USD (2023)
- 174th largest public company in world
- Move 12 million containers every year

Story: The Most Devastating Cyberattack

The Giant Victim



Ransomware NotPatya

Linkos Group M.E.Doc Update server

2017.6.27

Maersk Ukraine office

7,000 servers
49,000 pc
150 domain controller

24/7
Recovery center
400+200
Blank check

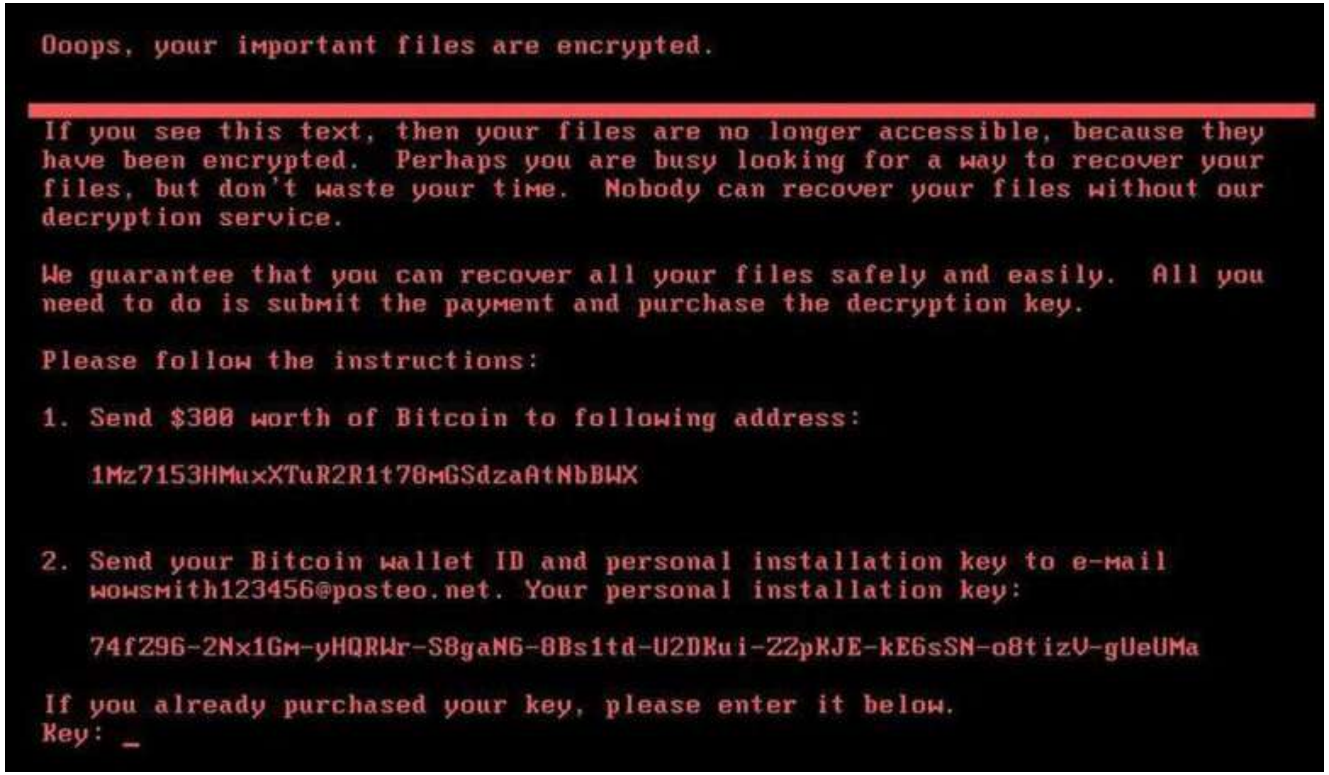
Hard drive from Ghana

Recovered +5Month

Story: The Most Devastating Cyberattack

Wide and Devastating

870M USD	Pharmaceutical company Merck
400M USD	Delivery company FedEx
384M USD	French construction company Saint-Gobain
300M USD	Danish shipping company Maersk
188M USD	Snack company Mondelēz
129M USD	British manufacturer Reckitt Benckiser
…	
10B USD	Total damages Estimated by the White House



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

Story: The Most Devastating Cyberattack

What we learn from the story?

- Awareness & Leadership
- Unexpected, accidentally, unfortunately, …
- From somewhere else (country, supplier)
- Backup and recovery plan (offline backup)
- Business continuity plan

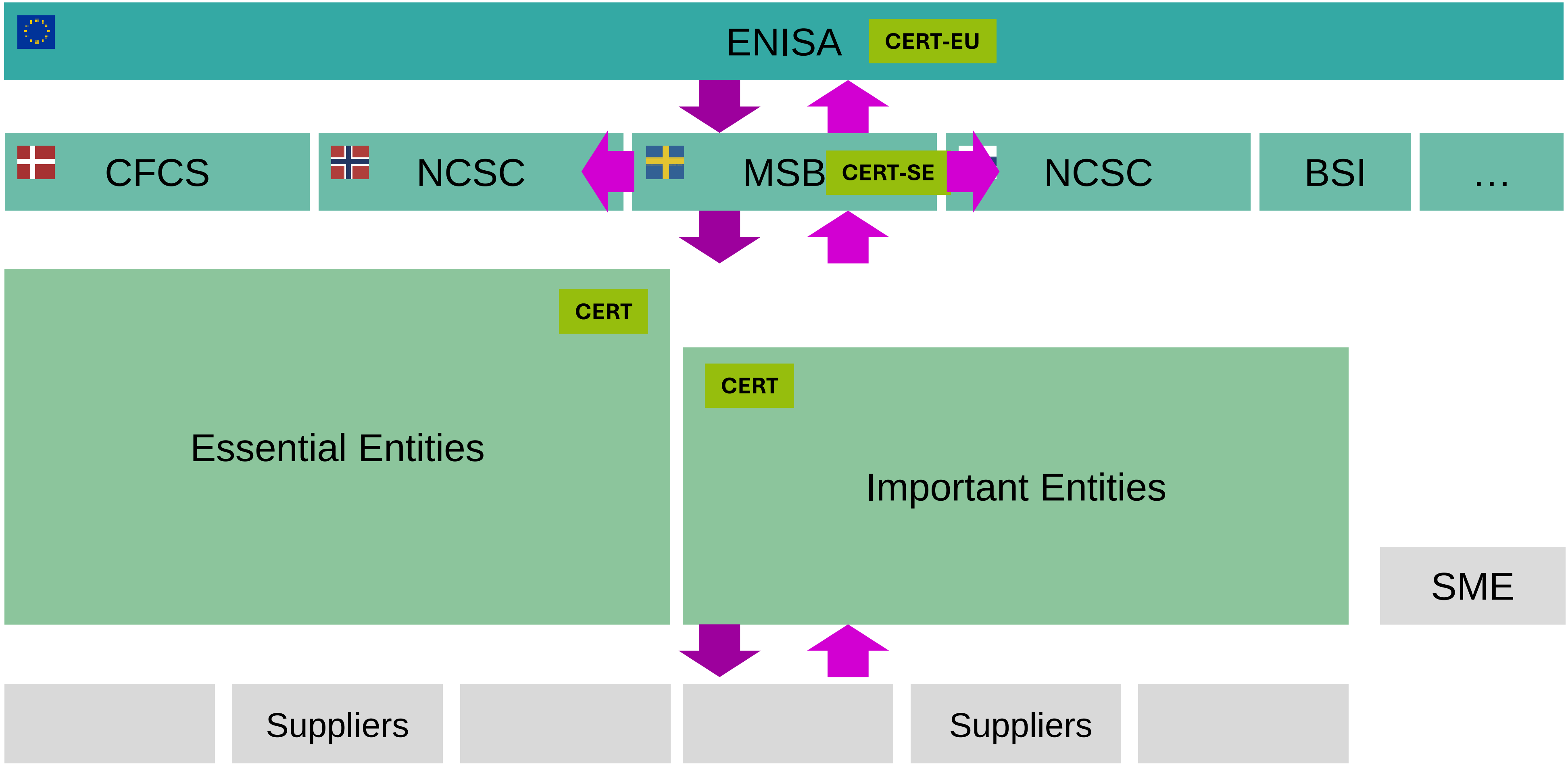
Cybersecurity becomes law

NIS2 Directive

- Network and Information Security, version 2
- EU Directive: defines the minimum national requirements and needs to be implemented into national law
- What’s new?
  - Increase collaboration
  - Wider scope of coverage
  - Strengthen security requirements
  - Incident reporting obligations
  - Enforcements

NIS2 directive

Increase Collaboration



ENISA CERT-EU

CFCS

NCSC

MSB CERT-SE

NCSC

BSI

...

CERT

Essential Entities

CERT

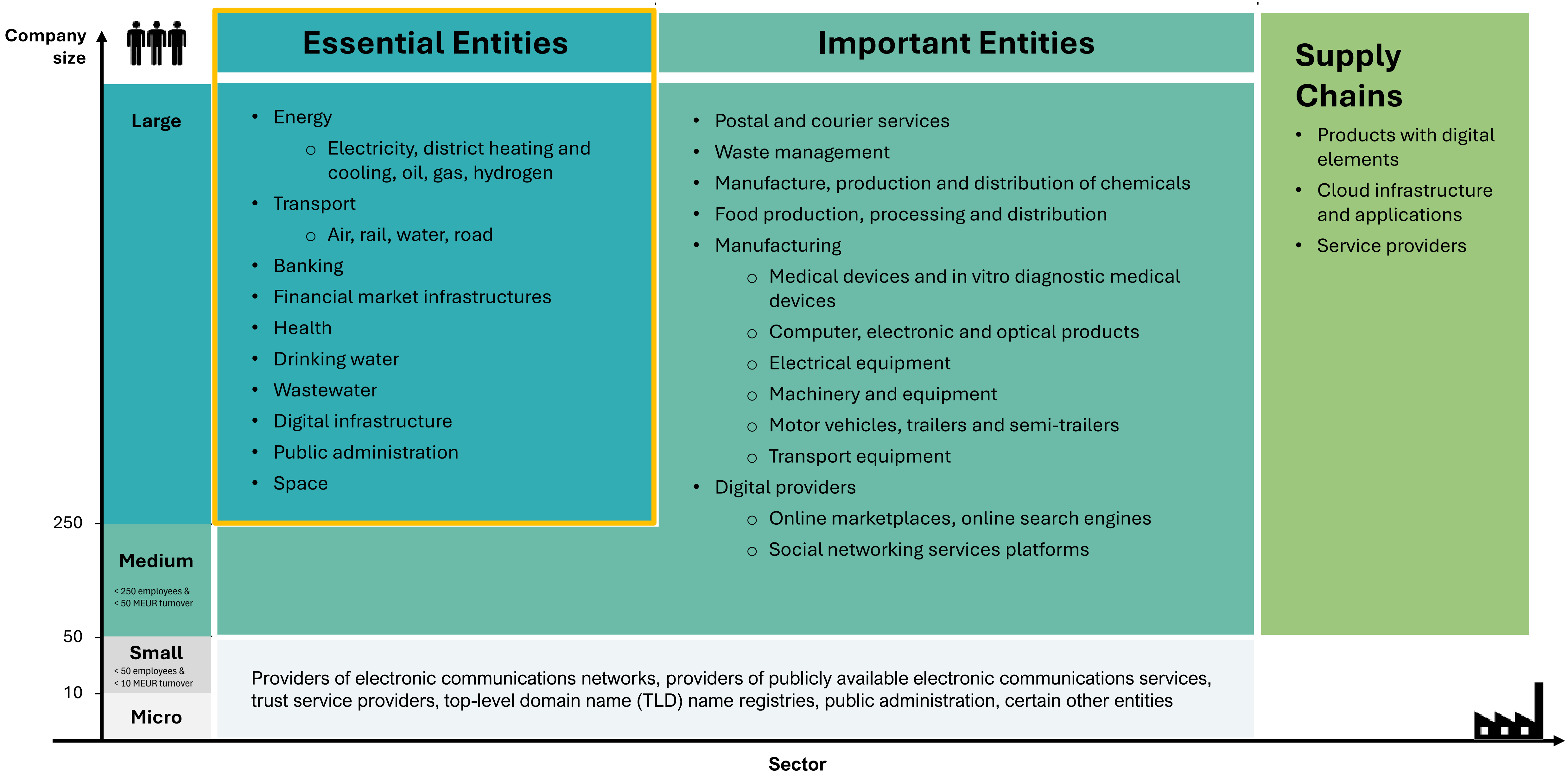
Important Entities

SME

Suppliers

Suppliers

Wider Scope of Coverage



Company size

Large

250

Medium

< 250 employees &
< 50 MEUR turnover

50

Small

< 50 employees &
< 10 MEUR turnover

10

Micro

Essential Entities

- Energy
  - Electricity, district heating and cooling, oil, gas, hydrogen
- Transport
  - Air, rail, water, road
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- Public administration
- Space

Important Entities

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Food production, processing and distribution
- Manufacturing
  - Medical devices and in vitro diagnostic medical devices
  - Computer, electronic and optical products
  - Electrical equipment
  - Machinery and equipment
  - Motor vehicles, trailers and semi-trailers
  - Transport equipment
- Digital providers
  - Online marketplaces, online search engines
  - Social networking services platforms

Supply Chains

- Products with digital elements
- Cloud infrastructure and applications
- Service providers

Providers of electronic communications networks, providers of publicly available electronic communications services, trust service providers, top-level domain name (TLD) name registries, public administration, certain other entities

Sector

NIS2 directive

Strengthen Security Requirements

CSMS (Cybersecurity Management System)

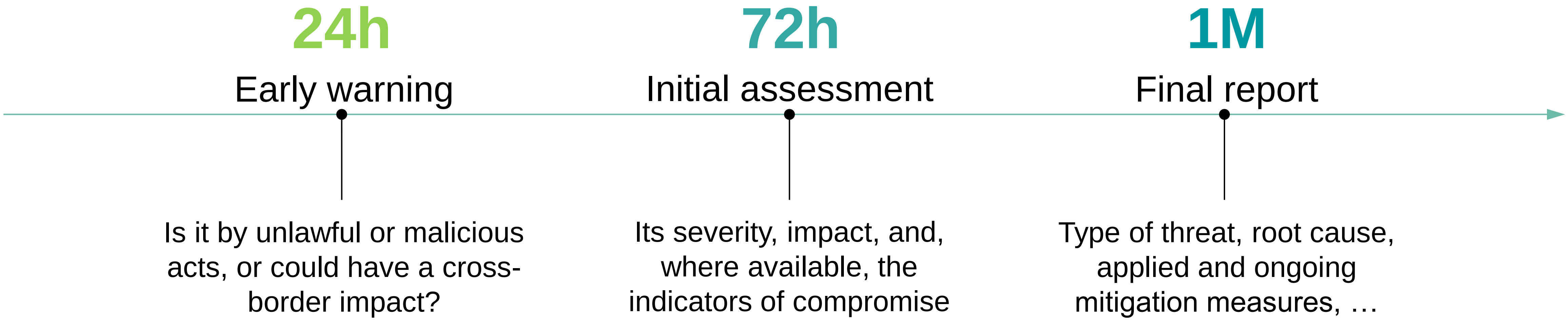
- Risk analysis and information systems security;
- Incident handling; prevention, detection and report of cyber incidents
- Business continuity, such as backup management and disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

- Assessment of the effectiveness of cybersecurity risk-management measures;
- Basic cyber hygiene practices and cybersecurity training;
- The use of encryption;
- Human resources security, access control and asset management;
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications

NIS2 directive

Incident Report Obligations

- Entities are obliged to report all **significant** cyber incidents
  - “it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned”, or
  - “it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.”



24h Early warning

Is it by unlawful or malicious acts, or could have a cross-border impact?

72h Initial assessment

Its severity, impact, and, where available, the indicators of compromise

1M Final report

Type of threat, root cause, applied and ongoing mitigation measures, …

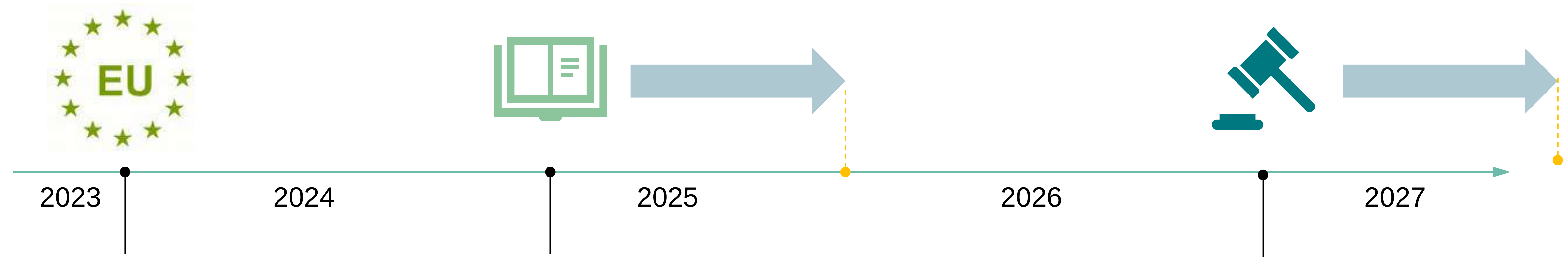
NIS2 directive

Enforcements – Fines and Sanctions

	Essential Entities	Important Entities
Fines	at least 10.000.000 €, or at least 2 % of the total worldwide annual turnover (whichever is higher)	at least 7.000.000 €, or at least 1,4 % of the total worldwide annual turnover (whichever is higher)
Sanctions	Management bodies of essential and important entities shall oversee the implementation and can be held liable for infringements	

NIS2 directive

Current Status



16 January 2023
Entry into force on
European level

18 October 2024
Implementation
into national law

2026/2027
Entry into force
on national level

Cybersecurity becomes law

What are the differences?

NIS2

Network & Information Security Directive, v2

Cybersecurity management in essential entities or important entities

CRA

Cyber Resilience Act

Product with digital element needs to be secure (securely designed, developed and maintained)

CER

Critical Entities Resilience Directive

Physical and cybersecurity threats to critical infrastructure and resilience

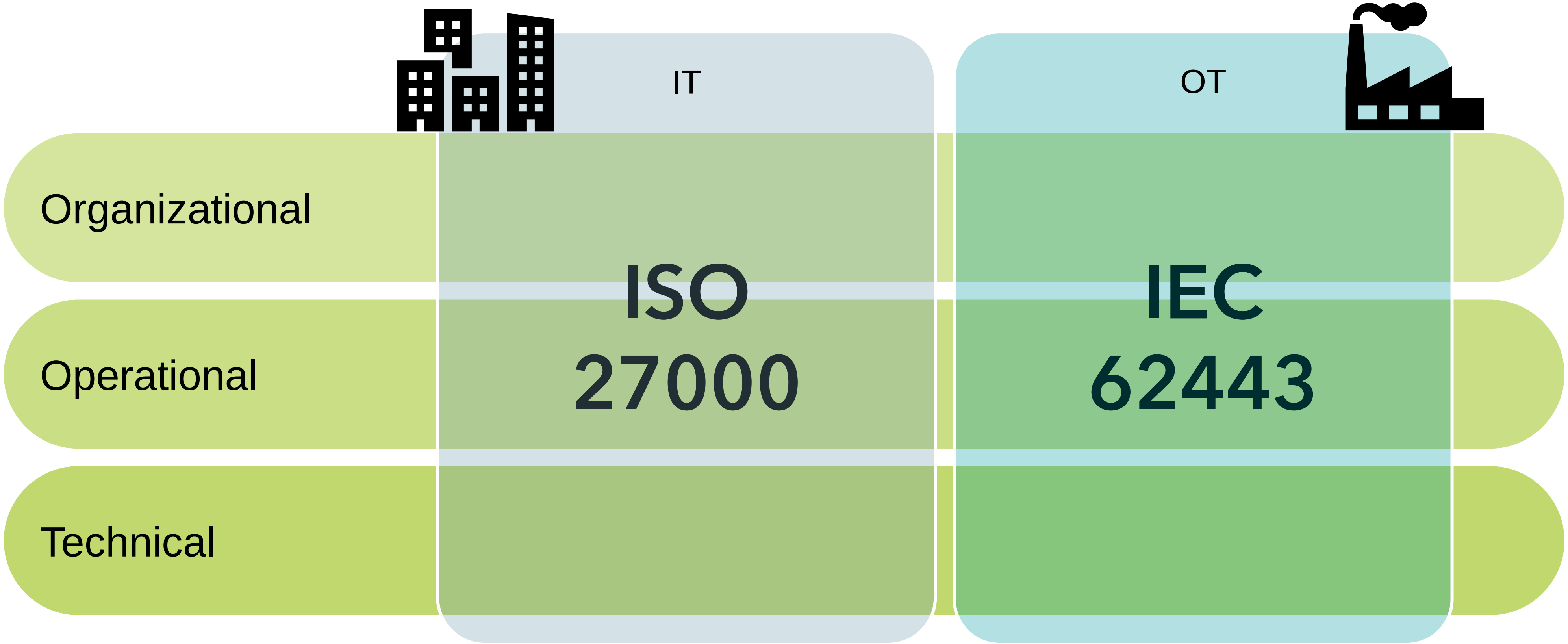
DORA

Digital Operational Resilience Act

IT security for financial entities such as banks, insurance companies and investment firms.

Are you ready?

Two Areas, Three Aspects



IT

OT

Organizational

Operational

Technical

ISO 27000

IEC 62443

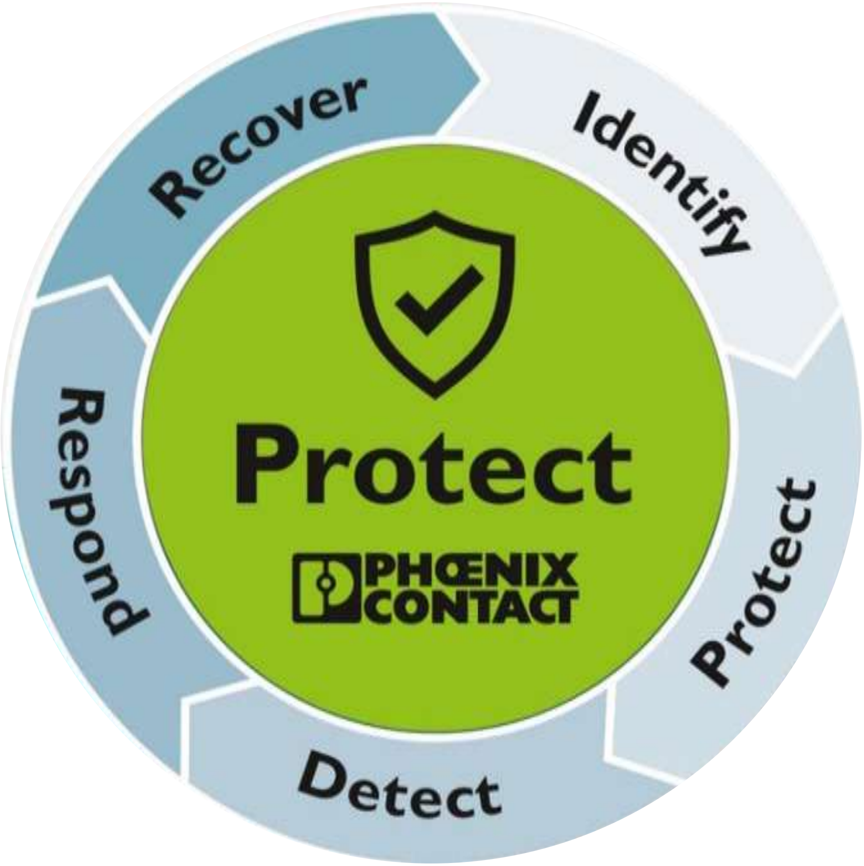
OT security standard

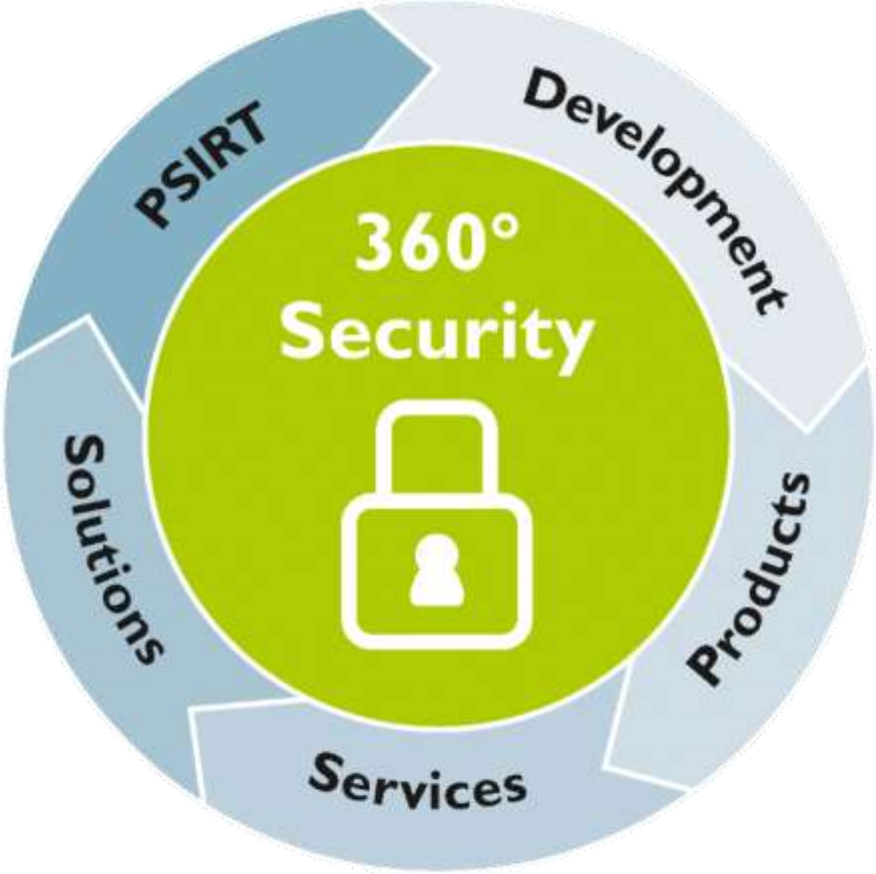
IEC62443

General	1-1 Technology, concepts, and models	1-2 Master glossary of terms and abbreviations	1-3 System security compliance metrics	1-4 System security lifecycle and use case	1-5 Rules for IEC62443 profiles	1-6 Application of the 62443 standards to industrial IoT
Policies & Procedures	2-1 Requirements for an IACS security management system	2-2 Security protection rating	2-3 Patch management in the IACS environment	2-4 Requirements for IACS solution providers	2-5 Implementation guidance for IACS asset owners	
System	3-1 Security technologies for IACS	3-2 Security risk assessment for system design	3-3 System security requirements and security levels			
Component	4-1 Secure product development lifecycle	4-2 Technical security requirements for IACS components				

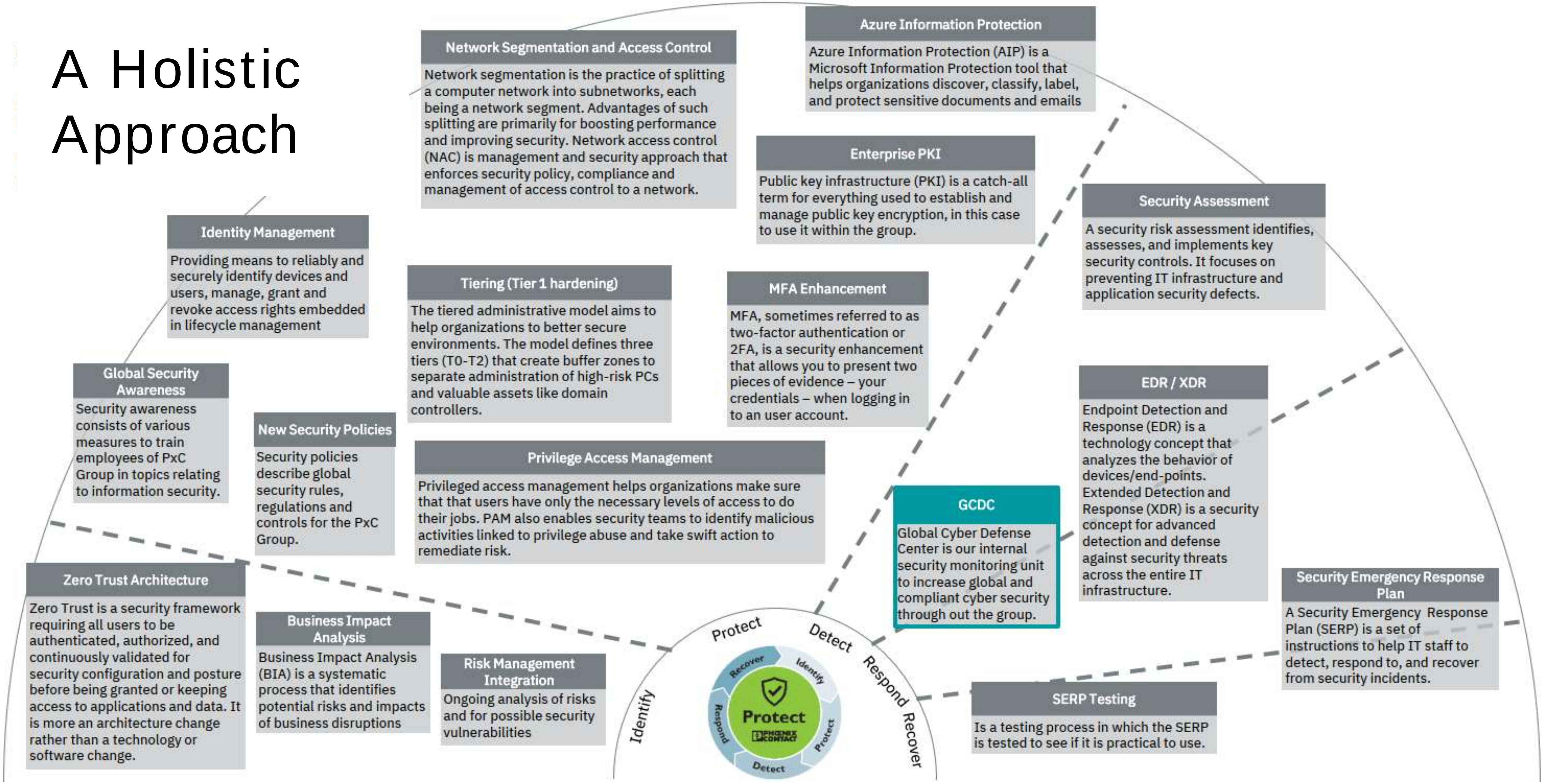
Cybersecurity in Phoenix contact

Your Most Trustworthy Supplier





A Holistic Approach



Zero Trust Architecture

Zero Trust is a security framework requiring all users to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. It is more an architecture change rather than a technology or software change.

Business Impact Analysis

Business Impact Analysis (BIA) is a systematic process that identifies potential risks and impacts of business disruptions

Risk Management Integration

Ongoing analysis of risks and for possible security vulnerabilities

Global Security Awareness

Security awareness consists of various measures to train employees of PxC Group in topics relating to information security.

Identity Management

Providing means to reliably and securely identify devices and users, manage, grant and revoke access rights embedded in lifecycle management

New Security Policies

Security policies describe global security rules, regulations and controls for the PxC Group.

Network Segmentation and Access Control

Network segmentation is the practice of splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security. Network access control (NAC) is management and security approach that enforces security policy, compliance and management of access control to a network.

Tiering (Tier 1 hardening)

The tiered administrative model aims to help organizations to better secure environments. The model defines three tiers (T0-T2) that create buffer zones to separate administration of high-risk PCs and valuable assets like domain controllers.

Privilege Access Management

Privileged access management helps organizations make sure that that users have only the necessary levels of access to do their jobs. PAM also enables security teams to identify malicious activities linked to privilege abuse and take swift action to remediate risk.

Azure Information Protection

Azure Information Protection (AIP) is a Microsoft Information Protection tool that helps organizations discover, classify, label, and protect sensitive documents and emails

Enterprise PKI

Public key infrastructure (PKI) is a catch-all term for everything used to establish and manage public key encryption, in this case to use it within the group.

MFA Enhancement

MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an user account.

Security Assessment

A security risk assessment identifies, assesses, and implements key security controls. It focuses on preventing IT infrastructure and application security defects.

EDR / XDR

Endpoint Detection and Response (EDR) is a technology concept that analyzes the behavior of devices/end-points. Extended Detection and Response (XDR) is a security concept for advanced detection and defense against security threats across the entire IT infrastructure.

GCDC

Global Cyber Defense Center is our internal security monitoring unit to increase global and compliant cyber security through out the group.

Security Emergency Response Plan

A Security Emergency Response Plan (SERP) is a set of instructions to help IT staff to detect, respond to, and recover from security incidents.

SERP Testing

Is a testing process in which the SERP is tested to see if it is practical to use.

Cybersecurity in Phoenix contact

High Management Team

[redacted]
Corporate Operational Technology Security Officer

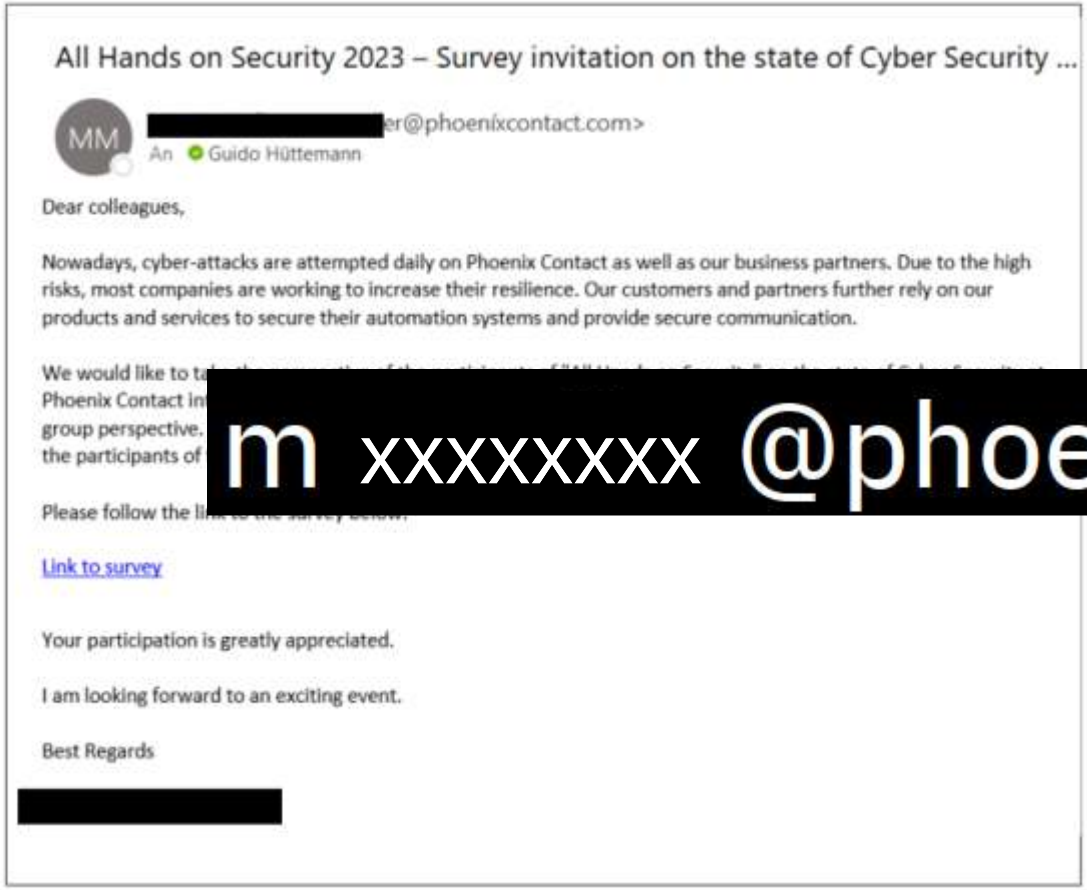
[redacted]
Product and Solution Security Officer

[redacted]
Program Management „Protect Phoenix Contact“

[redacted]
Corporate Information Security Officer (CISO)

Cybersecurity in Phoenix contact

Awareness Training



All Hands on Security 2023 – Survey invitation on the state of Cyber Security ...

MM [redacted]er@phoeníxcontact.com>

An Guido Hüttemann

Dear colleagues,

Nowadays, cyber-attacks are attempted daily on Phoenix Contact as well as our business partners. Due to the high risks, most companies are working to increase their resilience. Our customers and partners further rely on our products and services to secure their automation systems and provide secure communication.

We would like to ta
Phoenix Contact in
group perspective.
the participants of

Please follow the li

[Link to survey]

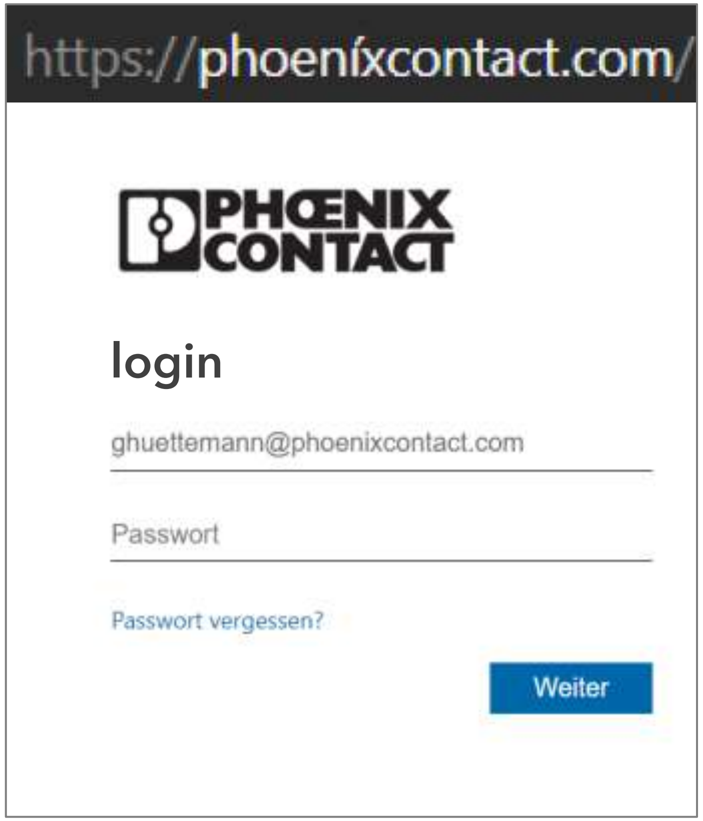
Your participation is greatly appreciated.

I am looking forward to an exciting event.

Best Regards

[redacted]

m xxxxxxxx @phoeníxcontact.com

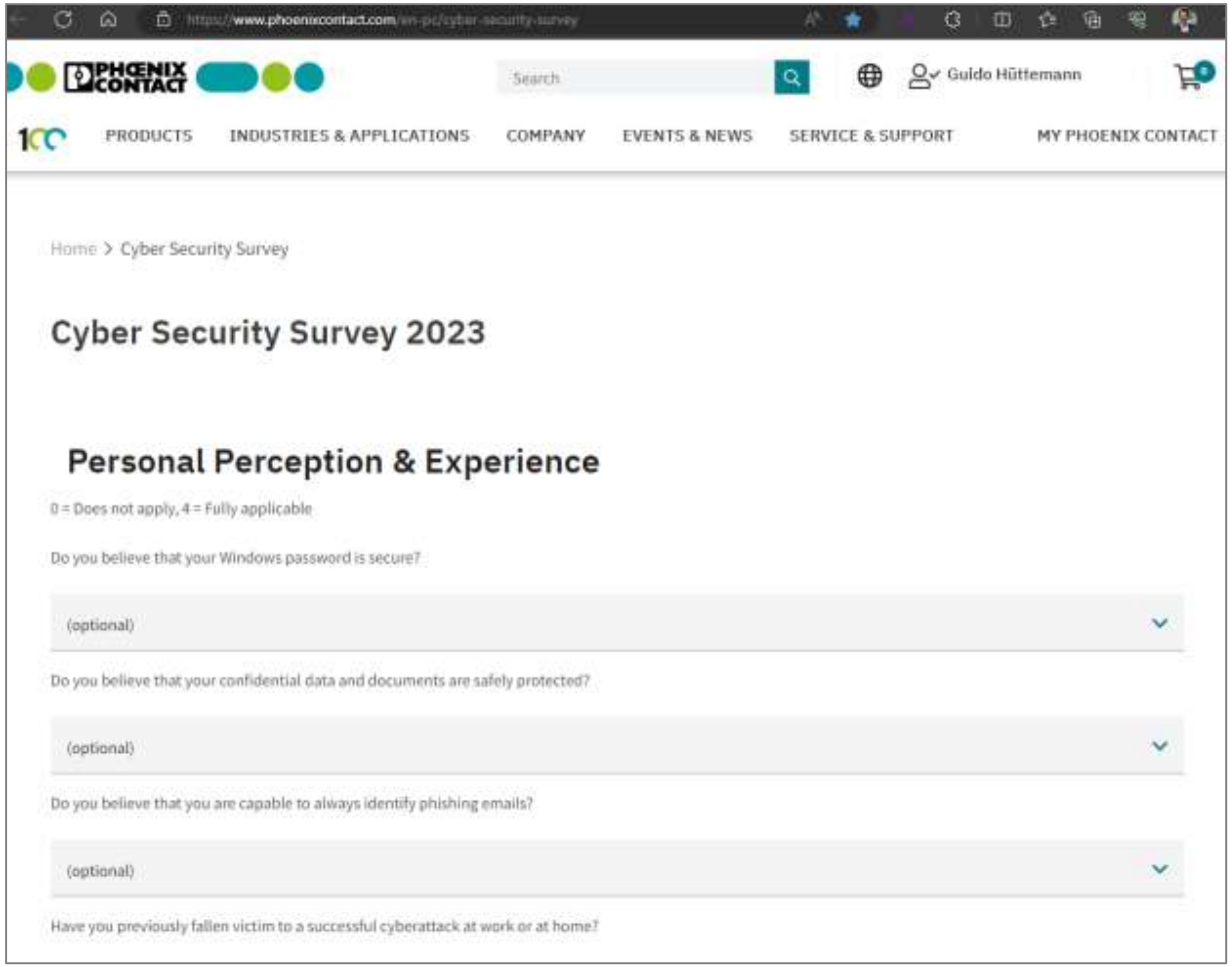


https://phoeníxcontact.com/

login

ghuettemann@phoenixcontact.com

Passwort



https://www.phoenixcontact.com/en-pc/cyber-security-survey

Cyber Security Survey 2023

Personal Perception & Experience

0 = Does not apply, 4 = Fully applicable

Do you believe that your Windows password is secure?

(optional)

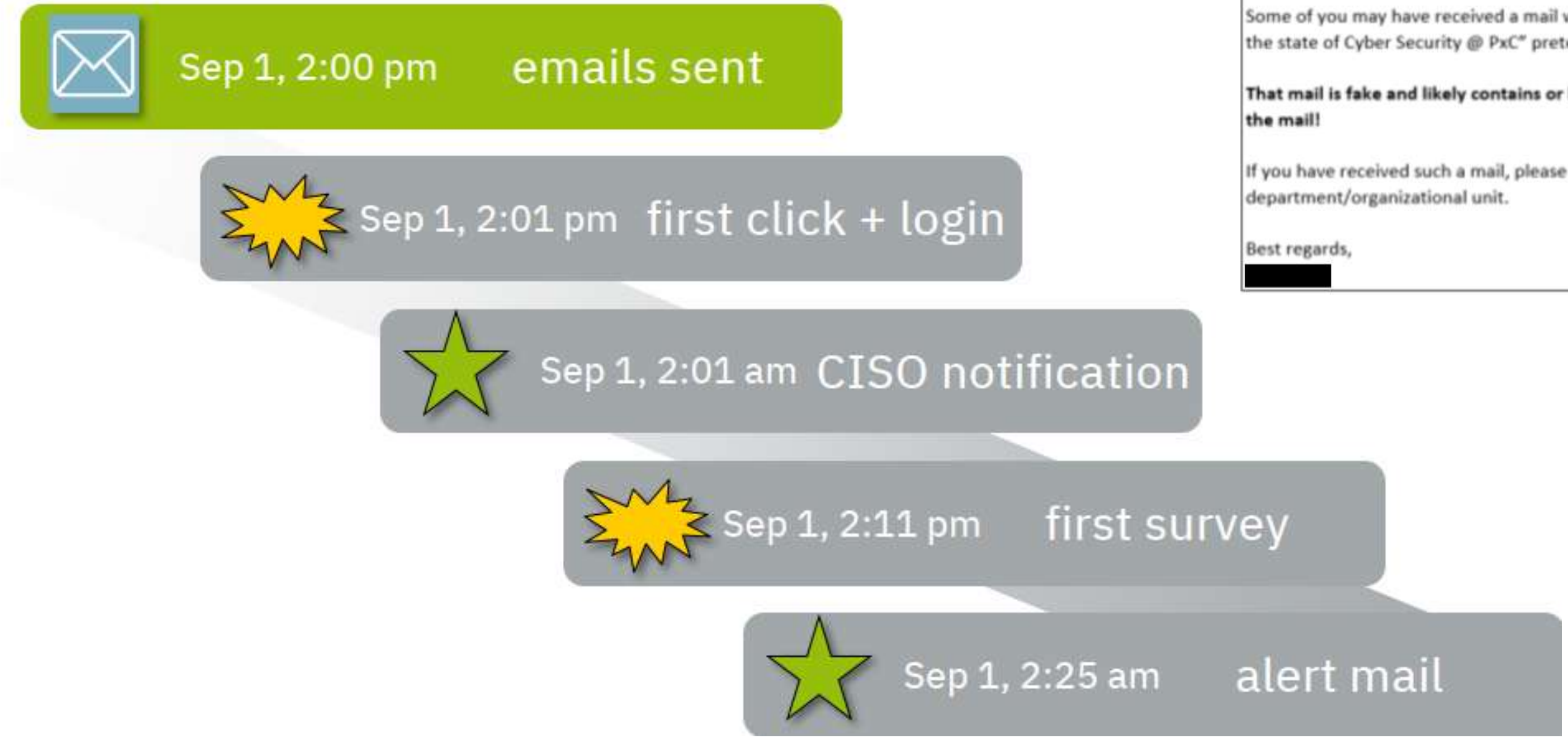
Do you believe that your confidential data and documents are safely protected?

(optional)

Do you believe that you are capable to always identify phishing emails?

(optional)

Have you previously fallen victim to a successful cyberattack at work or at home?



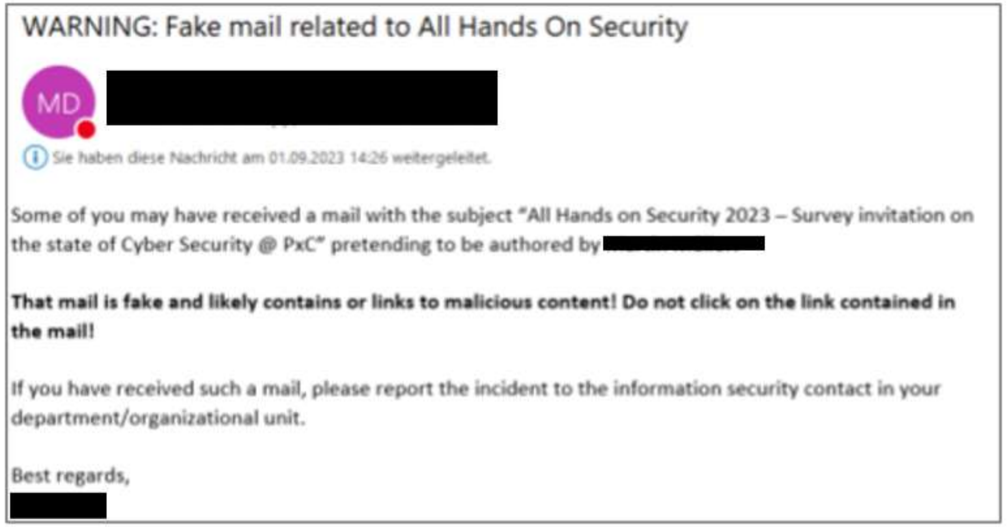
Sep 1, 2:00 pm emails sent

Sep 1, 2:01 pm first click + login

Sep 1, 2:01 am CISO notification

Sep 1, 2:11 pm first survey

Sep 1, 2:25 am alert mail



WARNING: Fake mail related to All Hands On Security

[redacted]

Sie haben diese Nachricht am 01.09.2023 14:26 weitergeleitet.

Some of you may have received a mail with the subject "All Hands on Security 2023 – Survey invitation on the state of Cyber Security @ PxC" pretending to be authored by [redacted]

That mail is fake and likely contains or links to malicious content! Do not click on the link contained in the mail!

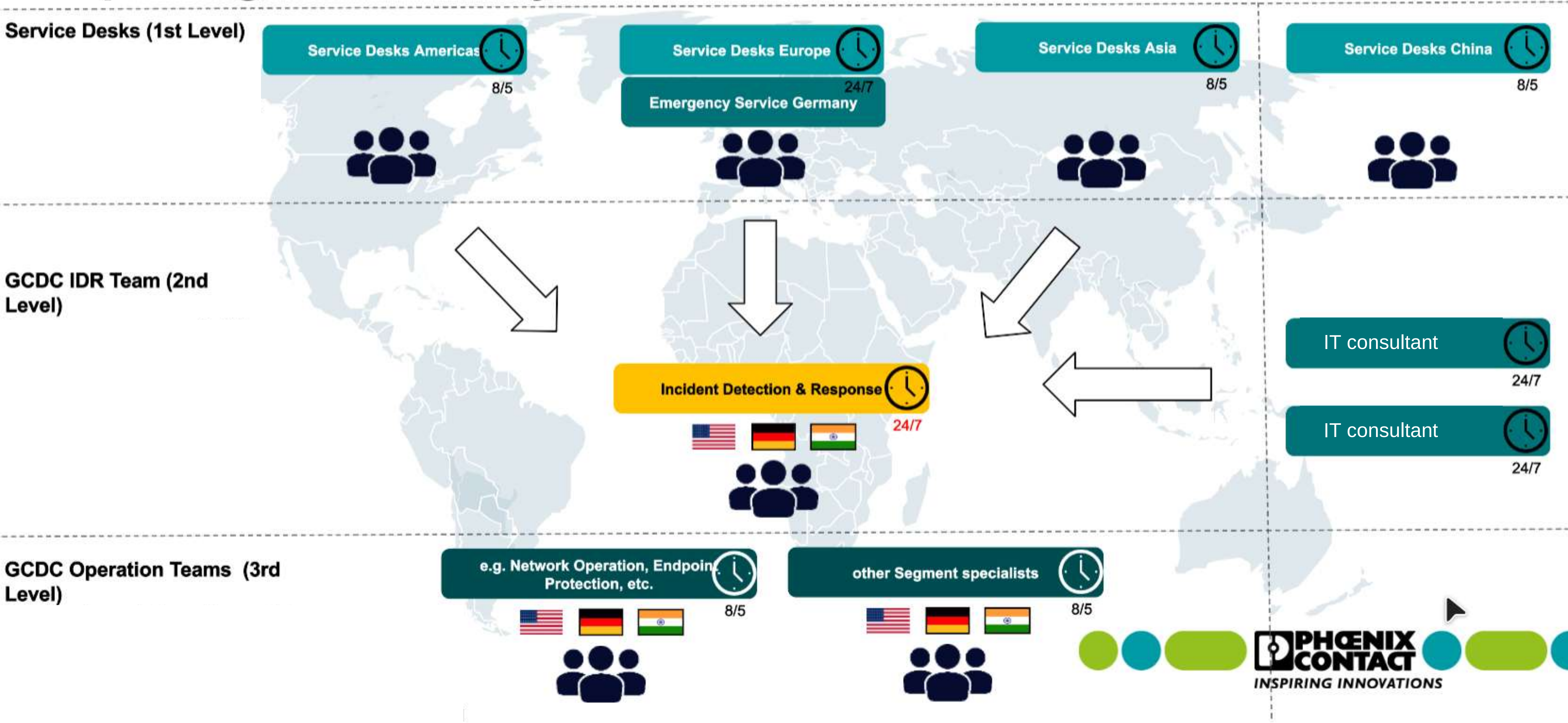
If you have received such a mail, please report the incident to the information security contact in your department/organizational unit.

Best regards,

[redacted]

Global Cyber Defense Center

Reporting of a Security Incident



Service Desks (1st Level)

Service Desks Americas

8/5

Service Desks Europe

24/7

Emergency Service Germany

Service Desks Asia

8/5

Service Desks China

8/5

GCDC IDR Team (2nd Level)

Incident Detection & Response

24/7

IT consultant

24/7

IT consultant

24/7

GCDC Operation Teams (3rd Level)

e.g. Network Operation, Endpoin Protection, etc.

8/5

other Segment specialists

8/5

PHOENIX CONTACT

INSPIRING INNOVATIONS

Incidents

A ransomware was detected in a software which was downloaded from a fake/malicious internet link.

(downloading and installing software is generally forbidden)

An auto-execution virus downloader was detected in an USB drive, which was a gift in an exhibition.

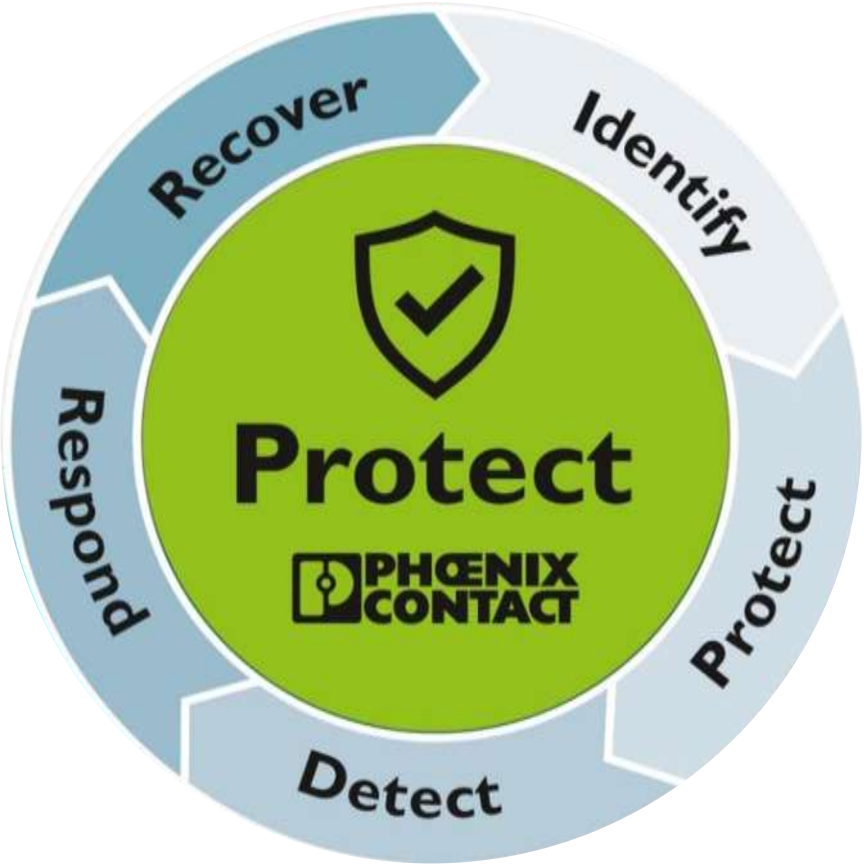
(stick to security policy, ban USB drive)

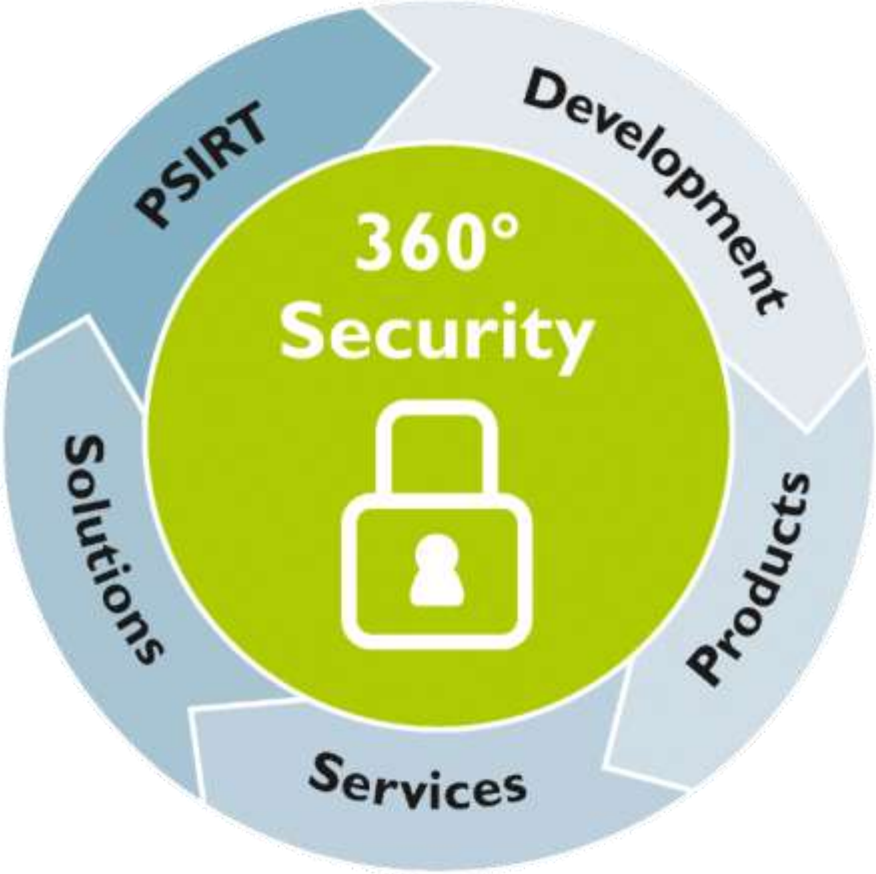
A malware was detected in office database. The malware came from an opensource web hosting module from the development department.

(network segmentation)

Cybersecurity in Phoenix contact

Your Most Trustworthy Supplier





Cybersecurity in Phoenix Contact

Security All-around

Security Between Zones

Industrial firewalls since 2001

Secure Remote Access

mGuard Secure Cloud

Your Security

Security In Zone

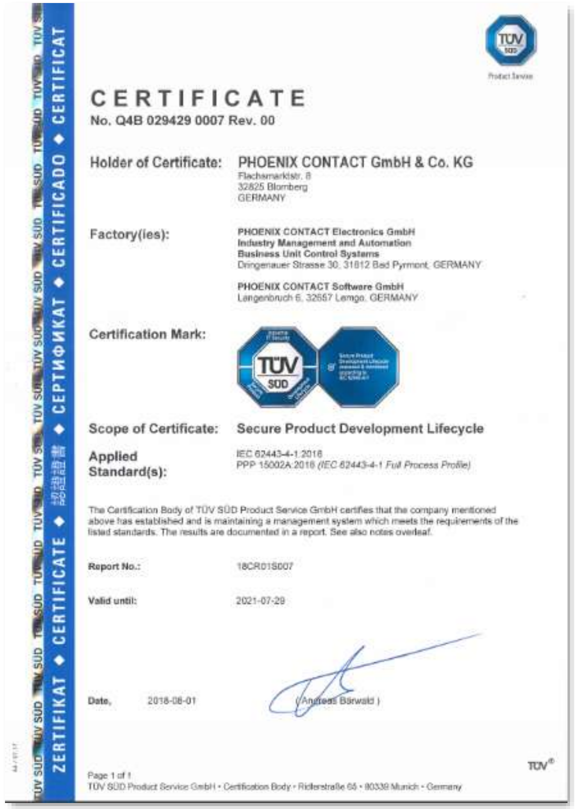
FL TSN, NAT and Managed Switches

Secure Components

PLCNext Technology

Cybersecurity in Phoenix Contact

IEC62443 Certificates



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Q4B 029429 0007 Rev. 00

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Factory(ies): **PHOENIX CONTACT Electronics GmbH**
Industry Management and Automation
Business Unit Control Systems
Dringenauer Strasse 30, 31812 Bad Pyrmont, GERMANY

PHOENIX CONTACT Software GmbH
Langenbruch 6, 32657 Lemgo, GERMANY

Certification Mark:

Scope of Certificate: **Secure Product Development Lifecycle**

Applied Standard(s): IEC 62443-4-1:2018
PPP 15002A:2018 *(IEC 62443-4-1 Full Process Profile)*

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: 18CR01S007

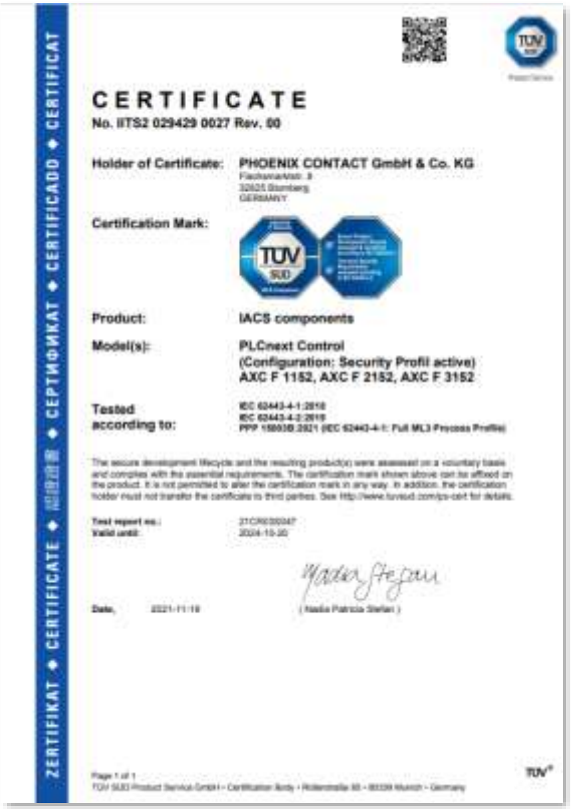
Valid until: 2021-07-29

Date, 2018-08-01 (Andreas Bärwald)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

IEC62443-4-1
certified product development process



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE

No. IITS2 029429 0027 Rev. 00

Holder of Certificate: **PHOENIX CONTACT GmbH & Co. KG**
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Product: **IACS components**

Model(s): **PLCnext Control**
(Configuration: Security Profil active)
AXC F 1152, AXC F 2152, AXC F 3152

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

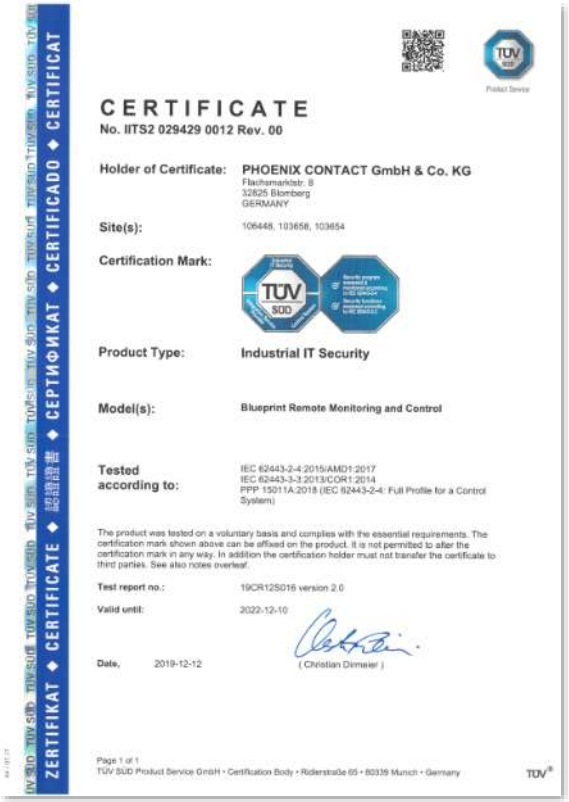
Test report no.: 21CR0030047
Valid until: 2024-10-30

Date, 2021-11-18 Nadia Stefan (Nadia Patricia Stefan)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

IEC62443-4-2
certified products



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. IITS2 029429 0012 Rev. 00

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Site(s): 106448, 103658, 103654

Certification Mark:

Product Type: **Industrial IT Security**

Model(s): **Blueprint Remote Monitoring and Control**

Tested according to: IEC 62443-2-4:2015/AMD1:2017
IEC 62443-3-3:2013/COR1:2014
PPP 15011A:2018 (IEC 62443-2-4: Full Profile for a Control System)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: 19CR12S016 version 2.0

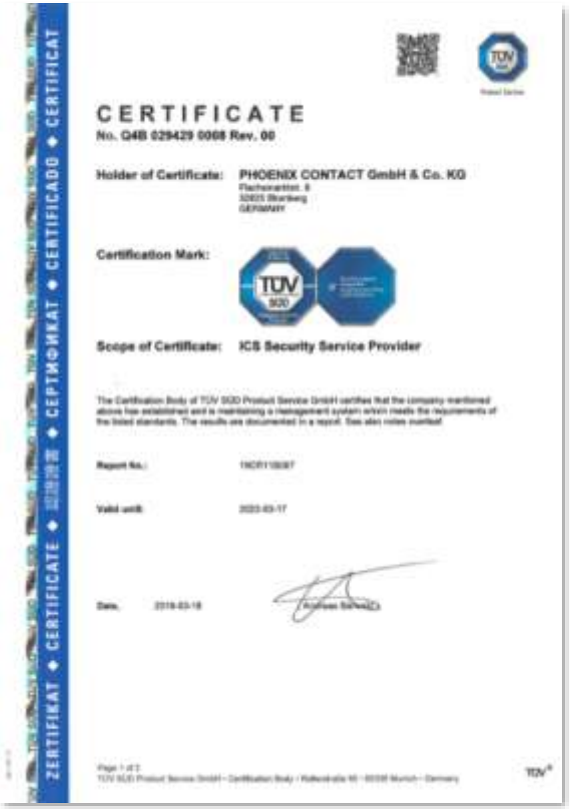
Valid until: 2022-12-10

Date, 2019-12-12 (Christian Dirmeier)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

IEC62443-3-3
certified blueprint remote monitor and control



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Q4B 029429 0008 Rev. 00

Holder of Certificate: **PHOENIX CONTACT GmbH & Co. KG**
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Scope of Certificate: **ICS Security Service Provider**

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: 19CR11S0[illegible]

Valid until: 2022-03-17

Date, 2019-03-18 (Andreas Bärwald)

Page 1 of 2
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

IEC62443-2-4
certified service provider

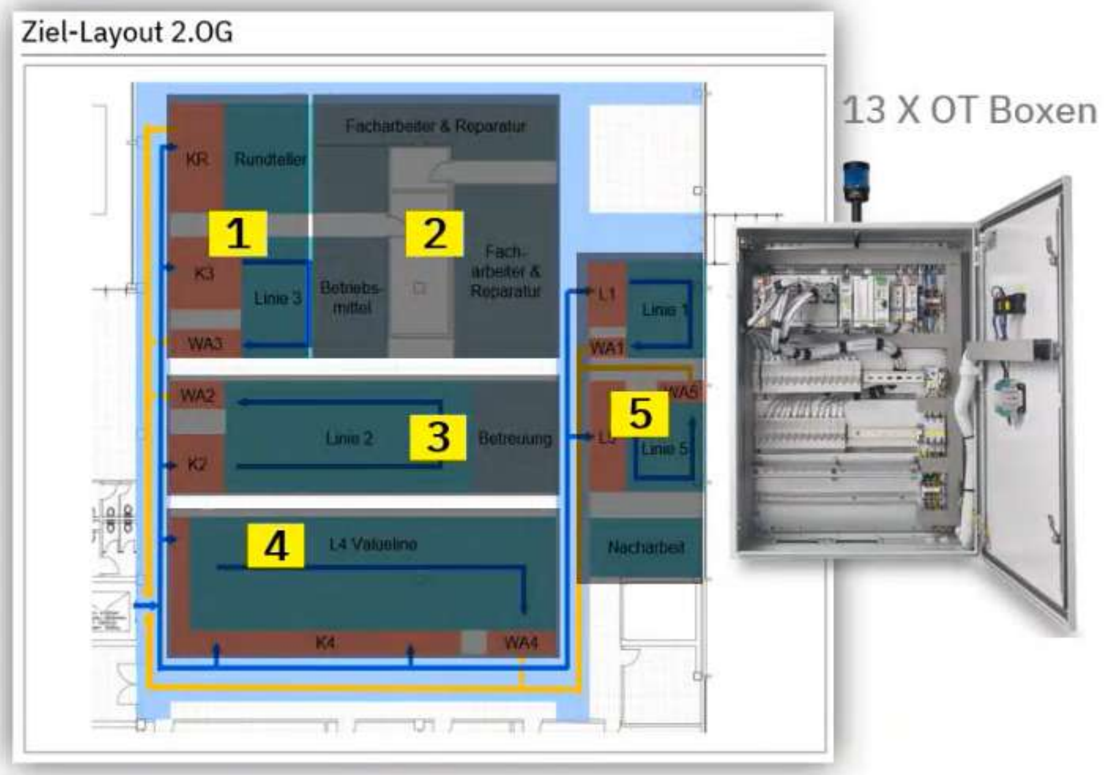
Cybersecurity in Phoenix Contact

Secure The Production Sites

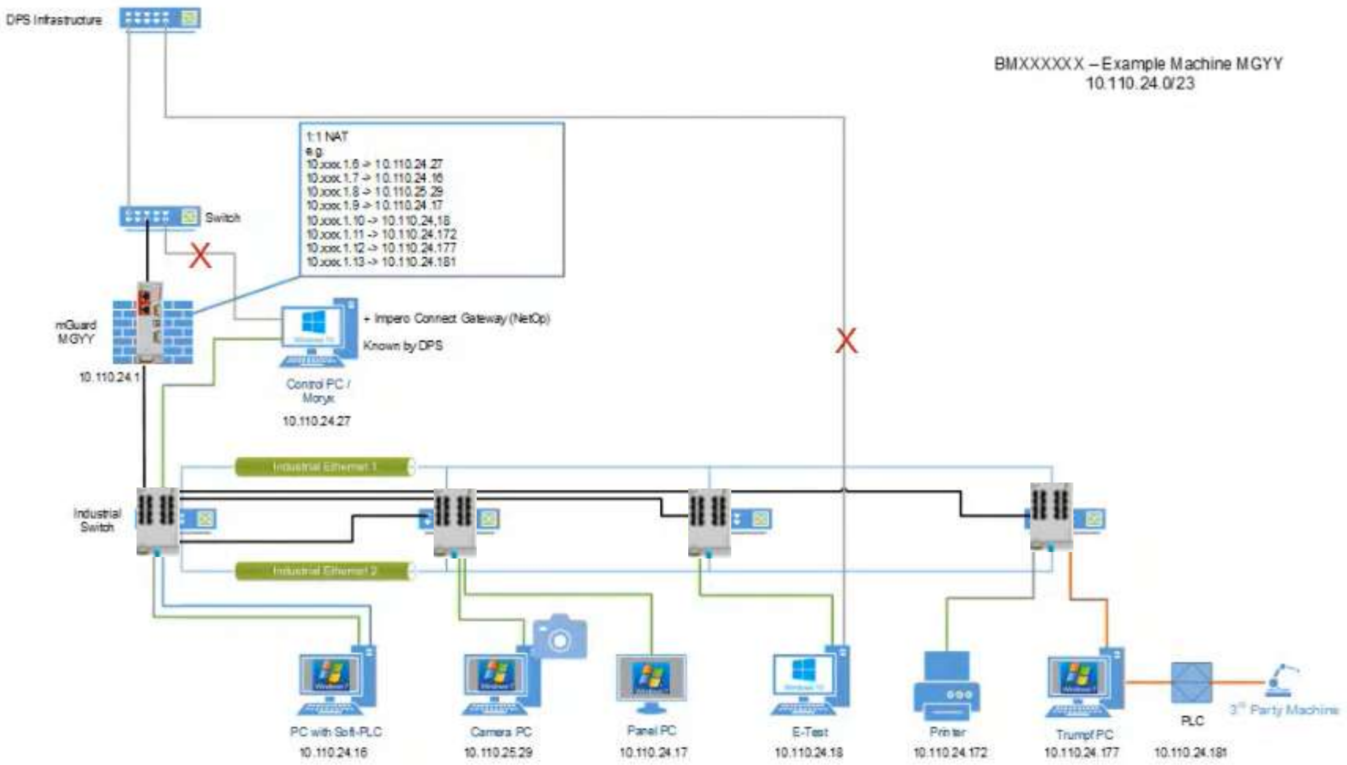
- Challenges
  - Missing high manager attention and missing resources
  - Unmanaged switches
  - Edge devices connect to the core switches to the office network
  - Various communication paths into the machines, control, ip camera, etc
  - Different remote maintenance solutions
  - …

Cybersecurity in Phoenix Contact

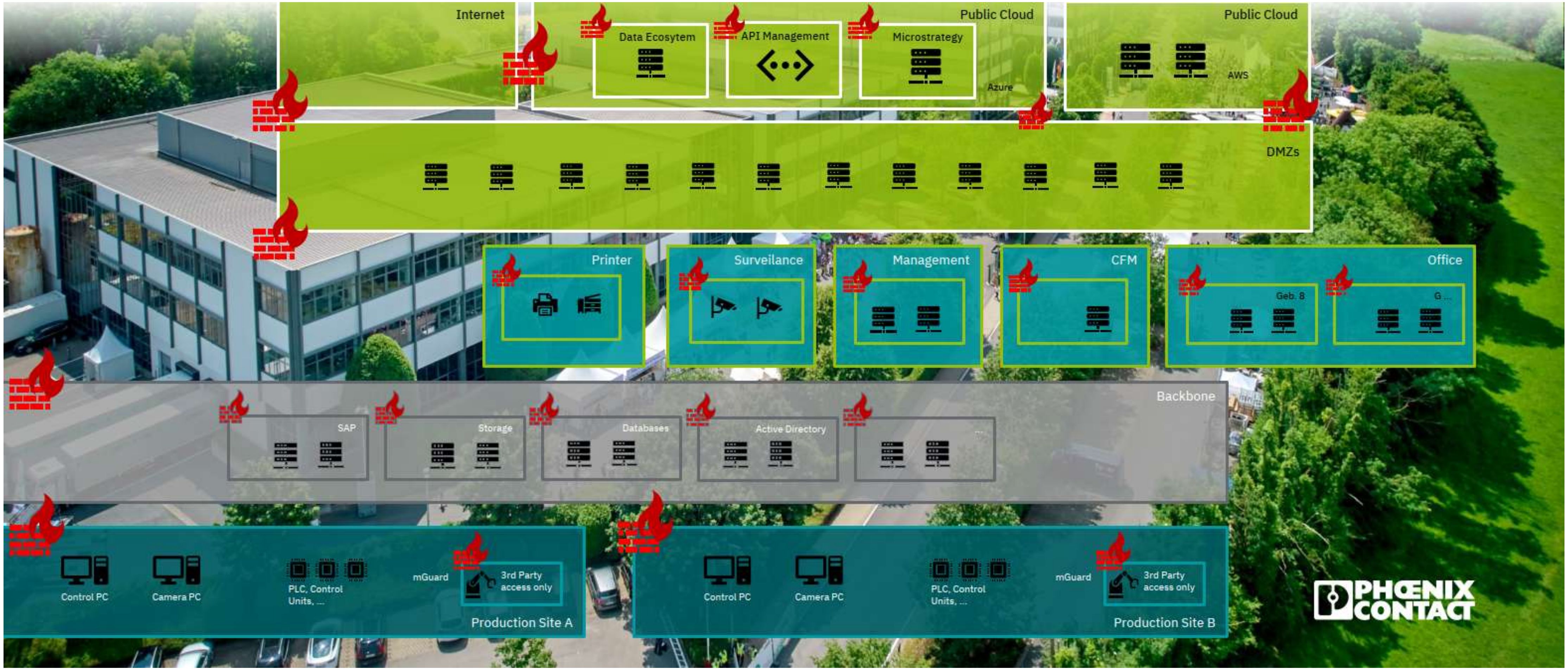
OT Security Box



13 X OT Boxen



Network Segmentation in Production Plant



Internet

Data Ecosytem

API Management

Microstrategy

Public Cloud

Azure

Public Cloud

AWS

DMZs

Printer

Surveilance

Management

CFM

Office

Geb. 8

G ...

Backbone

SAP

Storage

Databases

Active Directory

...

Control PC

Camera PC

PLC, Control Units, ...

mGuard

3rd Party access only

Production Site A

Control PC

Camera PC

PLC, Control Units, ...

mGuard

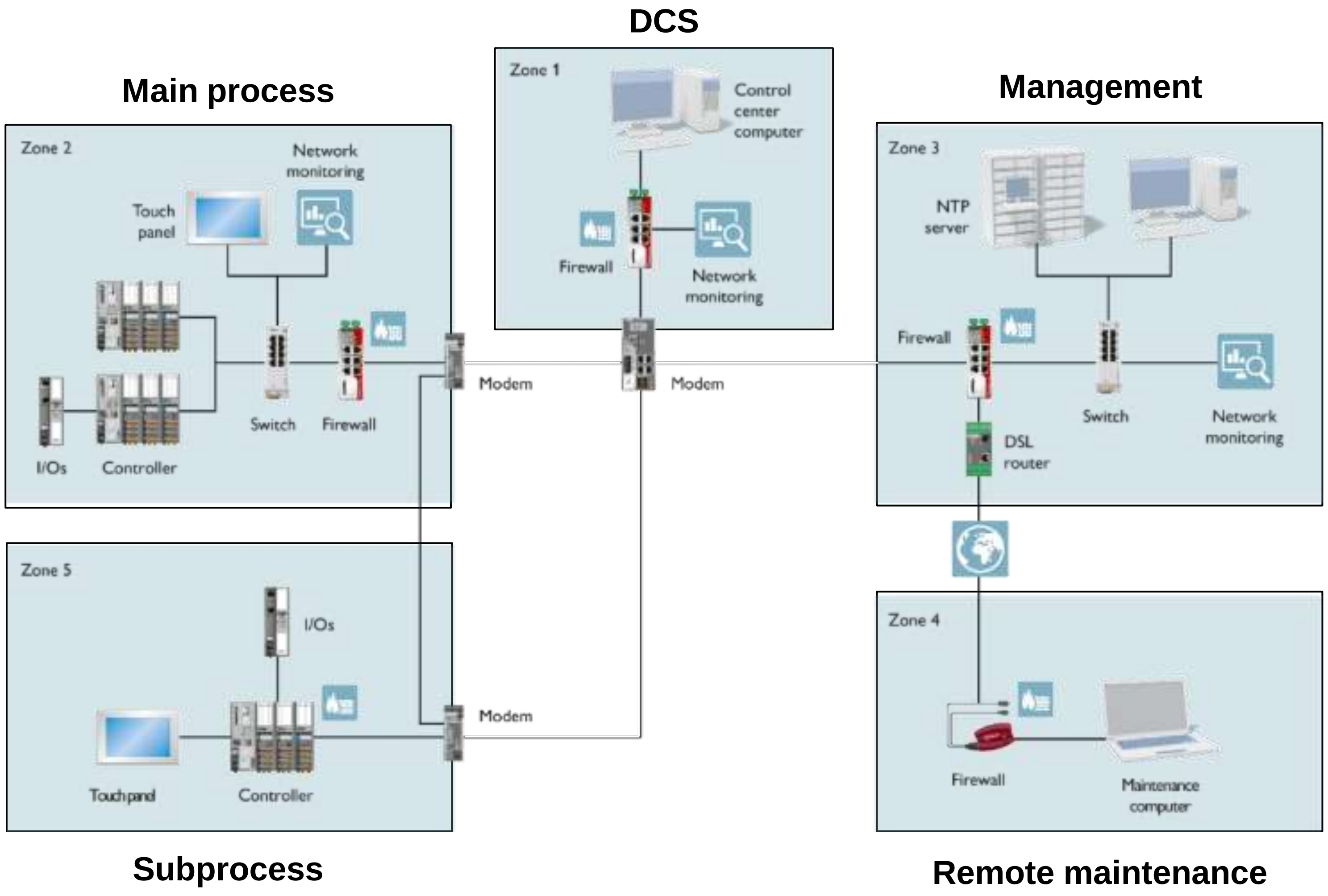
3rd Party access only

Production Site B

PHOENIX CONTACT

Cybersecurity in Phoenix Contact

Security Solutions

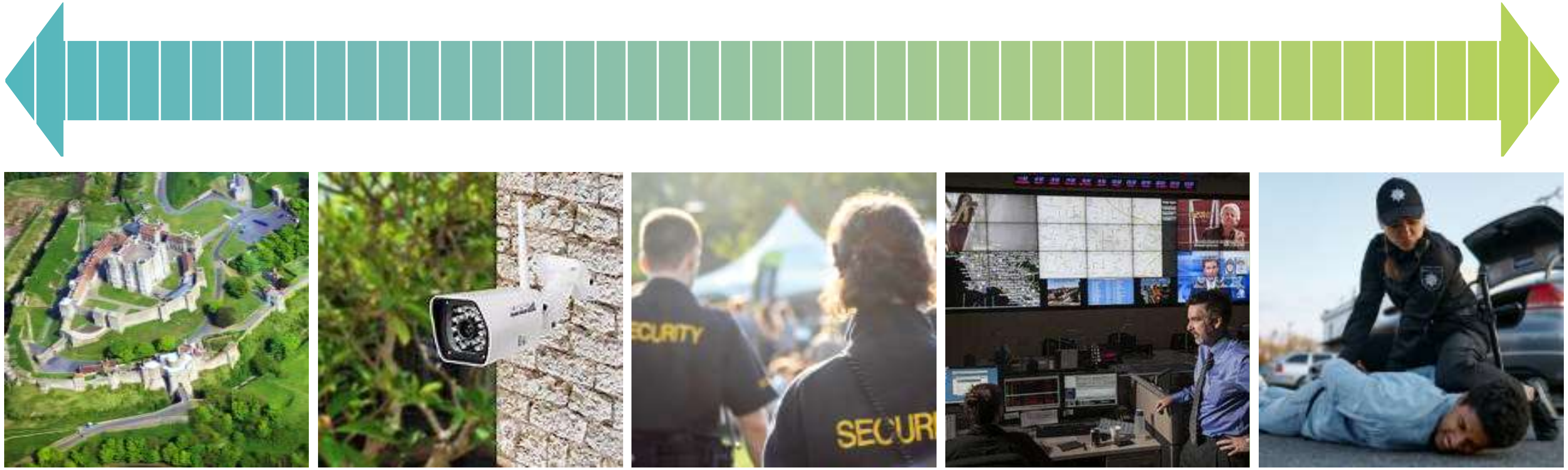


- Solution for Remote Monitoring and Control
- Certification according to IEC 62443-2-4 and 3-3

Industrial IT Security
TÜV SÜD
Integration Service Provider
Control System
Security program assessed & monitored according to IEC 62443-2-4
Security functions assessed according to IEC 62443-3-3

Summary

Plan Your Journey With Cybersecurity Strategy



The planning, establishing, and upkeep of systems with security in mind

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

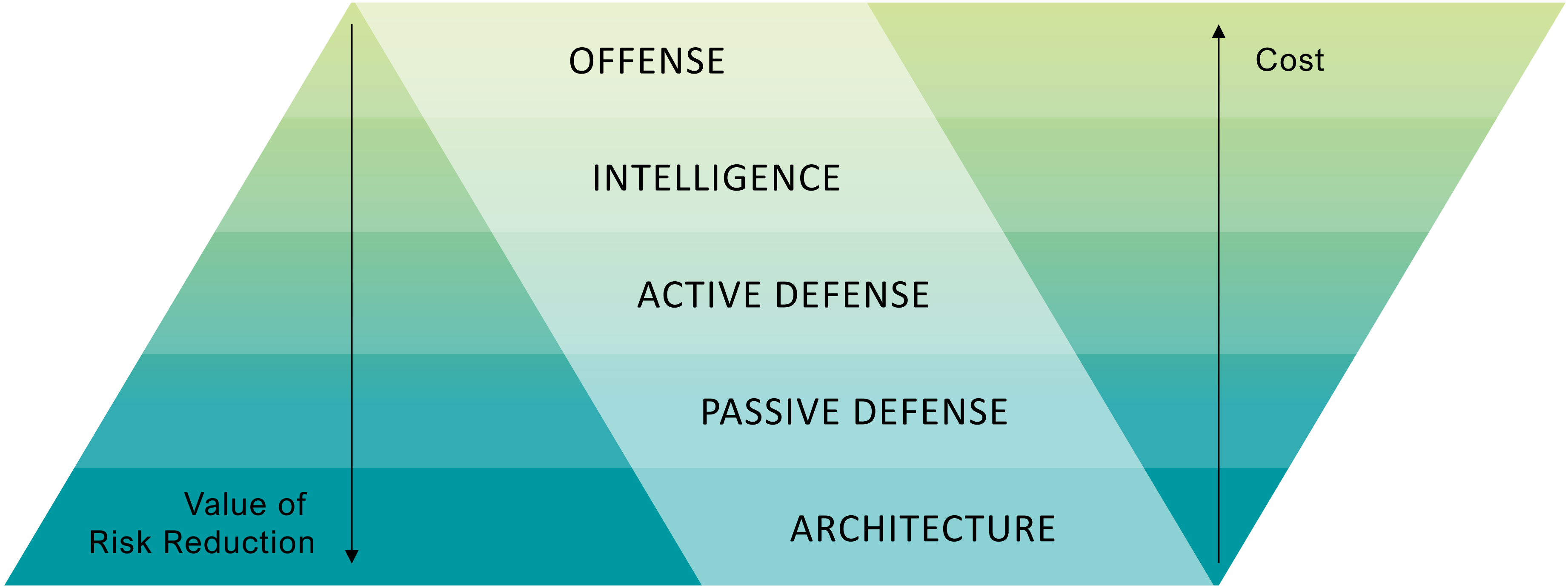
Collecting data, exploiting it into information, and producing Intelligence

Legal countermeasures and self-defense actions against an adversary

Source: Robert M. Lee, The Sliding Scale of Cyber Security, SANS

Summary

Plan Your Journey With Cybersecurity Strategy



Source: Robert M. Lee, Value Towards Security vs. Cost, SANS

Contact me

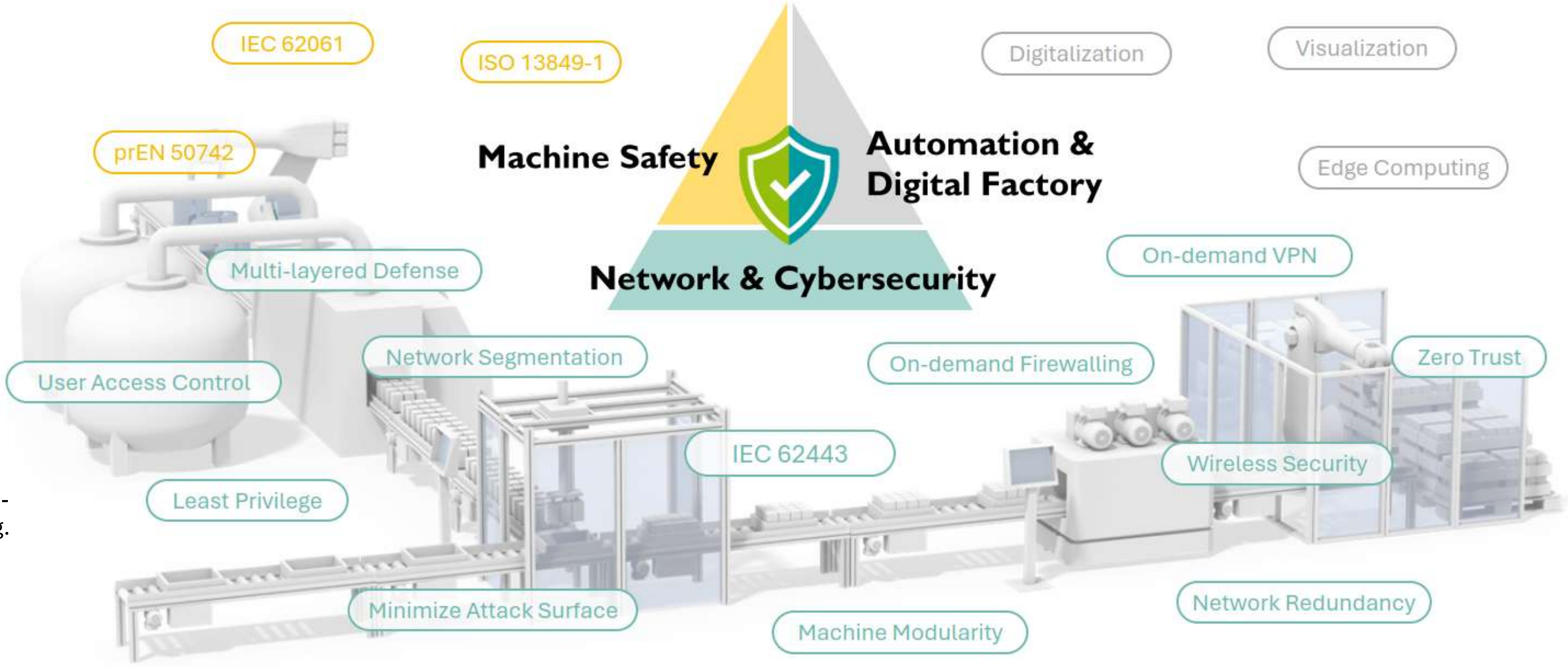
Network & Security Service

Jiunn-Jer Sun

Network & Cybersecurity

Approved specialist by TÜV Rheinland Cyber Security training program with 20-year experience in industrial networking.

jsun@phoenixcontact.com



PHOENIX CONTACT
INSPIRING INNOVATIONS

Axel Baur Siby
Machine Safety Expert
Approved safety specialist by
TÜV Rheinland # 3435 / 22 -
Machinery-CE Practice

Functional Safety Webinars

7 Feb.	Functional Safety And The New Machinery Regulation – An Overview
21 Feb.	Risk Assessment - An Essential Part
14 Mar.	Designing And Calculating A Safety Function
28 Mar.	News In ISO 13849-1:2023
11 Apr.	News In IEC 62061:2021

Thank you

PHOENIX CONTACT
INSPIRING INNOVATIONS