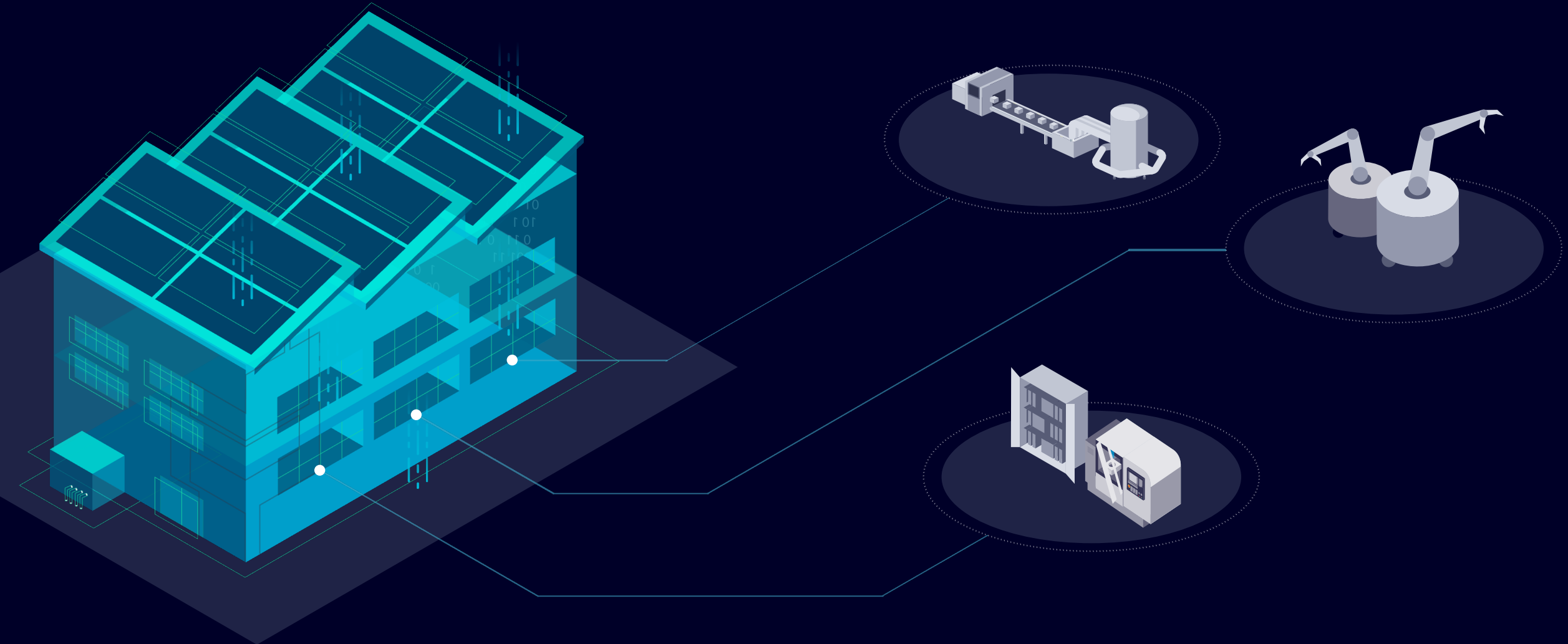


Cybersecurity for Industrial Operations

We help you to secure your operations –
You focus on your core business



Yesterday we had islands of communication





Today
everything is
connected ...





... and
at risk

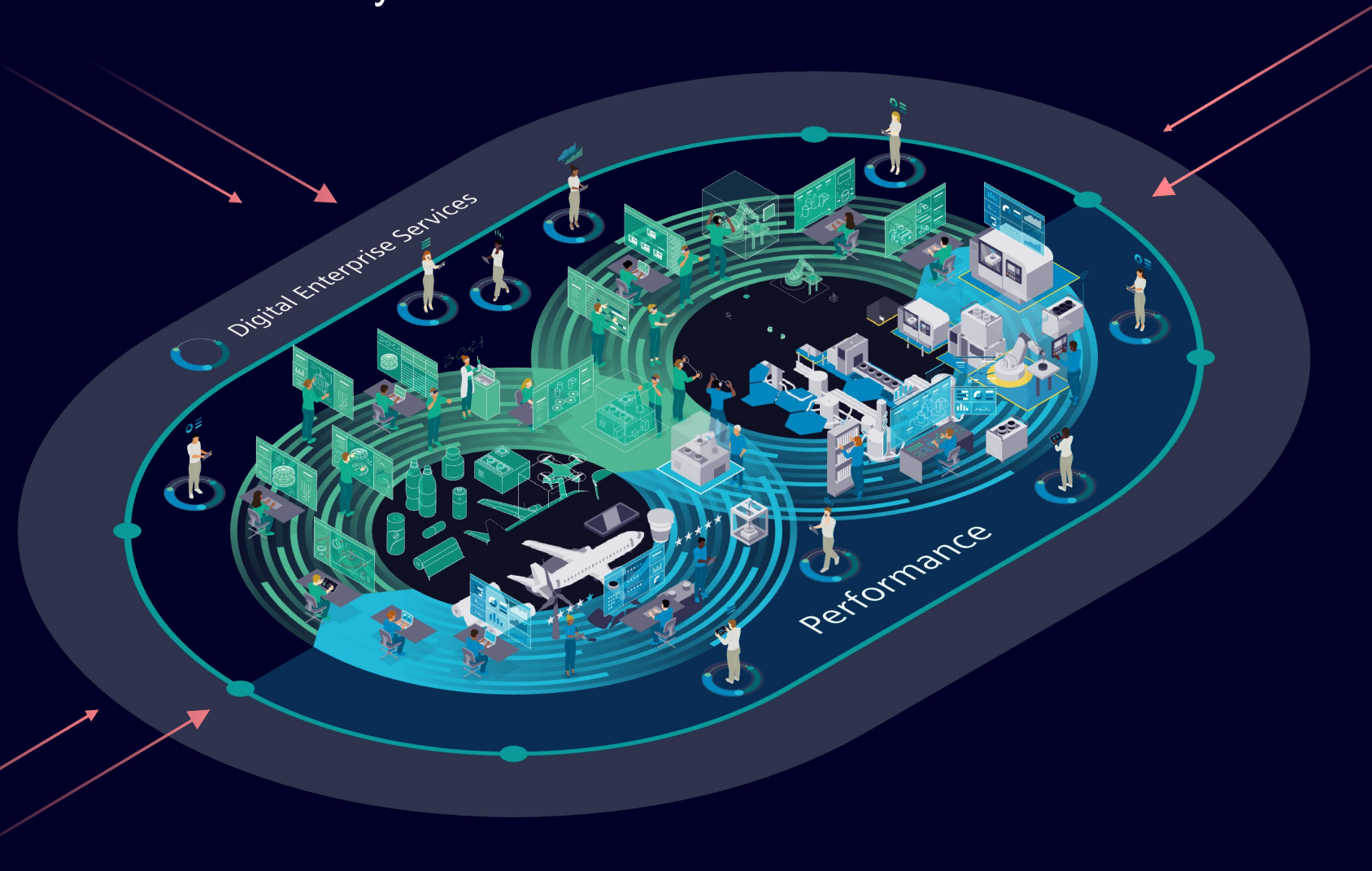


Production systems are part of the IoT

This means IT/OT integration across all areas and layers

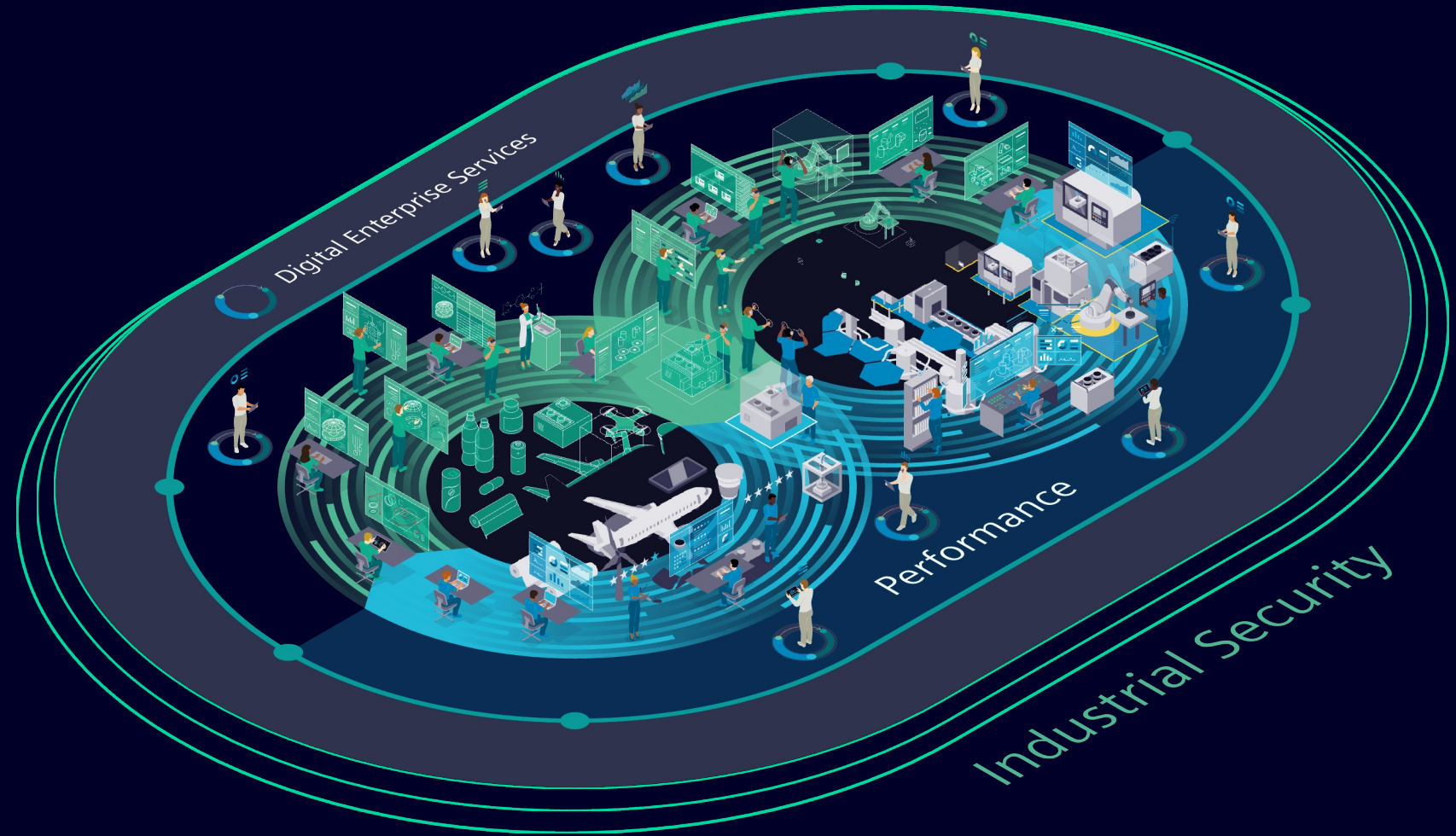
IT/OT collaboration means:

- 👍 More connectivity
- 👍 More data
- 👎 New cyber-risks





Embedded in a growing ecosystem





Why is Cybersecurity in OT such an important topic for industry?

Cyberattacks

The threat is real and – especially in OT

33%

of all
cybersecurity
incidents occur in
manufacturing

Source:
PMMI 2021 Assess your risk white paper

65%

of all ransomware
attacks happen
on the shop floor

Source:
Dragos 2021 ICS/OT Cybersecurity
year in review



Legislation is underway in many parts of the world

CIRCA and **SEC** regulations in **US** will change how companies address cybercrime
Focus is on: reporting, disclosure criteria and transparency

Source: [McKinsey, 2022](#)

Tightening cybersecurity obligations across **Europe** - the **NIS2** directive
Focus is on: new rules, more sectors included

Source: [European Parliament, 2023](#)

Key changes in data privacy and cyber security laws across **Southeast Asia** in 2022

Source: [Herbert Smith Freehills, 2022](#)

EU NIS 2 Directive¹

Overview



Aim



- Achieving a **high common level of cybersecurity within the EU**, while improving the functioning of the internal market
- Revision of NIS1¹ – the first + key piece of EU-wide cybersecurity legislation



Focus



Rules on security of **network and information systems**



Addressees



All 27 EU countries, Island, Liechtenstein + Norway (=MS)



Entry into force



Latest by 18th October 2024



Minimum harmonization



MS may adopt/maintain provisions ensuring a higher level of cybersecurity,
provided that such provisions are consistent with their obligations under EU law

¹ Directive (EU) 2016/1148 of the European Parliament and the Council [the Network and Information Security (NIS) Directive].

Entities

Essential entities

Fines:

Administrative fines non adherence to cybersecurity risk management measures or reporting obligations:

€10 M or 2%
Of annual global turnover



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

Important entities

Fines:

Administrative fines non adherence to cybersecurity risk management measures or reporting obligations:


€7 M or 1.4%
Of annual global turnover





On-site inspections and off-site ex post supervision




Essential entities¹

 **Medium**
entities

 **Large**
entities


 **Energy** (electricity, district heating and cooling, oil, gas and hydrogen)


 **Transport** (air, rail, water and road)

 Financial market infrastructures

 Banking

 Health including manufacture of **pharmaceutical** NEW products including vaccines

 **Drinking water**


 **Wastewater** NEW


NEW  Digital infrastructure


Space  NEW

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

Important entities¹


 **Medium**
entities


 **Large**
entities

NEW  Postal and courier services

Waste management  **NEW**

NEW  **Chemicals**

 **Food** **NEW** production, processing and distribution

 **Manufacturing** of **medical devices**, computers and electronics,
machinery equipment, **motor vehicles** **NEW**

NEW  Research

Digital providers 

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



**How does Siemens help you
to secure your operations?**

Our holistic Industrial Security concept based on Defense in Depth principle



Overview: Network Security

Adapted measures for production:

Network access control

- Secure interface to IT networks
- Secure architecture with DMZ
- Secure remote access via Internet
- Secure local network access (port security) via device and user authentication
- Secure cloud connection

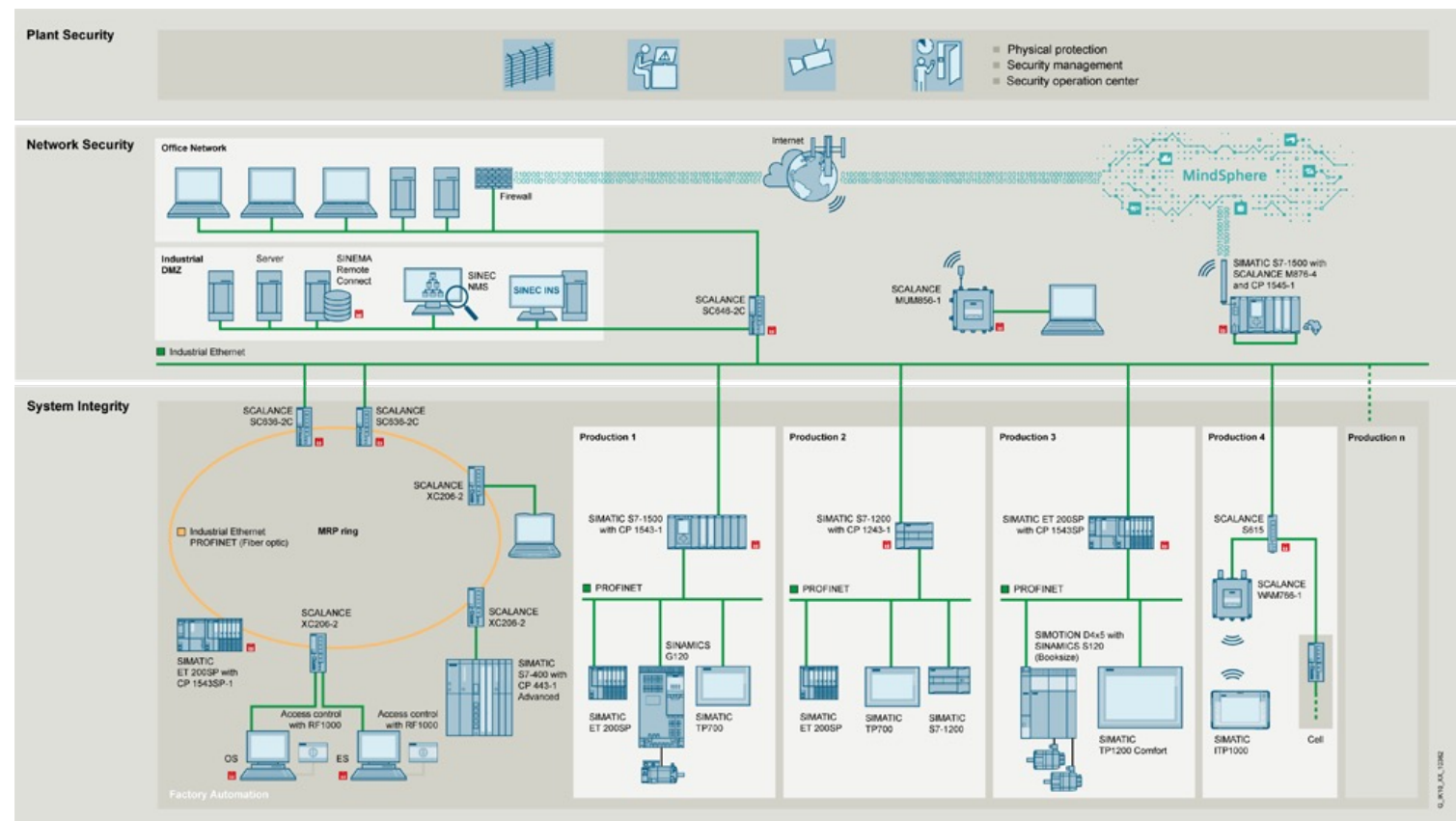
Redundancy

- Protection of redundant network topologies

Cell protection

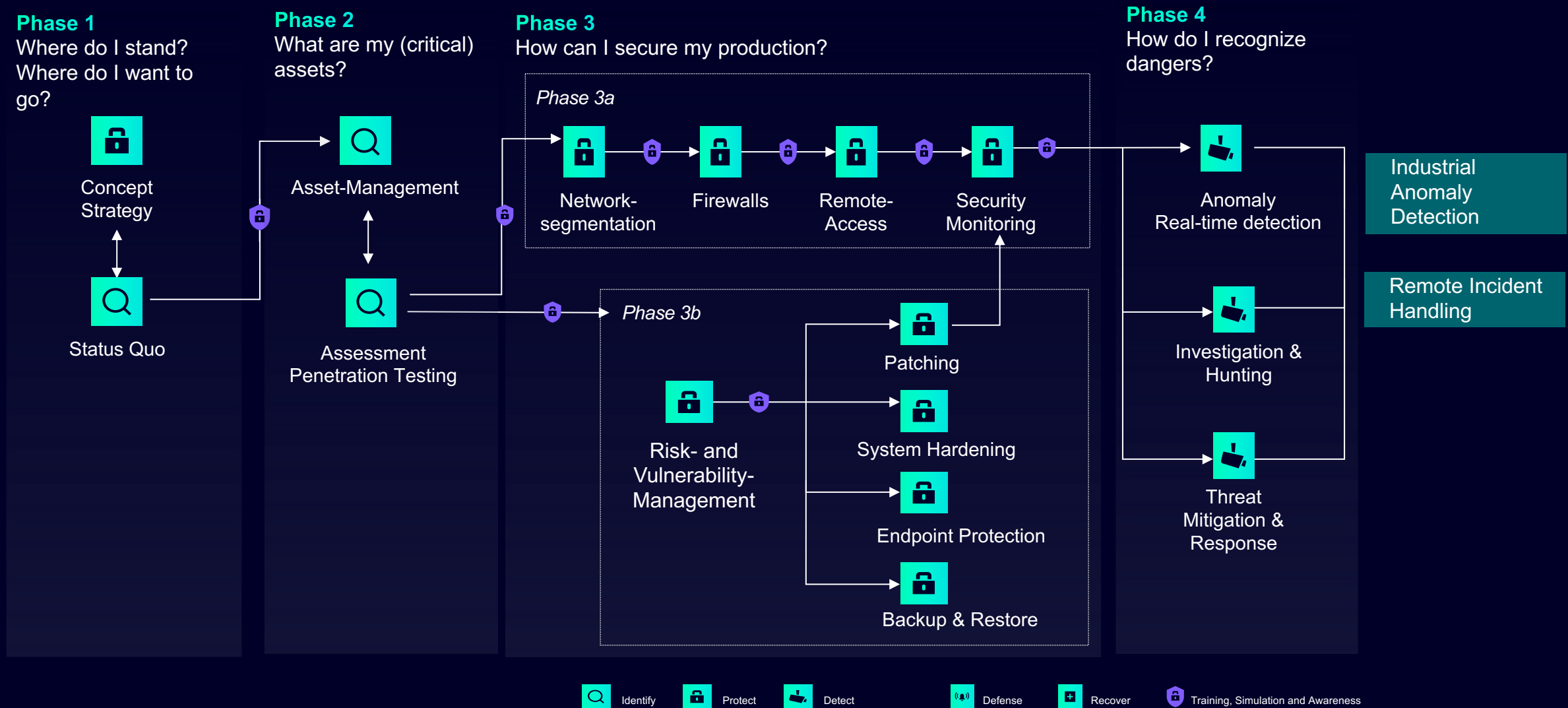
- Risk mitigation by means of network segmentation
- Extension of cell protection concept by means of:
 - Security communication processors
 - Flexible VLAN configuration

For information on cybersecurity solutions with RUGGEDCOM, visit www.siemens.com/ruggedcom/cybersecurity

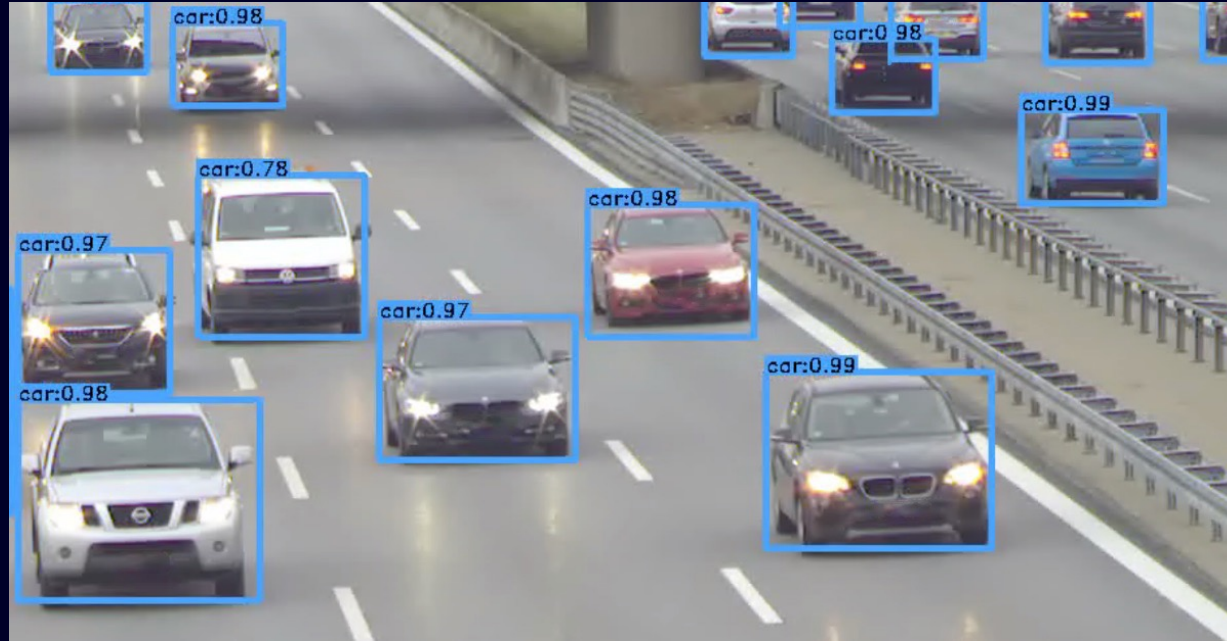


Products with firewall or VPN functionality

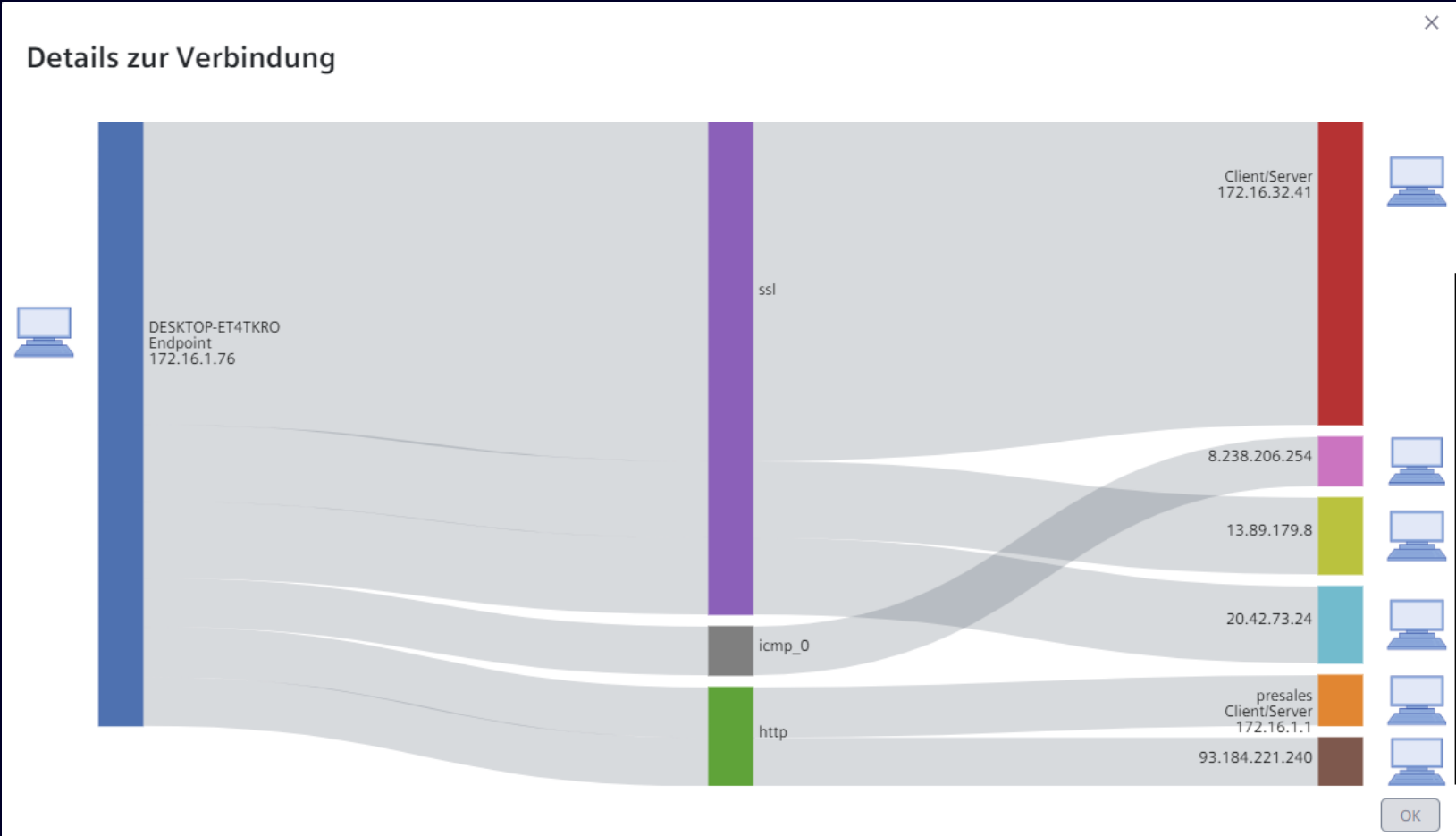
Cybersecurity Services – Step by Step



Anomaly Detection – Anlernphase (Überwachung des Verkehrs)



IP traffic – who is talking to whom via which protocol




Anomaly Threat Detection

Suspicious Device Behavior

(Alert #1000044)

A HP device was observed communicating to a substantial amount of malicious IP addresses


 ALERT INFORMATION

ALERT STATUS	ALERT CATEGORY	AFFECTED SITES	DETECTED
Unresolved	Communication	Clinton	7/22/22, 5:16 PM
NOTE			LABELS
Alert auto-assigned to SOC T2 for investigation			High Priority

Recommendations

Monitor inbound and outbound traffic from the device, and quarantine the device from the network if necessary.

Security Events - automatic event creation based on a control system

 **SIEMENS**
SINEC Security Monitor

DASHBOARD

ASSETS

SECURITY-EREIGNISSE

Risikolage

Security-Ereignisse

Logs

2023-10-04 17:07:19

Mitteeuropäische Zeit

Deutsch

Security-Ereignisse

Baumdiagramm

Änderungsverlauf

Batch-Verarbeitung

Einfache Suche

2023-10-04 - 2023-10-04

Alle Kategorien

Alle Zustände

Alle Datenquellen

Status	Zeitstempel	Ereignis-ID	Ereignistyp	Ereignisname	Datenquelle	Hostname	Anmerkungen
Nicht bearbeitet	2023-10-04 17:06:00	204	Warnung	New APP Flow	Virtual	172.16.32.199	New application communication (APP Flow) tcp_7680 is detected between src host 172.16.32.199 and dst host 172.16.21.2.
Nicht bearbeitet	2023-10-04 17:06:00	204	Warnung	New APP Flow	Virtual	172.16.32.199	New application communication (APP Flow) tcp_443 is detected between src host 172.16.32.199 and dst host 20.54.24.69.
Nicht bearbeitet							New application communication (APP Flow) tcp_7680 is detected between src host 172.16.32.199 and dst host 172.16.2.101.



SINEC Security Monitor

CYBERSECURITY REPORT

Report Period:

Aug 01, 2023 ~ Aug 31, 2023

Generated by:

admin

Time:

Sep 01, 2023

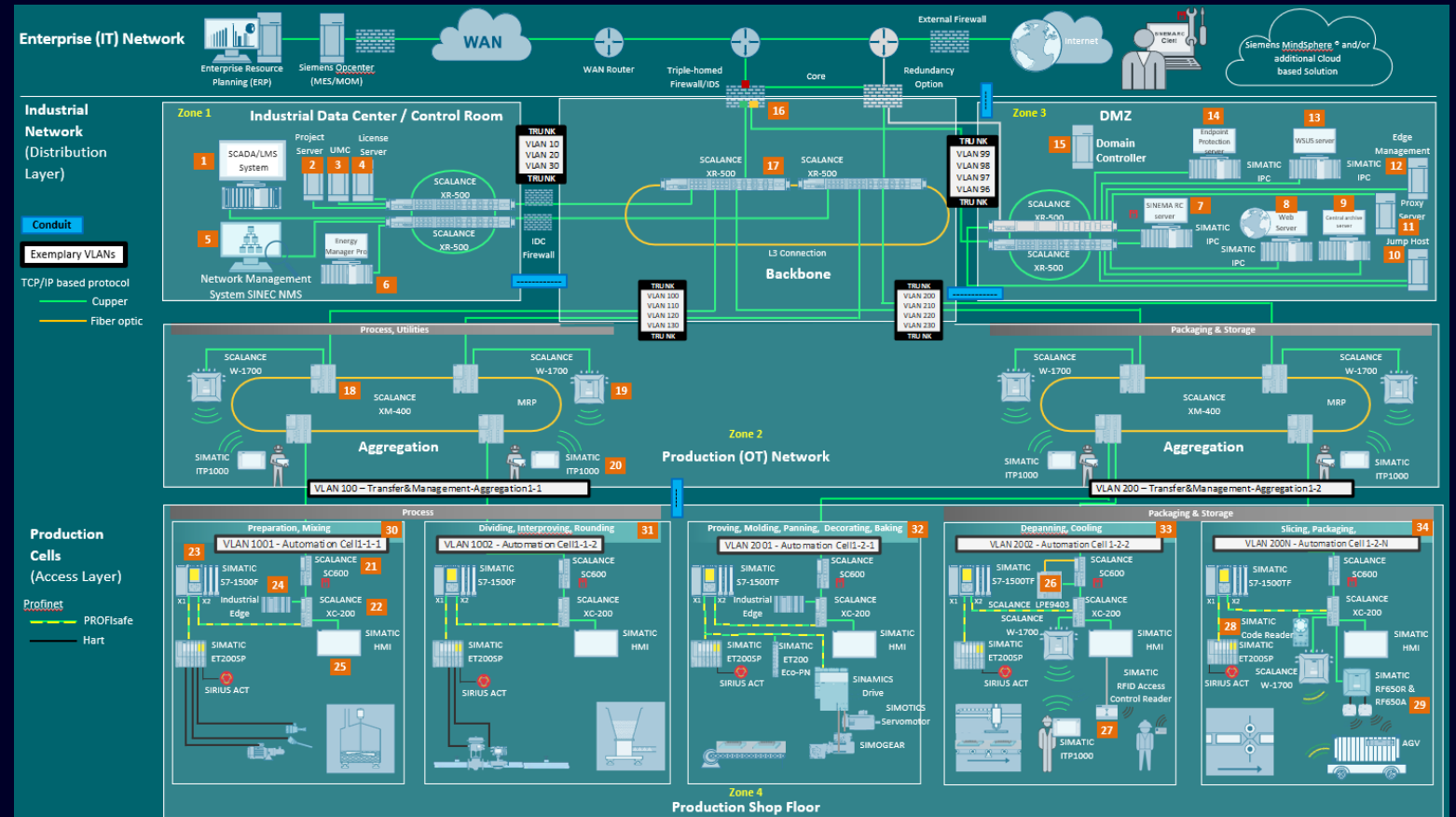
Classification:

Confidential

Our Cybersecurity experts enriched with our profound market knowledge support you for building up secure architectures for your industrial operation

Siemens provides **end to end security solution** from consulting to implementation of dedicated portfolio and optimization of your applications:

Tailor-made for your complete industrial operations – from sensor to cloud



Remote Access

Asset
Inventory
Scan

Assessment

Firewalls

End Point
Protection

Risk
Awareness

How we can
support you to protect
your operations

Whitelisting

DMZ

Patch
Management

Anomaly
Detection

Network
Segmentation

Network
Monitoring & Management



Thank You!





Published by Siemens AG Österreich

Wolfgang Siegel

Leitung Solutions Food & Beverage

Mobile +43 (664) 88553897

E-mail siegel.wolfgang@siemens.com

Michael Pirich

Sales Specialist

Mobile +43 (664) 88558671

E-mail michael.pirich@siemens.com