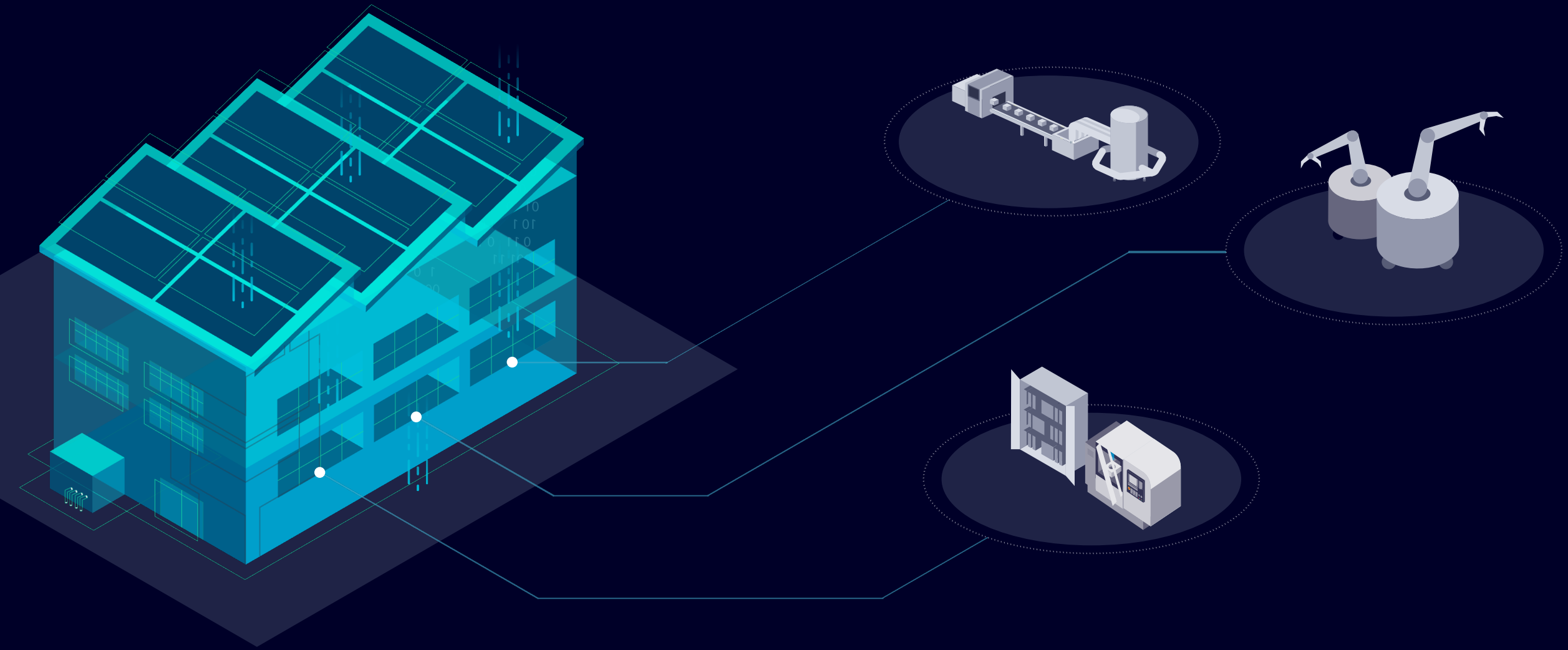
Cybersecurity for Industrial Operations

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

SIEMENS

Yesterday we had islands of communication



SIEMENS

Today everything is **connected ...**

SIEMENS

… and **at risk**

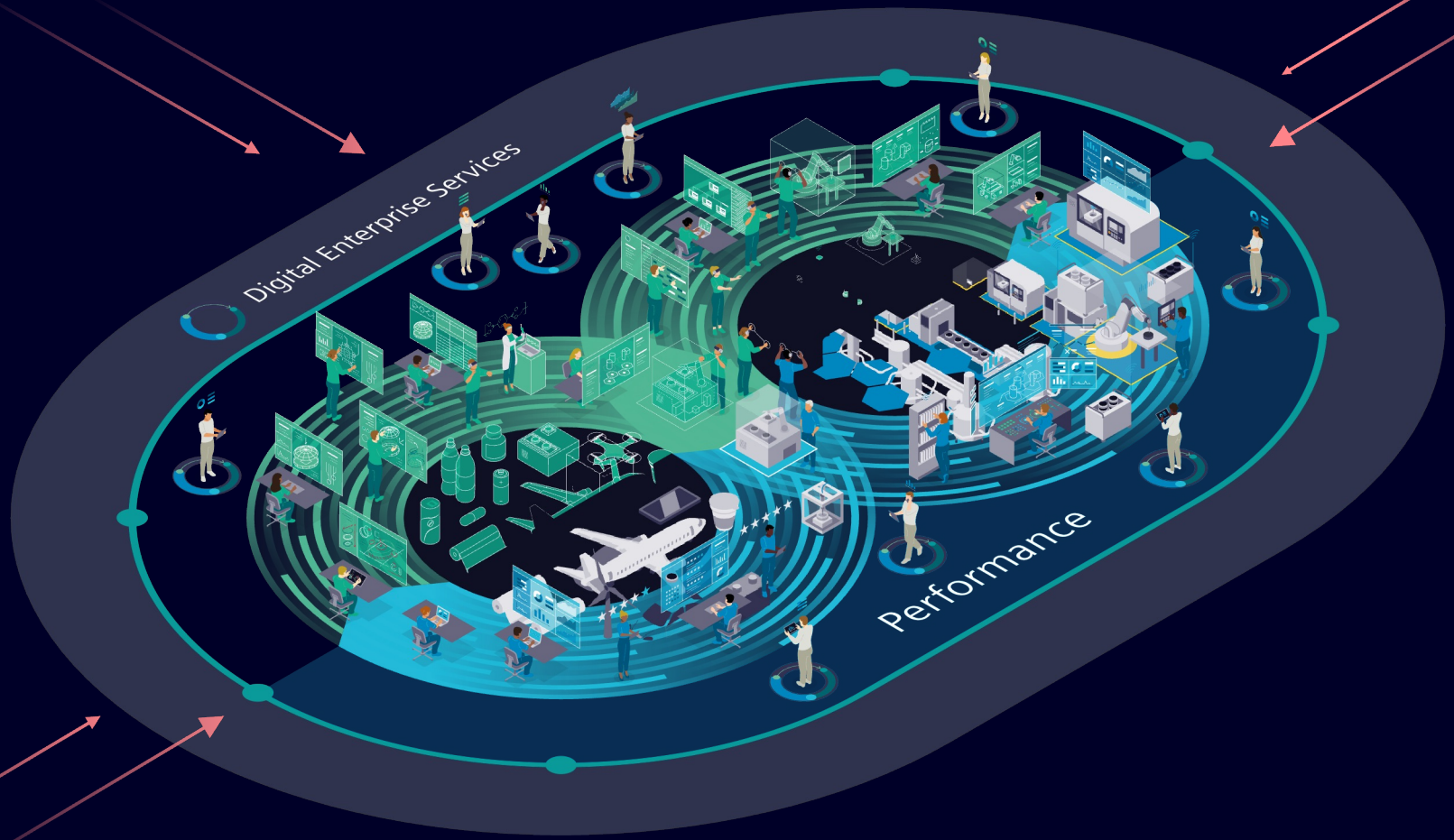
SIEMENS

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**

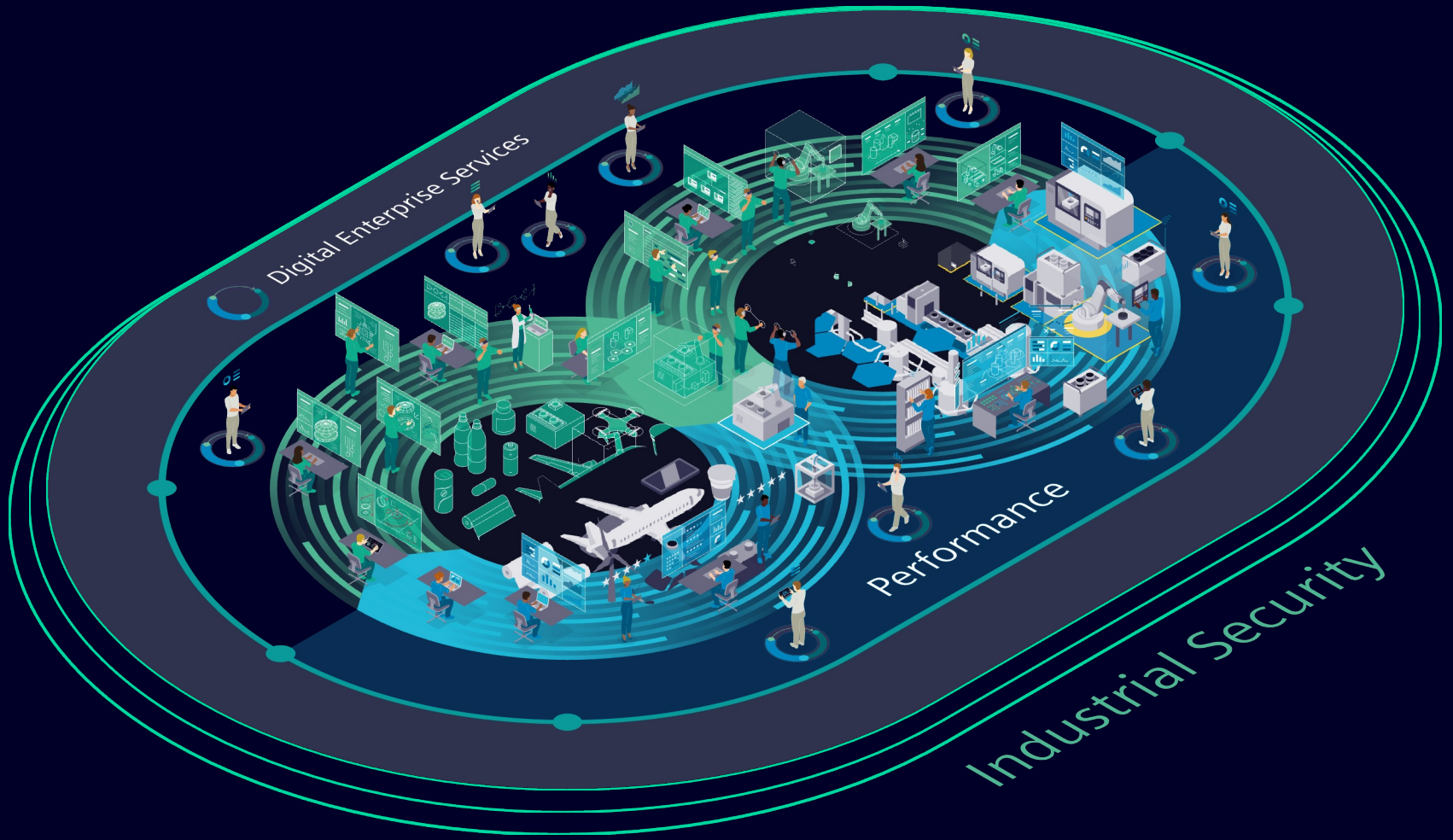


SIEMENS

Only a comprehensive security approach based on the defense in depth concept can provide an effective protection

Multi-layered industrial security concept

Embedded in a growing ecosystem



SIEMENS

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

SIEMENS

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

SIEMENS

Legislation is underway in many parts of the world

CIRCIA 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

SIEMENS

EU NIS 2 Directive[1]
Overview

Aim	• Achieving a **high common level of cybersecurity within the EU**, while improving the functioning of the internal market • Revision of NIS1[1] – 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 **N**etwork and **I**nformation **S**ecurity (NIS) Directive].

SIEMENS

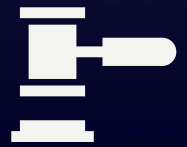
Entities

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 entities[1]

Medium entities

Large entities

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

Transport (air, rail, water and road)

Banking

Financial market infrastructures

NEW

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

Drinking water

NEW

Wastewater

NEW

Digital infrastructure

NEW

Space

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

SIEMENS

Important entities[1]

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

Digital providers

NEW Research

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

SIEMENS

How does Siemens help you to secure your operations?

SIEMENS

Our holistic Industrial Security concept based on Defense in Depth principle

Security threats demand action

Plant security

- Physical access protection
- Security Policies
- Security monitoring

Network security

- Cell protection, perimeter network and trusted zones
- Firewalls and VPN

System integrity

- System hardening
- Patch Management
- Authentication and access protection

SIEMENS

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

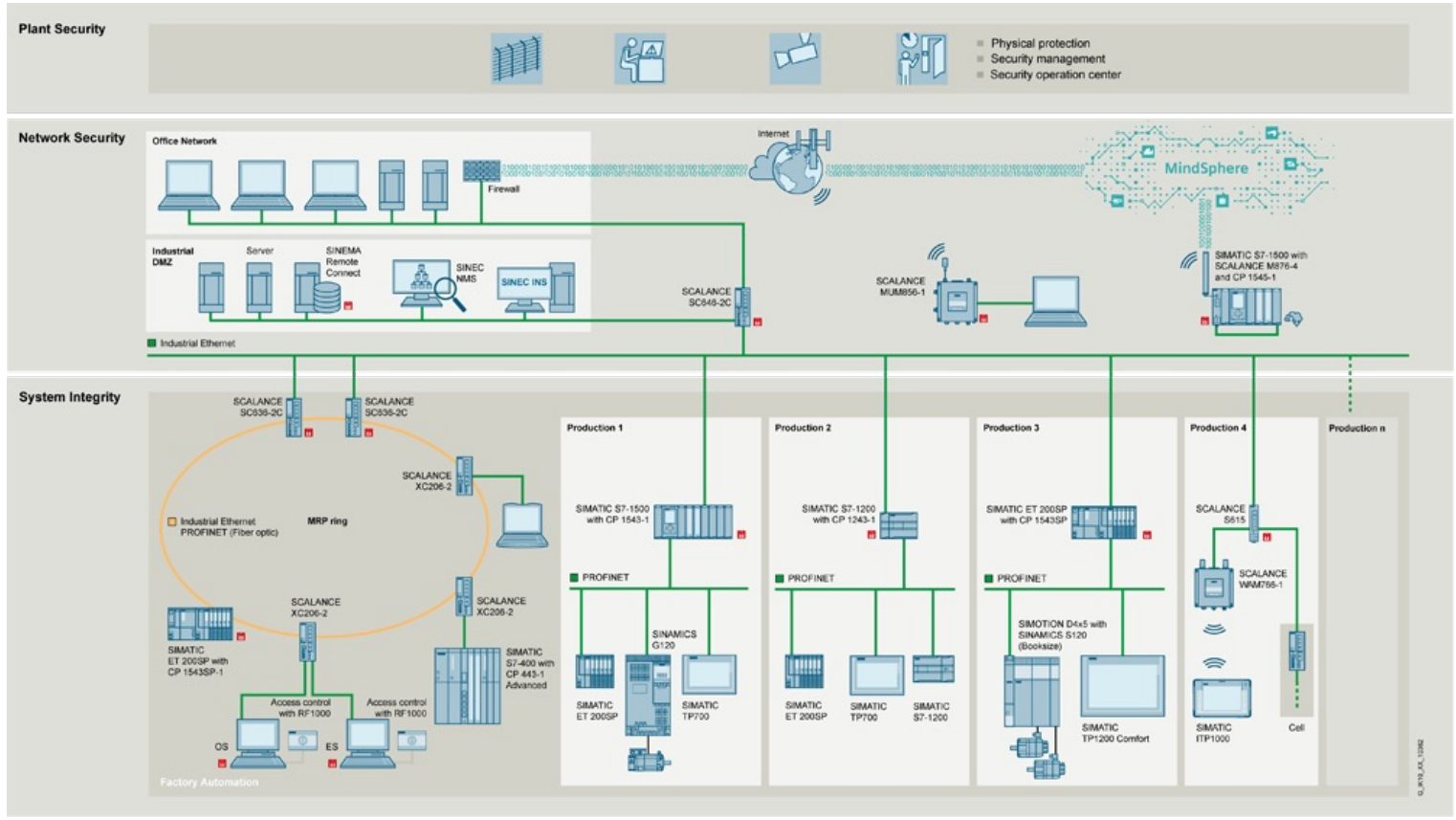
Redundancy

- 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

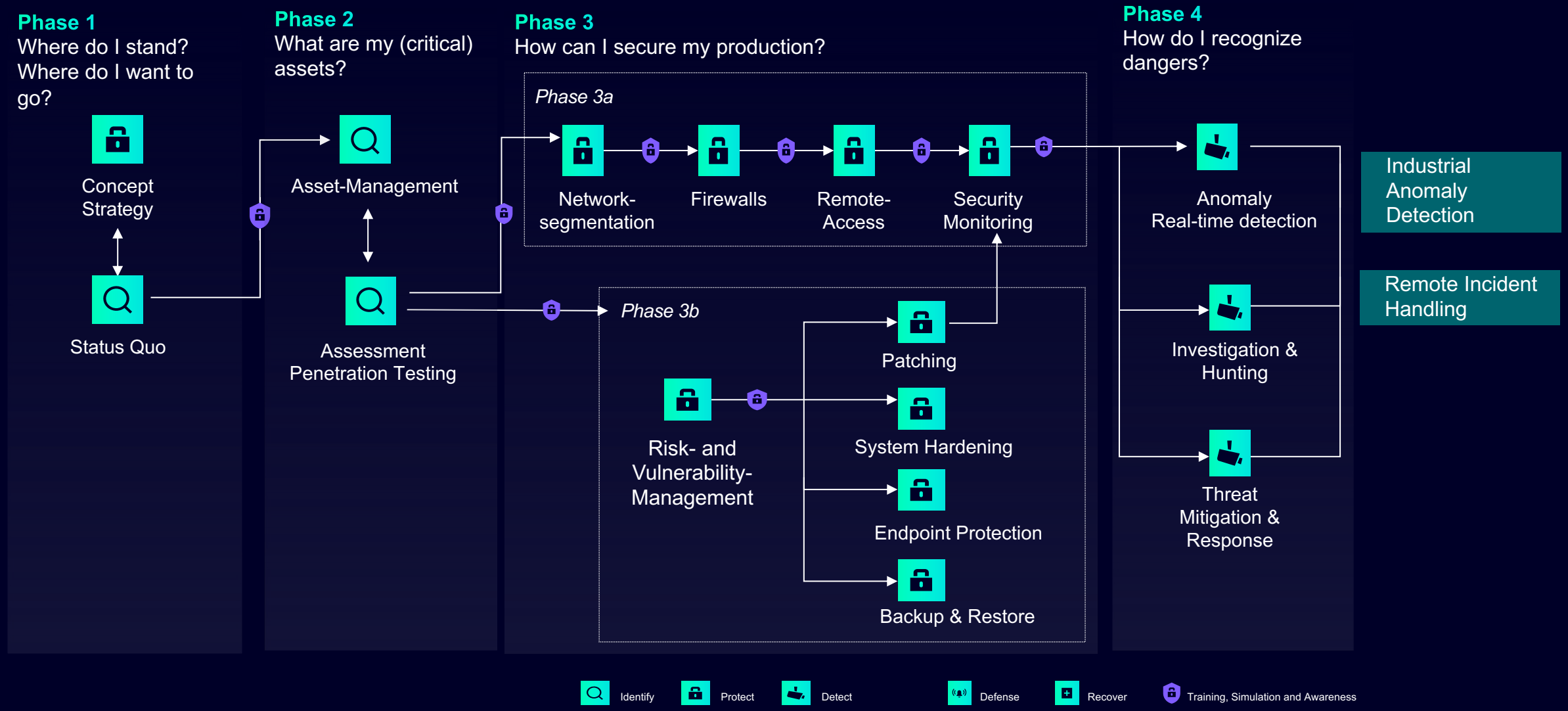
For information on cybersecurity solutions with RUGGEDCOM, visit
www.siemens.com/ruggedcom/cybersecurity



Products with firewall or VPN functionality

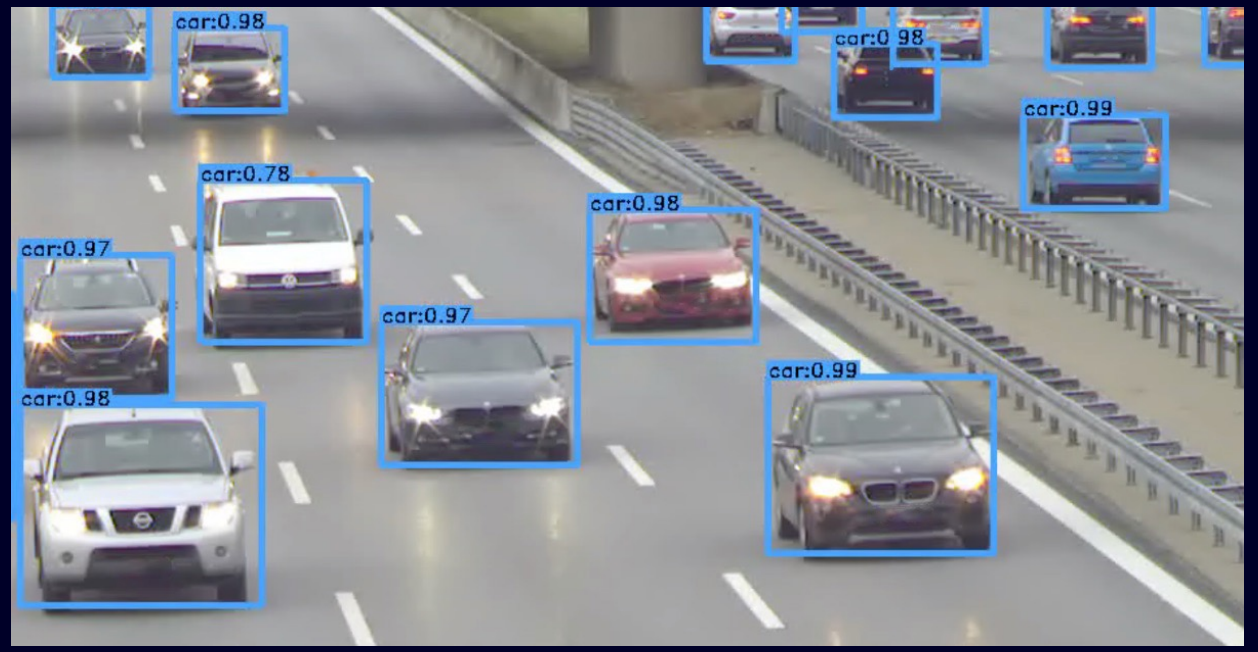
SIEMENS

Cybersecurity Services – Step by Step



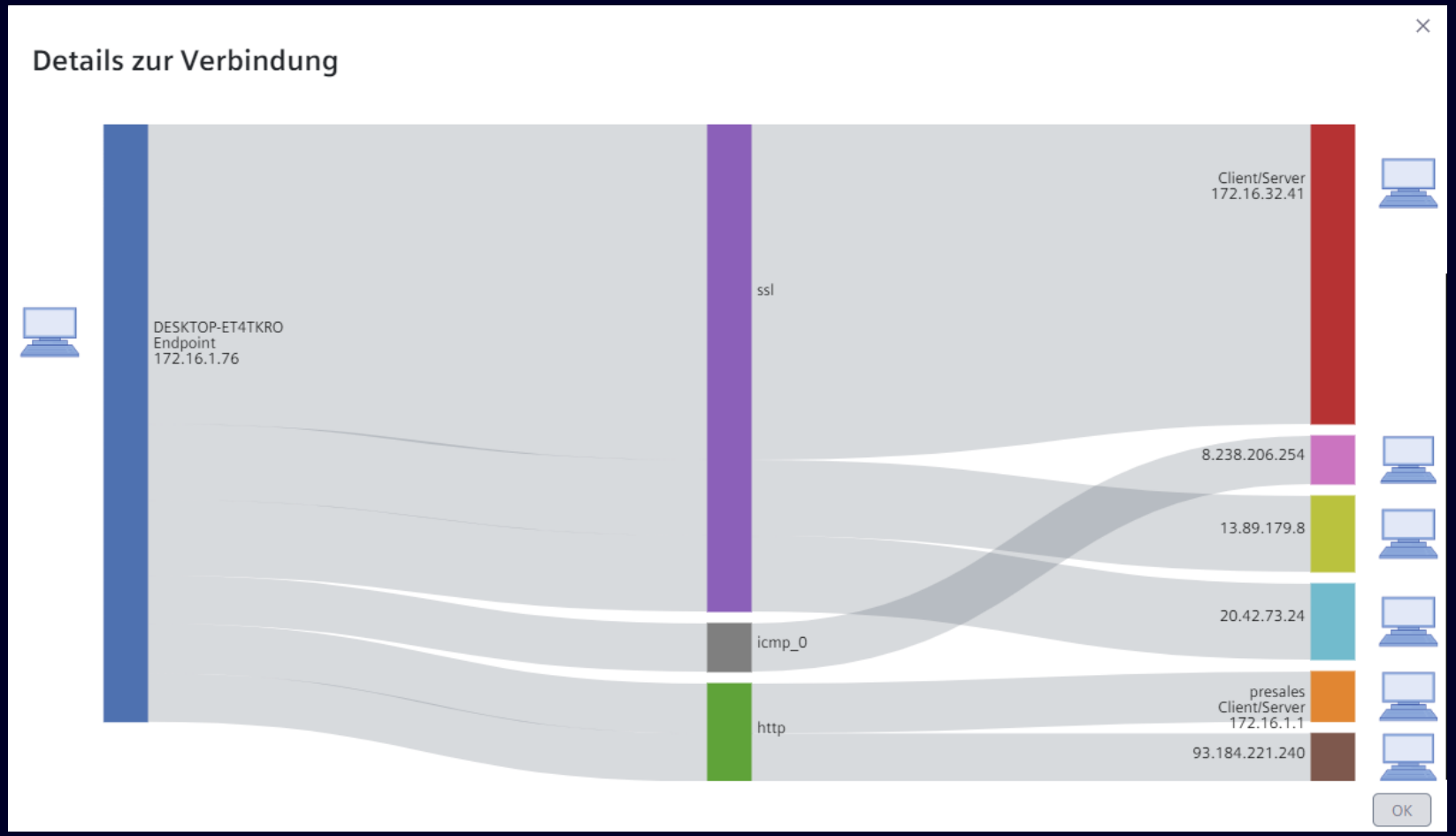
SIEMENS

Anomaly Detection – Anlernphase (Überwachung des Verkehrs)



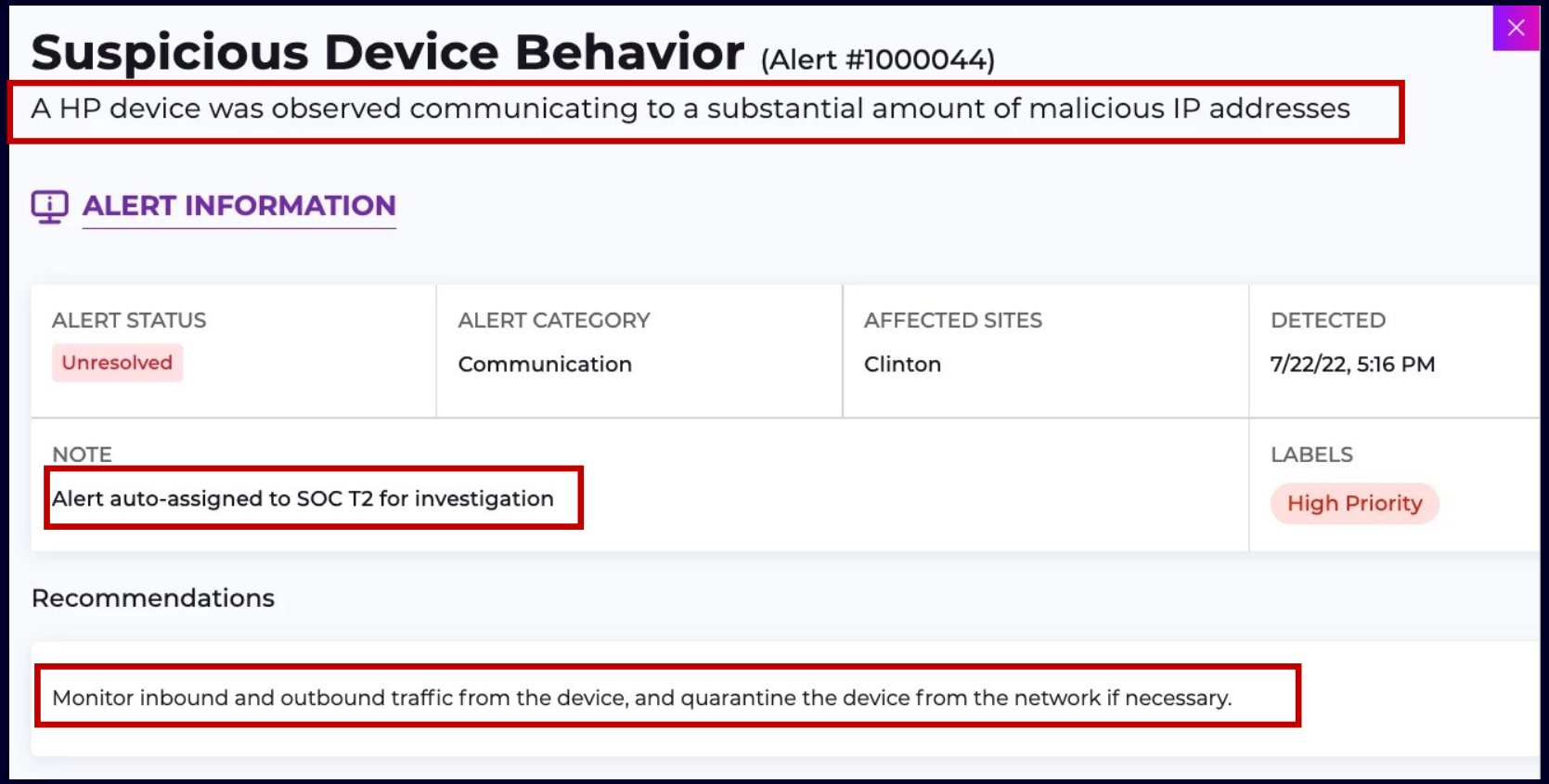
SIEMENS

IP traffic – who is talking to whom via which protocol



SIEMENS

Anomaly Threat Detection



SIEMENS

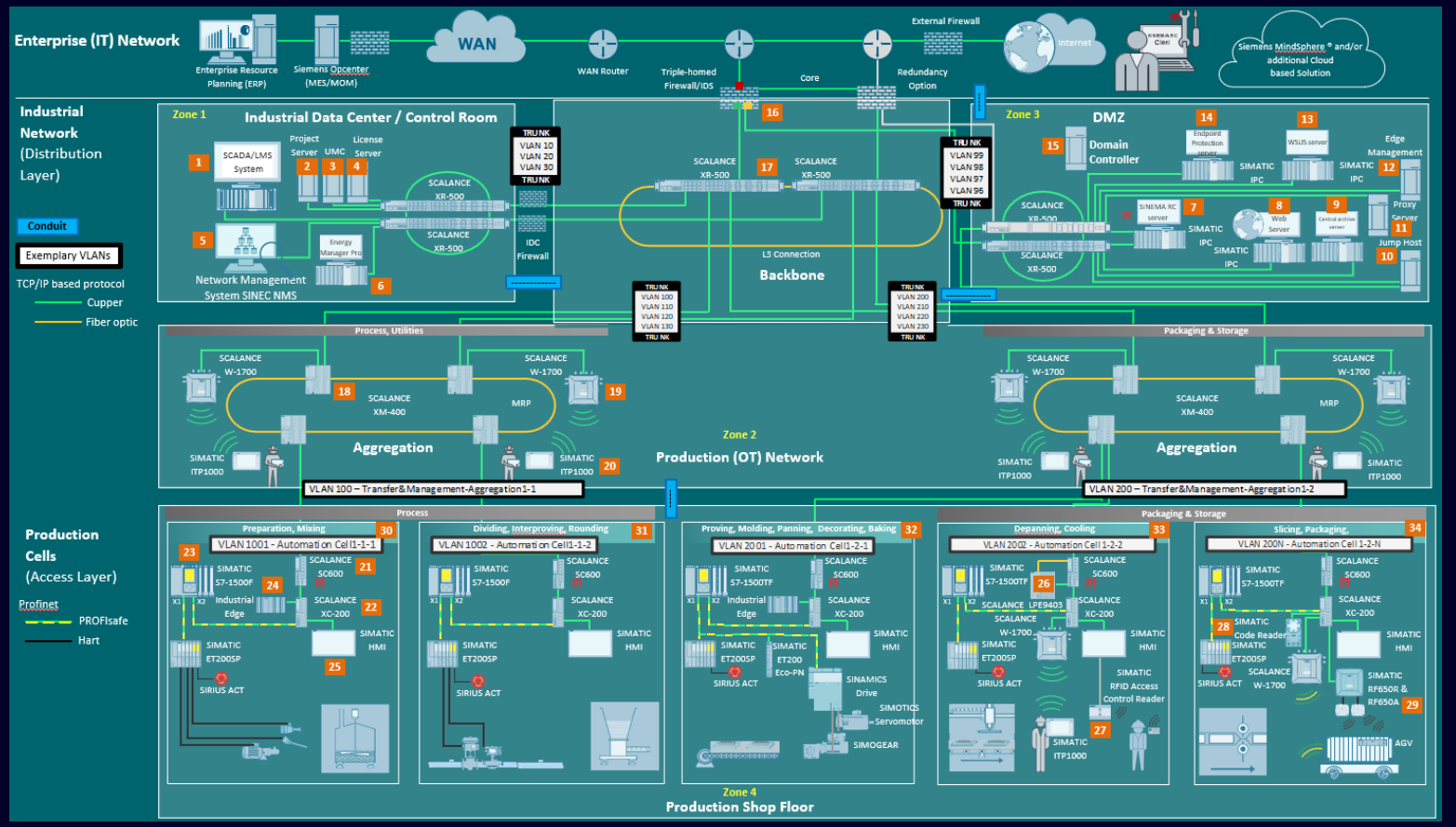
Security Events - automatic event creation based on a control system

SIEMENS

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



SIEMENS

Remote Access

Asset Inventory Scan

Assessment

Firewalls

End Point Protection

How we can support you to protect your operations

Risk Awareness

Whitelisting

DMZ

Patch Management

Network Segmentation

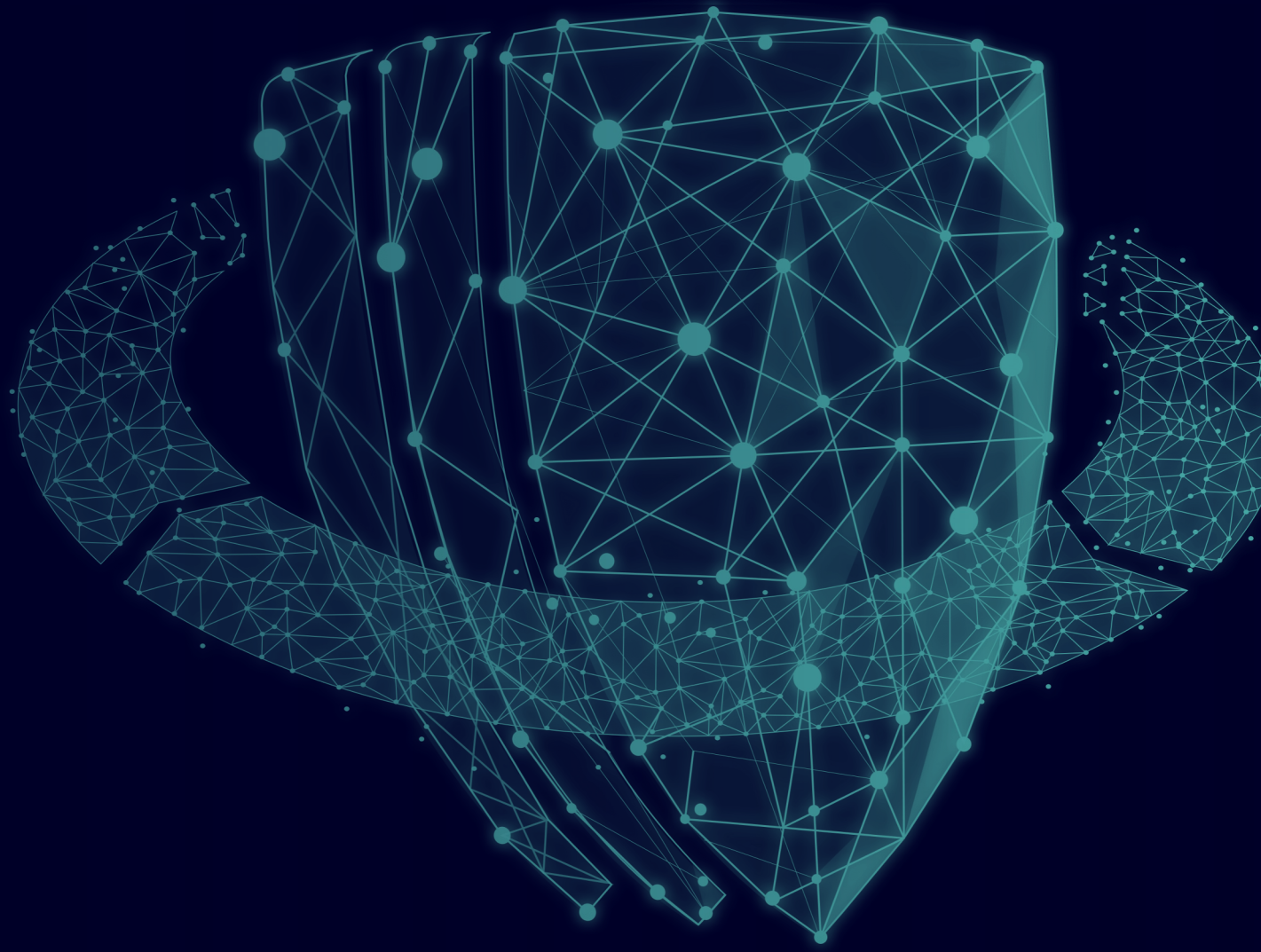
Anomaly Detection

Network Monitoring & Management

SIEMENS

Thank You!

SIEMENS



Published by Siemens AG Österriech

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

SIEMENS