Support and solutions for Cyber Resilience

Cybersecurity can only be tackled **together!**



© Siemens 2026 | Unrestricted | DI Horizontal Cybersecurity

SIEMENS



Our purpose has guided us
for more than 175 years:

We create technology **to transform the everyday, for everyone.**











Unrestricted | © Siemens 2026

SIEMENS

From Efficiency to Resilience

HSEQ



- Health
- Safety
- Environmental
- Quality & Regulations

Costs



- CAPEX Efficiency
- OPEX Reduction

Flexibility



- Individual products
- Volatile markets
- Technology Lifecycle

Time to market



- From Idea to Product
- Ramp-up of Plant
- Responsiveness

Output



- Increased Performance
- OEE Effectiveness
- Efficiency and Reliability

CYBER RESILIENCE AS FOUNDATION

© Siemens 2026 | Unrestricted | DI Horizontal Cybersecurity
SIEMENS


STOPPED
FOR
3 MONTHS

Cybersecurity is no longer an IT responsibility.

IT‘S A COMPANY-WIDE BUSINESS PRIORITY.

© Siemens 2026 | Unrestricted | DI Horizontal Cybersecurity
SIEMENS

The news are exploding

TECHNOLOGY AND IIOT

Why Do Cybercriminals Love Manufacturers So Much?

July 11, 2023 1

And will the problem ever stop getting worse?

In 2025, many manufacturers in **automotive and F&B industry** experienced a cyberattack including ransomware that stopped their production in several locations.

CSIS Programs > Strategic Technologies Program

Significant Cyber Incidents

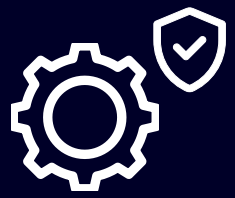
This timeline records significant cyber incidents since 2006, focusing on cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

Stopped productions



SIEMENS

Causes for the increase of IT / OT Breaches



Poor awareness of security risk



Very large attack surface



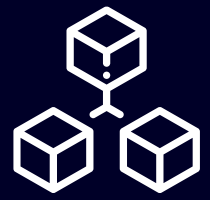
Legacy devices and weak security



The main reason…



Heterogeneous comm protocols



Growing (remote) interconnections



Poor User Management

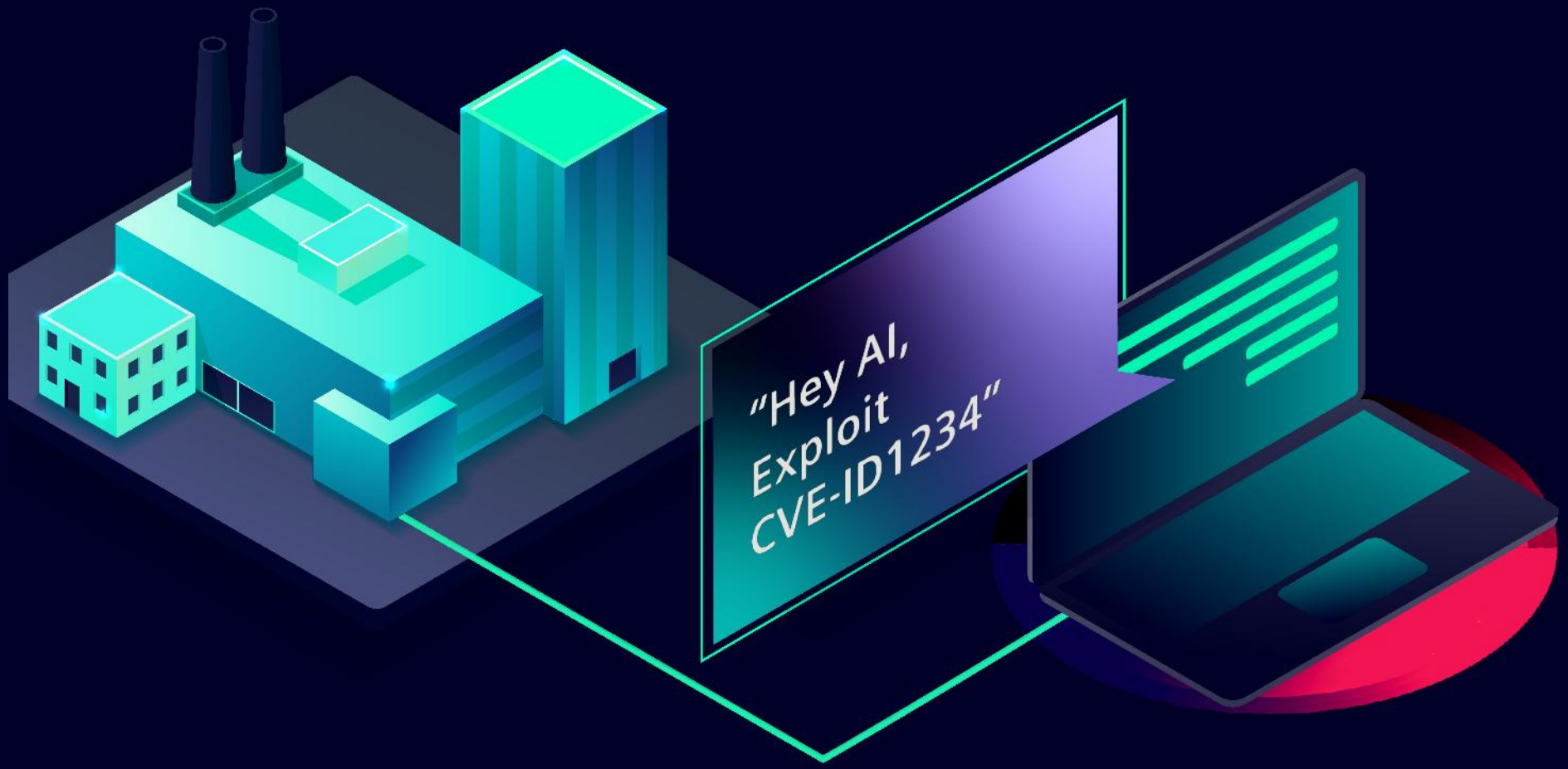
SIEMENS

Maybe it is my responsibility, but that still needs to be said.

Interview at Senior management
at a major global F&B company.



AI Agents running the first 3 steps of the Cyber Kill Chain with factory focus



SIEMENS

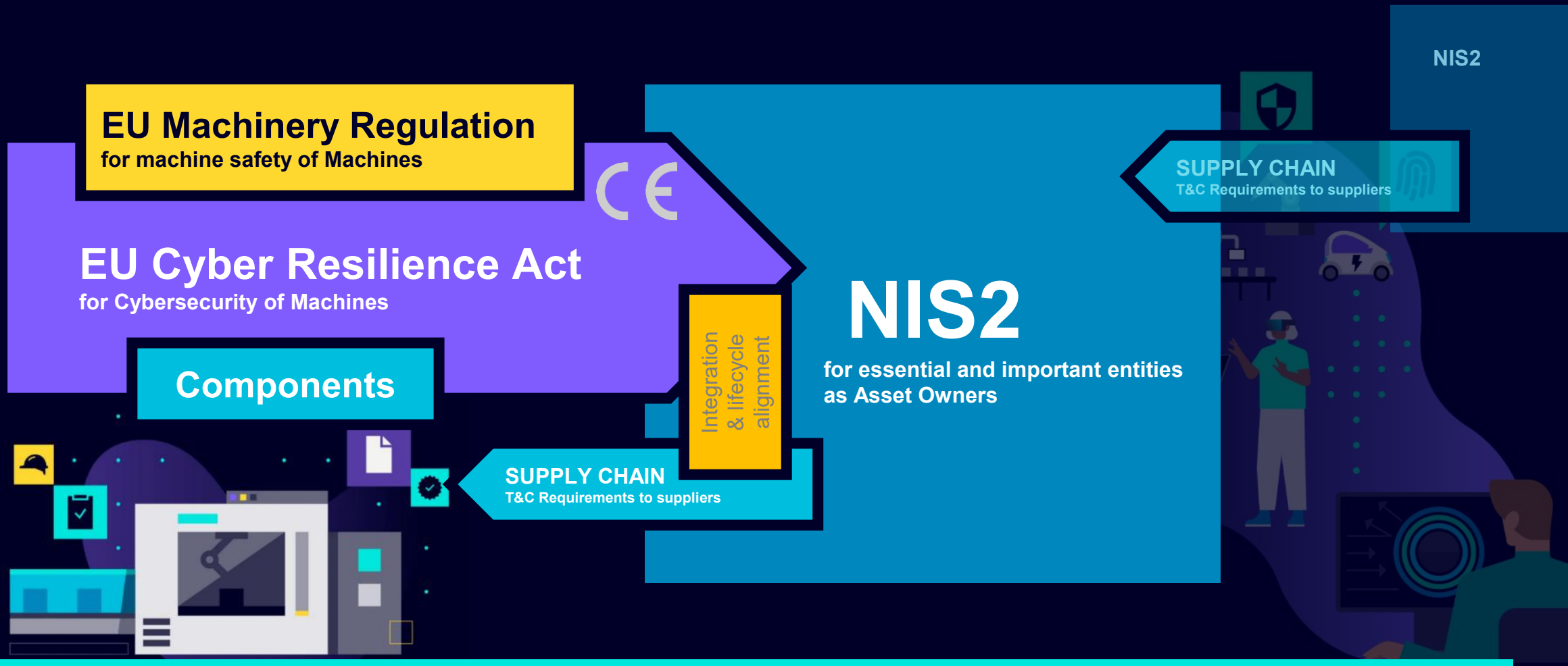
Legislators are responding globally

Demanding use of “Relevant Standards”



SIEMENS

How do cybersecurity regulations relate to each other?
Safety and cybersecurity are being connected

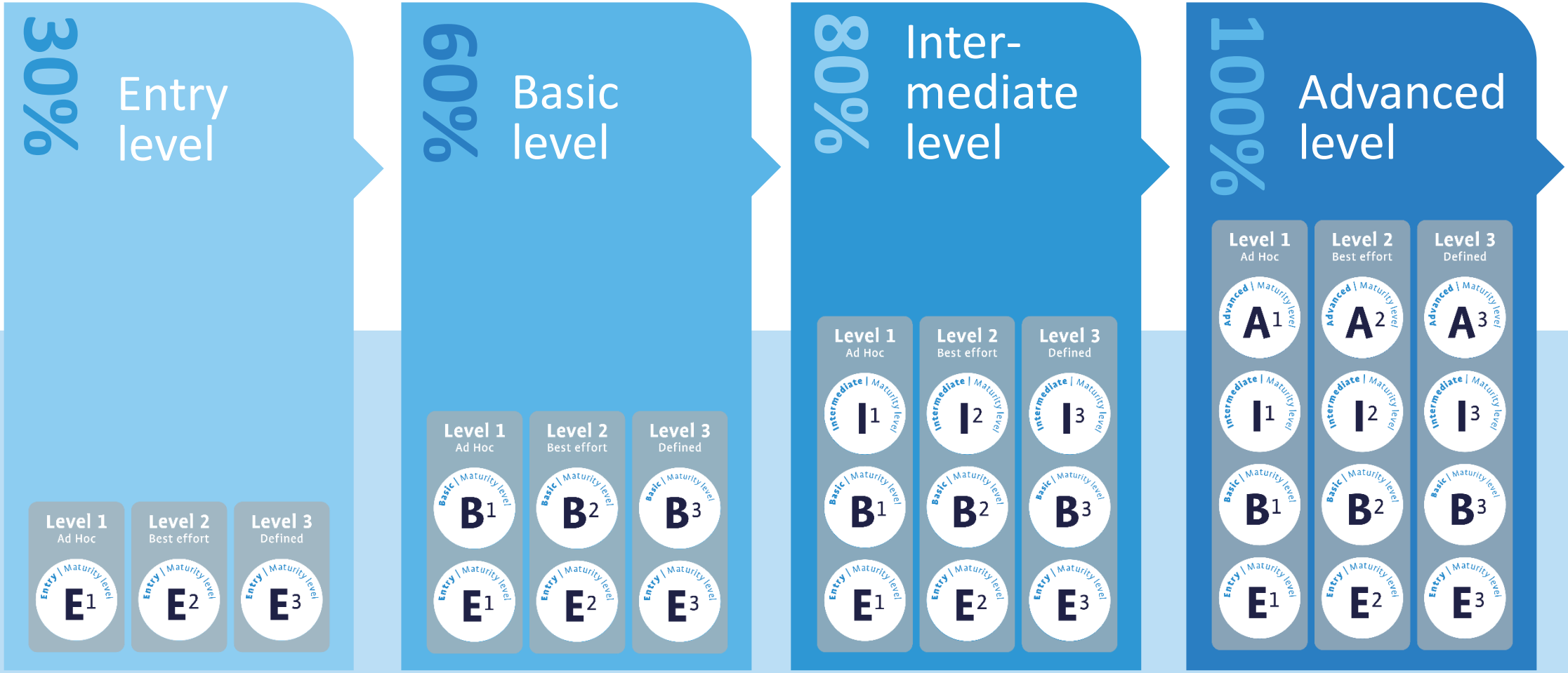


For industrial Cybersecurity: The *IEC62443* is the *"relevant standard"* for everyone

SIEMENS

The CYRA-method: grow maturity

Based on ISO27000 & IEC62443

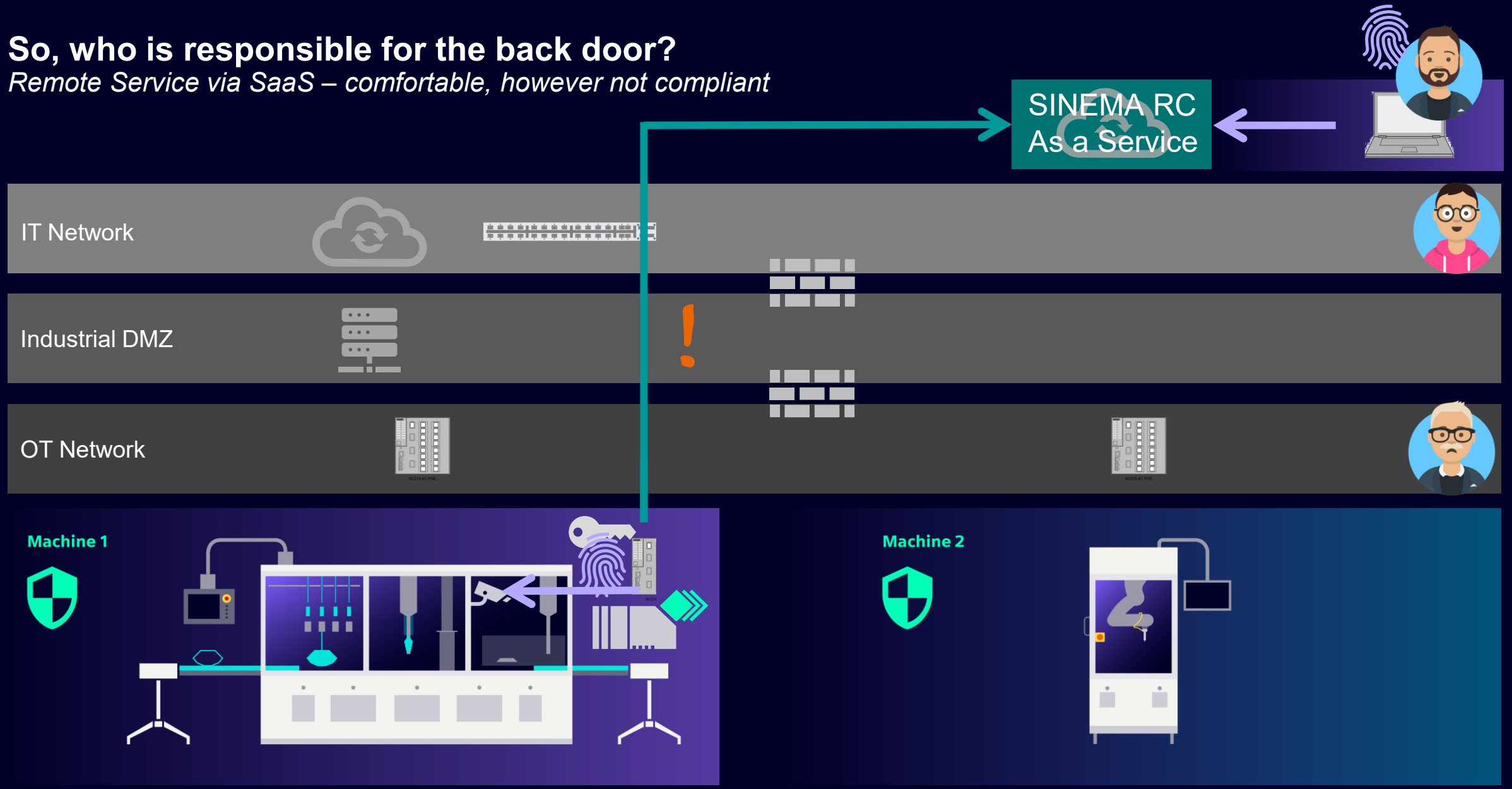


hetccv.nl/cyra

SIEMENS

So, who is responsible for the back door?

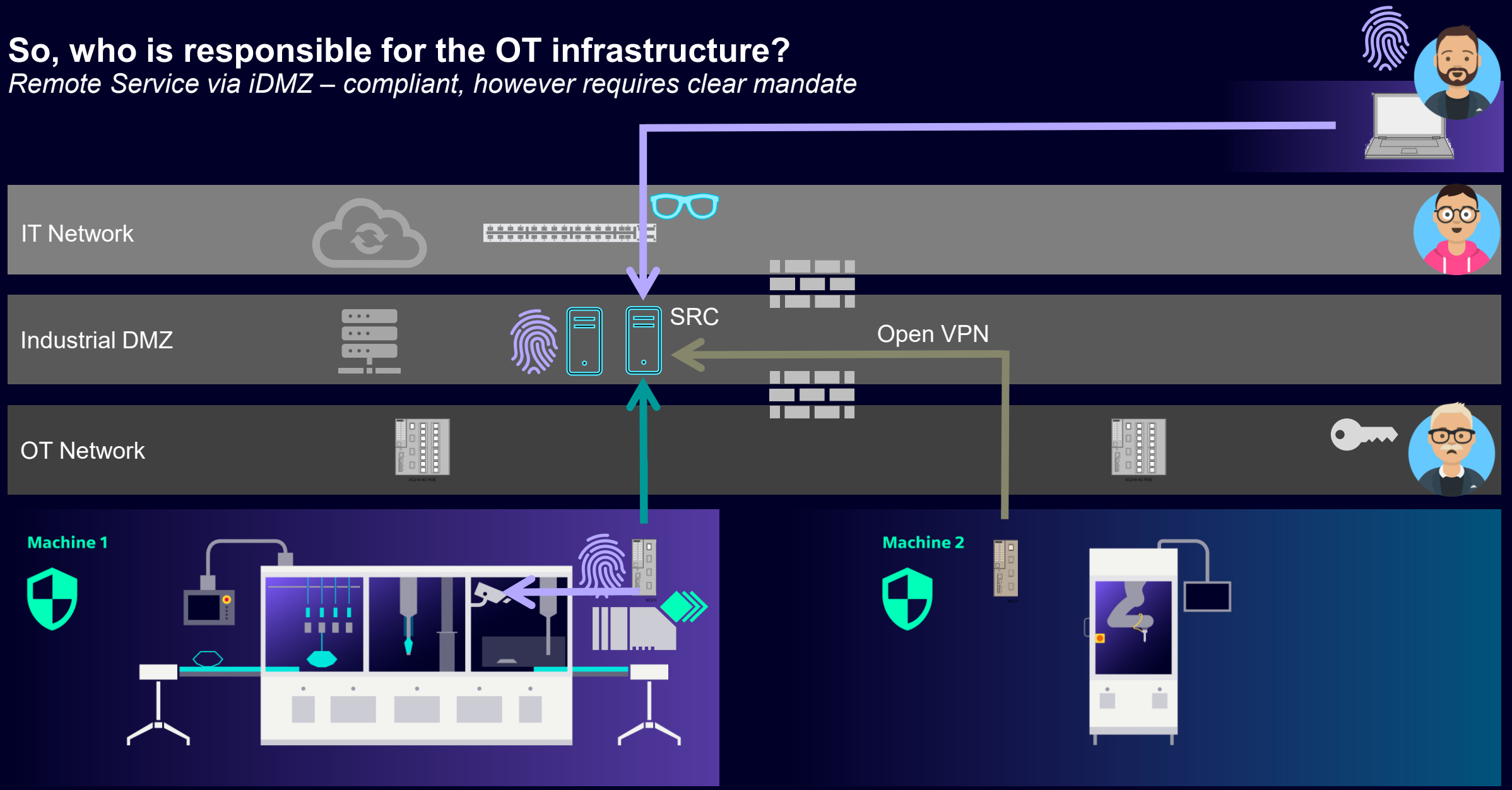
Remote Service via SaaS – comfortable, however not compliant



SIEMENS

So, who is responsible for the OT infrastructure?

Remote Service via iDMZ – compliant, however requires clear mandate



SIEMENS

System Lifecycle
Considering security capabilities

Project delivery

Last 5 years
Prepared, need for evaluation

Older than 5 years
Capable, need for research

Older than 10 years
Not built-in, need bolt-on

Older than 25 years
Take extra care



Remember, you cannot simply replace this equipment

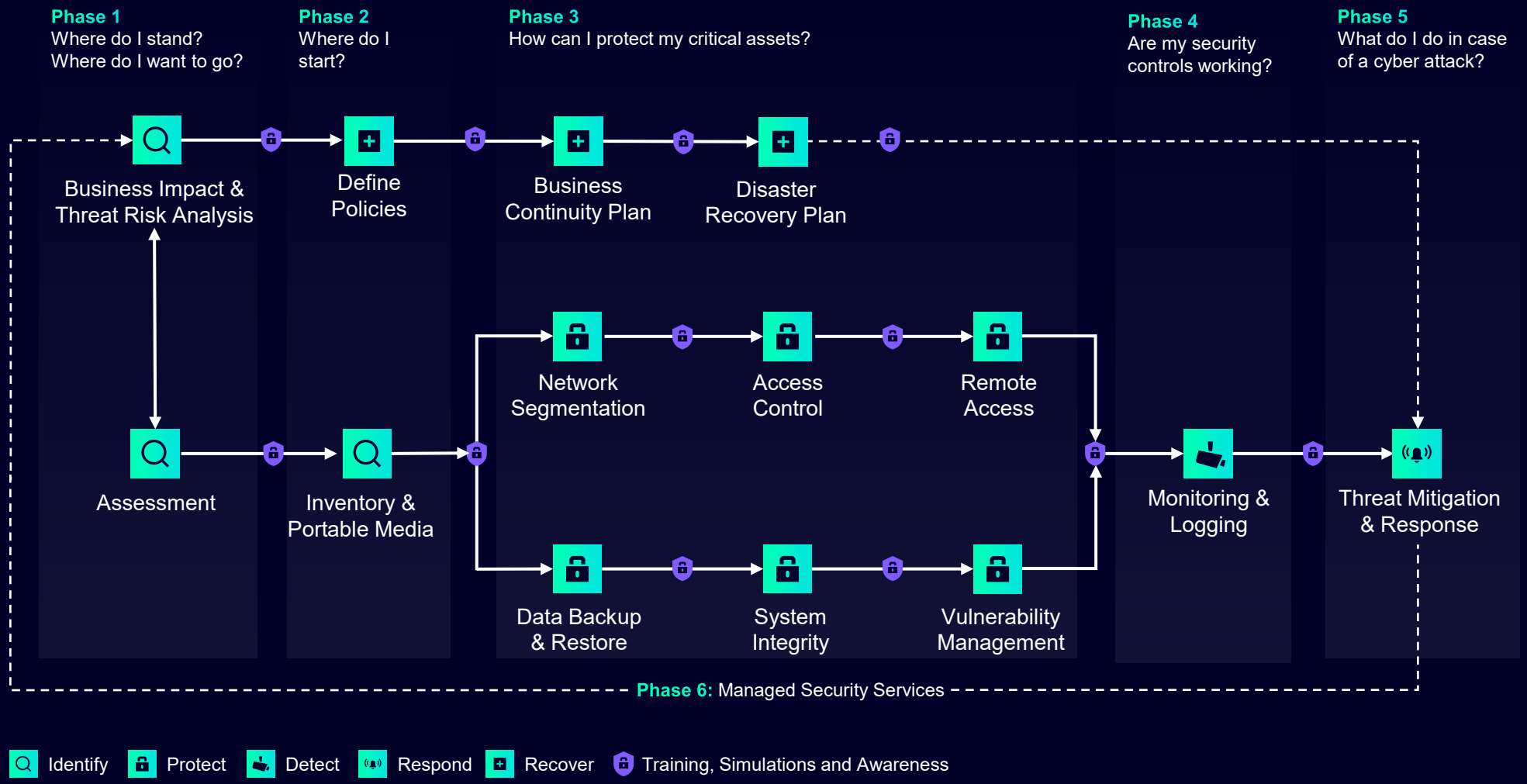
SIEMENS

No technology without a plan



Preventive measures: #OTsecurityJourney

Based on NIST & IEC62443

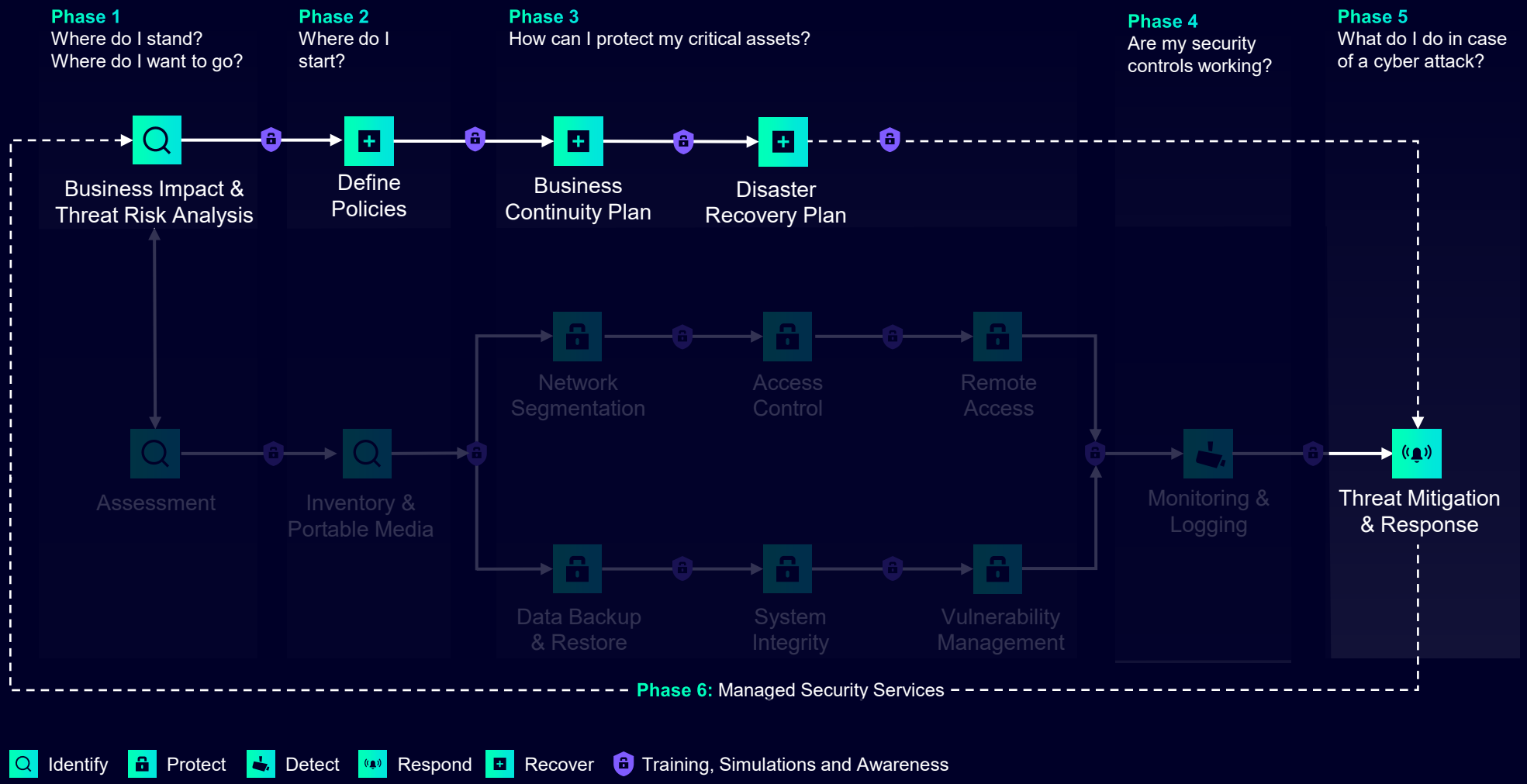


© Siemens 2025 | **Unrestricted** | DI Horizontal Cybersecurity

SIEMENS

Preventive measures: #OTsecurityJourney

Based on NIST & IEC62443

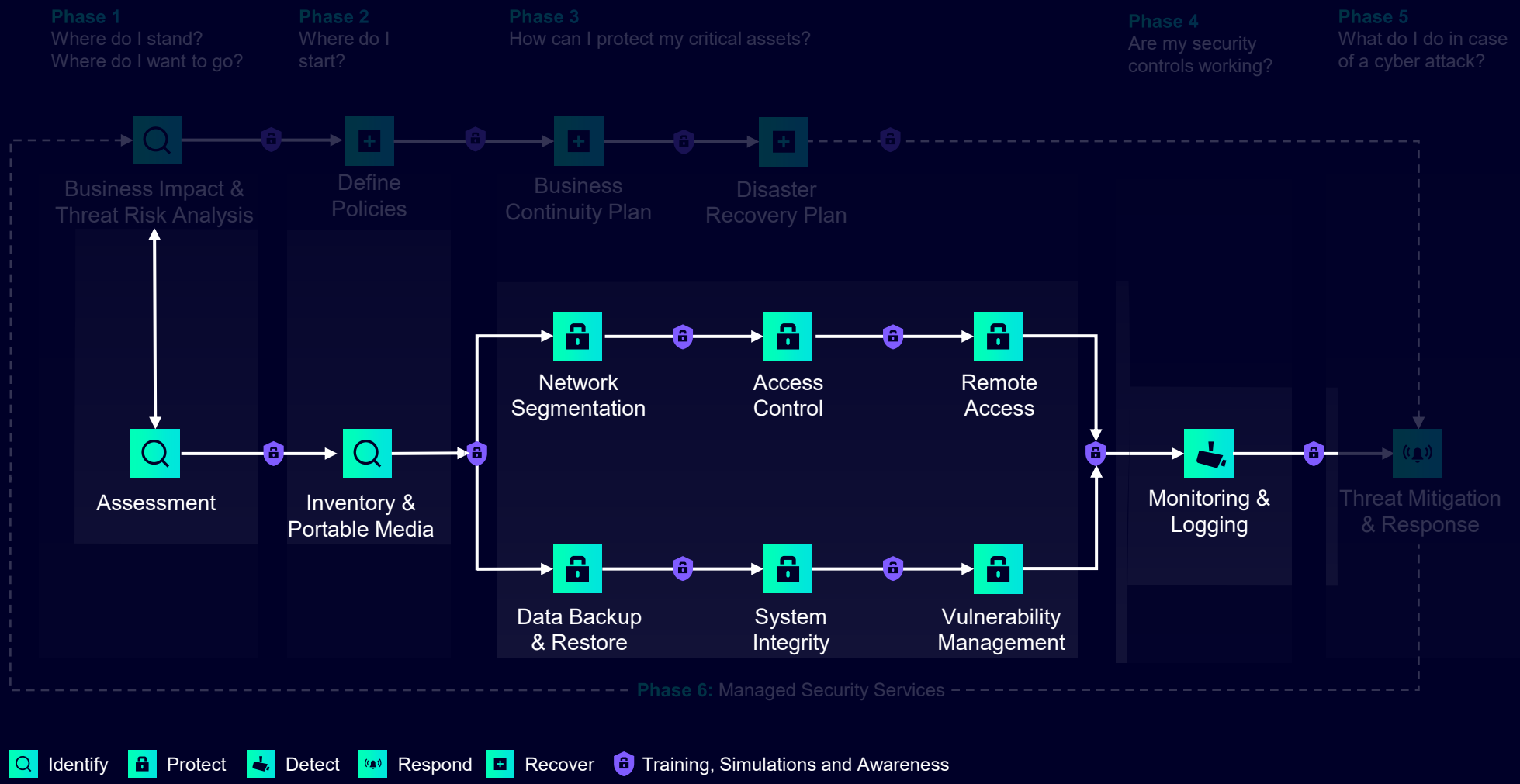


© Siemens 2025 | **Unrestricted** | DI Horizontal Cybersecurity

SIEMENS

Preventive measures: #OTsecurityJourney

Based on NIST & IEC62443



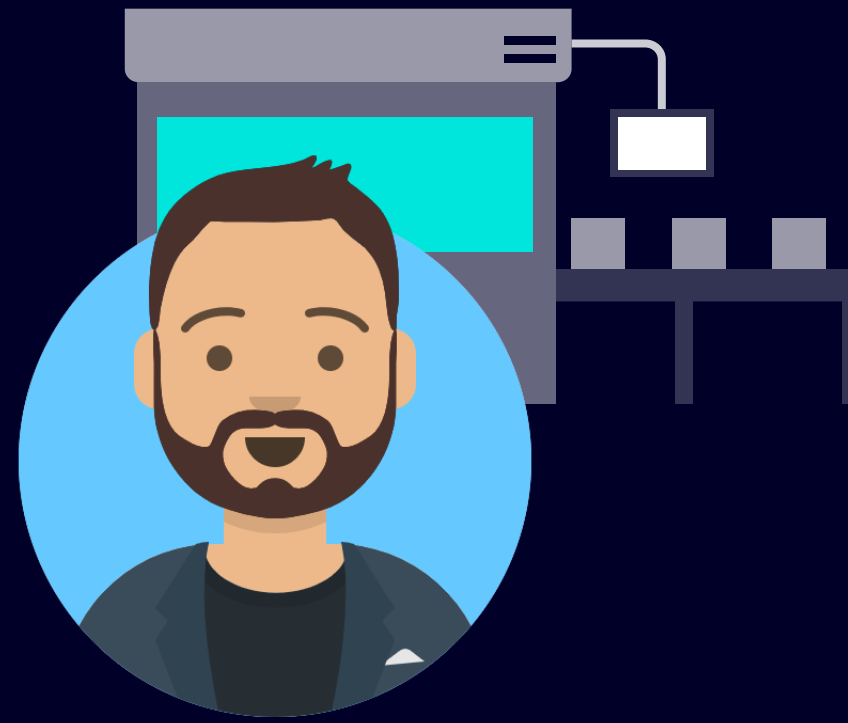
© Siemens 2025 | **Unrestricted** | DI Horizontal Cybersecurity

SIEMENS

Make, Buy or Partner?

This is the moment to redefine your strategy





© Siemens 2025 | **Unrestricted** | DI Horizontal Cybersecurity

SIEMENS

New guideline for production machines

NEW

How to design a secure machine

Hardening for PLC, HMI, Drive, Firewall

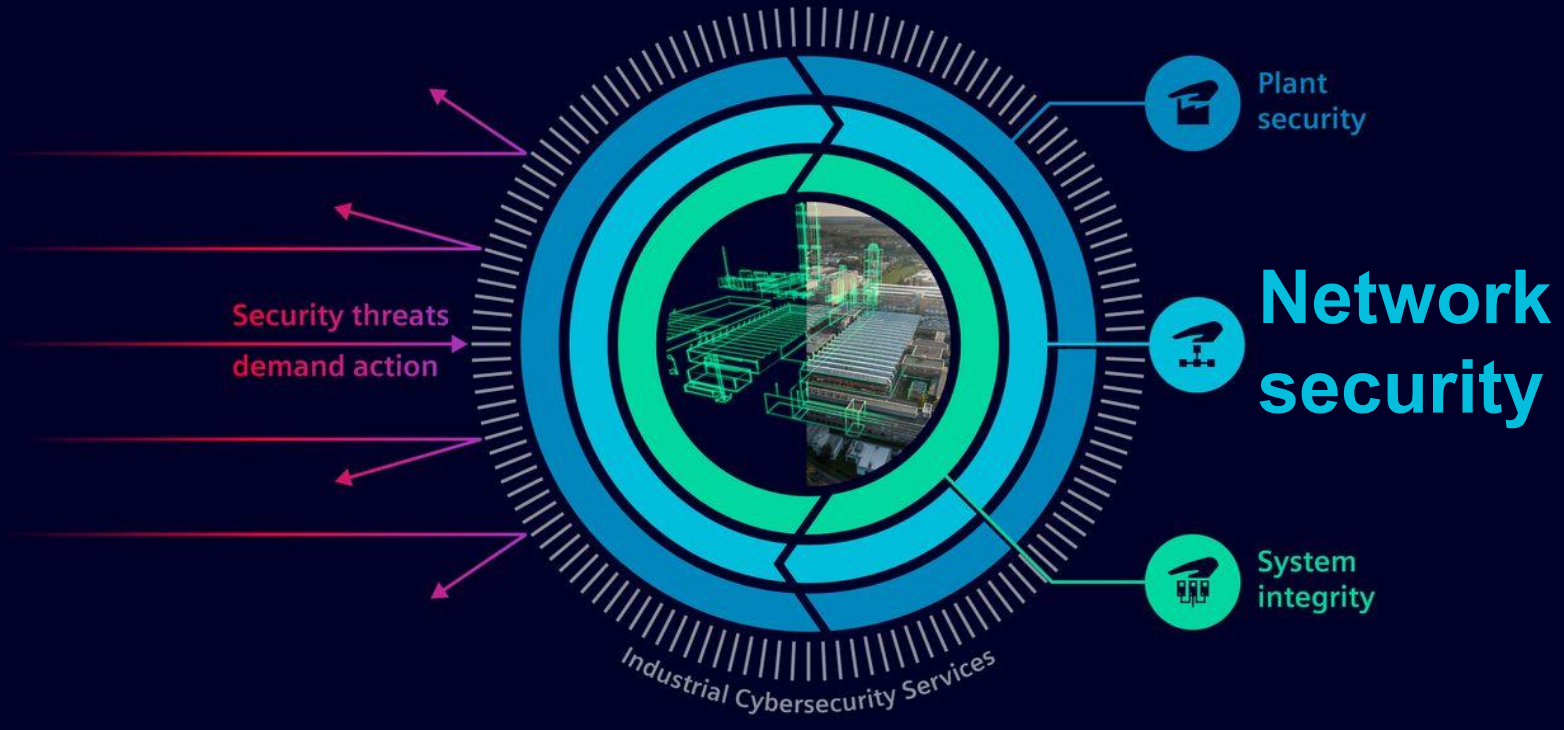
Detailed instructions for the configuration



SIEMENS

Elevating Defense in Depth
Seamlessly integrate existing deployments into advanced security architectures

Defense in Depth remains state-of-the-art.



“Defense in Depth” according to IEC 62443

Classical cell protection …

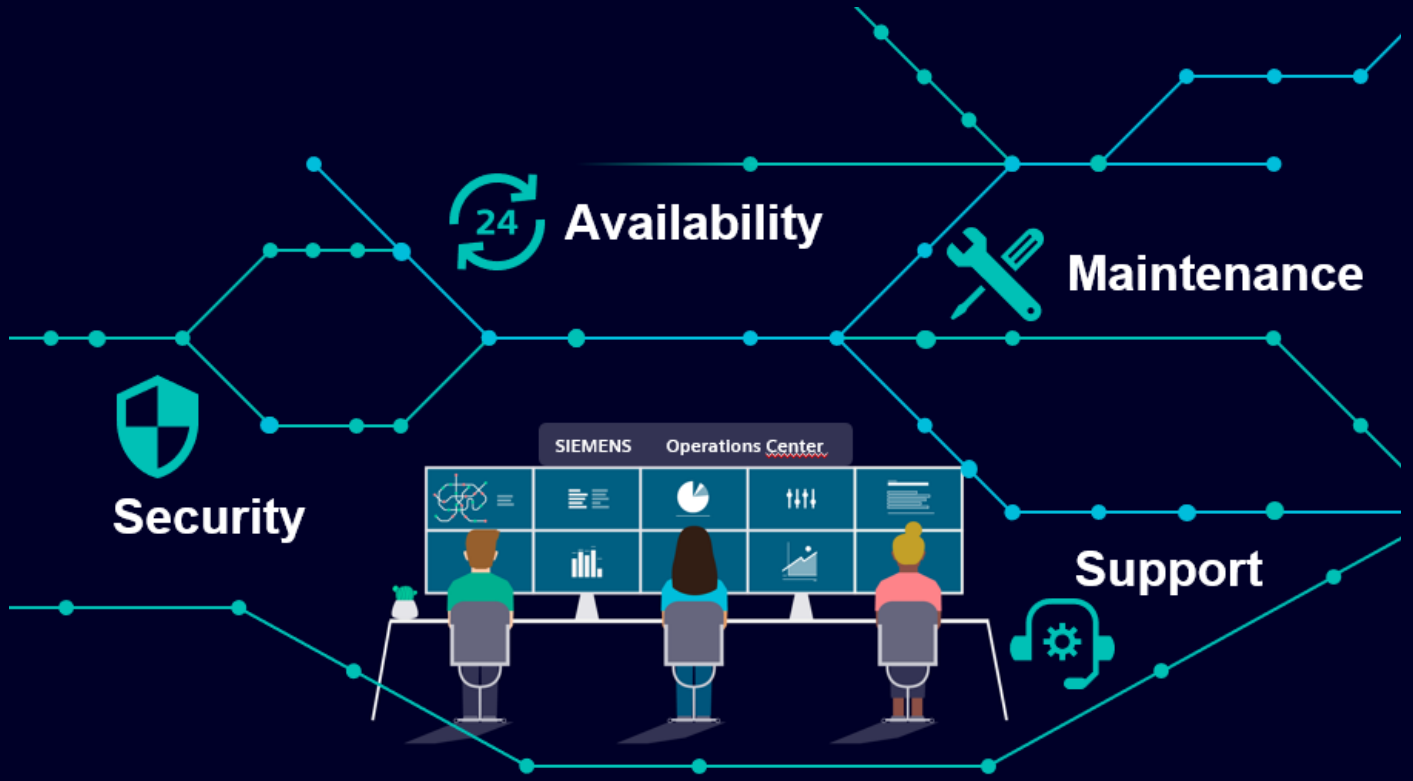


… enriched by Zero Trust with SINEC Secure Connect.



SIEMENS

Remote Industrial Operations Services?
Our OT - Operations Center takes care of…..



Services including reporting	
Available	Continuous Monitoring
	Incident Management
	Network Management
	Domain Management
Secured	Vulnerability Management
	Anomaly Detection
	Security Operations Center as a Service
Maintained	Periodic & Preventive Maintenance
	Updates & Patches
	Back-up & Restore
Supported	Remote Support (via secure VPN connection)
	Service Desk
	Service Request
	Technical Product & Hardware Support

SIEMENS



What is your next step…?

SIEMENS

Thank you



Cybersecurity can only
be tackled **together!**

Ruud Welschen

