NISDUC
NIS Directive User Community

Ministerie van Infrastructuur en Waterstaat

SIEMENS

NIS2 AND SUPPLY-DEMAND DYNAMICS

Johan de Wit (Siemens)
Jeroen Gaiser (Ministry of Infrastructure and Water Management)

April 23rd 2024

TLP:GREEN

WHO ~~NEEDS~~ *to pay for* WANTS CYBER RESILIENCE?

(ESPECIALLY IN OPERATIONAL TECHNOLOGY)

WHO ARE WE?

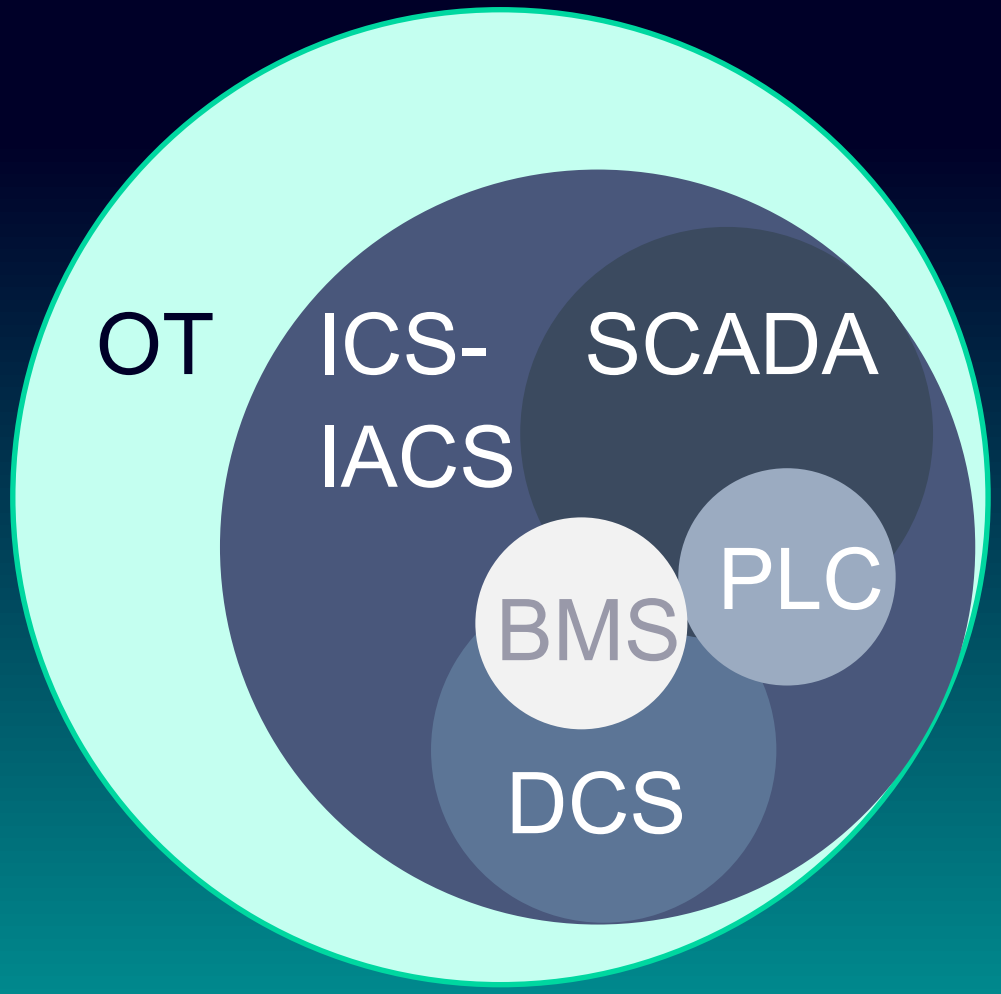
JOHAN DE WIT

JEROEN GAISER

WHAT IS OPERATIONAL TECHNOLOGY (OT)?

(AND WHY TALK ABOUT IT REGARDING NIS2?)

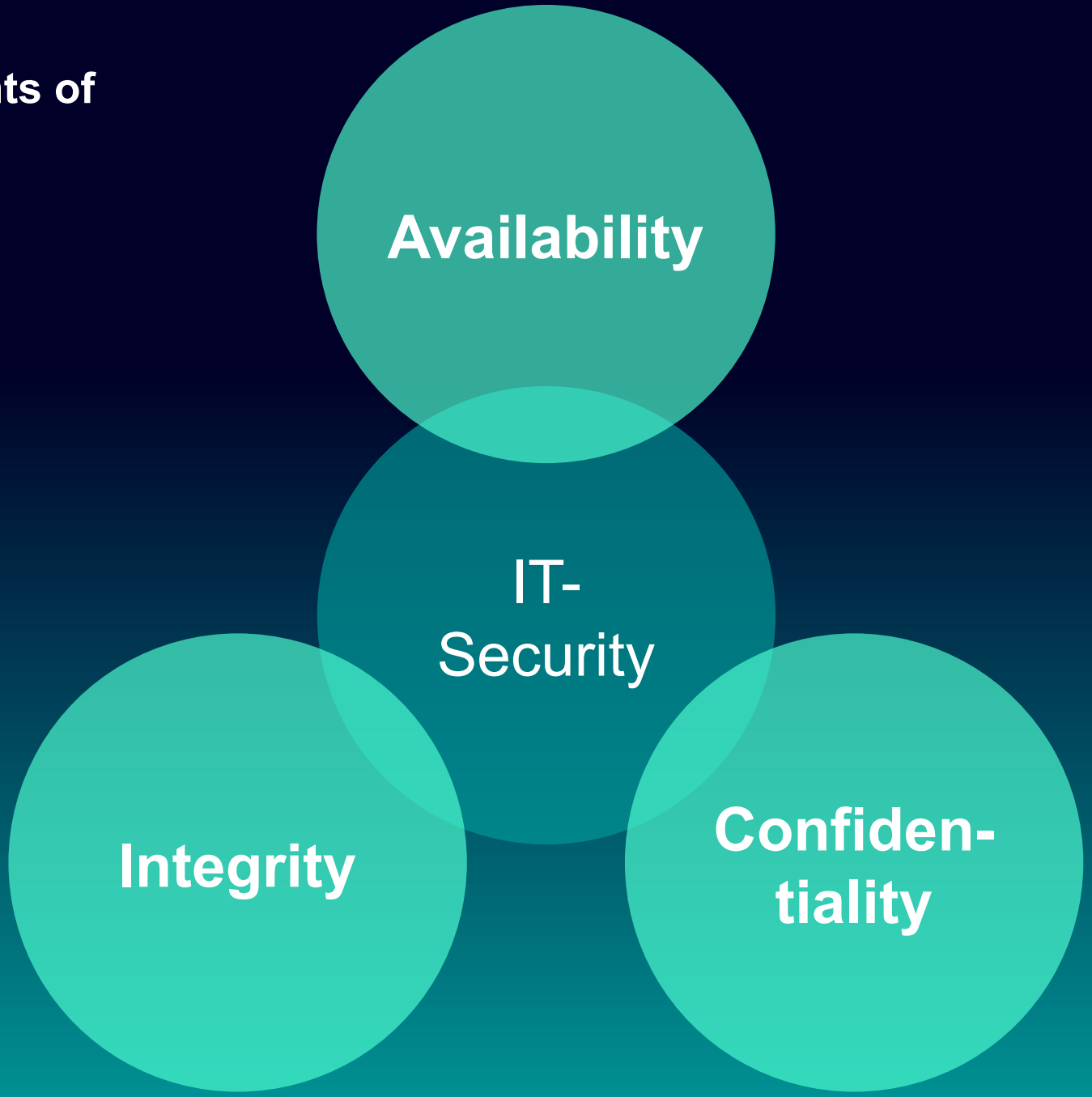
ICS, OT, SCADA, PCS, DCS, IACS: Proces Automation



OT: Operational Technology
ICS: Industrial Control System
IACS: Industrial Automation and Control System
SCADA: Supervisory Control And Data Acquisition
DCS: Distributed Control System
PCS: Process Control System
PLC: Programmable Logic Controllers
BMS: Building Management System

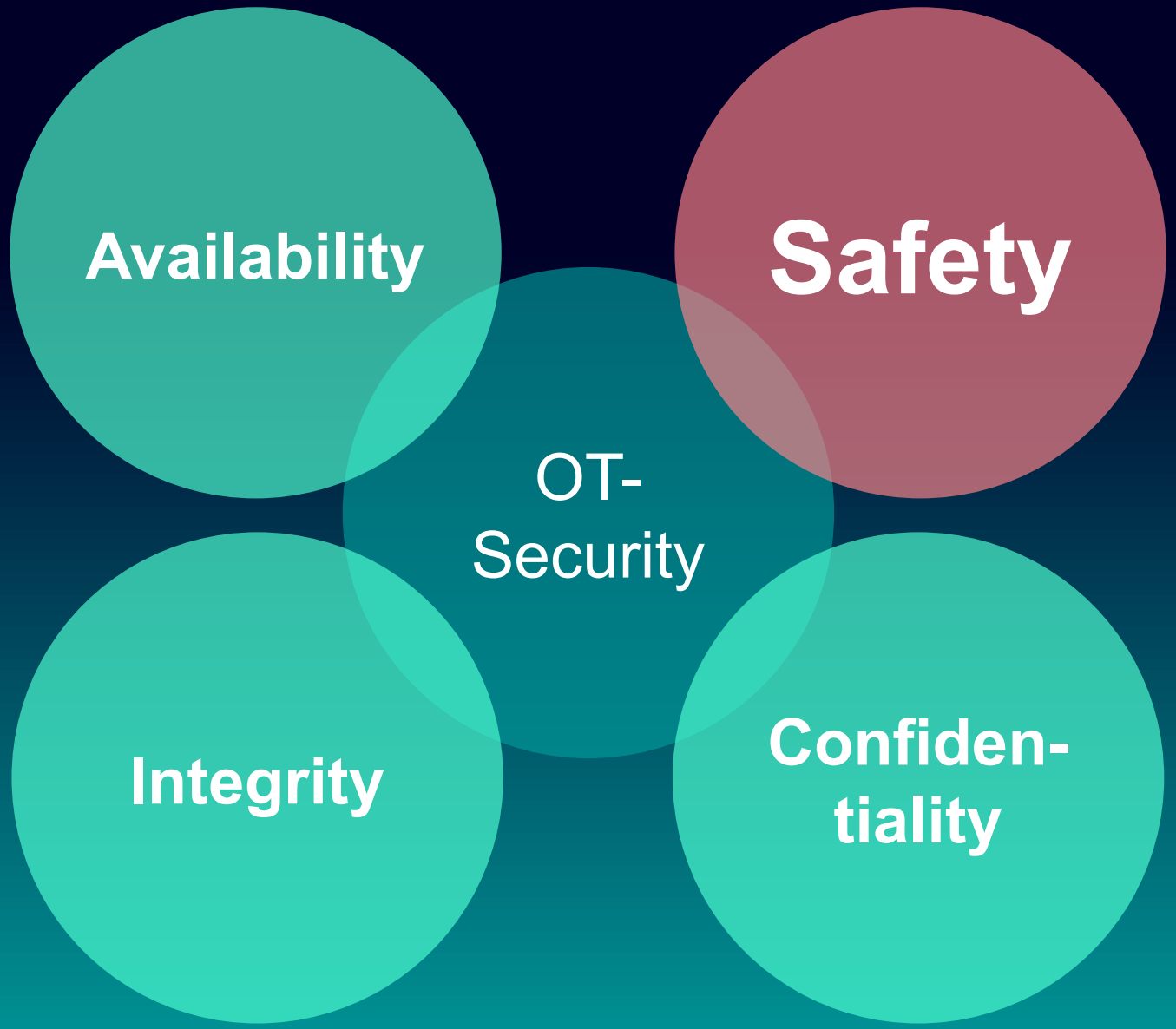
SIEMENS

The *three* components of IT security



SIEMENS

The four components of OT security



SIEMENS

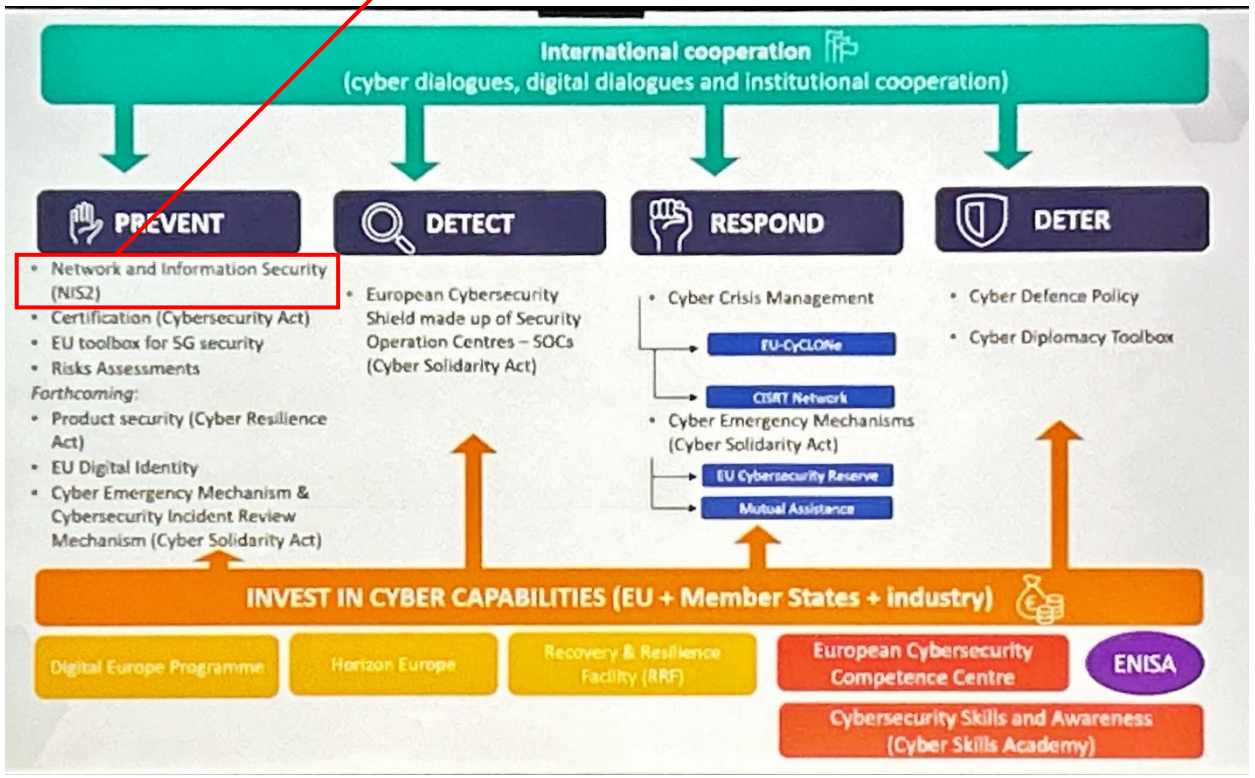
NIS2 GOAL

INCREASING EU-WIDE CROSS SECTORAL AND TRANSNATIONAL RESILIENCE TO CYBERRISK

NIS2 PLACE IN EU CYBERSTRATEGY

NIS2 (demand)

Deadline: October 2024

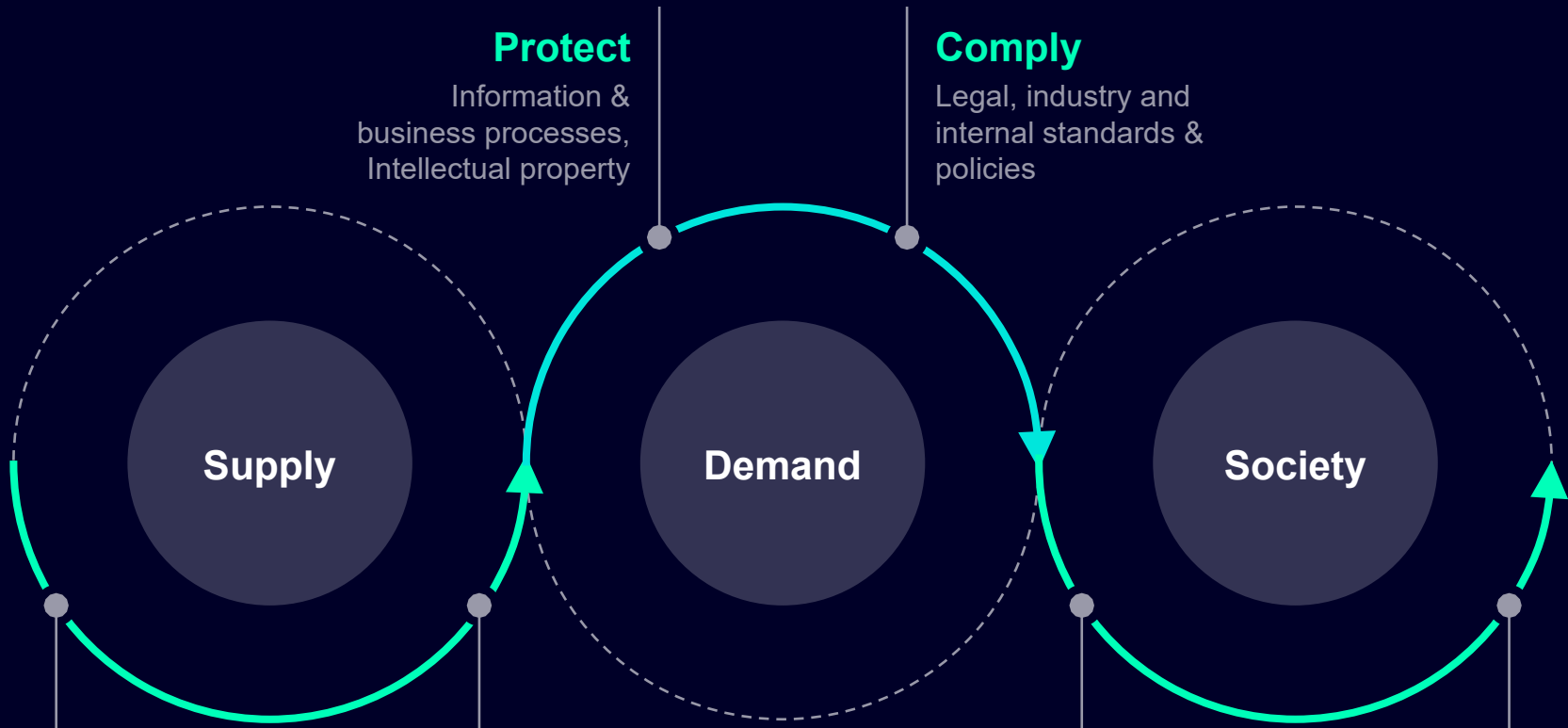


- NIS2 is part of the broader EU cybersecurity strategy
- Different aspects to increasing resiliency
- Start with the demand side: the user of digital technology

CREATING DEMAND: THE NECESSITY OF CYBER RESILIENT OT

- OT IS SEEN AS A VIABLE TARGET IN GEOPOLITICAL CONFLICTS
- IT TAKES A LOOOONG TIME TO CHANGE THINGS IN OT (SO START ASAP)
- CYBER RESILIENCE IS NOT WELL RECOGNIZED YET AS A RISK CATEGORY IMPACTING SAFETY/FUNCTION
- SECURITY BY DESIGN FOR OT IS A NEW PRINCIPLE FOR MOST
- HOW DO YOU DEFINE CYBERSECURITY REQUIREMENTS IN CONTRACTS THAT MAY SPAN DECADES?
- HOW DO YOU AUDIT AND REGULATE CYBERSECURITY IN OT (THIS IS A FAIRLY NEW SKILLSET)
- THE (POSSIBLE) EFFECT OF REGULATION ON ENFORCING CYBERSECURITY REQUIREMENTS INTO CONTRACTS

Cyber Security to protect:



SIEMENS

Cyber Security to protect:

Protect
Information & business processes, Intellectual property

Comply
Legal, industry and internal standards & policies

European Commission

Supply

Demand

Society

European Commission

NIS2 Directive

Product Supplier
Security capabilities & Development Process

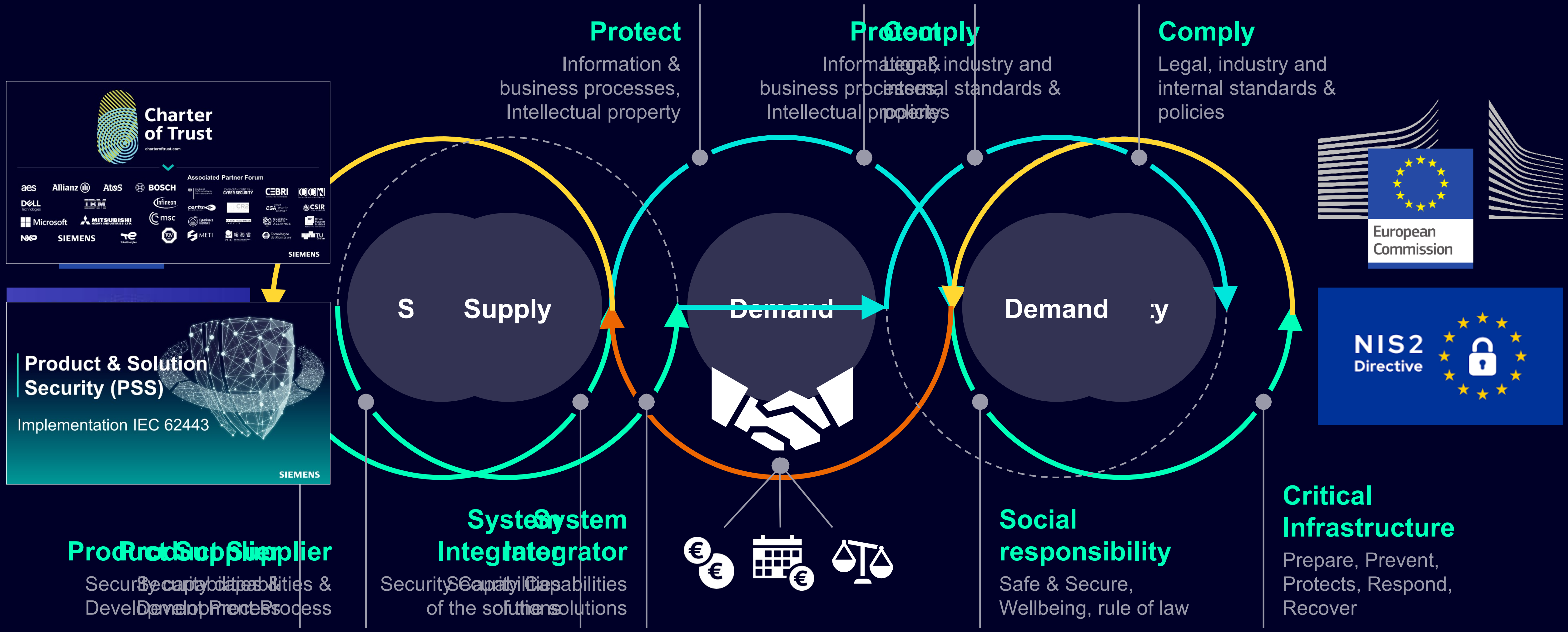
System Integrator
Security Capabilities of the solutions

Social responsibility
Safe & Secure, Wellbeing, rule of law

Critical Infrastructure
Prepare, Prevent, Protects, Respond, Recover

SIEMENS

Supply Demand Cooperation:

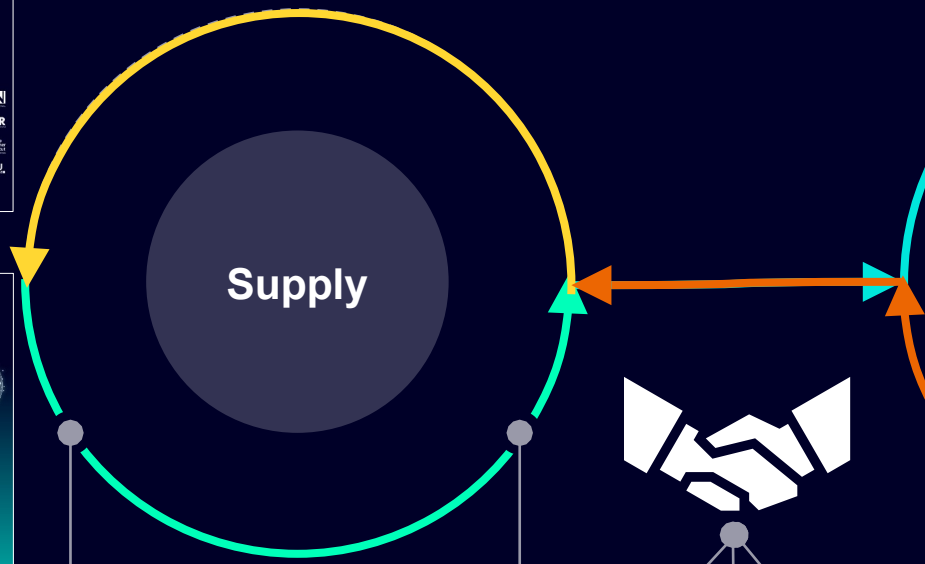


SIEMENS

Supply – Demand Cooperation:

Protect
Information & business processes, Intellectual property

Comply
Legal, industry and internal standards & policies



Product Supplier
Security capabilities & Development Process

System Integrator
Security Capabilities of the solutions

SIEMENS

CREATING AND SELLING SECURE SOLUTIONS

- OT AND IT ARE MOST OFTEN MANAGED BY DIFFERENT DEPARTMENTS
- IT DEPARTMENTS DO NOT ALWAYS UNDERSTAND THE DIFFERENCES
- OT DEPARTMENTS (OPERATIONS) ARE USUALLY LESS ‘CYBER SECURE AWARE’
- MINIMAL OT CYBERSECURITY DEMANDS IN TENDERS
- THEREFORE, THE SUPPLY SIDE (IN GENERAL) DOES NOT OFFER CYBERSECURITY
- NIS2 WILL LEVEL THE PLAYING FIELD
- CYBERSECURITY FOR OT IS NO LONGER OPTIONAL!

THE POTENTIAL EFFECT OF NIS2

- CREATE A LEGAL INCENTIVE TO IMPLEMENT CYBERSECURE SOLUTIONS
- CREATE MORE AWARENESS TO INCLUDE OT IN CYBERSECURITY POSTURE

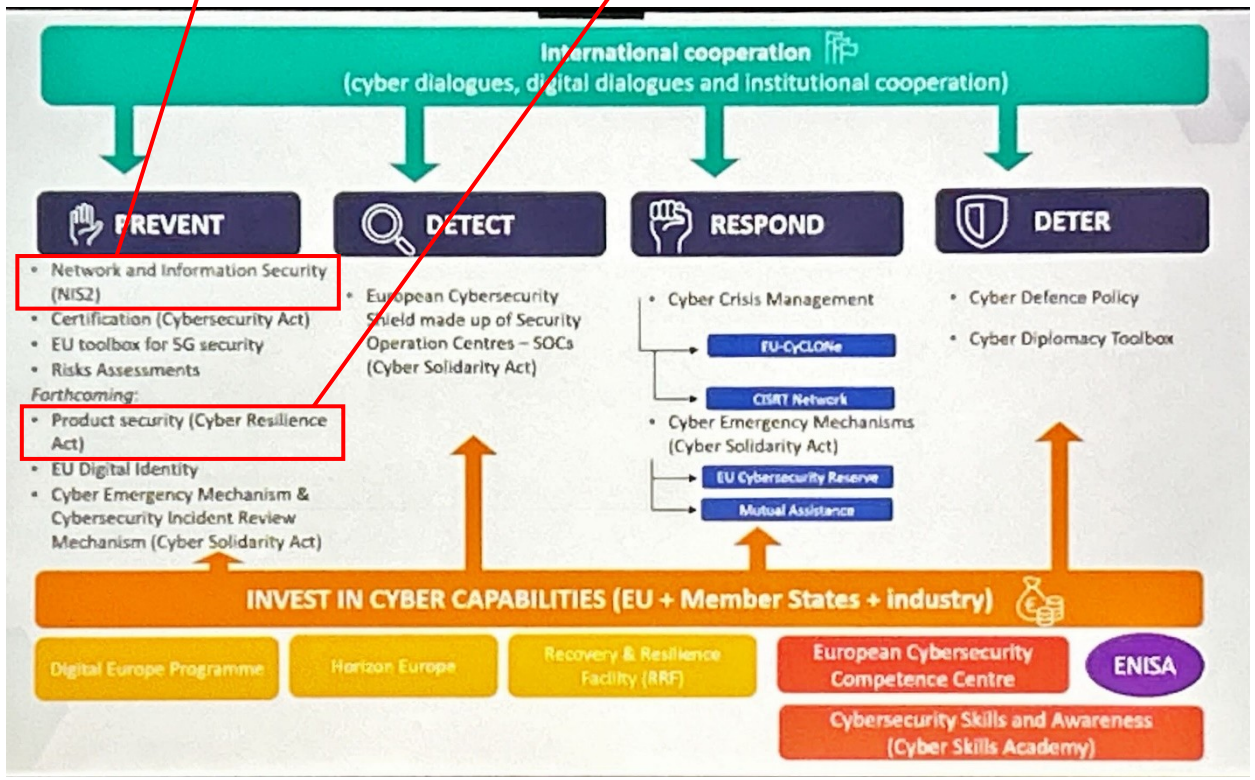
LOOK-AHEAD TO CYBER RESILIENCE ACT (CRA)

NIS2 (demand)

Deadline: October 2024

CRA (supply)

Deadline: early 2027



European Commission

CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity

#SOTEU

SEPTEMBER 2022 – UPDATED **DECEMBER 2023**

A first ever EU wide legislation of its kind: the **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle.

SIEMENS

Manufacturer's obligations

Cybersecurity is taken into account in **planning, design, development, production, delivery** and **maintenance** phase;

All **cybersecurity risks** are documented;

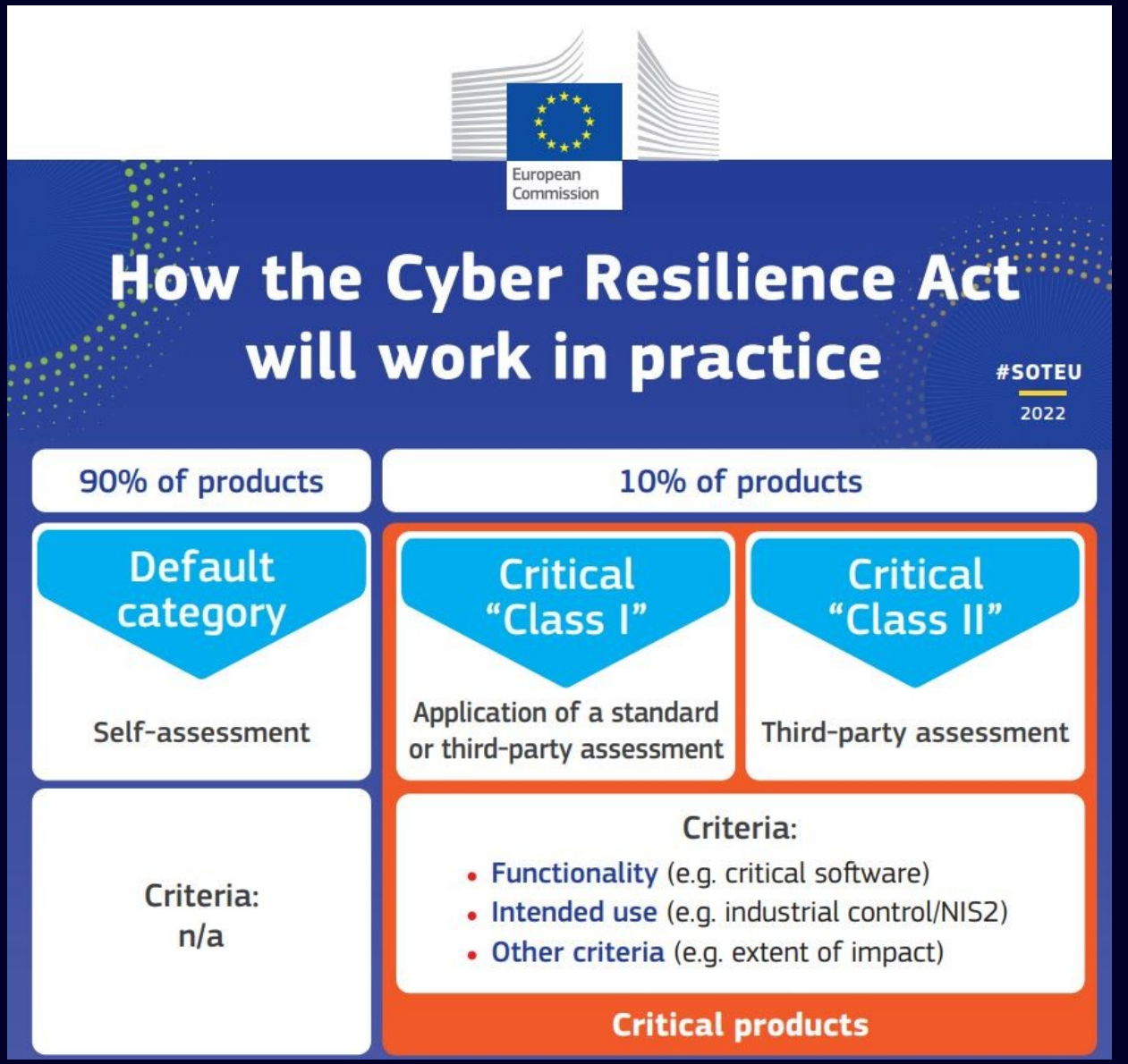
Manufacturers will have to **report actively exploited vulnerabilities and incidents**;

Once sold, manufacturers must ensure that for the **duration of the support period**, **vulnerabilities are handled effectively**;

Clear and understandable instructions for the use of products with digital elements;

Security updates to be made **available to users for the time the product is expected to be in use**.

SIEMENS


European Commission
How the Cyber Resilience Act will work in practice
#SOTEU 2022
90% of products
10% of products
Default category
Self-assessment
Critical "Class I"
Application of a standard or third-party assessment
Critical "Class II"
Third-party assessment
Criteria:
n/a
Criteria:
Functionality (e.g. critical software)
Intended use (e.g. industrial control/NIS2)
Other criteria (e.g. extent of impact)
Critical products

SIEMENS

THANK YOU

Contact info & QR to LinkedIn