

Cybersecurity in the Energy Industry

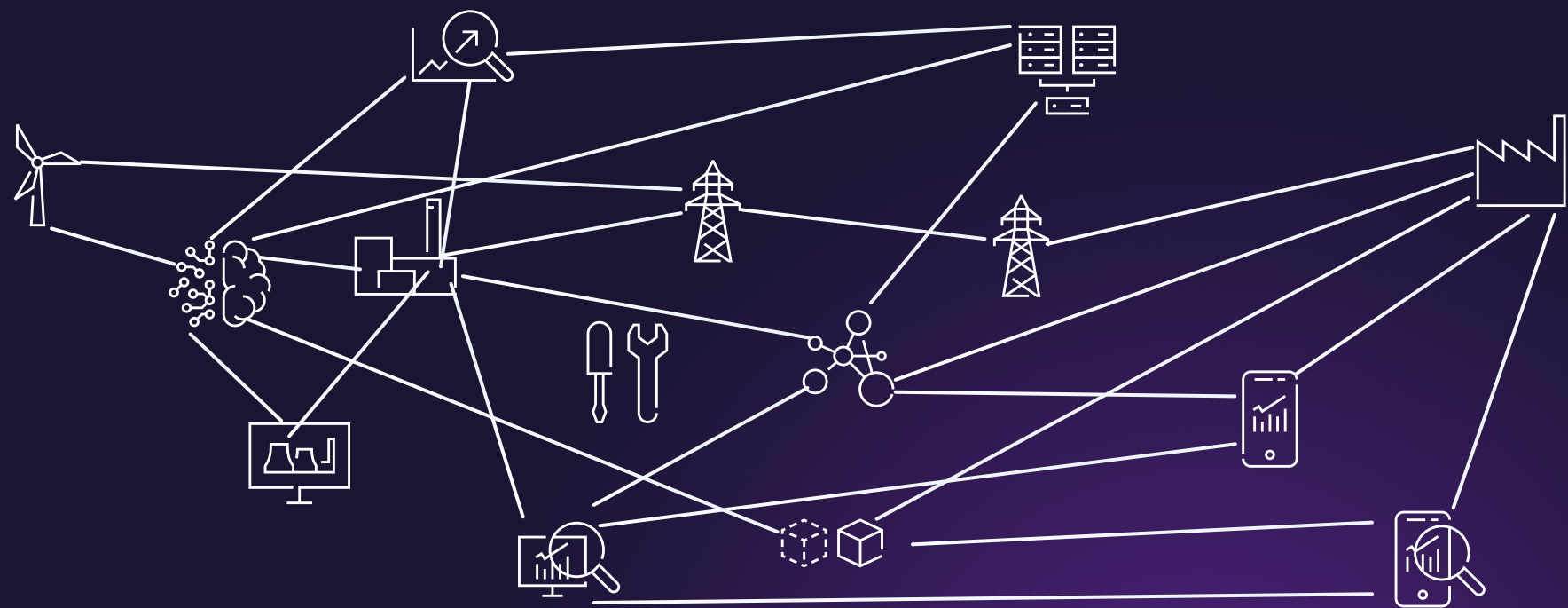
Defend. Together.

Cybersec*****



Everything is Connected with Everything

Defend. Together.
Cybersec*****



“The good old times”

“We should talk more”

The Present

“The Road ahead”



New Market Requirements From The Continental Neighbours

Defend. Together.
Cybersec*****

Cyber Resilience Act - Scope

- "Any **software or hardware** product and its **remote data processing solutions**, including software or hardware components to be placed on the market separately, whose **intended or reasonably foreseeable use** includes a **direct or indirect logical or physical data connection to a device or network**"

Highly Critical Sector

- NIS-2 Sector Energy means Class II

Non-Compliance Implication

- **No product placement on EU market**
- **Up to 15 Mio € or 2.5%**

**Effective
approximately
Summer/
Winter 2025**

New Market Requirements From The Continental Neighbours

Defend. Together.
Cybersec*****

Create and maintain a SBOM (Software Bill of Materials)

- Support the integrator
- Asset management
- Version management

Working vulnerability, patch management & incident handling process

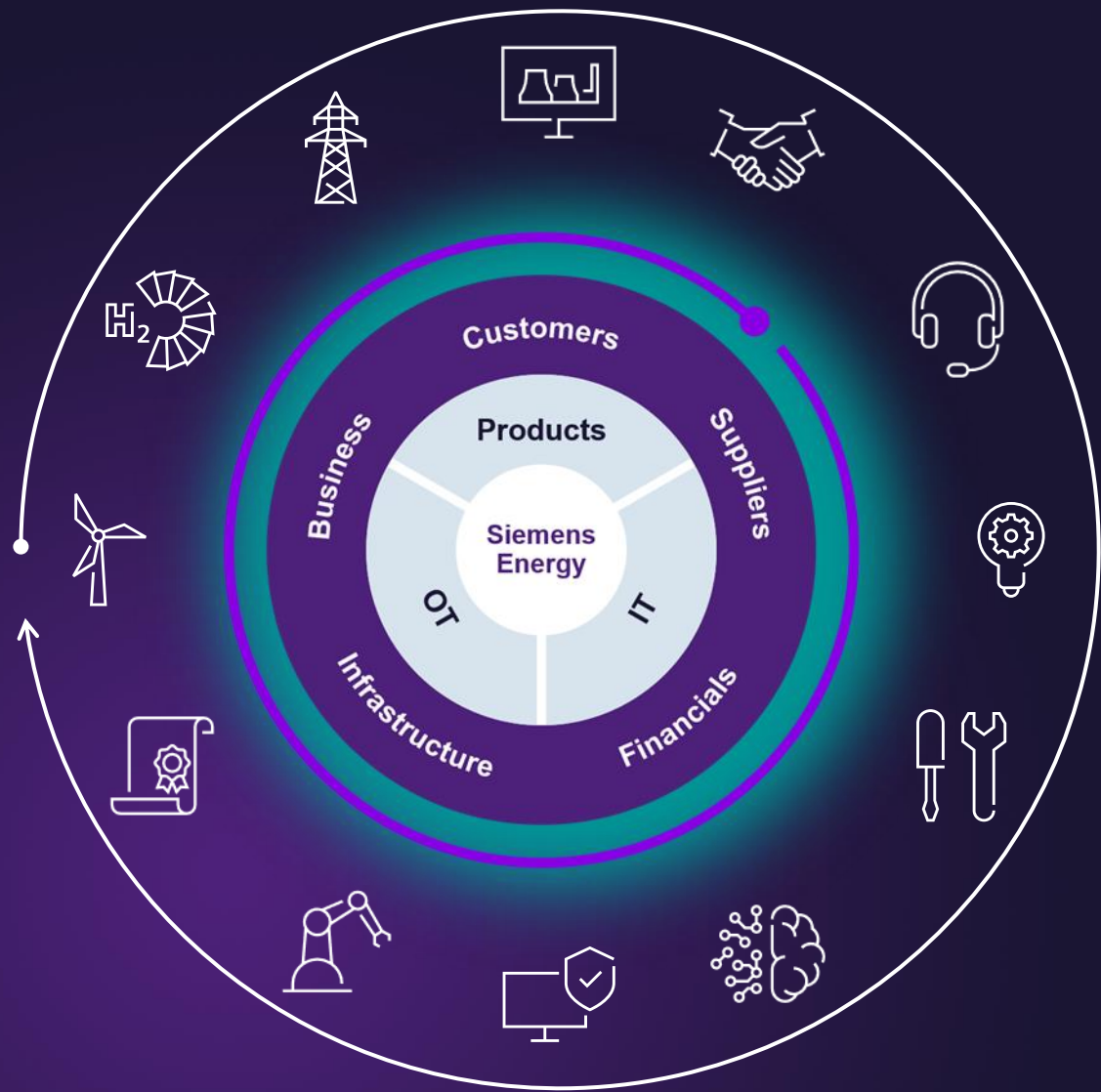
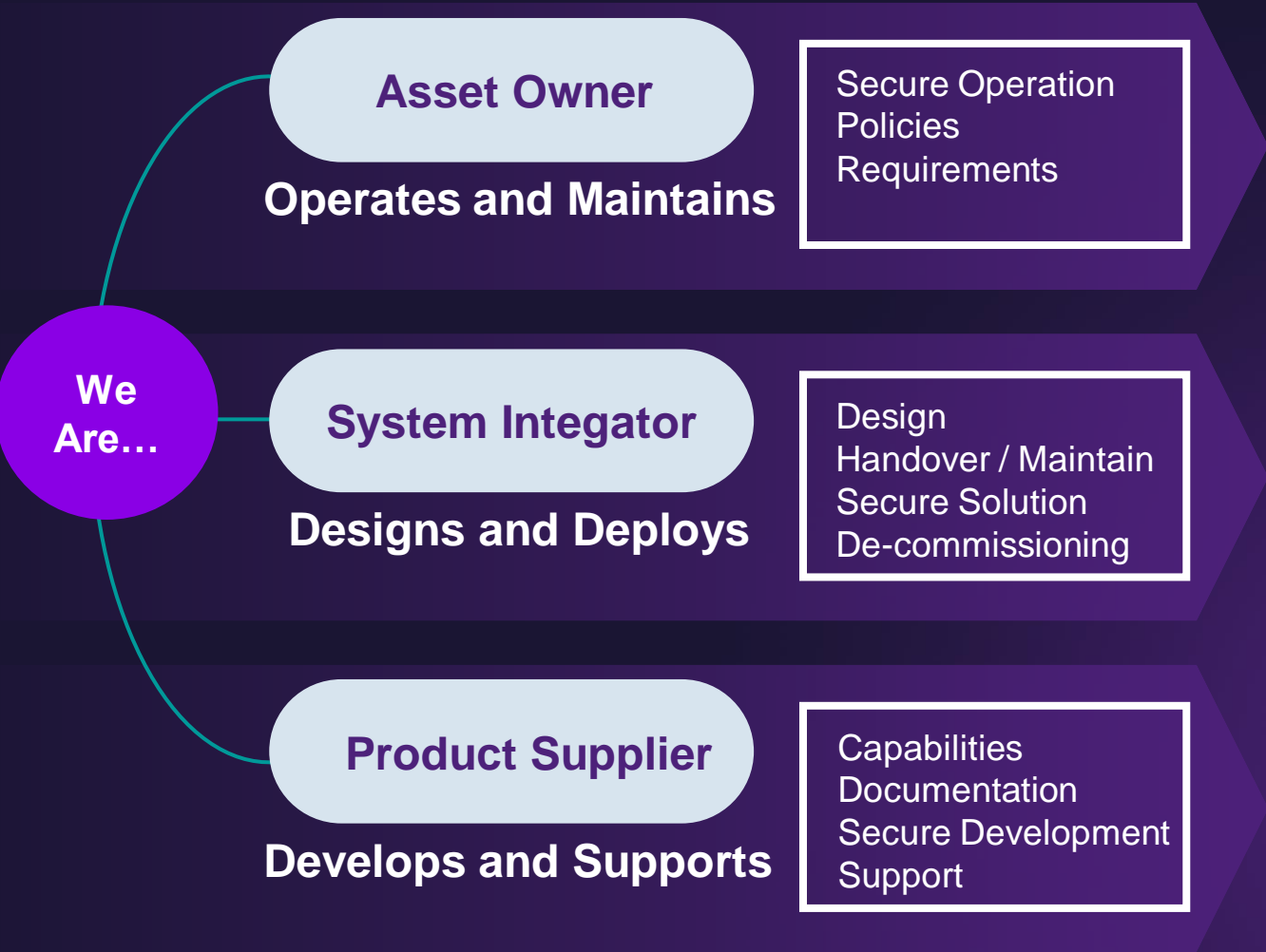
- Ensure vulnerabilities can be addressed
- Apply effective & regular tests
- Communicate to the supplier

IEC 62443

- Limit attack surfaces
- Minimize “own” negative impact
- Reduce impact of an incident
- Provide security related recording & monitoring

Siemens Energy | Thought Leader, Market Shaper & Key Enabler

Defend. Together.
Cybersec*****



Defend. Together.
Cybersec*****

SIEMENS
energy

“ Cybersecurity is everyone’s daily responsibility and a mandatory purpose for securing our economic and social stability. ”

