secunet

Cyber Regulation in Europe –

What are companies supposed to do now

Frank Sauber

October 2023

Your speaker today – Frank Sauber

Frank Sauber – Division Industry

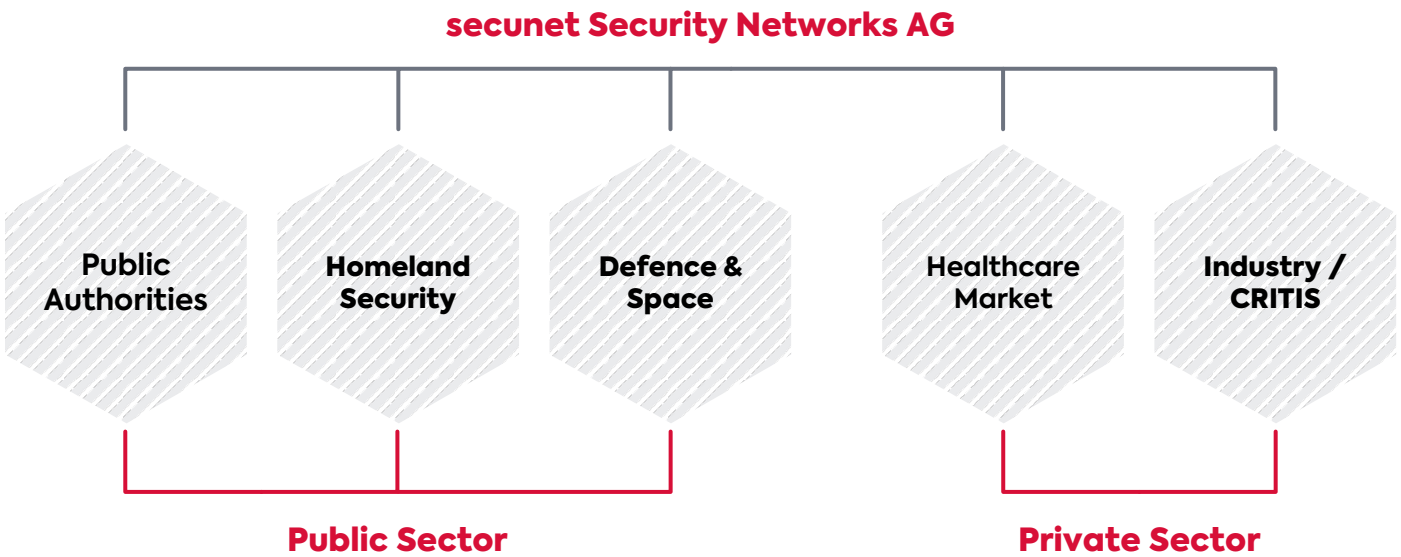
Global Head of Sales & Business Enablement

frank.sauber@secunet.com

secunet Security Networks AG

You’ ll find me and secunet in **hall 7A at 611**

secunet – 25 years of expertise in IT security



- More than 1,000 Employees
- 12 locations
- 347 million euros Revenue in 2022
- > 500 customers, including federal ministries, EU and > 20 DAX corporations
- Major shareholder: Giesecke + Devrient (75%)

Security partner of the Federal Republic of Germany

Joint venture

SecuStack
Cloud OS

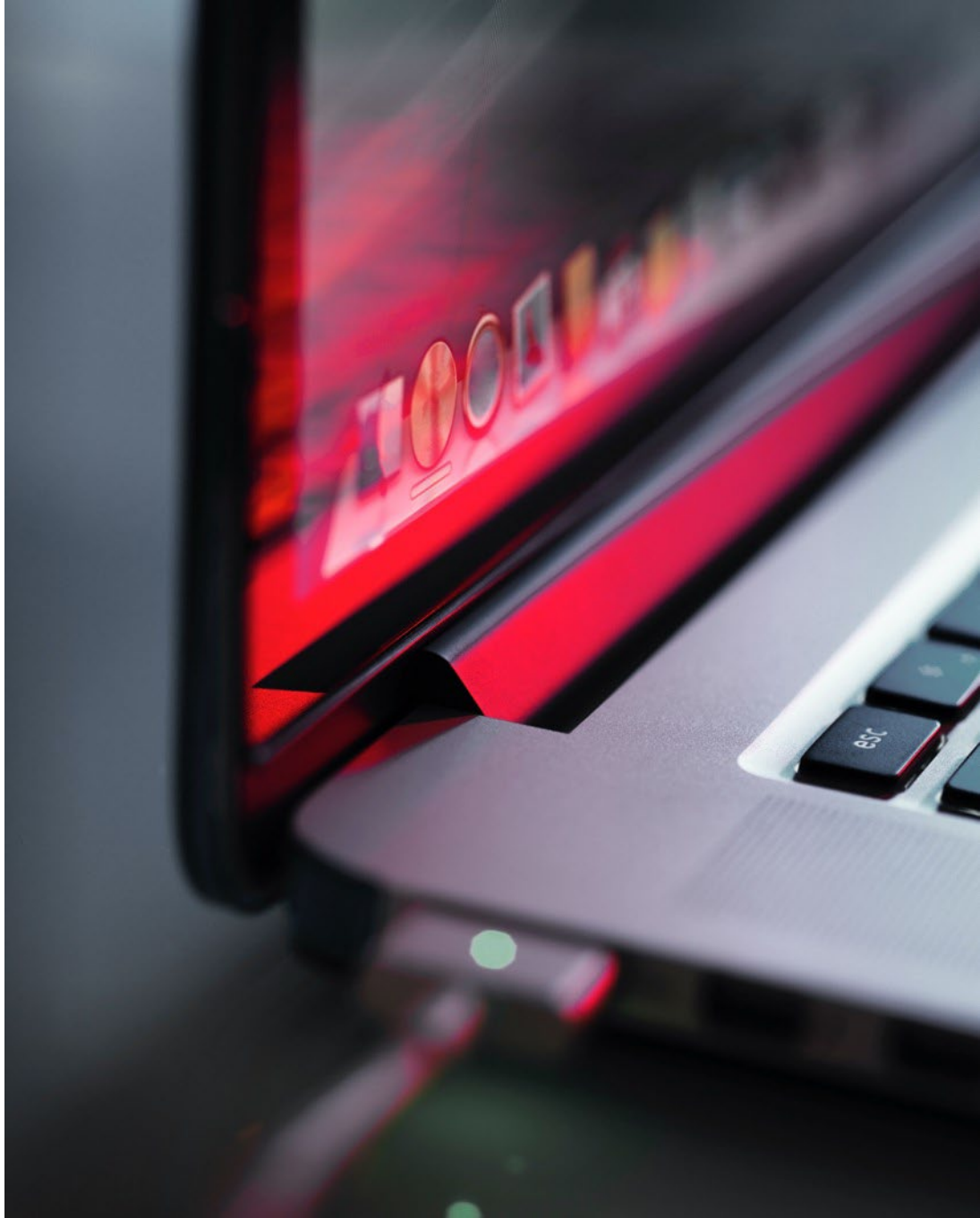
Subsidiaries

stashcat
Secure **Business** Messenger

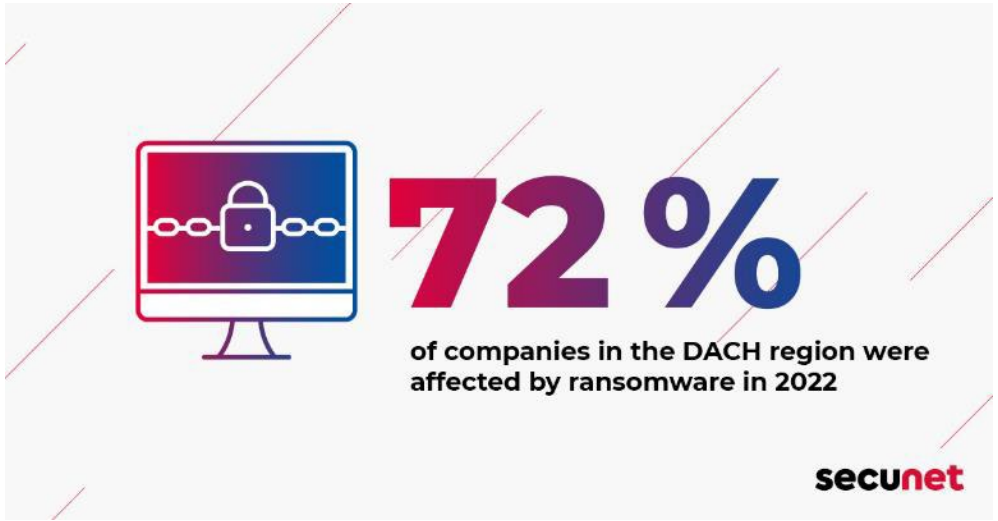
SysEleven
Cloud & Managed Kubernetes

Market Situation.

Current Threats development.



The Threats are increasing – for everyone

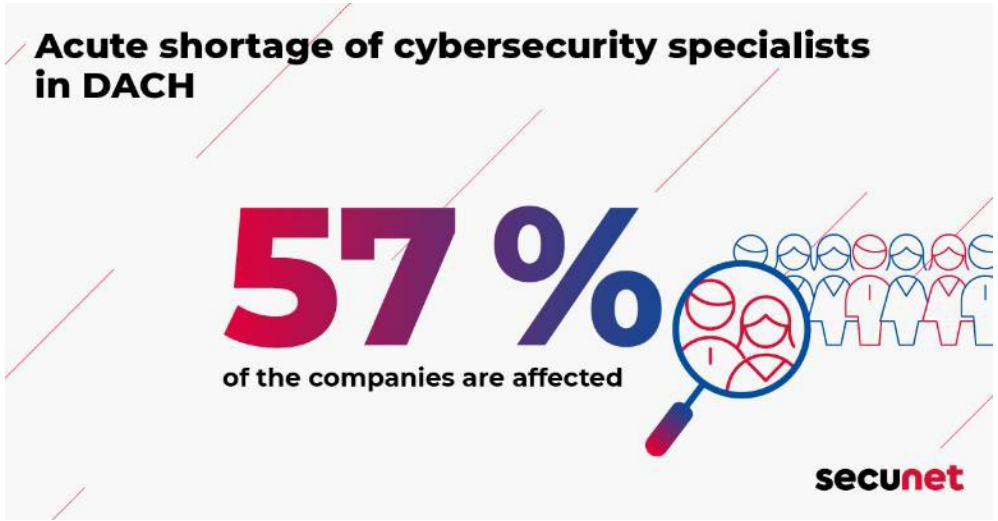


Source: IDC Study Cybersecurity in DACH 2022

Source: IDC Study Cybersecurity in DACH 2022

202 billion euros damage per year in Germany

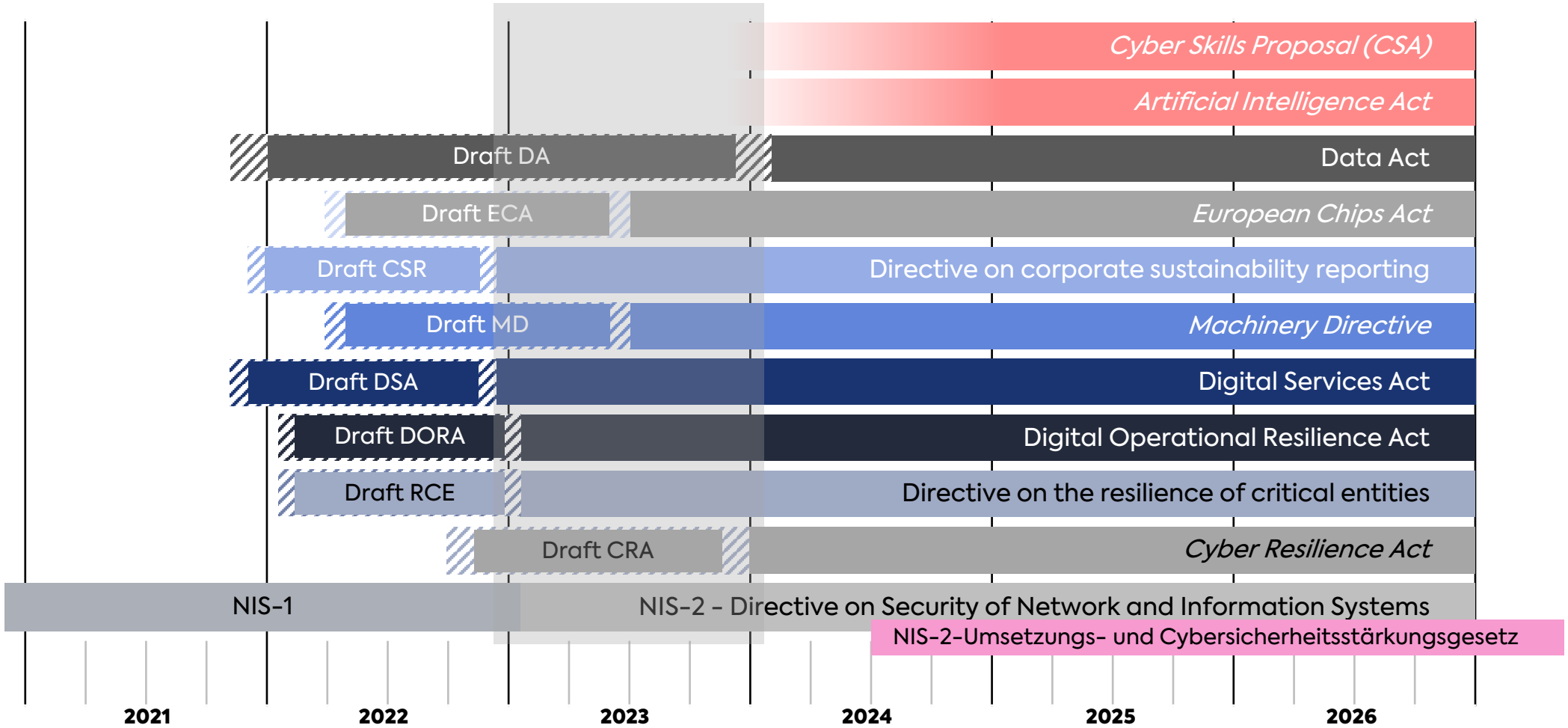
Source: Bitkom "Economic Protection 2022



European Security Legislation.

The track is getting paved.

The EU starts to react to increasing damage and threats



Zoom in – Security within European legislation

EU Directive on Security of Network and Information Systems (EU NIS-2 Directive)

- **Goal: Achieving a high common level of cybersecurity in the EU**
- Expansion of the affected sectors
- Security across supply chain

» In effect since 16.01.2023

EU Cyber Resilience Act (EU CRA)

- **Goal: Security for users and supply chain through security processes and elements.**
- Obligations for manufacturers, importers, and distributors of products with digital elements.

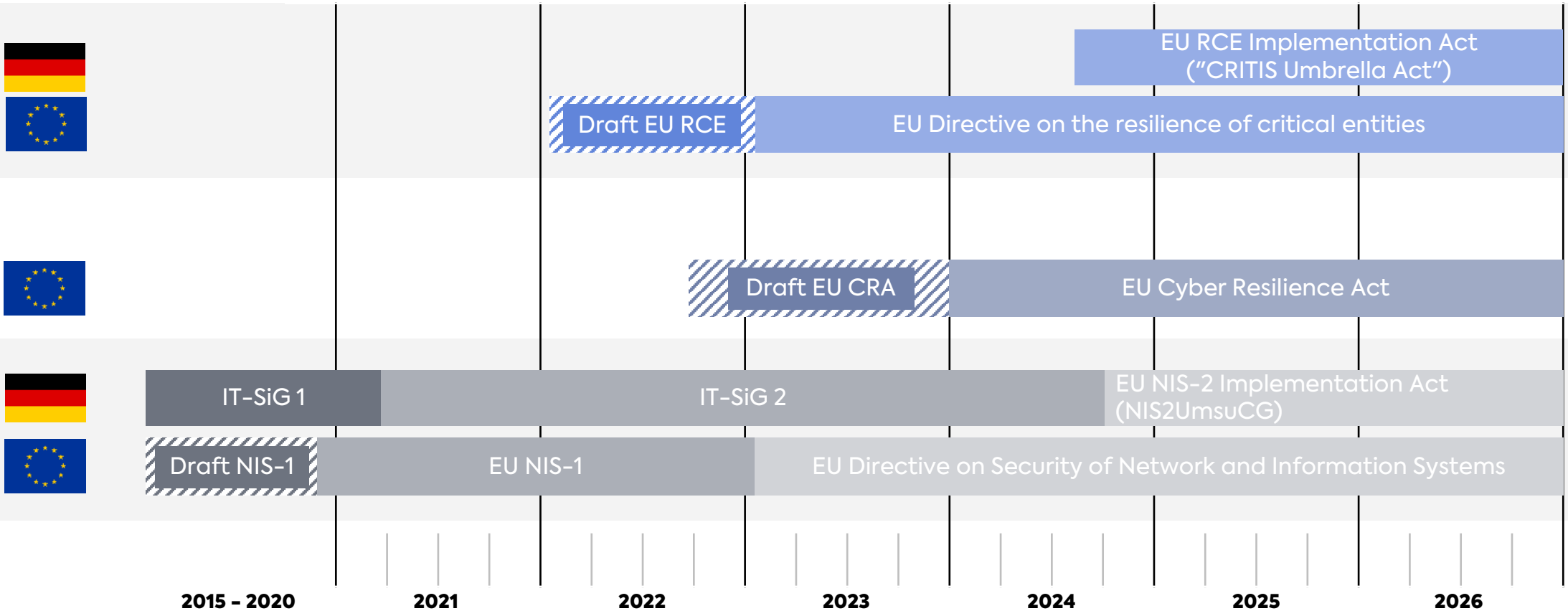
» The legislative process

EU Directive on the resilience of critical entities (EU RCE Directive)

- **Goal: Strengthening resilience (hybrid threats); alternative term definition; expansion of the sectors.**
- Obligations for operators of critical infrastructures.

» In effect since 16.01.2023

Roadmap for EU and national legislation



Wrap up of Status Quo.

Challenges.

Challenges

- **Increasing Threats** in Digital Transformation
- **Requirements by Regulation**
- **Skill and Resource shortage**
- Ensuring **business continuity**
- Preserving **digital sovereignty**

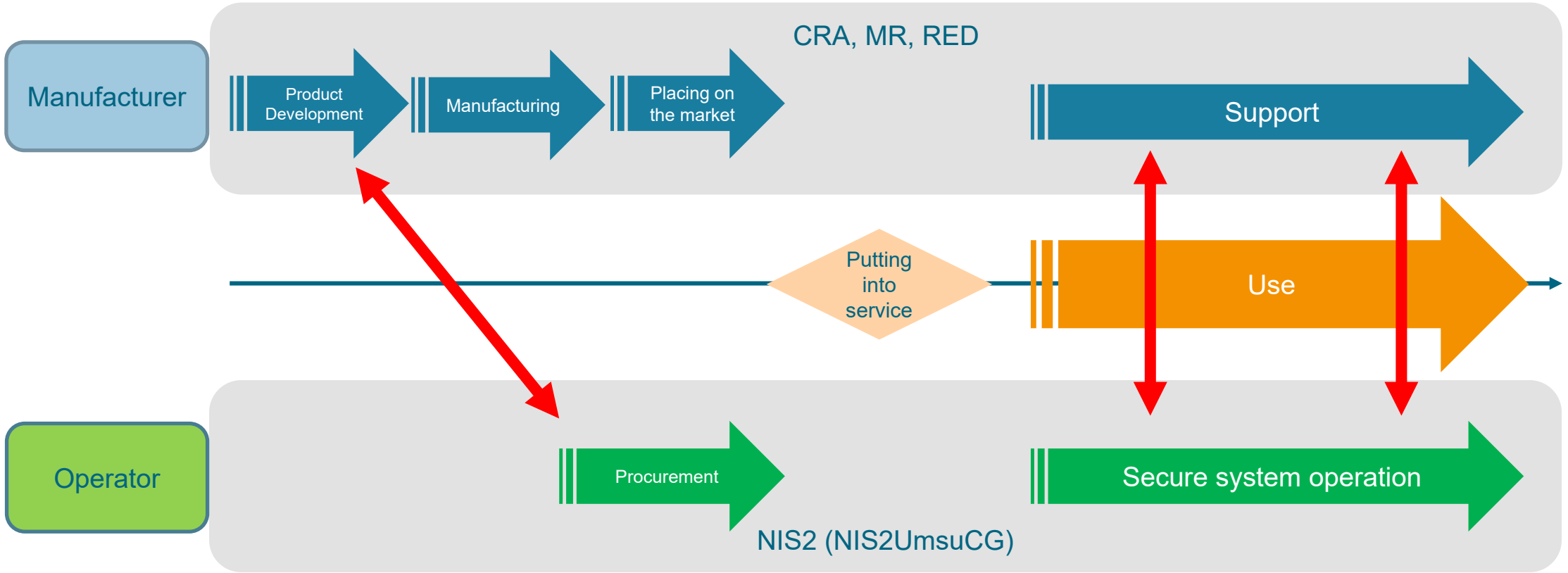
Do not wait.

Act now.

What should you do now?

- **Examination of** relevance
  (e.g. markets you **and** your customers sell to)
- **Review of** new **requirements**
  (e.g. supply chain, development)
- **Prepare reporting processes**
  (e.g. official bodies, customers, audits)
- **Set up risk management**
  (e.g. ISMS, BCM)

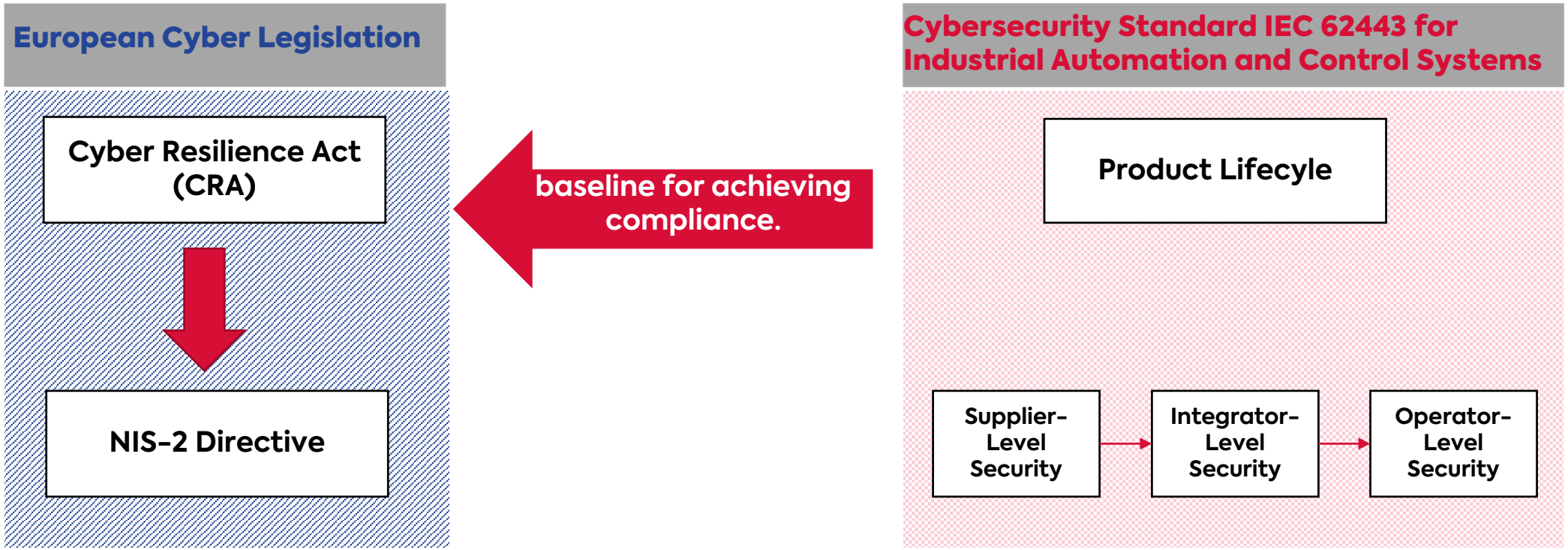
Cyber resilience in the product life cycle



CRA: Cyber Resilience Act
MR: Machinery Regulation (2023/1230)
RED: Radio Equipment Directive (Delegated Act 2022/30)
NIS2: Network and Information Security Directive 2 (2022/2555)
NIS2UmsuCG: NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Example: Production in Industry

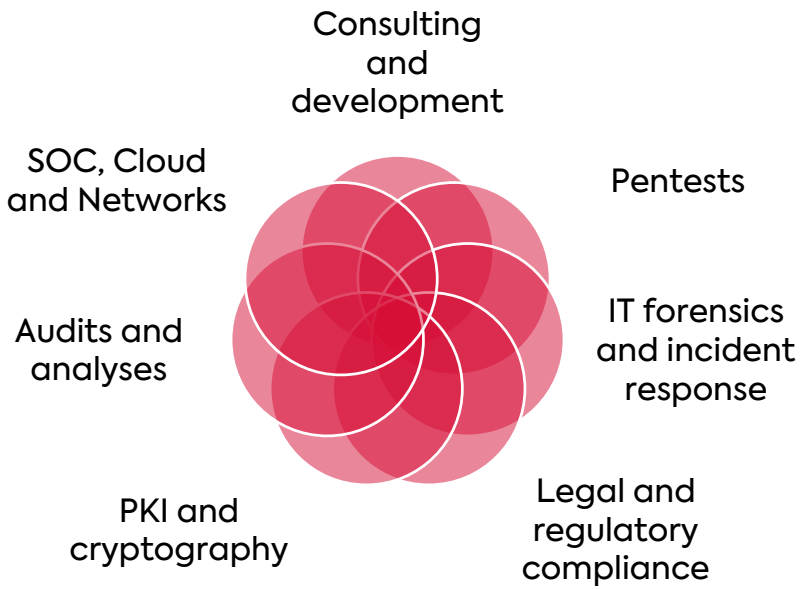
Achieving Cybersecurity Compliance with IEC 62443

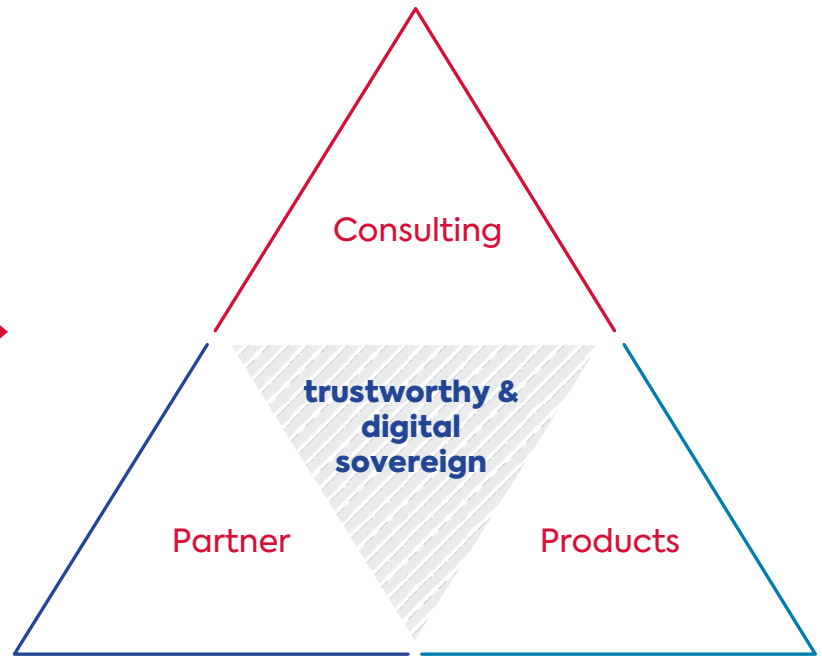


Mandatory for selling products and services in EU

secunet‘s approach – Integrated Value Chain

Comprehensive service from consulting, development and products





Take Aways – Cyber Security is of utmost importance

Security becomes a Governance Topic
=> it becomes Top Management Topic

For the bad guys it does not matter
They look for your weak points - they attack now

Follow us on
www.secunet.com/industrie

secunet

Frank Sauber

Global Head of Sales & Business Enablement

Industry Division

secunet Security Networks AG