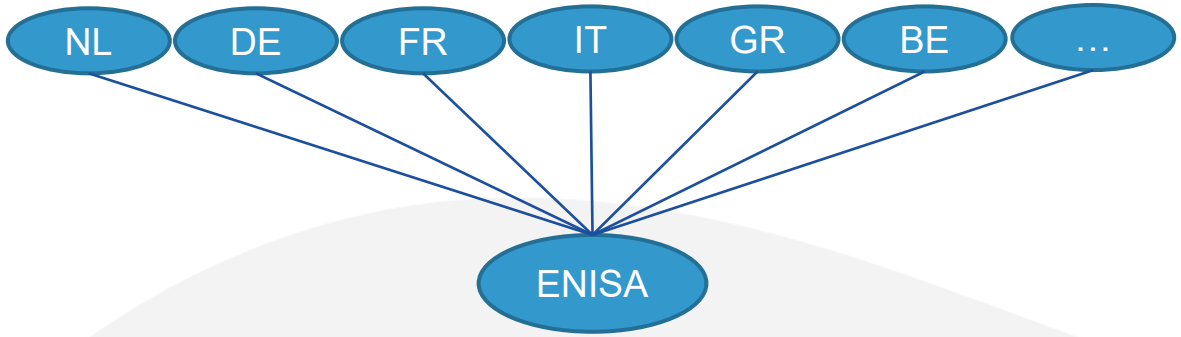
# Building up cyber resilience in the EU's critical sectors

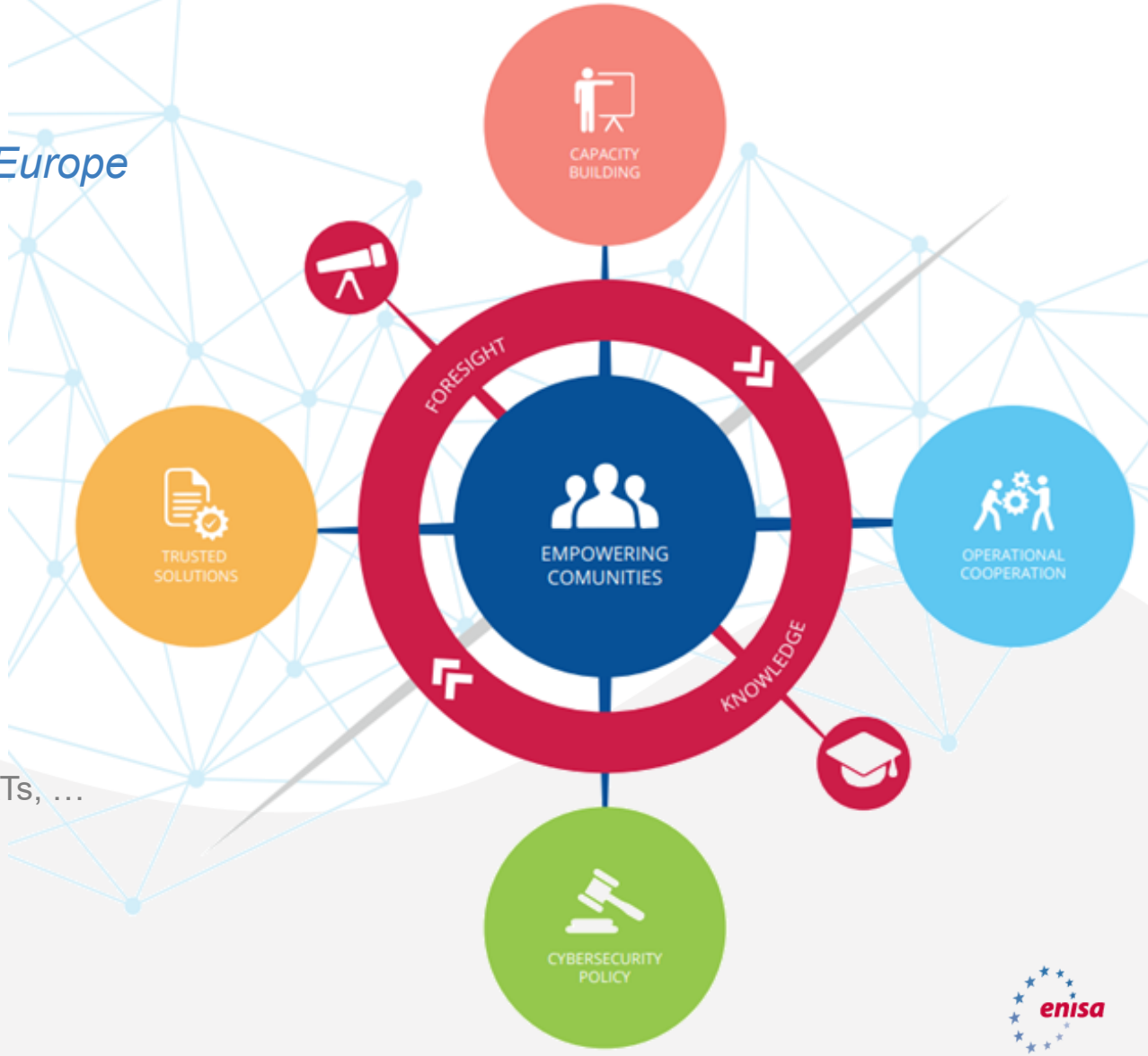
Marnix Dekker
Deputy Head of Unit Resilience of Critical Sectors
ENISA, the European Union Agency for Cybersecurity

19/05/2026

# ENISA’s mission

*Achieving a high common level of cybersecurity across Europe*




ENISA is supporting the national authorities, cybersecurity agencies, CSIRTs, …

# CYBER THREATS FOR THE EU

- DDoS attacks
- Ransomware
- Supply chain attacks
- Russia's war of aggression against Ukraine
- Industrial and state espionage
- Foreign interference
- Strategic ICT supply chain risks
- Emerging threats (IoT, AI), future issues (PQC)

Finland warns of hostile activities by Russia

Nordea has come under "unprecedented" denial-of-service attacks

NoName Cyberattacks Escalate, Targeting Diverse Sectors in Finland

Ireland's Health Services hit with $20 million ransomware demand

A Year After the SolarWinds Hack, Supply Chain Threats Still Loom

The Russia-led campaign was a wake-up call to the industry, but there's no one solution to the threat.

Exclusive: US sees increasing risk of Russian 'sabotage' of key undersea cables by secretive military unit

A year of wipers: How the Kremlin-backed Sandworm has attacked Ukraine during the war

China's Salt Typhoon hackers targeting Cisco devices used by telcos, universities

Chinese Hackers Suspected Of Airbus Cyberattacks—A350 Among Targets

Europe's election campaigns are under the constant threat of foreign interference

Eleven EU countries took 5G security measures to ban Huawei, ZTE

Mysterious Cyber Attack Took Down 600,000+ Routers in the U.S.

The threat posed by code-cracking quantum computers

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

# EU Policies for Cyber resilience

**ENISA in a leading role** - *driving the community*:

- NIS2 directive - Resilience of critical sectors — Our focus today
- EU Cyber certification (CSA) & EU Cyber label for digital products (CRA)
- Cyber solidarity act - Cyber reserve, national funding hubs
- Blueprint for EU-wide Operational cybersecurity collaboration
- EU Health action plan and EU support center
- Omnibus/Simplification initiative

**ENISA in a supporting and advisory role** - *pushing for NIS2 alignment:*

- Financial sector Resilience (DORA)
- Network Code Cross-border Electricity flows
- Critical Entities Resilience directive (CER)

# NIS2 in a nutshell – 3 pillars

Goal: To achieve a high common level of cybersecurity across the EU

## 1. National capabilities

- National authority
- National strategy
- National CSIRT
- National crisis management framework
- **National vulnerability disclosure framework**

## 2. EU collaboration

- NIS Cooperation group
- EU CSIRT network
- EU Cyclone

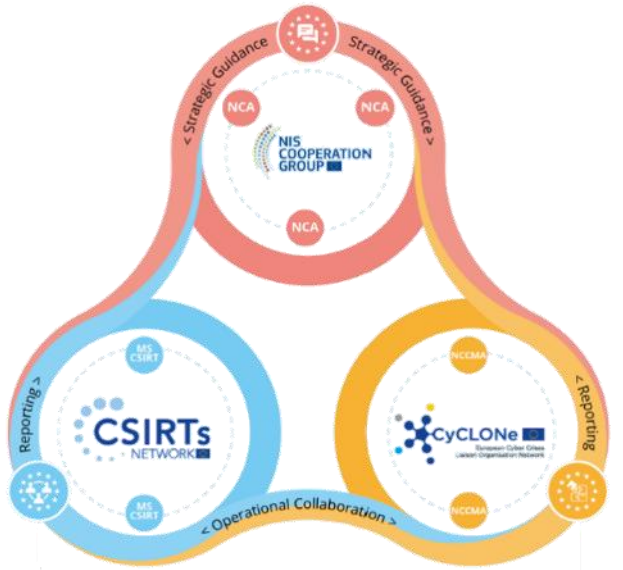
## 3. Supervision of critical sectors

- **Management responsibility**
- Security measures
- Incident reporting

**New mechanisms under the NIS2**

- Cybersecurity state of the union report
- **EU Vulnerability database (EUVD)**
- EU Digital infrastructure registry (EUDIR)
- WHOIS requirements
- Union evaluations of ICT supply chain risks

- Twice as many sectors
- More companies within a sector
- Management responsibility entities
- All hazard, including cyber-physical
- Supply chain security
- Cloud and datacenters essential under NIS2
- Managed service providers new under NIS2
- Telecoms and trust integrated into NIS2

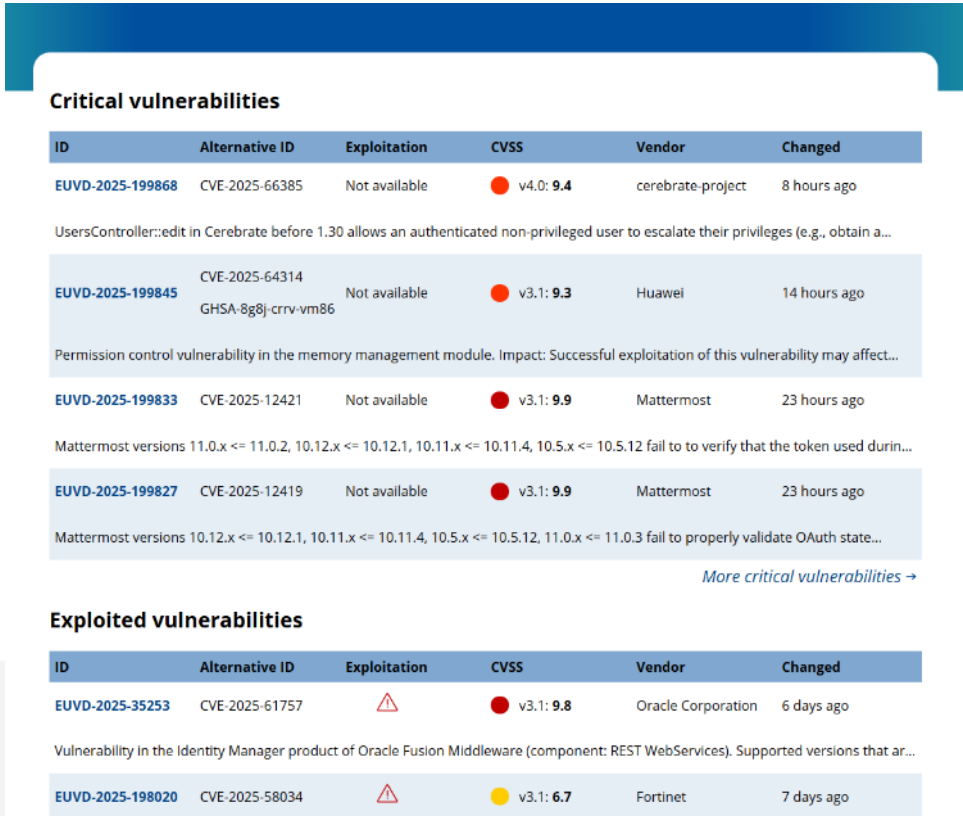


# Vulnerability management in the EU

*Building up European capabilities, to play our part in the global ecosystem*

EUROPEAN UNION VULNERABILITY DATABASE

- NIS2 asks EU MS to have Coordinated Vulnerability Policies
  - “Safe harbor” for security researchers (ethical hacking)
  - National CSIRTs act as coordinators between vendor and researcher
- NIS2 asks ENISA to develop and maintain EUVD
  - ENISA became a CVE Number Authority in June 2024
  - EUVD live since early 2025 (live)
  - ENISA became Root CVE Numbering Authority in November 2025
- European added value
  - Easier for EU vendors/suppliers to report/publish
  - More trust in EU digital products (link with CRA SRP)



**Critical vulnerabilities**

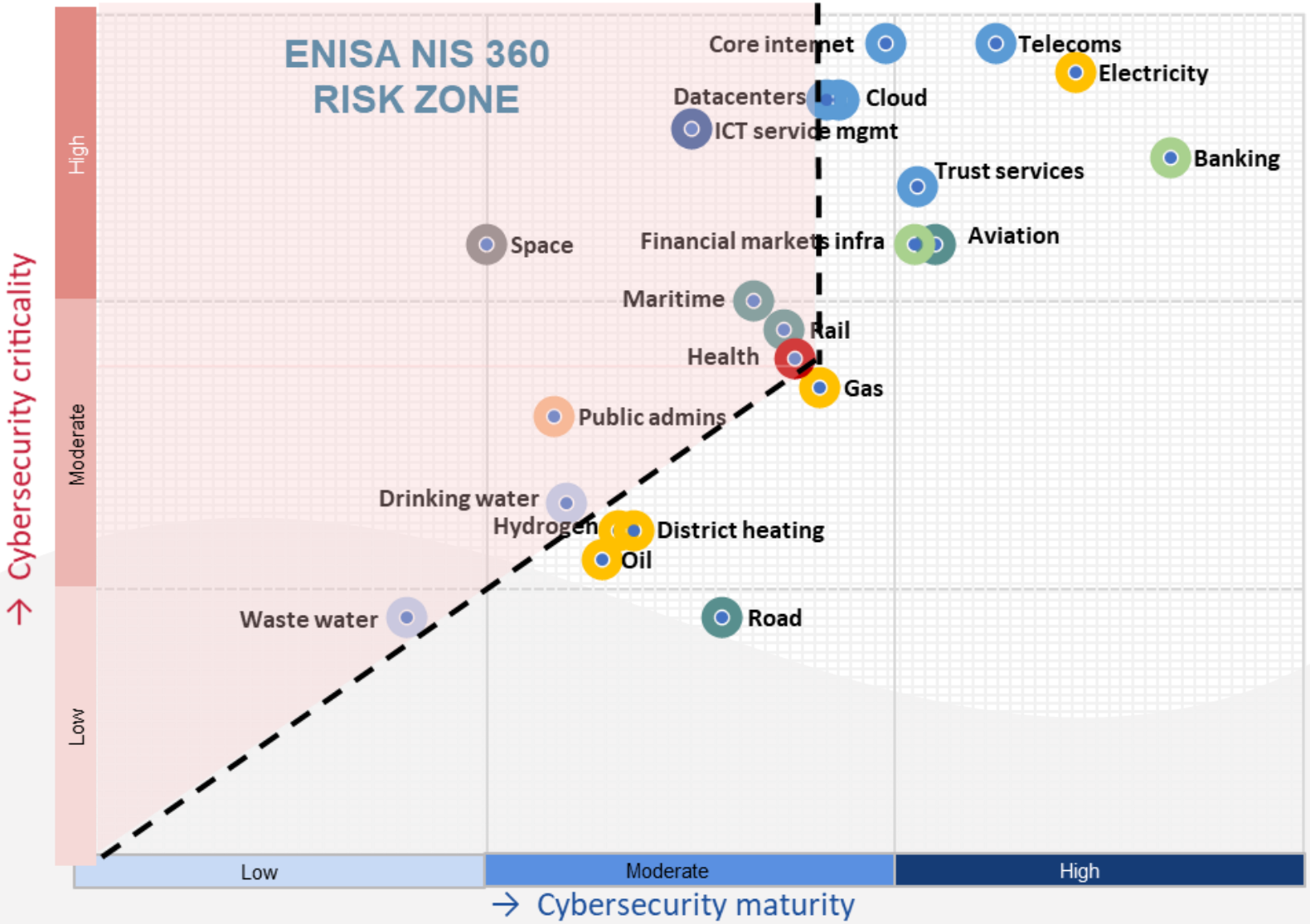
| ID | Alternative ID | Exploitation | CVSS | Vendor | Changed |
|---|---|---|---|---|---|
| EUVD-2025-199868 | CVE-2025-66385 | Not available | v4.0: **9.4** | cerebrate-project | 8 hours ago |
| UsersController::edit in Cerebrate before 1.30 allows an authenticated non-privileged user to escalate their privileges (e.g., obtain a... | | | | | |
| EUVD-2025-199845 | CVE-2025-64314 GHSA-8g8j-crrv-vm86 | Not available | v3.1: **9.3** | Huawei | 14 hours ago |
| Permission control vulnerability in the memory management module. Impact: Successful exploitation of this vulnerability may affect... | | | | | |
| EUVD-2025-199833 | CVE-2025-12421 | Not available | v3.1: **9.9** | Mattermost | 23 hours ago |
| Mattermost versions 11.0.x <= 11.0.2, 10.12.x <= 10.12.1, 10.11.x <= 10.11.4, 10.5.x <= 10.5.12 fail to to verify that the token used durin... | | | | | |
| EUVD-2025-199827 | CVE-2025-12419 | Not available | v3.1: **9.9** | Mattermost | 23 hours ago |
| Mattermost versions 10.12.x <= 10.12.1, 10.11.x <= 10.11.4, 10.5.x <= 10.5.12, 11.0.x <= 11.0.3 fail to properly validate OAuth state... | | | | | |

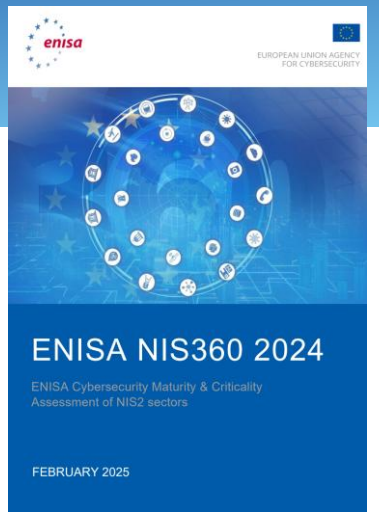
*More critical vulnerabilities →*

**Exploited vulnerabilities**

| ID | Alternative ID | Exploitation | CVSS | Vendor | Changed |
|---|---|---|---|---|---|
| EUVD-2025-35253 | CVE-2025-61757 | ⚠ | v3.1: **9.8** | Oracle Corporation | 6 days ago |
| Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: REST WebServices). Supported versions that ar... | | | | | |
| EUVD-2025-198020 | CVE-2025-58034 | ⚠ | v3.1: **6.7** | Fortinet | 7 days ago |

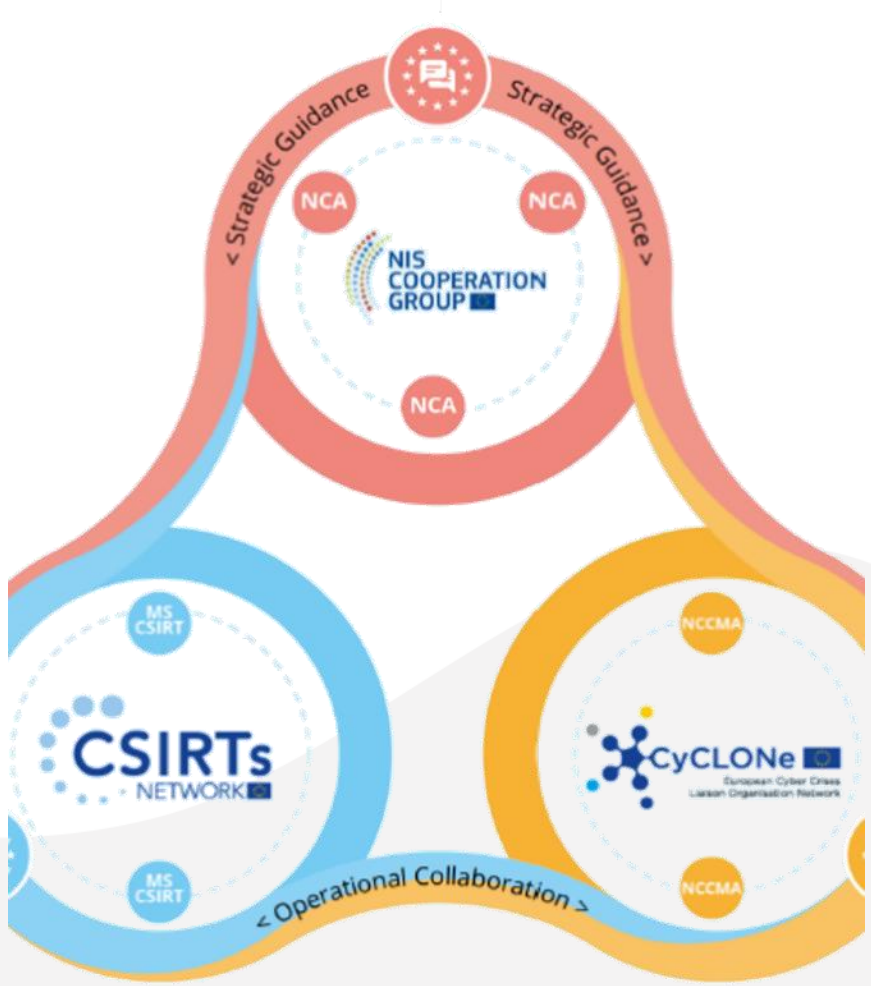
# ENISA NIS360



# ENISA working to implement the NIS2

- **Supporting EU collaboration**
  - NIS Cooperation group, CSIRTs Network, Cyclone
- **Annual MS Dialogues on NIS2 implementation**
  - And a NIS2 peer review process
- **EU Cybersecurity State of the Union**
  - Based on EU cyber index and ENISA NIS360
- **Horizontal NIS2 frameworks**
  - NIS2 Security measures, Incident reporting, and Supervision
- **Sectorial implementation of NIS2**
  - Working groups of sectorial national authorities
- **Incident and vulnerability tools**
  - EUVD and CIRAS (and SEP)
- **Union risk assessments (URAs)**
  - EU 5G toolbox, Nevers, ICT Supply chain toolbox



# Reflecting on 2 years of NIS2 transposition

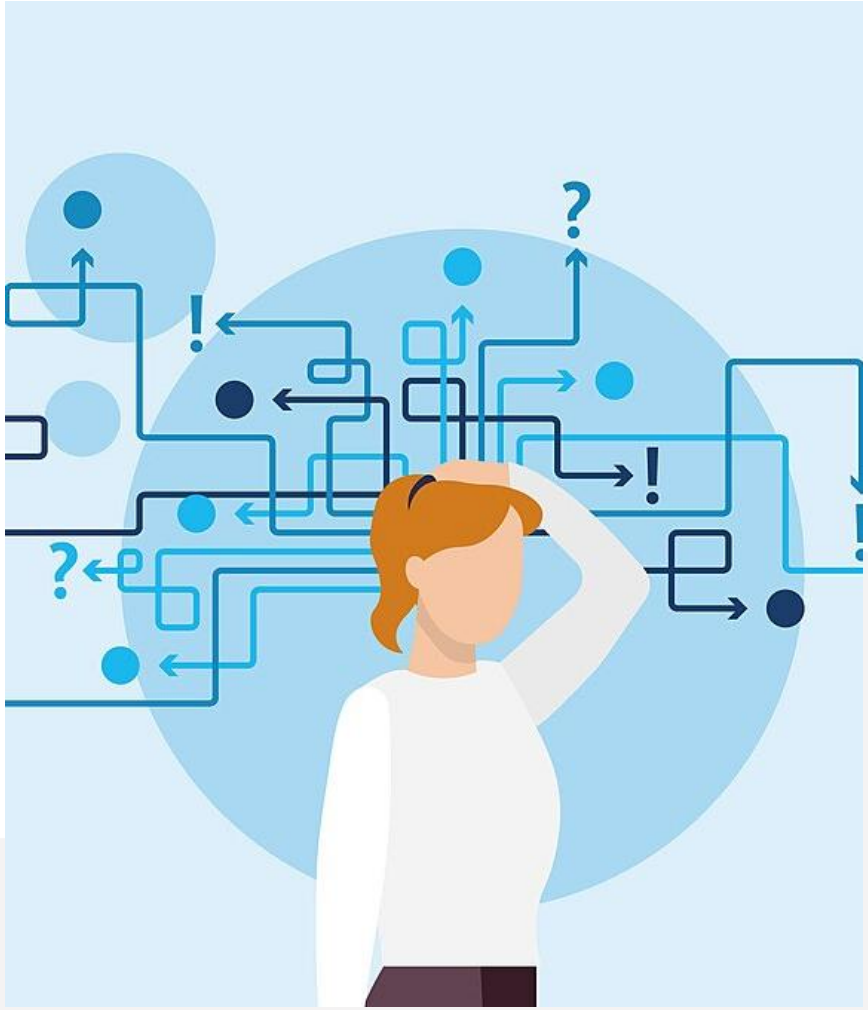
**All the good things!**

- Quick agreement about NIS2!
  - Continues and reinforces the NIS1 approach
- Some cool extras, closing some technical gaps
  - EUVD, Ethical hacking, mgmt. responsibility, …
- Big improvement in harmonization
  - Scope, security measures, incident reporting flow
- Integrates cyber crisis management
- Addresses also strategic matters (URAs)
- **NIS2 became the cybersecurity framework for the EU!**

# Reflecting on 2 years of NIS2 transposition

**Some issues to solve:**

- Broad scope within each sector
  - Basic cyber hygiene is taking all the attention now
    >> Second track needed for critical operators
- Main establishment principle
  - Most complex supervision for critical ICT suppliers serving multiple operators across sectors and EUMS
    >> Network of SPOCs connecting with sectorial authorities
- Many sectors, many authorities
  - Many NIS authorities need to learn a difficult skill
    >> Need to share supervision tricks and practices



# Observations

- **About cloud, ICT outsourcing and managed services**
  - Good cybersecurity reasons for this ICT trend!
    - Not only a risk!
      - But don’t make a spaghetti of dependencies
- **High risk vendors**
  - It is a real issue! ICT is no longer stand-alone (5G)
    - Very large cyber espionage campaigns (Salt Typhoon)
    - Do *not* confuse it with the digital sovereignty debate
      - Niinisto (short/mid term), Draghi (mid/long term)
- **Many rules and requirements**
  - ICT should be easy! Where is the (ICT) solution?
    - Especially in “OT” sectors like health care
  - We need to partner more with ICT suppliers

# Outlook – what is next?

## *Not only rules! Everything is easy on paper*

- **Funding and public-private partnerships**
  - EU Cyber reserve is maturing, Health Action Plan, Western Balkans agreement
- **Collaboration and sharing between companies**
  - ISACs! Sharing hubs and SOCs! Conferences! Sectorial workshops
- **Give solutions, not only more requirements!**
  - Help companies towards better ICT (stop scaremongering about cloud or outsourcing)
  - Trusted ICT suppliers: Make Europe an good/easy/secure place for ICT suppliers and companies

## *Time to put NIS2 in practice*

- MS transposition is ending this year. This was the easy part.
  - One cybersecurity framework for Europe
  - Less paper, more action – Omnibus simplification is important!
  - Steer away from legal discussions - Attackers don’t care about commas!

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

# Thank you for your attention


 +30 2814 409 711

 info@enisa.europa.eu

 https://enisa.europa.eu


**Connect on Linkedin! Send us your ideas, questions, follow our work!**


**ENISA**
European Union Agency
for Cybersecurity

**Athens Office**
Agamemnonos 14
Chalandri 15231, Attiki, Greece

**Brussels Office**
Rue de la Loi 107
1049 Brussels, Belgium