



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

INFORMATION SHARING AND INCIDENT REPORTING IN THE EU CYBERSECURITY REGULATORY FRAMEWORK

Dr. Athanasios Drougkas
Cybersecurity Expert
ENISA – The EU Agency for Cybersecurity

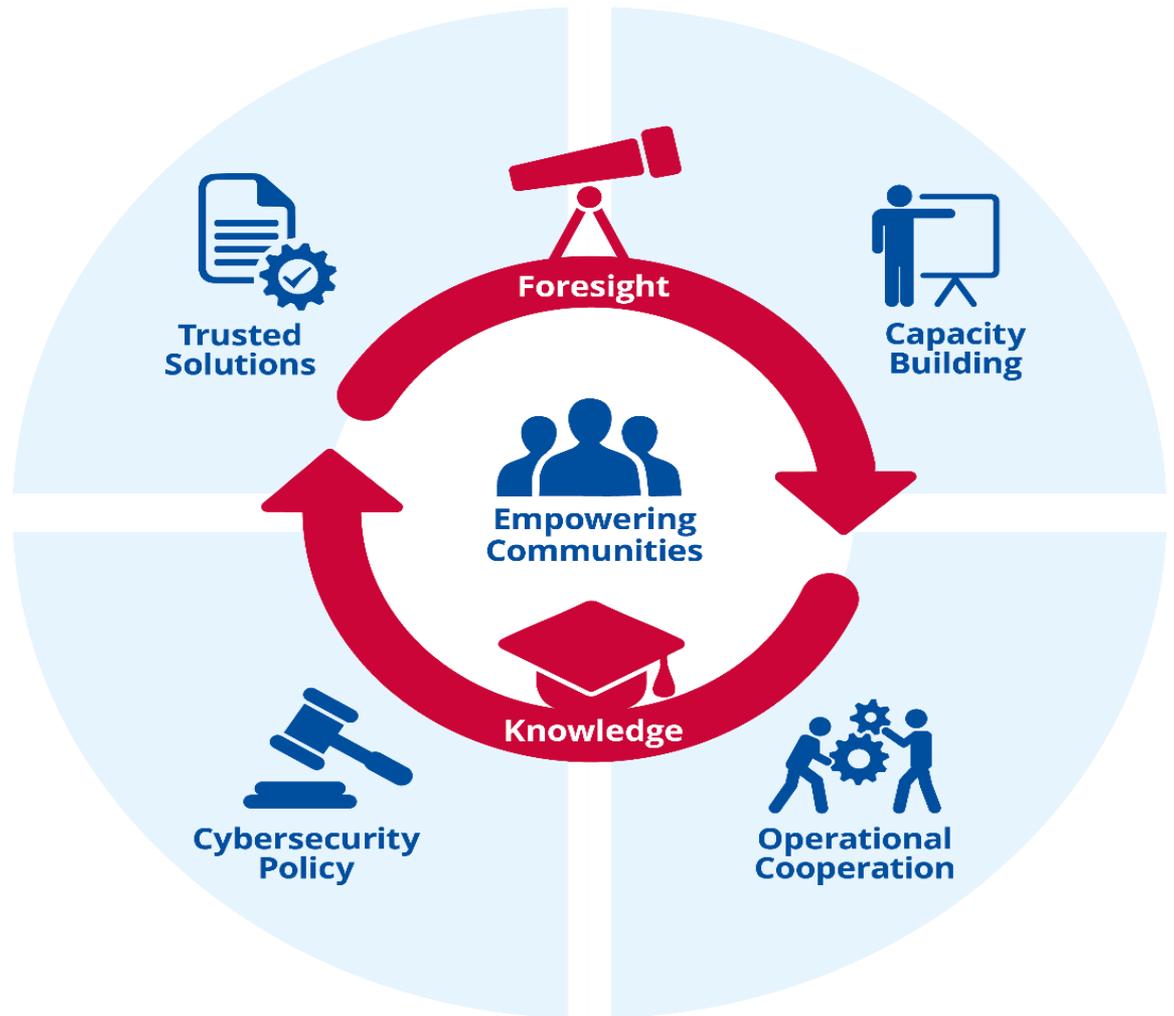
3rd EMSA Maritime Cybersecurity Conference
03 | 10 | 2024



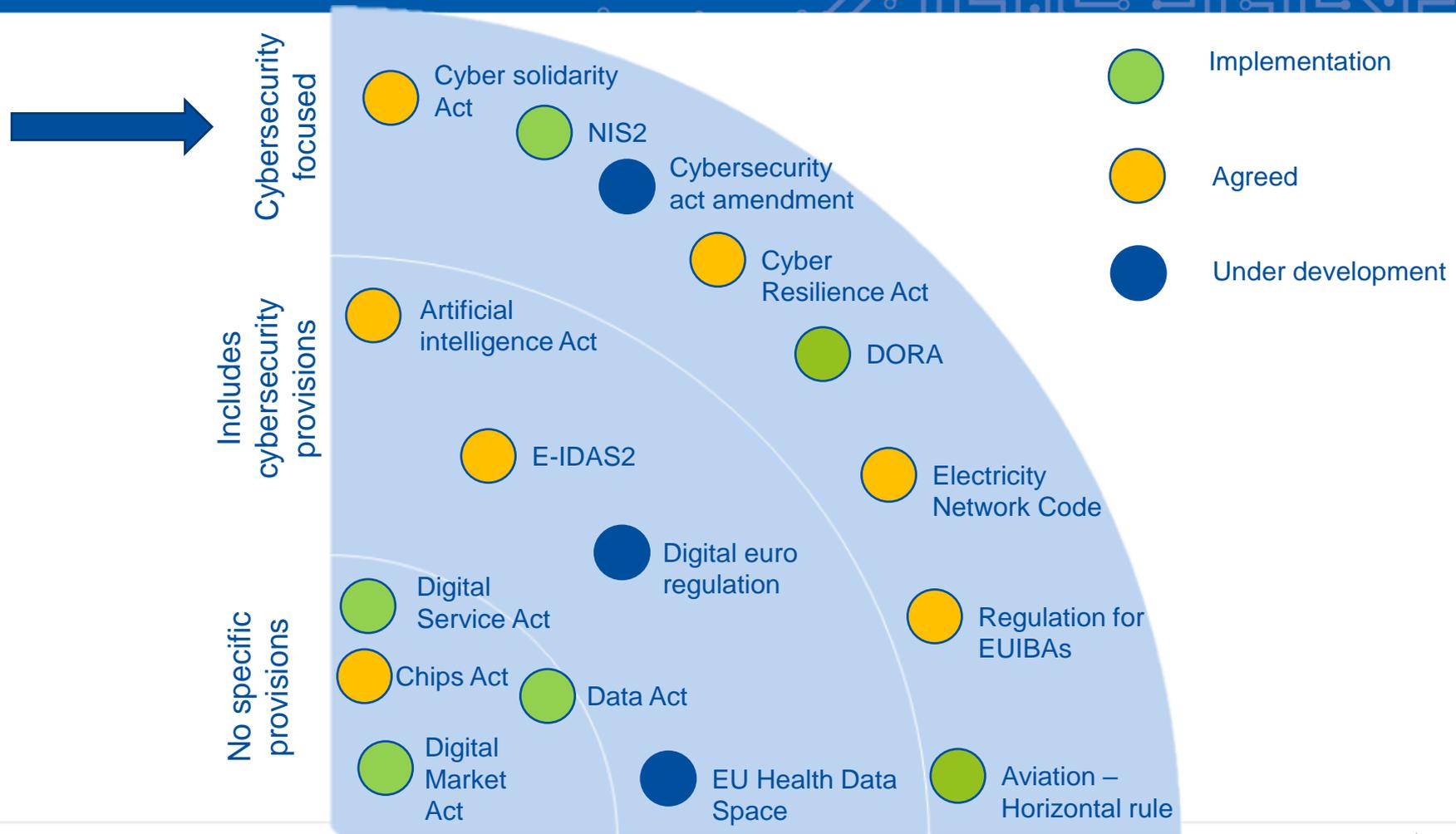
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve a **high common level of cybersecurity** across the Union in cooperation with the wider community



CYBERSECURITY POLICY LANDSCAPE

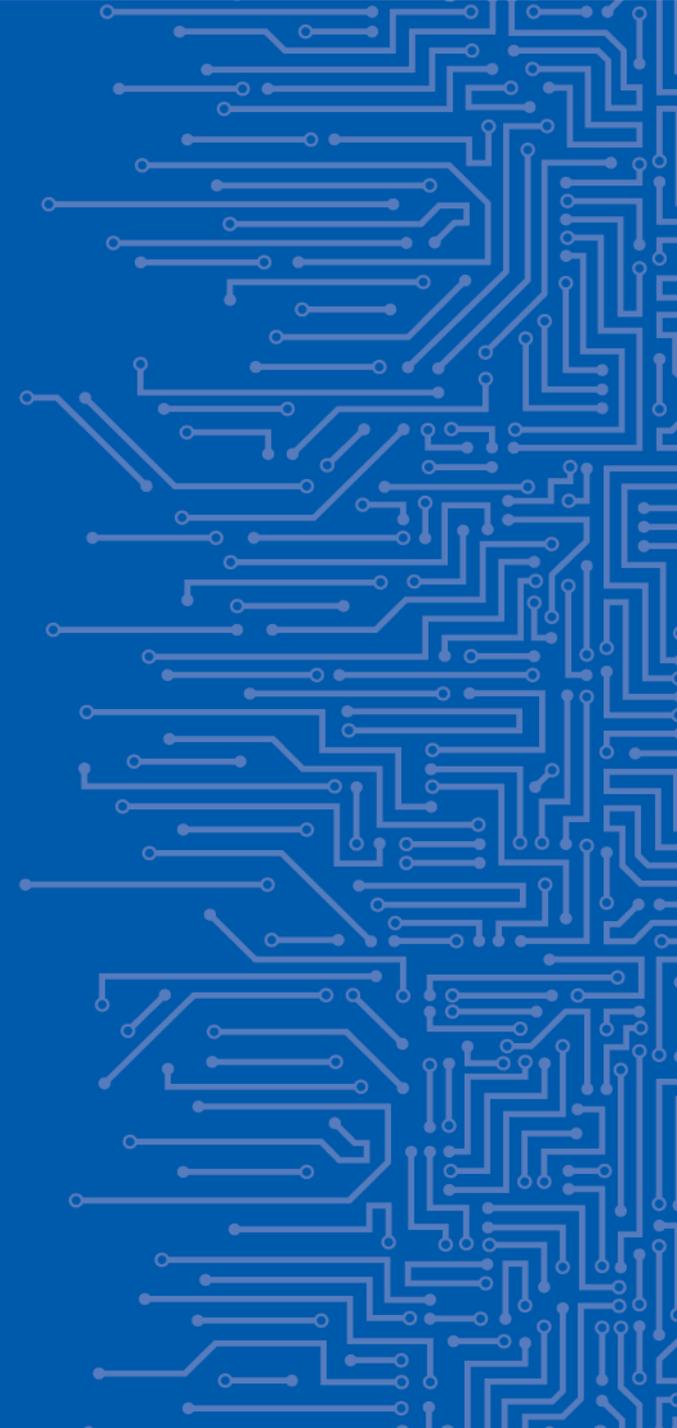


POLICY AREAS WITH CYBERSECURITY FOCUS

Common requirements

	Security Measures	Incident Reporting	Incident Response	Crisis Management	Information Sharing	Operational Cooperation	Certification / Standardisation	Vulnerability Disclosure	Trainings / Exercises
NIS2	✓	✓	✓	✓	✓	✓	✓	✓	✓
CRA	✓	✓			✓		✓	✓	
DORA		✓		✓	✓			✓	
NCCS	✓	✓	✓	✓	✓	✓	✓	✓	✓
Aviation – Horizontal Rule	✓	✓			✓		✓	✓	
Regulation for EUIBAs	✓	✓	✓	✓	✓	✓		✓	✓

NIS2



MAIN PILLARS FOR NISD2

Member State Capabilities

- Identification of National authorities
- National strategies
- **CVD frameworks**
- **Crisis management frameworks**

Risk Assessment

- **Accountability for top management for non compliance**
- Security measures for companies
- Incident notifications for companies
- European cybersecurity certification schemes

Cooperation and Information Exchange

- Cooperation group
- CSIRTs network
- **CyCLONE**
- **CVD and European vulnerability registry**
- **Peer reviews**
- **Biennial ENISA cybersecurity report**
- **EU registry for some entities (e.g. DNS service providers, TLDs, cloud providers)**



INFORMATION SHARING IN NIS2

Reporting obligations

Significant incidents reported to CSIRT/NCA (24h/72h/1m)

Cross-border incidents

Aggregated reports to ENISA every 3 months

Other forms of info sharing

NIS CG / CSIRTs Network / EU-CyCLONe

CVD - EUVDB

NCSS - support voluntary information sharing

Art. 29 - information-sharing arrangements

Voluntary notifications

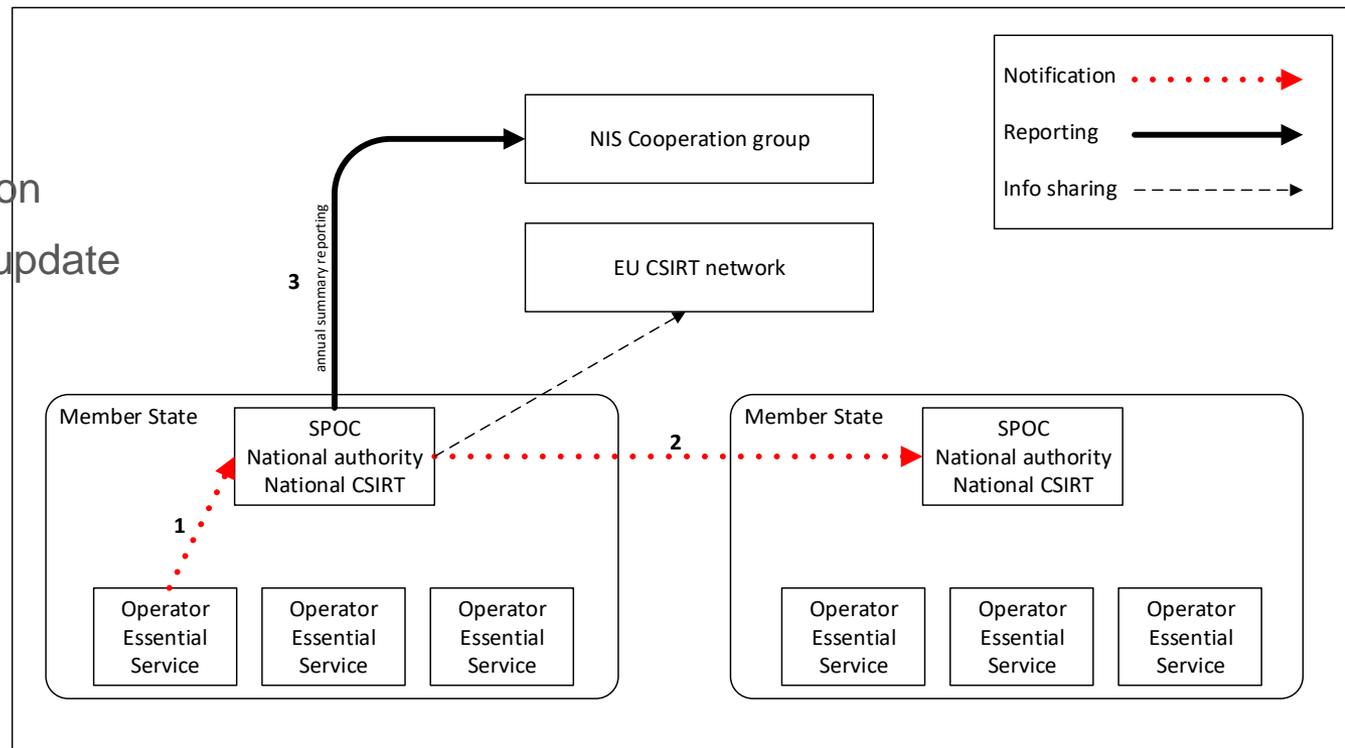
NIS2 – INCIDENT REPORTING

- What

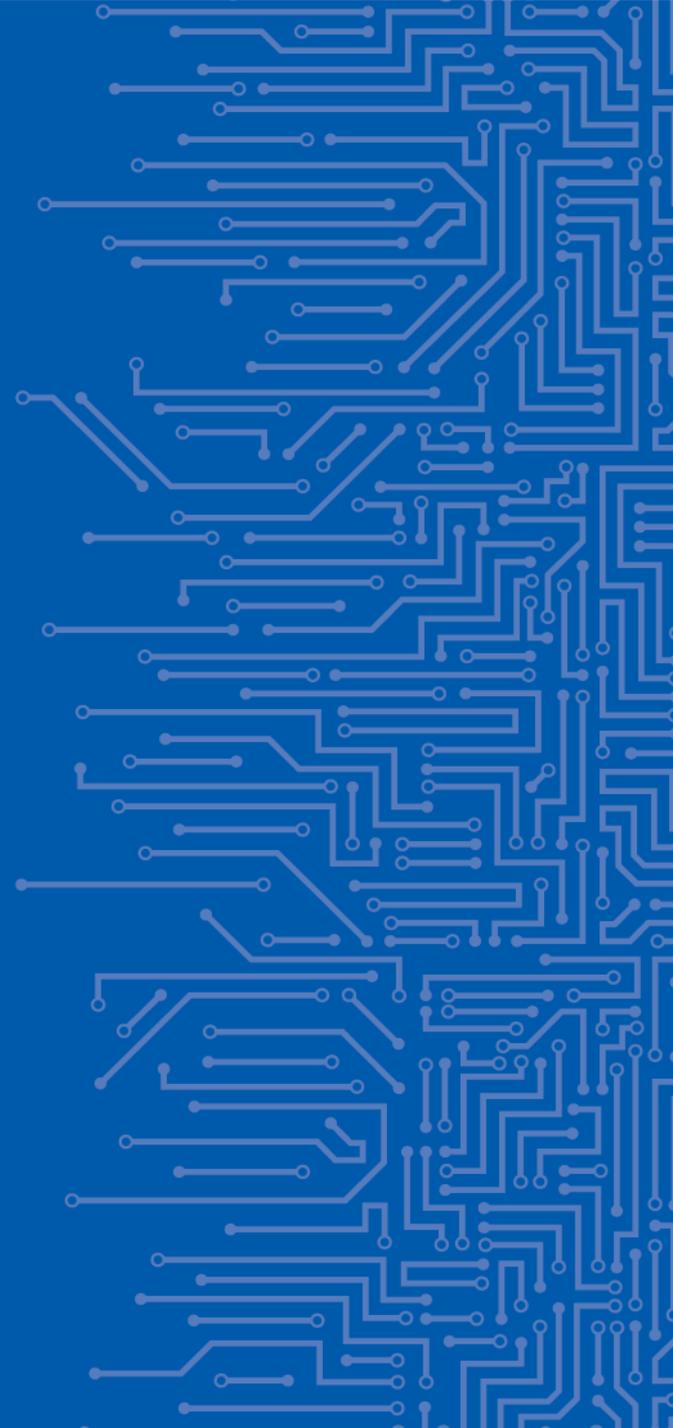
- significant incidents

- When

- 24h - early warning
- 72h - incident notification
- Upon request - status update
- 1 month - final report

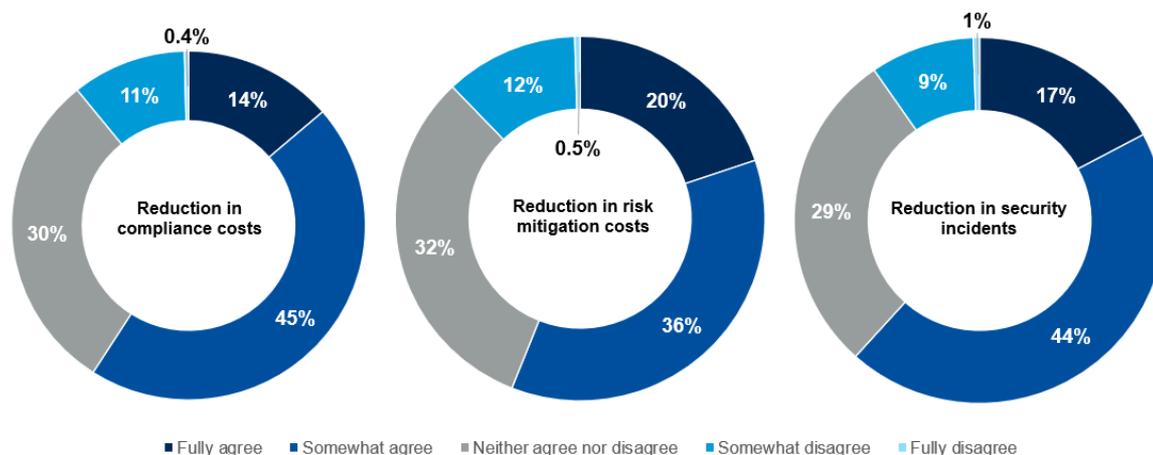


CRA



CYBER RESILIENCE ACT - CRA

- **Rules for placing on the market** of products with digital elements to ensure the cybersecurity of these products
- **Essential requirements** for product design, development and production and obligations for economic operators (manufacturers, distributors etc.)
- Essential requirements for vulnerability handling to ensure product **cybersecurity throughout the lifecycle**
- **Rules on market surveillance** and enforcement of requirements



Perceived impact of common requirements



INFORMATION SHARING IN THE CRA

Notification obligations

Actively exploited vulnerabilities reported to CSIRT and ENISA
(24h/72h/14d)

Severe incidents affecting product security reported to CSIRT and ENISA
(24h/72h/1m)

Single reporting platform

Other forms of info sharing

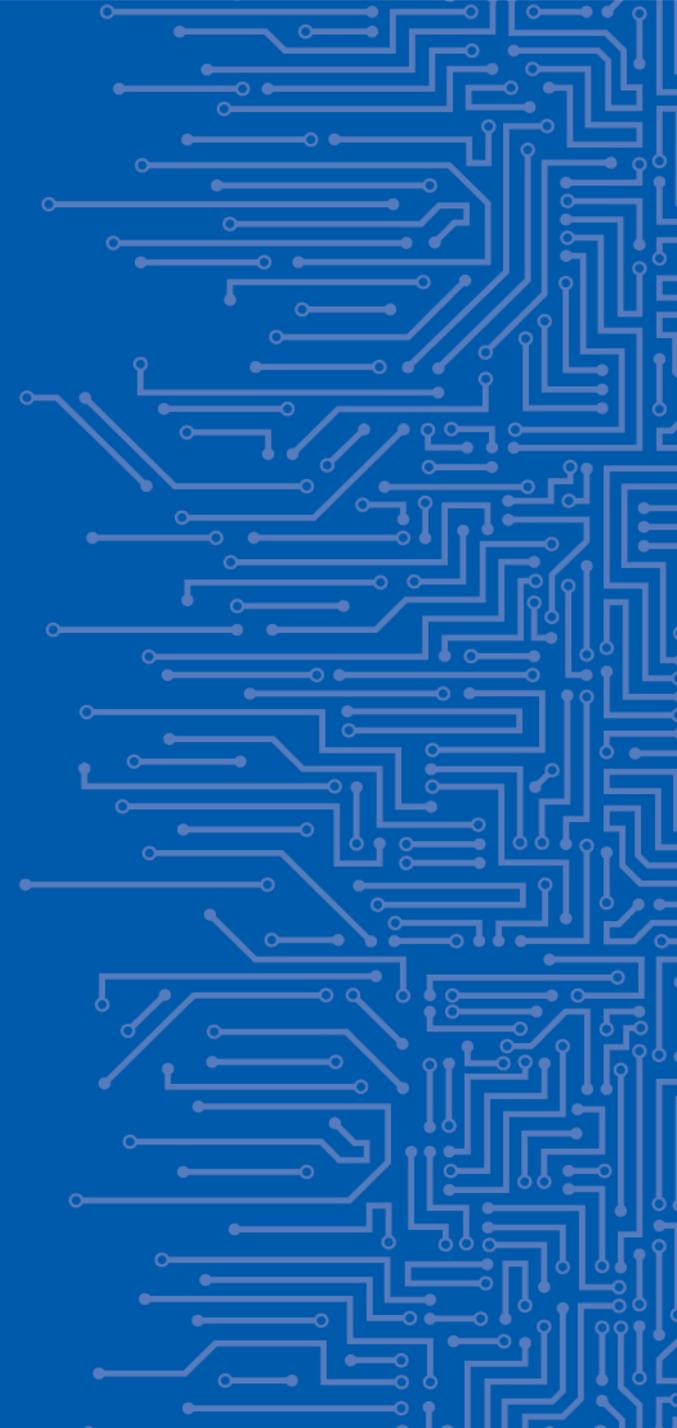
Manufacturers inform users

Voluntary reporting

Interface with NIS CG / EU-CyCLOne

Public awareness information

CSOA



CSSOA - MAIN PILLARS OF THE ACT



European Cybersecurity Alert System

Pan-European network of Cyber Hubs



Cybersecurity Emergency Mechanism

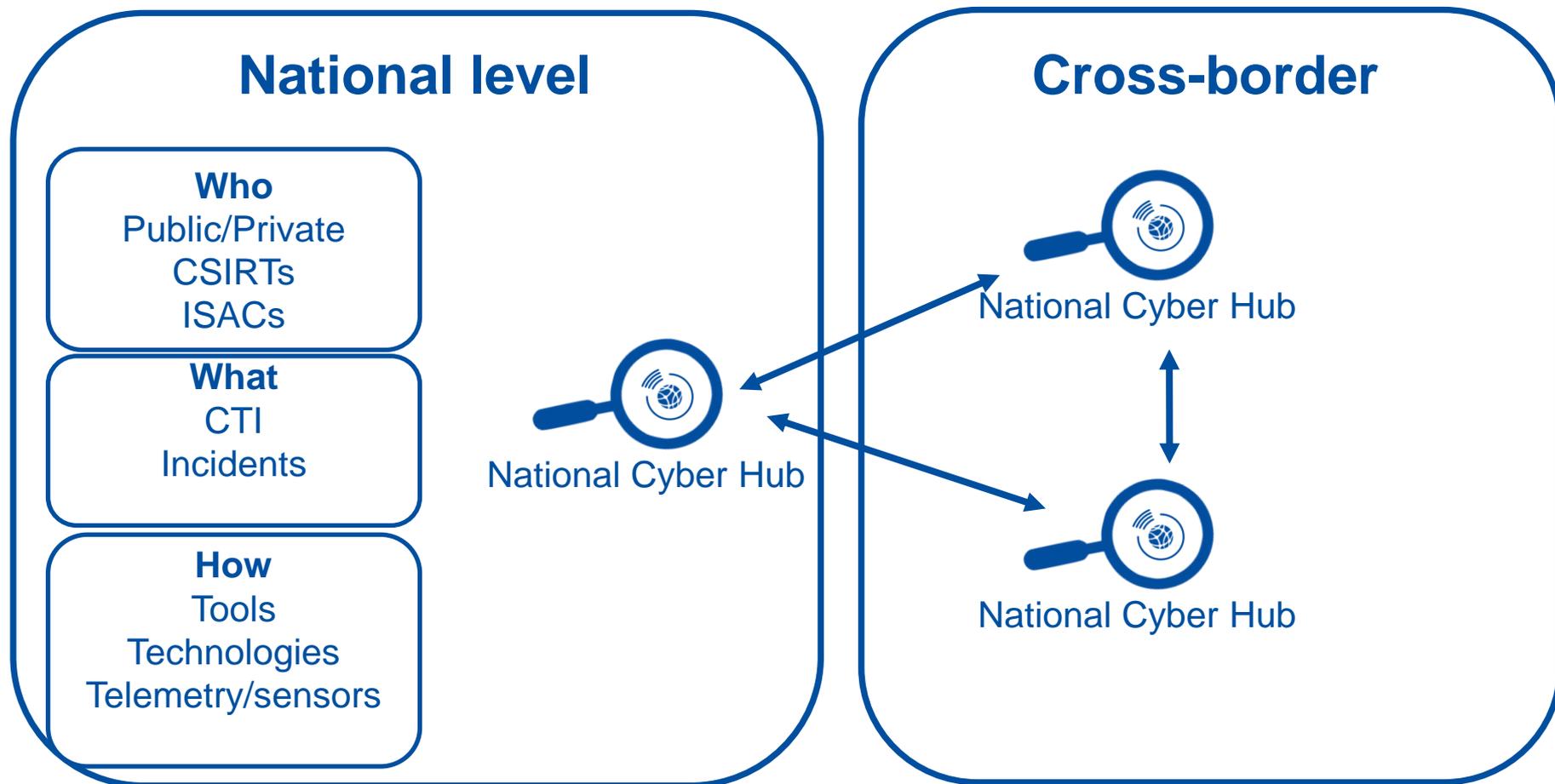
EU Cybersecurity Reserve and mutual assistance



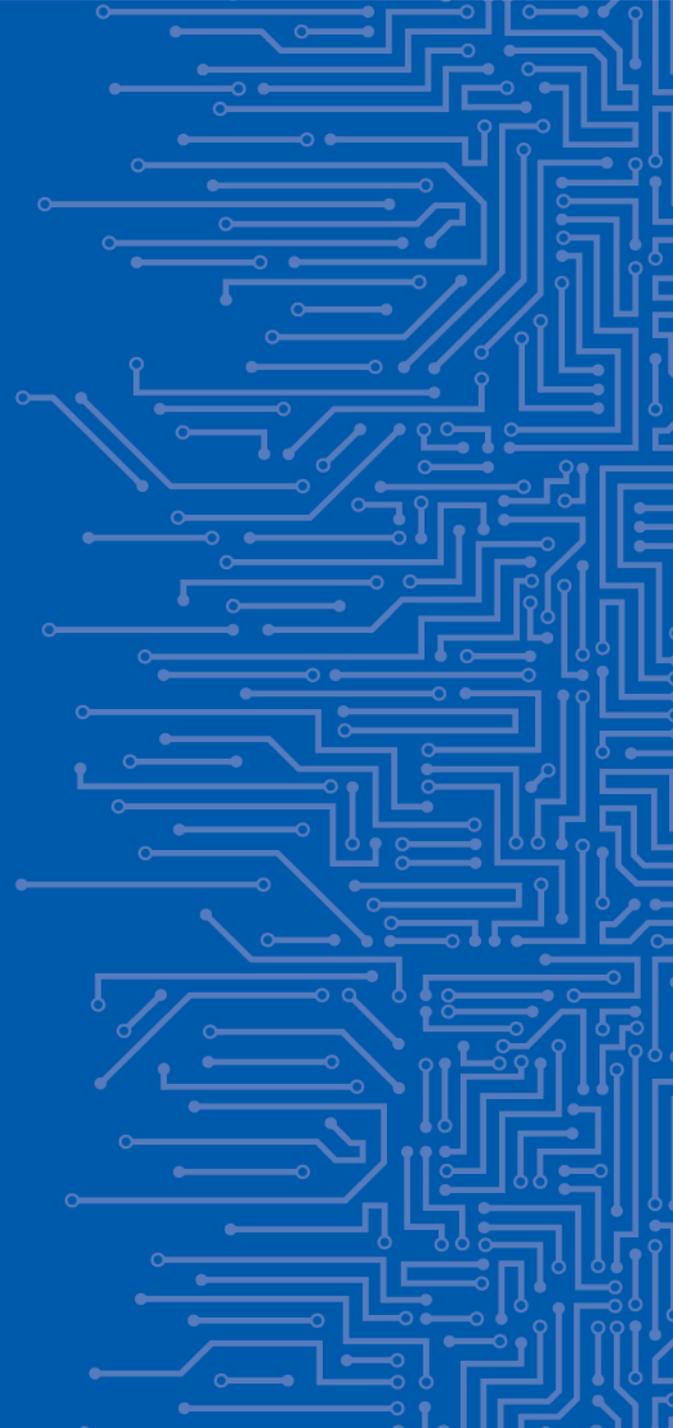
European Cybersecurity Incident Review Mechanism

Financed by the EU through the **Digital Europe Programme**

EUROPEAN CYBERSECURITY ALERT SYSTEM



BEYOND REGULATION

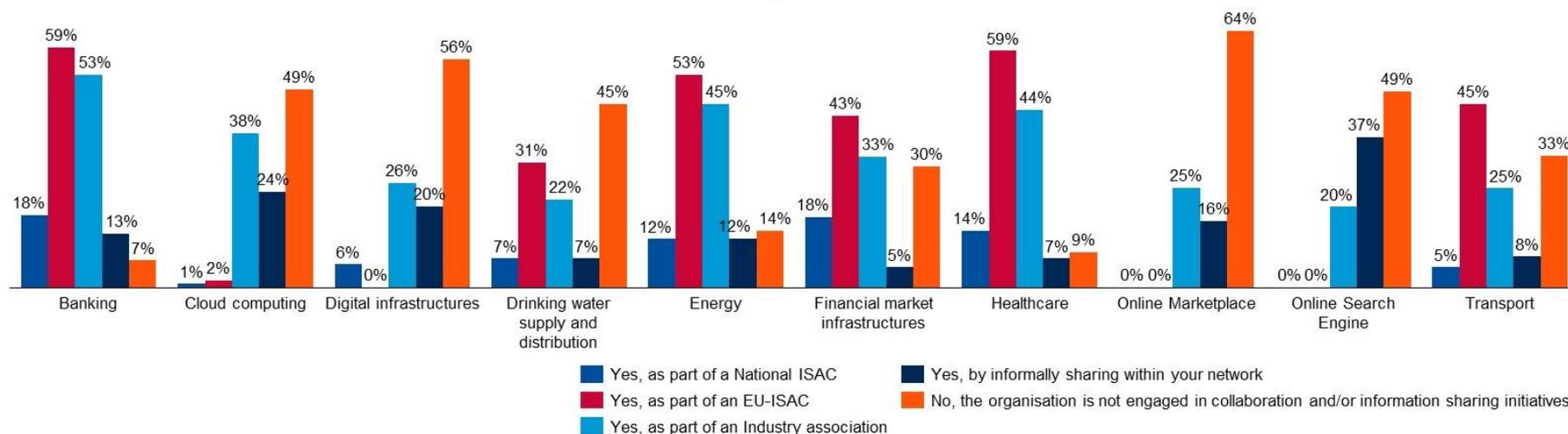
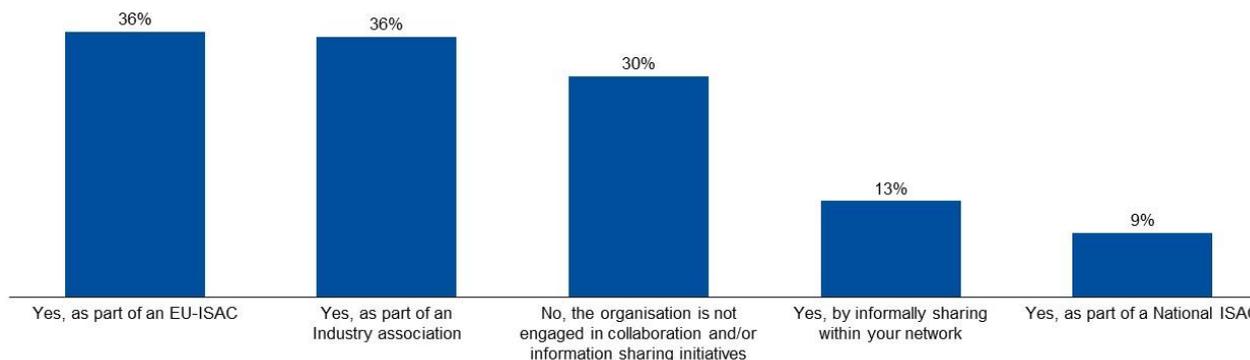


EM-ISAC



INFORMATION SHARING IN CRITICAL SECTORS- STATE OF PLAY

Participation in information sharing



THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 15231
Attiki, Greece

 +30 28 14 40 9711

 info@enisa.europa.eu

 www.enisa.europa.eu

