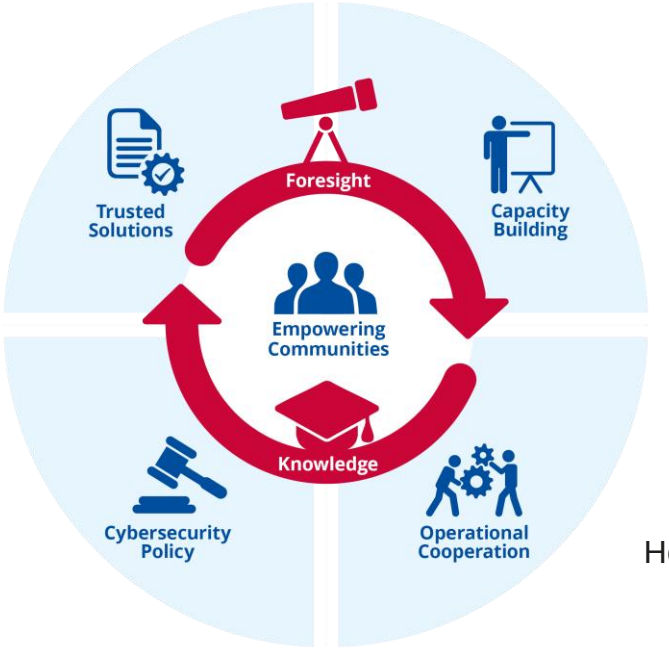
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

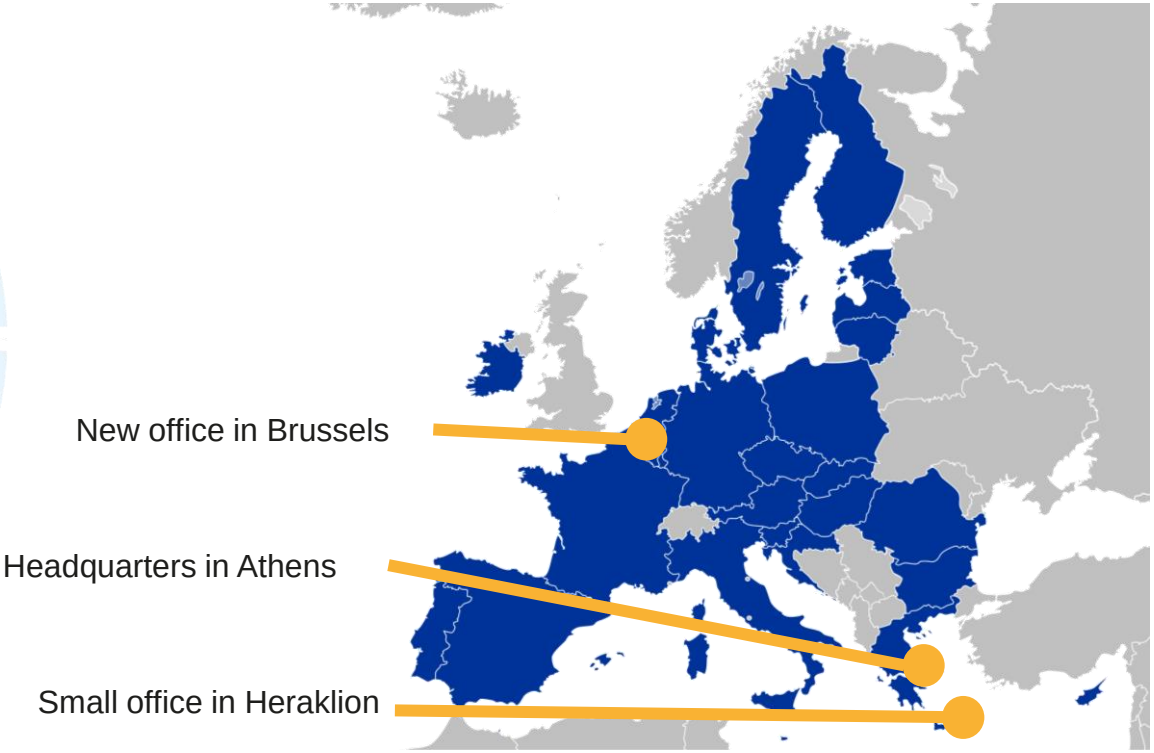
CYBERSECURITY POLICY IN THE EU

Evangelos Kantas
ENISA, the EU Agency for Cybersecurity

22 | 04 | 2024

ABOUT ENISA



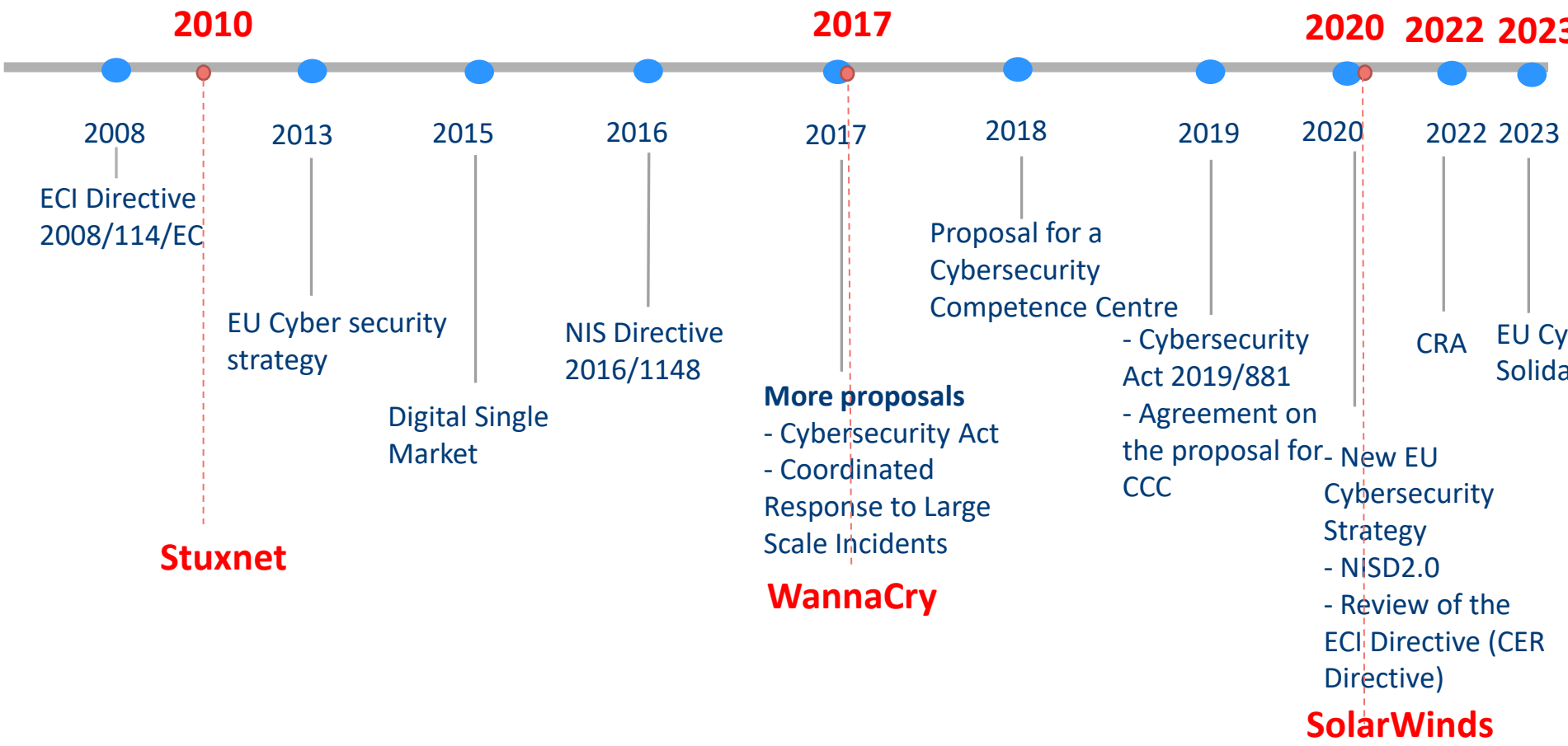


About 150 staff - steadily growing

4 units doing cybersecurity work

- Operational cooperation (Cyclone, CSIRT network)
- Cyber exercises, challenges, trainings (Cyber Europe)
- Certification and standardization (EU schemes)
- Policy unit (including EECC, eIDAS, NISD, 5G, eID wallets, critical sectors)

EU POLICY CONTEXT



NIS2 AND THE ROLE OF ENISA

NIS DIRECTIVE – IN A NUTSHELL

National cybersecurity capabilities

- National authorities
- National CSIRT
- National strategy

Cybersecurity collaboration between EU MS

- NIS Cooperation group
- EU CSIRT Network

Supervision of critical sectors by national authorities

- Security measures
- Incident reporting

ex-ante supervision

ex-post supervision

Policy	Sector	Subsectors
NISD OES – Article 14	Energy	Electricity
		Oil
		Gas
	Transport	Aviation
		Rail
		Maritime
		Road
	Finance	Financial market infra
		Banking
	Health	
	Drinking water	
	Digital infrastructure	IXP, TLDs, DNS providers
NISD DSP – Article 16	Digital service providers	Online marketplaces, online search engines, cloud computing providers
Article 19	Electronic trust services	Electronic trust service providers (TSPs) like certificate authorities
Article 13a	Electronic communications	Electronic communication providers, telcos and OTT service providers (EECC)

NIS2 PROPOSAL – SECTORS

New but old

IMPORTANT ENTITIES

Annex I "Other Critical Sectors"

or

Annex I "High Criticality" Sector

+

50<employees<250 and
€M10<turnover<€M50

ESSENTIAL ENTITIES

Annex I "High Criticality Sectors"

+

>250 employees and turnover >€M50

or

>€M43 total assets

Essential entities under NIS2	
Digital infrastructures	Telecom networks (mobile, fixed, satellite communications)
	Core internet infrastructure – IXPs, CDNs, TLDs, DNS,
	Trust services (webcertificates, e-signatures)
	Cloud and datacenters
Energy	Electricity
	District heating and cooling
	Oil
	Gas
	Hydrogen
Transport	Air – aviation
	Rail
	Water - Maritime transport, port management, vessel traffic services
	Road – road authorities and intelligent transport systems
Finance	Financial market infra, banking, trading, central counterparties
Health	Health care providers, EU reference laboratories, medicinal research, manufacturing of pharmaceuticals, critical medical devices
Drinking water	Suppliers and distributors
Waste water	Collection, disposal and treatment
Public administration	Central government and regions
Space	Ground-based infrastructure, supporting space-based services
Important entities under NIS2	
Digital providers	Online marketplaces, online search engines, social networks
Postal and courier services	
Waste management	
Chemicals	Manufacturing, production, distribution
Manufacturing	Medical devices, computer, electronic, optical products, electrical equipment, machinery, motor vehicles, other transport equipment

Cloud now critical (ex-ante regime)

New

New

New

New

New

New

New

IS THERE A NEED FOR UPDATED NIS2 SECURITY MEASURES?

1. **NIS2 introduces extra (cyber) security measures**

   → Update to the existing NIS Cooperation Group (CG) "Reference document on security measures for Operators of Essential Services"

2. **NIS2 art. 21(5) mandates the NIS CG and ENISA to provide input to the COM concerning the implementing act on security measures**

   → Draft input to COM for the implementing act, building on the updated reference document

INCIDENT REPORTING (ART. 23)

2 elements that are both to be considered when it comes to defining incidents:

- Event compromising:
  - Availability
  - Authenticity
  - Integrity
  - Confidentiality

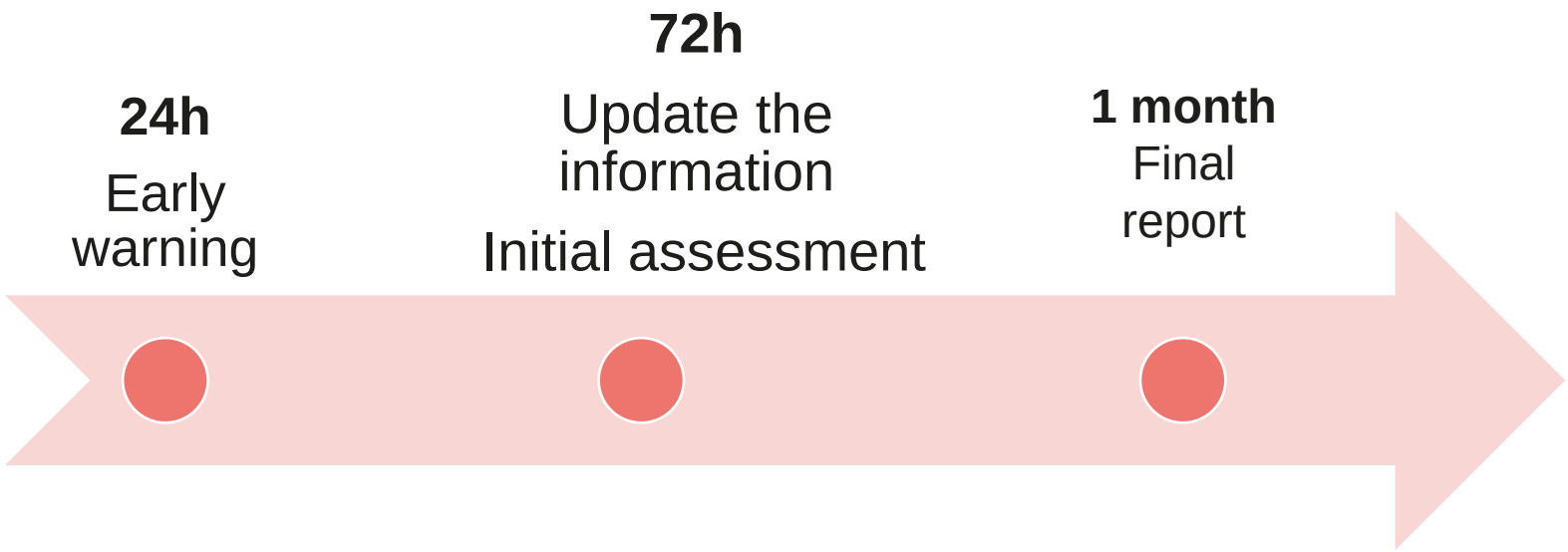
- Event having impact on:
  - Stored, transmitted or processed data
  - Services offered by, or accessible via, network and information systems
  - An event is defined as an incident when it covers any combination of the elements above.

An incident shall be considered to be significant if:
(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
(b)it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage

INCIDENT REPORTING

Notification of significant incidents

.



To CSIRT or Competent Authority

MANAGEMENT RESPONSIBILITIES

Approve the adequacy of the cybersecurity risk management measures taken by the entity

Supervise the implementation of the risk management measures

Follow training (identify risks and assess cybersecurity risk management practices and their impact)

Offer similar training to their employees on a regular basis

Be accountable for the non-compliance

https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf

ENISA NIS2 ACTIVITIES

- **NIS2 outreach campaign**

  → NIS2 Portal, targeted campaigns, ready-to-use material, multiple formats

- **NIS2 Cybersecurity Essentials training (for public stakeholders)**

  → Basic concepts, cybersecurity risk management measures, incident handling, risk scenarios

- **EU DI Registry**

  → EU Registry for cross-border entities

- **EU Vulnerability Database**

  → Enhance trust in EU products

THANKS!!!!

Evangelos.Kantas@enisa.europa.eu

enisa.europa.eu