# Cybersecurity in the EU

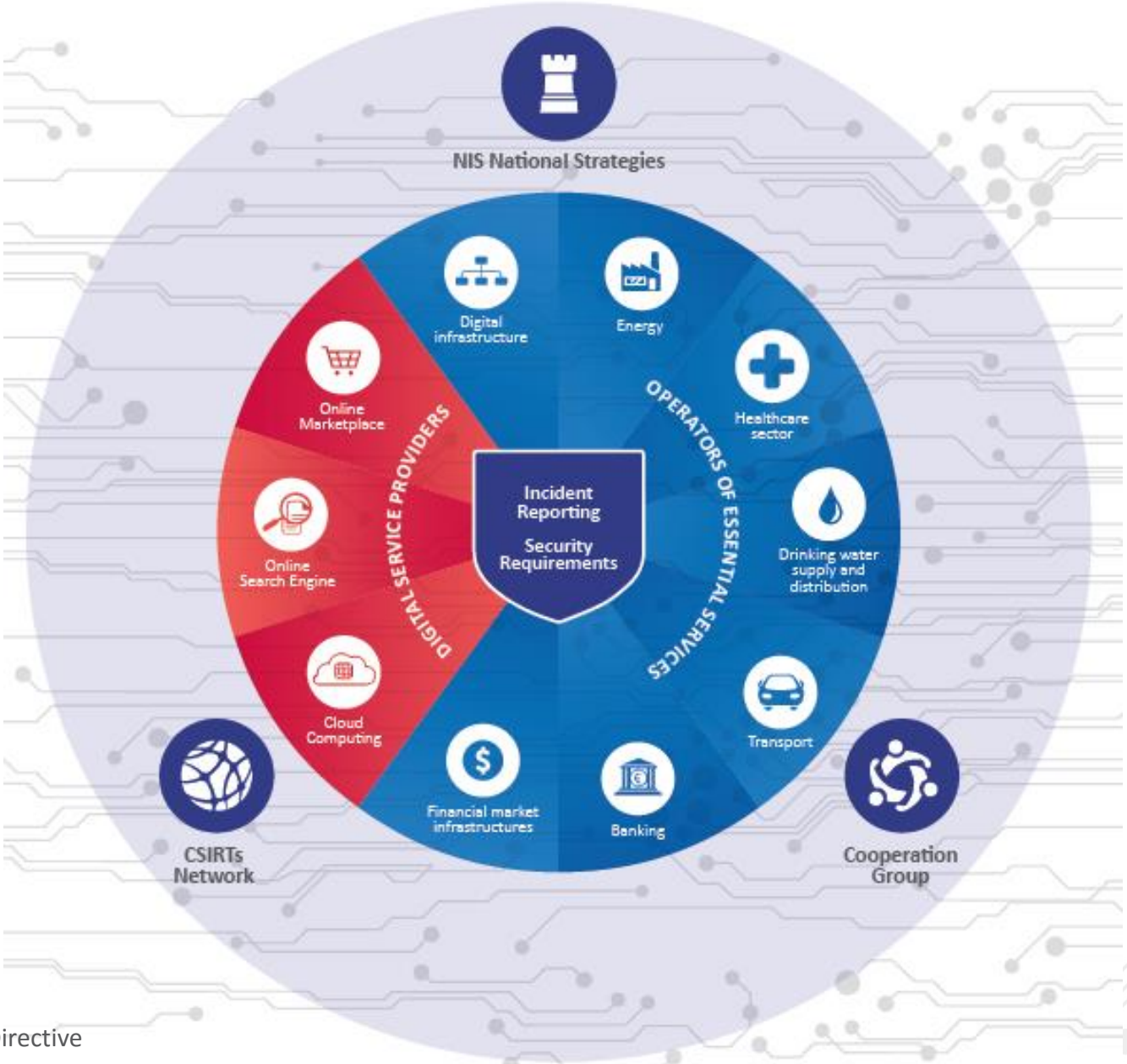
Steve Purser| Head of Operational Departments, ENISA

Regional Cybersecurity Forum| Sofia, Bulgaria| 29th November 2016

European Union Agency for Network and Information Security

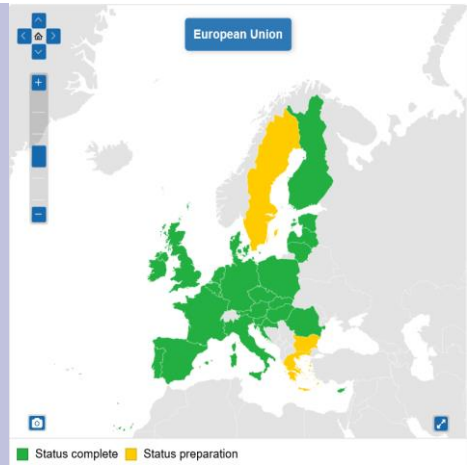
# Positioning ENISA activities

# The NIS Directive



# NCSS - ENISA Supports the MS

ENISA NCSS EU map




ENISA REPORTS


E-Learning & Workshops

ENISA NCSS Expert Group & Art.14 Requests

# ENISA CSIRTs in Europe and the EU CSIRTs Network

# CSIRTs in Europe state of affairs in 2016

- Publicly known more than 300 CSIRT teams and the number grows
- Representing different sectors and type of CSIRT
  - Public or private; national scope; company internal; academic, research, sectorial like governmental, financial, energy, health; etc.

- ~ 40 teams with national scope in Europe-wide scale

- Different setup model in almost every country (there is no supermodel!!!)
- Very few publicly known military and secret intelligence types (red teams)
  - > (growing tendency)

- CSIRTs operational groups and networks exist since early 2000 in Europe

- Mostly regional, sectorial or national-wide(TF-CSIRT, EGC, national-wide in AT, DE, LU, CH, CZ, NL, ES, …)

- National CSIRT usually acts as the catalyser or mediator for the efficient national cooperation (with other teams in the country, with government (policy) and with private sector (ISPs, threat intelligence, etc.)

# CSIRTs Network – EU expectations

- Unique characteristic (NISD obligation for all 28 EU MS and EU Institutions to have a national CSIRT.
- Joint and shared opportunity to enhance incident response operations across the whole EU
- Will operate in parallel to the existing groups and networks
  - in and outside EU
- Trust takes time – it's a process not status quo

Expected:

- 2017 onwards to become a stable group of trusted partners from all 28 EU MS and EU institutions
- Expected to have 28 national CSIRTs, CERT-EU and ENISA-CSIRT-relations representation (around 60 people)

(trust is not scalable for growing numbers)

# ENISA's support for national CSIRT capability building

- First NISD deadline and obligation by 09/02/2017 to nominate representatives for cooperation group and CSIRTs Network.
- Inform ENISA about CSIRT team and team reps. until 9th February'17

(cert-relations@enisa.europa.eu )

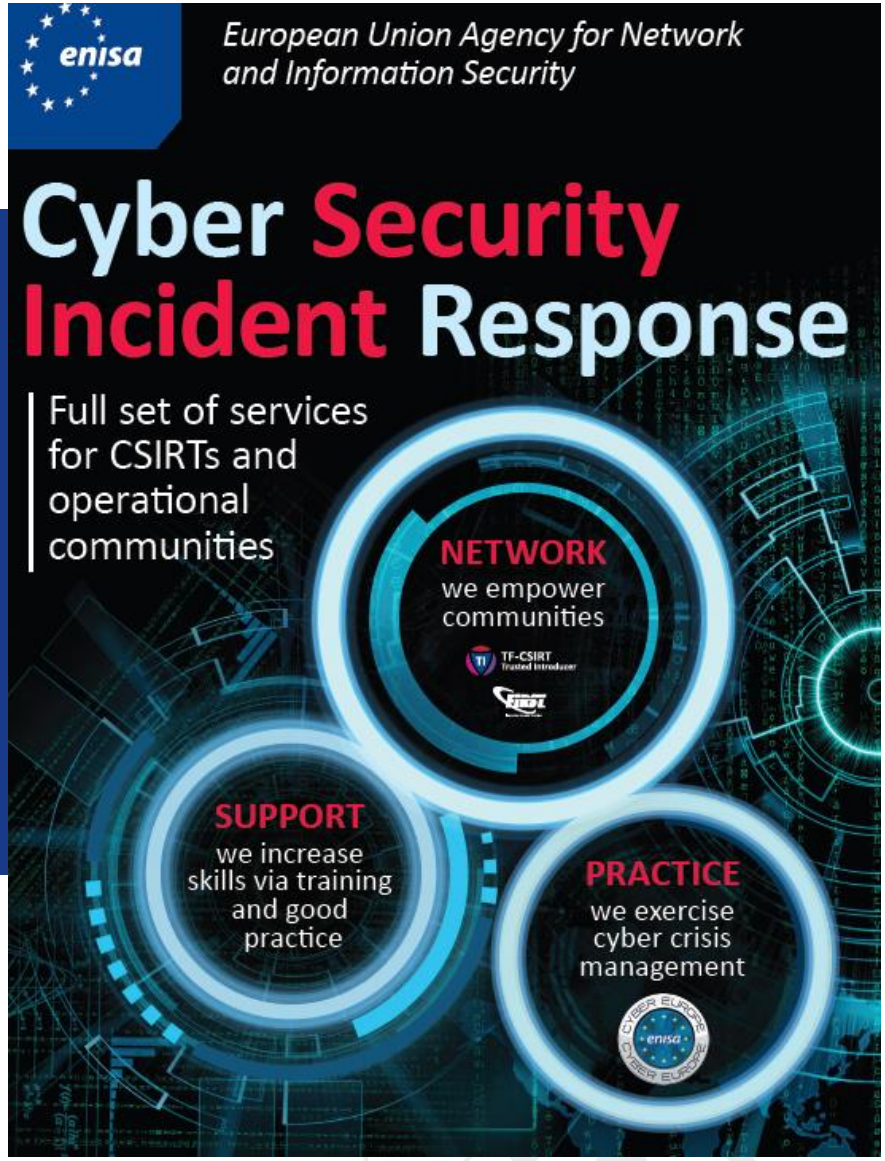
- First Formal CSIRT Network meeting on 22-23 February, Valletta, Malta

- National CSIRT capability building – ENISA continues to support MS individually!!

- Any inquires or questions: cert-relations@enisa.europa.eu

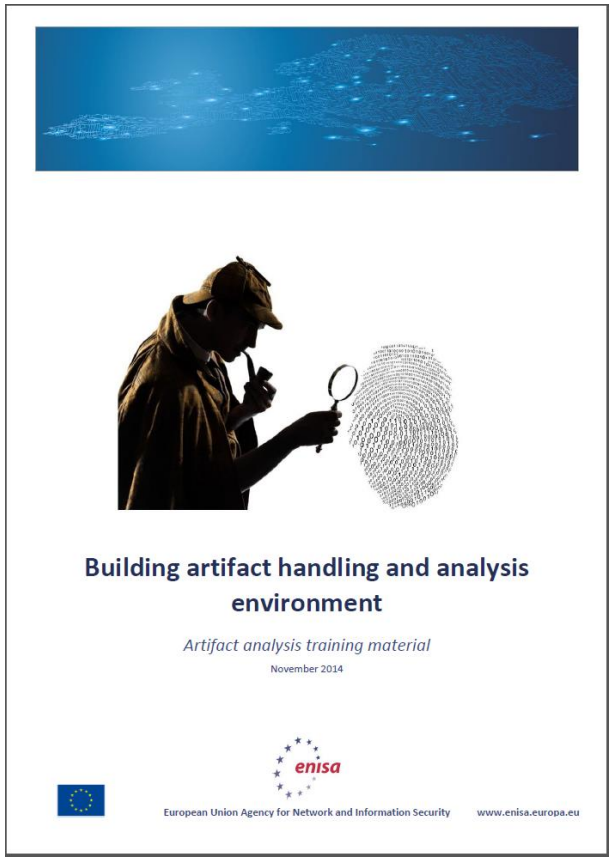
# Support Capacity building

## Trainings and exercises

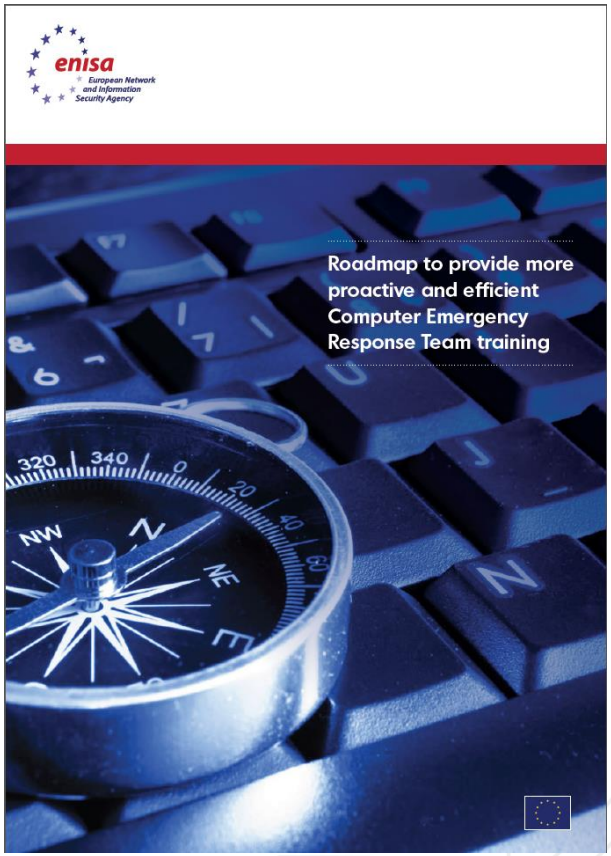


# Material, Roadmap and Methodology

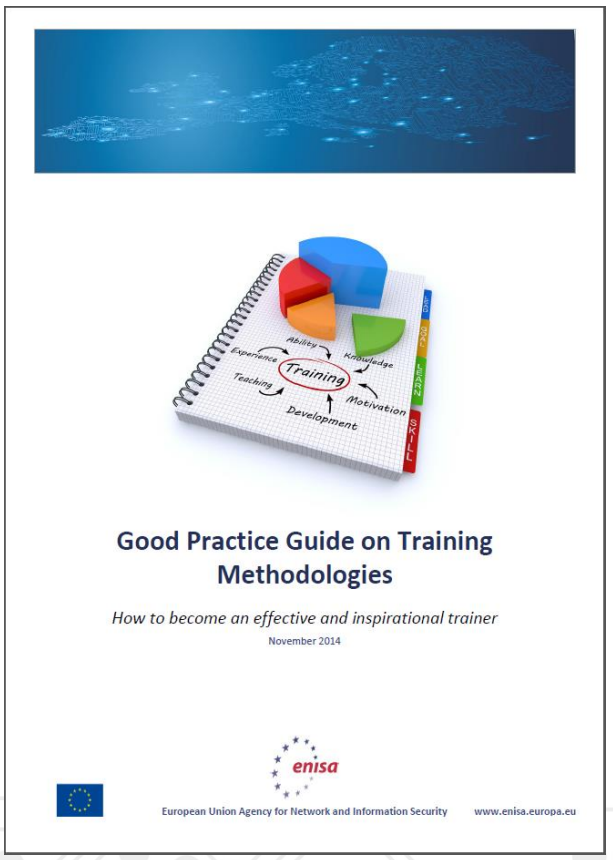
Material since 2008




Roadmap from 2012




Methodology from 2014



# Examples of training resources

Mobile threats incident handling

Digital forensics

Large scale incident handling

Network forensics

Triage & basic incident handling

Vulnerability handling

Artifact analysis fundamentals

Advanced artifact handling

Writing security advisories

Developing countermeasures

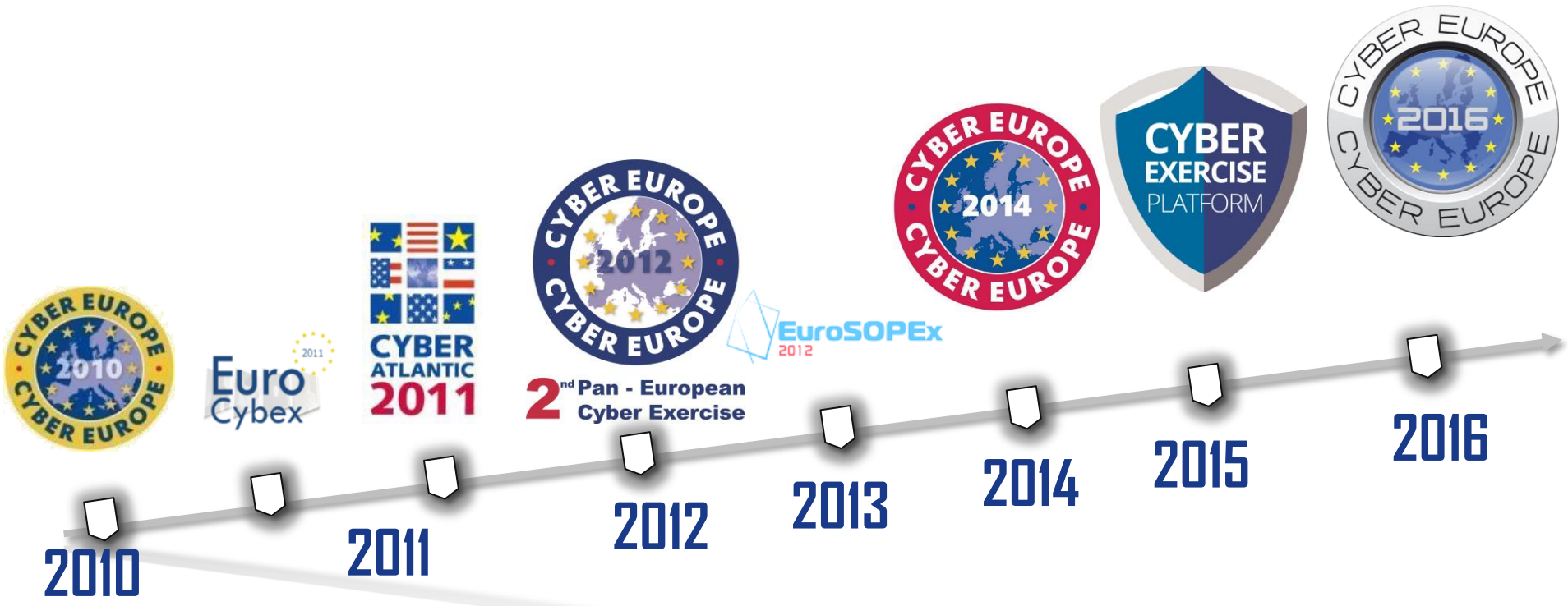
Identification and handling of electronic evidence

Automation in incident handling

# Cyber Exercises

Trainings and exercises

# Organisation of exercises



# CE2016 Overview

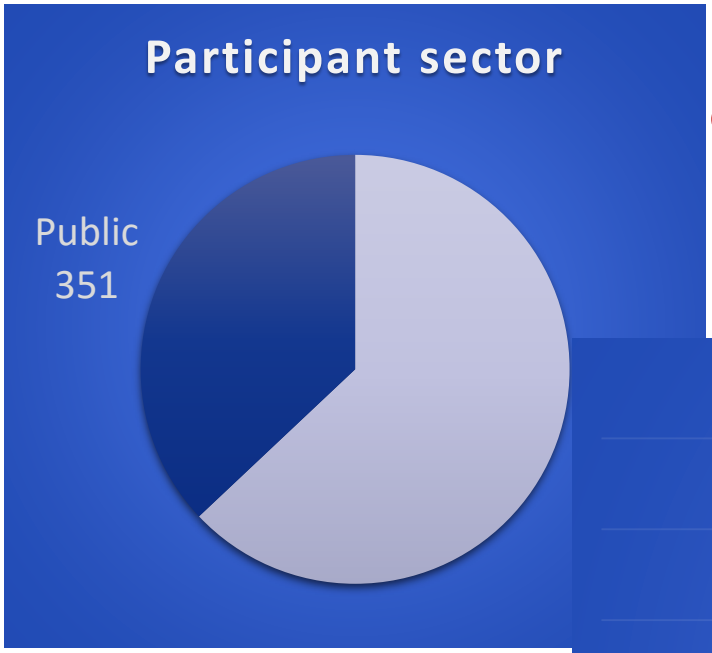
- Simulation of an EU-wide crisis triggered by cyber attacks

  Goals: 1) test EU- and national-level cooperation

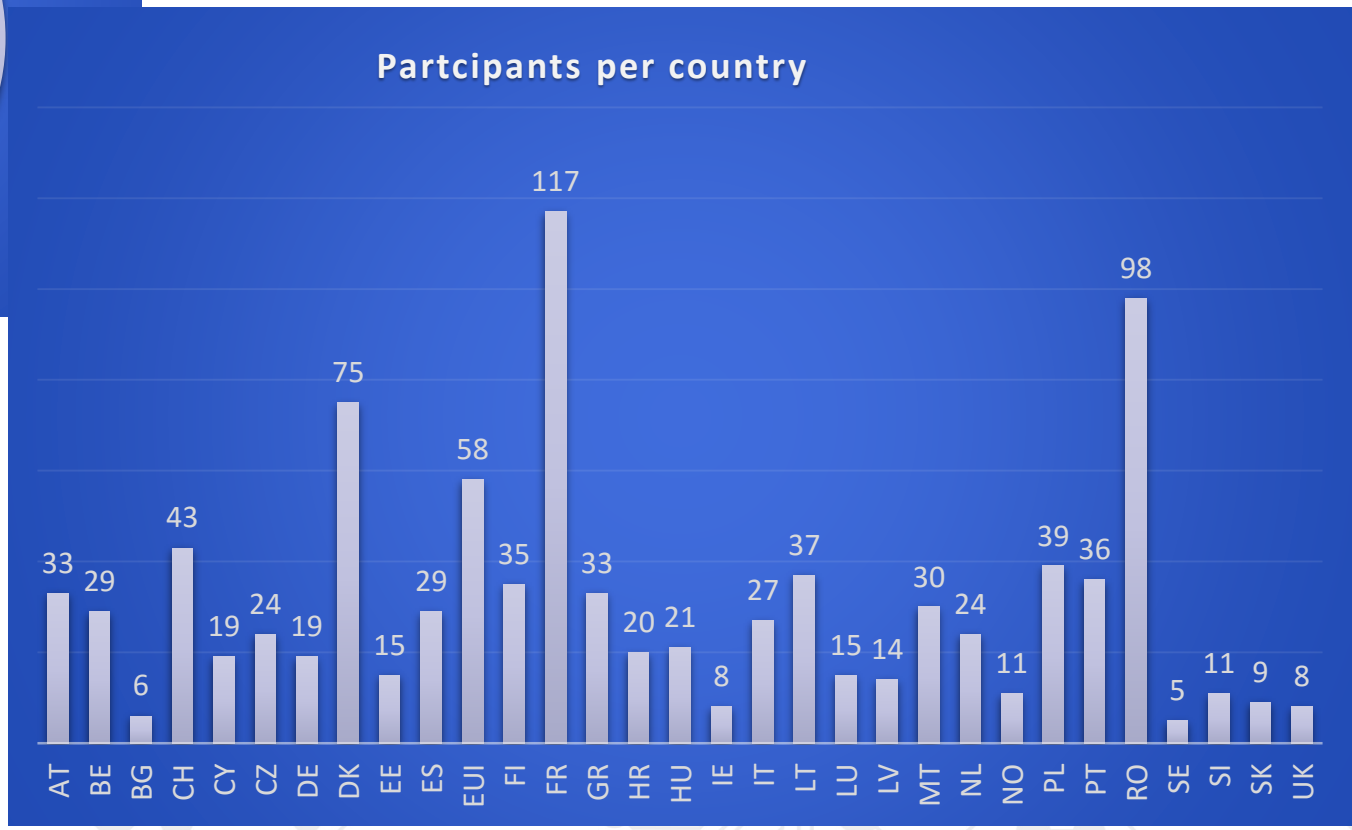
  2) improve technical and operational capabilities


- Six-month exercise simulating a crisis build-up
- October 13-14 with all participants to test cooperation
  - Operational together with technical incidents
- Enhanced reality: news, social media, blogs, websites, etc. (BCC News, Fakebook, Clickedin, …)

# Participation




948 Participants!

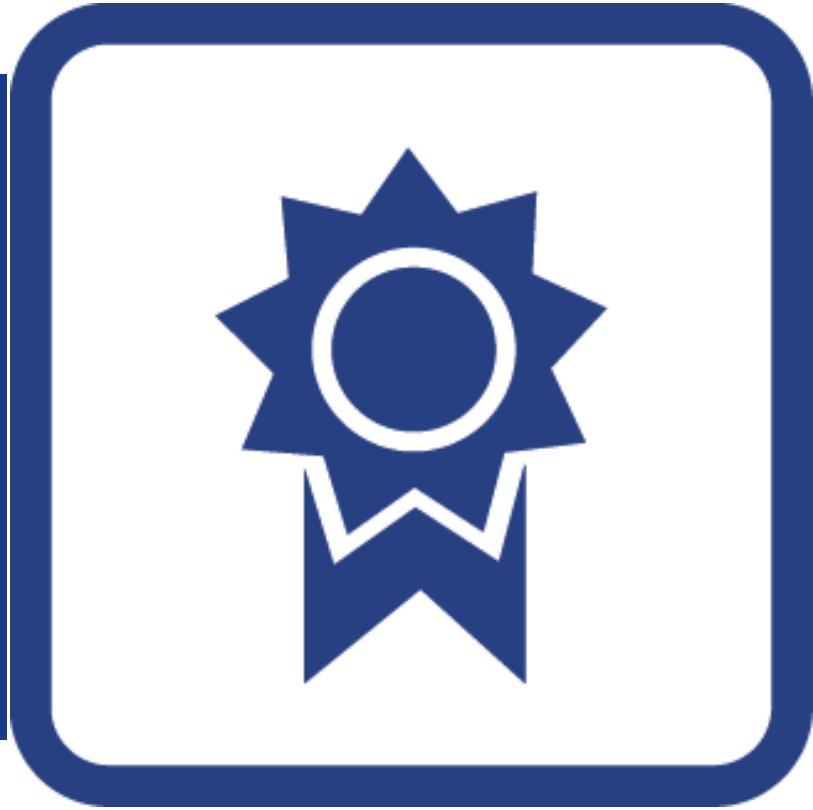


# CE2016 Videos

CE2016 Trailer: https://www.youtube.com/watch?v=qrDiaPo5QpQ

CE2016 Promo video: https://www.youtube.com/watch?v=2wVsB1WCfNg

# IT security certification



# SOGIS-MRA
## Technical framework for IT security certification

- SOGIS – Mutual Recognition Agreement (MRA) (v.3) – 2010
  - Signed by AT, FI, FR, DE, IT, NL, UK, ES, SE + NO
  - Participants to this Agreement are government organisations or government agencies
  - Recognition from all signatories of CC and ITSEC certificates up to EAL 4
  - Recognition of highest assurance levels defined for specific IT technical domains (including smart card technologies).
  - Peer review and information sharing amongst participants -> recognition of certificates issued
- The MRA is not part of the “EU acquis”
- The MRA does not apply to the 28 Member States

# Challenges
## from the EU perspective

- Recognition of trustworthiness of security products
  - Requested by EU legislative initiatives (eIDAS, NIS, GDPR)
  - CC as only reference
  - Absence of a lightweight process
- No common EU Framework
  - Lack of coherence
  - Absence of enforcement
- Existing
  - National efforts
  - Cross country initiatives

# ENISA actions

- 24 February 2016 – 1st workshop on certification (MS)
- 24 March 2016 – 2nd workshop on certification (industry)
- 2016 – roadmap for a common framework of certification of security products
- 2016 – collaboration with semiconductors industry
- 2016 – collaboration with the European Commission (cPPP)
- 2017 – Proposal of a common framework of certification of security products

# Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu