Supporting CSIRTs in the EU

Marco Thorbruegge

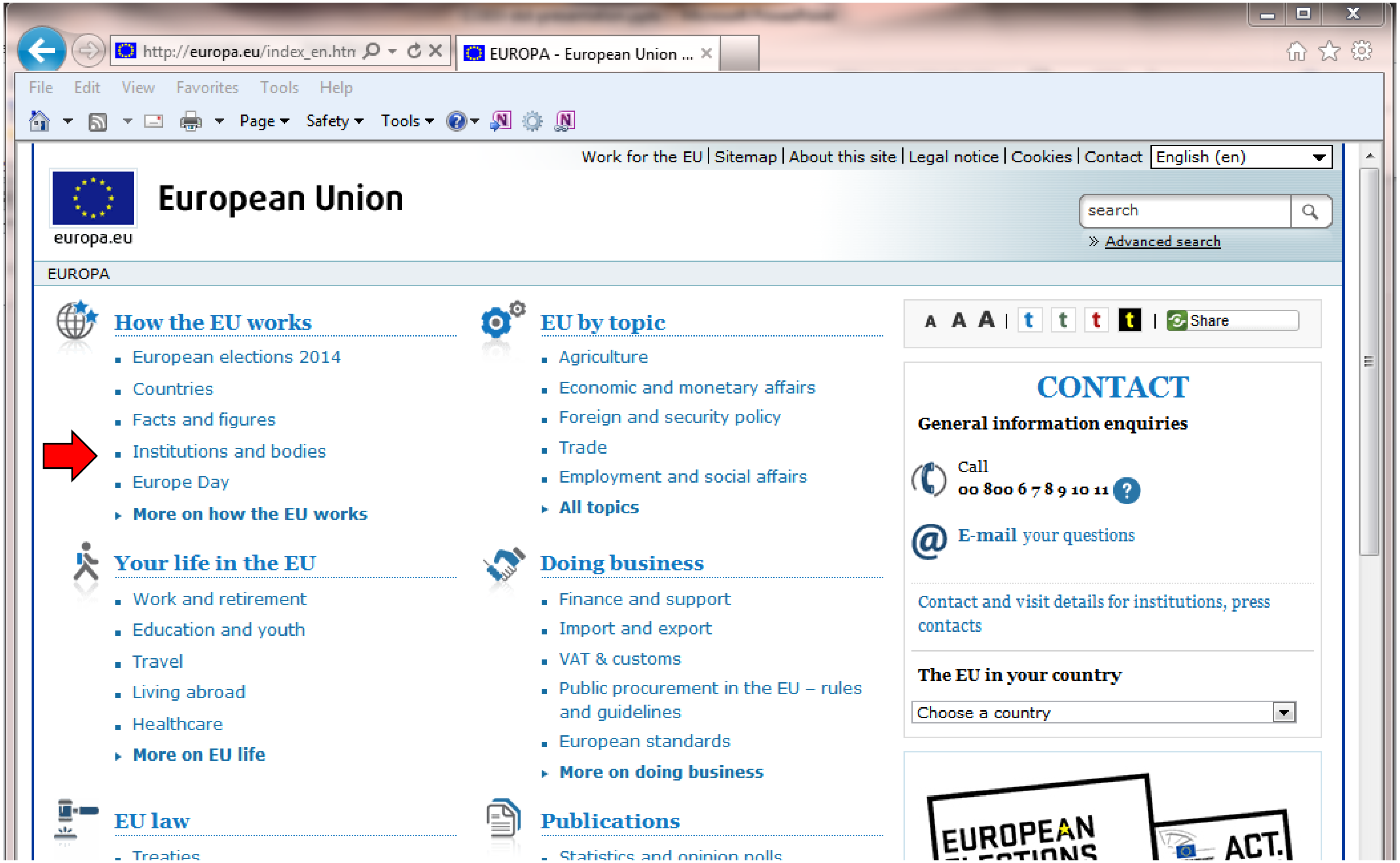
Head of Unit – Operational Security

European Union Agency for Network and Information Security

Agenda

- **Who is ENISA?**
- **EU Policy context**
- Examples of ENISAs work
  - Threat Landscape
  - Cyber Europe Exercises
- Support for EU CSIRTs
  - Fight against Cybercrime
  - Baseline capabilities for national CSIRTs
  - Capability building – training
  - ENISA and the CSIRT communities

Who is ENISA



http://europa.eu/index_en.htm
EUROPA - European Union ...
File Edit View Favorites Tools Help
Page Safety Tools

Work for the EU | Sitemap | About this site | Legal notice | Cookies | Contact | English (en)

European Union

europa.eu

search

» Advanced search

EUROPA

How the EU works

- European elections 2014
- Countries
- Facts and figures
- Institutions and bodies
- Europe Day
- **More on how the EU works**

EU by topic

- Agriculture
- Economic and monetary affairs
- Foreign and security policy
- Trade
- Employment and social affairs
- **All topics**

Your life in the EU

- Work and retirement
- Education and youth
- Travel
- Living abroad
- Healthcare
- **More on EU life**

Doing business

- Finance and support
- Import and export
- VAT & customs
- Public procurement in the EU – rules and guidelines
- European standards
- **More on doing business**

EU law

- Treaties

Publications

- Statistics and opinion polls

A A A | t t t t | Share

CONTACT

General information enquiries

Call
00 800 6 7 8 9 10 11 ?

@ E-mail your questions

Contact and visit details for institutions, press contacts

The EU in your country

Choose a country

Who is ENISA

Operational Office in Athens

Seat in Heraklion

EU Policy Context

EU Policy context

- EU Digital Agenda – COM(2010)245

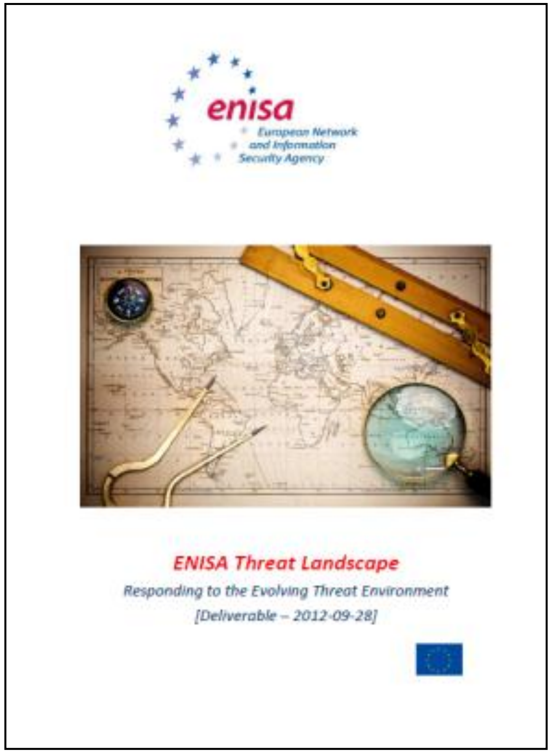
http://ec.europa.eu/digital-agenda/

- EU Cyber Security Strategy – JOIN(2013)1

http://ec.europa.eu/digital-agenda/en/cybersecurity

Agenda

- Who is ENISA?
- EU Policy context
- **Examples of ENISAs work**
  - Threat Landscape
  - Cyber Europe Exercises
- Support for EU CSIRTs
  - Fight against Cybercrime
  - Baseline capabilities for national CSIRTs
  - Capability building – training
  - ENISA and the CSIRT communities



enisa
European Network and Information Security Agency

ENISA Threat Landscape

Responding to the Evolving Threat Environment

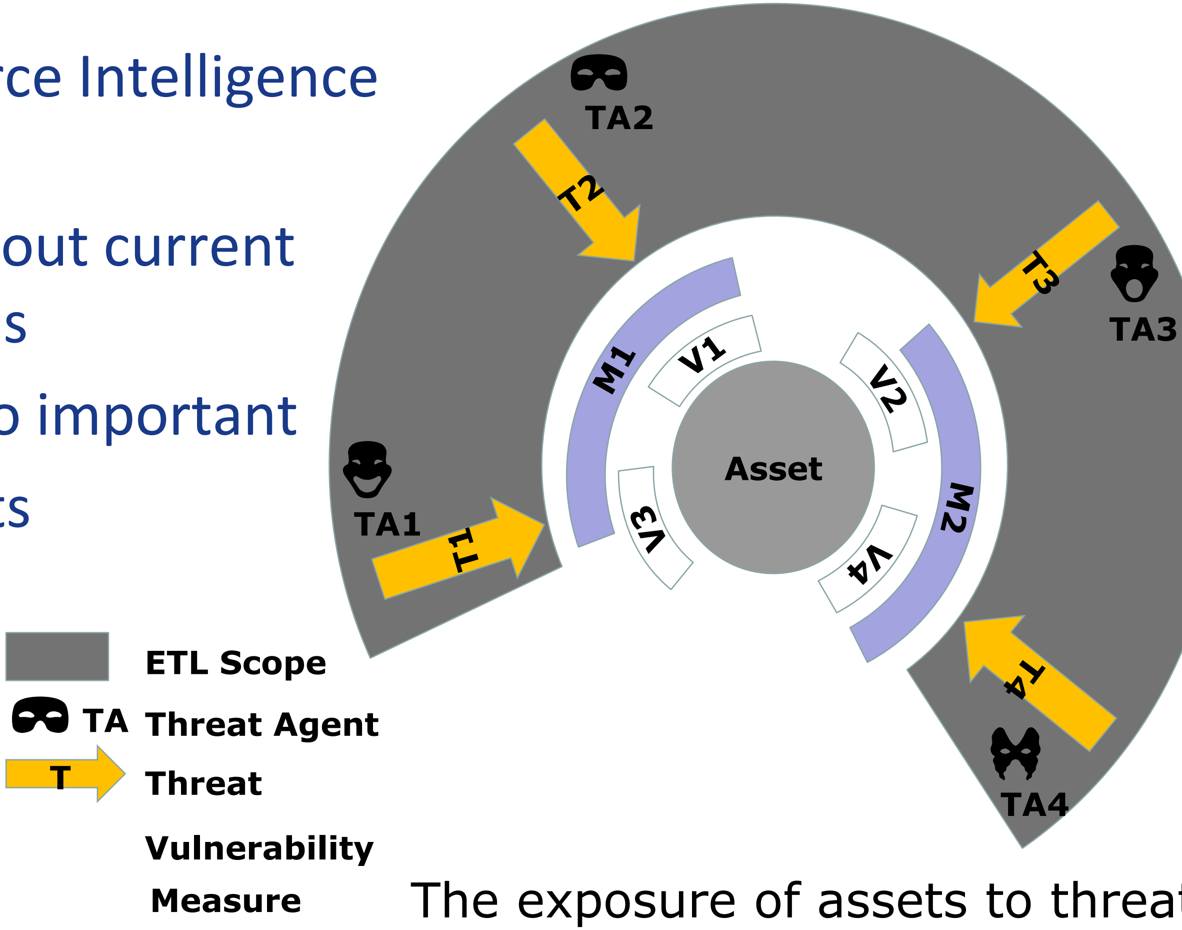
[Deliverable – 2012-09-28]

Examples of other work: Security Landscape

Report links:
http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

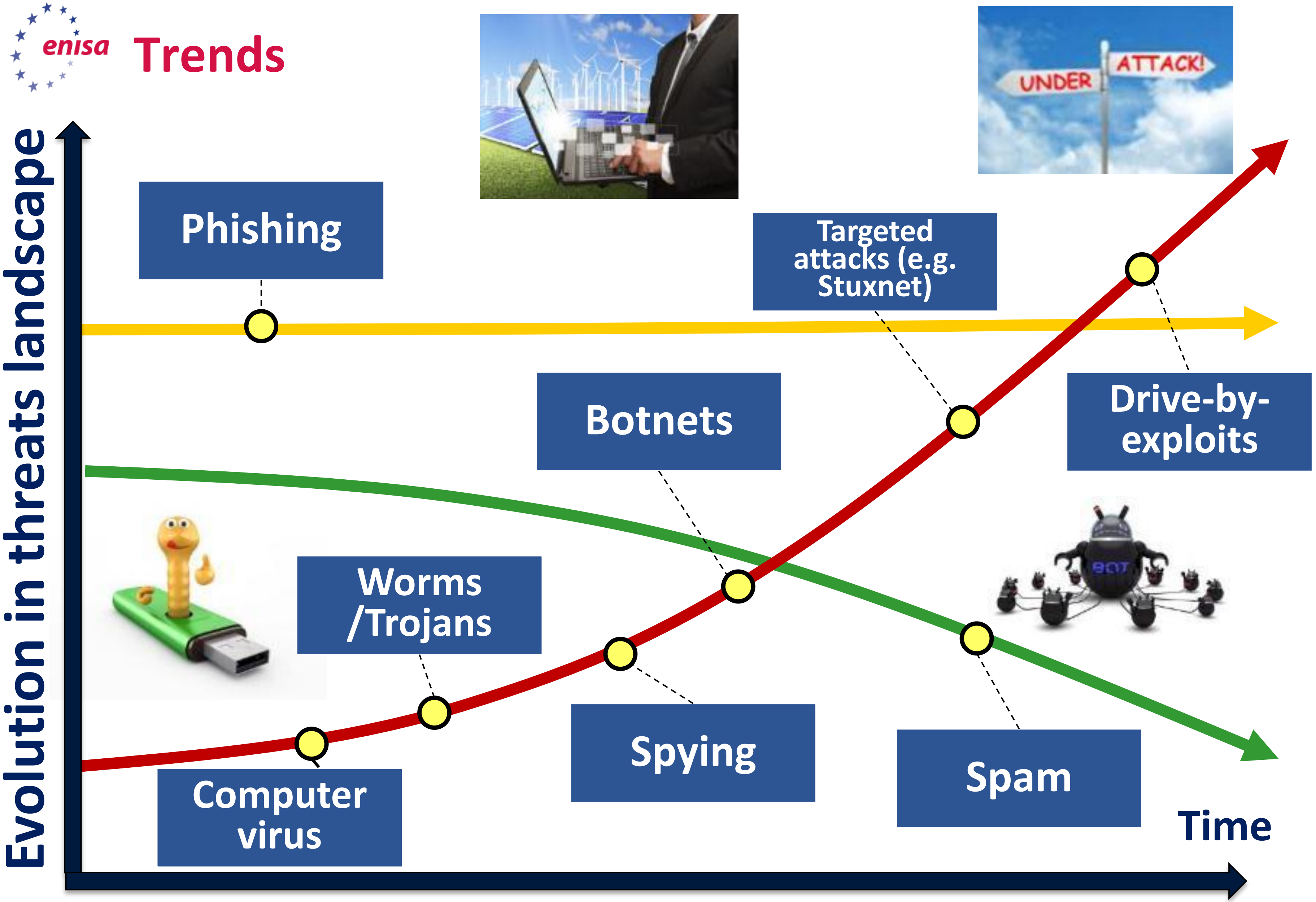
The ENISA Threat Landscape (ETL)

- Helps understanding the threats and threat sources
- It is Based on Open Source Intelligence (OSINT)
- Contains information about current threats and threat trends
- ENISA projects threats to important ICT areas/ sectors/ assets



The exposure of assets to threat

Trends



Evolution in threats landscape

Time

Phishing

Targeted attacks (e.g. Stuxnet)

Botnets

Drive-by-exploits

Worms /Trojans

Computer virus

Spying

Spam

Top Threats 2012	Assessed Trends 2012	Top Threats 2013	Assessed Trends 2013	Change in ranking
1. Drive-by exploits (this threat has been renamed)	⬆	1. Drive-by downloads	⬆	→
2. Worms/Trojans	⬆	2. Worms/Trojans	⬆	→
3. Code Injection	⬆	3. Code Injection	⬆	→
4. Exploit Kits	⬆	4. Exploit Kits	⬆	→
5. Botnets	⬆	5. Botnets	➡	→
6. Denial of Service	➡	6. Physical Damage/Theft/Loss	⬆	↑
7. Phishing	➡	7. Identify Theft/Fraud	⬆	↑
8. Compromising Confidential Information (this threat has been renamed to Data Breaches)	⬆	8. Denial of Service	⬆	↓
9. Rogueware/ Ransomware/Scareware	➡	9. Phishing	⬆	↓
10. Spam	⬇	10. Spam	➡	→

Examples of other work: Cyber Security Exercises

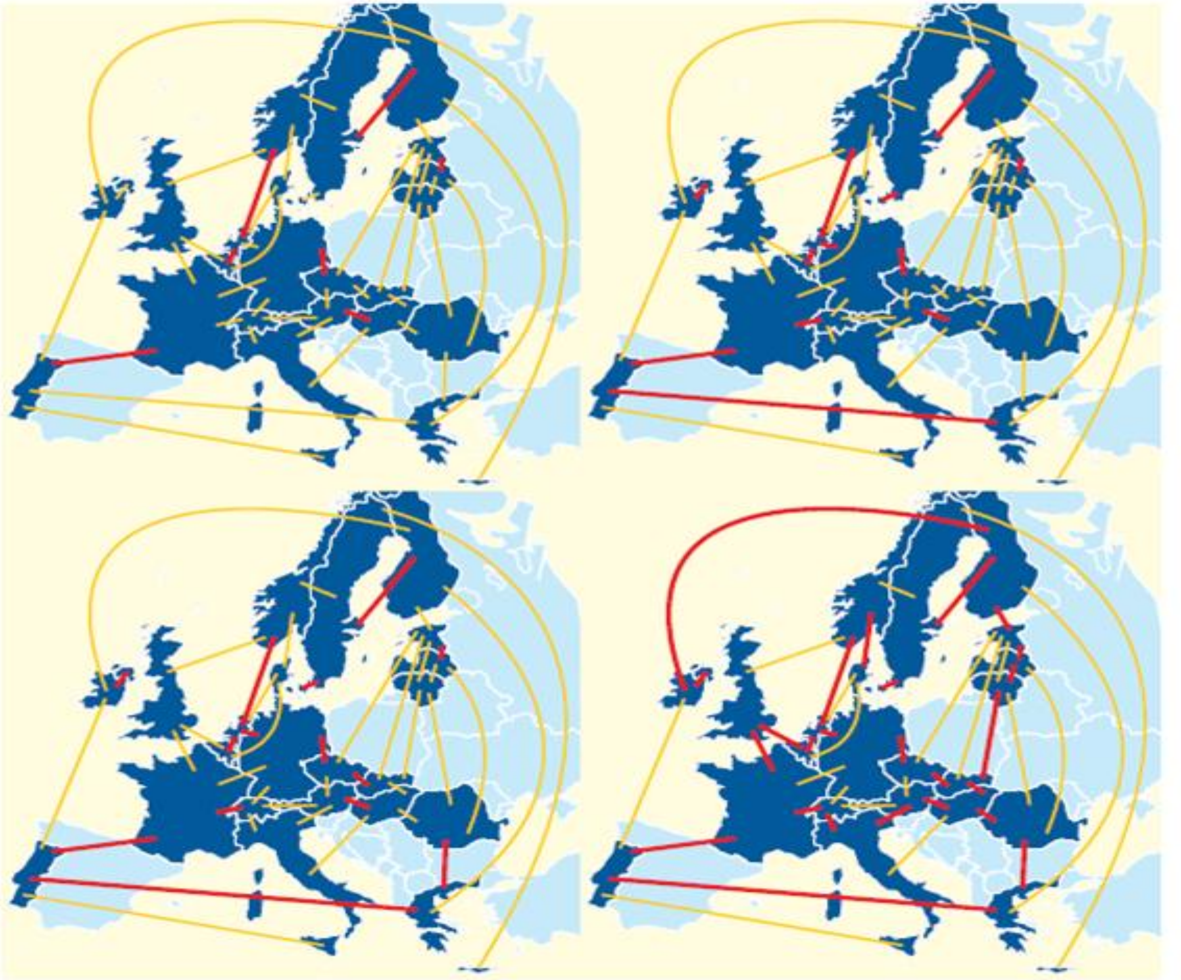
EU Cybersecurity Strategy - § 2.1 Achieving Cyber Resilience

The Commission asks ENISA to:

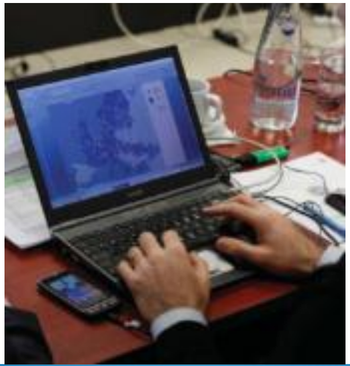
- Assist the Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure
- Continue supporting the Member States and the EU institutions in carrying out regular pan-European cyber incidents exercises which will also constitute the operational basis for the EU participation in international cyber incidents exercises.

Cybersecurity Exercises by ENISA

- Cyber Europe 2010
  - Europe’s first multinational cybersecurity exercise between public sector agencies
- Joint EU-US Cybersecurity Exercise 2011
  - First transatlantic cooperation exercise
  - Table-top exercise - ‘what-if’ scenarios
- Cyber Europe 2012
  - Large scale realistic cyber-crisis exercise
  - Public and private sectors involved
- Cyber Europe 2014
  - In planning phase
- Joint EU-US Cybersecurity Exercise 2014/2015
  - In planning phase



CYBER EUROPE 2010 CYBER EUROPE



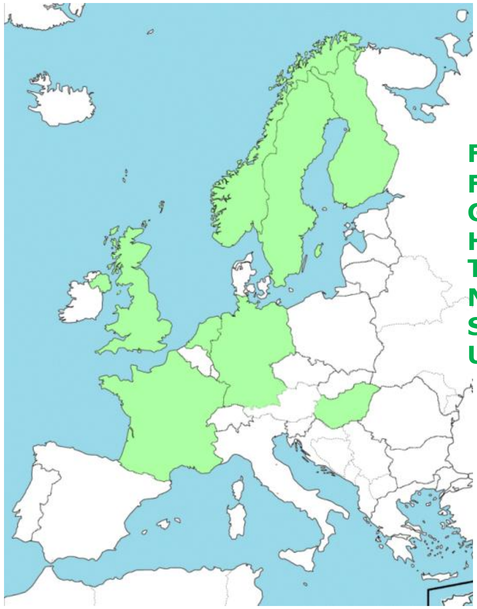
2nd Pan - European Cyber Exercise

Agenda

- Who is ENISA?
- EU Policy context
- Examples of ENISAs work
  - Threat Landscape
  - Cyber Europe Exercises
- **Support for EU CSIRTs**
  - Fight against Cybercrime
  - Baseline capabilities for national CSIRTs
  - Capability building – training
  - ENISA and the CSIRT communities

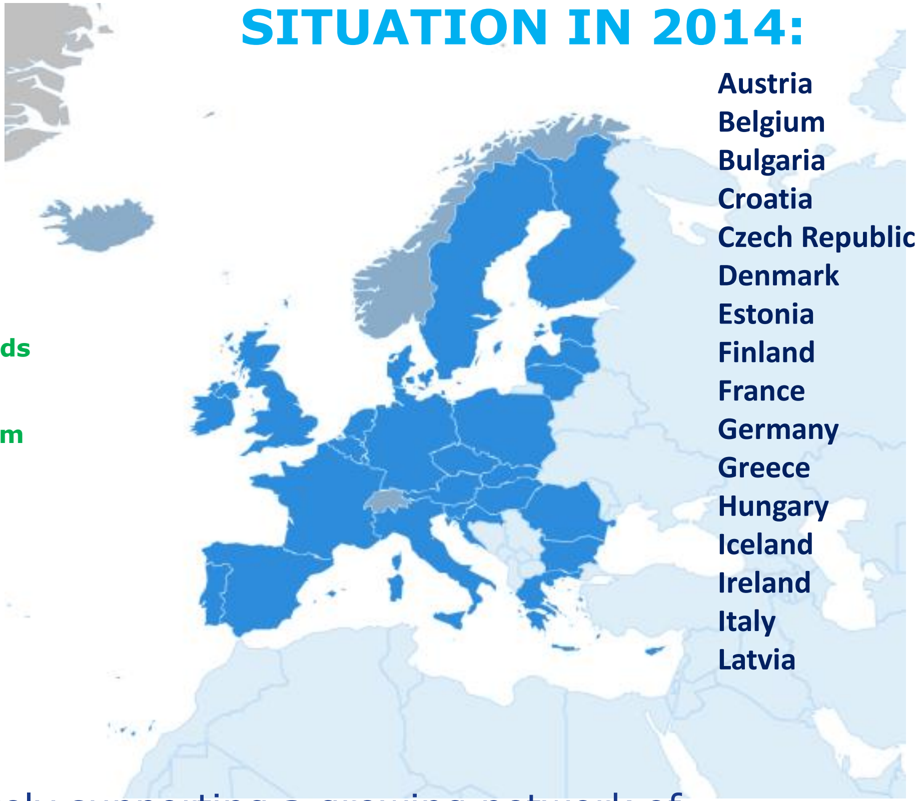
The situation in Europe (Status 02/2014)

ESTABLISHED IN 2005:



Finland
France
Germany
Hungary
The Netherlands
Norway
Sweden
United Kingdom

SITUATION IN 2014:



Austria
Belgium
Bulgaria
Croatia
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Ireland
Italy
Latvia

Lithuania
Luxembourg
Malta
Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
United Kingdom
EU Institutions

- We are building and actively supporting a growing network of national/governmental CERTs
- CERT Interactive MAP: http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map

CERT and other operational communities

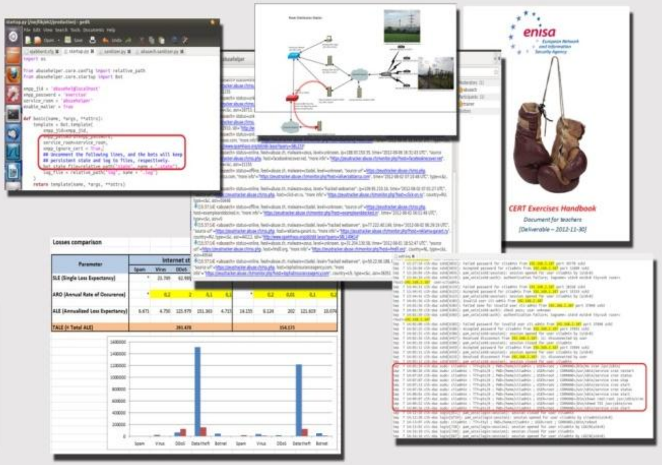
1. Baseline capabilities support
2. Capability building via training and good practice
3. Cooperation in the fight against cybercrime

Supporting the CERT community

ENISA Annual **CERT workshops** focus on national and governmental CERTs preparedness and response capabilities

New Exercise material 2012
- Technical trainings for CERTs
- Handbook for teachers
- Toolset for students
- SW ready to use from our website:

www.enisa.europa.eu/activities/cert/support



FIRST – to improve CERT capabilities

TRANSITS framework: support the basic and advanced training courses for CERTs

Cross-communities Support

INTERPOL Atomic exercise 2012

ENISA-EUROPOL joint workshop: “Addressing NIS aspects of cybercrime”

EU FI-ISAC exercise for CERTs, LEA and banks

CEPOL courses: (operational security unit supports cyber work-shops for police)

https://www.enisa.europa.eu/activities/cert

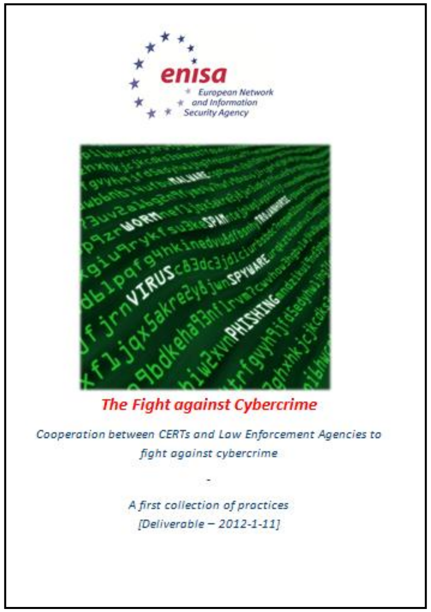
Agenda

- Who is ENISA?
- EU Policy context
- Examples of ENISAs work
  - Threat Landscape
  - Cyber Europe Exercises
- Support for EU CSIRTs
  - **Fight against Cybercrime**
  - Baseline capabilities for national CSIRTs
  - Capability building – training
  - ENISA and the CSIRT communities

Supporting CERTs to collaborate with law enforcement

- Cybercrime is **global** and not a “sectorial” problem
- Calls for cross-border and cross-sector collaboration
- ENISAs role is to foster cooperation
  - Among CERTs
  - CERTs and other stakeholders
- ENISA’s work in this field
  - Support CERT/LEA Cooperation

The Fight against Cybercrime



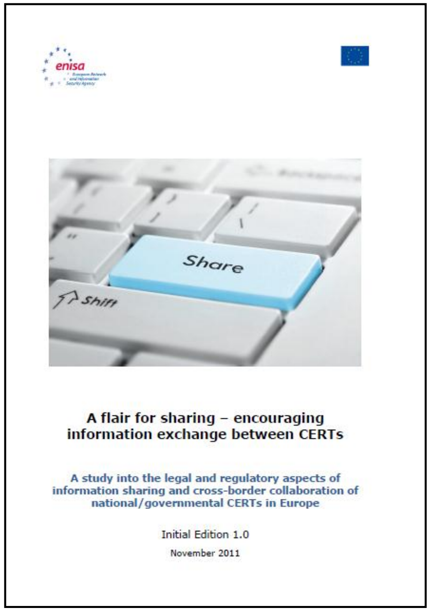
enisa
European Network and Information Security Agency

The Fight against Cybercrime

Cooperation between CERTs and Law Enforcement Agencies to fight against cybercrime

-

A first collection of practices
[Deliverable – 2012-1-11]

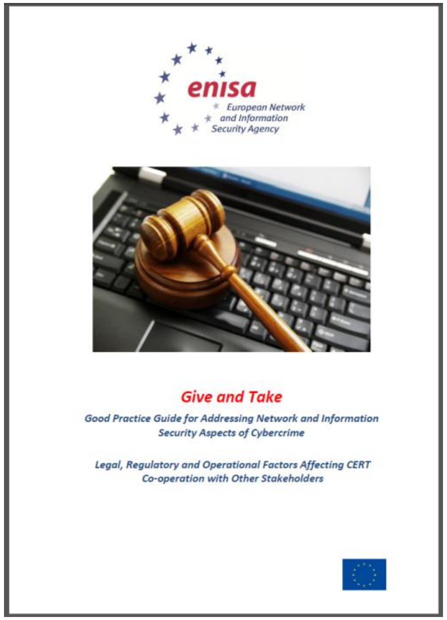


enisa
European Network and Information Security Agency

A flair for sharing – encouraging information exchange between CERTs

A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe

Initial Edition 1.0
November 2011

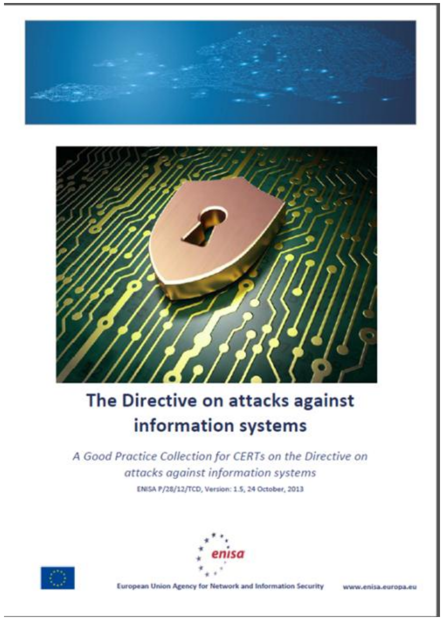


enisa
European Network and Information Security Agency

Give and Take

Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime

Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders



The Directive on attacks against information systems

A Good Practice Collection for CERTs on the Directive on attacks against information systems

ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu

2011 2012 2013

http://www.enisa.europa.eu/activities/cert/support

ENISA-EUROPOL/EC3 joint workshops

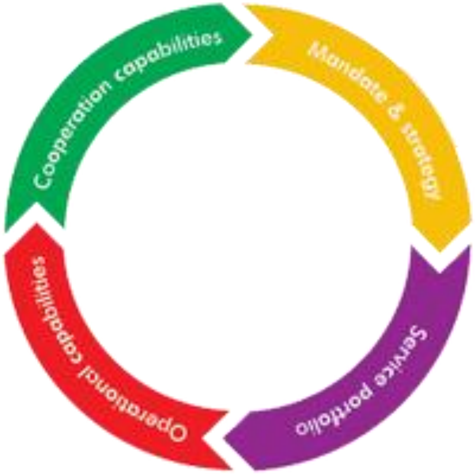
- Closed meeting - by invitation only
- Cybercrime topics
- Organised together with Europol/EC3
- Workshops (so far) include:
  - ENISA training (Identifying and handling cyber-crime traces and cooperation in the area of cybercrime)
  - Round-table discussions
  - Creating opportunities for new contacts between communities
- Organised on annual basis

Agenda

- Who is ENISA?
- EU Policy context
- Examples of ENISAs work
  - Threat Landscape
  - Cyber Europe Exercises
- Support for EU CSIRTs
  - Fight against Cybercrime
  - **Baseline capabilities for national CSIRTs**
  - Capability building – training
  - ENISA and the CSIRT communities

CERT capabilities

1. **Formal capabilities** (mandate; definition of roles and responsibilities, …)



2. **Operational-technical capabilities** (provided services)
3. **Operational-organisational capabilities** (working format; host organisation; business continuity,…)
4. **Co-operational capabilities** (national level, cross-border, regional, different partners)

Baseline capabilities - MANDATE

(Mandate / official framework covers the powers and justification that need to be granted to the team by the respective government)

National cyber security strategy (-> n/g CERT role specified)

- recommended – a CERT needs to act in the right framework

Official mandate by the government in place

- must - to represent the country in the CERT communities

Duties, roles and responsibilities defined

- must - Official national Point of Contact (PoC) for CERTs and other members of the security community
- recommended – clarify "status quo" with regards to the relevant NIS key players in a country and their relationship must be taken into account when the mandate for the n/g CERT is formulated.

CERT of 'last resort' function

- recommended (in case of doubt and emergency, the team is available to relay incident reports (and other security related information) to the right stakeholders in its country.

Suitable organizational model

- recommended to carefully evaluate the role of n/g CERTs in governmental structure to decide which sector, ministry, agency or other structure is the most appropriate place for the CERT in the particular country

Baseline capabilities – SERVICE PORTFOLIO

(Service portfolio covers the services that a team provides to its constituency or is using for its own internal functioning)

Core services

- must do Incident handling, analysis and reporting

Secondary services

- recommended Alerts and Warnings and Announcements for the constituency in a both reactive and proactive way.

Additional services

- recommended - Sharing of security related information on alerts and warnings in immediate cases of upcoming threats or other emergencies.

Internal functioning services

- recommended - Constant situation awareness by technology watch, training and exercises. Further develop service portfolio.

Baseline capabilities – OPERATIONAL

(Operational capabilities covers technical and operational requirements a team must comply with)

Resources

- must 3-5 FTE initially;
- minimum 6-8 FTE for 24/7 reachability

Communication

- minimum telephone, team email address and website with incident reporting option
- must - role and responsibility of a n/g CERT is clearly communicated to all relevant stakeholders, national and in international level.

Reachability

- must 24/7 for own constituency and inter/national cooperation partners for responding to NIS incidents.

Physical security

- must be able to secure sensitive information (needs further clarifications).

Baseline capabilities – COOPERATION

(Cooperation capabilities subsumes the requirements with regards to information sharing with other teams, that are not covered by the previous three categories)

Trust and trust building

- minimum – personal knowledge and reputation of team members.
- recommended Trust criteria (technical expertise with a proven track record, membership in CERT initiatives, ability to respond quickly and act on security threats and a stable team, etc. Needs further clarification!)

National and international cooperation

- minimum – a key role (driver) on the national level;
- must - PoC role for the international cooperation

Informal groups

- recommended membership in fora like FIRST and TI

Common terminology and schemes

- recommended to follow national and international best practices

Agenda

- Who is ENISA?
- EU Policy context
- Examples of ENISAs work
  - Threat Landscape
  - Cyber Europe Exercises
- Support for EU CSIRTs
  - Fight against Cybercrime
  - Baseline capabilities for national CSIRTs
  - **Capability building – training**
  - ENISA and the CSIRT communities

Tier 1: Good Practice Guides for CERTs

A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT

Including examples and a checklist in form of a project plan

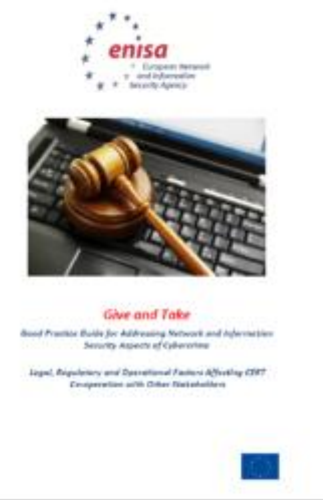
Deliverable WP2006/5.1(CERT-D1/D2)

PART I

A basic collection of good practices for running a CSIRT

Deliverable WP2007/2.4.9/1 (CERT-D3.1)

Good Practice Guide for Incident Management


Give and Take

Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime

Legal, Regulatory and Operational Factors Affecting CERT Cooperation with Other Stakeholders

https://www.enisa.europa.eu/activities/cert/support

Alerts, Warnings and Announcements

Best Practices Guide

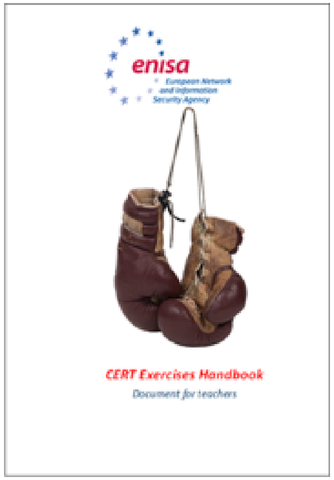
Good practice guide for CERTs in the area of Industrial Control Systems

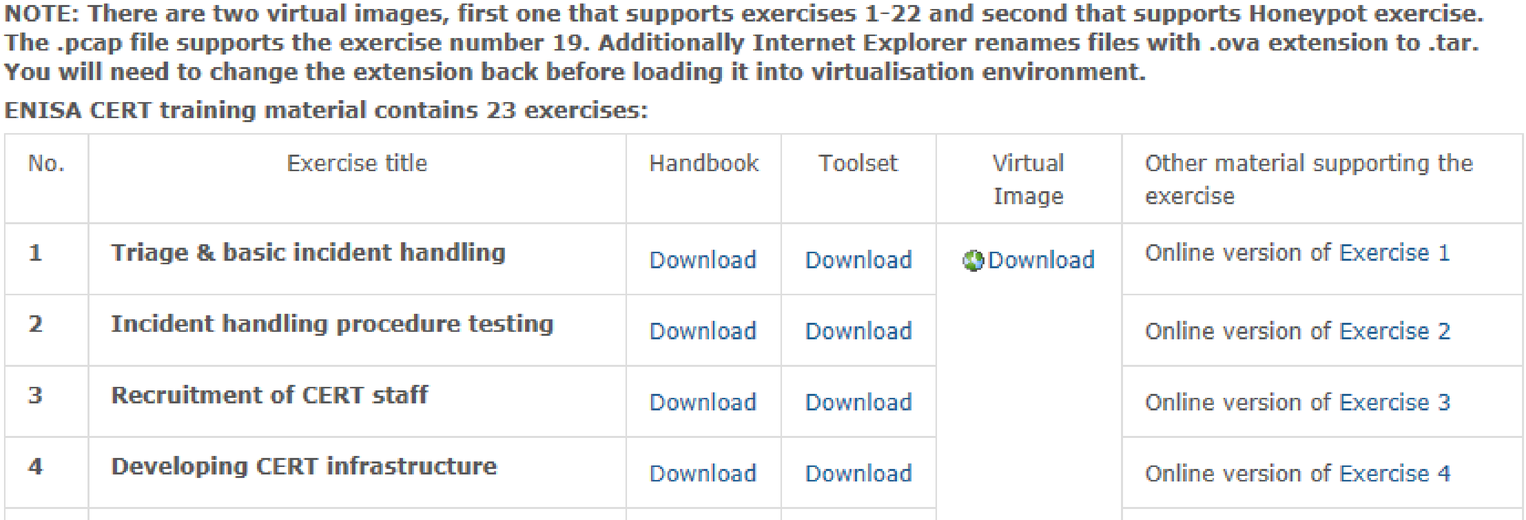
Computer Emergency Response Capabilities considerations for ICS

The Directive on attacks against information systems

A Good Practice Collection for CERTs on the Directive on attacks against information systems

Tier 2: Training material available





NOTE: There are two virtual images, first one that supports exercises 1-22 and second that supports Honeypot exercise. The .pcap file supports the exercise number 19. Additionally Internet Explorer renames files with .ova extension to .tar. You will need to change the extension back before loading it into virtualisation environment.

ENISA CERT training material contains 23 exercises:

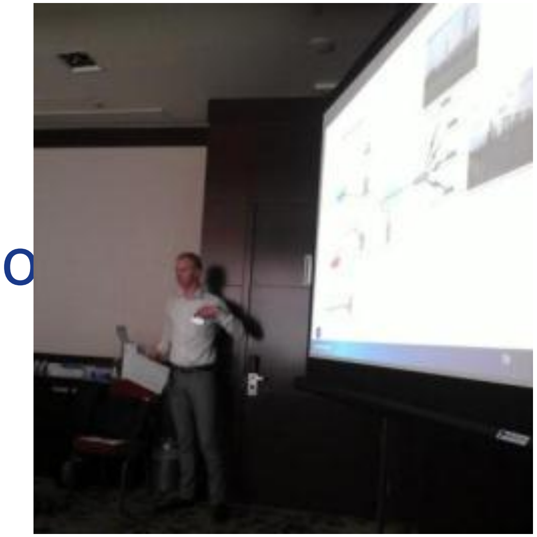
No.	Exercise title	Handbook	Toolset	Virtual Image	Other material supporting the exercise
1	**Triage & basic incident handling**	Download	Download	Download	Online version of Exercise 1
2	**Incident handling procedure testing**	Download	Download		Online version of Exercise 2
3	**Recruitment of CERT staff**	Download	Download		Online version of Exercise 3
4	**Developing CERT infrastructure**	Download	Download		Online version of Exercise 4

https://www.enisa.europa.eu/activities/cert/support/exercise

Tier 3: Training for national / governmental CERTs

- ENISA starts to rollout its own training!
- First: May 2013 in Bucharest, Romania
- 3 scenarios presented by ENISA trainers
  - Honeypots
  - Incident handling during an attack on Critical Information Infrastructure
  - Mobile threats incident handling

- Since then: more than 15 events o
  request by the EU MS



Tier 3: Training for national / governmental CERTs

- Trainers come on-site!
- Each training is tailored to fulfil the needs of this specific event and audience!
- Other trainings (TRANSITS) can be organised!
- Hands on class with virtual images
- More info: cert-relations@enisa.europa.eu

Agenda

- Who is ENISA?
- EU Policy context
- Examples of ENISAs work
  - Threat Landscape
  - Cyber Europe Exercises
- Support for EU CSIRTs
  - Fight against Cybercrime
  - Baseline capabilities for national CSIRTs
  - Capability building – training
  - **ENISA and the CSIRT communities**

Content regularly updated and renewed with the help of community

- The creation process of material involves community
- The target audiences feedback will lead to better material

Community Support

- European CERT Community
  - Meetings 3x a year
  - Teams Accreditation & Certification
  - http://www.terena.org/activities/tf-csirt

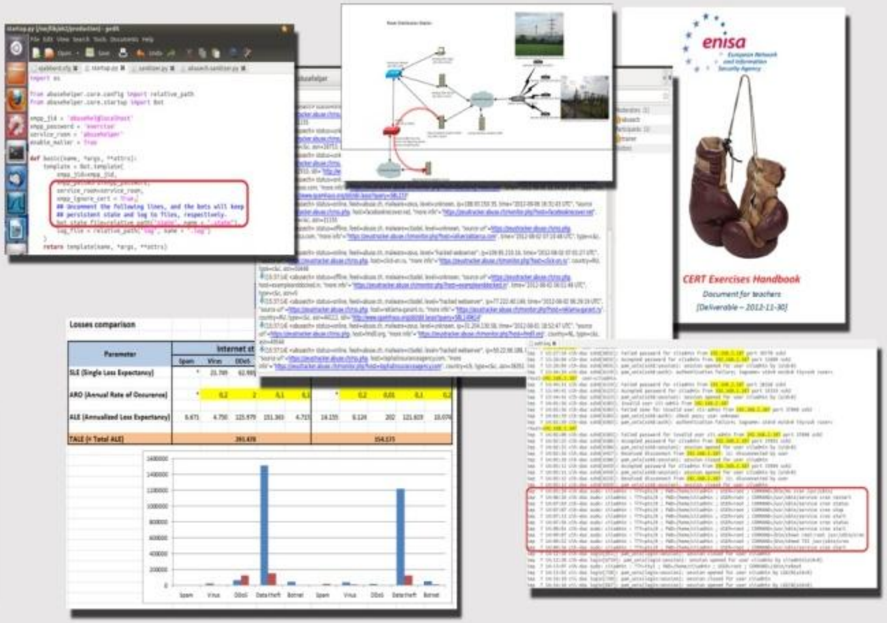
- Worldwide CERT Community
  - Yearly Conference
  - Regular Technical Colloquia
  - http://www.first.org/

- Fundamental training
  - Organisation, Operations, Legal, Communication
  - http://www.terena.org/activities/transits

Supporting the CERT community

ENISA Annual **CERT workshops**
focus on national and governmental CERTs preparedness and response capabilities

New Exercise material 2012
- Technical trainings for CERTs
- Handbook for teachers
- Toolset for students
- SW ready to use from our website:
www.enisa.europa.eu/activities/cert/support


enisa
European Network and Information Security Agency
CERT Exercises Handbook
Document for teachers
[Deliverable – 2012-11-30]
Losses comparison
Parameter
SLE (Single Loss Expectancy)
ARO (Annual Rate of Occurrence)
ALE (Annualized Loss Expectancy)
TALE (= Total ALE)

FIRST – to improve CERT capabilities

FIRST Improving Security Together · TF-CSIRT FIRST SIG · CSIRT Metrics FIRST SIG

TRANSITS framework:
support the basic and advanced training courses for CERTs

TRANSITS

Cross-communities Support

INTERPOL
Atomic exercise 2012

INTERPOL

ENISA-EUROPOL joint workshop:
"Addressing NIS aspects of cybercrime"

EUROPOL

EU FI-ISAC exercise for CERTs, LEA and banks

CEPOL European Police College

CEPOL courses:
(operational security unit supports cyber work-shops for police)

https://www.enisa.europa.eu/activities/cert

Contact details

European Union Agency for Network and Information Security (ENISA)

http://www.enisa.europa.eu

Follow us on