



Supporting the CERT community

Lauri Palkmets





About ENISA



- The European Union Agency for Network and Information Security
 - gives advice on information security issues
 - to national authorities, EU institutions, citizens, businesses
 - acts as a forum for sharing good NIS practices
 - facilitates information exchange and collaboration
- ENISA focuses on prevention and preparedness
- Set up in 2004 – mandate has been extended
- Around 65 staff
- Offices in Heraklion and Athens





Supporting the CERT community

- Cooperation in the fight of cybercrime
- Baseline capabilities
- Capability building via training and good practice

Supporting the CERT community

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

FIRST – to improve CERT 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

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

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

Cross-communities Support

INTERPOL
Atomic exercise 2012

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

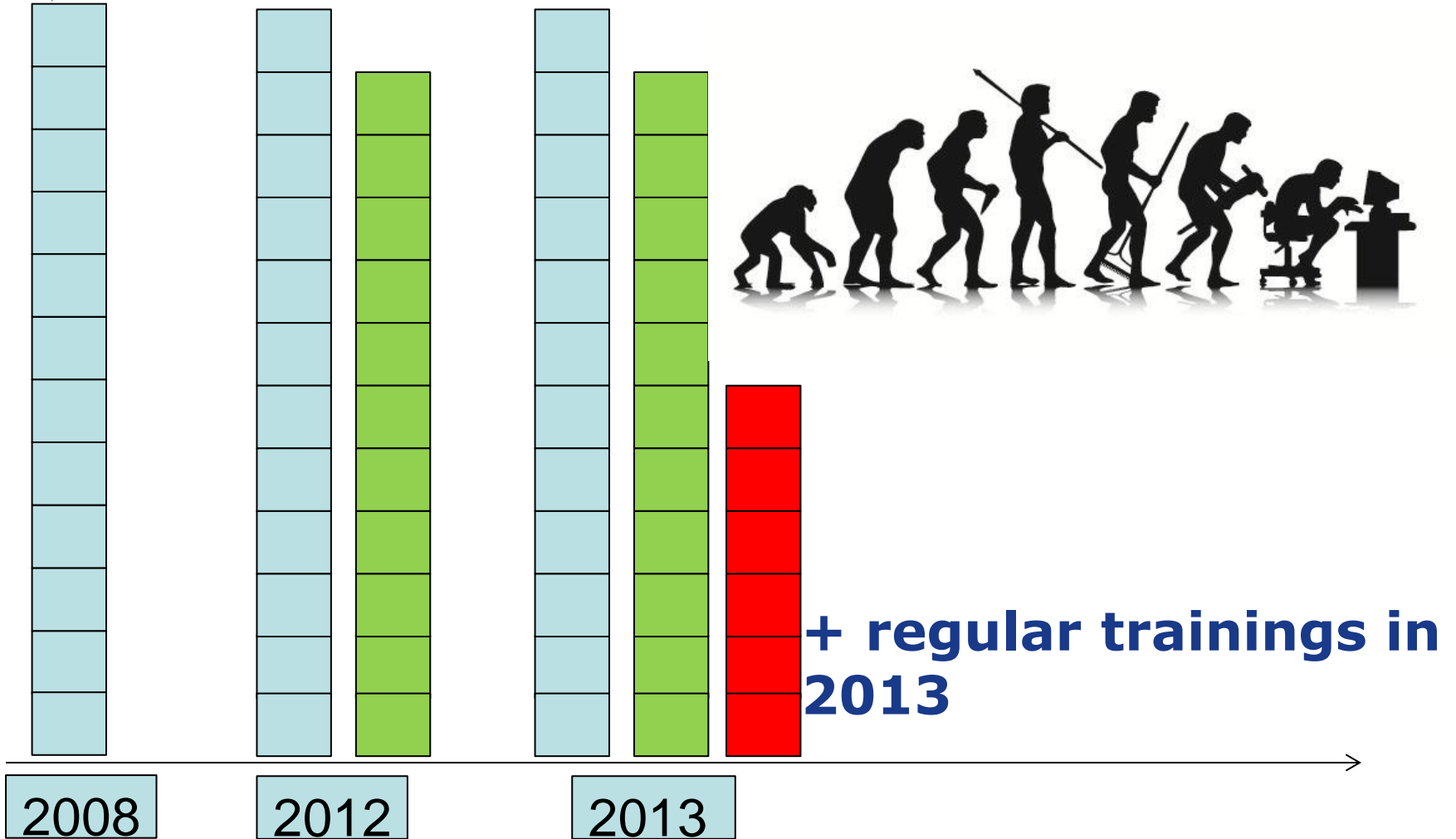
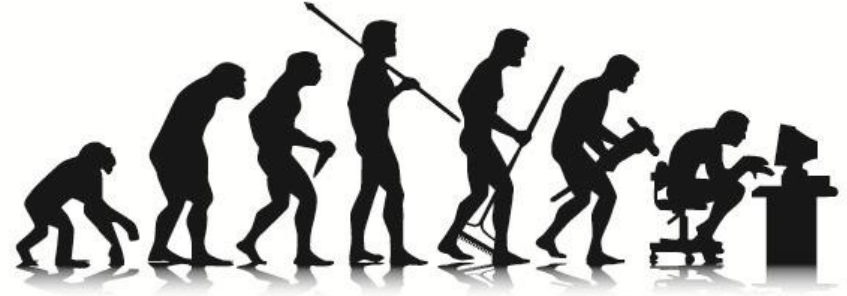
EU FI-ISAC exercise
for CERTs, LEA and banks

CEPOL courses:
(operational security unit supports cyber workshops for police)





ENISA CERT training





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




Material available on website



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>

14. Exercise: Proactive incident detection

Main Objective	Setting up and working with AbuseHelper
Targeted Audience	Technical and management CERT staff

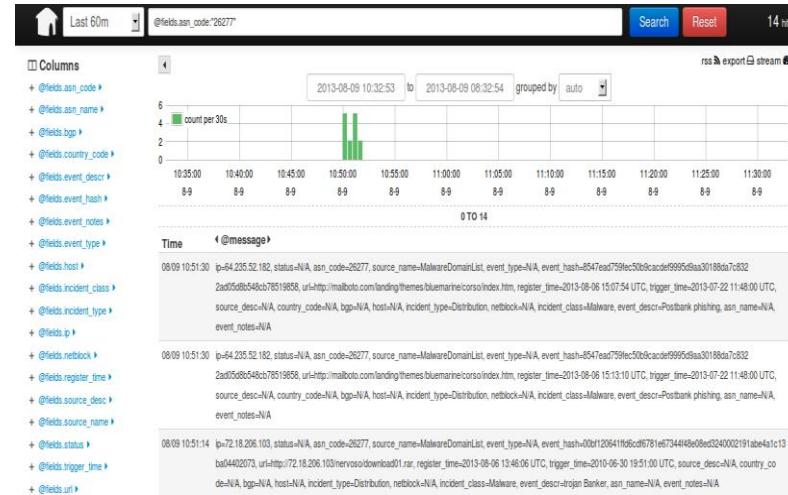
+ Visualising the feeds



Proactive Detection of Network Security Incidents



Proactive Detection of Security Incidents
Honeypots
2012-11-20



2011

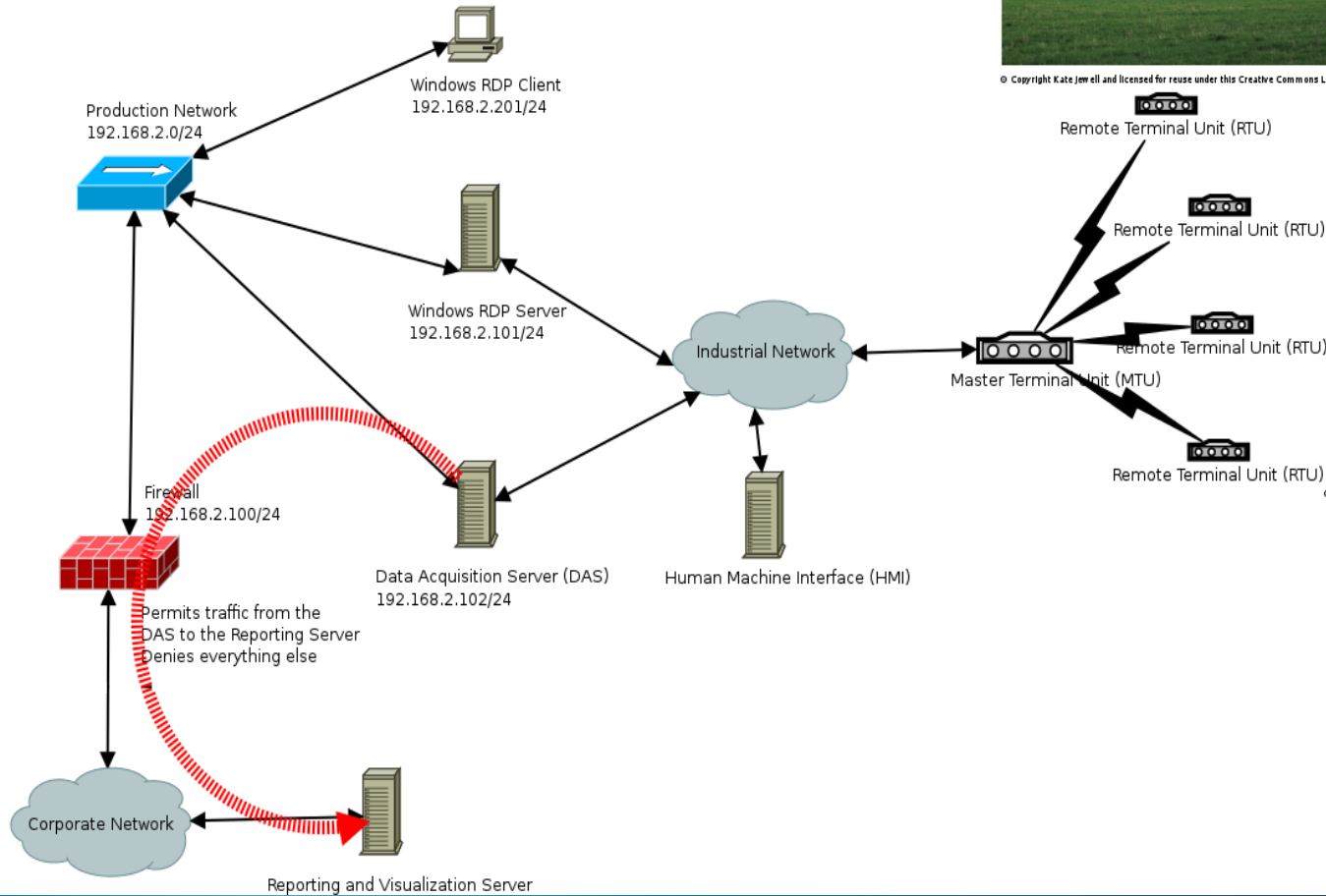
2012

2013

- For a different levels of experience and expertise
 - Legal
 - Operational
 - Technical
 - Cooperation



Power Distribution Station



© Copyright Kate Jewell and licensed for reuse under this Creative Commons Licence.



© Copyright John Allan and licensed for reuse under this Creative Commons Licence.





```
trainee@exercise: ~  
trainee@exercise:~$ echo sms send +123456789 'TAN 123321' | nc localhost 5554  
Android Console: type 'help' for a list of commands  
OK  
OK  
trainee@exercise:~$
```

5554:ENISA-EXERCISE

9:43

Downloaded All On SD card Running

- Settings** 10MB
1 process and 0 services
- Trusteer Rapport** 3.9MB
1 process and 1 service 08:01
- Google Services** 8.3MB
1 process and 1 service 14:10
- Android keyboard** 5.2MB
1 process and 1 service 14:12

Navigation icons: Camera, Volume, Power, Call, Home, MENU, Back, Search

1	2@	3#	4\$	5%	6^	7&	8*	9(0)
Q	W	E	R	T	Y	U	I	O	P=
A	S	D	F	G	H	J	K	L	DEL
Home	Z	X	C	V	B	N	M	.	Back
ALT	SYM	@						/ ?	ALT



What is the file from the Remote file inclusion?

*(See in
/opt/glaspot/trunk/files/)*

50:50



**A: a SIP OPTIONS scanner
in PHP**

B: a malicious PDF

C: a PHP shell

D: a PHP photo album

New material presented in 2013

#	Title	Number of experts
1	Digital forensics	12
2	Identification and handling of electronic evidence	13
3	Identifying and handling cyber-crime traces	12
4	Incident handling and cooperation during phishing campaign	9
5	Visualizing cyber-crime traces	6
6	Cooperation in the area of cyber-crime	7



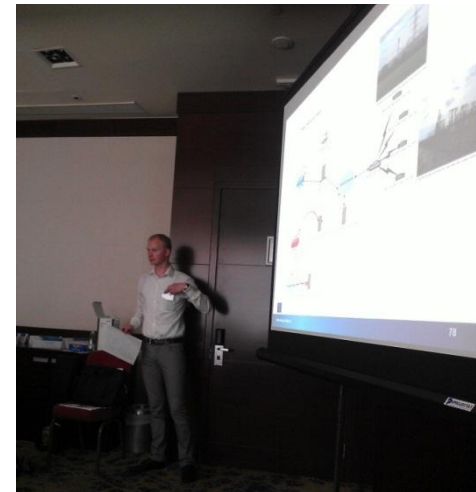
ENISA 8th annual workshop 'CERTs in Europe' - Part I





ENISA 8th annual workshop 'CERTs in Europe' - Part I

- 21 & 22 May 2013 in Bucharest, Romania
- 3 scenarios from ENISA CERT training/exercise material presented by ENISA trainers
 - Honeypots
 - Incident handling during an attack on Critical Information Infrastructure
 - Mobile threats incident handling
- Participants rated ENISA training with **4,4** out of **5** points



ENISA 8th annual workshop 'CERTs in Europe' - Part II

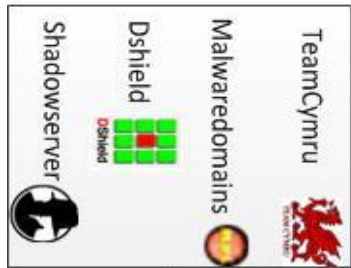
- 2 scenarios from ENISA CERT training/exercise material presented by ENISA trainers
 - Presenting, correlating and filtering various feeds
 - Identifying and handling of electronic evidence





Putting the pieces together

Security Data-Feeds



XMPP (XML based standard)
<?xml version="1.0"?> <stream:stream to="example.com" xmlns="jabber:client" xmlns:stream="http://etherx.jabber.org/streams" version="1.0">

AH Bots
Via
XMPP



AbuseHelper

XMPP



Jabber client

XMPP

AbuseHelper
Python Splunk extension
Tomas Lima CERT.PT

xmpp2syslog

Syslog



Logstash

log collection, parsing, storage



Search/Filter

RabbitMQ
Index/search



Open source search engine

Syslog example:

[Date][Timestamp][IP][daemon][Message]

Sep 5 06:50:58 ip-10-252-71-73 syslog-ng[694]: Configuration reload request received, reloading configuration;

Sep 5 06:50:58 ip-10-252-71-73 syslog-ng[694]: EOF on control channel, closing connection;

Sep 5 06:50:58 ip-10-252-71-73 CRON[28578]: (CRON) info (No MTA installed, discarding output)



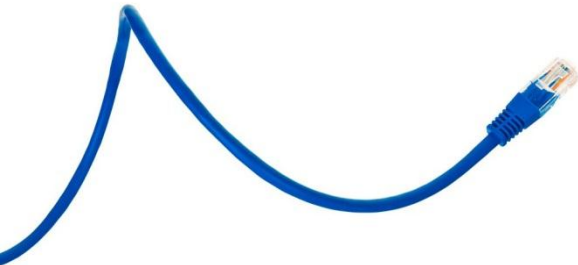

```
enisa@enisa-VirtualBox: ~/enisa/forensic/data
enisa@enisa-VirtualBox:~/enisa/forensic/data$ zdecrypt.py config.bin key.bin
Total size: 364
Storage flags: 0
Items count: 5
Config MD5: aa12e1ba17b2b1a31ac716ecfcd4fa1b (VERIFIED)
-----
CFGID_LAST_VERSION:
- flags: ITEMF_IS_OPTION
- size (real): 4 (4)
- value: '0x2000809'
-----
CFGID_LAST_VERSION_URL:
- flags: ITEMF_IS_OPTION
- size (real): 31 (31)
- value: 'http://alazqwryx.cn/z12/bot.exe'
-----
CFGID_URL_SERVER_0:
- flags: ITEMF_IS_OPTION
- size (real): 32 (32)
- value: 'http://alazqwryx.cn/z12/gate.php'
-----
CFGID_HTTP_FILTER
- flags: ITEMF_COMPRESSED|ITEMF_IS_OPTION
- size (real): 133 (161)
- value: '\xdb\xff\xff\xff!*.microsoft.com/*\x00!http://\tm\xd6}\xed\xfdyspace\x16\x15\x14s\x15w\x00\xb0\xbf\xbd\xfd.gru
p1ant\x02der.es5\xc0\xda\xff?odnoklassniki.)\x1b\xfb?\xbb{vko3kte\x16@*/login.K0`0vmp\x12atl\x10\x00\x00\x00\x00\x00
\x00H\x00\xff'
-----
CFGID_HTTP_POSTDATA_FILTER:
- flags: ITEMF_IS_OPTION
- size (real): 36 (36)
- value: 'http://bank.pl/*\x00username;password\x00\x00'
-----
enisa@enisa-VirtualBox:~/enisa/forensic/data$
```

Recommendations

- Online training material, and handing out material for self-study is good, but...
- Talking with each other actually is useful
- People, who have created or worked together, tend to cooperate in the future
- Every training is a performance and every trainer is an actor

Methodology of ENISA training

- Trainers can come on-site
- Each training is tailored to fulfil the needs of this specific event and audience



National/governmental CERTs the situation has changed...

ESTABLISHED IN 2005:



Finland
France
Germany
Hungary
The Netherlands
Norway
Sweden
United Kingdom

ESTABLISHED IN 2013:



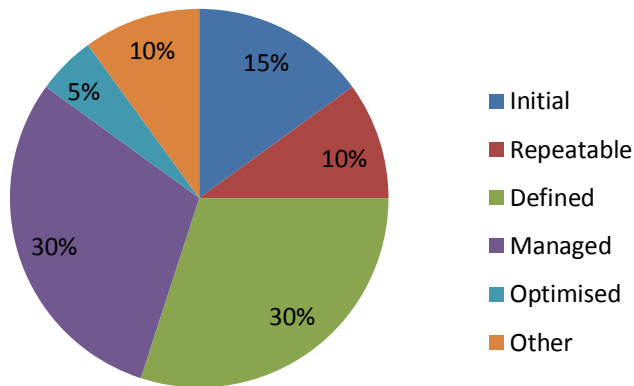
Armenia
Austria
Belgium
Bulgaria
Croatia
Czech Republic
Denmark
Estonia
Finland
France
Georgia
Germany
Greece
Hungary
Iceland
Ireland
Israel
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom
EU Institutions

- 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 maturity

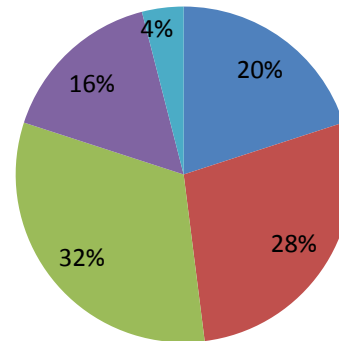
Total: 45 responses to the questionnaire (25 from n/g CERTs; 20 from other CERTs and other stakeholders)

Self-Assessment of the Maturity Status of National / Governmental CERTs



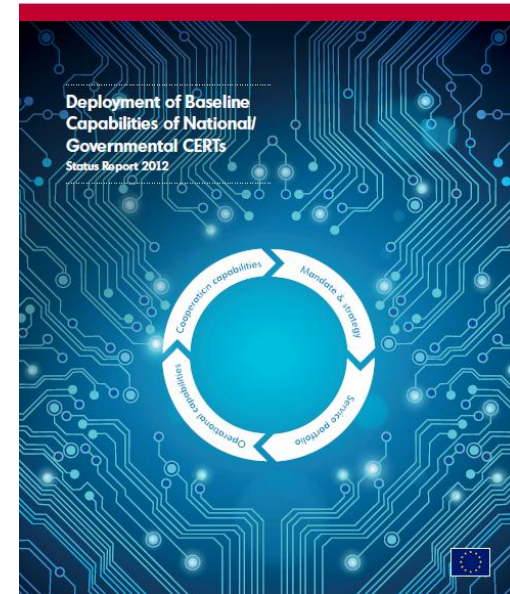
Years of Operation of National / Governmental CERT

■ Up to one year
 ■ 1-2 years
 ■ 3-5 years
■ 6-8 years
 ■ Over 8 years



Interviewed teams assessed themselves as either governmental or national/governmental CERTs indicated the years of operations between: 4 months and 11 years.

(France, Germany, Norway, Hungary, Denmark, Sweden, Spain, Ireland, Latvia, Czech Republic, Slovakia, Romania, CERT-EU)





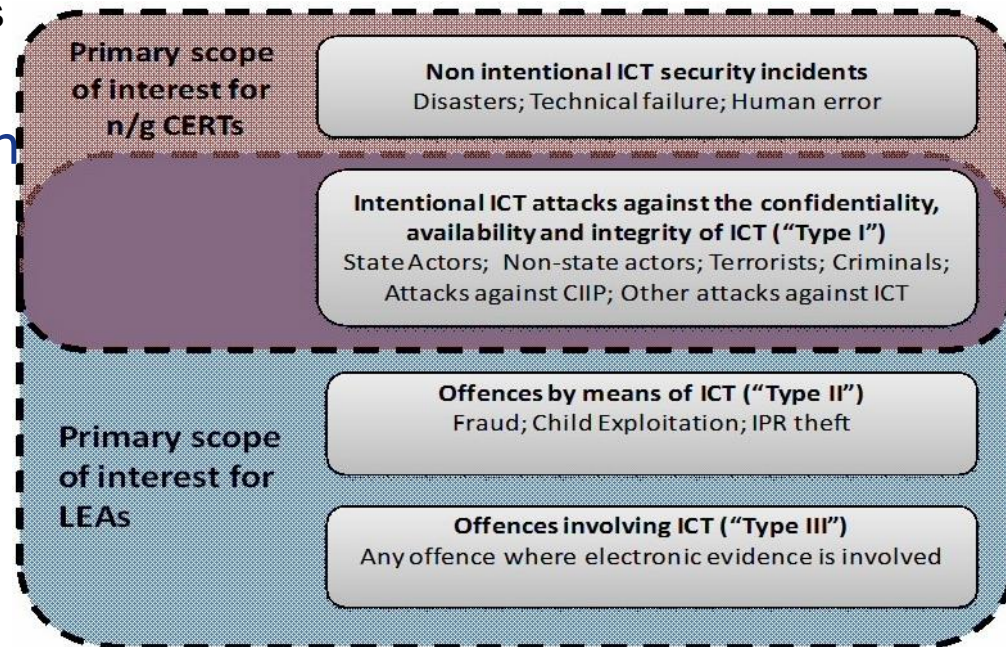
Fight against cybercrime – support for CERT / LEA cooperation

- Main goals:
 - Define key concepts
 - Describe the technical and legal/regulatory aspects of the fight against cybercrime
 - Compile an inventory of operational, legal/regulatory and procedural barriers and challenges and possible ways to overcome these challenges
 - Collect existing good and best practices
 - Develop recommendations

- Focus on CERT-LEA cooperation

- Differences:

- Definitions cybercrimes/attacks
- Meanings of sharing
- Character of the organizations
- Objectives
- Types of information
- Directions of requests





Thank you for your attention!





Contact details

European Union Agency for Network and Information
Security

Science and Technology Park of Crete

P.O. Box 1309

71001 Heraklion

Crete

Greece

<http://www.enisa.europa.eu>

