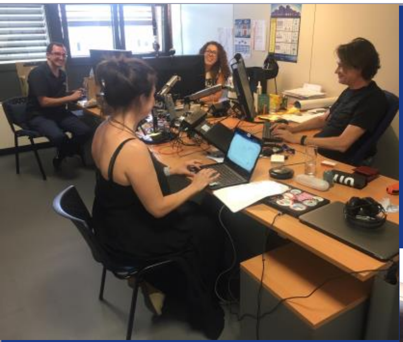
Event: ITU Cyber Drill – ALERT for Europe Region
Date: 28th November 2018
Place: Limassol, Cyprus



Building and advancing incident response in Europe

Andrea DUFKOVA
ENISA, CSIRT – Relations

European Union Agency for Network and Information Security

TLP: GREEN

Securing Europe's Information society

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

Approach

Expertise-Policy-Capacity-Community

- Cloud and Big Data
- Critical Infrastructures and Services
- CSIRT Services
- CSIRTs and communities
- CSIRTs in Europe
- Cyber Crisis Management
- Cyber Exercises
- Cyber Security Education
- Data Protection
- Incident Reporting
- IoT and Smart Infrastructures
- National Cyber Security Strategies
- Standards and certification
- Threat and Risk Management
- Trainings for Cyber Security Specialists
- Trust Services

https://www.enisa.europa.eu/topics

Capacity & Community

https://cybersecuritymonth.eu/

https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists

https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

https://www.europeancybersecuritychallenge.eu/

https://www.enisa.europa.eu/topics/cyber-exercises/

ENISA CSIRT Relations team portfolio in a nutshell

CSIRT Relations

Active support and Secretariat

Leading tool development and maturity assessment

Enabling opsec tools

CSIRTs self Assessment tool

MeliCERTes

CSIRTs NETWORK

Powered by ENISA

CSIRTs in Europe

CSIRTs map

Reference Taxonomy WG

CSIRTs Community projects and services

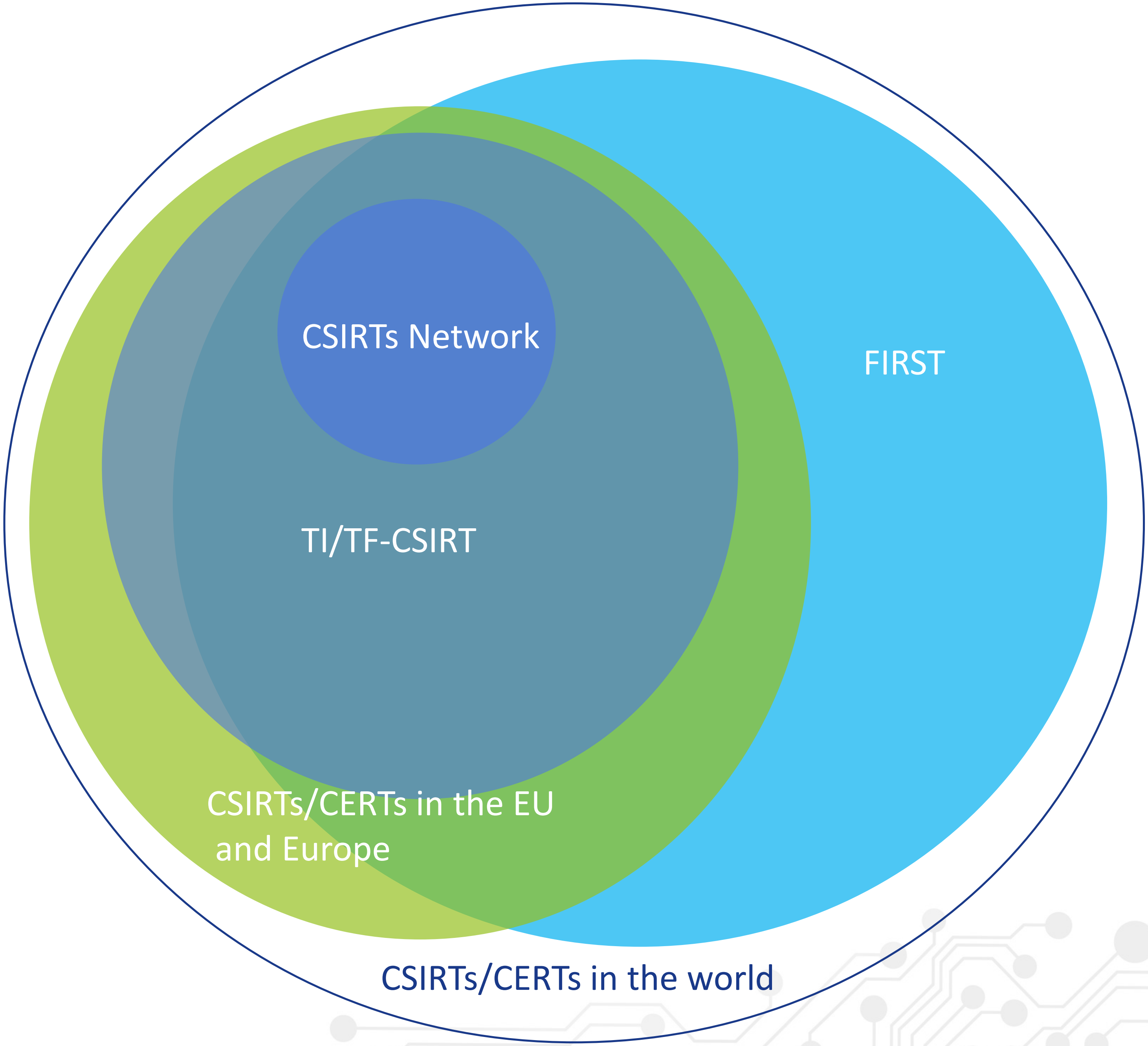
CYBER SECURITY enisa TRAINING

Onsite

VMs, tutorials

Train the trainers

Sectorial


CSIRTs Network
FIRST
TI/TF-CSIRT
CSIRTs/CERTs in the EU and Europe
CSIRTs/CERTs in the world

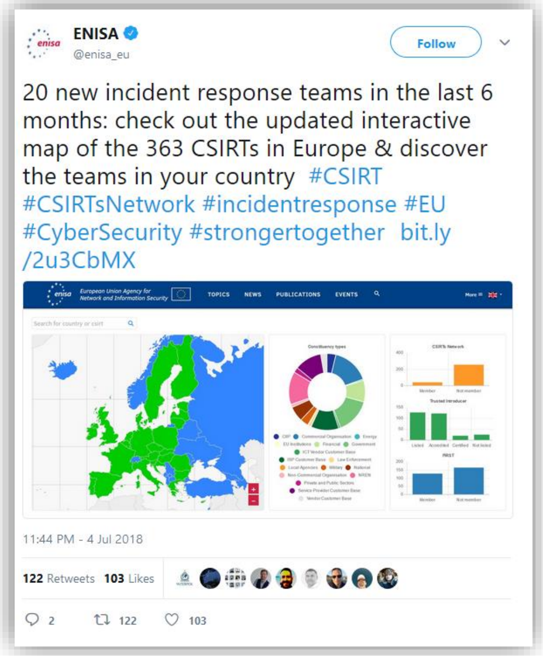
How to identify CSIRT that you need to contact?

✓ 363 ENISA Inventory listed teams

✓ Out of it:

- ✓ teams in CSIRTs Network: 37
- ✓ Trusted Introducer listed: 165
- ✓ Trusted Introducer accredited: 143
- ✓ Trusted Introducer certified: 24

  6 out of 24 are members of the CSIRTs Network
- ✓ FIRST members:~450/~200



ENISA
@enisa_eu

Follow

20 new incident response teams in the last 6 months: check out the updated interactive map of the 363 CSIRTs in Europe & discover the teams in your country #CSIRT #CSIRTsNetwork #incidentresponse #EU #CyberSecurity #strongertogether bit.ly/2u3CbMX

11:44 PM - 4 Jul 2018

122 Retweets 103 Likes

2 122 103

http://enisa.europa.eu/csirts-map

How does it work on EU level for national CSIRTs?

CSIRTs Network – new CSIRT structure in Europe since 2016

- Established by the NIS Directive "in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation".
  - representatives of the Member States’ CSIRTs and CERT-EU can
    - cooperate
    - exchange information
    - build trust
    - improve the handling of cross-border incidents
    - discuss how to respond in a coordinated manner to specific incidents.
- ENISA provides the secretariat and actively supports the cooperation among members:
  - organizes meetings of the CSIRTs Network
  - provide com. infrastructure
  - provides its expertise and advice both to the EC and MS

http://www.csirtsnetwork.eu/

Building and advancing incident response in Europe

How ‘good’ is your CSIRT?

CSIRT capabilities development

Baselining, Evaluation, Improvement

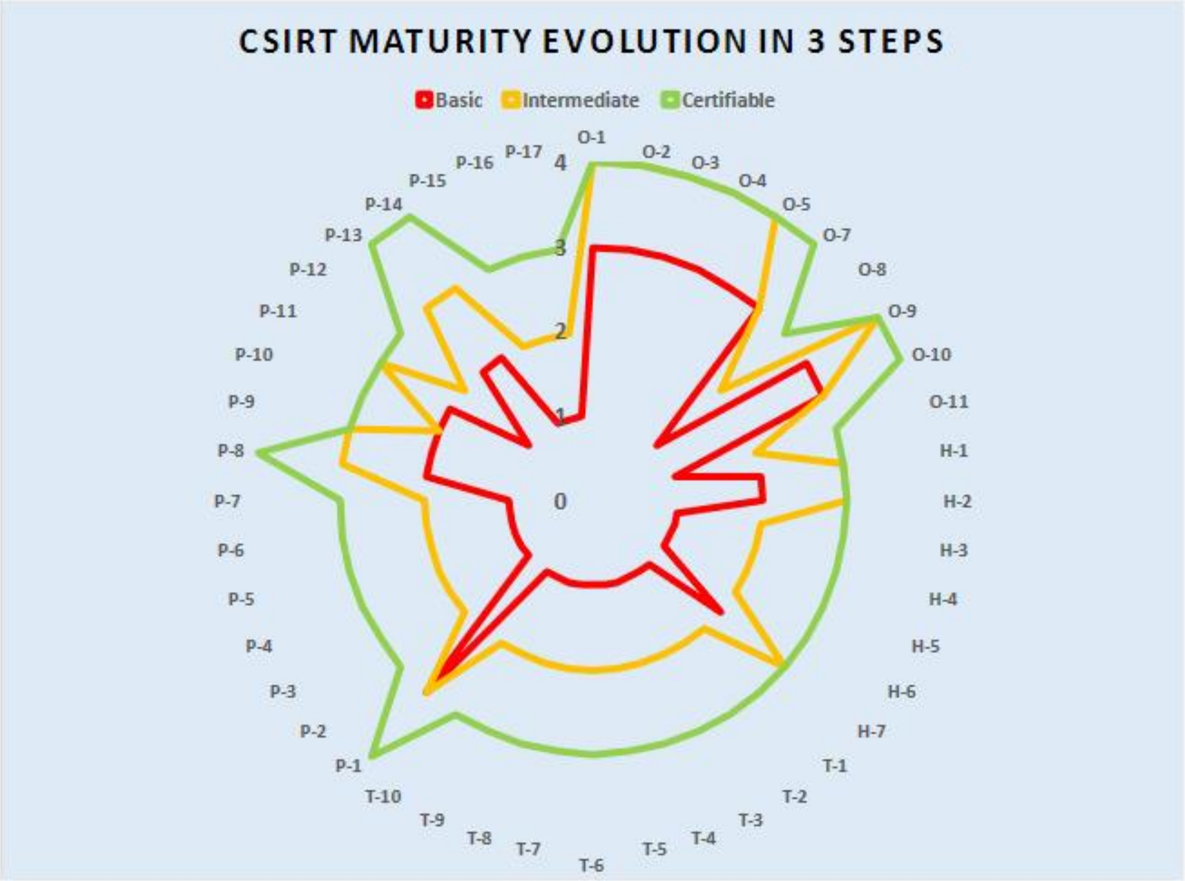
- ENISA drives this effort continuously since 2009
  - Goal: common baseline practices across EU to improve operational cooperation and information exchange
  - Primary audience national and governmental CSIRTs, CSIRTs Network teams, and their leadership

- CSIRT Maturity - What it is about?
  - Teams can assess their team’s maturity instantly
  - 44 questions based on SIM3 model define results

This tool helps CSIRTs to self-assess their team’s maturity in terms of the SIM3 model:

https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CSIRTs Maturity assessment framework



Online self assessment tool :

1. Basic (red)
2. Intermediate (yellow)
3. Certifiable (green)
4. Your own self-assessment (blue)

https://www.enisa.europa.eu/csirts-maturity-sas

How to improve your CSIRT skills and expertise?

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

https://www.enisa.europa.eu/trainings

Detection of Network Security Incidents

Guidelines for implementing

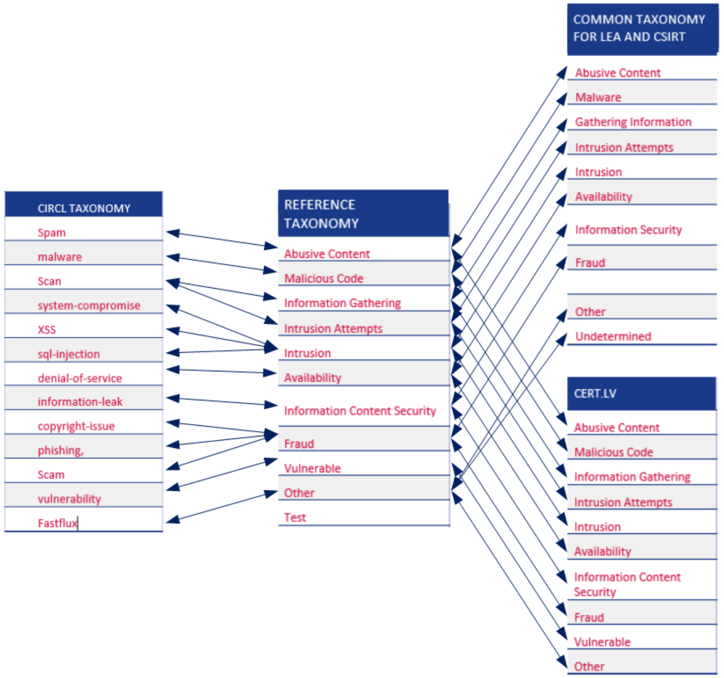
- Data feeds
- Honeypots
- Incident exchange formats
- Threat intelligence

Trainings

- Proactive incident detection: *handbook and VM*
- Automation in incident handling: *handbook and VM*
- Honeypots: *handbook and VM*
- Presenting, correlating and filtering various feeds: *handbook and 2 VMs*

https://www.enisa.europa.eu/csirt-services

How to use the ‘same language/terminology’ across Europe?



CIRCL TAXONOMY

- Spam
- malware
- Scan
- system-compromise
- XSS
- sql-injection
- denial-of-service
- information-leak
- copyright-issue
- phishing,
- Scam
- vulnerability
- Fastflux

REFERENCE TAXONOMY

- Abusive Content
- Malicious Code
- Information Gathering
- Intrusion Attempts
- Intrusion
- Availability
- Information Content Security
- Fraud
- Vulnerable
- Other
- Test

COMMON TAXONOMY FOR LEA AND CSIRT

- Abusive Content
- Malware
- Gathering Information
- Intrusion Attempts
- Intrusion
- Availability
- Information Security
- Fraud
- Other
- Undetermined

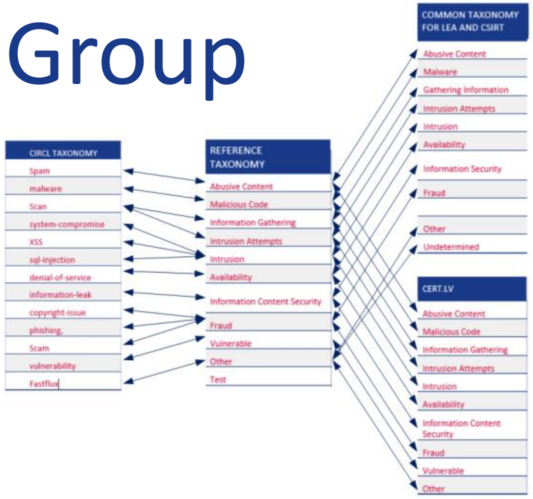
CERT.LV

- Abusive Content
- Malicious Code
- Information Gathering
- Intrusion Attempts
- Intrusion
- Availability
- Information Content Security
- Fraud
- Vulnerable
- Other

Everybody is talking about incidents

- Incident handling
- Incident reporting
- Cross border incidents
- Statistics
- Performance and internal KPI
- Comparison with other entities
- Trends
- Global / annual overview
- Explanation of external report
- Media outreach
- Policy discussion

Reference Security Incident Taxonomy Working Group



CIRCL TAXONOMY

Spam
malware
Scan
system-compromise
XSS
sql-injection
denial-of-service
information-leak
copyright-issue
phishing,
Scam
vulnerability
Fastflux

REFERENCE TAXONOMY

Abusive Content
Malicious Code
Information Gathering
Intrusion Attempts
Intrusion
Availability
Information Content Security
Fraud
Vulnerable
Other
Test

COMMON TAXONOMY FOR LEA AND CSIRT

Abusive Content
Malware
Gathering Information
Intrusion Attempts
Intrusion
Availability
Information Security
Fraud
Other
Undetermined

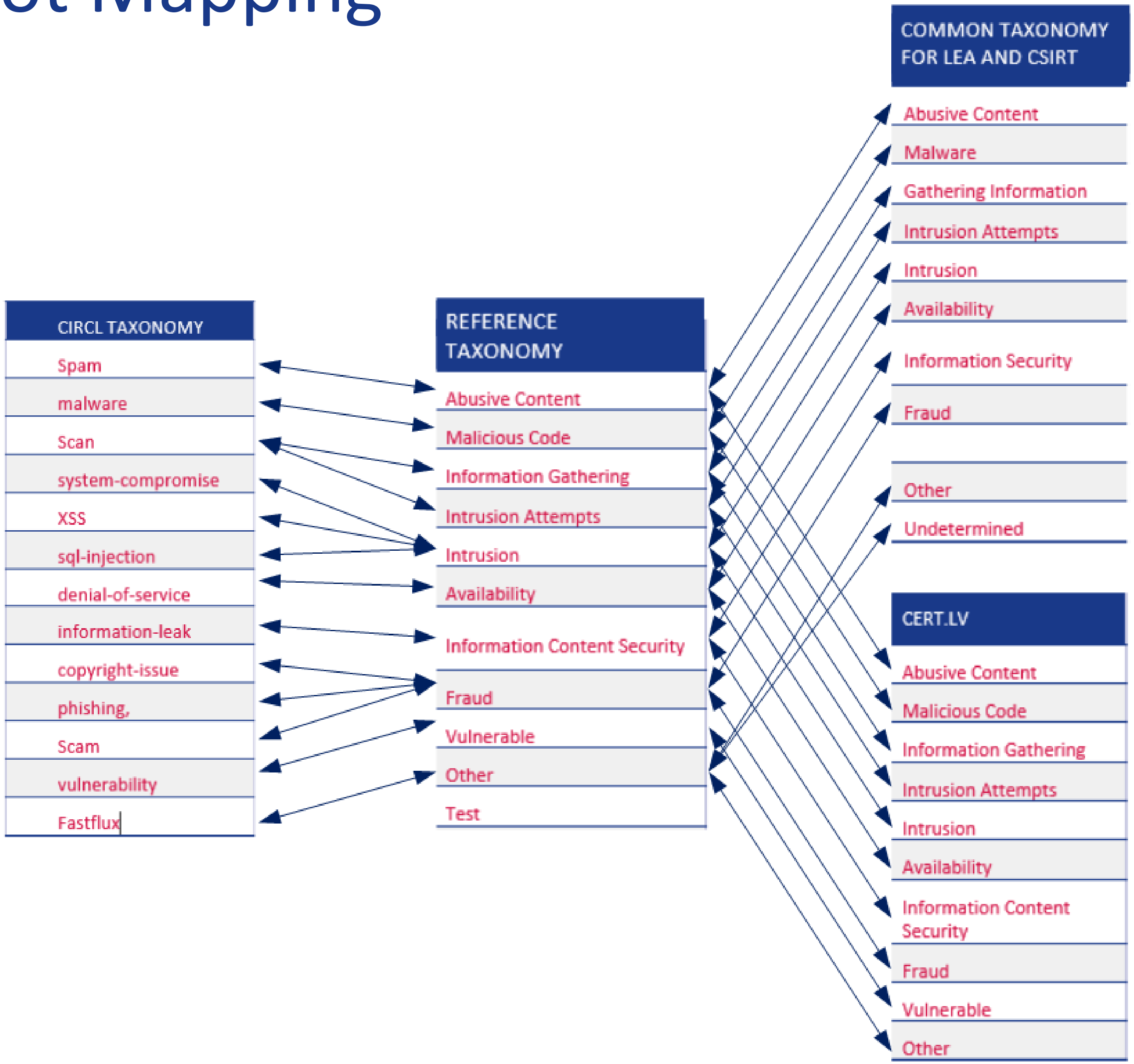
CERT.LV

Abusive Content
Malicious Code
Information Gathering
Intrusion Attempts
Intrusion
Availability
Information Content Security
Fraud
Vulnerable
Other

- ENISA introduces this idea in 2017 to the TF-CSIRT
- 52 participants from 17 MS within European CSIRT community
- Building a common language to face future incidents

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

Pivot Mapping



CIRCL TAXONOMY

- Spam
- malware
- Scan
- system-compromise
- XSS
- sql-injection
- denial-of-service
- information-leak
- copyright-issue
- phishing,
- Scam
- vulnerability
- Fastflux

REFERENCE TAXONOMY

- Abusive Content
- Malicious Code
- Information Gathering
- Intrusion Attempts
- Intrusion
- Availability
- Information Content Security
- Fraud
- Vulnerable
- Other
- Test

COMMON TAXONOMY FOR LEA AND CSIRT

- Abusive Content
- Malware
- Gathering Information
- Intrusion Attempts
- Intrusion
- Availability
- Information Security
- Fraud
- Other
- Undetermined

CERT.LV

- Abusive Content
- Malicious Code
- Information Gathering
- Intrusion Attempts
- Intrusion
- Availability
- Information Content Security
- Fraud
- Vulnerable
- Other

Use cases

Incident handling

Incident reporting

Media outreach

Policy discussion

Cross border incidents

Pivot mapping with existing initiatives

Statistics

- Performance and internal KPIs
- Comparison with other entities
- Trends
- Global / annual overview
- Explanation of external report

Update and Versioning Mechanism

Where to find it?

Taxonomy text as a working copy on GitHub in MISP machine tag schema.

Use GitHub 's "pull request" feature to transparently document change requests via a JSON file .

Anyone can add or change text and he/she is allowed to propose these changes on GitHub via pull requests.

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES
Abusive Content	Spam
	Harmful Speech
	Child/Sexual/Violence/...
Malicious Code	Virus
	Worm
	Trojan
	Spyware
	Dialler
	Rootkit
Information Gathering	Scanning
	Sniffing
	Social engineering
Intrusion Attempts	Exploiting known vulnerabilities
	Login attempts
	New attack signature
Intrusions	Privileged account compromise
	Unprivileged account compromise
	Application compromise
	Bot
Availability	DoS
	DDoS
	Sabotage
	Outage (no malice)
Information Content Security	Unauthorised access to information
	Unauthorised modification of information
Fraud	Unauthorized use of resources
	Copyright
	Masquerade
	Phishing
Vulnerable	Open for abuse
Other	All incidents which do not fit in one of the given categories should be put into this class.
Test	Meant for testing

enisa

V1

CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)	Description / Examples
Abusive Content	Spam	Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content.
Abusive Content	Harmful Speech	Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.
Abusive Content	Child Porn/Sexual/Violent Content	Child pornography, glorification of violence, etc.
Malicious Code	Infected System	System infected with malware, e.g. PC, smartphone or server infected with a rootkit.
Malicious Code	C2 Server	Command-and-control server contacted by malware on infected systems.
Malicious Code	Malware Distribution	URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.
Malicious Code	Malware Configuration	URI hosting a malware configuration file, e.g. webinjects for a banking trojan.
Malicious Code	Malware DGA Domain	Domain name generated by a domain generation algorithm (DGA) used by malware for contacting a C2 server.
Information Gathering	Scanning	Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
Information Gathering	Sniffing	Observing and recording of network traffic (wiretapping).
Information Gathering	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

Thank you

🌐 https://www.enisa.europa.eu/

✉ CSIRT-Relations@enisa.europa.eu