THE EU CYBERSECURITY AGENCY

SUPPORTING EU INCIDENT RESPONSE CAPABILITIES

Rossella Mattioli
CSIRT Relations Team
Expert in Network and Information Security
& proud TALTECH alumni

21 | 01 | 2019

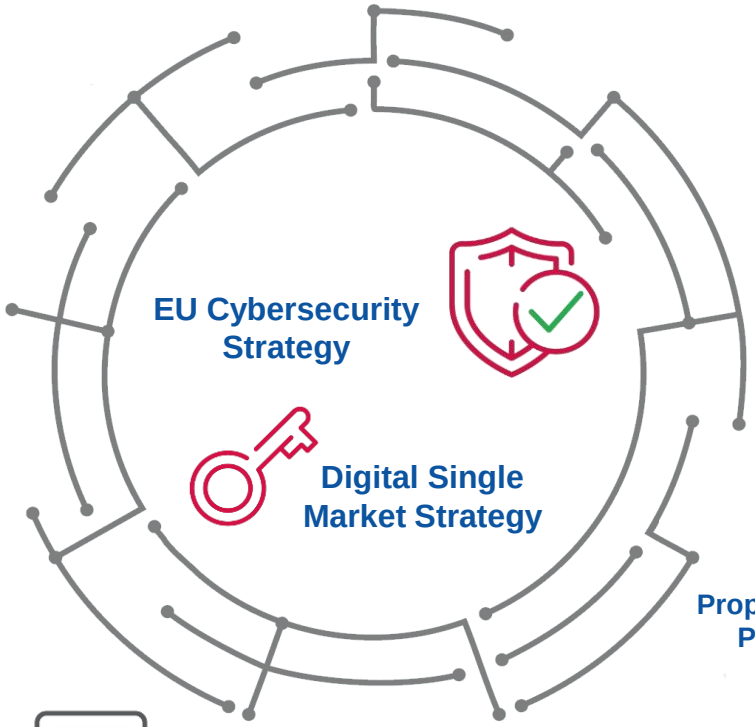
ENISA MISSION:

SECURING EUROPE'S INFORMATION SOCIETY

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

https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

TODAY POLICY FRAMEWORK



Network and Information Security Directive

eIDAS Regulation

Payment Services Directive 2

General Data Protection Regulation

Proposal for a Regulation on Privacy and Electronic Communications

POSITIONING ENISA'S ACTIVITIES

1

RECOMMENDATIONS ON CYBER SECURITY AND INDEPENDENT ADVICE

2

SUPPORT MS & EC IN POLICY IMPLEMENTATION AND HARMONISATION ACROSS EU

3

'HANDS-ON' WORK, COLLABORATING WITH OPERATIONAL TEAMS THROUGHOUT EUROPE

EXPERTISE

- 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

COMMUNITY

CSIRTs NETWORK
Powered by ENISA

http://www.csirtsnetwork.eu/

CYBER SECURITY enisa TRAINING

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

EUROPEAN CYBER SECURITY MONTH

https://cybersecuritymonth.eu/

CYBER EUROPE enisa 2018

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

EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!

https://www.europeancybersecuritychallenge.eu/

ENISA CSIRT RELATIONS TEAM PORTFOLIO

CSIRTS SITUATION IN EUROPE TODAY

- 383 ENISA Inventory listed teams:
  - teams in CSIRTs Network: 37
  - Trusted Introducer listed:173 out of 174
  - Trusted Introducer accredited: 152 out of 158
  - Trusted Introducer certified: 25 out 25*
    - 7 out of 25 are CSIRTs Network members
  - FIRST members: 175 out of 450

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

* 16 certified and 9 Re-Certification Candidate

BUILD AND ADVANCE INCIDENT RESPONSE IN EU

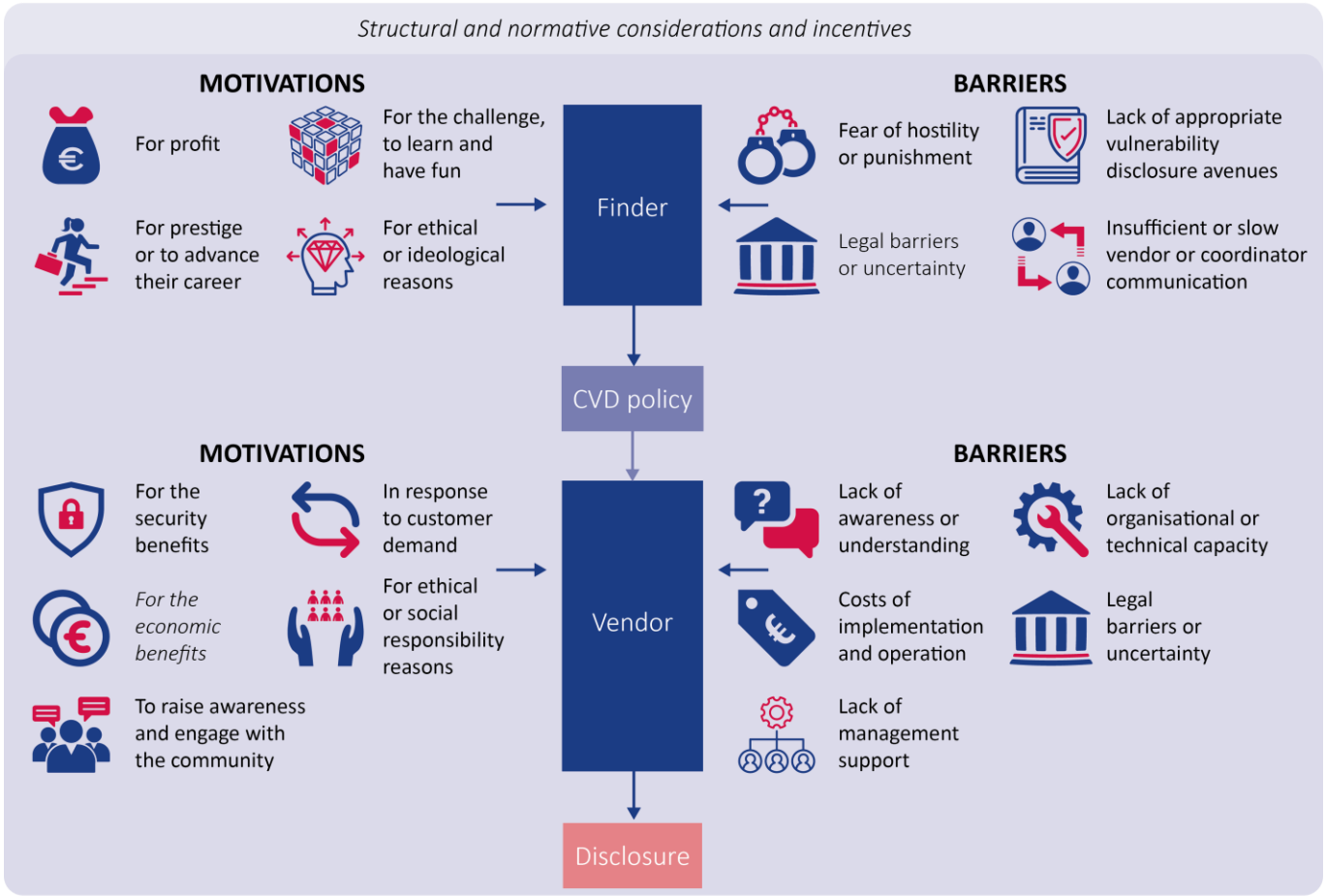
73 studies so far:

- CSIRT Setting up Guide in 21 languages
- Incident Management
- Baseline Capabilities of National/Governmental teams
- Maturity assessment framework
- Information sharing - Threat Data - Actionable information
- Proactive detection of network security incidents – monitoring - honeypots
- Computer Emergency Response Capabilities for ICS/SCADA
- Cooperation between CERTs and Law Enforcement Agencies - Electronic evidence - interaction with the Judiciary
- Vulnerability Disclosure

https://www.enisa.europa.eu/publications#c8=CSIRTs

2019 ECONOMICS OF VULNERABILITY DISCLOSURE

Economic incentives, motivations and barriers in a coordinated vulnerability disclosure process



Source: ENISA study on the economics of vulnerability disclosure

https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

2019 ECONOMICS OF VULNERABILITY DISCLOSURE

Conclusions

- The speed at which major vendors develop and roll out appropriate remediation measures can have direct effects on limiting the impact and costs of attacks.
- The inability or lack of incentives for users to monitor security developments and apply appropriate security updates or patches – even when faced with significant threats
- Stockpiling vulnerabilities can backfire (equities problem).
- More coordinated vulnerability disclosures is needed.

https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

2019 “COOPERATION BETWEEN CSIRT AND LAW ENFORCEMENT: INTERACTION WITH THE JUDICIARY”:

Conclusions:

- CSIRTs interact much more with LE than with the prosecutors and they interact very rarely with the judiciary
- There are legal provisions on CSIRTs and LE cooperation and their interaction with the judiciary
- The understanding of whether CSIRTs have to report to/inform LE and/or prosecutor of suspicious criminal activities could be improved. Depending on the Member State, the CSIRTs may be obliged or not
- There is need for a more extensive usage of information from CSIRTs in criminal investigations

https://www.enisa.europa.eu/publications/csirts-le-cooperation

2019 “COOPERATION BETWEEN CSIRT AND LAW ENFORCEMENT: INTERACTION WITH THE JUDICIARY”:

Recommendations:

- ENISA, Europol EC3, Eurojust and CEPOL: to facilitate joint training across the three communities on aspects of their cooperation among the EU and EFTA
- National/governmental CSIRTs, LE and possibly prosecutor services: to work together towards a better mutual understanding of the strengths, needs and limitations of the 3 communities
- National/governmental CSIRTs, LE and possibly prosecutor services: to appoint liaison officers to facilitate the cooperation and the interaction.
- National/governmental CSIRTs, LE and possibly prosecutor services: to investigate how the tools they use can be further improved to better receive the information provided by other communities and to better formulate their request for information addressed to the other communities.

https://www.enisa.europa.eu/publications/csirts-le-cooperation


CSIRTs
NETWORK
Powered by ENISA

CSIRTS NETWORK

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.

http://www.csirtsnetwork.eu/

members

CERT.at
GovCERT Austria
AEC
CERT.be
CERT Bulgaria
CSIRT-CY
CSIRT.CZ
GOVCERT.CZ
CERT-Bund
CFCS
CERT-EE
CCN-CERT
CERTSI
CERT-EU
NCSC-FI
CERT-FR
NCSC (UK)
NCERT-GR
CERT ZSIS
CERT.hr
GovCERT-Hungary
CSIRT-IE
IT-CERT
CERT-LT
CIRCL
CERT.LV
CSIRT Malta
NCSC-NL
CERT POLSKA
CERT.PT
CERT-RO
CERT-SE
SI-CERT
CSIRT.SK
SK-CERT
NCERT.LU
GOVCERT.LU

ENISA provides the secretariat and actively supports the cooperation among members:

- organizes meetings of the CSIRTs Network
- provides infrastructure
- provides its expertise and advice both to the EC and MS

http://www.csirtsnetwork.eu/

ENISA TRAININGS SINCE 2008

- Online training material – with over 40 trainings made available online, free to use by the community
- Training Courses on site
- Train the trainer programme – to scale trainings in the different MS

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

ENISA TRAININGS PORTFOLIO

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

Setting Up a CSIRT
Incident handling management
Recruitment of CSIRT staff
Developing CSIRT infrastructure

Technical
Building artefact handling and analysis environment
Processing and storing artifacts
Artefact analysis fundamentals
Advanced artefact handling
Introduction to advanced artefact analysis
Dynamic analysis of artefacts
Static analysis of artefacts
Forensic analysis: Local Incident Response New
Forensic analysis: Network Incident Response New
Forensic analysis: Webserver Analysis New
Developing Countermeasures
Common framework for artefact analysis activities
Using indicators to enhance defence capabilities
Identification and handling of electronic evidence
Digital forensics
Mobile threats incident handling
Mobile threats incident handling (Part II)
Proactive incident detection
Automation in incident handling
Network forensics
Honeypots
Vulnerability handling
Presenting, correlating and filtering various feeds

Operational
Incident handling during an attack on Critical Information Infrastructure
Advanced Persistent Threat incident handling
Social networks used as an attack vector for targeted attacks
Writing Security Advisories
Cost of ICT incident
Incident handling in live role playing
Incident handling in the cloud
Large scale incident handling

Legal and Cooperation
Establishing external contacts
Cooperation with law enforcement
Assessing and Testing Communication Channels with CERTs and all their stakeholders
Identifying and handling cyber-crime traces
Incident handling and cooperation during phishing campaign
Cooperation in the Area of Cybercrime
CERT participation in incident handling related to the Article 13a obligations
CERT participation in incident handling related to the Article 4 obligations

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

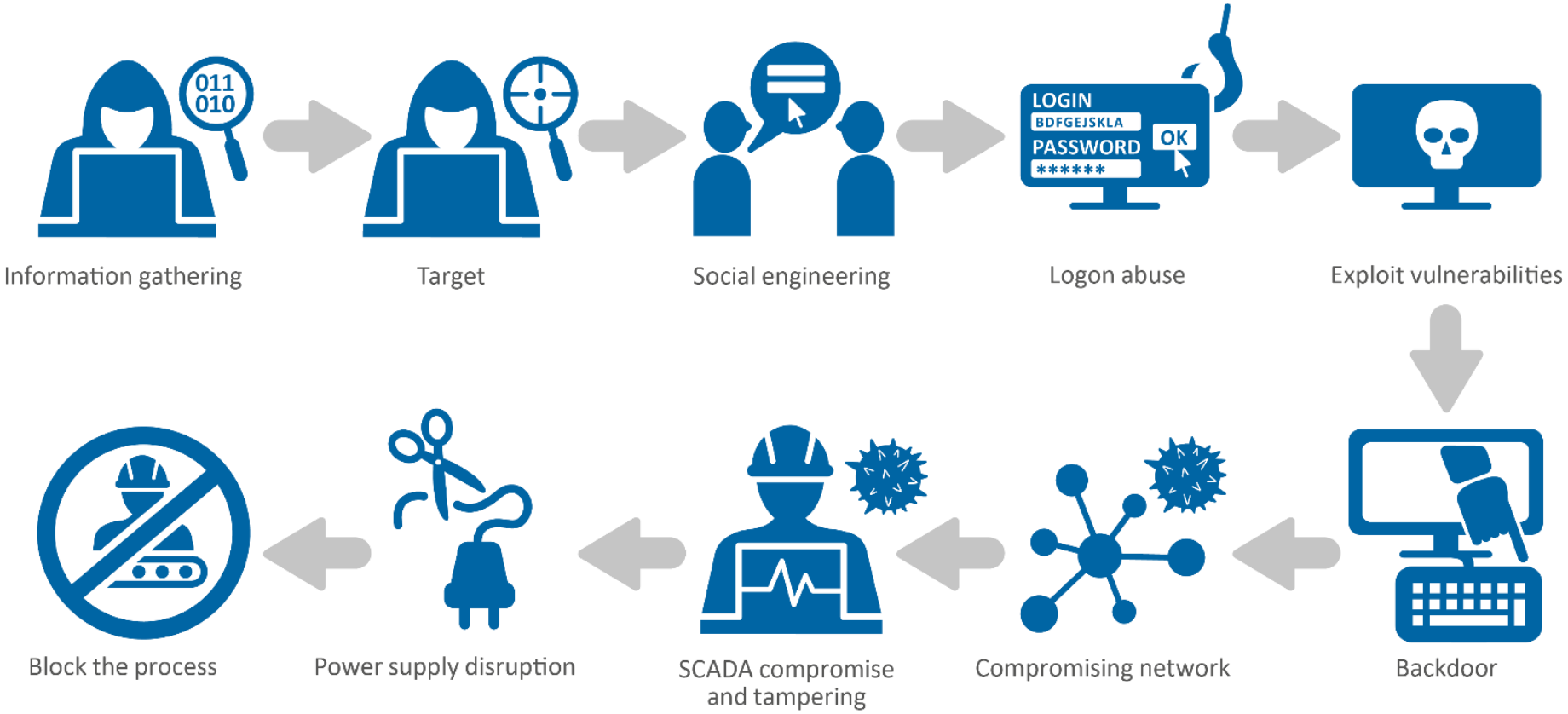
enisa

enisa European Union Agency for Network and Information Security

EASA European Aviation Safety Agency

ENISA training on aviation cybersecurity co-organized with EASA

ATTACK SCENARIO: SCADA SYSTEM COMPROMISE



ENISA training on finance cybersecurity co located with the EU Financial Information Sharing and Analysis Centre FI-ISAC in Athens, Greece in November 2018.

2018 UPDATE OF CSIRT TRAINING MATERIAL

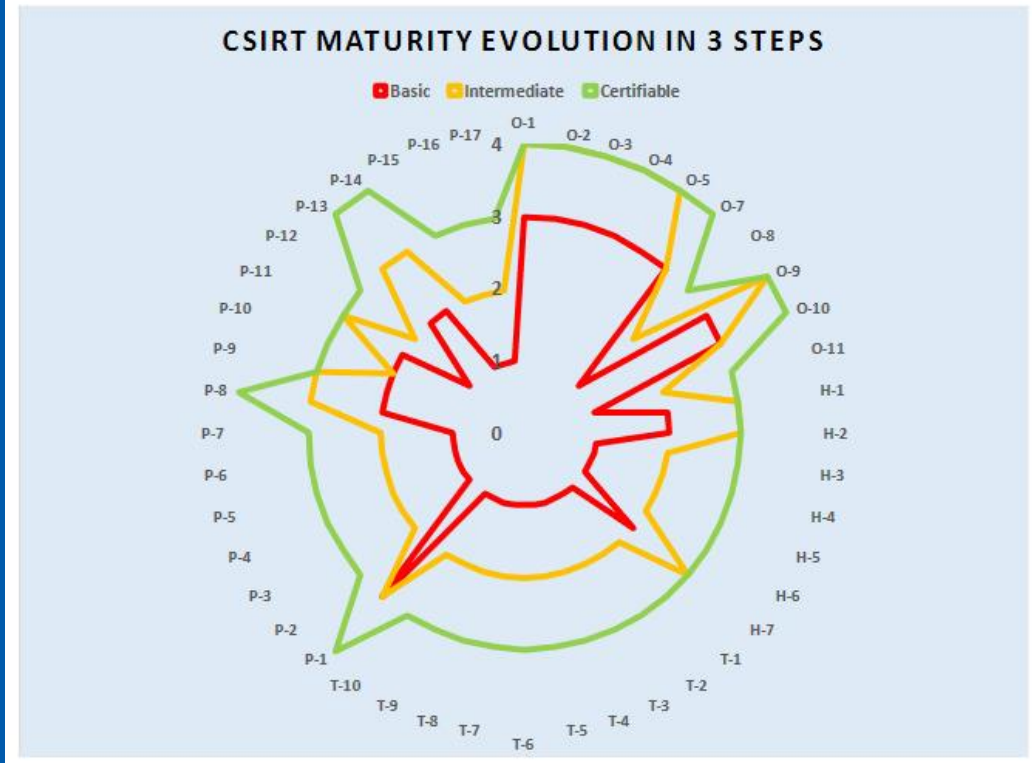
Out this week!!!

Introduction to Network Forensics:

- Exercise # 1: ICS/SCADA environment
- Exercise # 2: Detecting exfiltration on a large finance corporation environment
- Exercise #3: Analysis of an airport third-party VPN connection compromise

Network forensics

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



CSIRT CAPABILITIES DEVELOPMENT AND MATURITY ASSESSMENT METHODOLOGY

CSIRT CAPABILITIES DEVELOPMENT

BASELINING, EVALUATION, IMPROVEMENT

ENISA drives this effort continuously since 2009

In 2016 ‘How to assess maturity’
3 tier model introduced (basic, intermediate, ‘certifiable’)

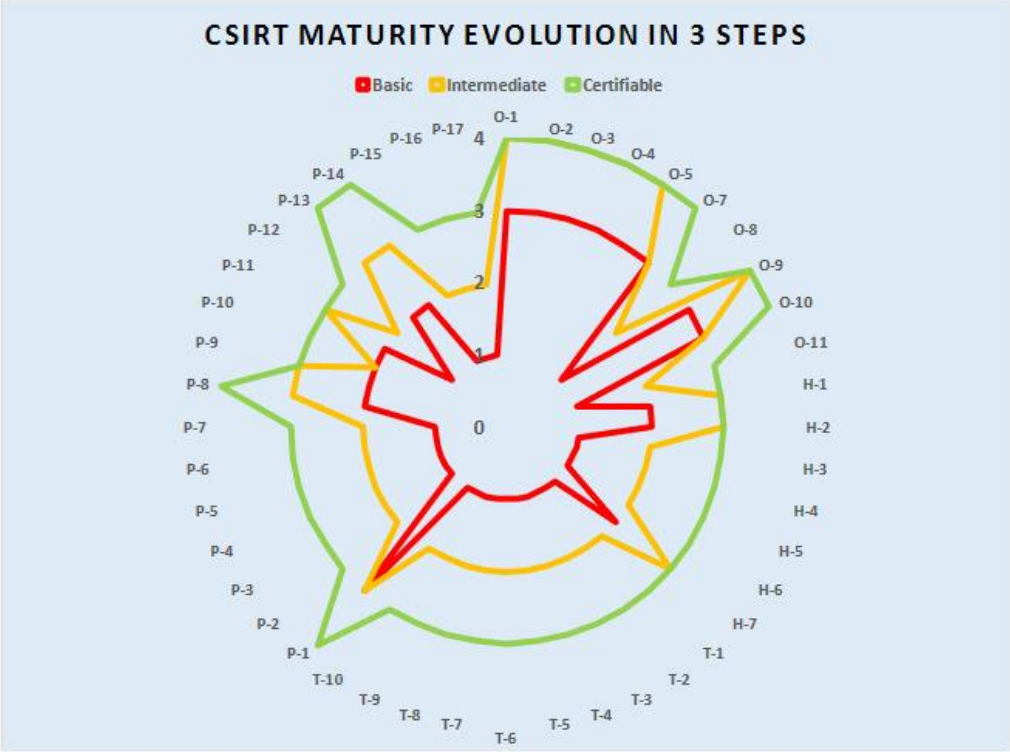
In 2017 ENISA released Maturity Self-assessment Survey
Teams can assess their team’s maturity instantly

44 questions based on SIM3 model define results

ENISA suggests an additional peer review methodology for CSIRTs Network practice

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

CSIRTS MATURITY ASSESSMENT METHODOLOGY



ENISA online assessment tool:

1. Basic (red)
2. Intermediate (yellow)
3. 'Certifiable' (green)

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

SIM3 Parameter	Parameter description	Assessed maturity: Current	Minimum demand for the 3 maturity steps: Basic	Intermediate	Certifiable
O-1	Mandate	0			
O-2	Constituency	0			
O-3	Authority	0			
O-4	Responsibility	0			
O-5	Service Description	0			
O-7	Service Level Description	0			
O-8	Incident Classification	0			
O-9	Participation in Existing CSIRT Frameworks	0			
O-10	Organisational Framework	0			
O-11	Security Policy	0			
H-1	Code of Conduct/Practice/Ethics	0			
H-2	Personal Resilience	0			
H-3	Skillset Description	0			
H-4	Internal Training	0			
H-5	(External) Technical Training	0			
H-6	(External) Communication Training	0			
H-7	External Networking	0			
T-1	IT Resources List	0	1	1	1
T-2	Information Sources List	0	1	2	3
T-3	Consolidated E-mail System	0	1	2	3
T-4	Incident Tracking System	0	1	2	3
T-5	Resilient Phone	0	1	2	3
T-6	Resilient E-mail	0	1	2	3
T-7	Resilient Internet Access	0	1	2	3
T-8	Incident Prevention Toolset	-1	1	1	1
T-9	Incident Detection Toolset	0	1	1	1
T-10	Incident Resolution Toolset	0	1	1	2
P-1	Escalation to Governance Level	0	3	3	3
P-2	Escalation to Press Function	0	1	2	3
P-3	Escalation to Legal Function	0	1	2	3
P-4	Incident Prevention Process	-1	1	2	2
P-5	Incident Detection Process	1	1	2	2
P-6	Incident Resolution Process	0	1	2	2
P-7	Specific Incident Processes	0	1	2	3
P-8	Audit/Feedback Process	0	2	3	4
P-9	Emergency Reachability Process	0	2	3	3
P-10	Best Practice Internet Presence	0	2	2	2
P-11	Secure Information Handling Process Question	0	2	3	3
P-12	Information Sources Process	0	1	2	3
P-13	Outreach Process	0	1	2	3
P-14	Reporting Process	0	2	3	4
P-15	Statistics Process	-1	1	2	3
P-16	Meeting Process	0	1	1	2
P-17	Peer-to-Peer Process	0	1	1	2

Online self assessment tool for incident response teams with 44 parameters covering:

- O - Organization
- H - Human
- T - Tools
- P - Processes

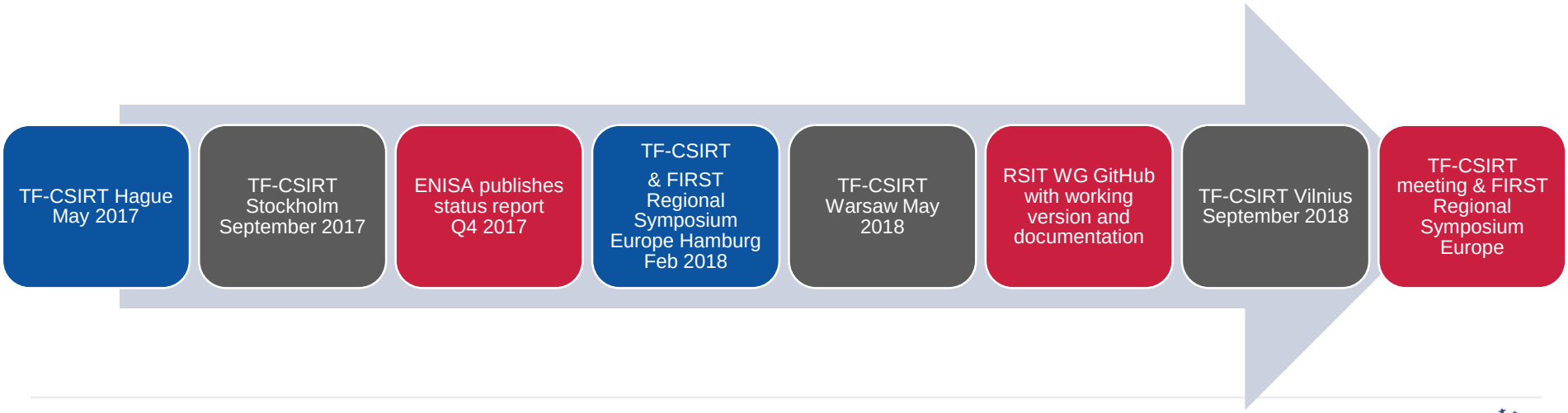
https://www.enisa.europa.eu/csirts-maturity-sas

```
{
  "values": [
    {
      "entry": [
        {
          "description": "Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the
          "expanded": "Spam",
          "value": "spam"
        },
        {
          "description": "Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more
          "expanded": "Harmful Speech",
          "value": "harmful-speech"
        },
        {
          "description": "Child pornography, glorification of violence, etc.",
          "expanded": "Child Porn/Sexual/Violent Content",
          "value": "violence"
        }
      ],
      "predicate": "abusive-content"
    },
    {
      "entry": [
        {
          "description": "System infected with malware, e.g. PC, smartphone or server infected with a rootkit.",
          "expanded": "Infected System",
          "value": "infected-system"
        },
        {
          "description": "Command-and-control server contacted by malware on infected systems.",
          "expanded": "C2 Server",
          "value": "c2-server"
        },
        {
          "description": "URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.",
          "expanded": "Malware Distribution",
          "value": "malware-distribution"
        },
        {
          "description": "URI hosting a malware configuration file, e.g. webinjects for a banking trojan.",
          "expanded": "Malware Configuration",
          "value": "malware-configuration"
```

REFERENCE SECURITY INCIDENT TAXONOMY WORKING GROUP – RSIT WG

REFERENCE INCIDENT TAXONOMY WORKING GROUP – RSIT WG

- ENISA introduced this idea in 2017 to the TF-CSIRT
- 52 participants from 17 MS
- Approved as official TF-CSIRT working group by the TF-CSIRT Steering Committee on 26 September 2018.



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

VERSION 1

REFERENCE TAXONOMY INCIDENT Taxonomy (human readable version)

This is the Reference Security Incident Classification Taxonomy.

See the machine readable version as well. It should have an identical contents to the human readable version. Note that the 1st column is mandatory, the 2nd colum is an optional but desired field.

Version: 1 Generated from machine readable version. Please do not edit this file directly in github, rather use the machinev1 file.

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.

Next meeting in Wednesday 23rd January 2018 from 15:00 to 17:00 in the Conference Hall.

Join us!

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

ENISA CSIRT Relations Team

Active support and Secretariat

Leading tool development and maturity assessment

CSIRTs in Europe

CSIRTs map

Reference Security Incident Taxonomy WG

CSIRTs self Assessment tool

CSIRTs Community projects and services

Onsite

VMs, tutorials

Train the trainers

Sectorial

WHAT WE DO

Foster expertise with reports, trainings and community projects

Provide the secretariat of the CSIRTs Network

Actively support the cooperation among CSIRTs Network members

Facilitate incident exchange and collaboration

Help incident response teams to grow and advance

Support incident response capabilities to protect European citizens

THANK YOU FOR YOUR ATTENTION

AITAH TALTECH & CERT-EE

+30 28 14 40 9711

CSIRT-Relations@enisa.europa.eu

www.enisa.europe.eu