EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# COOPERATION ACROSS CSIRTs, LAW ENFORCEMENT AND THE JUDICIARY

Dr. Silvia Portesi

Dr. Alexandra Michota

Cybercrime Webinar, Council of Europe

11 | 05 | 2020

# AGENDA

1. Introduction to ENISA
2. CSIRT-LE-Judiciary: roles and interactions
3. Overview of ENISA's activities to support CSIRT-LE cooperation
4. Summary

# INTRODUCTION TO ENISA

# EXAMPLES OF ENISA ACTIVITIES

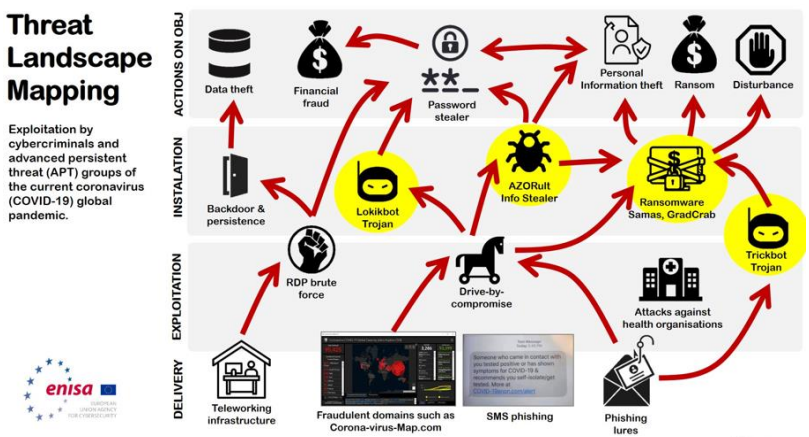
CSIRTs NETWORK

CYBER SECURITY TRAINING enisa

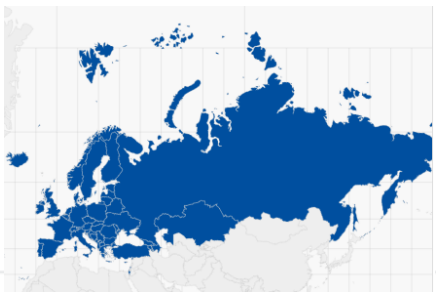
CSIRTs MATURITY ASSESSMENT enisa

CYBER EUROPE enisa 2020

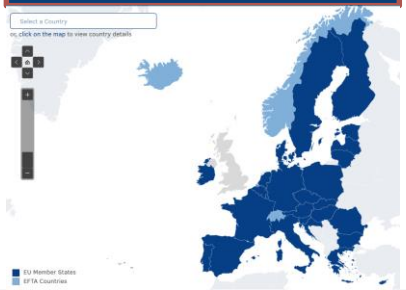
**For more information, please click on the images**




CSIRTs by Country - Interactive Map



National Cyber Security Strategies - Interactive Map

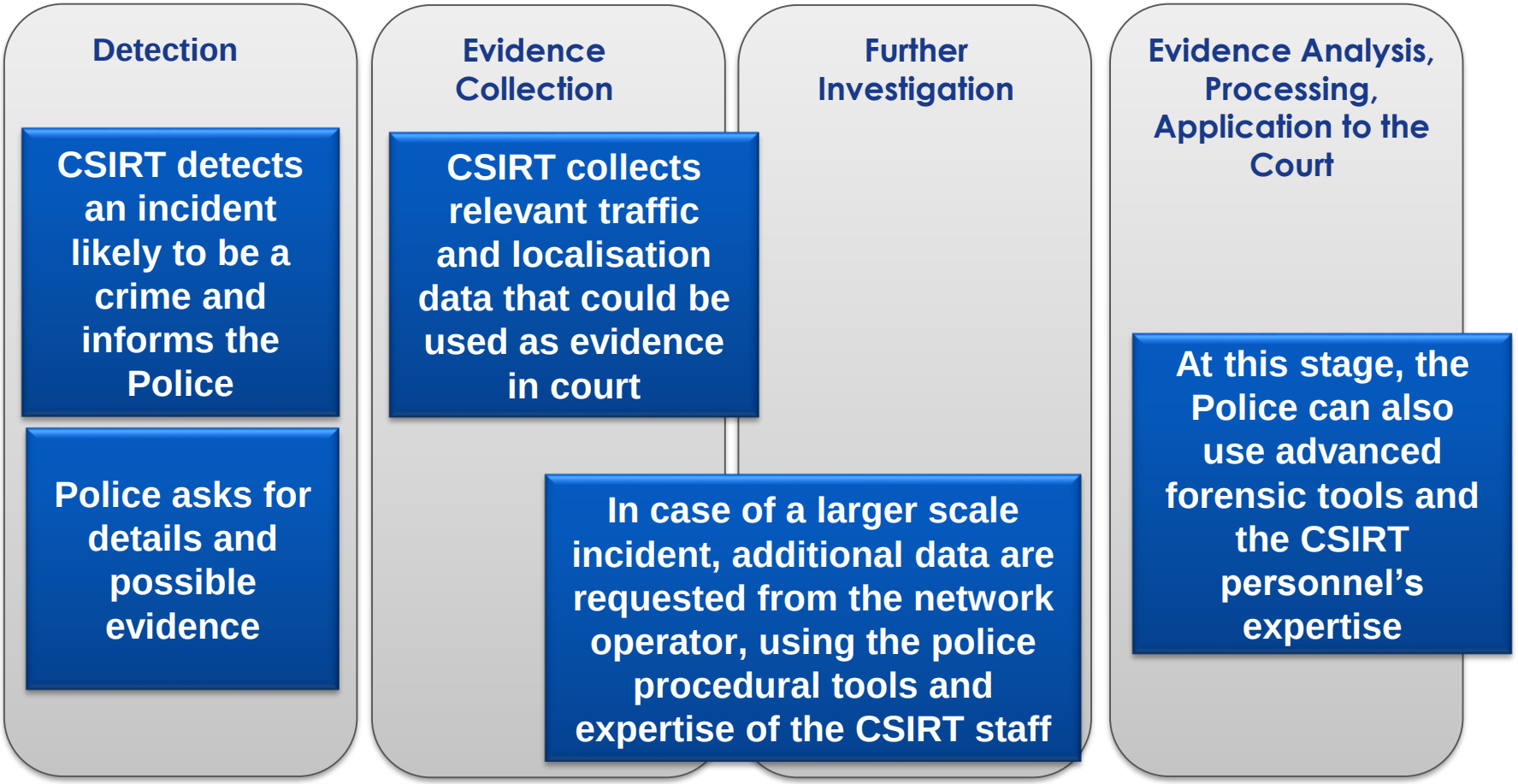


# CSIRTs, LE, AND JUDICIARY: ROLES AND INTERACTIONS

# HOW CSIRTs, LE, AND JUDICIARY ARE ORGANISED?

| CSIRTs | LE | JUDICIARY (PROSECUTORS AND JUDGES) |
|---|---|---|
| • National, governmental, sectoral, cooperative, private, academic, military, etc.<br>• Roles, responsibilities and constituency vary<br>• ≠ level of maturity | • Local, federal, national, supranational and international<br>• Responsibilities and powers vary LE Agencies specialised in cybercrime investigations | • Composition and rules vary in different countries<br>• Sometimes prosecutors/judges specialised in cybercrime |

# AN EXAMPLE OF CSIRTS-LE-JUDICIARY WORKING TOGETHER



# COOPERATION CHALLENGES

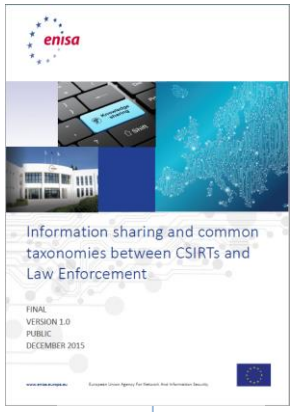
| | |
|---|---|
| 1 **Legal** | **Variety of legal systems** and legal provisions across the countries |
| 2 **Technical** | **Limited common tools and technical platforms**, integration interfaces and automation; **limited real time means of communication** and coordination |
| 3 **Organisational** | Limited skilled personnel**; insufficient training**; lack of agreed procedures on information sharing; trust deficit |
| 4 **Cultural/ behavioural** | **Human factor** as “the weakest link” in cybersecurity; ineffective approaches for mitigating behavioural risk |

# OVERVIEW OF ENISA'S ACTIVITIES TO SUPPORT CSIRT-LE COOPERATION

# TIMELINE


CERT workshop

CERT ENISA/EC3 workshop



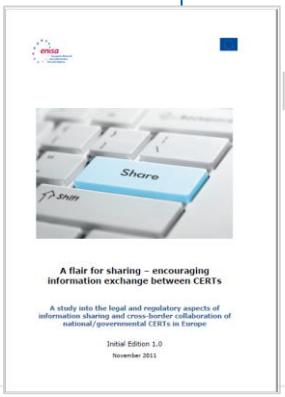

NISA/EC3 workshop


7th ENISA/EC3 workshop

ENISA Report on CSIRT-LE Cooperation

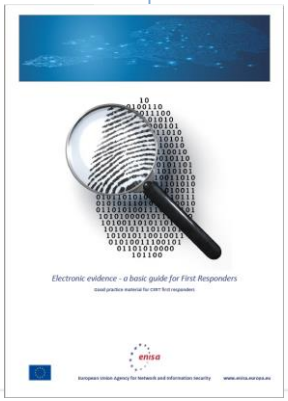
2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021

CERT workshop




CERT workshop


ENISA/EC3 workshop

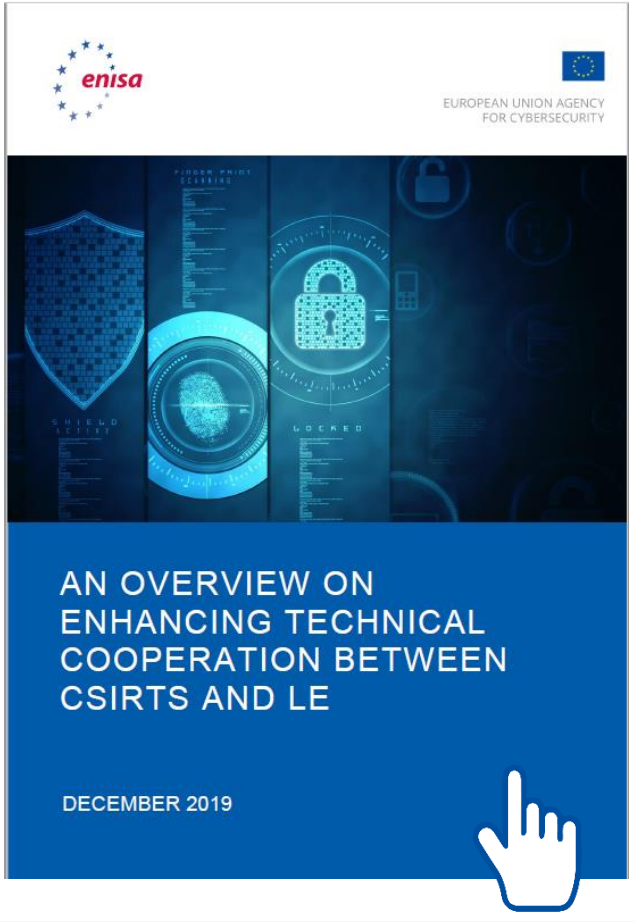



6th ENISA/EC3 workshop


8th ENISA/EC3 workshop

9th ENISA/EC3 workshop

# 2019 ENISA DELIVERABLES

# 2020 ENISA REPORT

- Development of a methodology to analyse legal and organisational framework defining CSIRT and LE **duties** and **competences** in fighting cybercrime, **synergies** and **overlaps**
- Analysis focused on some countries

  - CZ, DE, FR, LU, PT, RO, SE, NO

- Internal ***expertise***, informal expert group, input from the countries, other EU Agencies, and Council of Europe
- Desk research, questionnaire, Segregation of Duties (SoD) Matrix

# SEGREGATION OF DUTIES MATRIX

| Cybercrime Fighting Activities | CSIRTs | LE | Judges | Prosecutors | Examples of Training Topics |
|---|---|---|---|---|---|
| **Prior to incident/crime** | | | | | |
| Delivering/participating in training | | | | | Problem-solving and critical thinking skills |
| **During the incident/crime** | | | | | |
| Discovery of the cyber security incident/crime | | | | | Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis |
| Collecting data that may be evidence/Evidence collection | | | | | Knowledge of what kind of data to collect; how to collect the data; organisation skills |
| Leading the criminal investigation | | | | | Knowledge of the incident response plan; leadership skills |
| **Post incident/crime** | | | | | |
| Admitting and assessing the evidence | | | | | Evidence in a criminal trial |
| Reviewing the response and updating policies and procedures | | | | | Knowledge how to draft a post incident report and internal procedures |

# SOD FOR STRENGTHENING COOPERATION


The **aim** of this matrix is to:

**1.** prevent **conflicting** or **overlapping duties**

**2.** ensure **proper allocation of tasks**

SoD involves **breaking down tasks** within a process into multiple tasks so that each actor is responsible for separate parts

This matrix could be drafted **at national level**

# TRAINING MATERIAL

## HANDBOOKS & TOOLSETS

# ANNUAL ENISA-EC3 WORKSHOP FOR CSIRTs AND LE


- Target audience: CSIRT-LE communities
- Scope: CSIRT (national/governmental) - LE cooperation in EU
- By invitation only event

# SUMMARY

# SUMMARY

CSIRTs, LE and Judiciary have their own **roles, structures, strengths** and **constraints**

**Information sharing** across the communities is for mutual benefit of the communities and for the benefit of fighting cybercrime

Fighting cybercrime requires **comprehensive approach**, **continuous investment** and **joint efforts**

# THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu - CSIRT-LE-cooperation@enisa.europa.eu

www.enisa.europa.eu

# REFERENCES (1/5)


- **ENISA website:** https://www.enisa.europa.eu/
- **Regulation (EU) 2019/881 (Cybersecurity Act)**, 17 April 2019, https://eur-lex.europa.eu/eli/reg/2019/881/oj
- **ENISA Programming Document 2020-2022,** https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022
- **CSIRTs Network,** https://csirtsnetwork.eu/
- **Cyber Europe 2020,** https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2020/
- **CSIRTs by Country - Interactive Map,** https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

# REFERENCES (2/5)


- **National Cyber Security Strategies - Interactive Map**, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
- **Threat and Risk Management ENISA webpage**, https://www.enisa.europa.eu/topics/threat-risk-management
- **Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement** (2017), www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement
- **Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects** (2017), www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement

# REFERENCES (3/5)


- **Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary** (2018), https://www.enisa.europa.eu/publications/csirts-le-cooperation
- **Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity** (2018), https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/
- **Roadmap on the cooperation between CSIRTs and LE** (2019), https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation
- **An overview on enhancing technical cooperation between CSIRTs and LE** (2019), https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le/
- **Reference Security Incident Taxonomy Working Group,** https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

# REFERENCES (4/5)


- **Training material on CSIRT-LE cooperation area** (2019), https://www.enisa.europa.eu/news/enisa-news/training-material-to-enhance-cooperation-across-csirts-and-law-enforcement
- **Trainings for Cybersecurity Specialists,** https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
- **Trainings for Setting up a CSIRT,** https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/setting-up-a-csirt
- **CSIRT Setting up Guide in English,** https://www.enisa.europa.eu/publications/csirt-setting-up-guide
- **9th ENISA-EC3 Workshop: CSIRTs and LE Cooperation,** https://www.enisa.europa.eu/events/9th-enisa-ec3-workshop

# REFERENCES (5/5)


- **European FI-ISAC,** https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership
- **No More Ransom website,** https://www.nomoreransom.org
- **FIRST,** https://www.first.org/
- **Trusted Introducer,** https://www.trusted-introducer.org/
- **TF-CSIRT:** https://tf-csirt.org
- **ENISA Vacancies,** https://www.enisa.europa.eu/recruitment/vacancies
- **ENISA Call for Expression of Interest - List of NIS Experts (Ref. ENISA M-CEI-17-T01)**, https://www.enisa.europa.eu/procurement/cei-list-of-nis-experts