EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ASPECTS OF COOPERATION BETWEEN CSIRTS AND LE

Handbook, Document for trainers

JANUARY 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

For contacting the authors please use CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS (IN ALPHABETICAL ORDER BY SURNAME)

Philip Anderson, Sandra Blanco Bouza, Smaragda Karkala (ENISA), Gregoire Kourtis, Alexandra Michota (ENISA), Catalin Patrascu, Silvia Portesi (ENISA), Václav Stupka, Koen Van Impe.

ACKNOWLEDGEMENTS

ENISA would like to thank the following people and organisations:

- The following subject matter experts, selected from the List of Network and Information Security (NIS) Experts compiled following the ENISA Call for Expressions of Interest (CEI) (ref. ENISA M-CEI-17-C01):
  - Philip Anderson, Sandra Blanco Bouza, Catalin Patrascu, Václav Stupka and Koen Van Impe, who, together with the ENISA project team, drafted the handbook;
  - François Beauvois and Yonas Leguesse who contributed as reviewers.
- Gregoire Kourtis, who provided input to the drafting of the handbook, in particular the graphical representations.
- Europol's European Cybercrime Centre (EC3) for the peer-review of the handbook.
- The ENISA colleagues who provided input and reviewed the handbook, in particular Jo De Muynck and Christian Van Heurck.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-436-7, DOI: 10.2824/71834

TABLE OF CONTENTS

1. INTRODUCTION

1.1 THEMATIC AREA

This training material has been developed based particularly on the *ENISA 2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries*[1]. Some of the 2020 report's conclusions are that, in terms of incident response and cybercrime, the position and role of the computer security incident response teams (CSIRTs) and law enforcement (LE) in the national institutional framework varies from country to country. Similarly, the structure and the organisation of the judiciary also depends on the country.

In addition, between the three communities - CSIRTs, LE and judiciary - different approaches and different levels of cooperation exist. While the operational cooperation, especially in the daily interactions and informal communication, seems to be well-established, sometimes it seems that more structured cooperation could be achieved to have less fragmented information flow between the three communities. Also, there is a more significant gap in the interaction between CSIRTs and the judiciary, compared to the cooperation established between LE and the judiciary. CSIRTs would rather often interact with the judiciary in case they are called as an expert witness in court.

Moreover, LE is not solely involved in the detection and investigation of cybercrimes. A key component of their role is the preventive aspects of cybercrime, and it is in this role that cooperation with other communities, particularly the CSIRT community, becomes apparent to support preventive strategies. Preventive aspects of incidents/cybercrimes can also be seen as the initial ground for establishing cooperation between the CSIRTs and the LE communities, which can then extend to other phases of the incident/crime investigation. On the other hand, CSIRTs play an important role in informing (potential) victims of cybercrime and providing them with information on how to report a crime to the police.

CSIRT and LE communities also need to closely cooperate to mitigate the risks of having evidence compromised or destroyed.

Regarding the incident handling and cybercrime investigation, several competences are required. While each community has developed its own set of skills and knowledge, they can all benefit from the competences of the other communities.

Finally, the 2020 report on CSIRT and LE cooperation also concluded that despite the initiatives that are already in place to facilitate training within each community, or joint trainings engaging two communities (e.g. CSIRTs and LE, or LE and the judiciary), it seems that there is a need for more training and exercises addressing the three communities together.

The 2020 report on CSIRT and LE, this handbook and the related toolset are a set of deliverables complementing each other as follows:

- The report analyses roles, duties, competences, synergies and potential interferences across the three communities (CSIRTs, LE and judiciary).
- The handbook helps the trainer explain these concepts through scenarios.
- The toolset contains exercises for trainees based on these scenarios.

[1] ENISA, 2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries, https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation (26 January 2021)

The following figure provides an overview of this handbook and the related toolset (also available on the ENISA website), especially in terms of background, methods and recommended material.

Figure 1: ENISA training on CSIRT-LE cooperation – Syllabus

ENISA Training on CSIRT – LE Cooperation - Syllabus	
Keywords	Computer Security Incident Response Teams (CSIRTs), Law Enforcement (LE), Judiciary, Cybercrime, Cooperation, Interaction
Background	This module is intended to provide trainees with a better understanding of the CSIRT, LE and judiciary cooperation, including the segregation of duties (SoDs) of each community (CSIRTs, LE and judiciary) when dealing with cybersecurity incidents of criminal nature.
Method of teaching and learning	• Class lectures, interactive learning (class discussions, group work) and practical problems solved in class • Case studies are assigned to the trainees and are reviewed in class
Recommended material	• ENISA reports • Handbook and toolset

1.2 TRAINING OUTCOMES

As a result of attending this training, the trainee should be able to:

- demonstrate knowledge of interactions across the three communities (CSIRTs, LE and judiciary); synergies, interferences and challenges
- use the SoD matrix to collect the data to identify the key responsibilities for their communities (CSIRTs, LE and judiciary) and link them with the skills required to fulfil these duties
- better understand the legal and organisational framework defining the competences of CSIRTs, LE, and the judiciary, in their activities related to fighting cybercrime
- understand different decision-making processes among the communities
- capture potential synergies and possible overlaps
- overcome possible interferences of cooperation between CSIRTs and LE and their interaction with the judiciary
- ensure structured integration of liaison officers for coordination between the different communities
- perform uniform and effective communication between CSIRTs, LE and the judiciary toward victim and relevant stakeholders
- coordinate basic first responder actions at victim site (collecting evidence without tampering it, informing partners of which evidence is gathered)
- explain technical terms to non-technical participants, e.g. to the judiciary
- better translate legal constraints to CSIRTs
- identify appropriate approaches and tools to help support effective collaboration
- identify and develop a common plan to enhance cooperation

1.3 TARGET AUDIENCE

The intended target audiences are the CSIRTs (mainly national and governmental CSIRTs but not limited to them), LE and the judiciary (public prosecutors and judges).

1.4 COURSE DURATION

2-3 hours

1.5 FREQUENCY

Yearly (indicative)

2. GENERAL DESCRIPTION

2.1 IMPORTANCE OF COOPERATION BETWEEN CSIRTS, LE AND THE JUDICIARY

There are powers, information, equipment, expertise or contacts that are available exclusively to one of the communities – CSIRTs, LE or judiciary – but, at the same time, these resources could be tremendously useful to others. In addition, it often happens that these communities deal with the same cases; what should be avoided in these cases is that one community interferes with goals and activities of the other communities. It is therefore vital for these communities to cooperate as much as possible and make use of available synergies while managing potential interferences.

However, technical, legal, organisational and cultural challenges can hinder this cooperation. Also, those challenges are managed differently in each country. Past reports developed by ENISA provide valuable insight into the current state of cooperation and recommendations on how to improve it[2].

Taking into consideration that cybersecurity incidents do not always amount to cybercrimes (cybersecurity incidents are not necessarily of criminal nature), cooperation between CSIRTs and LE/judiciary does not take place in all cases. But cooperation should take place in cases of cyber incidents that are criminal in nature. In these cases, the role of each community varies, more specifically:

- CSIRT's role is to mitigate the incidents
- LE's role is to conduct the investigations
- the judiciary's role is to prosecute (prosecutors) and judge (judges)

Also, within the CSIRTs community, there are differences depending on the type of CSIRT (governmental, national, sectoral, etc.). The same applies to LE and the judiciary communities (for instance, local, regional, national, federal, or international law enforcement agencies).

When dealing with a cybersecurity incident of criminal nature, each community should consider the outreach to other actors that could be involved, keeping in mind the multiple ways of cooperating and the importance of receiving reciprocal feedback on a case. Additional stakeholders may be approached in this cooperation process, such as the service operators and service providers, intelligence services, military, and international agencies.

Both formal (e.g. official written requests) and informal procedures (e.g. information shared orally during a phone call) may be followed throughout this cooperation process. The cooperation channel may be supported through appointed liaison officers.

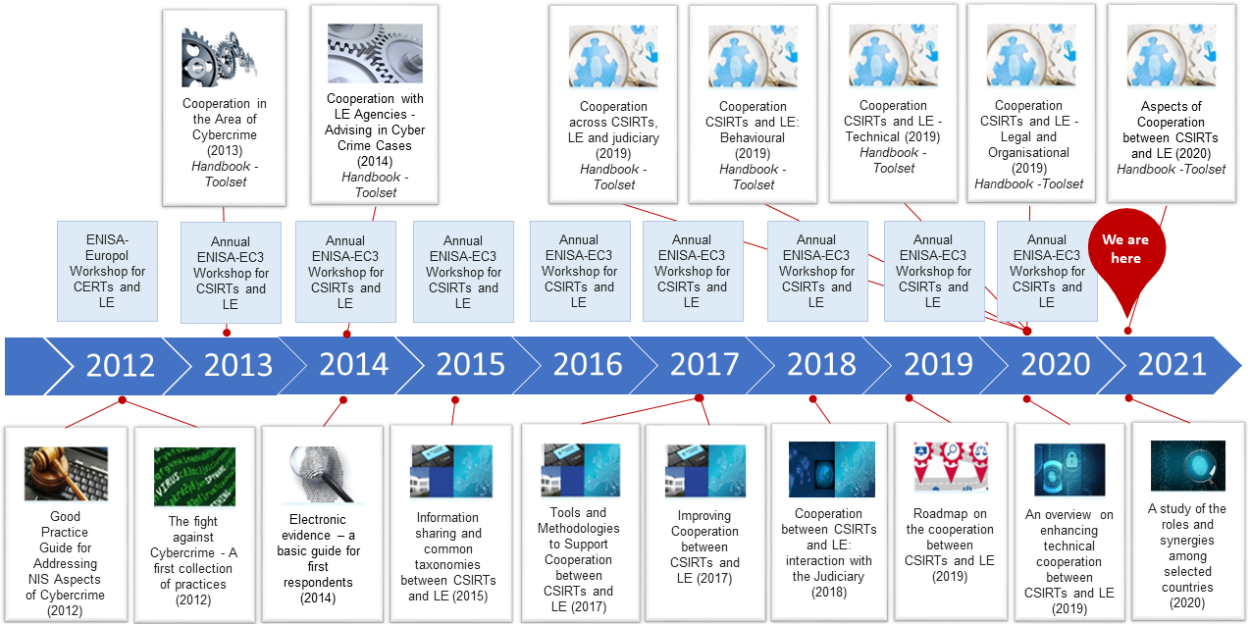
[2] In particular, see: ENISA, *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (2017), www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement ; ENISA, *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (2017), www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement ; ENISA, *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary* (2018), https://www.enisa.europa.eu/publications/csirts-le-cooperation ; ENISA, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity* (2018), https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity ; ENISA, *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

2.2 RELEVANT ENISA WORK ON CSIRT/LE COOPERATION

As mentioned previously, this training material has been developed based in particular on the ENISA *2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries*[3]. This training material is a follow up of previous ENISA training material in the area of CSIRTs and LE cooperation.[4]

An overview of ENISA's work in the area of CSIRTs and LE cooperation is provided in the figure below. All reports and training material mentioned in the figure below are available on ENISA's website and in the Bibliography section at the end of this handbook.

Figure 2: Overview of ENISA's work in the area of CSIRTs and LE cooperation



Some of the cooperation aspects highlighted in previous ENISA work that should be kept in mind for this training are the following:

- CSIRTs interact much more with LE than with prosecutors, and rarely interact with the judiciary
- Cooperation across CSIRTs, LE and the judiciary is shaped by the legal and organisational framework, which varies from country to country

[3] ENISA, 2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries, https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation (26 January 2021)

[4] See in particular latest years material: ENISA, *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 (retrieved on 13 October 2020); ENISA, *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary* (2018), https://www.enisa.europa.eu/publications/csirts-le-cooperation (retrieved on 13 October 2020); ENISA, *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (2017), www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement (retrieved on 13 October 2020); ENISA, *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 (retrieved on 13 October 2020); ENISA, *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 (retrieved on 13 October 2020); ENISA, *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 (retrieved on 13 October 2020).

- Working together (in the same building/office), or at least having liaison officers, is recognised as being one of the most efficient ways of ensuring good cooperation and information sharing between CSIRT and LE
- There are cases of CSIRTs supporting LE (as well as prosecutors and judges) in a criminal investigation
- CSIRTs have the technical expertise and can support LE by sharing expertise as well as data about incidents

2.3 SUMMARY OF 2020 REPORT

To support the key actors of a cybercrime investigation, i.e. the CSIRT and LE communities as well as the judiciary to reach a better understanding of each other's duties based on the roles each community plays, the 2020 *ENISA Report on CISRT-LE cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries* proposed[5] a Segregation of Duties (SoD) matrix. A snippet of the SoD can be seen below, while the full version can be found in Annex B of this handbook.

Figure 3: Snippet of the SoD matrix

Version 1.6 of 5 June 2020

- **Responsible (R):** Who is responsible for performing this duty? Who is the decision maker?
- **Supporting (S):** Who is providing support when performing this duty? (if applicable)
- **Consulted (C):** Who is consulted during the performance of this duty? (if applicable)
- **Informed (I):** Who is informed when performing this duty? (For instance, if CSIRT should report a crime to LEA; this means that LEA is informed) (if applicable)

Duties related to (supporting) cybercrime fighting activities	CSIRTs	LE	Prosecutors	Judges	Training topics (e.g. technical skills etc	ADDITIONAL COMMENTS (including information on possible synergies and potential interferences)
Prior to incident/crime						
1. Delivering training						
2. Participating in training						
3. Collecting cyber threat intelligence						
4. Analysing vulnerabilities and threats						

This SoD can be used to collect and analyse the cooperation at a national level and identify synergies and potential overlapping duties across the three communities.

By using this SoD matrix, key responsibilities of CSIRTs, LE, judges and prosecutors can be identified and linked with the skills required to fulfil these duties. In addition, synergies and potential interferences can be captured.

2.4 CORE READING

ENISA, *2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries*[6].

[5] This SoD matrix is inspired by COBIT methodology. For more information on this matter, see Section 2.3 of the ENISA *2020 Report on CSIRT-LE cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries* https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation.

[6] ENISA, 2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries, https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation (26 January 2021)

3. CASE STUDIES

Case studies are used to test the ability of individual communities to cooperate in the event of a cybersecurity incident. The topics of the case studies were chosen to reflect the experience of the practice, but any resemblances to real incidents are entirely coincidental.

The case studies focus on attacks involving the theft of confidential data, the spread of ransomware and DDoS attacks. Each case study includes descriptions of:

- a scenario that explains the situation
- the organization at risk
- the position of the trainee

The descriptions are followed by a set of tasks that the trainees have to perform based on the described assignment.

To facilitate orientation for the techniques and tactics applied in the scenario, definitions from the knowledge database MITRE ATT&CK®[7] were used. The MITRE ATT&CK® framework was chosen because it is a comprehensive knowledge base of the tactics, techniques and procedures (TTPs) used by attackers during real incidents. It reflects the capabilities and methodologies used by adversaries as observed in the real world. The tactics provide the “why”, the adversary’s tactical objective for performing an action. The techniques, on the other hand, represent “how” an adversary achieves a tactical objective by performing an action.

The framework also includes guidance on the data sources and mechanisms that can be used to detect computer security incidents, and it provides a common taxonomy, or standardization, to describe TTPs. As such, it is complementary to the Reference Security Incident Taxonomy (RSIT) incident classification. The latter classifies the incident, whereas the former describes how the incident takes place and how it can be detected.

A possible other solution to describe cyber incidents is the Cyber Kill Chain®.[8] This seven-step model provides visibility to the stages of a cyberattack, from reconnaissance to the final objectives. The model is, however, more high-level and does not offer the same level of detail for understanding and detecting the behaviour and activities of attackers.

The three scenarios presented below have been developed for training purposes. Since the focus of this training material is on CSIRTs, LE and the judiciary and their cooperation, the emphasis is put in particular on these three actors. However, when analysing real cases, other important actors need to be considered, such as the victim, the attacker, the service providers, and third parties (including witnesses for instance). Also in real cases, in some countries, both a national and a governmental CSIRT might be present (in addition to several other public and private CSIRTs). Also, the structures of LE and the judiciary might be more complex (for instance LE and the judiciary might be organised in local, regional, state and federal levels).

[7] MITRE ATT&CK®, https://attack.mitre.org/ (retrieved on 28 November 2020).
[8] Lockheed Martin, The Cyber Kill Chain®, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (retrieved on 20 October 2020).

3.1 CASE STUDY 1: THEFT OF CONFIDENTIAL DATA

Figure 4: Overview of case study 1

Overview of the case study 1	
Targeted Audience	This exercise is useful for incident responders and members of law enforcement of all experience levels. It is particularly helpful for national CSIRT members and law enforcement officers involved in cybercrime investigations.
Total Duration	45 minutes
Scenario	This is a group exercise. Each trainee is a member of CSIRT, LE or the judiciary who is involved in the prevention, mitigation and investigation of the cybersecurity incident/crime. Their goals are to address key ramifications resulting from the theft of confidential data, identify synergies that could be exploited by cooperating with the other communities, and potential interferences in case of lack of cooperation/coordination
Task 1	Identify and describe the organisational profile
Task 2	Describe measures that CSIRT and/or LE can take to prevent the incident/crime
Task 3	Use the SoD Matrix to analyse possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary
Task 4	List possible measures that CSIRT and/or LE can take during the incident response/crime investigation while performing different duties
Task 5	Group discussion on balancing the incident mitigation (asset protection) and criminal investigation (evidence collection and preservation)

When possible, this case study should be conducted in groups so that the different results and approaches of each group can be compared. Then, the advantages and disadvantages of individual solutions should be discussed.

3.1.1 Objectives

In this exercise, the trainees will learn when and how CSIRT, LE, and judiciary representatives can cooperate. In particular, the objectives of the exercise are to:

- Understand and appreciate the specifics of CSIRT/LE activities
- Analyse roles of different actors and how they can cooperate
- Identify synergies that can be exploited
- Grasp the complexity of cooperation

3.1.2 Scenario

3.1.2.1 Setting the stage

This scenario describes an incident where carefully selected individuals working for different Member States (MS A, MS B, and MS C) subscribe to a fake event. The event website mimics an event organized by an EU Commissioner and contains malicious documents. Once installed on the victim's computer, the malware included in the document exfiltrates domain and VPN access login credentials and selected documents with sensitive information. The credentials and the sensitive information is then monetized by the attacker via a semi-public website.

The internal security team of the Ministry of Education of MS A, to which one of the victims belongs, detects the incident. The internal security team of the Ministry of Education of MS A notifies the MS A national CSIRT, which in turn contacts law enforcement (of MS A).

The location where the exfiltration of data took place is in European MS D - whereas the website making the exfiltrated data available is located in Country Z, a non-EU/EFTA country.

In this case study, we use the concept of lanes to describe two distinct events that are part of the same security incident. The concept of lanes is used to demonstrate to the students that different security events which at first seem unrelated, can in fact be related to the same security incident. It is an opportunity for students to understand that separate investigations, started from different security events, will eventually merge because they deal with the same security incident. Students should cover both lanes to grasp the full details of the security incident.

Figure 5: Graphical representation of scenario 1 – Attack

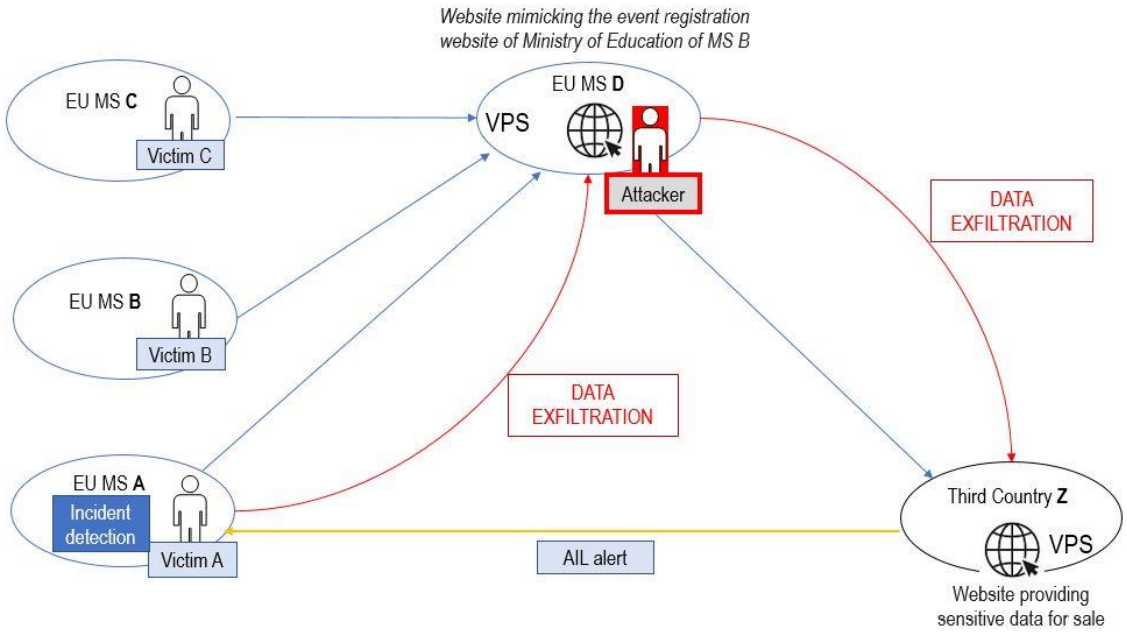
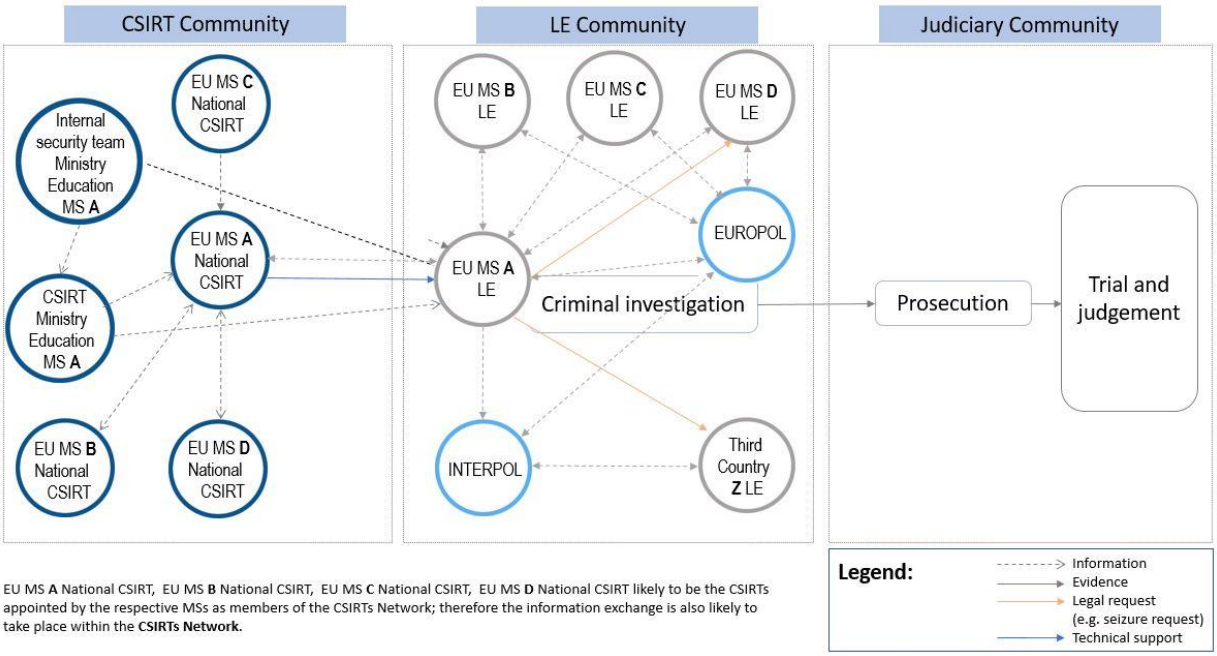


Figure 6: Graphical representation of scenario 1 – Overview of interactions



3.1.2.2 Before the breach

Reconnaissance

The attackers in this scenario spent a considerable amount of time on the reconnaissance of their potential new victim. They used online research of the Ministry of Education of MS A to find individuals of interest. They mapped out with whom these individuals typically collaborate, in particular with individuals at other ministries in MS A but also at Ministries of Education in other countries and with the European Commission. The attackers supplemented this information with the publicly available calendar information from the Commissioner.

The attackers used the following tactics and techniques:

Tactic TA0017 - Organizational Information Gathering[9]	"Organizational information gathering consists of the process of identifying critical organizational elements of intelligence an adversary will need about a target in order to best attack. Similar to competitive intelligence, organisational intelligence gathering focuses on understanding the operational tempo of an organization and gathering a deep understanding of the organization and how it operates, in order to best develop a strategy to target it."[10]
Tactic TA0016 - People Information Gathering[11]	"People Information Gathering consists of the process of identifying critical personnel elements of intelligence an adversary will need about a target in order to best attack. People intelligence gathering focuses on identifying key personnel or individuals with critical accesses in order to best approach a target for attack. It may involve aspects of social engineering, elicitation, mining social media sources, or be thought of as understanding the personnel element of competitive intelligence."[12]

[9] MITRE Corporation, *Organizational Information Gathering*, https://attack.mitre.org/tactics/TA0017/ (retrieved on 13 October 2020).
[10] MITRE Corporation, *Organizational Information Gathering*, https://attack.mitre.org/tactics/TA0017/ (retrieved on 13 October 2020).
[11] MITRE Corporation, *People Information Gathering*, https://attack.mitre.org/tactics/TA0016/ (retrieved on 13 October 2020).
[12] MITRE Corporation, *People Information Gathering*, https://attack.mitre.org/tactics/TA0016/ (retrieved on 13 October 2020).

Technique T1301 - Analyze business processes[13]	"Business processes, such as who typically communicates with who, or what the supply chain is for a particular part, provide opportunities for social engineering or other".[14]

The attackers then used one of the appointments in the Commissioner's calendar to set up a fake round table event to collect future views on a specific topic, hosted by the Ministry of Education of MS B. The attackers identified which individuals in the Ministry of Education of MS A would be the most interested in this topic. Then, the attackers set up fake personas to impersonate representatives of the Ministry of Education of MS B, and they created a website mimicking the event registration website of the Ministry of Education of MS B.

Technique T1295 - Analyze social and business relationships, interests, and affiliations[15]	"Social media provides insight into the target's affiliations with groups and organizations. Certification information can explain their technical associations and professional associations. Personal information can provide data for exploitation or even blackmail."[16]
Tactic TA0023 - Persona Development[17]	"Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy throughout an operation using that persona or identity." [18]

Initial access

Armed with a list of targets selected during reconnaissance, the attackers used the personas impersonating staff working for the Ministry of Education of MS B to send out invitations for the fake event. The event website requested that visitors enter personal information, and it contained documents, such as a call for proposals or Q&A, which were prepared by the attackers to include malicious code.

Technique T1566 - Phishing: Spear phishing Link[19]	"Adversaries may send spearphishing emails with a malicious link in an attempt to elicit sensitive information and/or gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in the email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments."[20]

Execution

The event website included text to lure the visitors into opening the documents because they contained "essential" information on the event. The malicious documents were Office documents, with a blurred image and a text stating that to see the content, the user needed to "Enable Decryption via Enable Content", which enabled Word macros. Once the macro was enabled, it downloaded and ran the malicious executable file.

[13] MITRE Corporation, *Analyze business processes*, https://attack.mitre.org/techniques/T1301/ (retrieved on 13 October 2020).
[14] MITRE Corporation, *Analyze business processes*, https://attack.mitre.org/techniques/T1301/ (retrieved on 13 October 2020) (See also the reference of *Gregory Scasny. (2015, September 14) "Understanding Open Source Intelligence (OSINT) and its relationship to Identity Theft"*, retrieved March 1, 2017).
[15] MITRE Corporation, *Analyze social and business relationships, interests, and affiliations*, https://attack.mitre.org/techniques/T1295/ (retrieved on 13 October 2020).
[16] MITRE Corporation, *Analyze social and business relationships, interests, and affiliations*, https://attack.mitre.org/techniques/T1295/ (retrieved on 13 October 2020) (See also the reference of *Gregory Scasny. (2015, September 14) "Understanding Open Source Intelligence (OSINT) and its relationship to Identity Theft"* as retrieved March 1, 2017).
[17] MITRE Corporation, *Persona Development*, https://attack.mitre.org/tactics/TA0023/ (retrieved on 13 October 2020).
[18] MITRE Corporation, *Persona Development*, https://attack.mitre.org/tactics/TA0023/ (retrieved on 13 October 2020).
[19] MITRE Corporation, *Phishing:Spearphishing Link*, https://attack.mitre.org/techniques/T1566/002/ (retrieved on 13 October 2020).
[20] MITRE Corporation, *Phishing:Spearphishing Link*, https://attack.mitre.org/techniques/T1566/002/ (retrieved on 13 October 2020).

Technique T1204 - User Execution[21]	"An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behaviour from forms of Phishing."[22]

Credential access and collection

The malicious executable was, in fact, a variant of a well-known keylogger specifically designed to collect credentials entered by a user when starting a VPN client. The captured credentials were regularly sent out to an external website. Apart from a keylogger, the malware was also able to collect files on the local system of the victim. It searched for specific types of files with particular names which were sent out to an external website.

MITRE Technique T1056 – Input Capture[23]	"Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Credential API Hooking) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. Web Portal Capture)."[24]
Technique T1567 – Exfiltration Over Web Service[25]	"Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to the compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection." [26]
Technique T1029 – Scheduled Transfer[27]	"Adversaries may schedule data exfiltration to be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability." [28]
Technique T1560 – Archive Collected Data[29]	"An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender." [30]
Technique T1005 – Data from the local system[31]	"Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to Exfiltration."[32]

[21] MITRE Corporation, *User Execution*, https://attack.mitre.org/techniques/T1204/ (retrieved on 13 October 2020).
[22] MITRE Corporation, *User Execution*, https://attack.mitre.org/techniques/T1204/ (retrieved on 13 October 2020).
[23] MITRE Corporation, *Input Capture*, https://attack.mitre.org/techniques/T1056/ (retrieved on 13 October 2020).
[24] MITRE Corporation, *Input Capture*, https://attack.mitre.org/techniques/T1056/ (retrieved on 13 October 2020).
[25] MITRE Corporation, *Exfiltration Over Web Service*, https://attack.mitre.org/techniques/T1567/ (retrieved on 13 October 2020).
[26] MITRE Corporation, *Exfiltration Over Web Service*, https://attack.mitre.org/techniques/T1567/ (retrieved on 13 October 2020).
[27] MITRE Corporation, *Scheduled Transfer*, https://attack.mitre.org/techniques/T1029/ (retrieved on 13 October 2020).
[28] MITRE Corporation, *Scheduled Transfer*, https://attack.mitre.org/techniques/T1029/ (retrieved on 13 October 2020).
[29] MITRE Corporation, *Archive Collected Data*, https://attack.mitre.org/techniques/T1560/ (retrieved on 13 October 2020).
[30] MITRE Corporation, *Archive Collected Data*, https://attack.mitre.org/techniques/T1560/ (retrieved on 13 October 2020).
[31] MITRE Corporation, *Data from Local System*, https://attack.mitre.org/techniques/T1005/ (retrieved on 13 October 2020).
[32] MITRE Corporation, *Data from Local System*, https://attack.mitre.org/techniques/T1005/ (retrieved on 13 October 2020).

3.1.2.3 Initial response

Breach notification

Lane 1
During a weekly review of network activity, the security operations team of the Ministry of Education of MS A noticed that there was a substantial amount of outbound traffic to an external website located in MS D. Their initial investigation showed that the internal source of the traffic was on a network segment used by individuals working on sensitive material.

The security team of the Ministry of Education of MS A alerted its internal CSIRT and started collecting information on the affected assets.

Lane 2
At the same time, the CSIRT team of the Ministry of Education of MS A got an alert from one of their public crawlers. The team received an internal notification from the AIL framework[33] showing that there was a hit on the name of the Ministry of Education of MS A for a website located on a VPS in Country Z. The website was protected with a password and required payment to access it. It provided some screenshots and extracts of texts to show what type of information was available for potential "customers".

Upon inspection of the screenshot of the alert, they immediately spotted that the document contained sensitive information which shouldn't be publicly accessible.

The response of the CSIRT
The CSIRT handler on duty for the Ministry of Education of MS A classified the incidents according to the ENISA RSIT[34] as "Information Content Security", "Leak of confidential information".

The CSIRT requested the security operations team to safeguard the logs of the affected assets in their SIEM and use EDR tooling to capture live system memory and collect important system artefacts. Unfortunately, the EDR had not been deployed to all assets. In the meantime, the security operations team was able to isolate the system process responsible for the exfiltration of the data. Additionally, they still saw active network activity to the external website. This activity meant that the exfiltration was ongoing.

The CSIRT notified the CISO and the Secretary-General of the Ministry of Education of MS A of the possible security incident. A crisis team was formed, including the Press Officer, the legal department, the HR department and a representative of the General Secretariat of the Ministry of Education of MS A.

At this stage, it was unknown which type of data was exfiltrated. Still, because of the volume of data already exfiltrated and the type of assets (workstations and individuals involved), the CSIRT of the Ministry of Education of MS A suggested filtering traffic to the IP in MS D until further investigation. Additionally, according to the representative of the Ministry of Education of MS A, the screenshot in the AIL alert was of a document which had not been published and which was processed on one of the affected assets.

[33] GitHub, *CIRCL / AIL-framework*, https://github.com/CIRCL/AIL-framework (retrieved on 13 October 2020).
[34] GitHub, *enisaeu / Reference-Security-Incident-Taxonomy-Task-Force*, https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force (retrieved on 13 October 2020).

The CSIRT of the Ministry of Education of MS A immediately instructed the network team to filter all traffic to and from the IP in MS D.

The CISO of the Ministry of Education of MS A, together with the head of CSIRT of the Ministry of Education of MS A, contacted the national CSIRT of MS A to report the incident and LE of MS A to file a complaint.

Criminal investigation in MS A

LE officials of MS A were informed of the case details, including the fact that this concerned sensitive information and that there was a very high suspicion that data had been exfiltrated to a server in MS D.

LE conducted an investigation and went on-site to the Ministry of Education of MS A to review the available log material.

The CSIRT of the Ministry of Education of MS A provided LE with their collected reports on network traffic, together with the screenshots and information of the leaked documents on the server in Country Z, a non-EU/EFTA country.

The CSIRT of the Ministry of Education of MS A informed LE that the activity was still ongoing and that they implemented a network filter.

Investigation analysis

Because of the network filter, the malware was unable to contact the server in MS D. This triggered a failsafe mechanism, and it started encrypting all the files on the workstation.

The CSIRT of the Ministry of Education of MS A informed LE that the evidence on the workstation was most likely no longer usable. The logs in the SIEM were still available.

Lane 1

LE analysed the network traffic with support from the MS A national CSIRT. The logs clearly showed the volume of traffic to the server in MS D.

LE of MS A reached out to their contacts in MS D (with the support of Europol) requesting to seize the server and collect the evidence. Unfortunately, the hosting company, a bulletproof hoster, did not respond to the request. LE then attempted to get a warrant for the server.

Together with the information from the MS A national CSIRT, the LE created a timeline of events.

Lane 2

Based on the alert data of the CSIRT of the Ministry of Education of MS A, LE identified the hosting company where the website was offering the sensitive information. LE contacted their peers in Country Z (with the support of INTERPOL) to formally request the server be seized and investigated. They used the evidence received from the agency to support their case.

Criminal investigation in MS D

Lane 1

LE in MS D was able to identify the individuals that registered and set up the website and VPS. An investigation of the activity on the server showed that it was accessed multiple times via IP addresses belonging to VPN nodes, but also included one residential IP address from MS D. This most likely occurred after a glitch of the VPN killswitch exposed the IP of the user behind

the VPN. The activity on the server corresponded with the victim's VPN login attempts of stolen credentials.

Most of the logs included VPN node accesses, but also had one residential IP address from MS D, most likely after a glitch of the VPN service which exposed the IP of the user behind the VPN. The activity on the server corresponded with VPN login attempts of stolen credentials.

The server also had temporary copies of some of the sensitive documents, sorted according to the collection date.

The server in MS D, however, did not show any activity related to the server in the Country Z.

Lane 2
LE was unable to collect the server in Country Z because, by the time the hosting company received the request, the owners of the server had destroyed their VPS server.

However, LE was able to identify the individuals that purchased the VPS at the hosting company.

LE investigation did take different screenshots of the website before the server's destruction. These screenshots showed the nature of the site's documents, along with the methods used to request money to access the website.

LE / Prosecutor requested a warrant and seizure of the electronic devices of this individual.

LE investigation of the computers of the individuals in MS D showed that their devices contained traces of the sensitive documents. An examination of the SSH history, browser and e-mail activity also revealed frequent access to the server in Country Z.

The investigation also showed frequent open-source IM (instant messaging) conversations with another individual in MS D, not linked to the website in MS D but seemingly with a form of control on the server in Country Z.

The forensic investigation of these electronic devices showed that this individual had configured and set up the server in Country Z. The e-mail conversation stored on the devices showed an exchange of the content of the documents and methods of payment.

3.1.3 Tasks

3.1.3.1 Task 1: Identify and describe the organisational profile

This task requires the students to identify and describe the organisational profile; specifically, the main subjects (actors) involved in the scenario, in particular, CSIRT/LE and judiciary actors.

Some examples of subjects(in column 1), whether they belong to CSIRT/LE/judiciary (column 2), and their roles (column 3). related to the scenario, are provided in the figure below. The last column (column 4) can be used to note additional comments.

Figure 7: Subjects/Roles – Examples

Subjects	Community (CSIRT, LE, Judiciary, other)	Specific role related to the scenario	Comments
Security team of the Ministry of Education of MS A	CSIRT	First responder Mitigates and responds to this incident targeting the Ministry of Education	
National CSIRT of MS A	CSIRT	Provides early-warning alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents (such information might also be relevant for the specific incident) Shares information (tactical and operational intelligence; indicators and TTPs of attackers), with other national CSIRTs from other countries that might also be relevant for the incident	Also a government CSIRT might be present in MS A and might play a role. But no information on this is provided in the scenario.
LE of MS A	LE	MS A LE carries out the investigations aiming at collecting information and evidence to determine whether a crime has been committed and by whom Give insight to prosecutor on how relevant information sharing is	
Judiciary of MS A	judiciary	The prosecutor in charge of the case in MS A coordinates and supervises criminal investigations to determine whether a crime has been committed and by whom and formulates the charge The judge of MS A assigned to the case will decide, based on the evidence provided, whether a crime has been committed and by whom and guarantees that the whole investigation and trial complies with civil liberties and the rights of persons charged with a criminal offence The judiciary gets in contact and coordinates the investigation with their relevant counterparts in the other MSs and in Country Z	
National CSIRT of MS B	CSIRT	Shares information, with other national CSIRTs from other countries that might also be relevant for the incident	
National CSIRT of MS C	CSIRT	Shares information, with other national CSIRTs from other countries that might also be relevant for the incident	
National CSIRT of MS D	CSIRT	Shares information, with other national CSIRTs from other countries that might also be relevant for the incident	
National CSIRT of MS Z	CSIRT	Shares information, with other national CSIRTs from other countries that might also be relevant for the incident	
LE of MS B	LE	Supports LE of MS A to collect evidence that might be stored in Country B	
LE of MS C	LE	Supports LE of MS A to collect evidence that might be stored in Country C	
LE of MS D	LE	Supports LE of MS A to collect evidence that is stored in Country D	
LE of MS Z	LE	Supports LE of MS A to collect evidence that might be stored in Country Z	
Judiciary of MS D	Judiciary	Guarantees the investigation that might be conducted in MS D complies with civil liberties and the rights of persons charged with a criminal offence	

3.1.3.2 Task 2: Describe measures that CSIRT and/or LE can take to prevent the incident/crime

This task requires the students to describe the measures that CSIRT and/or LE take to prevent the incident/crime.

Although the actual preventive measures for the prevention of the incident, such as implementing proper security controls and network segmentation were already in place, there are a couple of additional activities where CSIRT and/or LE can play an active role. Taking into account the SoD matrix in Annex B and especially the phase “prior to incident/crime”, which activities can you identify?

An example of table to be used to capture duties related to the “prior to incident/crime” phase (column 1) and the suggested measures (column 2) is provided below. The last column (column 3) can be used to note additional comments.

Figure 8: Duty/suggested measure – Example

Duty (task)	Suggested measure	Comments
Analysis of vulnerabilities and threats	The fake website and the fake persona can be detected by monitoring the certificate transparency list, monitoring registered domain names and crawling social media sites for assets and keywords of interest. CSIRT can provide the technical expertise to set up an intelligence data feed to LE. The certificate transparency list (http://www.certificate-transparency.org/what-is-ct) is the stream of all the issued certificates, for example, used on websites.	
Collect cyber threat intelligence	n/g CSIRT can use tools such as AIL to receive early alerts on possible breaches of their constituency.	
Collect cyber threat intelligence	LE can process and analyse the received data and complement this data with their own risk assessment of potential victims, for example, government agencies or critical infrastructure	This can also be supported via a cybersecurity act or similar, to enable the immediate effective bilateral transfer of information on threats
Advising potential victims on preventive measures against cybercrime	LE and CSIRT can compile advice on finding a balance between making the Ministries (and other government sites) accessible to the public without disclosing too much information, potentially useful for attackers. Review the websites and the displayed information. Is there a necessity to display for example, fixed line, office location and mobile phone number on public infrastructure?	
Advising potential victims on preventive measures against cybercrime	CSIRT can provide advice on proper network segmentation and security measures. For example, on how to handle systems with sensitive information. This advice can include guidelines on logging best practices. Additionally, LE can provide input on cybercriminal TTPs	CSIRT and LE can create joint documentation on security hygiene on the one hand, and making systems/network forensic ready on the other hand

3.1.3.3 Task 3: Use the SoD Matrix to analyse possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary

This task requires the students to familiarize themselves with the SoD matrix and use it to analyse possible duties (tasks), synergies and interferences between CSIRT, LE and the

judiciary, related to the scenario. The SoD matrix is available in Annex B together with an explanation of how to use it[35].

In particular, students are asked to select some duties from column 1 of the SoD in Annex B and in relation to some of these duties, briefly describe the measures that could be taken by each community in the scenario.

Below is an example of duties (tasks) (column 1, with duties taken from column 1 of the SoD matrix in Annex B) and related synergies and potential interferences (column 2) related to the scenario provided. Column 3 can be used to add comments.

Figure 9: Duties, synergies and potential interferences – Example

Duty (task)	Synergies and potential interferences	Comments
Collect cyber threat intelligence	LE can process and analyse the received data and complement this data with their own risk assessment of potential victims, for example, government agencies or critical infrastructure. On the other hand, this can also influence the level of trust of other CSIRTs.	
Advising potential victims on preventive measures against cybercrime	CSIRT and LE can create joint documentation on security hygiene on the one hand, and make systems/network forensic ready on the other hand	
Leading the criminal investigation	The incident spans multiple nations and regions. LE and judciary can facilitate the work across nation-states via the collaboration of Interpol/Europol. This can ensure swifter seizure of the evidence. On the other hand, CSIRTs might choose to contact the hosting facility directly, possibly via informal channels or via, for example, FIRST or TI. This can result in a faster take-down, but also in a higher risk of losing crucial evidence.	
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	The CSIRT can, for example, implement network filters to contain the incident, but can have as a side-effect the destruction of evidence. This is the case in the scenario where the malware attempts encrypting the data once network filtering is in place.	
Mitigation of an incident	Similar to the previous task	
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	The leak of sensitive information might require the victim to inform other stakeholders. However, this can result in these stakeholders 'searching' for the same traces of the attackers in their network, possibly tipping them off.	
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling	In line with the previous measure, the CSIRT of the victim can create threat events to be shared with other CSIRTs and describe how the information should be handled and acted upon, for example, no obvious or intrusive actions in the environment which could alert the attackers.	
Discovery of the cybersecurity incident/crime	The CSIRT can analyse the collected samples/malware. The risk is that a sample is shared in error with public resources such as Virustotal. This can alert attackers and cause them to clean up traces of other intrusions not yet detected by victims.	

[35] See also See https://github.com/enisaeu/CSIRTLEA/tree/main/SoD-Matrix

3.1.3.4 Task 4: List possible measures that CSIRT and/or LE can take during the incident response/crime investigation while performing the different duties

This task requires the students to list possible measures that CSIRT and/or LE can take during the incident response/crime investigation while performing different duties.

A table can be used for this exercise. Column 1 should be used to list the duties (tasks) taken from the SoD matrix in Annex B, in particular duties during the incident/crime (duties 7 to 22 of the SoD matrix in Annex B). Column 2 should be used for the suggested measures related to each duty with specific reference to the scenario. Column 3 could be used for comments.

Two examples of filled-in tables for duties and related suggested measures are provided below.

Figure 10: Duty/suggested measure – Example 1

Duty (task)	Suggested measure	Comments
Discovery of the cybersecurity incident/crime	CSIRT and LE learn and use the ATT&CK mapping as a framework to layout possible attacker actions and follow-up investigations	
Identification and reporting of crimes	LE computer intrusion and leak of confidential data	
Collection and sharing evidence	CSIRT collects system logs, network logs and e-mail logs LE informs that the screenshots as such are not enough and that more evidence might be needed. Ideally, the evidence also contains the full web pages together with their metadata.	
Identification and classification of the cybersecurity incident/crime	CSIRT/LE identify and classify the incident/crime	

Figure 11: Duty/suggested measure – Example 2

Duty (task)	Suggested measure	Comments
Identification and reporting of crimes	LE identify the owner of the website and VPS	
Collection and sharing evidence	CSIRT provides network reports; VPN logs; screenshots of the sensitive information CSIRT creates forensic images of the assets;CSIRT deploys EDR to all assets LE analysis of server activity linked to VPN logins LE collects the transaction logs from SIEM LE/Judiciary discuss if taking screenshots of a website is sufficient and whether instead of screenshots, captures of the full web page are needed LE seizes the computers of the individuals in MS D	
Active support to LE	CSIRT provides evidence to LE CSIRT analyses logs and reports CSIRT provides evidence that documents leaked in Country Z contain sensitive information about the agency CSIRT can support the LE during the criminal investigation, e.g. provide technical expertise, some contacts, or information useful for the investigation CSIRTs support the forensic investigation of the workstations	

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	LE discuss with CSIRT why the compromised workstations were not disconnected from the network/server and why imaging/containing the evidence was not done with high-urgency/directly at the machine	
Conducting the criminal investigation	LE investigate conversations LE show the need to clarify "conversations". What did you use? Messaging, e-mail? Topology? Discuss details of the warrant and how to seize the devices	
Authorising the investigation carried out by the LE	Judiciary authorises the seizure and investigation	

3.1.3.5 Task 5: Group discussion on balancing the incident mitigation (asset protection) and the criminal investigation (evidence collection and preservation)

This task requires the students to discuss together the issue of balancing the incident mitigation (asset protection) and the criminal investigation (evidence collection and preservation) with reference to the scenario.

One of the responses of the CSIRT of the Ministry of Education of MS A involves filtering outgoing network activity to the attackers, effectively preventing the further exfiltration of sensitive information. This filtering is an understandable activity, certainly as a short-term containment measure. The side-effect of this measure, however, triggers the malware and results in encrypted workstations, and as such a loss of evidence.

The students will need to discuss the pros and cons of short-term containment actions to protect the victim, but which might alert the attacker that they have been detected. In general, this depends on the type of incident and the victim.

As a reference, the courses of action matrix from Lockheed Martin[36] can be used. This action matrix includes two significant categories of actions:

- passive (Discover and Detect)
- active (Deny, Disrupt, Degrade, Deceive and Destroy)

Note that this discussion is not about the chain of custody as such, but rather which options to choose for either taking an active or passive approach in containing an incident.

[36] Eric M. Hutchins E. M., Clopperty M. J., Amin R. M., *Lockheed Martin Corporation Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (retrieved on 20 October 2020).

Figure 12: Examples of activities to discuss, including their advantages and risks

Activity	Advantage	Risk
(Active) **Deny traffic by network filtering**	Limit data exfiltration; prevent leakage of sensitive information, with possible financial or (national) security consequences Prevent further infection. It's not clear how the malware behaves. Similar to 'traditional' ransomware, it might require additional network activity to spread further	The attackers are informed their activities have been detected which can lead to retaliation or destruction of evidence Retaliation can be severe if the scope of the infection is not fully known. There might be other remote access features installed by the attacker and not yet detected. Retaliation can also lead to 'public shaming' of the victim or potentially to a DDoS, for example
(Passive) **Discover and observe activity**	CSIRT and LE can learn more about the objectives, goals and techniques of the attacker Understand the full scope of the incident Extract additional indicators and share this information via trusted channels with potential victims in the same region and/or sector	
Safeguard logs	The CSIRT instructed the SOC to safeguard the logs of the affected assets in their SIEM. This guarantees that, even if the original workstations are un-recoverable, there are still a set of relevant logs. It also prevents logs from being overwritten (rotated) accidentally.	If the incident is far-spread in the victim environment, the attacker might have noticed this activity or the communication and already started erasing logs and removing evidence.

3.1.3.6 Outcomes

The scenario illustrates the roles, synergies and potential interferences in incident handling and criminal investigation of confidential data theft.

3.1.4 Lessons Learned

Theft of confidential data is rather complex and demands different skills, including technical and legal.

Although for training purposes the scenario is presented as less complicated than real cases might be, it still allows each party to understand the complexities in terms of actors involved, roles played, duties (tasks) performed, synergies to exploit, and risks of interference.

3.2 CASE STUDY 2: RANSOMWARE

Figure 13: Overview of the case study 2

Overview of case study 2	
Targeted Audience	This exercise is useful for incident responders and members of law enforcement of all experience levels. It is particularly helpful for national CSIRT members and law enforcement officers involved in cybercrime investigations.
Total Duration	45 minutes
Scenario	This is a group exercise. Each trainee is a member of either a CSIRT team and/or law enforcement that is involved in the prevention, mitigation and investigation of cybersecurity incidents. Their goal is to address the key ramification of a ransomware attack against the municipal hospital.
Task 1	Notification of the incident
Task 2	Setting up the task force, division of duties
Task 3	Possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary
Task 4	Incident handling, evidence collection, cooperation
Task 5	International cooperation and information sharing
Task 6	Post-incident preventive measures

Where possible, this case study should be conducted in groups so that the different results and approaches of each group can be compared. Then, the advantages and disadvantages of individual solutions should be discussed.

3.2.1 Objectives

In this exercise, the trainees will learn when and how CSIRT members cooperate with LE. In particular, the objectives of the exercise are to:

- Explain CSIRT and LE cooperation in a health sector-related ransomware scenario
- Raise the trainees' awareness regarding the differences between the legal systems of various countries and the consequences of these differences
- Understand and appreciate the specifics of CSIRT/LE activities
- Practice setting up and coordinating a task force for dealing with large scale attacks
- Provide information on how to cooperate and share information
- Practice how to identify and propose post-incident reactive and preventive measures

3.2.2 Scenario

3.2.2.1 Setting the stage

A ransomware attack has been discovered in a large municipal hospital on the hospital patient records servers. All computers are locked and display a message indicating that the files have been encrypted; the hacker is demanding 11 bitcoins (approx. €100,000) to provide the decryption key. The image on the computer screens also states that if the payment is not received within five days, the price will increase. Within ten days, the patient data will be erased on the servers and leaked to a public website, and a notification will be sent to the national data privacy agency.

You are a member of a task force established to help the hospital's network and information security team to deal with the incident. You have been assembled; it is now 05:45. It appears that all significant servers are affected. An initial assessment shows that the hospital email system and patient record systems are inaccessible, and the hospital intranet sites are also unavailable.

Figure 14: Graphical representation of scenario 2 – Attack

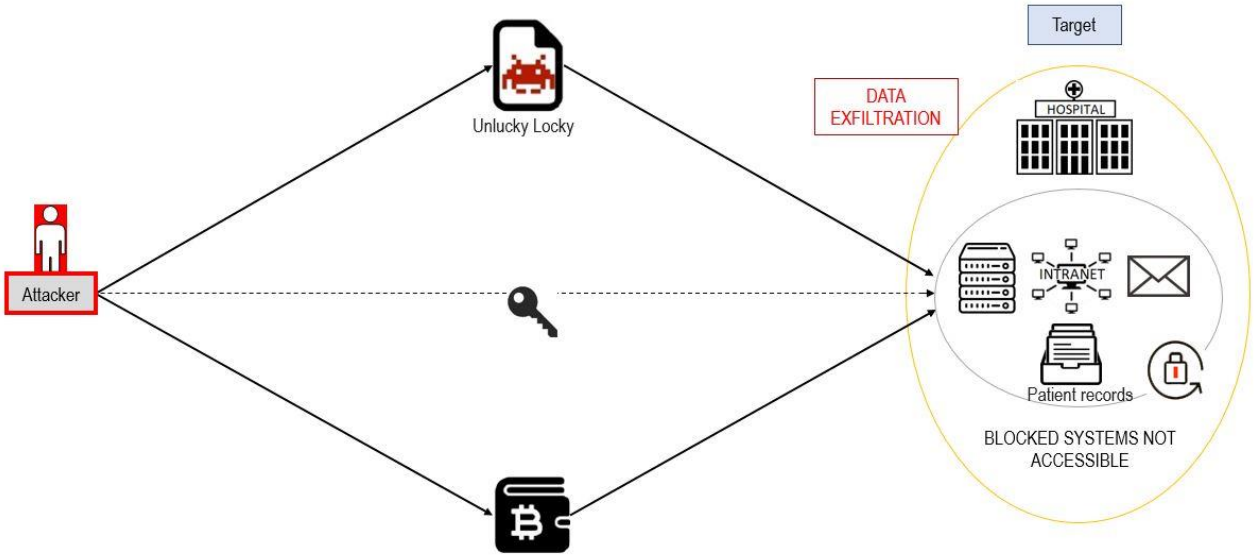
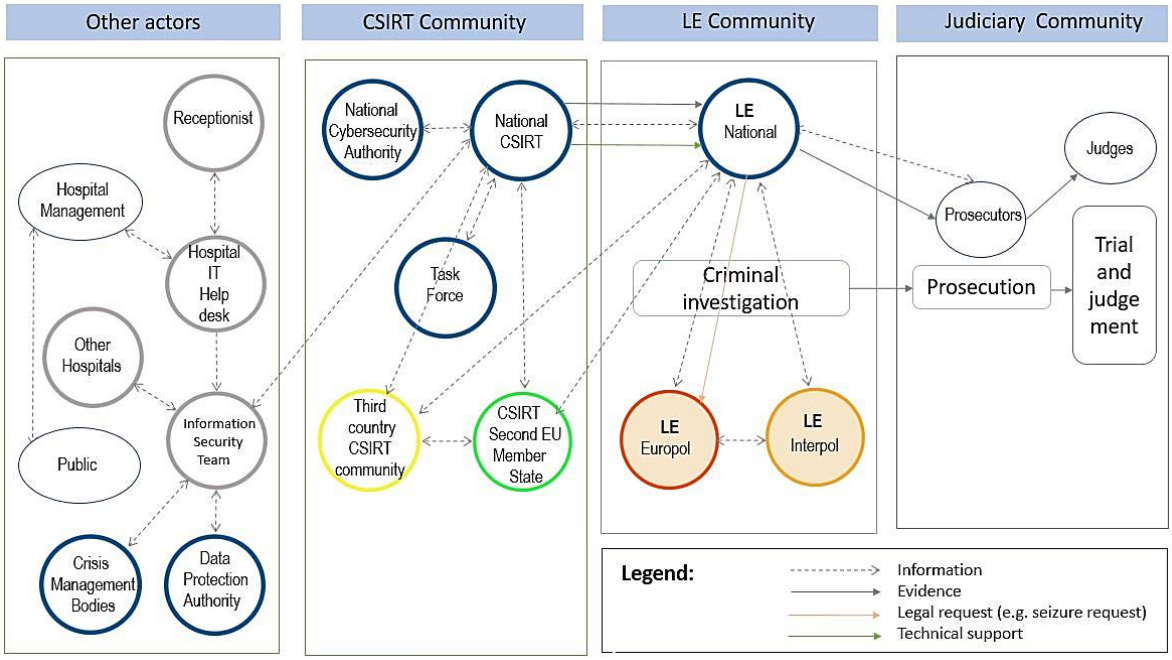


Figure 15: Graphical representation of scenario 2 – Overview of interactions



3.2.2.2 Organisational profile

The hospital is the largest municipal hospital in your area. Last year the hospital took care of almost 1 million patients and had about 5,000 employees. As such, the hospital relies on a network with up to 10,000 connected devices, which includes workstations, diagnostic tools and servers storing patients' data. Outside exposure is important through several hundreds of public IP addresses. In recent years, hospital management was somewhat reluctant to invest in cybersecurity, and even though most computers are relatively well taken care of, some, especially those operating specialised equipment, are running legacy systems like Windows XP, due to compatibility issues. The network is not segmented, and critical systems are in the same network as specialised equipment, as well as all workstations. The hospital has no clear rules on data management and backup. Patient data that are stored in the hospital's information systems are backed up and protected from ransomware. Still, a lot of relevant data about currently hospitalised and treated patients are not stored in the information systems, but on the doctors' workstations, which are not being backed up.

3.2.2.3 Before the breach

The COVID-19 pandemic is still very much going on, which leads to heavy pressure on your country's hospital system. Some cybercriminals decided to take advantage of this situation and started targeting medical facilities with their ransomware campaigns. The hospital's security team issued and distributed a directive that explained this threat to the employees and informed them how to be cautious and prevent their devices from getting infected with malware.

3.2.2.4 Initial response

Breach notification

When a receptionist in the X-ray department tried to log in at the start of her shift, she could not open the files and a message indicating that the files have been encrypted appeared on her screen. She notified a supervisor who then called the hospital's IT helpdesk to report what happened, who in turn notified the hospital's network and information security team.

The response of the CSIRT team

The hospital's network and information security team handler received the alert from the hospital staff and identified it as a high priority threat. The handler classified it according to the ENISA RSIT[37] as an incident of "Information Content Security", "Unauthorised modification of information", caused by the ransomware.

From an initial analysis, it appeared that the ransomware was called UnluckyLocky, a new type of ransomware with limited online information. Therefore, it was assumed that there was no known decryption key. The handler uncovered a news report online that described another hospital that seemed to have been infected by a similar attack with ransomware named Gotcha. The news article suggested that the response to the incident was slow and that almost all the computers and servers were infected. Additionally, the public was made aware of the incident as it had a significant impact on the hospital not being able to offer essential services. The incident went on for six days during which time even the hospital's most basic functionality was forced to stop.

The handler then attempted to identify the source of the ransomware with the limited publicly available information on UnluckyLocky published by the respected security company.They were able to find out that the source was a malicious website that informed about the Covid-19 pandemic and offered for download a tool for analysis of the decease symptoms. The executable, however, contained malicious code that was executed by the user who downloaded it from the website.

Technique T1204 - User Execution[38]	"An adversary may rely upon specific actions by a user to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behaviour from forms of Phishing." [39]

Upon execution, the malware first enumerated and exfiltrated data, then encrypted the data within the target computer system and any connected storages. This rendered most of the data unavailable to the user while still allowing the user to operate the essential functions of the computer system. The malware also regularly prompted a window warning the user that the system was encrypted and decryption keys would be provided upon payment of the ransom.

Technique T1486 - Data Encrypted for Impact[40]	"Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted. In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR." [41]

[37] GitHub, *enisaeu / Reference-Security-Incident-Taxonomy-Task-Force*, https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force (retrieved on 13 October 2020).
[38] MITRE Corporation, *User Execution,* https://attack.mitre.org/techniques/T1204/ (retrieved on 13 October 2020).
[39] MITRE Corporation, *User Execution,* https://attack.mitre.org/techniques/T1204/ (retrieved on 13 October 2020).
[40] MITRE Corporation, *Data Encrypted for Impact*, https://attack.mitre.org/techniques/T1486/ (retrieved on 13 October 2020).
[41] MITRE Corporation, *Data Encrypted for Impact*, https://attack.mitre.org/techniques/T1486/ (retrieved on 13 October 2020).

The malware also regularly launched a task that attempted to spread the malicious code via email messages sent to stored addresses and through legitimate network tool (psexec).

Technique T1053 - Scheduled Task/Job[42]	"Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically requires being a member of an admin or otherwise privileged group on the remote system." [43]

The handler proceeded to analyse the extent of the issue by randomly checking workstations within the hospital for signs of the malware. He found out that the malware managed to spread across the whole hospital, rendering some of the critical data and equipment unavailable.

The hospital's network and information security team was overwhelmed by the attack, so they reached out to the national CSIRT.

Note: In this scenario, you are a member of the national CSIRT that is helping the hospital with this security breach.

Criminal investigation

The national cybersecurity authority reported this incident to law enforcement. The police cyber unit started the investigation. They immediately contacted the national CSIRT, which provided general information, a sample of the ransomware and a link to the source website. A sample was sent to Europol through the EMAS sandbox for crossmatching.

The police found out that the website was hosted by a web hosting provider based in one of the EU MSs. They ordered the provider, via European investigation order, to provide stored subscriber and traffic data related to the relevant account.

Provided data revealed that the malicious content was uploaded from a country outside the EU. Even though the police immediately requested legal assistance and also asked Europol for assistance, based on past experiences with this particular country, it was virtually impossible to get any cooperation in such cases from the official authorities.

Information sharing

Even though it was unlikely that LE would get assistance through official channels, in the third country there is a well-functioning CSIRT community which is regularly and openly sharing information. The national CSIRT involved in dealing with the incident offered LE to request traffic data if they are given identifiers provided by the web hosting provider.

3.2.3 Tasks

3.2.3.1 Task 1: Notification of the incident

As stated above, the hospital's network and information security team notified the national cybersecurity authority of the incident. Who else should be notified within and outside of the hospital? Are there any legal obligations for the hospital to report such incidents to public institutions?

This task requires students to to list individuals, authorities and other parties that should be informed about the incident. A table could be used for this purpose. Column 1 should be used to

[42] MITRE Corporation, *Scheduled Task/Job*, https://attack.mitre.org/techniques/T1053/ (retrieved on 13 October 2020).
[43] MITRE Corporation, *Scheduled Task/Job*, https://attack.mitre.org/techniques/T1053/ (retrieved on 13 October 2020).

list the parties to be notified and column 2 to identify whether the notification is required or recommended. Column 3 can be used for comments. An example of filled in table is provided below.

Figure 16: Notification list – Example

Who to notify	Required/ Recommended	Comments
Hospital management	Recommended	Hospital management needs to be aware of the attack and related possible damages.
Hospital staff	Recommended	All hospital staff should be notified of the breach and provided with guidelines on how to use IT and medical equipment, how to prevent spreading of the malware and who to contact in case of suspected malware infection.
National cybersecurity authority	Required	Any operator of essential services is required to report cybersecurity incident of this kind pursuant to act no. XY
Data protection authority	Required	Any personal data controller is required to report any breach of personal data protection to the DPA in accordance with the GDPR
Law enforcement	Required/ Recommended	In most cases, according to the competent legal framework, it is required to report cybercrimes to LE, but even when it is not mandatory, it is recommended
Crisis management bodies	Required/ Recommended	The government is dealing with the COVID-19 pandemic and any restrictions on the availability of the hospital capacity needs to be considered within the crisis management processes.
CSIRT network	Recommended	CSIRT networks could not only disseminate information about this specific attack to other threatened organisations, but their members may also have more experience with this kind of attack/ransomware they can share
Other hospitals	Recommended	Other hospitals may face a similar situation should their employees also install the ransomware. By letting them know what happened, you may prevent this from happening elsewhere.

3.2.3.2 Task 2: Setting up the task force, division of duties

While in the context of a criminal investigation the prosecutor/judge is in charge of assigning roles for dealing with the investigation of the cybercrime, the national CSIRT may establish a task force to respond to the incident and deal with the crisis generated by the incident.

The national cybersecurity authority decided that a task force should be established to deal with the crisis. The purpose of the task force is not to govern the investigation but rather to consult and coordinate the incident response. Who should be involved in this task force (e.g. which organisations or [inter]national authorities, the expertise level of members of the task force)? Are there any rules on this in your country?

This task requires students to use a table to list individuals/organisations that should be involved in the task force. Column 1 should be used to list the parties to be involved, column 2 to identify what kind of expertise can they contribute and column 3 to identify which tasks they can be involved in and what role should they play. Column 4 can be used for comments. The students can then discuss whether there are any relevant rules or best practices on this in their countries. An example of filled in table is provided below.

Figure 17: Task force members list - Example

Organisation	Expertise	Tasks/Role	Comments
Hospital	Management CSIRT members Systems operators	Management – executive decision making CSIRT – incident mitigation, coordination of activities within the organisation Operators – knowledge of the infrastructure, involvement in incident mitigation	
National Cybersecurity Authority	Incident handlers Liaisons	Incident handlers – support to the hospital CSIRT, information sharing with the community Coordination with other authorities and stakeholders	
Law enforcement	Investigators Forensic Experts	Investigators – evidence collection, investigation of criminal activities, information sharing with other LE Experts – technical support to investigators, evidence collection	
Crisis management bodies	Liaisons	Coordination with national crisis management bodies	

The university that cooperates with the hospital offered their volunteer ICT experts (students and employees) who can help to deal with the crisis. Can they be involved? In which activities (e.g. reinstallation of hospitals computers, incident handling, attempting to break the encryption, track the source of the attack, etc.)?

This task requires students to explain which activities related to the incident handling can volunteers be involved and how. A table can be used where Column 1 should be used to name the activity and column 2 to describe the involvement. An example of filled in table is provided below.

Figure 18: Involvement of volunteers – Example

Activity	Description
Systems repair	Most volunteers would probably be involved in simple tasks like reinstallation of workstations, etc.
Advanced activities	Selected volunteers could also be involved in advanced tasks – in such cases, the task force should consider if their involvement could interfere with activities of the CSIRT and/or LE, who should they cooperate with and how to deal with legal limitations. Volunteers that have access to sensitive information or personal data need to sign at least an NDA and, in some cases, should be vetted to some extent (e.g. clear criminal record, recommendation, etc.)

3.2.3.3 Task 3: Possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary

This task requires the students to familiarize themselves with the SoD matrix and use it to analyse possible duties (tasks), synergies and interferences between CSIRT, LE and the judiciary, related to the scenario. The SoD matrix is available in Annex B together with an explanation of how to use it.

In particular, the students will be asked to select some of the duties from column 1 of the SoD in Annex B and with some of these duties, briefly describe the measures to that could be taken by each community in the scenario.

A table can be used to list the duties (tasks) in column 1 (to be taken from column 1 of the SoD matrix in Annex B) and describe synergies and potential interferences in column 2. The last column, column 3, can be used to add comments. A example of filled in table is provided below.

Figure 19: Duties, synergies and potential interferences – Example

Duty (task)	Synergies and potential interferences	Comments
Collect cyber threat intelligence	LE can process and analyse the received data and complement this data with their own risk assessment of potential victims, for example, government agencies or critical infrastructure. LE can crossmatch collected data with known TTPs. On the other hand, this can also influence the level of trust of other CSIRTs.	
Advising potential victims on preventive measures against cybercrime	CSIRT and LE can create joint documentation on security hygiene on the one hand, and making systems/network forensic ready on the other hand	

3.2.3.4 Task 4: Incident handling, evidence collection, and coordination

Experts in the task force found out by using sandbox analysis that the ransomware is not only encrypting data from the information systems but is also exfiltrating patient data outside the organisation. CSIRT members immediately proposed to block communication to the C&C server to prevent further disclosure of sensitive information. LE, however, suggested to wait with this measure and try to track the data in an attempt to locate the attacker, since they're suspecting that the attacker is based in the EU even though he used servers located in third countries to disseminate the malware.

This task requires students to explain how they would deal with this issue, what should have priority (protecting sensitive data or locating the attacker), and whether there are any official rules on this in their country.

A table can be used to list the duties (tasks) in column 1 (to be taken from column 1 of the SoD matrix in Annex B) and the measures to be taken to deal with the issue in column 2. The last column of the template below, column 3, can be used to add comments. Following, an example of fill in table is provided.

Figure 20: List of suggested measures to deal with mutual interferences – Example

Duty (task)	Suggested measure	Comments
Mitigation of an incident	Deny traffic by network filtering. This will limit further data exfiltration but can potentially inform attackers they have been discovered. This can then lead to retaliation. Retaliation can be that the attackers "publish" the incident (public shaming). Learning "more" about the attacker's location can only be done if LE can access the C&C server and do the investigation on the server, or via the hosting company. The "location" of the C&C server is known because you have the IP address or hostname and can look up where it is hosted/located.	This is similar to Task 5 in the first scenario
Evidence collection	Capture the network traffic to learn more about which techniques or tools the attackers are using.	Hopefully, the network traffic is not encrypted; most likely, it is not; otherwise, you would not be able to know that patient data is leaking.
Identify the type and severity of the compromise	Redirect the traffic to a system under the control of the victim. This prevents further exfiltration, but the ransomware still 'thinks' everything is ok. This allows learning more about how the ransomware works without keeping the 'flow' open for exfiltration. One of the extra learning objectives (this is also the case for the previous measure) is that you can maybe discover additional C&Cs 'programmed' in the malware. The ransomware can contain different C&C servers and be programmed to try the next one if the first fails. This is also the case for filtering traffic.	
Mitigation of an incident	Filter the network traffic from the internal network to the C&C server but "replay" a set of captured network traffic to the attacker. Careless attackers will then maybe think that the exfiltration is still happening, allowing LE to progress with accessing the C&C server hosting company	
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	Share the exfiltration IP address or domain name with other stakeholders in the health sector?	

3.2.3.5 Task 5: International cooperation and information sharing

As stated above, the CSIRT offered LE, they can ask the third country network operators to unofficially provide traffic data that could help to identify the attacker.

This task requires students to explain whether LE would be able to provide the CSIRT with necessary identifiers and traffic data acquired from the web hosting provider for this purpose. Also, whether the unofficial data collected by the third country network operator that leads to identifying the attacker would be usable as evidence in court by LE. An example of information sharing and use is provided as following.

Figure 21: Information sharing and use – Example

Information sharing and use
Sharing information with the CSIRT Although this might vary depending on the legal systems, in exceptional cases, it is possible to share information collected during a criminal investigation with other parties. This can be done only with the consent given by the public prosecutor, and only the data necessary can be shared. In some cases, it is impossible to share the information without permission from the operator that provided it to LE. This will be decided based on criminal procedure law in each MS. **Use of the data unofficially obtained by the CSIRT** This largely depends on legal regulation and customs in the individual country. In most countries, the evidence is admissible when it is obtained legally and followed procedural rules. However, in this case, the reliability of the evidence could be questioned since it is obtained from unofficial sources. So the court would have to decide on admissibility as well as reliability of such evidence.

3.2.3.6 Task 6: Post-incident preventive measures

This task requires students to explain, based on information they have about the incident and hospitals systems, what kinds of post-incident preventive measures they would recommend to the network and information security team to implement.

A table can be used to categorise proposed measures in column 1 (whether these measures are organisational, technical or legal by nature), and list and describe the proposed measures in column 2 and 3. The last column of the template below, column 4, can be used to identify who should implement these suggested measures. An example of filled in table is provided below.

Figure 22: List of preventive security measures – Example

Category (e.g. organisational, technical, legal)	Measure	Description	To be implemented by
Organisational	Update of security policies	Internal policies of the hospital proved to be insufficient and ineffective in dealing with this kind of incident, the management in cooperation with the CSIRT should therefore draft new policies setting up processes for prevention, detection and mitigation of such security incidents	Hospital management, CSIRT
Organisational	Training of the staff	The staff did nott know how to behave and handle IT equipment in case of such incident, so the management in cooperation with CSIRT and systems operators should provide staff with training focused on IT security	Hospital management, CSIRT, systems operators
Technical	Segmentation of hospital network	The network is not segmented. Separation of critical systems from specialised equipment, and other work stations would have increased the minimise the vulnerability.	CSIRT
Technical	Implementation of shared SOC	A key element to ensure that the technology and platforms used sync well with the information systems across the different organisations.	Hospital CSIRT, national CSIRT, regional SOC operator
Legal	Review of existing outsourcing agreements	In some cases such incidents prove the inability of suppliers to act; therefore the organisation should review existing agreement whether they include a provision on what kind of assistance can the organisation expect in case of a security incident involving outsourced systems/services.	Hospital management

3.2.3.7 Outcomes

The scenario illustrates the roles, synergies and potential interferences during the incident handling and criminal investigation of a ransomware scenario.

3.2.4 Lessons Learned

Ransomware cases are rather complex and demand many different skills, including technical and legal, as well as the ability for other communities to share information and cooperate.

Although for training purposes the scenario is presented as less complicated than real cases might be, it still allows each party to understand the complexities in terms of actors involved, roles played, duties (tasks) performed, synergies to exploit, and risks of interference.

3.3 CASE STUDY 3: DDOS AND MALWARE BLENDED ATTACK

Figure 23: Overview of case study 3

Overview of case study 3	
Targeted Audience	This exercise is useful for incident responders and members of the law enforcement of all experience levels. It is particularly helpful for national CSIRT members and law enforcement officers involved in cybercrime investigations.
Total Duration	30 minutes
Scenario	This is a group exercise. Each trainee is a member of either the CSIRT team and/or law enforcement who is involved in the prevention, mitigation and investigation of cybersecurity incidents. Their goal is to address the key ramification of a DDoS and malware blended attack against a large size airport in a European capital city.
Task 1	Notification of the incident
Task 2	Setting up task force, division of duties
Task 3	Possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary
Task 4	International cooperation and information sharing
Task 5	Post incident preventive measures

This case study should be conducted in groups so that different results and approaches of each group can be compared. Then, the advantages and disadvantages of individual solutions should be discussed.

3.3.1 Objectives

The current exercise scenario aims to familiarize the trainees with technical, procedural and legal aspects of incident management. In particular, the objectives are to:

- Raise awareness about what types of cyber incidents might affect an airport and what can be the impact of such incidents
- Learn about the role of the CSIRT, law enforcement, and National Cybersecurity Authority,
- Understand the importance of efficient coordination between main stakeholders during a large scale/high impact incident
- Practice setting up and coordinating task force for dealing with large scale attack
- Understand the importance of information sharing during cybersecurity attacks
- Practice how to identify and propose post-incident reactive and preventive measures
- Learn about preventive measures against such type of incidents

3.3.2 Scenario

3.3.2.1 Setting the stage

A large size airport in a European capital city is under massive DDoS attack, combined with a malware attack, causing key systems outages and malfunctioning (i.e. systems assuring functions like flight scheduling, passengers' check-in, baggage routing, etc.).

Already the situation has had significant adverse effects on the airport's operations and safety. Undetected attacks resulted in the change of the flight plans provoking delays and influencing the aircrafts cleaning and fuelling process, as well as the time required to load the luggage, affecting the world-wide traffic.

You are a member of a task force established to help the airport company to deal with the incident. An initial assessment shows that the IT team has yet to come up with a course of action for stopping the attack and restoring the services. The pressure from the media, authorities, and passengers is rapidly growing.

Figure 24: Graphical representation of scenario 3 – Attack

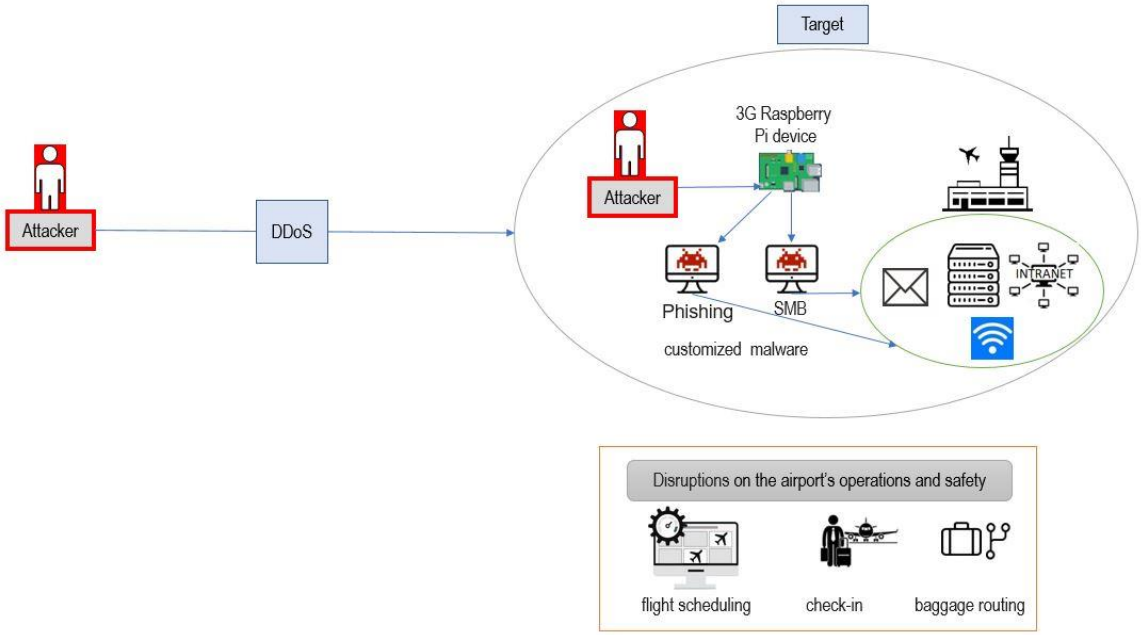
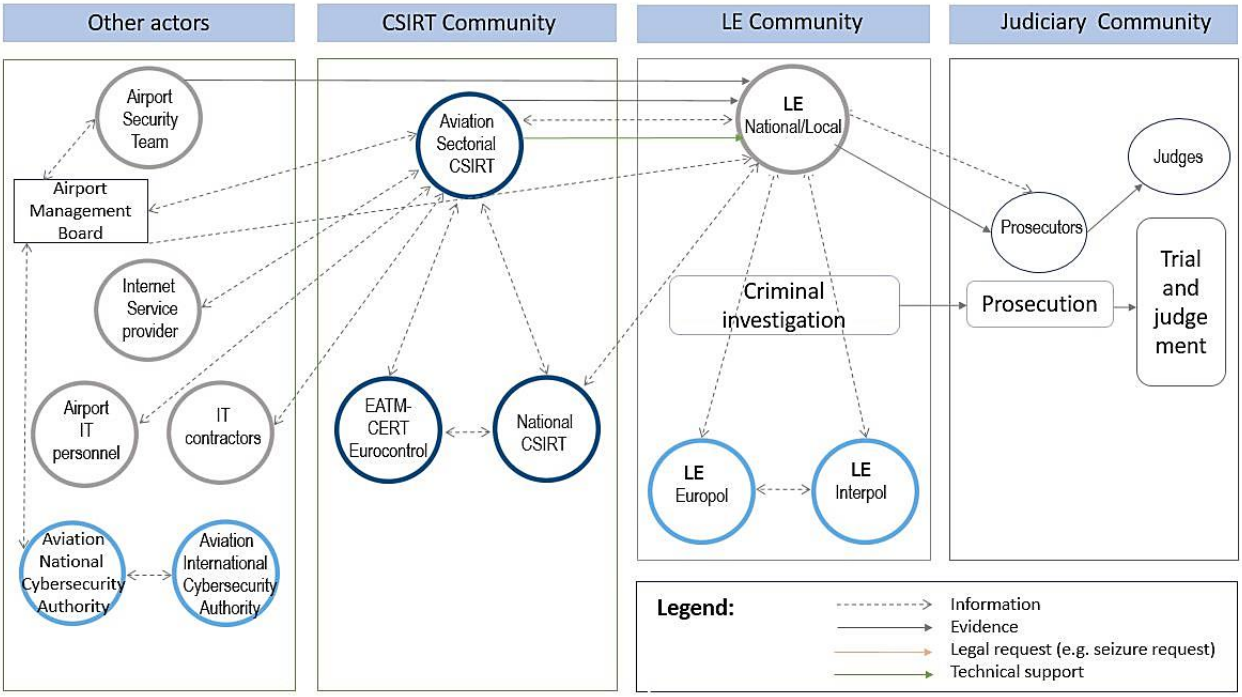


Figure 25: Graphical representation of scenario 3 – Overview of interactions



3.3.2.2 Organisational profile

The affected airport is one of the biggest air traffic hubs in Europe, with an average of more than 100,000 passengers passing through per day.

The management of the airport invested only in perimetral security in recent years (firewalls, gateways, etc.). At the same time, internal network suffers from lack of proper segmentation, and some of the critical systems are running old operating systems due to legacy and compatibility constraints.

The airport is running its own on-prem data centre doubled by a disaster recovery site, but the BCP plan wasn't tested in the last two years.

3.3.2.3 Before the breach

The attackers gathered information online about the airport company and identified useful data: the IP addresses space, systems and applications, management and key personnel names and contact details, etc.

Reconnaissance was also done at the physical perimeter of the airport by attackers disguised as passengers.

Attackers managed to plant a rogue 3G Raspberry Pi device in the airport network. The device is used to sniff the network traffic for systems discovery and credentials extraction (plain-text credentials sent over the network or easy-to-crack hashes).

While the attacker created a diversion with the DDoS attack, some of the internal systems of the airport were infected with a customized malware delivered using two different infection vectors: spear-phishing emails sent from the rogue device to avoid email gateway filtering, and Windows SMB exploits launched from the same device.

Technique TA0015 – Technical information gathering[44]	"Technical information gathering consists of the process of identifying critical technical elements of intelligence an adversary will need about a target in order to best attack. Technical intelligence gathering includes, but is not limited to, understanding the target's network architecture, IP space, network services, email format, and security procedures".[45]
Technique TA0016 – People information gathering[46]	"People Information Gathering consists of the process of identifying critical personnel elements of intelligence an adversary will need about a target in order to best attack. People intelligence-gathering focuses on identifying key personnel or individuals with critical accesses in order to best approach a target for attack. It may involve aspects of social engineering, elicitation, mining social media sources, or be thought of as understanding the personnel element of competitive intelligence".[47]
Technique T1465 – Rogue Wi-Fi access points[48]	"An adversary could set up unauthorized Wi-Fi access points or compromise existing access points and, if the device connects to them, carry out network-based attacks such as eavesdropping on or modifying network communication".[49]
Technique T1566.001 – Spearphishing attachment[50]	"Adversaries may send spearphishing emails with a malicious attachment in an attempt to elicit sensitive information and/or gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution".[51]
Technique T1210 - Exploitation of Remote Services[52]	"Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system."[53]

3.3.2.4 Initial response

Breach notification

A lot of people are reporting at the check-in desks that their flights seem to have disappeared from the schedule display systems or they have long delays. At the same time, people can't obtain information from other online sources because the internet is inaccessible from the airport Wi-Fi network and even if they use their 3G/4G/5G connection the airport website and other related platforms are unavailable.

It becomes clear that the IT infrastructure and applications are affected by an incident, and a cyber-attack is suspected. The network team starts to investigate, and they report that a huge DDoS attack is conducted against the airport's internet-facing systems.

The security team is also reporting that a high number of database operations were executed in a short interval of time using credentials of a user that is claiming to know nothing about the situation.

[44] MITRE Corporation, *Technical information gathering,* https://attack.mitre.org/techniques/TA0015/ (retrieved on 13 October 2020).
[45] MITRE Corporation, *Technical information gathering,* https://attack.mitre.org/techniques/TA0015/ (retrieved on 13 October 2020).
[46] MITRE Corporation, *People information gathering,* https://attack.mitre.org/techniques/TA0016 (retrieved on 13 October 2020).
[47] MITRE Corporation, *People information gathering,* https://attack.mitre.org/techniques/TA0016 (retrieved on 13 October 2020).
[48] MITRE Corporation, *Rogue Wi-Fi access points,* https://attack.mitre.org/techniques/T1465 (retrieved on 13 October 2020).
[49] MITRE Corporation, *Rogue Wi-Fi access points,* https://attack.mitre.org/techniques/T1465 (retrieved on 13 October 2020).
[50] MITRE Corporation, *Spearphishing attachment,* https://attack.mitre.org/techniques/T1566.001 (retrieved on 13 October 2020).
[51] MITRE Corporation, *Spearphishing attachment,* https://attack.mitre.org/techniques/T1566.001 (retrieved on 13 October 2020).
[52] MITRE Corporation, Exploitation of remote services, https://attack.mitre.org/techniques/T1210/ (retrieved on 13 October 2020)
[53] MITRE Corporation, Exploitation of remote services, https://attack.mitre.org/techniques/T1210/ (retrieved on 13 October 2020)

The airport management board decides to notify the aviation sectorial CSIRT and to file a complaint to the police.

Technique T1498 – Network Denial of Service[54]	"Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes[1] and to support other malicious activities, including distraction[2], hacktivism, and extortion".[55]
Technique TA0006 – Credential Access[56]	"Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals" [57]

Response of the CSIRT team

The CSIRT Team uses lessons learned from recent similar attacks against airports and starts the Incident Response process with actions meant to contain the incident as much as possible.

The user account responsible for altering the airport databases is disabled, and the user workstation is isolated from the network and sent to the digital forensics laboratory. All recent activity of the user is tracked because there's plausible suspicion that the user was the victim of a spear-phishing attack which resulted in his workstation being infected with malware.

Additionally, the CSIRT team is working with the airport IT personnel, the ISP, airport IT vendors, and international partners to try to come up with a mitigation plan for the DDoS attack. Multiple scenarios are studied, but for the moment it is decided to ask the ISP to filter the traffic coming from outside of the country the airport is located in.

Next, the technical investigation of the incident is started:

- Analyse logs from perimeter security solutions (firewall, web and email gateway, proxy, etc.)
- Analyse the recent activity of the user causing database malicious actions and conduct a forensically sound investigation of his workstation
- Try to identify rogue devices in the network

Criminal investigation

The national cybersecurity authority reported this incident to LE. The local police cyber unit started the investigation by:

- Analysing security video cameras from the airport in the last month to try to identify attackers planting rogue devices
- LE/Prosecutor requesting a warrant and seizure of the electronic devices of possible suspects

Information sharing

The CSIRT is conducting an information exchange about the incident with other CSIRTs (especially the ones in the aviation sector/sectorial CSIRTs), trying to find out if similar attacks

[54] MITRE Corporation, *Network Denial of Service,* https://attack.mitre.org/techniques/T1498 (retrieved on 13 October 2020).
[55] MITRE Corporation, *Network Denial of Service,* https://attack.mitre.org/techniques/T1498 (retrieved on 13 October 2020).
[56] MITRE Corporation, *Credential Access,* https://attack.mitre.org/techniques/TA0006 (retrieved on 13 October 2020).
[57] MITRE Corporation, *Credential Access,* https://attack.mitre.org/techniques/TA0006 (retrieved on 13 October 2020).

were conducted recently and gather information about investigation results and mitigation measures.

In cooperation with the airport management, CSIRT will share the gathered information with the national LE authorities and will offer their further support to continue the investigations and facilitate information exchange nationally and internationally.

3.3.3 Tasks

3.3.3.1 Task 1: Notification of the incident

The airport security team needs to quickly do an initial assessment of the situation and notify the incident according to existing procedures and legal framework.

As previously mentioned, The National Competent Cybersecurity Authority or the National CSIRT is notified.

To whom else and when should the incident be reported?

Some example are provided below.

Figure 26: Notification list – Example

Who to notify	Required / recommended	Comments
Chief Information Security Officer / Head of IT Security	Required	CISO should be informed first about the incident to be able to coordinate the response and further notification measures.
The Management Board	Required	The Airport management needs to be aware of the attack and its current and possible impact.
The IT Manager	Recommended	IT needs to assess the situation quickly and together with the security team come up with a plan for containing the incident and for business continuity.
The Airport Staff	Recommended	All the airport staff needs to be aware of the ongoing incident to be able to follow the procedures for assuring the business continuity and avoid further incident consequences (avoid speaking in public about the incident, pay attention to avoid any other SCAM.Phishing tentative, etc.)
The Public Relations Team/Responsible	Recommended	Effective and coordinated public communication is crucial in such situations when pressure from the media can be overwhelming.
The Police (fill a cybercrime report)	Required /Recommended	It is recommended to report cybercrimes to law enforcement authorities; in some cases, it is even required if conditions stipulated within the procedural criminal law are met.
The Aviation Cybersecurity Authority (national and or international)	Required	The sectorial authority needs to be informed about coordinating the information sharing with other airports and providing industry-specific guidance for incident mitigation.
Data Protection Authority (GDPR related)	Required	Personal data might be affected, so it's a legal obligation to notify the DPA.
Affected Business Partners	Required	If any of the business partners are affected, they need to be informed to start their own incident mitigation measures.

The ISPs and IT Contractors	Recommended	The most efficient mitigation measures might be found based on a consultation with the ISP and IT contractors.
Other Authorities	Required	National cybersecurity authority since airport is a critical infrastructure but also other authorities. According to incident notification legal obligations there might be one or more authorities

3.3.3.2 Task 2: Setting up the task force, division of duties

While in the context of a criminal investigation the prosecutor/judge is in charge of assigning roles for dealing with the investigation of the cybercrime, the national CSIRT may establish a task force to respond to the incident and deal with the crisis generated by the incident.

The National CSIRT is in charge of establishing a task force to deal with the crisis generated by the incident.

Analyse the legal and organisational framework by defining the competences of CSIRTs, LE, and the judiciary in their activities related to fighting cybercrime, and capture potential synergies and possible overlaps. Analyse the possible interferences in the cooperation between CSIRTs and LE and their interaction with the judiciary. To collect data and roles and duties, use the SoD matrix in ANNEX B.

The role of the IT contractors of the airport should be decided: will they be part of the task force? A example of task force is provided below.

Figure 27: Task force – Example

Organisation	Expertise	Tasks/Role	Comments
The Airport	Management System operators The IT Contractors	Management – executive decision making Operators – knowledge of the infrastructure, involvement in incident mitigation The IT Contractors - provide technical support for business continuity and service restoration	
The National Cybersecurity Authority/CSIRT	Incident Handlers Liaisons Investigators	Incident Handlers – support to the airport IT team, information sharing with the community, coordinate the technical investigation and Incident Response Coordination with other authorities and stakeholders Investigators – evidence collection, investigation of criminal activities	
Law Enforcement	Forensic Experts	Experts - coordinate the cybercrime investigation and will guide the technical teams on e-evidence gathering	
The ISP	Network Experts	Experts - Will assist with traffic filtering (to try to mitigate the DDoS attacks)	
Crisis Management Bodies	Liaisons	Coordination with national crisis management bodies	

3.3.3.3 Task 3: Possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary

This task requires the students to familiarize themselves with the SoD matrix and use it to analyse possible duties (tasks), synergies and interferences between CSIRT, LE and the judiciary, related to the scenario. The SoD matrix is available in Annex B together with an explanation of how to use it.

In particular, the students will be asked to select some of the duties from column 1 of the SoD in Annex B and with some of these duties, briefly describe the measures to that could be taken by each community in the scenario.

A table can be used be used to list the phase (e.g. during the incident/crime) in column 1, the duties (tasks) in column 2 (to be taken from column 1 of the SoD matrix in Annex B), and the synergies and potential interferences in column 3. The last column of the template below, column 4, can be used to add comments. A example of filled in table is provided below.

Figure 28: Duties, synergies and potential interferences – Example

Phase	Duty (task)	Synergies and potential interferences	Comments
Prior to the incident/crime	Advising potential victims on preventive measures against cybercrime	CSIRT/LE Regularly exercise preparedness and response time on test incidents Joint training activities with LE to train airport personnel and also specialised IT security training	
During the incident/crime	Identification and classification of the cybersecurity incident/crime	CSIRT/LE	
During the incident/crime	Collection and sharing evidence	CSIRT collects system logs from perimeter security solutions (firewall, web and email gateway, proxy), analyses recent activity of the user, identifies rogue device in the network; Screenshots of the sensitive information; video images LE seizes the computers of the individuals and server used for DDoS	
During the incident/crime	Identification and reporting of crimes	LE analysis of images from the airport and identification of possible suspects to report to the Prosecution Office	
During the incident/crime	Conducting the criminal investigation	LE/Prosecutor Investigate the logs, rogue device, screenshots of sensitive information, video images Discuss details of the warrant and how to seize the devices	
During the incident/crime	Conduct the incident response	CSIRT and involved ISPs need to carefully coordinate with LE to avoid take down and or take down requests that might affect the cybercrime investigation (avoid putting attacker on-guard and delete evidence)	

3.3.3.4 Task 4: International cooperation and information sharing

This task requires students to briefly explain how Interpol, Europol and Eurocontrol can collaborate with CSIRTS/LE/Judiciary during the international criminal investigation.

A table can be used to list the name of the organisation in column 1, the name of the organisation it collaborates with in column 2 and the kind of collaboration they have in column 3. An example of filled in table is provided below.

Figure 29: Information sharing and use – Example

Name of the organisation	Name of the organisation it collaborates with	Kind of collaboration
IT team airport/management	Aviation Sectorial CSIRT/LE	Notification of the cybersecurity alerts and incidents to the aviation sectorial CSIRT Complaint to LE
National CSIRT	LE/Judiciary	CSIRTs provide evidence to LE and can support the LE/Judiciary during the criminal investigation by providing technical expertise information useful for the criminal investigation CSIRT personnel can act as forensic expert or witness during a criminal trial
European Air Traffic Management Computer Emergency Response Team (EATM-CERT)- Eurocontrol	National CERTs	Supporting National CERTs coordinating plan-European responses to cybersecurity alerts and incidents in the aviation sector and collecting relevant cyber intelligence
LE	CSIRT/Judiciary	Collaborates with CSIRTs to prepare the evidence to be sent to the Court and ask CSIRTs for specific technical advice Prepares evidence to be sent to the judiciary (e.g. logs, rogue device, screenshots of sensitive information, video images)
Judiciary	CSIRT/LE	Discuss details of the warrant and how to seize the devices Approves seizure; investigation; guarantees the confidentiality of information Can ask CSIRT personnel as forensic expert or witness during a criminal trial
Europol (EC3) and Joint Cybercrime Action Taskforce (J-CAT)	LE/Judiciary	Supports international operations and investigations that affect EU Member States and their citizens by offering operational analysis, coordination and expertise. Collaborates with LE/Judiciary of different EU Member States during their criminal investigations providing specialised technical and digital forensic support

3.3.3.5 Task 5: Post-incident preventive measures

This task requires students to explain based on information they have about the incident, what kinds of post-incident preventive measures would they recommend to the airport information security team to implement and how they formulate the outcome as a gap analysis and a remediation roadmap.

A table can be used to list the duties (tasks) in column 1 (to be taken from column 1 of the SoD matrix in Annex B), and the proposed preventive security measures in column 2. An example of filled in table is provided below.

Figure 30: Suggestion on preventive security measures – Example

Duty (Task)	Proposed preventive security measures
Advising potential victims on preventive measures against cybercrime	CSIRT/LE Secondary internet connection and another IP range for emergency cases Security hardening of airport IT devices and networks Firewalls, network fragmentation Volumetric protection from the Internet Service Provider (ISP) as most ISPs can detect potential DDoS attacks and filter requests from possible sources Anti-spoofing control, filtering, dual authentication, malware protection and other technical security measures, as well as user training and security awareness. Encouraging employees to “Think before clicking a link” and being suspicious regarding emails that look strange or very attractive; e.g. invitations from social media, other official institutions, etc. Filtration and examination of email addresses and notification to the IT security team and management in case of doubt or suspicion.
Analysis of vulnerabilities and threats	CSIRT/European Air Traffic Management Computer Emergency Response Team (EATM-CERT) Review the protection guidelines against cyber threats that can impact the confidentiality, integrity and operational IT assets and data.

3.3.3.6 Outcomes

The scenario illustrates the roles, synergies and potential interferences during the incident handling and criminal investigation of a DDoS and malware blended attack.

3.3.4 Lessons Learned

DDoS and malware blended attack cases are rather complex and sophisticated. They demand many skills as it’s not easy to identify what is the primary attack vector or what is the ultimate target of the attacker. The scenario allows each party to understand its role under the legal framework of each member state.

Although for training purposes the scenario is presented as less complicated than real cases might be, it still allows each party to understand the complexities in terms of actors involved, roles played, duties (tasks performed), synergies to exploit, and risks of interference.

4. BIBLIOGRAPHY

ENISA (2018), *Review of Behavioural Sciences Research in the Field of Cybersecurity*, https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity (retrieved on 13 October 2020)

ENISA, *2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries*, https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation (26 January 2021)

ENISA, *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 (retrieved on 13 October 2020)

ENISA, *Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices* (2012), https://www.enisa.europa.eu/publications/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices (retrieved on 15 October 2020)

ENISA, *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary* (2018), https://www.enisa.europa.eu/publications/csirts-le-cooperation (retrieved on 13 October 2020)

ENISA, *CSIRTs by Country –Interactive Map*, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map (retrieved on 13 October 2020)

ENISA, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity* (2018), https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity (retrieved on 13 October 2020)

ENISA, *Electronic evidence - a basic guide for First Responders* (2014), https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders (retrieved on 15 October 2020)

ENISA, *Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime (2012)*, https://www.enisa.europa.eu/publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime (retrieved on 15 October 2020)

ENISA, *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (2017), www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement (retrieved on 13 October 2020)

ENISA, *Information sharing and common taxonomies between CSIRTs and Law Enforcement* (2015), https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement (retrieved on 15 October 2020)

ENISA, *Reference Incident Classification Taxonomy,* https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (retrieved on 13 October 2020)

ENISA, Reference Security Incident Taxonomy Working Group, https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force (retrieved on 13 October 2020)

ENISA, *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 (retrieved on 13 October 2020)

ENISA, *ENISA Threat Landscape – 2020*, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends (retrieved on 10 November 2020)

ENISA, *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 (retrieved on 13 October 2020)

ENISA, *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 (retrieved on 13 October 2020)

ENISA, Training Resources page: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material (retrieved on 14 October 2020)

ENISA, *Trainings for Cybersecurity Specialists*, (handbooks and toolsets) https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material (retrieved on 13 October 2020)

Eric M. Hutchins E. M., Clopperty M. J., Amin R. M., *Lockheed Martin Corporation Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf*

Lockheed Martin, *The Cyber Kill Chain®*, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (retrieved on 20 October 2020).

Reference Security Incident Classification Taxonomy (RSIT taxonomy), https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md (retrieved on 13 October 2020)

ANNEX A: MAIN ABBREVIATIONS

Abbreviation	Description
AIL	Analysis of Information Leaks
BCP	Business Continuity Plan
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
C&C	Command and Control
DDoS	Distributed Denial of Service
DPA	Data Protection Authority
EATM-CERT	European Air Traffic Management Computer Emergency Response Team
EDR	Endpoint Detection and Response
EFTA	European Free Trade Association
EMAS	Europol Malware Analysis Solution
ICT	Information and Communication Technology
IOC	Indicators Of Compromise
IP	Internet Protocol
ISP	Internet Service Provider
LE	Law Enforcement
LEA	Law Enforcement Agency
MS	Member State
n/g	National/governmental
Q&A	Question and answer
RSIT	Reference Security Incident Taxonomy
SIEM	Security Information and Event Management
SOC	Security Operation Centre
SoD	Segregation (or separation) of Duties
SSH	Secure SHell

TTP	Tactics, Techniques and Procedures
VPN	Virtual Private Network
VPS	Virtual Private Server

ANNEX B: SEGREGATION OF DUTIES (SOD) MATRIX

Version 1.6 of 5 June 2020

- **Responsible (R)**: Who is responsible for performing this duty? Who is the decision maker?
- **Supporting (S)**: Who is providing support when performing this duty? (if applicable)
- **Consulted (C)**: Who is consulted during the performance of this duty? (if applicable)
- **Informed (I)**: Who is informed when performing this duty? (For instance, if CSIRT should report a crime to LEA; this means that LEA is informed) (if applicable)

Duties related to (supporting) cybercrime fighting activities	CSIRTs	LE	Prosecutors	Judges	Training topics (e.g. technical skills etc.	ADDITIONAL COMMENTS (including information on possible synergies and potential interferences)
Prior to incident/crime						
1. Delivering training						
2. Participating in training						
3. Collecting cyber threat intelligence						
4. Analysing vulnerabilities and threats						
5. Issuing recommendations for new vulnerabilities and threats						
6. Advising potential victims on preventive measures against cybercrime						
During the incident/crime						
7. Discovering of the cybersecurity incident/crime						
8. Identifying and classifying the cybersecurity incident/crime						
9. Identifying the type and severity of the compromise						
10. Collecting data that may be evidence/evidence						
11. Providing technical expertise						
12. Preserving the evidence that may be crucial for the detection of a crime in a criminal trial						
13. Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)						
14. Informing the victim of a cybercrime						
15. Informing other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)						
16. Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling						

17. Mitigating a cybersecurity incident						
18. Conducting the criminal investigation						
19. Leading the criminal investigation						
20. In the case of disagreement, having the final say for a criminal investigation						
21. Authorizing the investigation carried out by the LE						
22. Ensuring that fundamental rights are respected during the investigation and prosecution						
Post incident/crime						
23. Advising on systems recovery						
24. Protecting the constituency						
25. Preventing and containing cybersecurity incidents from a technical point of view						
26. Analysing and interpreting collected evidence						
27. Requesting testimonies from CSIRTs and LE						
28. Admitting and assessing the evidence						
29. Judging who committed a crime						
30. Assessing cybersecurity incident damage and cost						
31. Reviewing the response and updating policies and procedures						

Some explanations regarding the SoD matrix:

- At the top of the SoD Matrix all the four **possible roles** that each actor (CSIRT, LE, Prosecutors, and Judges) may play are listed and briefly explained: Responsible (R), Supporting (S) (if applicable), Consulted (C) (if applicable), and informed (I) (if applicable).
- In the rows, the **duties** are listed and numbered for convenience (e.g. 10. Collecting data that may be evidence/Evidence collection). It must be noted that "duties" is used here as a synonymous of "tasks"
- Column 2, Column, 3, Column 4, Column 5, refer to the **actors**, respectively CSIRT, LE, Prosecutors, and Judges.
- The interviewees are asked to indicate which role(s) each actor (CSIRTs, LE, prosecutors, judges) has in the performance of duties during a cybercrime (supporting) fighting activity. In other words, the interviewees are asked to identify whether the CSIRTs, the LE, the prosecutors or the judge are for a particular duty responsible (R) for that duty, and, if applicable, which other actor is Supporting (S) the performance of that duty, is Consulted (C) or is Informed (I) during the performance of that duty.
- Column 6 (optional) is used to capture information on **training topics**, which is closely connected to the competencies that are required for the performance of the specific duties.
- Column 7 is used for any **additional information** that the interviewee might provide and to record possible synergies and potential interferences, especially for those cases where a task is performed by more than one community.

An example of completed information related to one duty in the SoD Matrix in the table below.

Table 1: Example of completed information related to one duty in the SoD Matrix

- **Responsible (R): Who is responsible for performing this duty? Who is the decision maker?**
- **Supporting (S): Who is providing support when performing this duty? (if applicable)**
- **Consulted (C): Who is consulted during the performance of this duty? (if applicable)**
- **Informed (I): Who is informed when performing this duty? (For instance, if CSIRT should report a crime to LEA; this means that LEA is informed) (if applicable)**

Duties related to (supporting) cybercrime fighting activities	CSIRTs	LE	Prosecutors	Judges	Training topics (e.g. technical skills etc.)	ADDITIONAL COMMENTS (including information on possible synergies and potential interferences)
Prior to incident/crime						
10. Collecting data that may be evidence/Evidence collection	S	R	I C		Digital forensics	Prosecutor depending on the specific case may be informed or consulted, in other words requested to provide guidance.

978-92-9204-436-7

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-436-7
DOI: 10.2824/71834