Incident Handling Management

Handbook, Document for Teachers

1.0

DECEMBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use cert-relations@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Table of Contents

1. Objective and descriptions

Main Objective	This exercise provides students with experience of real-life incident reports, their ambiguity and complexity. After completing the exercise they should understand: • What to focus on during initial analysis • How different factors may affect priorities • How to communicate with media reporters as well as third parties • What kind of technical tools to use to resolve an incident During the exercise, they will apply a given classification scheme to incidents – the purpose of this part of the exercise is to work on the consistent classification of disputable cases among all team members and possibly to suggest a clearer, more unambiguous classification scheme for the team.
Targeted Audience	The exercise is aimed at incident handlers at any level of experience. It requires a good understanding of Internet topology and services.
Total duration	2 hours
Frequency	It is recommended to conduct the exercise once for every new team member and to repeat it when there are planned or introduced significant changes in the incident management process in the organisation.

This exercise can be used with real reports as an intra-team exercise for all incident handlers in a CSIRT. In this case, the goal is to make sure there is a consistency between the classification and prioritization of reports by different team members.

2. Exercise course

The course of this exercise is as follows. All discussions should be moderated by the trainer.

The exercise's parts are:

- Introduction to the Incident Handling Management
    - Incident handling workflow
    - Incident handling phases
    - Incident handling tools
- Incident handling tasks

2.1 Introduction to the Incident Handling Management

CSIRTs nowadays are involved not only in pure incident handling activities but have also become one of the most important parts of an organisation by ensuring IT security capabilities. Nevertheless, the specific task of incident management is still a CSIRT's primary role and a CSIRT should perform this task in a very mature manner. The specific workflows and incident handling phases should apply especially in the most sophisticated cases and environments. In such situations, sticking to best practises plays a significant role in successful incident response.

2.1.1 Incident handling workflow

There are many incident handling workflows. They include different phases in a more or less detailed approach. How a proposed workflow is really used by incident handlers in their daily operations is most important. Sometimes, especially experienced practitioners, perform tasks without following specific rules but instead following their experience and routine. Definitely, experience is an important factor in successful incident handling, but it should not override best practices or following established rules. Only including both best practices and experience can ensure that everyone uses all methods in successful incident handling.

An example of an incident handling process flow is presented below.

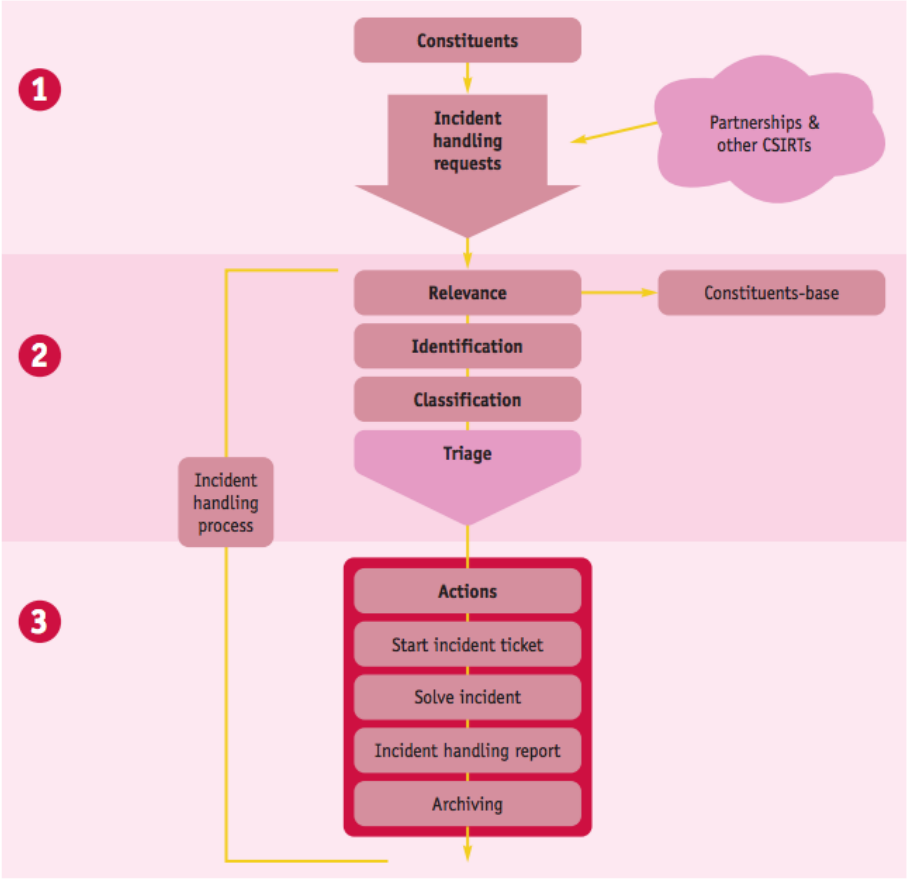

Figure 1 - Incident handling process flow[1]

2.1.2 Incident handling phases

Like incident handling workflows, particular phases of this process are differently defined. However, most workflows include similar activities like receiving incident reports, registration of reports, incident classification and triage.

In practice, those phases which are critical to the whole process are the phases related to incident resolution. Incident resolution has five phases: data analysis, resolution research, action proposed, action performed and eradication and recovery. The phases can be repeated if one cycle does not resolve the incident.

[1] Source: "ENISA Good Practice Guide for Incident Management" : https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

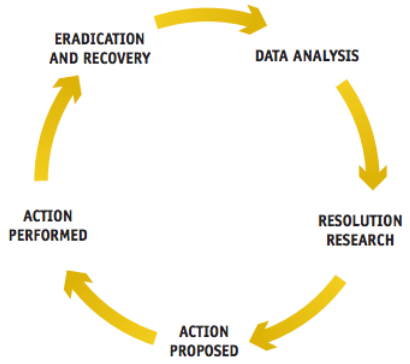

Figure 2 - Incident handling cycle[2]

2.1.2.1 Data Analysis

To start data analysis, first notify the parties involved and collect data from them. First, inform those who may be affected the most. Include initial advice and information about further proceedings to resolve the incident in this notification. In this step collect as much data as possible. There are several main sources of such data:

- Incident reporter – depending on how much information was given in the initial report you should ask for additional data you need, such as:
  - detailed contact information
  - detailed description of the incident
  - incident classification suggested by the incident reporter
  - logs
  - the exact time of the incident
  - operating systems and network setup
  - security systems setup (e.g. antivirus software or firewall)
  - incident severity (in the incident reporter's opinion).
- Monitoring systems – try to search for information related to the IP addresses involved in your network monitoring systems (e.g. netflow database).
- Referring database – check if this kind of incident or this incident reporter are already in your incident database. By doing this you can learn a lot and speed up the resolution of the incident.
- Other sources – relevant log-files (routers, firewalls, proxy servers, switches, web application, mail servers, DHCP servers, authentication servers, etc.).

The target of attack and the incident reporter do not have to be the same party. Sometimes a target does not know that he is being attacked. In such cases your information is very important as it allows an attack target to learn about his situation and to mitigate the threat. Of course, also try to determine the source of

[2] Source: "ENISA Good Practice Guide for Incident Management" : https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

the incident. To be successful at the latter task, contact as many relevant parties as possible. These parties – the attack target, ISPs involved on both attacking and attack target sides, Internet content provider (ICP), law enforcement agencies (LEA) – can help you to collect the necessary information related to your incident. In practice, solving the incident is practically impossible without involving many or all of these parties. Contacting them and working with them may require many attempts to reach them or schedule a phone call or meeting. Sometimes contact is easy and a party is very responsive and helpful, while at other times you must be persistent to obtain a single piece of vital information or to convince someone to take action. To get the support you need, use the following arguments:

- Giving information provides an opportunity to improve the security level of many organisations and individuals.
- An incident can result in a real legal case. It is worth taking effective steps towards its mitigation and the proper collection of evidence about the incident.

Making demands ("you must do X because it is your computer that is doing bad things on the network") usually does not result in cooperation or compliance. Sometimes, though, it is your last resort. Sharing that you will be forced to contact the management of an uncooperative party may convince some to help you; involving an organisation's management may even be part of your defined incident handling procedure.

Having completed the notification and data collection tasks, you can now start data analysis. Your success depends on this task. After collecting data, the next step is to decide which data to analyse and in what order. To decide, ask yourself the following questions:

- Which data will most likely contain the information you need to resolve the incident?
- What sources of data do you trust the most?
    - What security devices do you trust the most?
    - What people do you trust the most?

The work of data analysis can start after these questions are answered. It is important to distribute this work properly within the team. In general, consider two factors: a team member's expertise and a team member's current workload. Adjust the action plan to take these factors into account.

2.1.2.2 Resolution Research

Very often during the data analysis phase people exchange their ideas, observations and draw conclusions. This means that your team has practically entered the resolution research phase. The ideas people propose during these 'sessions' are usually very valuable but the problem is that hardly anyone makes proper use of them. The ideas are broadcasted in an office and only a few of them, if any, are implemented in practice. This is a kind of specific brainstorming session, so you need a way to avoid wasting and losing this valuable information. The solution is simpler than you may expect – just advise, convince or order team members to collect any observations they make by writing them down on a sheet of paper. Then you can hold periodic review sessions (e.g. every day or every two hours for very urgent incidents) and exchange, discuss and decide which ideas you will use for the resolution of the incident. Also try to avoid the pitfall of perfectionism. Sometimes you feel that you have to collect and analyse much more data to be sure that you have done everything to be successful. To be successful in the resolution of an incident, it is not necessary to know absolutely everything about an incident. Equally important is the timeliness of your reaction. Sometimes a quick response has the same or a higher value than a comprehensive and complete dataset.

2.1.2.3 Action Proposed

In this phase of an incident, whether you want it or not, you are the incident owner. Most things depend on you. Therefore, you should prepare a set of concrete and practical tasks for each party involved. Remember to adjust your language to your interlocutor. Use quite advanced technical terms talking to another CSIRT or ISP, but you should switch to a 'descriptive mode' when giving advice to the attack target, unless you know (e.g. from an incident report) that he/she is also a technically advanced person. Any action proposed should be clear and you should be sure that the recipient understands what you are proposing. Below are some examples of actions you can propose to particular parties:

- Attack target
    - How to stop and mitigate an ongoing attack:
        - turn off a service
        - check the system for malware
        - patch a system or an application
        - perform or order an audit if you are not able to improve your system security yourself.
        - How to deliver more data:
        - concrete practical instructions (e.g. how to obtain a full e-mail header); having some of your most often used instructions ready and available on your website is good as then it is enough just to point links to them.
    - ISP/ICP
        - To collect, save and archive data. Some of this data can be available without any special restrictions; other data requires special protection (e.g. personal data) – in this case all you can ask for is for the data to be saved so that it is available if the target of the attack reports a case to the police.
        - To monitor network traffic related to the case and inform you if something important happens.
        - To filter network traffic in the case of an ongoing attack if such filtering can help to stop or mitigate it.
    - CSIRTs
        - To contact the local ISP/ICP within its constituency. Usually contacting an ISP/ICP which is outside your constituency, especially in other countries, through the relevant CSIRT will work much better than contacting the ISP's customer service channels.
        - To ask for advice on how to deal with an incident where a similar incident happened to another CSIRT. It is good practice to use trusted information distribution channels such as the TERENA TI mailing list or FIRST mailing list38.
    - Law enforcement agency (usually the police):

- To follow a case if it is significant (e.g. you suspect organised crime activity)
- To assist the reporter of a crime if an incident is to be reported to the police39.

- Source of an incident (the attacker)
  - To advise and propose similar actions to those given to the attack target (see above).
  - DO NOT contact the source of the incident if you suspect that you may be contacting a real criminal. Notifying a potential attacker that someone is aware of his or her activities could decrease the effectiveness of the investigation. In such a case it is highly recommended that the incident handling is coordinated with an LEA.

2.1.2.4 Action performed

Whatever in your plan is identified as your action – it is your decision as to whether it will be carried out or not. You have limited power to decide what others will do. It is a rather optimistic assumption that all, or even most, of your proposed actions will be executed by other parties. In practice this will not happen. Parties you ask to do something are outside your direct control. The only exception is where you are an internet service provider's CSIRT and your Terms of Service allow you to limit customers' Internet access under certain conditions.

There are some basic rules for monitoring the responses to your requests and actions:

- Monitor technically whatever you are able to monitor, for example:
  - Is the attack target's service turned off?
  - Is the attack target's service still vulnerable?
  - Is the traffic which should be filtered still visible in the network?
  - Other responses can be checked by traditional means such as e-mail, phone or any other kind of direct contact. Ask what has been done.

2.1.2.5 Eradication and recovery

All your actions have one main goal – the eradication of the incident. The real resolution of a problem is to recover or restore to normal the service that was attacked during the incident. For example: it means that the application is working again, e-mails are reaching mailboxes, a website is available once more and displays proper content with proper response times, a computer is not part of a DDoS army and is not sending spam, etc. General speaking – an attacked system now does what it should do and not what it should not do. If you have doubts that you eradicated a problem and recovered a service, it is good practice to check yourself as much as possible and/or get a positive confirmation from each party that in their opinion everything is operating normally again.

2.2 Incident handling tools

The tools proposed below are specific for the proposed incidents. They can be used to resolve them and they will be the components for usage during performing the exercise tasks.

TOOL NAME	TOOL DESCRIPTION	URL

Mimikatz	Mimikatz is a tool I've made to learn C and experiment with Windows security. It's now well known to extract plaintexts passwords, hash, PIN code and Kerberos tickets from memory. mimikatz can also perform pass-the-hash, pass-the-ticket or build *Golden tickets*.	https://github.com/gentilkiwi/mimikatz
RegRipper	RegRipper is an open source forensic software application. RegRipper, written in Perl, is a Windows Registry data extraction tool. RegRipper can be customized to the examiner's needs through the use of available plugins or by users writing plugins to suit specific needs.	https://github.com/keydet89/RegRipper2.8
LOKI	Simple IOC and Incident Response Scanner	https://github.com/Neo23x0/Loki
Internet History Browser	Quick internet history overview supporting main browsers on the market	http://www.mitec.cz/ihb.html
Bro bro	Bro is a powerful network analysis framework that is much different from the typical IDS you may know.	https://www.bro.org/
IOC Finder	The FireEye Indicators of Compromise (IOC) Finder is a free tool for collecting host system data and reporting the presence of IOCs. IOCs are open-standard XML documents that help incident responders capture diverse information about threats.	https://www.fireeye.com/services/freeware/ioc-finder.html
FTK Imager	It scans a hard drive looking for various information. It can for example locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption	http://accessdata.com/product-download/digital-forensics/ftk-download-page
DB Browser for SQLite	DB Browser for SQLite is a high quality, visual, open source tool to create, design, and edit database files compatible with SQLite.	https://github.com/sqlitebrowser/sqlitebrowser/releases
Ransomware Response Kit	The kit almost 320MB in size, includes guides for getting rid of TeslaCrypt, CryptoLocker and CoinVault crypto-malware pieces, as well as police ransomware that tricks victims into paying up by plastering a message allegedly from law enforcement (FBI in most cases)	https://bitbucket.org/jadacyrus/ransomwareremovalkit/overview

	saying that illegal content has been accessed and they have been fined as a consequence.	
Argus	The network Audit Record Generation and Utilization System. The Argus Project is focused on developing all aspects of large scale network situational awareness derived from network activity audit	http://qosient.com/argus/
Wireshark	**Wireshark** is the world's foremost network protocol analyser. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.	https://www.wireshark.org/
KiTrap0D	Windows SYSTEM Escalation	https://www.exploit-db.com/exploits/11199/
ChopShop	ChopShop is a MITRE developed framework to aid analysts in the creation and execution of pynids based decoders and detectors of APT tradecraft.	https://github.com/MITRECND/chopshop
pwdump7	password dumper for windows	http://www.tarasco.org/security/pwdump_7/
Xplico	Xplico System is composed from 4 macro-components: a Decoder Manager called DeMa an IP decoder called Xplico (its status is here) a set of data manipulators a visualization system to view data extracted	http://www.xplico.org/
REMnux	A Linux Toolkit for Reverse-Engineering and Analysing Malware	https://remnux.org/
BrowsingHistoryView	BrowsingHistoryView is a utility that reads the history data of 4 different Web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Safari) and displays the browsing history of all these Web browsers in one table	http://www.nirsoft.net/utils/browsing_history_view.html
Fgdump	A Tool For Mass Password Auditing of Windows Systems	http://foofus.net/goons/fizzgig/fgdump/
Scalpel	Scalpel is an open source data carving tool.	https://github.com/sleuthkit/scalpel

Windows File Analyzer	Tool for forensic file analysis	http://www.mitec.cz/wfa.html
ID Ransomware	To identify the ransomware that has encrypted data.	https://id-ransomware.malwarehunterteam.com/index.php
OSForensics	Extract forensic data from computers.	http://www.osforensics.com/
Windows Registry Explorer	to back up the registry, how to edit the registry.	Windows OS feature
Pestudio	The goal of pestudio is to spot these artefacts in order to ease and accelerate the Malware Initial Assessment. The tool uses a powerful parser and a flexible set of configuration files that are used to provide many of indicators and determine thresholds	https://www.winitor.com/
Ntop	Packet Capturing , Traffic Recording, Network Probe, Traffic Analysis	http://www.ntop.org/
Rekall	Rekall is the most complete Memory Analysis framework. Rekall provides an end-to-end solution to incident responders and forensic analysts. From state of the art acquisition tools, to the most advanced open source memory analysis framework	http://www.rekall-forensic.com/
Log2timeline	Tool designed to extract timestamps from various files found on a typical computer system(s) and aggregate them.	https://github.com/log2timeline/plaso/wiki
Netcat	General purpose tool described by its author as a TCP/IP Swiss army knife.	https://debian-administration.org/article/58/Netcat_The_TCP/IP_Swiss_army_knife
Keimpx	Keimpx is an open source tool, released under a modified version of Apache License 1.1. It can be used to quickly check for valid credentials across a network over SMB	https://github.com/inquisb/keimpx
Belkasoft RAM Capturer	Belkasoft Live RAM Capturer is a tiny free forensic tool that allows to reliably extract the entire contents of computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system.	https://belkasoft.com/ram-capturer
Cain & Abel	Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network,	http://www.oxid.it/cain.html

	cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analysing routing protocols.	
Windows Registry Recovery	The best tool for crashed machine registry configuration data recovery	http://www.mitec.cz/wrr.html
WinHex	WinHex is in its core a universal hexadecimal editor, particularly helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security. An advanced tool for everyday and emergency use: inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards.	https://www.x-ways.net/winhex/
FlowViewer	FlowViewer provides a convenient web-based user interface to Mark Fullmer's flow-tools suite and CMU's netflow data capture/analyser, SiLK. The inclusion of the underlying SiLK tool set enables FlowViewer users to continue to use the tool with the newer IPFIX netflow data protocol, which includes support for IPv6 and Cisco's v9 and FNF netflow.	https://sourceforge.net/projects/flowviewer/
Autopsy	Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer.	http://www.sleuthkit.org/autopsy/
Proxifier	Proxifier allows network applications that do not support working through proxy servers to operate through a SOCKS or HTTPS proxy and chains.	https://www.proxifier.com/

Table 1 - Incident handling tools

2.3 Incident descriptions

Below there are descriptions of three incidents which will be used in the exercises. They represent different types of incidents but all are normal for CSIRTs.

2.3.1 Phishing campaign (malware analysis)

The incident is based on the NoCompany123 Inc. phishing campaign scenario from the exercise "Using indicators to enhance defence capabilities"[3] and phishing scenario from the exercise "Identifying and handling cyber-crime traces"[4].

NoCompany123 Inc. is a leading contractor in the defence industry, working on highly classified military projects.

One day, employees of the company received emails with information about a change in the agenda of an upcoming event in an attached PDF file. The employees opened the file and learnt about the changed event. One called the event organiser about the new agenda. The organiser was surprised and said he did not send any emails and there was no change to the event agenda. This aroused suspicion among the employees. They suspected cyberattack. Thus they decided to contact their internal CSIRT and inform the team about the emails.

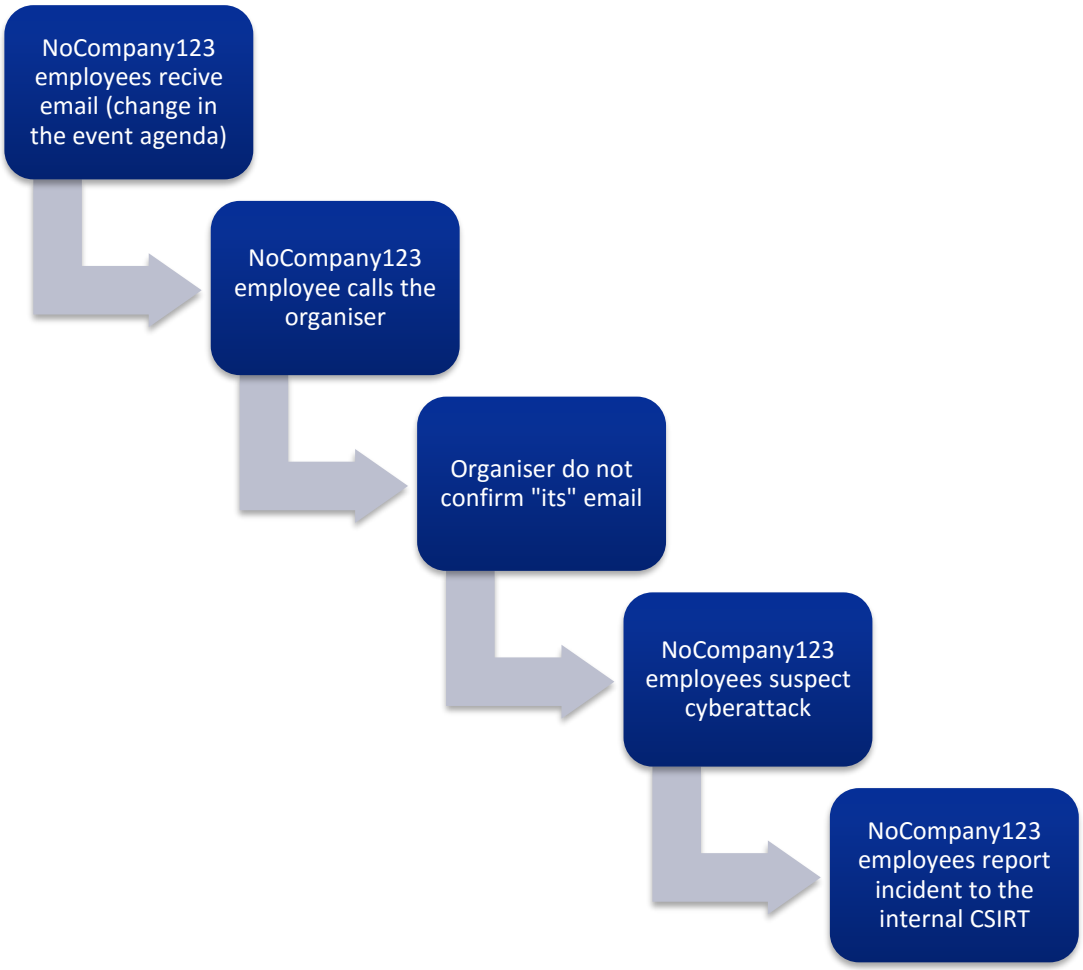

Figure 3 – Phishing campaign incident phases

[3] https://www.enisa.europa.eu/topics/csirt-cert-services/reactive-services/copy_of_actionable-information/Usingindicatorstoenhancedefencecapabilities.pdf

[4] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/legal-cooperation#identifying-and-handling-cyber-crime-traces

2.3.2 Computer break-in (computer forensics)

A customer's organization has found that some of its sensitive data has been detected in an online text sharing application. Due to legal obligations and for business continuity purposes, the CSIRT team has been tasked to conduct an incident response and incident investigation to mitigate the threat.

The breach contains sensitive data and includes a threat: in a short while more data will follow. As the breach leads to a specific employee's computer, the CSIRT team, tasked to investigate the incident, follows the leads.

During analysis, the team discovers another break-in. The whole analysis includes both Windows and Linux systems as well as analysis of a WordPress website based on the LEA request.

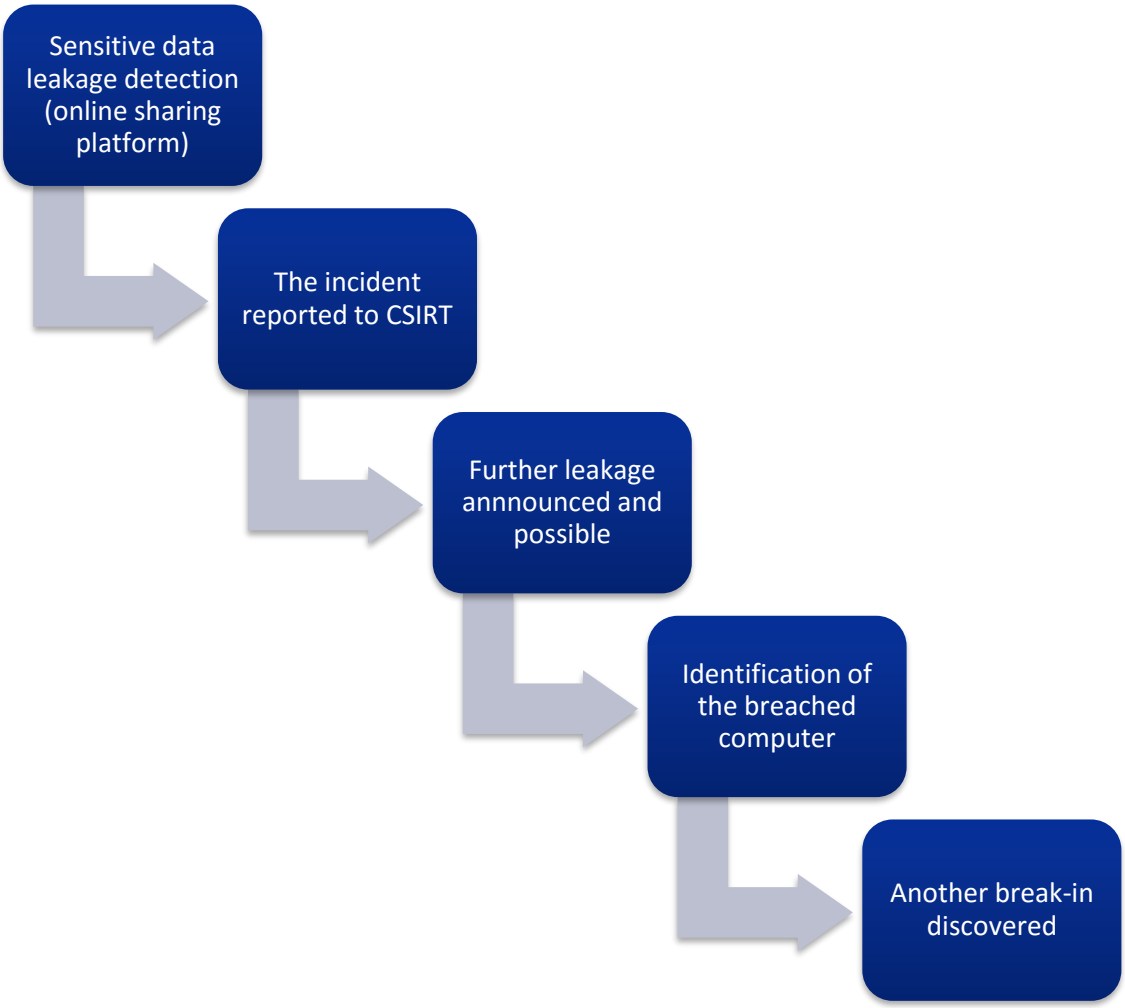

Figure 4 – Computer break-in incident phases

2.3.3 Ransomware

The incident occurred in the IT environment of some SME (Energy Support Ltd), which is a contractor of a large critical infrastructure company (Electro Energy Inc.). Employees of Energy Support received emails pretending to be a request from Electro Energy. They could not find any content in the attached .docx file so they sent it back asking for help opening the attachment.

The email reply, with original attachment, reached Electro Energy and an employee assigned for the contract (the apparent “sender” of the first email) opened it. The employee at the Electro Energy also could not see any content in the file, so he sent it to his colleagues and asked them to try to open the file to help Energy Support. Ten people at Electric Energy opened the file. As you might expect, the file was in fact a ransomware computer program, which began to encrypt local and mapped disks.

An obvious solution to remedy the ransomware was to recover the files from backup. Unfortunately, part of the enterprise backup system was not available. A request for help and action was sent to the internal CSIRT.

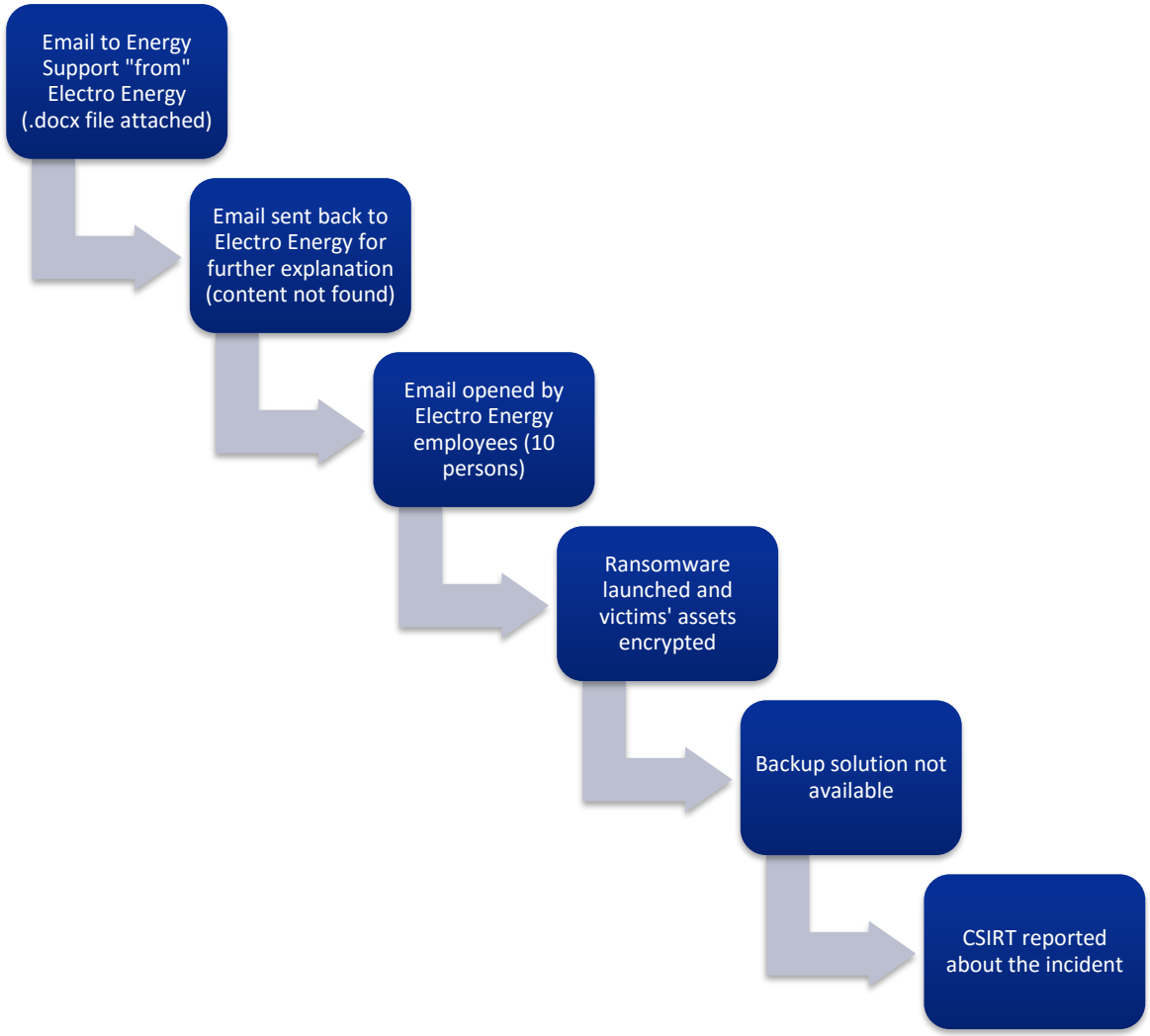

Figure 5 – Ransomware incident phases

3. Incident handling tasks

Below there are a number of various tasks. All of them represent specific actions which could be performed by incident handlers during the described scenarios. The list includes technical tasks as well as organizational ones. The task for the students is to match them to the specific scenarios presented above. Then, they should propose a course of action in the right sequence. It is possible that some tasks will be summarized and represented more generally – e.g. technical tasks related to some kind of analysis like artefact analysis.

Students should propose the workflow by putting text boxes in the preferred order, sequence and relationships.

We recommend having groups of two to three people perform the tasks.

Figure 6 – Incident handling task, actions and functions

3.1 Incident handling workflow / process

There will be three tasks:

Task 1 – Identify and present the generic model for an incident handling process with the main phases and their assignment to the particular specialist (students should propose their specialization breakdown – e.g. malware analyst, network forensic specialist, IH manager, legal department support, etc.)

Task 2 – Identify and present the detailed process for particular scenarios, where they will use elements from Figure 6 – Incident handling task, actions and functions.
For this purpose, students should use the rectangle boxes presented on Figure 6 – Incident handling task, actions and functions. They should cut them (or have them cut out before the exercise begins).

The example linking could be as presented below on Figure 7 - The example linking between IH process phase and particular action performed during it. It is possible to link more than one tool to each process.

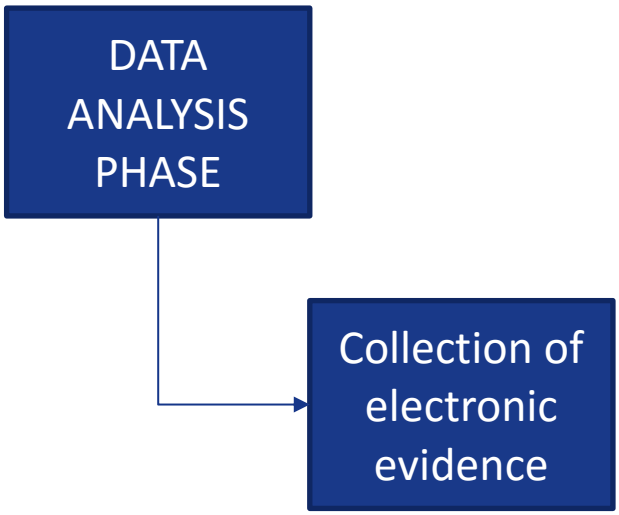

Figure 7 - The example linking between IH process phase and particular action performed during it.

Task 3 – Recognize the functionality of the tools mentioned and presented in chapter 2.2 and match them to the specific incident handling process phases identified during Task 2.

For this purpose, students should use the rectangle boxes presented below – Figure 9 – Incident response tools boxes. They should cut them (or have them cut out before the exercise begins).

The example linking could be like this presented on Figure 8 – The example of linking between IH process phase, particular action performer and one of the tools. It is possible to link more than one tool to each process and activity.

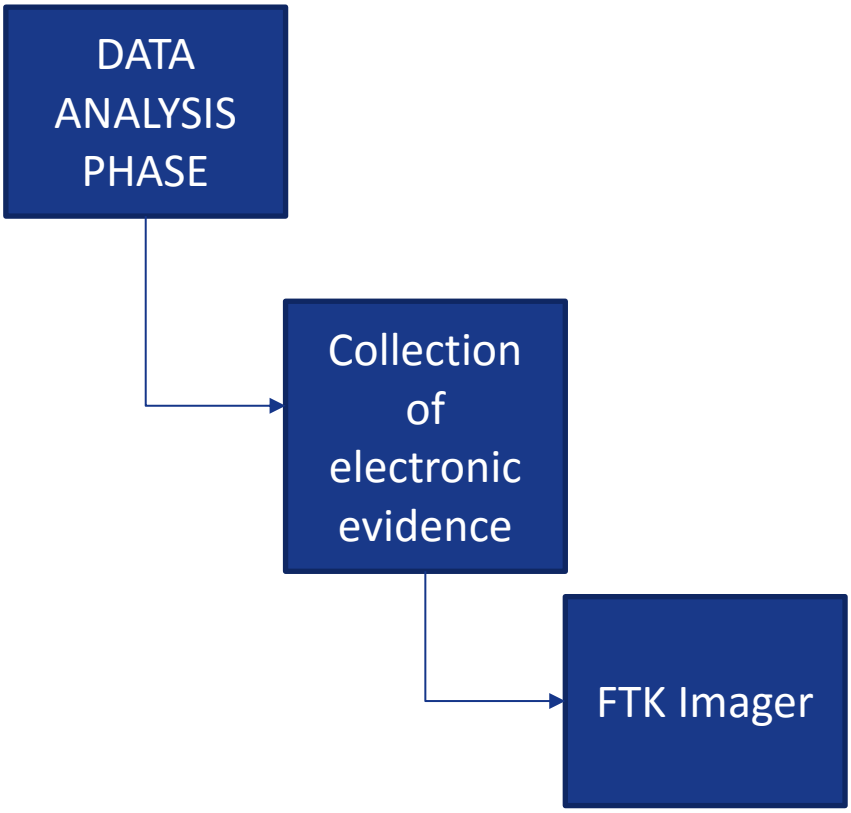

Figure 8 – The example of linking between IH process phase, particular action performer and one of the tools.

Figure 9 – Incident response tools boxes

3.2 Incident classification

Students will classify all three incidents according to the following taxonomies:

- eCSIRT.net taxonomy (http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6)
- CSIRT.PT taxonomy (http://www.cncs.gov.pt/CSIRT-pt-2/documents-2/)[5]

[5] This taxonomy was pointed out as the most appropriate in the ENISA paper on taxonomy for CSIRT and LEAs cooperation - see: https://www.enisa.europa.eu/news/enisa-news/enisa-report-on-information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement-agencies

4. Evaluation metrics

The proposed tasks have many solutions. The only well-developed solution which should be treated as referential is the incident handling general workflow presented on Figure 2 - Incident handling cycle. The other proposed solutions should be discussed between participating groups and moderated by a trainer.

One way to link the process phases, activities and tools is below. It does not include all cases and potential links, nor is it customised for the particular incident.

- Data analysis
  - Collection of electronic evidence
    - RegRipper
  - Data collection "generated" by the malicious code (pcap file)
    - Wireshark
- Resolution research
  - Incident resolution action proposed
    - Ransomware Response Kit
  - Preparing visualization of the attack
- Action proposed
  - Contact with hosting company
  - Contact with LEA
  - Restoring encrypted data from the backup
    - Windows Registry Recovery
- Action performed (based on "Action proposed")
- Eradication and recovery
  - Incident resolution – eradication and recovery
    - Ntop
  - Proposed "lessons learnt"
    - IOC Finder

Potentially, the classification proposal should match with solutions provided in the chapter 4.1 , but as there are different approaches to the classification, a trainer should be flexible and open for a discussion regarding the classification task.

4.1 Performance indicators

4.1.1 Phishing campaign (malware analysis)

Figure 10

MAIN METRICS	DETAILED METRICS
IH workflow/process	Check if the proposal is correct according to the process proposed in the ENISA "Good Practice Guide for Incident Management"
IH classification	Discuss the solutions proposals. The potential best choice is "Masquerade" (eCSIRT.net) and "Phishing" (CSIRT.PT classification)
Tools	Check if proposed tools match with the particular phases of the incident handling process

4.1.2 Computer break-in (computer forensics)

MAIN METRICS	DETAILED METRICS
IH workflow/process	Check if the proposal is correct according to the process proposed in the ENISA "Good Practice Guide for Incident Management"
IH classification	Discuss the solutions proposals. The potential best choice is "Exploiting of known Vulnerabilities" (eCSIRT.net) and "Exploit" (CSIRT.PT classification)
Tools	Check if proposed tools match with the particular phases of the incident handling process

4.1.3 Ransomware

MAIN METRICS	DETAILED METRICS
IH workflow/process	Check if the proposal is correct according to the process proposed in the ENISA "Good Practice Guide for Incident Management"
IH classification	Discuss the solutions proposals. The potential best choice is "Other" (eCSIRT.net) and "Ransomware" (CSIRT.PT classification)
Tools	Check if proposed tools match with the particular phases of the incident handling process

5. References

- ENISA Good Practice Guide for Incident Management

  https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management (last accessed on September 27th, 2016)

- mimikatz

  https://github.com/gentilkiwi/mimikatz (last accessed on September 27th, 2016)

- RegRipper

  https://github.com/keydet89/RegRipper2.8 (last accessed on September 27th, 2016)

- LOKI

  https://github.com/Neo23x0/Loki (last accessed on September 27th, 2016)

- Internet History Browser

  http://www.mitec.cz/ihb.html (last accessed on September 27th, 2016)

- Bro bro

  https://www.bro.org/ (last accessed on September 27th, 2016)

- IOC Finder

  https://www.fireeye.com/services/freeware/ioc-finder.html (last accessed on September 27th, 2016)

- FTK Imager

  http://accessdata.com/product-download/digital-forensics/ftk-download-page (last accessed on September 27th, 2016)

- DB Browser for SQLite

  https://github.com/sqlitebrowser/sqlitebrowser/releases (last accessed on September 27th, 2016)

- Ransomware Response Kit

  https://bitbucket.org/jadacyrus/ransomwareremovalkit/overview (last accessed on September 27th, 2016)

- Argus

  http://qosient.com/argus/ (last accessed on September 27th, 2016)

- Wireshark

  https://www.wireshark.org/ (last accessed on September 27th, 2016)

- KiTrap0D

https://www.exploit-db.com/exploits/11199/ (last accessed on September 27th, 2016)

- ChopShop

  https://github.com/MITRECND/chopshop (last accessed on September 27th, 2016)

- pwdump7

  http://www.tarasco.org/security/pwdump_7/ (last accessed on September 27th, 2016)

- Xplico

  http://www.xplico.org/ (last accessed on September 27th, 2016)

- REMnux

  https://remnux.org/ (last accessed on September 27th, 2016)

- BrowsingHistoryView

  http://www.nirsoft.net/utils/browsing_history_view.html (last accessed on September 27th, 2016)

- Fgdump

  http://foofus.net/goons/fizzgig/fgdump/ (last accessed on September 27th, 2016)

- Scalpel

  https://github.com/sleuthkit/scalpel (last accessed on September 27th, 2016)

- Windows File Analyzer

  http://www.mitec.cz/wfa.html (last accessed on September 27th, 2016)

- ID Ransomware

  https://id-ransomware.malwarehunterteam.com/index.php (last accessed on September 27th, 2016)

- OSForensics

  http://www.osforensics.com/ (last accessed on September 27th, 2016)

- Pestudio

  https://www.winitor.com/ (last accessed on September 27th, 2016)

- Ntop

  http://www.ntop.org/ (last accessed on September 27th, 2016)

- Rekall

  http://www.rekall-forensic.com/ (last accessed on September 27th, 2016)

- Log2timeline

https://github.com/log2timeline/plaso/wiki (last accessed on September 27th, 2016)

- Netcat

  https://debian-administration.org/article/58/Netcat_The_TCP/IP_Swiss_army_knife (last accessed on September 27th, 2016)

- Keimpx

  https://github.com/inquisb/keimpx (last accessed on September 27th, 2016)

- Belkasoft RAM Capturer

  https://belkasoft.com/ram-capturer (last accessed on September 27th, 2016)

- Cain & Abel

  http://www.oxid.it/cain.html (last accessed on September 27th, 2016)

- Windows Registry Recovery

  http://www.mitec.cz/wrr.html (last accessed on September 27th, 2016)

- WinHex

  https://www.x-ways.net/winhex/ (last accessed on September 27th, 2016)

- FlowViewer

  https://sourceforge.net/projects/flowviewer/ (last accessed on September 27th, 2016)

- Autopsy

  http://www.sleuthkit.org/autopsy/ (last accessed on September 27th, 2016)

- Proxifier

  https://www.proxifier.com/ (last accessed on September 27th, 2016)

- Using Indicators to enhance defence capabilities

  https://www.enisa.europa.eu/topics/csirt-cert-services/reactive-services/copy_of_actionable-information/Usingindicatorstoenhancedefencecapabilities.pdf (last accessed on September 27th, 2016)

- Identifying and handling cyber-crime traces

  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/legal-cooperation#identifying-and-handling-cyber-crime-traces (last accessed on September 27th, 2016)

- eCSIRT.net taxonomy

  http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6 (last accessed on September 27th, 2016)

- CSIRT.PT taxonomy

http://www.cncs.gov.pt/CSIRT-pt-2/documents-2/ (last accessed on September 27th, 2016)

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu