Incident Handling Management

Name | Job Title

Event | Location | Date

European Union Agency for Network and Information Security

The exercise objectives

What to focus on during initial analysis

Factors that affect incident handling priorities

How to communicate with media reporters and other third parties

What technical tools are used to resolve an incident

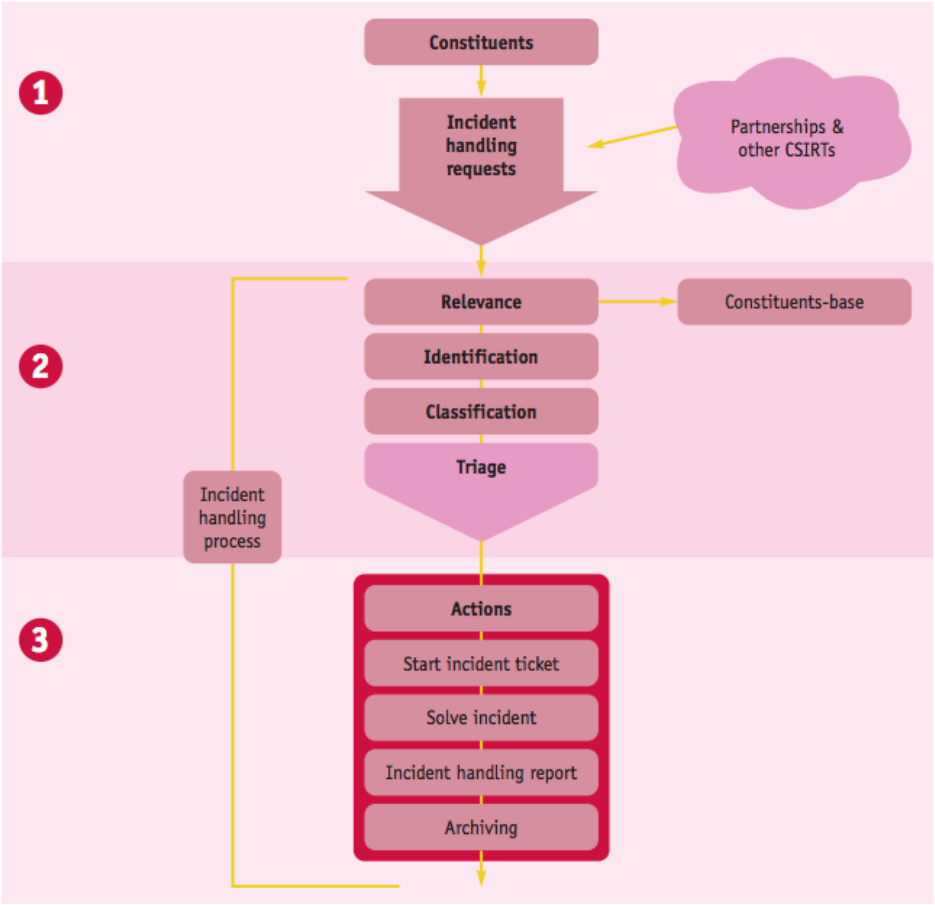
Introduction to the Incident Handling Management

Incident handling workflow

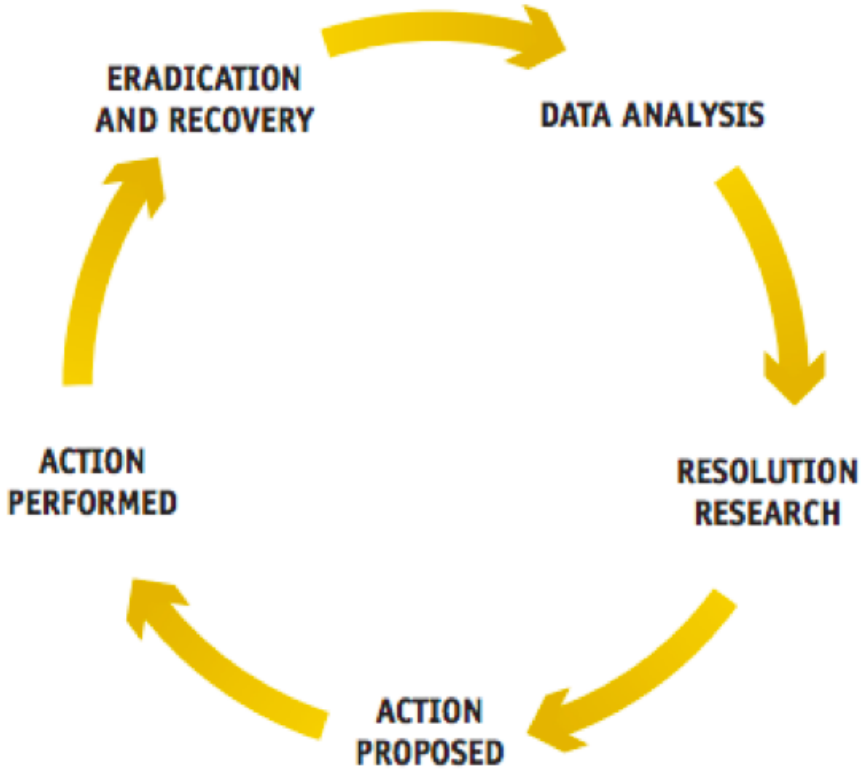
Incident handling phases

Incident handling tools

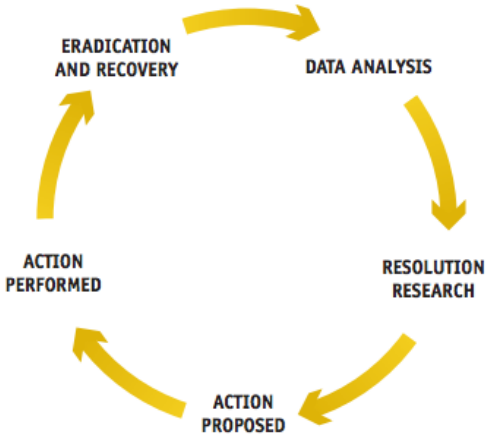
Introduction - Incident handling workflow



Introduction - Incident handling phases (cycle)



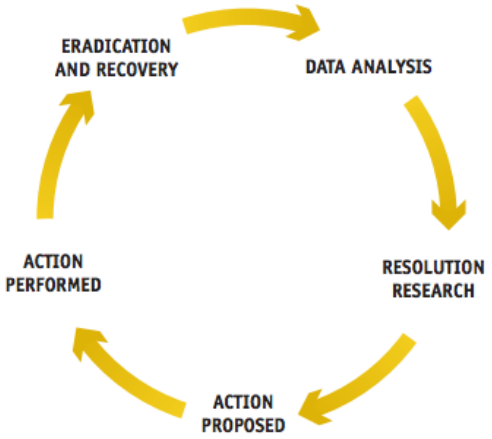
Introduction - Incident handling phases (cycle)



Data analysis

- Collect the data
  - Incident reporter
  - Monitoring systems
  - Reffering database
  - Other sources
- Consider future legal action
  - Use the best practices in collecting legally acceptable evidence

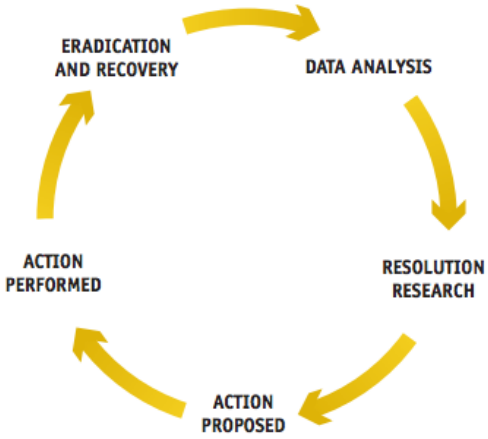
Introduction - Incident handling phases (cycle)



Data analysis

- Ask yourself:
  - 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?

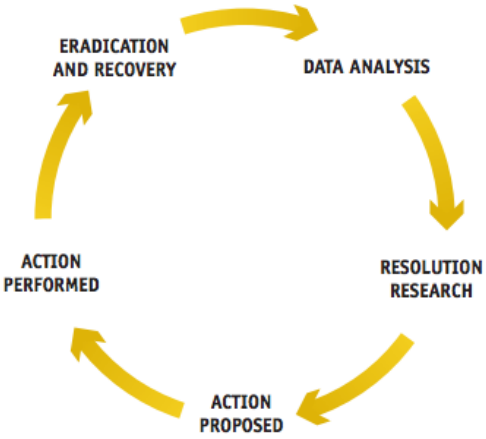
Introduction - Incident handling phases (cycle)



Resolution research

- Exchange ideas and observations
- Use the brainstorming model
- Organise short briefing sessions
- Reaction time is very important

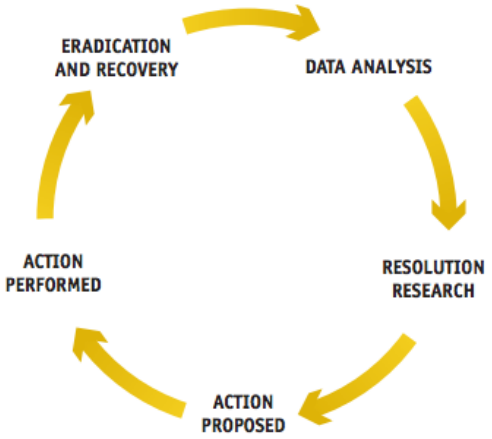
Introduction - Incident handling phases (cycle)



Action proposed

- You are the incident owner! Feel responsible for its resolution
- When contacting external parties – communicate in understood adjusted language – using “descriptive mode”
- Think what could be done by:
  - Attack target
  - CSIRTs
  - LEA
  - “Attacker” (owner of the attacking side)

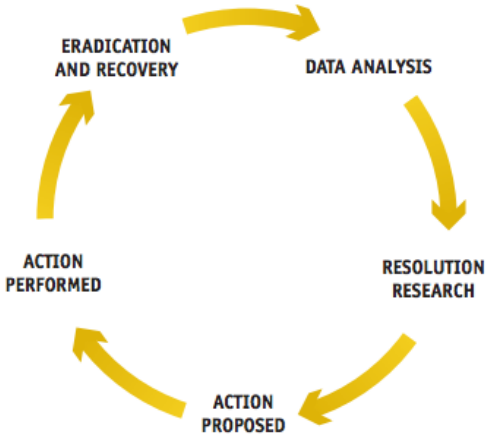
Introduction - Incident handling phases (cycle)



Action performed

- Use the action proposed as the plan
- Monitor the performance of actions:
  - 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.

Introduction - Incident handling phases (cycle)



Eradication and recovery

Recover or restore to normal the service

Incident handling tools

The table of the incident handling tools

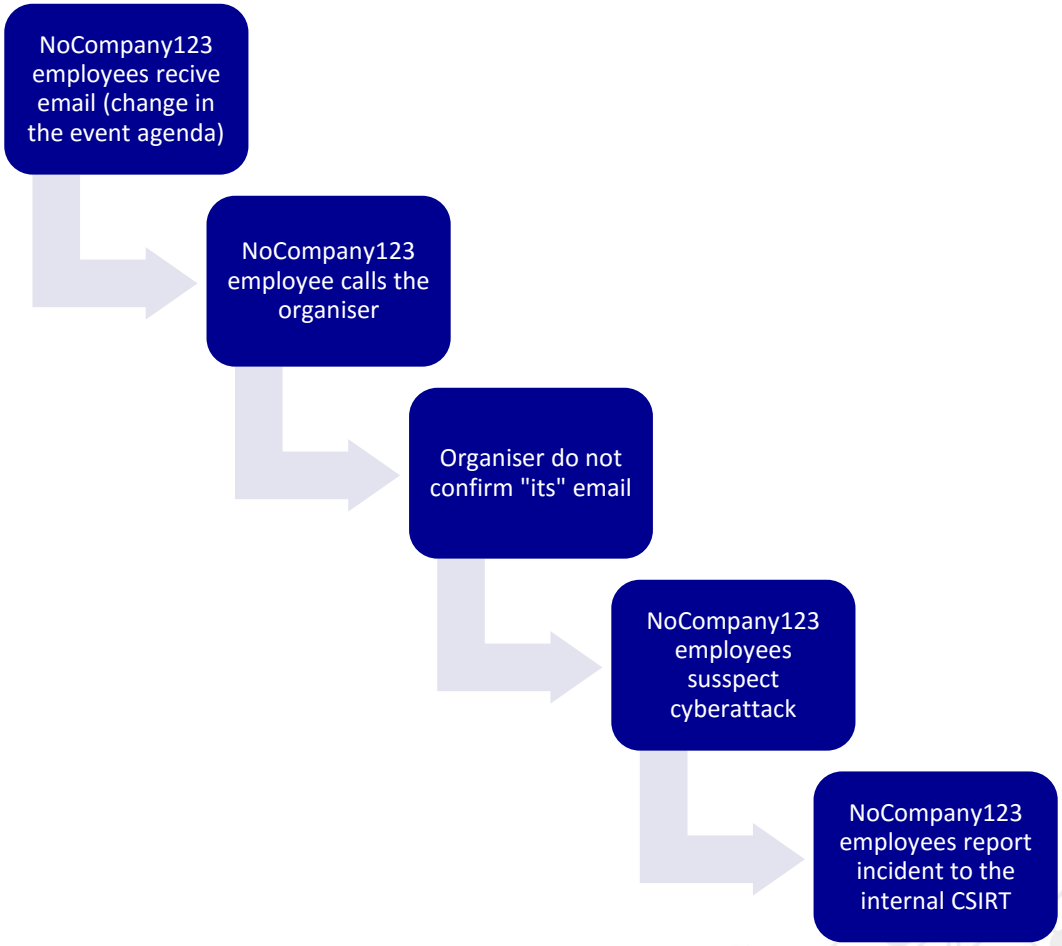
Recognize them

Learn the basics of their functionality

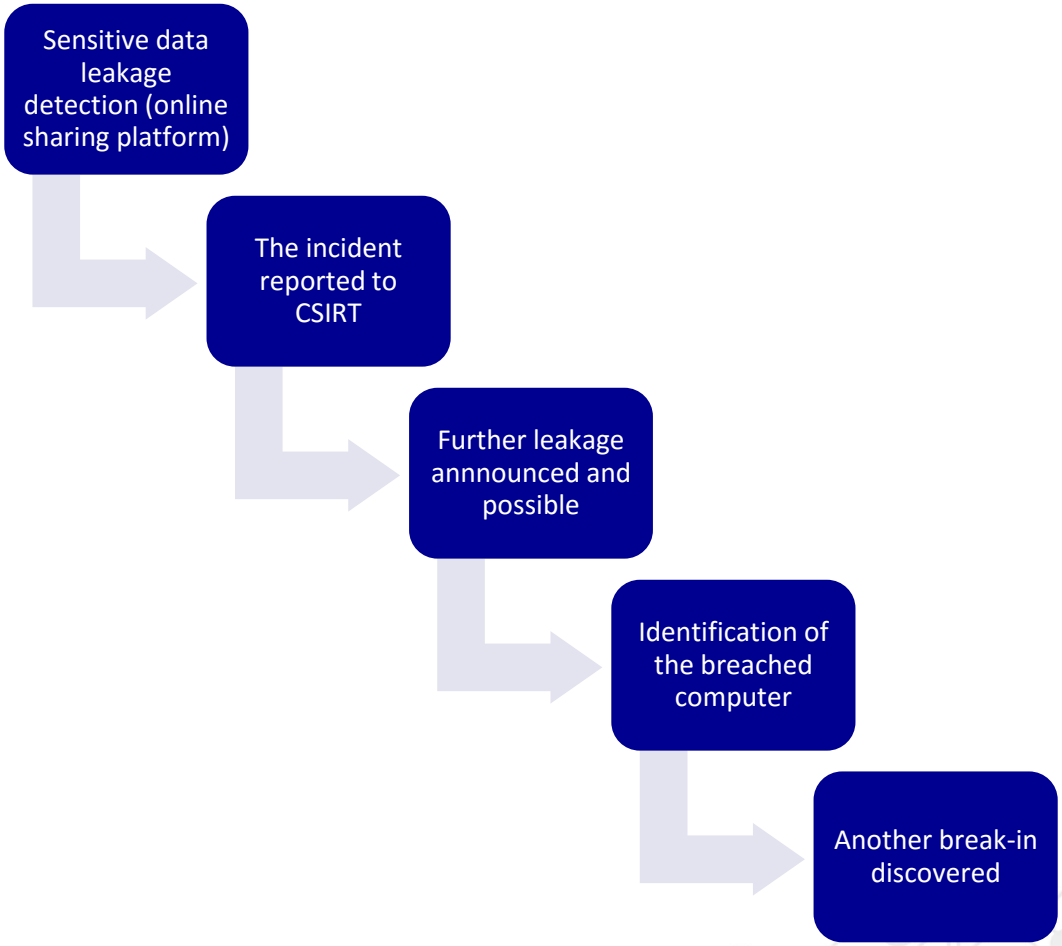
What do you think about these tools? Do you have any favourites?

What other tools do you consider useful?

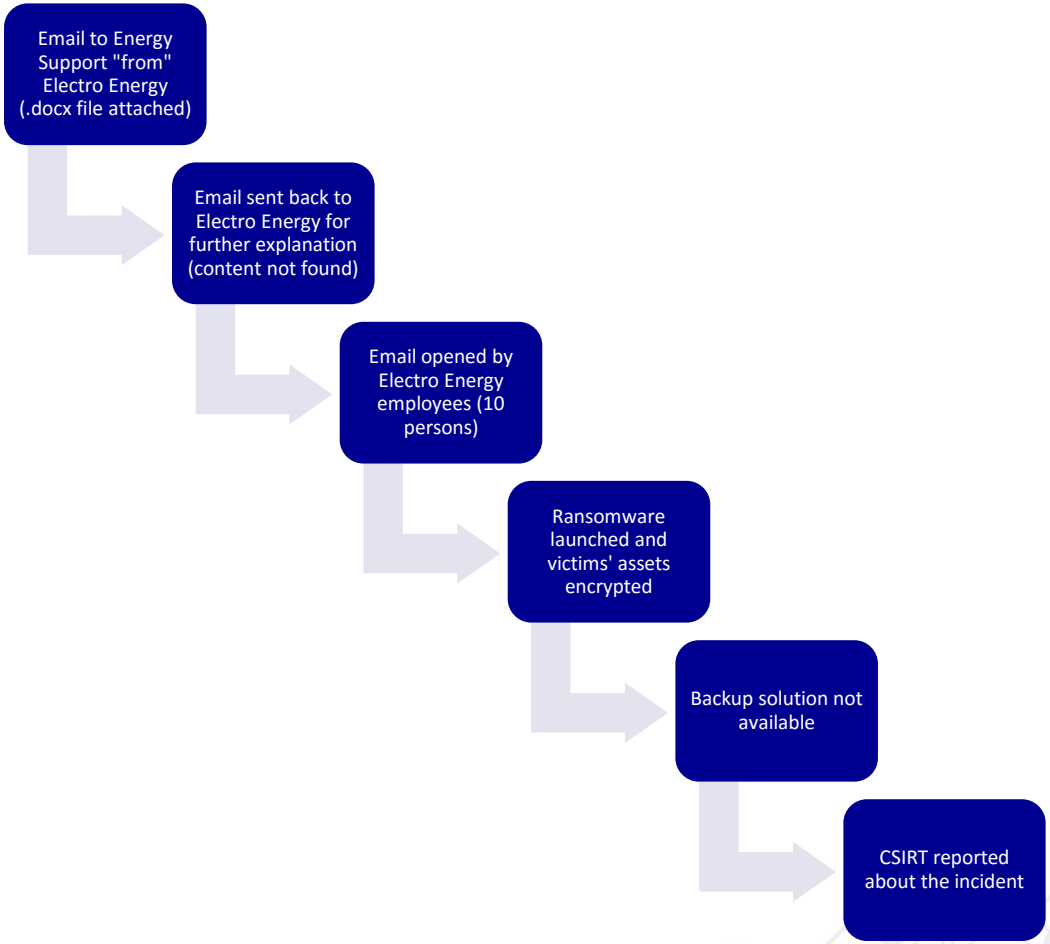
Incident 1 – Phishing campaign



Incident 2 – Computer brake-in



Incident 3 – Ransomware



Incident handling tasks

Incident resolution – action proposed

Collection of electronic evidence

Contact with hosting company

Ensuring validity of data (hardware / software)

Contact with LEA

Collected data validation

Incident resolution – data analysis

Physical disconnection of infected machines from the organization network

Defining Indicators of Compromise

Imaging the disk and memory dump

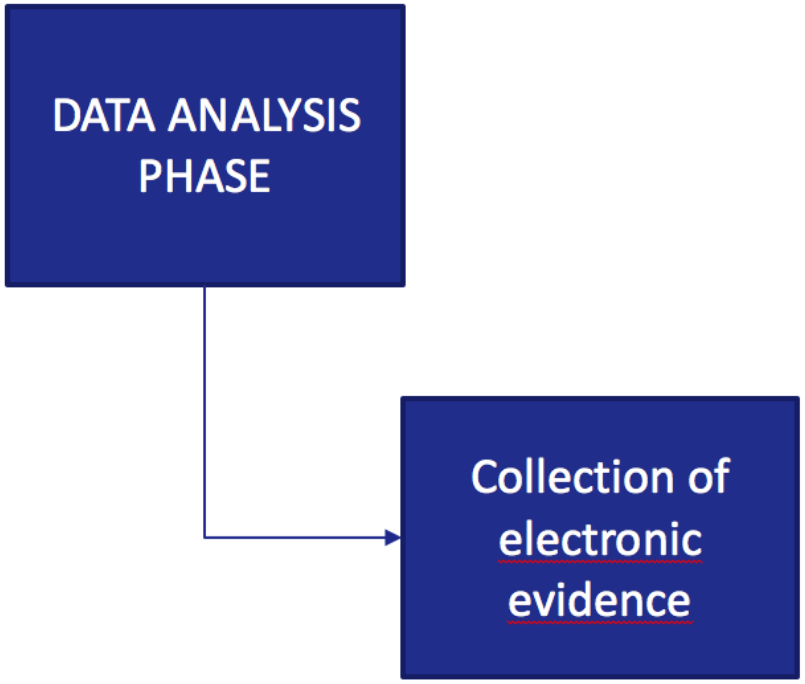
Contact with “attacking side” CSIRT

Incident verification

Incident handling workflow / process - Task 1

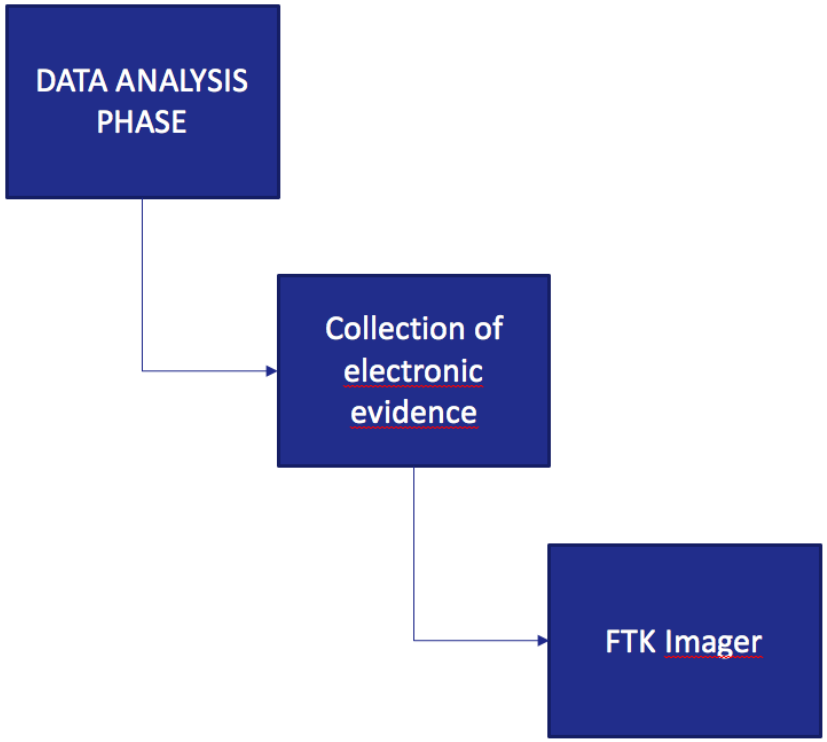
To identify and present the generic model for IH process

Incident handling workflow / process – Task 2



To identify and present the detailed process for particular scenarios

Incident handling workflow / process – Task 3



To recognize the functionality of the tools

Incident classification task – CSIRT.PT taxonomy

INCIDENT CLASS	INCIDENT TYPE
Malicious Code	Malware
	Botnet Drone
	Ransomware
	Malware Configuration
	C&C
Availability	DDoS
Information Gathering	Scanner
Intrusion Attempts	Exploit
	Brute-force
	IDS alert
Intrusion	Defacement
	Compromised
	Backdoor
Information Content Security	Dropzone
Fraud	Phishing
Abusive Content	SPAM
Vulnerable	Vulnerability Service
Other	Other

Incident classification task – eCSIRT.net taxonomy

Incident Class (mandatory input field)	**Incident Type** (optional but desired input field)	**Description / Examples**
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having an identical content.
	Harassment	Discreditation or discrimination of somebody (i.e. Cyberstalking)
	Child/Sexual/Violence/...	Child Pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...).
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting of known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoors, cross side scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	new attack signature	An attempt using an unknown exploit.

Incident classification task – eCSIRT.net taxonomy

Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYS- a. PING- flooding or E-mail bombing (DDoS: TFN, Trinity, etc.). However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore attacks are possible that intercepts and access information during transmission (wiretapping, spoofing or hijacking).
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Selling or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
Other	All incidents which don't fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

Get to work!

Any questions?

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu