Developing CSIRT Infrastructure

Handbook, Document for teachers

1.0

DECEMBER 2016

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 description

Main Objective	To learn what kind of software and hardware solutions could be used to provide a particular CSIRT service for a constituency.	
Targeted Audience	Technical and management CSIRT staff.	
Total duration	~3-4 hours	
Time Schedule	**Introduction to the exercise**	0.25 hour
	Task 1: Incident handling – incident analysis	1.00 hour
	Task 2: Further 3-5 services	2.00 hours
	Task 3: Summary	0.50 hour
Frequency	The exercise should be carried out when a new team is being established or plans to expand its services.	

The purpose of this exercise is to learn what kind of software and hardware solutions could be used to provide a particular CSIRT service for a constituency. By doing this exercise, students will learn about the connection between a set of services defined for their team and available IT solutions. This will help them to provide their services more easily and more effectively.

As a trainer, you should become familiar with the CSIRT services base, listed by the CERT/CC CSIRT[1]. This will be the basis of the discussion. It is recommended that for every service, the trainer should compose a list of freely available (as well as commercial, if needed) software solutions needed to provide the service.

All discussions should be moderated by the trainer.

[1] CERT/CC CSIRT Services overview https://www.cert.org/incident-management/services.cfm

2 Exercise course

2.1 Introduction to the exercise

At the beginning, introduce students to the exercise, outlining what its main tasks are and how the exercise will be carried out. This exercise consists of two main tasks:

TASK 1: Discuss the proposed infrastructures for the incident handling – incident analysis service

TASK 2: A further 3-5 scenarios.

At the beginning the students should receive a short introduction to the CSIRT services base, listed by the CERT/CC CSIRT[2]. Next, challenge the students to create a concept for providing these services using a proposed hardware and software infrastructure. Give an example of a step-by-step exercise to help the students understand how to proceed. In this exercise, we have chosen the incident handling – incident analysis service. The following scenarios will depend on what CERT/CC CSIRT services you and the students agree upon.

Explain the major topics and services of an incident response team to the students:

- **Reactive Services**
  These are the services in which the CSIRT responds to external influences, indicators, warnings, attacks, information and processes these according the organisational targets.
  - **Alerts and Warnings**
    Build and maintain infrastructure and processes to collect actionable information regarding incidents and distribute useful warnings to your constituency.
  - **Incident Handling**
    Collect or receive incident information, filter and communicate it with others
  - **Vulnerability Handling**
    An analogue to alerts and warnings: build and maintain the processes to receive or research information regarding vulnerabilities and distribute the information to your stakeholders.
  - **Artefacts Handling**
    Artefacts are files, objects or information related to a security incident found during the analysis. Handling these artefacts involves finding, preserving and analysing them.
- **Proactive Services**
  Proactive Services improve the protection of a CSIRT's constituency or prepare the field for successful containment and analysis of security incidents.
  - **Announcements**
    Announcements are broader than alerts and warnings and include new security developments, upcoming attacking vectors and background information.
  - **Technology Watch**
    The CSIRT monitors new technological developments and informs and prepares its community for them.

[2] CERT/CC CSIRT Services overview https://www.cert.org/incident-management/services.cfm

- **Security Audits or Assessments**
  Audits or assessments can help the organisations in your constituency improve and focus organisational and technical security measures.
- **Configuration and Maintenance of Security Tools, Applications, and Infrastructures**
  Provide guidance, consulting and operation of technical security measures.
- **Development of Security Tools**
  Develop tools to support CSIRT-specific processes and tasks.
- **Intrusion Detection Services**
  Provide the technical infrastructure and personnel to identify intrusions and other security-related incidents.
- **Security-Related Information Dissemination**
  Collect and prepare security information in a feasible manner for your stakeholders.

- **Service Quality Management Services**
  - **Risk Analysis**
    CSIRTS can provide valuable information to the Risk Analysis process using data acquired during the investigation of incidents regarding qualitative and quantitative measures. CSIRTS also benefit from the process by acquiring information regarding the status of network and systems, vulnerable or exposed systems and critical assets.
  - **Business Continuity and Disaster Recovery Planning**
    Similar to the Risk Analysis, CSIRTS can provide useful information and experience to BCM processes.
  - **Security Consulting**
    Defined between Proactive and SQM services, consulting its constituency (customers, users) can provide an IRT with a communication channel to improve the shape of the systems to be protected as well as gather information directly.
  - **Awareness Building**
    An incident response team will see attacks aimed at exploiting human behaviour often and early and will be able to prepare users for new approaches by attackers.
  - **Education/Training**
    Sharing knowledge with operation teams and users alike will improve the robustness and defensibility of the organisation.
  - **Product Evaluation or Certification**
    Defining standards and testing the compliance of products during the purchase process will help improve the security of the environment when new systems are introduced.

2.2 Keys to the exercise

2.2.1 Task 1: Discuss the proposed infrastructures for the incident handling – incident analysis service

Hand out the diagrams below to the students. Your goal is to discuss them with the students, asking the students to point out the strengths and weaknesses of the proposed solutions.

Lead the students by asking them questions, and bring them closer to possible answers step by step. Note, the answers do not have to be same as in this example, but should cover a similar range of options. The questions are presented below.

2.2.1.1 Simple (legacy) infrastructure

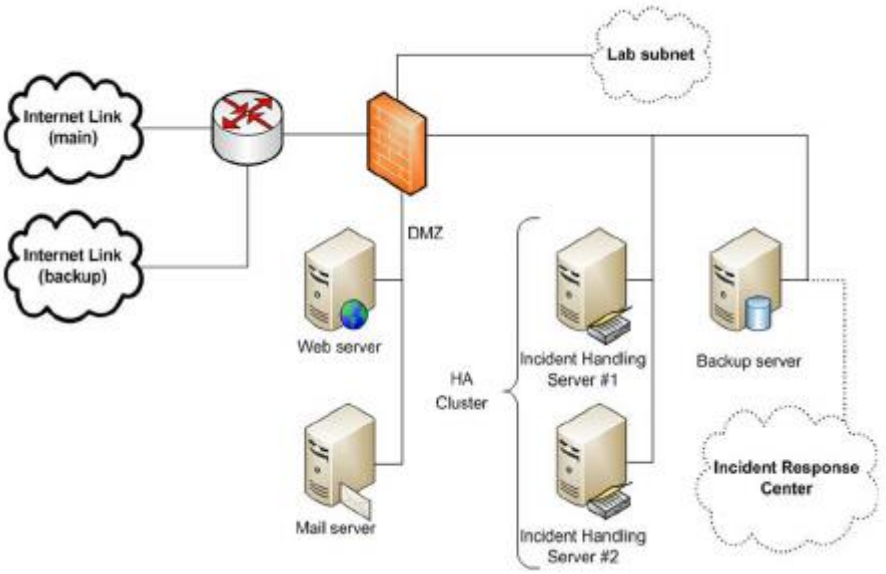

Figure 1 Simple CSIRT network infrastructure

Figure 1 shows a simple infrastructure for an incident response team. It includes the most important building blocks (Lab, Communication, Incident Handling, Incident Response), but is not very sophisticated and does not use the variety of technologies available today. This might be considered as a good starting point for a team in an early development phase.

2.2.1.2 Updated infrastructure with virtualisation

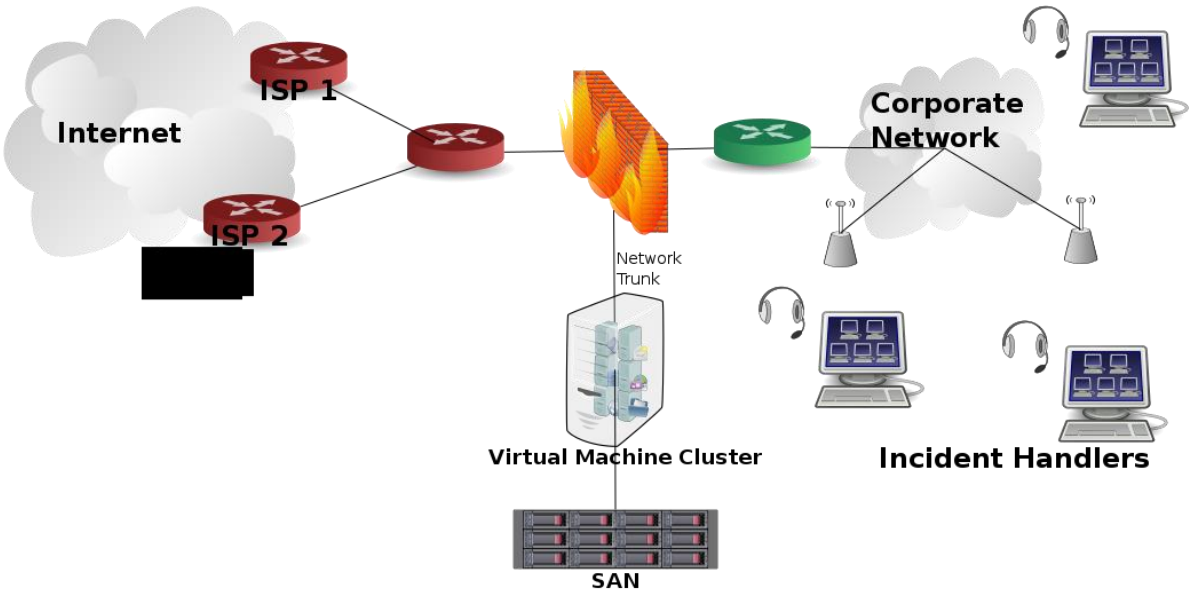

Figure 2 CSIRT infrastructure including virtualisation technologies

Figure 3 adds some more recent technology to the infrastructure like virtualisation, a storage area network (SAN) and Voice over IP (VoIP).

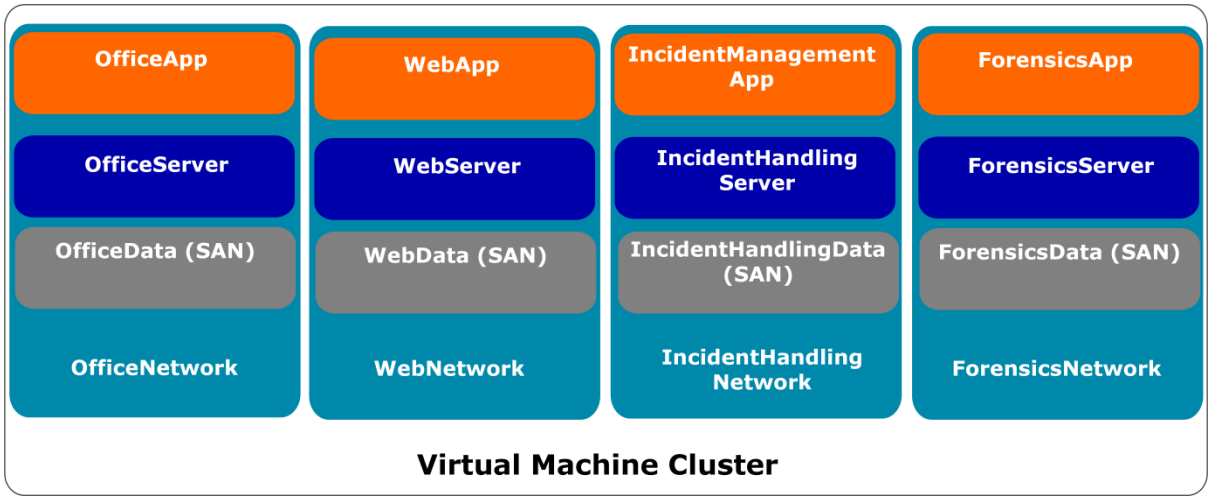

Figure 3 CSIRT infrastructure VM layers

Here we have a more detailed perspective of the different layers and incident handling applications deployed on the virtualisation hosts. The layers are Frontend, Services, Data/Storage and Network.

2.2.1.3 Enterprise-scale network architecture

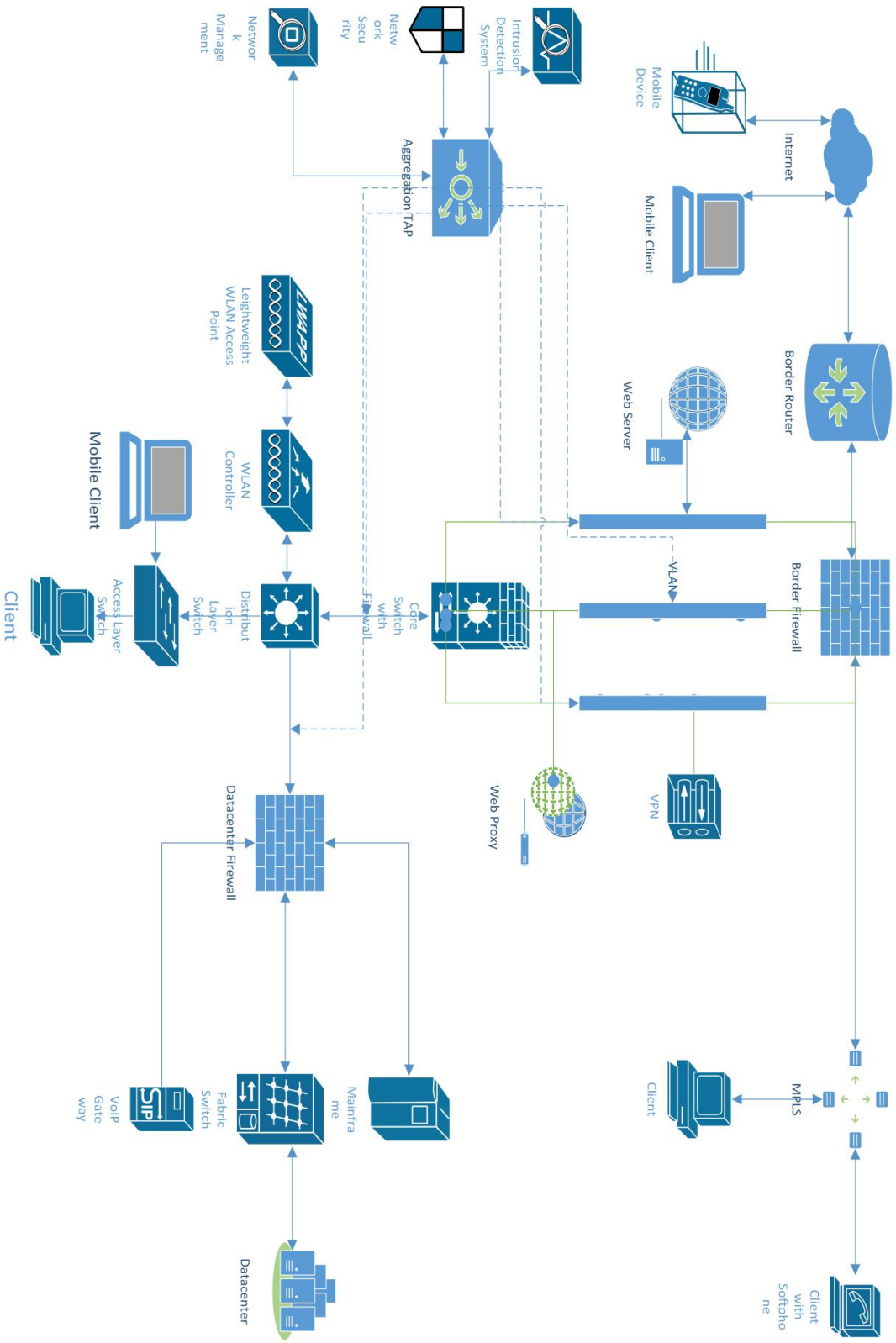

Figure 4 CSIRT Enterprise scale network

Figure 5 shows a network diagram trying to include technologies and devices to the picture that are usually found in enterprise networks and present a variety of challenges to incident response teams. The main blocks are Mobility and VPN, Physical and Virtual Network Segmentation, Datacentre (including Mainframes), Lightweight WLAN Deployment, VoIP and Traffic Access, and Analysis. This diagram can be used to ask the students to identify the building blocks, the technologies and technological challenges in each, and especially to ask them for potential sensible data sources in the network.

2.2.1.4 Incident response process

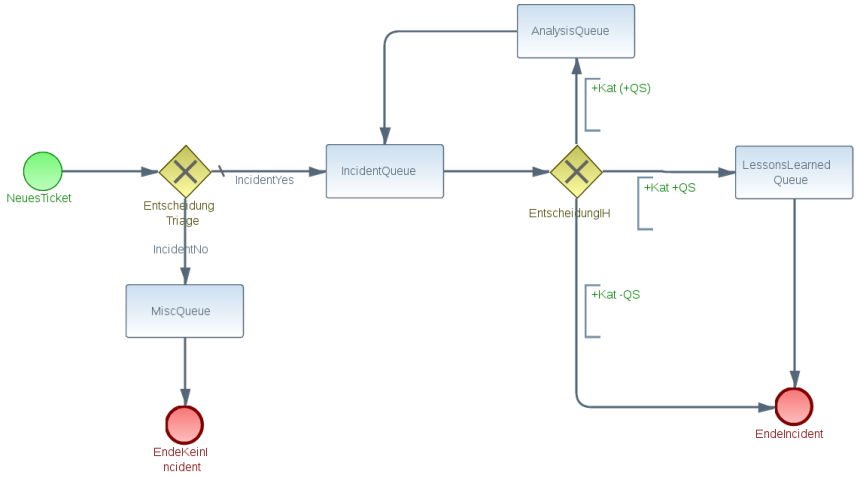

Figure 5 Incident response workflow

The chart in Figure 6 shows an example Incident Handling workflow (in this case it has been implemented in OTRS).

The following is an example workflow:

1. A new ticket is opened by an incoming report
2. A decision has to be made whether the report contains a security incident or not
3. If the report is related to a security incident the ticket will be moved into the IncidentQueue otherwise into the MiscQueue
4. In the next step, the assigned Handler decides how to proceed with the incident:
    a. The report is related to a previously known, analysed and solved incident, and the ticket will be closed immediately.
    b. The incident has been analysed and solved recently but the lessons learned phase has not been completed. The ticket will be moved to the LessonsLearnedQueue.
    c. The ticket contains a new incident; it will be moved into the AnalysisQueue.
5. In the AnalysisQueue, the incident will be taken care of by an analyst. When the incident has been understood, the ticket will be moved back into the IncidentQueue.
6. In the LessonsLearnedQueue the incident, its analysis and countermeasures will be prepared for and added to the knowledge base.

2.2.1.5 Example questions, hints and answers

Listed below are possible questions that could be asked regarding the incident handling service. Note that these are just suggestions and not an attempt at enumerating every possible issue. The answers are just examples as well and may not cover every issue. You should carefully think through the issues below and come up with additional answers or answers of your own, so that you will be able to moderate the discussion accordingly.

- Incidents could be reported via several ways or channels. Which of them should be maintained by CSIRT teams as a minimum?
    - The most basic channel is via the Internet. Usually, CSIRT teams use e-mail or web-page forms. Also telephone and fax should be available at a minimum. Every team should have a publicly available PGP[3] key.
    - More diverse channels would include social media presence like Facebook, Twitter and Chat environments (Signal, WhatsApp, Threema). Consider reasons to choose certain communication channels over others. What factors would impact the choice of communication channels (e.g. encryption, web-based versus mobile apps)? How would the communication channel used influence the information conveyed?
    - Discuss the requirements for social communication tools to be accepted as incident report channel.
- What tools can be used to better organize teamwork and information flow – especially for incidents reported via the Internet?
    - A possible open source incident handling system that could be used is Request Tracker for Incident Response[4] . If students do not know about RTIR, you could give a short overview of this tool. Look at the RTIR requirements.
    - Other open source ticket request solutions would be OTRS[5] or osTicket[6]
    - A mail server is needed. If you use Linux, free ones include Postfix[7], Sendmail[8] or Exim[9].
    - All mails targeted at the incident response centre should be passed through – no anti-spam or anti-virus rules should block traffic, or if they do, they should do it in a manner that enables the analysis of such traffic (look also at the question “how to secure CSIRT infrastructure?” below).
    - A web server will be useful: Apache[10] is a possible choice, nginx[11] would be another.
    - A large information display in the incident response centre, which everyone can see, is a good idea: it could be a projector which projects information onto a wall or screen or LCD/plasma displays. Information about current threats could be displayed here.
    - What are the possible sources of such information?

---

[3] The GNU Privacy Guard https://gnupg.org/
[4] RTIR http://bestpractical.com/rtir/
[5] OTRS https://www.otrs.com/
[6] osTicket https://github.com/osTicket/osTicket
[7] Postfix http://www.postfix.org/
[8] Sendmail http://www.sendmail.com/sm/open_source/
[9] Exim Internet Mailer http://www.exim.org/
[10] Apache Webserver: https://httpd.apache.org/
[11] nginx Webserver https://nginx.org/

    - How to build informative and usable dashboards?
- How should we organise the incident response process? (use Figure 5 Incident response workflow)
    - Ask the students to analyse and improve the given example process.
    - There should be an established position of 'duty officer of the day'. Every team member should hold this position interchangeably. The duty officer is responsible for, amongst other things, all incoming communication.
    - Discuss how many layers of seniority should be applied. Two layers meaning one 'duty officer' and everybody else, three differentiating handlers by work experience and introducing an additional escalation opportunity.
    - How incident notifications are to be handled outside working hours should also be addressed.
- Where should we store[12] incident reports, and why is this so important?
    - Every result of incident handling could be potential evidence. Every incident (report, analysis and the effect of the investigation) and all information gathered should be documented and safely stored. All electronic communications and data must be stored in a safe and secure way on servers. All non-electronic data must be stored safe and secure (for example a safe or lockbox). If you have the means, you should record your calls, but take note of privacy requirements in your jurisdiction. "This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence".
- How can we prevent a failure or outage of communication channels and servers?
    - There should be a backup Internet connection (via another autonomous ISP).
    - A backup telephone line (for example via GSM or other mobile service) is also a good idea.
    - To eliminate single points of failure, failover clusters should be deployed (critical services such as incident handling servers should consist of redundant nodes).
    - To minimize downtime and maximize availability, servers should be equipped with hot-swap RAID arrays and be connected to a UPS system.
    - Making regular backups is extremely important. Automatic backup system/scripts can be used. Created copies should be periodically verified to see whether they are usable.
- How can we monitor our network for the failure or outage of servers, internet connections, etc.?
    - A network monitoring system should be deployed to warn about failures or service status changes (open source solutions such as Nagios, Argus, Munin, and OpenNMS can be used). This information should be displayed on an information displayer (projector or LCD/plasma displays).
- How should we respond to network failures?
    - Emergency procedures should be developed in case of a network failure.
- How should we secure all CSIRT infrastructures?
    - Discuss the use of organisational and technical controls. Create a list of the most important ones.
    - Firewall(s) – where are they appropriate and not, how many should be deployed, which features should be used (Packet filter, intrusion prevention, application control, application level gateways)?
    - Discuss the usage of antivirus products, whether, where and how to deploy them.

[12] For more information, see "Processing and storing artefacts" https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational

- The physical security of infrastructure elements should be assured.
- Physical security should also cover confidential papers, faxes, documents, etc. Use a safe or locked cabinet.
- Server hardening as necessary and feasible.
- Pay special attention to designing virtual architectures, prepare different network zones as required by sensitivity and criticality. Discuss the use of VLAN versus physical separation.

Sometimes incident analysis requires going outside the network centre or lab. What tools are helpful in working remotely?

- Laptop
- Mobile phone
- Portable HDD or flash drive with large storage space
- Mobile device with internet connection and e-mail client, web browser, etc.?
- VPN

Some teams work as so-called "virtual teams", these do not share a physical location or office but rely on the communication and collaboration capabilities of internet services. Discuss the requirements for virtual teams in terms of the following topics.

- Workspace guidelines
- Real-time (text, voice, video) communication and information sensitivity
- Data exchange
- Hosting of server infrastructure
- Teambuilding
- Customer/constituency relationship

What basic software should you have for incident handling in the context of the first questions?

- For handling an incident via e-mail you should have an e-mail client installed.
- For handling an incident via RTIR/OTRS you should have Internet browsers installed.
- Supporting tools
  - Maltego CE[13]
  - AbuseHelper[14]
  - IntelMQ[15]
  - AIL Framework[16]
- Web services / Feeds[17]
  - Team Cymru[18]

[13] Maltego CE https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php
[14] AbuseHelper https://github.com/abusesa/abusehelper
[15] IntelMQ https://github.com/certtools/intelmq
[16] AIL Framework https://github.com/CIRCL/AIL-framework
[17] See also "Presenting, correlating and filtering various feeds" https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational
[18] Team Cymru https://www.team-cymru.org/

- Shadowserver[19]
- Virustotal[20]
- malwr[21]
- CIRCL[22]

What basic software[23] is needed to perform incident analysis?

- For network forensics
  - Tools for obtaining information about addresses, domain names, etc. (CLI: whois, dig, host; there are also web-based online versions of these tools.
  - Tools for analysing pcap files (CLI: tcpdump, GUI: Wireshark)
  - Tools for analysing netflow data (CLI: nfdump, GUI: nfsen)
  - Lab isolated with firewall: subnet and hosts computer forensics:
  - Tools for data preservation (hardware: DriveBlocker, etc.)
  - Tools for data analysis (EnCase)
  - Isolated lab: hosts and subnet
- For malware/binary analysis
  - Isolated and monitored lab: host or subnet with different types of operating systems, an IDS/IPS like Snort/Suricata/Bro to identify malware
  - Virtual environment (software: VirtualBox, VMware)
  - Reverse engineering tools

2.2.2 Task 2: Discuss the proposed infrastructure for a further 3-5 services

Once the first task has been completed, a set of services should be chosen, partly by the trainer, and partly by the students. The set chosen should include services from all main categories such as reactive services, proactive services and security quality management services. About 3-5 services should be chosen (see list of CERT/CC defined services in the table below).

In a manner similar to the previous exercise, the students should create a concept of providing those particular services using a hardware and software infrastructure. They should design a network environment, including computers, network devices and connections between them. It is important that the students face the task of the separation of the services in relation to their criticality. It is advisable that the trainer prepares, for each service, a basic set of solutions (as in the example exercise) in order to facilitate discussion. A checklist would be useful to evaluate proposals. How could the topology presented in the first task be extended to accommodate the new services?

Reactive Services	Proactive Services	Security Quality Management Services
- Alerts and Warnings	- Announcements	- Risk Analysis

[19] Shadowserver https://www.shadowserver.org/wiki/
[20] Virustotal https://www.virustotal.com/
[21] malwr https://malwr.com/
[22] CIRCL https://www.circl.lu/
[23] For an in-depth paper, look at “Building artefact handling and analysis environment” https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational

- Incident Handling - Incident analysis - Incident response on site - Incident response support - Incident response coordination - Vulnerability Handling - Vulnerability analysis - Vulnerability response - Vulnerability response coordination - Artefact Handling - Artefact analysis - Artefact response - Artefact response coordination	- Technology Watch - Security Audits or Assessments - Configuration and Maintenance of Security Tools, Applications, and Infrastructures - Development of Security Tools - Intrusion Detection Services - Security-Related Information Dissemination	- Business Continuity and Disaster Recovery Planning - Security Consulting - Awareness Building - Education/Training - Product Evaluation or Certification

Table 1 List of CSIRT services by CERT/CC

3 Conclusions

Summarize the exercise. By going through so many services, you and your students have created quite a large infrastructure. Compare these infrastructures with the one you initially thought of. Did the discussion contribute anything? If you have carried out this exercise before, how was the outcome different this time?

Encourage students to exchange their opinions, ask questions, and give their feedback about the exercise.

4 Evaluation Metrics

Evaluating the results of this exercise. The main criteria should be how active the students were during the discussions. Did they introduce new ideas? Use the checklists you prepared beforehand to track what students missed.

Use the following table as a starting point what to look for.

Question No.	Topic	Answers	Comment
1.	Incident report channels		
2.	Workflow organisation		
3.	Workflow organisation tool requirements		
4.	Incident information storage		
5.	Infrastructure availability		
6.	Infrastructure monitoring / Failure response		
7.	Infrastructure security		
8.	On premises incident response tools		
9.	Virtual team requirements		
10.	Incident handling tools		
11.	Basic incident analysis tools		

5 References

- CERT/CC CSIRT Services overview
  https://www.cert.org/incident-management/services.cfm (last accessed on September 27th, 2016)
- The GNU Privacy Guard
  https://gnupg.org/ (last accessed on September 27th, 2016)
- RTIR
  http://bestpractical.com/rtir/ (last accessed on September 27th, 2016)
- OTRS
  https://www.otrs.com/ (last accessed on September 27th, 2016)
- osTicket
  https://github.com/osTicket/osTicket (last accessed on September 27th, 2016)
- Postfix
  http://www.postfix.org/ (last accessed on September 27th, 2016)
- Sendmail
  http://www.sendmail.com/sm/open_source/ (last accessed on September 27th, 2016)
- Exim Internet Mailer
  http://www.exim.org/ (last accessed on September 27th, 2016)
- Apache Webserver
  https://httpd.apache.org/ (last accessed on September 27th, 2016)
- nginx Webserver
  https://nginx.org/ (last accessed on September 27th, 2016)
- For more information, see “Processing and storing artefacts”
  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational (last accessed on September 27th, 2016)
- Maltego CE
  https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php (last accessed on September 27th, 2016)
- AbuseHelper
  https://github.com/abusesa/abusehelper (last accessed on September 27th, 2016)
- IntelMQ
  https://github.com/certtools/intelmq (last accessed on September 27th, 2016)
- AIL Framework
  https://github.com/CIRCL/AIL-framework (last accessed on September 27th, 2016)
- See also “Presenting, correlating and filtering various feeds”
  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational (last accessed on September 27th, 2016)
- Team Cymru
  https://www.team-cymru.org/ (last accessed on September 27th, 2016)
- Shadowserver
  https://www.shadowserver.org/wiki/ (last accessed on September 27th, 2016)
- Virustotal
  https://www.virustotal.com/ (last accessed on September 27th, 2016)
- malwr
  https://malwr.com/ (last accessed on September 27th, 2016)
- CIRCL
  https://www.circl.lu/ (last accessed on September 27th, 2016)

- For an in-depth paper, look at “Building artefact handling and analysis environment” https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational (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