Guideline on Methodology of Organization and Functioning of CSIRTs at National Level

Content Table

Table List

Figures List

Introducion

This Guideline as drafted pursuant to Law No.2/2017 “On Cyber Security”, Article 7, point 3 and describes the process of establishing a sectoral CSIRT from the perspective of team managment, work process managment and technical perspective.

Communication networks and information systems have become an essential factor in economic and social development. The security of communication networks and information systems, and in particular their availability, ia s growing concern for society. This is due to the increased risk of problems that may occur in information systems, due to the complexity of the system, accidents, errors and attacks on physical infrastructure that provides essential services to citizens.

The Guideline serves as a working methodology for the establishmet and organization of CSIRTs by operators of critical and important information infrastructures, according to VKM No.222 date 26.04.2018 “On the approval of the List of Critical Information Infrastructures and the List of Important Information Infrastructures”.

Purpose

Defining rules for the establishment and operation of CSIRTs at the national level for the protection and enhancement of security levels in critical and important information infrastructures.

Objectives

1. Defining the rules/tasks for the funnctioning of the national and sectorial CSIRT.

2. Securing and maintaining communication networks and information systems to ensure availability, integrity and confidentiality, at OIKI and OIRI.

3. Establishment of a sectoral cooperation network to increase the level of security.

Definitions

"National CSIRT" – according to article 5, of Law No. 2/2017 "On Cyber Security"

"Sectoral CSIRT" – is the team/person responsible for Cyber Security Incidents, in the structure of an operator that manages critical and important information infrastructure. Sectoral CSIRTS are treated by name in the attached appendix VKM No.222 dated 26.04.2018 "On the appoval of the List of Critical Information Infrastructure and the List of Important Infrastructures of Information".

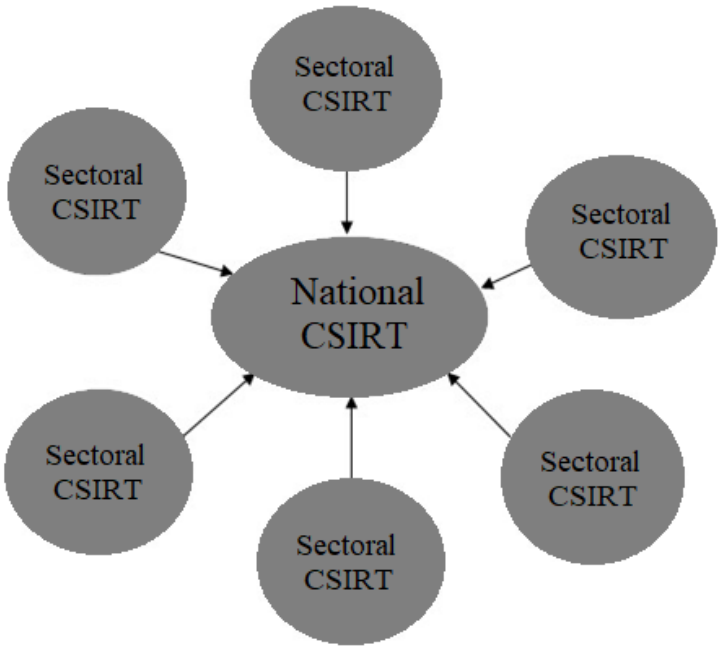


Figure 1. CSIRT presentation and reporting diagram

1. CSIRT life cycle managment

Several factors need to be considered before setting up a CSIRT. International organizations such as ENISA and FIRST recommend that the Plan-Do-Check-Act (PDCA) method be considered to properly plan team bulding and allow continuous structure improvement.

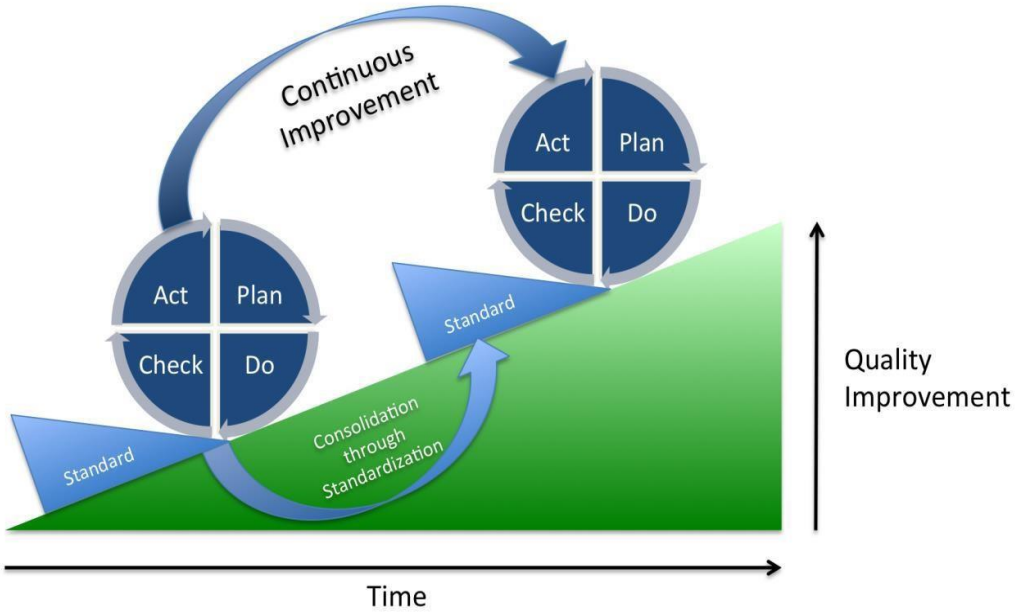


Figure 2. Presentation of PDCA cycle

Senior decision makers should consider the following elements, accordinf to the cycle presented above:

PLAN

Establishmet of the general framework of CSIRT

- This issue will be described in detail the next chapter and in the Appendix: "CSIRT General Framework Form"

Creating a budget

- Develop a multi-year budget plan, clearly separating costs and investmet costs and investmet costs
- Do not add unnecessary items to the budget and try to include any items necessary for the day-to-day operation of the team

Create a clear work plan

- The work plan should reflect the goals of CSIRT within the organization and show how the goals relate to the budget

DO

Implement the work plan

- As described in Chapters 4 and 5 ◦ Create an overview of information sources ◦ Create an Information Exchange and Handling policy ◦ Communicate the CSIRT (Inform other parties) ◦ Build trust network by attending conferences and seminars ◦ Practice this process continuously
- Perform CSIRT day-to-day incident handling operations (as described in the relevant chapter) and basic services (as described in Chapter 6).

CHECK

Analyze team performance

- Focus on the most important porcesses and tasks ◦ The ones you accomplish most often ◦ Those that require inconsistent accomplishment ◦ Those that require your extra control to imporve
- Set measurable objectives
- Involve all team members to share the commitment to accomplish tasks ◦ Identify what they have accomplished successfully and here improvement is needed ◦ Work with Quality Assurance (Department that insures safety of quality) if it exists in your organization ◦ Consider the involvmment of external consultants
- Conduct intervieiws with other employees of the organization ◦ What has CSIRT successfully accomplished? ◦ What are the areas that need improvement?
- Manage quality ◦ Is the work done according to processes and standards? ◦ Is the work documented? ◦ Are all the team members aware of the location of the documentation? ◦ Are meeting minutes reserved for future reference according to CSIRT needs? ◦ How is the cooperation within the team realized? ◦ Are records kept for attending training, conferences and seminars?

ACT

Determine what needs improvement

- After the results of the “CHECK” phase, improvements can be made according to the areas where they have been identified.
- As team services mature, additional services may be needed, as described in Chapter 6
- Start planning another “PLAN” phase to mplement the improvements, and follow all the phases up to the “ACT” phase.

After the creation of the CSIRT team, it is recommended that the "PDCA" cycle be performed once a year, to ensure that CSIRT requirements are reflected in the budget and are in line with the requirements of the organization itself.

1.1 Measuring and improving the mature level of CSIRT

One way to select the services that CSIRT will provide by measuring the level of team maturity, which varies from reactive services to the implementation of proactive services and quality managment.

Maturity levels along with a description for each level.

Maturity Level	Description
1. Beginner	CSIRT exists as a contact point for incident coordination and resolution. Regulations and policies have also been established for coordination with other reponsible authorities.
2. Basic	In addition to the first level qualitites, at this level CSIRT has implemented a process for dealing with new threats. A dedicated system is used for incident reporting, such as RTIR.
3. Active	In addition to the second level qualities, at this level CSIRT has implemented tools to analyze threats and there are procedures for classification and exchange of information.

4. Proactive	In addition to the third level qualities, at this level the CSIRT conducts regular checks to maintain security status and has planned ongoing training of team members.
5. Advanced	In addition to the fourth level qualities, at this level CSIRT monitors incidents and threats in real time. Guidelines for new threats and incident prevention are drafted and shared within and outside the organization in order to raise awareness.

CSIRT maturity levels refer to the five pillars of CSIRT functionality :

Creation
Work plan and identification of legal restrictions.

Organization
The mission and other internal organizational structures within the organization, and coordination with the other CSIRTs.

Human Factor
Team stuff, structure, expertise, code of behavior and training opportunities.

Tools
Everything needed to completed the given tasks.

Processes
For handling threats and incidents or interacting with the media.

Trusted Introducer has developed a standard for CSIRT maturity divided into three levels(trusted Introducer process: < https://www.trusted-introducer.org/processes/overview.html >

1. Listing
2. Accreditation
3. Certefication

1.2 Maturity self-assessment

The maturity of CSIRT can be assessed by the online team members themselves in one of the following sources:

- GCCS and NCSCNL[1]
- ENISA[2]

2. CSIRT General Framework

The general CSIRT framework explains in detail what CSIRT does, what resources it operates on and which target group of services it provides. Although CSIRTs operate in different fields and environments, the constituent elements needed to create them are the same. A form for these items can be found in Appendix A.

What is CSIRT?

CSIRT is a team of cyber security experts whose primary responsibility is to respond to cyber security incidents. The CSIRT team provides the necessary services to deal with incidents and to restore the affected system to working condition.

To minimize cyber risks, most CSIRTs can provide prevention and training services in the environment where they operate. They provide advices on vulnerabilities identified in the used software and hardware, as well as informs users of various threats, and updates to be made to devices and systems on a case-to-case basis.

2.1 Benefits of setting up CSIRT

A dedicated team of cyber security incident response, helps the organization to mitigate and prevent potential incidents, as well as protect its most valuable assets.

Other potential benefits are:

- Centralized coordination on security issues within the organization, through the designation of a central point of contact within the CSIRT for communication with the National CSIRT.
- Centralized and specialized treatment and response to security incidents.
- Providing expertise to the employees of the organization at any time in order to recover from security incidents.

[1] <https://check.ncsc.nl/>
[1] <https://www.enisa.europa.eu/topics/csirts-in-europe/csirtcapabilities/csirt-maturity/csirt-maturity-self-assessmentsurvey>

- Preservation of computer records in case lawsuits are field against the organization.
- Monitoring developments in the field of security and their integration within the organization.
- Promoting cooperation with other employees of the organization and raising awareness of safety issues for all its employees.
- Obtaining information on cyber aattacks in real time from counterparts in order to prevent cyber incidents.

2.2 Functional requirements of CSIRTs:

1. CSIRTs shoul ensure a high level of availability of their services and have some means at their disposal to contact and connect with others at all times.
2. Information systems administered by CSIRT must be located in physically secure areas.
3. CSIRTs should enable communication through an interacted platform for requests managments and their direction, in order to faciliate the managment of incident handling.
4. CSIRTs should have sufficient and qualified staff to ensure availability at all times.
5. CSIRTs CSIRTs must rely on an infrastructure, the continuity of which must be guaranteed.
6. CSIRTs should create opportunities to cooperate with international counterpart networks, to guarantee a higher standard of treatment and resolution of cyber incidents.

3. Basic skills of CSIRTs

According to ENISA, the basic skills that a CSIRT should posses are divided in four categories:

1. Services provided by CSIRT
2. Competencies and responsibilities of CSIRT
3. Operational skills of the CSIRT team
4. Dissemination of information

3.1 Services provided by CSIRT

The portofolio of services that a CSIRT provides to the organization:

<table>
<tr><th><u>Reactive Services</u></th><th><u>Proactive Services</u></th><th><u>Artifact training</u></th></tr>
<tr>
<td>

Alerts and warnings
Incident handling
Incident analysis
Support in responding to incidents
Coordination in responding to incidents
On site incident reponse
Addressing vulnerabilities
Vulnerability analysis
Responding to vulnerabilities

</td>
<td>

Announcements
Audit and safety assessments
Security configurations and maintenance
Development of security tools
Intrusion Detection Services
Distribution of valuable information to increase security

</td>
<td>

Artifacts analysis
Response to artifacts
Coordination for reponse to artifacts

Safety Quality Managment

Risk analysis
Business Continuity dhe Disaster Recovery
Security consulting
Awareness
Education/Training

</td>
</tr>
</table>

Tabela 1. CSIRT services based on CERT/CC

Proactive services aim to prevent incidents through awareness and training, while reactive services aim to address incidents and minimize harm.

Handling artifacrs involves analyzing any files or objects found on the organization's systems that could be involved in malicious actions, such as debris after a virus attack, trojan, etc. This includes handling and disseminating information to third parties to prevent further spread of malware and mitigate risks.
Quality assurance managment services are long-term services and include advisory and educational measures.

From the list above, Incident handling and incident analysis are the main and mandatory service to be performed by CSIRT teams. Furthermore, international organizations recommend that warnings be provided proactively and reactively. Dissemination of security information improves the functioning of the team and facilitates building trust in its capabilities in the face of the organization where it is set up.

Incident managment and alerts are services that CSIRT must provide itself, but may also outsource some of the lesser medium and long term emergency services.

Other services and measures should be implemented for the internal functioning of a CSIRT. It is generally necessary for a team to be aware of the security situation at all times in the organization where it operates, and on the Internet in general. All other services from the above list are considered in principle optional and their provision depends on the needs of the organization.

Most CSIRTs initially offer “Alerts and Warnings”, make “Announcements” and provide “Incident Treatment” for their organization. These basic services give a good profile to the organization and are a considered added values to it.

A good practice is to provide a small set of services, in the form of a pilot organization and then add services according to the needs of the organization and the history if attacks.

Once you understand the benefits of having a CSIRT and the types of services the team can provide to the organization, the next step is to set up a CSIRT by considering:

- Determine how to communicate with the rest of the organization
- Clearly define the mission of CSIRT
- Define a realistic project and implementation plan with achievable objectives
- Define the organizational structure of CSIRT
- Define Information Security policy
- Hire the right staff
- Seek the cooperation of other CSIRTs within the sector

Each of these issues is explained in detail below.

Communication way with the rest of the ogranization’s team

As stated above, it is very important to know the needs of the organization as well as the communication strategy of the organization, using the most appropriate communication channels.

CSIRTs operate using a set of communication channels. The most useful and important for an organization are listed below:

- Public website
- Private area of the organization’s webiste that requires membership according to certain criteria
- Web form to report incident
- Email lists
- Personalized case-to-case emails
- Telephone / Fax
- SMS
- Monthly and / or annual reports

Information must be disseminated securely, for example if e-mail communication is used, the latter must be digitally signed with PGP. Sensitive data when disturbed by e-mail should always be sent encrypted.

3.2 Competencies and responsibilities of CSIRT

The mandate / framework covering the competencies and responsiibilities of CSIRT

After analyzing the needs of the organization, the mission of CSIRT should not be defined. The CSIRT mission statement describes the basic function of the organization for the environment in which it operates, in terms of the products and / or services it provides. The mission also serves to define the functions of the CSIRT and to make known its existence.

It is good pracice to compactly define the mission statement, not in a narrow prism to ensure long-term compliance with CSIRT activity. Below is an example of the CSIRT mission statement:

Example 1

<CSIRT name> provides information and assistance to this <its constituents> in implementing proactive measures to reduce the risks of security incidents as well as responding to incidents when they occur.

Example 2

Provide support to the <Organization> for prevention and response to security incidents.

The role and responsibilities of CSDIRT should be clearly communicated to all other relevant actors in the industry where the team operates. Communicating the mission of each CSIRT to counterparts is important to avoid confusion and delays in disseminating information.

Tasks of secoral CSIRTs

1. Monitors critical and / or important information infrastructure systems on potential cyber incidents and / or attacks.
2. Provides back up of system data available.
3. Controls and manages cyber incidents.
4. Identifies and categorizes cyber incidents.
5. Access the extent of the incident and the damage caused.
6. Investigates in time and assesses the impact of the incident.

7. Informs in time about incidents that have an impact on OIKI / OIRI administrators.
8. Provide dynamic analysis of risk and incident and performs control over its content.
9. Keeps and preserves the chronology of all prrofs of the incident, in accordance with the legislaction in force for the protection of confidentiality.
10. Notify AKCESK immediately after identifying the incident.
11. Strictly follows the warning measures of the national CSIRT and / or notifies AKCESK in case of quick resolution of the incident.
12. Prepares and sends to the national CSIRT incident reports, according to the format approved by AKCESK.
13. Prevents similiar incidents in the future by taking preventive measures.
14. Recovers data and returns to normal the affected system within the time specified in the incident classification regulation, approved by AKCESK.
15. It should ensure increasing of staff capacities, through periodic training and certifications.

Tasks of National CSIRT

1. The national CSIRT organizes and coordinates the work with all operators of Critical and Important Information Infrastructures
2. The national CSIRT meets at least once every three months the sectoral CSIRT, in various problems in the field and increase cooperation.
3. Manages and handles any requests submitted by sectorl CSIRTs regarding potential cyber incidents.
4. Provides real-time assistance to sectoral CSIRTs, according to their requirements.
5. Provides early warning and disseminates the necessary information for taking preventive measures to operators regarding cyber risks and incidents.
6. Requires detailed reports from sectoral CSIRTs, for each cyber incident procedure.
7. In addition to its role as the National CSIRT, it also plays the role of the sectoral CSIRT in the case of the availability of critical and / or important information infrastructures.
8. Promotes and approves standards for incident handling procedures and measures for their prevention.
9. Develops and updates the incident classification scheme.
10. Publishes annual statistics of reported incidents.
11. The National Authority for Electronic Certification and Cyber Security (AKCESK) monitors the fulfillment of the tasks of the sectoral CSIRTs defined in this Guideline.
12. Organizes and coordinates periodic qualification trainings for capacity building of CSIRT teams in the field of cyber security.

The national CSIRT, in cooperation with international organizations, organizes at least one annual exercise, which simulates a cyber security incident, in order to test and update the protection capabilities of the systems as well as the training of CSIRT employees, for more professional incident management cybernetic.
At the end of the training, the participating CSIRT manager / employee prepares a brief report to the OIKI / OIRI administrator on the benefits received from the training.

3. 3 Operational skills of the CSIRT team

The structure of CSIRT is closely related to the structure of the organization of which CSIRT. The structure also depends on the approach of qualified experts who will be full-time part of the team or will work on an ad-hoc basis.

In order for a CSIRT to be effective, it must be proactive and define at least three key roles to help resolve the security incident.

1. The team responsible for incident response (technical operational team) that possesses the necessary technical knowledge and expertise to mitigate incident damage performs necessary repairs, regular audits, patches and handles incidents.
2. A legal expert, who drafts the necessary policies, advises the management team on the necessary legal actions and performs quality assurance tasks to ensure that the legal position of an organization is protected in the event of a security incident.
3. A communication expert, who helps the organization to communicate properly about the security incident with the public and other relevant channels to demonstrate trust even in times of crisis, and to facilitate open and adequate communication in order to protect the reputation of the organization.

A typical CSIRT is led by the general manager and the following roles are identified within the team:

- Technical operational team:
  - Technical team leader
  - Technical experts providing CSIRT services
  - Researchers

Role	Duty	Skills
CSIRT Manager	• General coordination for incident response • Communication with the decision makers of the organization • Provides appropriate staff, resources and skills to respond to incidents and requires outsourcing when needed • Periodically tests and updates the Incident Response Plan (PPI) • Document decisions, actions, procedures, inputs and outputs pertaining to PPI • If services are outsourced, he evaluates and controls the work on a case-by-case basis	• Ability to work in stressful situations • Knowledge of the organization's IT systems and work processes • Knowledge in effective personnel management • Excellent communication skills • Excellent organizational skills • Decision-making skills
Technical Leader	•Responsible for the technical work of the team • Responsible for the technical work of the team	• Excellent knowledge of cyber threats and incident response procedures • Excellent knowledge of internal team structure • Excellent communication skills
Other teammates	• Reacts to incidents according to PPI • Often takes responsibility for intrusion detection • Provides recommendations regarding new vulnerabilities and threats • Contributes to education and awareness raising within the organization	• Excellent technical skills related to network administration, programming, technical support or intrusion detection • The best situation would be for CSIRT to have at least one member capable in every important technological aspect • Specializing in technical areas such as network intrusion detection, malware analysis or forensics. • Problem solving skills and critical thinking

Table 2 Responsibilities of the CSIRT operational team

- Support team:
  - Legal consultant
  - Communication consultant

Role	Duty	Skills
Legal consultant	**Before the incident** • Reviews PPI for compliance with applicable legislation • Compiles notification forms for each type of incident • Disccuss with the communications consultant for edits in the press release format giving priority to the protection of confidential information and the interests of the organization	• Know the legal framework of cyber security • Experience in drafting agreements • Experience in dealing with law enforcement agencies • Problem solving skills • Well prepared and well organized to react properly and quickly in any situation.
	• Develops formats for information sharing agreements **During the incident** • If necessary, completes the raport of the incident with the communication consultant, and ensures that the notification is made known in a timely manner • Assists in gathering evidence when needed • Ensures proper documentation of events by considering the opening of legal issues to organization at any time • Can serve as a point of contact with agencies law enforcement	

Table 3 Responsibilities of CSIRT Legal Advisor

Roli	Detyra	Aftësitë
Communication consultant	• Assists in establishing communication policy on legal and managerial issues • Manages communication with the public • Manages communication with the media • Manages communication with employees of the organization • Acts as a contact point for any communication except law enforcement agencies • Sends security incident notifications to stakeholders after consultation with legal counsel	• Know the policies of the organization • Understand legal obligations, especially those related to the processing of sensitive and personal information • Understand the work of CSIRT • Excellent communication skills

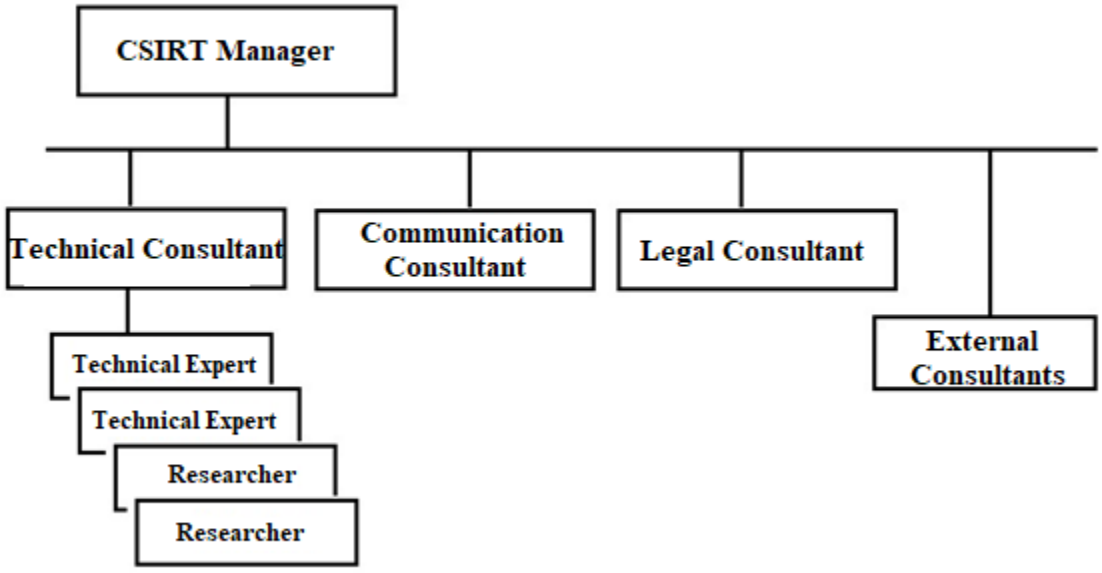
Table 4 Responsibilities of the CSIRT Communication Consultant

- External consultants:
  - Employed according to the needs of the organization

The presence of a legal consultant is very important, especially in the initial stages of setting up CSIRT. You may think it will increase costs, but in the end it will save you time and legal trouble.

Depending on the variety of expertise that CSIRT will offer, especially in cases where the organization has a high media profile, the presence of a communication expert is very important. The latter will translate technical issues into messages understandable to the media and the public. The communication expert will also serve as a bridge for CSIRT communication with the rest of the team, whenever explanations on various security issues will be needed.

The following is the organizational chart for the most common CSIRT organizational structure:



In the independent organizational structure model CSIRT acts as an independent and sole organization for managing its team employees.

3. 4 Dissemination of information

In this context, there are three elements that are considered important:

- trust and trust building
- quality and consistency of information and feedback
- common schemes and terminology

Trust and also building it, is a very complex issue that is influenced by many factors, so it is difficult to determine concrete requirements in this area. It is recommended to follow the guidelines of the National CERT in terms of cooperation and dissemination of information.

Sharing information between CSIRTs can only be successful if two requirements are met: all parties involved contribute equally and the level of quality of information provided is almost equal among all participants. The first request obliges CSIRTs to participate in information exchange activities to contribute with information in order to obtain it in exchange for the information they will provide. The second requirement ensures that the parties involved in the exchange of information benefit from the information disseminated by each team.

The information exchanged is understandable only if the terminology used by the parties is equally understandable by all. This helps to avoid ambiguities, and consequently, to avoid wrong reactions. Teams should use similar procedural schemes, for example for classifying information or for encrypting information. It is always advisable to review best practice and implement it where possible and appropriate.

4. Organization and functioning of CSIRT work

4.1 Staff employment criteria

After determining the services and the level of support that CSIRT will provide, the staff should be selected to carry out the work.

From the point of view of the necessary technical staff it is almost impossible to determine how many experts are needed, but the team has to perform the following tasks:

- In order to realize key incident warning and incident handling services international organizations advise that at least 4 full-time technical experts are needed
- For full operation of CSIRT and maintenance of systems owned by the organization, it is advisable to have a minimum of 6 to 8 full-time experts.
- For a 24/7 operation with two team shifts, it is advisable to have a minimum of 12 technical experts.

CSIRT technical experts must possess the following competencies:

Personal competencies

- Flexible, creative, ability to work in a team
- Strong analytical skills
- Ability to work in difficult situations
- Confidentiality in procedural matters
- Good organizational skills
- Writing and communication skills
- Open minded and willing to learn

Technical competencies

- Extensive knowledge of Internet technology and protocols
- Knowledge in Linux and Unix systems, depending on the systems used by the organization
- Knowledge in Windows systems
- Knowledge of network infrastructure devices (Router, switch, DNS, Proxy, Mail, etc.)
- Knowledge of web applications (SMTP, HTTP (S), FTP, SSH, etc.)
- Knowledge of security threats (DDoS, Phishing, Defacing, sniffing, etc.)
- Knowledge of risk assessment and practical applications

Additional competencies

- Ability to work 24/7 or be available when there is an emergency
- Similar work experiences in the past
- Level of education according to the job profile

Position	Qualifications and experience
CSIRT Manager	• Bachelor's and master's degrees in computer science, telecommunications and other fields related. • Professional certifications in the fields of CISSP / GCFA / CEH are an advantage • At least 5 years of experience in the field
Technical Experts	• Bachelor's and master's degrees in computer science, telecommunications and other fields related. • Professional certifications in the fields of CISSP / GCFA / CEH are an advantage • At least 1 year of experience in the field
Communication Consultant	• Bachelor's and master's degree in computer science, telecommunications or in the field of communication. • At least one year of field experience • Very good knowledge of at least one European language, English is an advantage
Legal Consultant	•Bachelor's and master's degree in law. •At least one year of field experience •Very good knowledge of at least one European language, English is an advantage

4. 2 Physical safety and use of equipment

Because CSIRT mainly processes sensitive information, it is recommended that the CSIRT team apply elements of physical security. This depends on the infrastructure and logistics of the organization, as well as the existing information security policy that the organization applies.

The functioning of a new CSIRT depends on the cooperation of the organization on which it stands in terms of policies, internal rules and other legal issues.

Listed below are the main facilities of a CSIRT:

General building rules

- Use of access control system
- The CSIRT office should only be accessible by the CSIRT team
- Monitoring of offices and entrances with cameras
- Archiving confidential information in safes
- Use of secure IT systems

General rules for IT equipment

- Use of equipment that the organization can support
- System maintenance
- Update systems before connecting to the Internet
- Use of security software (Firewall, anti-virus scanners, anti-spyware, etc.)
  More information is contained in Appendix C.

4. 3 Information security policies

Depending on the type of CSIRT, should be developed an information security policy. In addition to administrative, procedural and operational processes, security policy must be in line with applicable legislation and international security standards. The functioning of the CSIRT is conditioned by national laws and regulations, which are often based on the context of European legislation in the field, mainly on European directives and international agreements.

Laws and policies with which the information security policy for CSIRT should be in line are listed below, which are linked in Appendix E:

National Aspect

- Legislation in the field of information and communication technology[1]
- Laws on privacy and personal data protection[2]
- Codes of conduct for internet governance[3]

European aspects

- Directive on Electronic Signature (EU / 910/2014) [4]
- Directive on data protection and privacy in electronic communications GDPR (EU / 2016/679)[5]
- Directive on electronic communications networks and services (2002/19 / EC - 2002/22 / EC) [6]

International aspect

- Basel II Agreement (issues related to operational risk management) [7]
- European Convention on Cybercrime (23.11.2001) [8]
- European Convention on Human Rights (Article 8 on privacy) [9]

Standards

- BS 7799 Standard (Information Security) [10]
- ISO 2700X11 Standard [11]
- IT-Grundschutzbuch, EBIOS and others [12]

To ensure that CSIRT is complying with national and international legislation, consultations with the team's legal expert should be conducted, as well as cooperation with European counterparts.

Cooperation with other European CSIRTs

Assisting in resolving cyber incidents requires cooperation with European counterpart structures. A starting point for cooperation with European CSIRTs is the Inventory of European CERT activities published by ENISA.

European CSIRT Initiatives

TF - CSIRT

The CSIRT Task Force promotes cooperation between CSIRTs in Europe. Its main purpose is to provide a forum for the exchange of knowledge and experiences, to assist in the smooth running of new CSIRTs.

Competencies of the Task Force are:

- Provides a forum for the exchange of experiences and knowledge
- Establishes pilot services for the CSIRT community
- Promotes standards and procedures for responding to security incidents
- Assists in the creation of new CSIRTs in the training of their staff

[3] Activity inventory by ENISA http://www.enisa.europa.eu/cert_inventory/

CSIRT Global Initiatives

FIRST

FIRST is the global leader in responding to security incidents. Membership in FIRST enables member teams to respond more effectively to security incidents reactively and proactively. FIRST has members from various sectors starting from the government, commercial and academic sectors. FIRST aims to increase cooperation and coordination between member teams to stimulate faster response to incidents, and promote the exchange of information between members.

5. Handling incidents

This chapter describes the complete process and workflow for dealing with incidents. Each step is described in short paragraphs. Appendix C provides a complete overview of security tools.

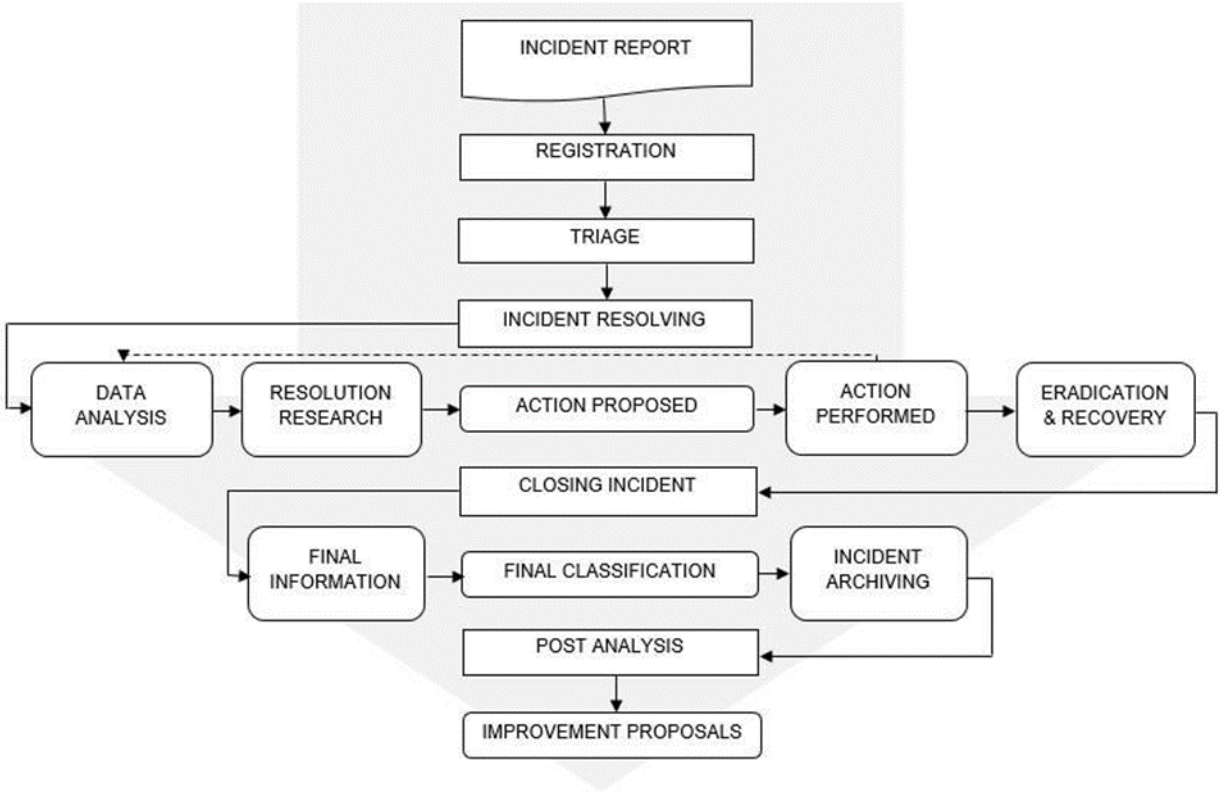


Figure 3. CSIRT independent model

[4] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.html

5.1 Reporting and recording the incident

5.1.1 Reporting

Incident reports come in a variety of forms and sources. Appendix B contains a cyber incident reporting form with all the information needed to record and handle an incident.

To receive an incident report, the CSIRT team must have the following information published:

- E-mail
- Telephone
- Fax
- etc.

In the communication forms that you make available for incident reporting do not forget to become independent from the internet. This means making contact forms such as telephone available to reporters, so that you can reach out to respond even if the internet is down.

Other sources include:

- Events identified by the internal monitoring network
- Membership of mailing lists with groups and organizations
- Membership in automatic subscription notifications. They can also refer to Appendix D on information sources.
- Radio, television and newspapers.

5.1.2 Registration

All reports must be recorded on the ticket. The ticket will be used throughout the incident handling process as a reference and will have a unique identification number. The ticket reference number will be used in all communications on it in the future, communications which refer specifically to the incident it represents.

Ticket registration systems can be configured automatically by linking to an email address. All emails sent to that address will create a new ticket (for new incidents) or add communication on an existing ticket, if the subject of the ticket includes the ticket reference number.

It is very important that all incidents are managed by the CSIRT team and handled by the same team. This is necessary because other incidents in the future will be handled by the same team and the solution will be given more quickly based on the treatment history.
Centralized incident recording also allows the use of early communications and similar treatments in the past.

Free systems for using incident tickets are RTIR (Request Tracker for Incident Response) and ORTS (Open Technology Real Services).

5.2 Selection

This is one of the most important steps in the incident handling process because some critical decisions are made.

Firstly, the verification is done; are we really dealing with an incident? How reliable is the source from which we received the incident report.

Once we find out that we are dealing with a cyber incident, CSIRT should answer the following questions:

- Is the incident within the competence of CSIRT?
- What is the impact of the incident?
- Are there opportunities for chain damage?
- How urgent is the resolution of the incident?
- Can the damage be caused with the incident increasing over time?
- Is there a possibility that the incident will spread?

Respond to the incident reporter:

- Let them know that you have received the report
- Explain how to proceed and what the reporter should expect from you
- Suggest what to do in the meantime, until the incident is resolved.

In this case, ready-made incident response forms can also be used, as they save you time.

5.2.1 Incident classification

Classify incidents. You may not have complete information from the initial reporting moment, but all of this information can be corrected in a second. The classification will help you determine the priority of incident handling, as well as help you determine the resources needed for further incident handling.

The following is an example of prioritizing incident handling by major organizations and governments around the world, according to ENISA sources.

Group	Priority	Example
Red	Very high	DdoS, Phishing
Orange	High	Trojan, unauthorized access
Yellow	Low	Spam

Table 5. Priority of incident handling

The categorization of incidents has a very important statistical function, because it allows CSIRT to:

- Recognize the trend of incident types
- Provide statistics / graphs for decision makers
- Compare the data available to other CSIRT teams

Examples of incident classification can be found in the following sources:

- On Common Language for Incident Response (by CERT / CC)
- eCSIRT.net taxonomy (developed during the eCSIRT.net project)

Incident classification can also be done by the CSIRT team members themselves. When deciding to define the incident categorization taxonomy yourself, comparison with other CSIRT teams can be difficult. Also make sure not to create too complex taxonomies (example: it is not recommended to define an incident category for each malware type); Although this may provide a very detailed picture of the types of incidents covered by CSIRT, it will take you longer to determine the type of incident than to resolve it.

An example of an incident classification based on the eCSIRT.net taxonomy is below.

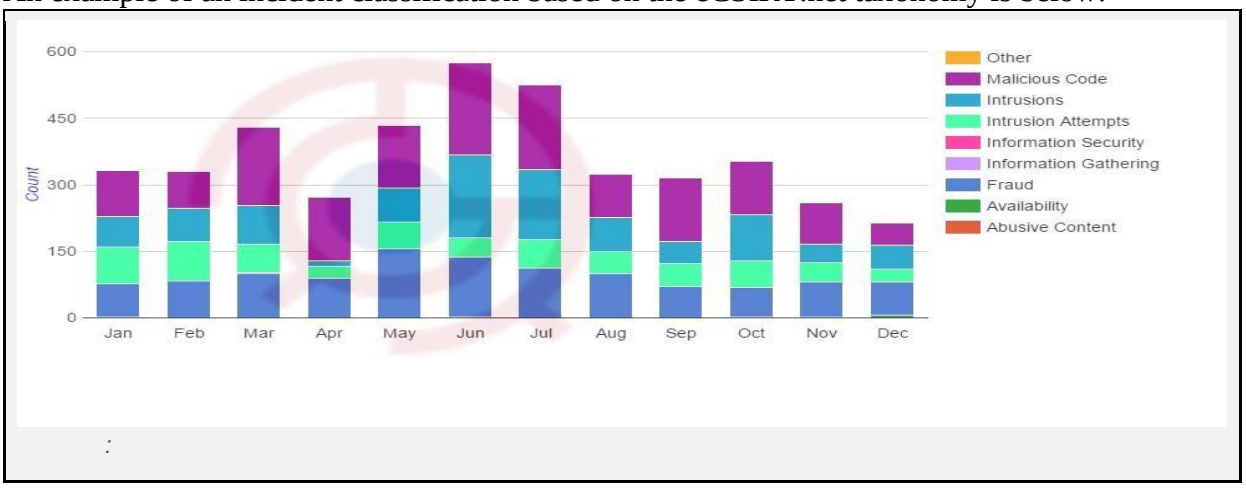


Table 6. Examples of incident classification

The final step of this phase is to designate one or more team members to resolve the incident, who will perform further ongoing tasks until the incident is fully resolved or closed.

5.3 Incident resolution

5.3.1 Data analysis

In this step, you should try to find as much information as possible to complete the panorama of the incident occurrence, along with the reasons that led to its occurrence.

Collect data from the reporting and from the system environment / systems affected by the incident:

- Detailed contact information
- Detailed description of the incident
- Incident classification as suggested by the incident reporter
- System operating system and network configuration data
- Accurate data on the time of the incident
- Data on the configuration of the security system of the organization
- Damage caused by the incident
- Logs that are included in the report

There are several places where the data you need can be found:

- Router logs
- Proxy server logs
- Web application logs
- Mail server logs
- DHCP server logs
- Authentication server logs
- Relevant databases of the affected system
- Firewall or intrusion detection devices

In cases where incident information is not located within the organization, you should determine what data you need, who has the data you need, and after notifying the parties who have this data, you should ask for access to the information they have.

5.3.2 Solution

With all the information gathered in the previous phase in this phase the best possible solution of the incident will be found. This is accomplished by analyzing the conclusions of similar incidents in the past. For more complex incidents it is suggested to perform brainstorming.

5.3.3 Treatment

Depending on the complexity of the incident, one or more actions are needed to handle the incident.
Before suggesting actions to be taken, consider the people who will carry out the actions - technical experts will understand the technical solutions, but if you need to take actions that are not technical but have a financial nature, for example, you should use appropriate terminology with responsible people.

Actions you may suggest include:

- Shutting down a service
- Scanning for malwares
- Perform patching for the system
- Isolation of the system or service
- Audit the system
- Gathering more information (perhaps by hiring third parties)
- Purchasing a service - such as DDoS protection
- Escalation of the incident to legal experts or senior decision makers
- Involvement of communication experts
- Involvement of law enforcement agencies for further investigation considering it a cybercrime
- If the system or application is provided by third parties, let them know and work with them if necessary

5.3.4 Verify

Verify the actions taken:

- Is the target of the attack achievable?
- Was the incident resolved by the treatment carried out in the previous step?
- Is the traffic properly filtered?

If the target of the attack is still vulnerable and the proposed solution has not closed the incident, repeat steps 1-3.

5.3.5 Recovery

Once the incident is resolved, the system can be restored to working condition. Keep in mind that in some cases restoring the system to working condition may take time even after the incident has been resolved, as a criminal investigation may be in progress.
In the event that communication experts are involved in the incident, make sure the information they will convey is up to date.

5.4 Closing the incident

There should be a clear policy on when the incident needs to be closed, as incident handling time constitutes an important statistic for the organization.

Some teams choose not to close the incident because new information may arrive at any time; some CSIRTs decide to close the incident when it is technically resolved, others CSIRTs close the incident only after other actions such as follow-up of the technical solution are taken.

5.4.1 Final information

Make sure all documents are included in the ticket identifying the incident. This is the moment to inform all parties involved:

- A brief description of what happened
- The result of the work
- Findings and recommendations

5.4.2 Final classification

Once you have provided all the information on the incident you should verify if the initial classification was correct. If the classification turns out to be different, consider it as a recommendation for other similar incidents in the future.

5.4.3 Incident archiving

At this stage the incident can be closed and archived.

It is advisable that the incident ticket be closed but be available for research purposes to members of the CSIRT team. Similar incidents may occur in the future, and consulting previous incident resolution strategies would save you a lot of time.

5.5 Post analysis

You can learn a lot from an incident, to prevent it in the future or to treat it faster.

Examples of recommendations you can implement after analyzing an incident are:

- Improvements to the organization's security policy
- Improvements in network architecture
- Improvements in detection mechanisms

CSIRT teams can share lessons learned with the security community or their counterparts to benefit from the knowledge gained.

6. CSIRT services

Session 3.1 defined the full list of services offered by a CSIRT, as defined by CERT / CC.

In addition to the services provided by CSIRT itself, other services can be obtained in the form of outsource. This can be a good solution for costly services such as digital forensics.

6.1 Reactive services

Reactive services serve to respond to requests / incident reports from the CSIRT organization and any threat or attack on CSIRT systems. Some services may be initiated by third-party notifications or by analyzing IDS monitoring or logs and alarms.

Alarms and warnings

This service includes the absorption of information coming from an attack, security vulnerability, alert, virus, etc., and provides short-term recommendations to deal with the problem. Information can be shared with other experts in the field within the organization.

Incident handling

Incident handling includes receiving, verifying and responding to requests and reports, as well as analyzing cyber incidents and events. Some of the activities at this stage include:

- taking action to protect systems and networks affected or threatened by attack
- apply incident treatment solutions and strategies based on recommendations
- look for possible attacks on other parts of the network
- filter network traffic
- patch system or equipment
- develop new strategies for responding to attacks

Since incident-handling activities are implemented in different ways by different types of CSIRTs, they are further categorized based on the type of activities performed and the type of assistance provided as follows:

Incident analysis

There are several levels of incident analysis, which are associated with sub-services. Incident analysis consists of examining all available information and accompanying evidence related to an incident or event. The purpose of incident analysis is to identify its purpose, extent of damage, nature of incident, and possible response strategies.
CSIRT can use the artifact analysis (described below) to find out more about the incident and the system it has affected.

CSIRT correlates activity across incidents to determine any correlation, trend or pattern. Two sub-services that can be done as part of incident analysis, depending on the mission, goals and processes of CSIRT, are:

- **Collecting evidence**

This subservice consists of collecting, storing, documenting, and analyzing records from a compromised device to a system. The tasks involved in this case are the realization of an image of the affected system, the control for changes such as new programs, files, services or users, the control of the processes that are being executed and the open gates, etc.

CSIRT staff performing this service may be called to criminal proceedings to testify on the evidence gathered.

- **Tracking**

Tracing the origin of the attack or identifying the system to which the attacker has access. This activity involves tracking how the attacker gained access to the system or network, which systems were used to gain access, what is the origin of the attack, and which systems or networks were used to carry out the attack until the final target. This may include identifying the attacker when possible. This service may require the cooperation of law enforcement agencies, Internet service providers or other stakeholders.

- **Incident response on site**

CSIRT provides direct on-site assistance to help the organization recover from an incident. CSIRT analyzes the affected system and performs system repair and recovery physically, instead of giving advice via email or phone, as will be described below. This service includes all verifications to be undertaken locally when an incident is suspected to have occurred or when the incident actually occurred. If the CSIRT employment offices are not physically located in the environment where the incident took place, members of the technical team should go to where the attack took place and respond. In other cases, a local team should always be physically close to the organization where it is set up and provide incident response services as part of their day-to-day work.

- **Incident response support**

CSIRT assists and directs the "victim" of the attack to achieve recovery by telephone, email, fax or other additional documentation. This may include technical assistance in interpreting the data collected, providing contact information or assistance with harm minimization and recovery strategies. In this case, no physical support is provided, on-site as in the case explained above. In this situation, CSIRT does not act on its own to achieve system or network recovery, but the personnel located near the affected system can perform recovery.

- **Coordination of incident response**

The CSIRT coordinates incident response efforts with all parties involved in the incident. Usually this includes the victim of the attack, other actors close to him, etc. Also there may be involved parties providing IT support to the victim of the attack, such as Internet service providers, other CSIRT partners, and the system or network administrator. Coordination work may include collecting contact details, announcing steps to be taken for the parties involved in the attack, collecting statistics on the number of parties involved, and facilitating the exchange of information.
Part of the coordination work can also be reporting and collaborating with the organization's legal department, human resources or public relations department. These include cooperation with law enforcement agencies. This service does not include on-site interaction for incident response.

- **Addressing vulnerabilities**

Vulnerability handling includes obtaining information and reporting on hardware and software vulnerabilities; analyzing the nature of vulnerability, its mechanisms, and consequences; as well as developing response strategies to detect and repair the system after the attack. Since the treatment of vulnerabilities is realized in different ways by different CSIRTs, this service is further categorized based on the type of activity that is realized and the type of assistance provided, as follows:

Vulnerability analysis

CSIRT conducts technical analysis and examinations of vulnerabilities in hardware and software. This includes verifying suspected vulnerabilities and technical examination of hardware or software to determine where the vulnerability is located and how it can be combated. The analysis may involve reviewing the source code using a debugger to determine where the vulnerability occurred, or the system may be copied to a test environment to perform all necessary examinations.

Responding to vulnerabilities

This service involves determining the appropriate response to repair or minimize vulnerability damage. This may include developing patches etc. Also included is announcing damage minimization strategies by creating stakeholder alerts.

Vulnerability response coordination

CSIRT notifies various parts of the organization about vulnerabilities and shares information on how to recover or minimize vulnerabilities. CSIRT verifies whether the vulnerability response strategy has been successfully implemented. This service may include communicating with

vendors, other CSIRTs, technical experts, constituent members, and individuals or groups who initially identified or reported the vulnerability.
Activities include facilitating the analysis of the vulnerability or vulnerability report; coordination of production schedules of corresponding documents, patches; and synthesizing technical analyzes done by different parties. This service may also include the preservation of a public or private archive or register of knowledge gained as a result of vulnerabilities addressed and corresponding response strategies.

Handling artifacts

Artifact is any file or object found on a system that may be involved in investigating or attacking systems and networks or being used to challenge system or network security measures.
Artifacts may include, but are not limited to, computer viruses, Trojan programs, worms, user scripts, and other toolkits.
Artifact handling involves obtaining information and copies of artifacts used in intrusion attacks, revelations, and other unauthorized or destructive activities. Once received, the artifact is reviewed. This includes analyzing the nature, mechanism, version, and use of artifacts; and developing (or suggesting) response strategies for detecting, removing, and protecting from these artifacts. As facility treatment activities are implemented in different ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance provided as follows:

Artifact analysis

CSIRT performs technical examination and analysis of any artifacts found in a system. The analysis done may include identifying the file type and structure of the object, comparing a new target against existing objects or other versions of the same artifact to see similarities and differences, reverse engineering or disassembly code to determine purpose and the function of the object.

Response to artifact

This service includes determining the appropriate actions for detecting and removing objects from a system, as well as actions to prevent the installation of objects. This may include updating your antivirus software or IDS system.

Coordinating the artifact response

This service involves sharing and synthesizing analysis results and response strategies belonging to an artifact with other researchers, CSIRTs, partners, and other security experts. Activities include notifying others and synthesizing technical analysis from a variety of sources. Activities may also include maintaining a public or private archive of known artifacts, their impact, and corresponding response strategies.

6.2 Proactive services

Proactive services are designed to improve the organization's security infrastructure and processes before any incident or event occurs or is detected. The main goals are to avoid incidents and reduce their impact and scope when they occur.

Notifications

This includes, but is not limited to, intrusion alerts, vulnerability alerts, and security advice. Such announcements inform the members of the organization about new developments with medium and long-term impact, such as new vulnerabilities or intruder tools.
Notifications enable participants to protect their systems and networks against new problems found before they can occur.

Technological developments

CSIRT monitors new technological developments, intervention activities and related trends to help identify future threats. Topics can be expanded to include the study of legal or legislative decisions, social or political threats, and new technologies. This service includes reading security posts, security websites, and current news and journal articles in the fields of science, technology, and policy to extract information relevant to the security of component systems and networks. This may involve communicating with other parties operating in these areas to ensure that the information or interpretation is accurate. The result of this service can be a kind of notice, Guideline or recommendation focused on the most important medium and long-term issues.

Audits and safety assessments

This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements set by the organization or the applicable industry standards. It may also include a review of organizational security practices.

There are different types of audits or safety assessments, including:

• Infrastructure Review: Manually review hardware, software, routers, firewalls, servers, and desktop configurations to ensure that they comply with security policies and standard organizational or industry best practice configurations.
• Best Practice Review: Interview system and network employees and administrators to determine if their security practices comply with defined organizational security policy or certain industry specific standards
• Scanning: Using vulnerability or virus scanning to determine which systems and networks are vulnerable.
• Penetration testing: Testing the security of an organization by intentionally attacking its systems and networks.

Prior to conducting such audits or evaluations, the approval of senior decision makers needs to be obtained. Some of the above assessments may be prohibited by organizational policy.
The provision of this service may include the development of a common set of practices against which tests or assessments are performed, together with the development of a required skills scheme or certification requirements for staff performing the tests, assessments, audits or reviews. This service may also be provided to a third party contractor or security service provider with the appropriate expertise in conducting audits and evaluations.

Configuration and Maintenance of Security Tools, Applications, Infrastructure and Services

This service identifies or provides appropriate guidance on how to securely configure and maintain the tools, applications, and general IT infrastructure used by the organization or CSIRT itself. In addition to providing instructions, CSIRT can perform configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, firewalls, virtual private networks (VPNs), etc. CSIRT can provide these services as part of their core function. CSIRT can also configure and maintain servers, computers, laptops, tablets, smartphones and other mobile devices according to security guidelines. This service involves scaling up the management of any problem towards high levels of decision-making considering the CSIRT system vulnerable to attacks.

Development of security tools

This service includes the development of any new, specific tools required by the organization or by CSIRT itself. This may include, for example, developing security patches for software that the organization uses or the secure distribution of software that can be used to rebuild compromised hosts. It may also include the development of tools or scripts that extend the functionality of existing security tools, such as a new plug-in for network vulnerability scanners, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms. .

Intrusion Detection Services

The CSIRTs that perform this service review existing IDS logs, analyze and initiate a response to any event that is within their competence or forward alerts under predefined service level agreements or escalation strategies.
Detecting intrusions and analyzing security-related records may not be an easy task - not only in determining where sensors can be found in the environment, but also in collecting and analyzing large amounts of data collected. In many cases, specialized tools or expertise are required to synthesize and interpret information to identify false alarms, attacks, or network events, and to implement strategies to eliminate or minimize such events. Some organizations choose to outsource this activity to others who have more expertise in performing these services, such as security management service providers.

Dissemination of security-related information

This service provides the organization with a comprehensive and easy-to-find collection of useful information that helps improve security. Such information may include:

IR reporting instructions and contact information for CSIRT:

- Archives of alerts, warnings and other notices
- Documentation about current best practices
- General guidelines for cyber security
- Policies, procedures and checklists
- Information on patch development and distribution
- Connections with partners
- Current statistics and trends in incident reporting
- Other information that may improve general security practices. This information may be developed and published by CSIRT or another part of the organization (IT, human resources or media relations) and may include information from external sources, like other CSIRTs, partners and security experts.

6.3 Safety and quality management services

Services in this category are not unique to incident handling or CSIRT in particular. They are services to improve the overall security of an organization. Utilizing the experiences gained in providing the reactive and proactive services described above, a CSIRT can bring unique perspectives to quality management services. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities and attacks. Such experiences in the services described below as part of a security and quality management process can enhance the long-term security efforts in an organization. Depending on the organizational structures and responsibilities, a CSIRT may offer some of these services, as follows:

Risk analysis

CSIRTs can perform risk analysis and assessments. This can improve the organization's ability to assess real threats, provide realistic qualitative and quantitative risk assessments for information assets, and evaluate defense and response strategies. CSIRTs providing this service will perform or assist information security risk analysis activities for new systems and business processes or assess threats and attacks on assets and component systems.

Business Continuity and Disaster Recovery Planning

Based on past events and future forecasts of incidents or safety trends, more and more incidents have the potential to result in a serious degradation of business activities. Therefore, planning should be oriented towards CSIRT experience and recommendations on how to respond to such incidents to ensure continuity of business operations. CSIRTs performing this service are involved in business continuity and disaster recovery planning for events related to cyber security threats and attacks.

Security consulting

CSIRTs can be used to provide advice and guidance on best security practices to apply to voter's business operations. A CSIRT that provides this service is involved in preparing recommendations or identifying requirements for purchasing, installing or securing new systems, network equipment, software applications, or business-wide processes. This service includes providing guidance and assistance in developing organizational security policies.
It may also include giving advice to law enforcement or other government bodies.

Awareness

The CSIRT should be able to identify what more information and guidance members of the organization require in order to better comply with security practices and organizational security policies. Raising security awareness not only improves understanding of security issues, but also helps to carry out day-to-day operations in a safer way. This can reduce the occurrence of attacks and increase the likelihood that detection and reporting will occur more quickly, minimizing losses.

CSIRTs that perform this service raise safety awareness through the development of articles, posters, newspapers, websites, or other information resources that explain best security practices and provide advice on precautions to take.

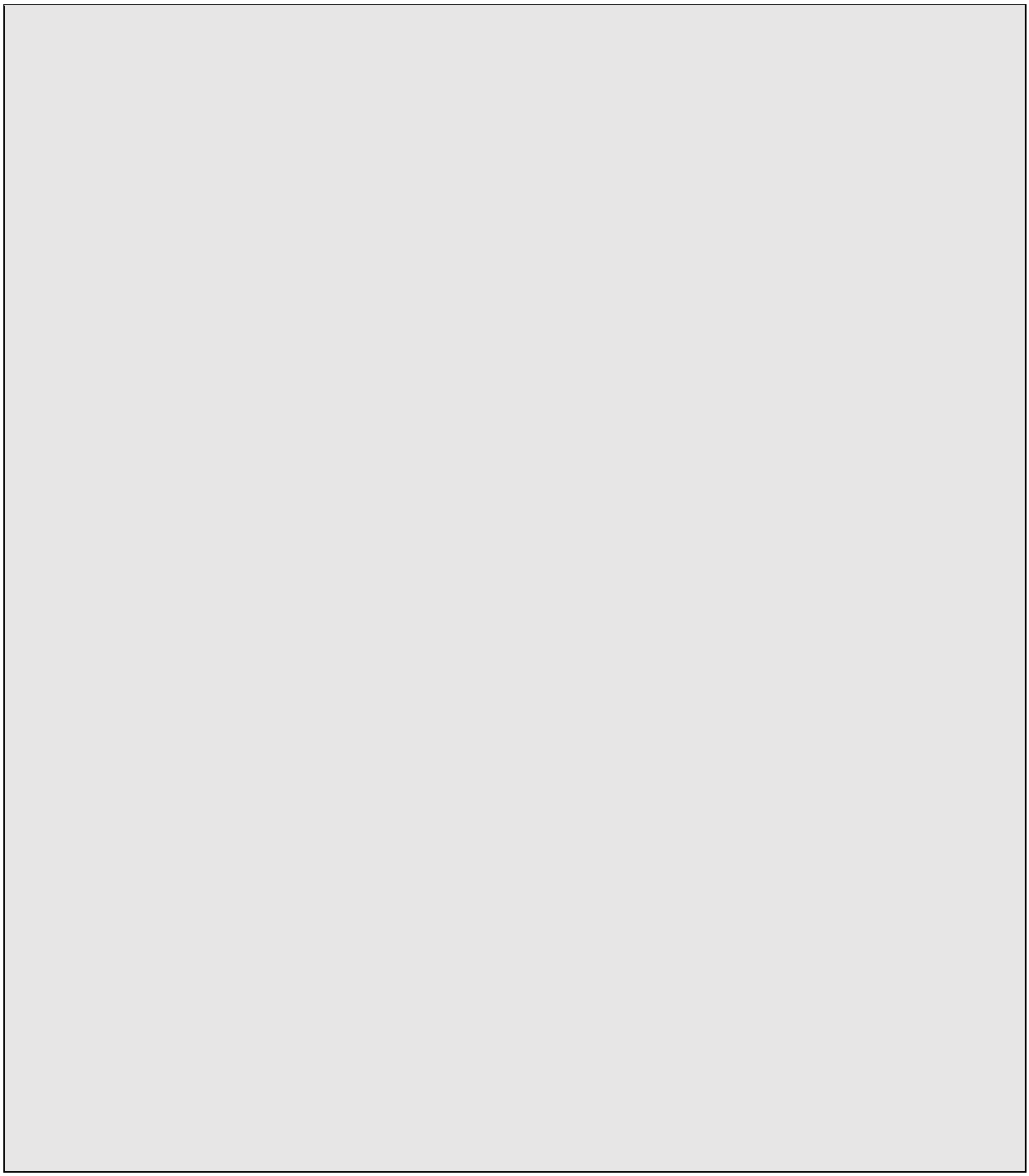
Activities may also include planning meetings and workshops to stay in touch with ongoing security procedures and potential threats to organizational systems.

Education / Training

This service includes providing information to the organization's employees about cyber security issues through seminars, workshops, courses and tutorials. Topics may include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information needed to protect, detect, report, and respond to cyber security incidents.

Appendix A: CSIRT General Framework Form

CSIRT General Framework
CSIRT's Name: Mission: Intitution / Organization: Organizational structure: Availability: Services: Staff: Infrastructure and available tools: Relations with other parties: Financial model:



Appendix B: Incident Reporting Form

INCIDENT REPORTING FORM

Please fill in the form and send it by email to the address....
Fields with * are required to be completed:

Contact details:
1. Name *:
2. Name of the organization *:
3. Sector:
4. Country *:
5. City:
6. E-Mail *:
7. Telephone number *:
8. Next:

Hosts affected
9. Number of hosts:
10. Hostname & IP *:
11. Host Function *:
12. Time-Zone:
13. Hardware:
14. Operating System:
15. Affected software:
16. Affected files:
17. Protocol / port:

Incident
18. Reference number ref #:
19. Type of Incident:
20. Incident start (time):
21. This is an ongoing incident: YES NO
22. Time and method of detection:
23. Known vulnerabilities:
24. Suspicious files:
25. Countermeasures:
26. Detailed description *:

Appendix C: Security Tools

There are many tools to assist CSIRTs in their work in dealing with incidents, and many of them are free to use.
Remember that most log files are saved in plain text format and can be easily retrieved from command-line like sed, awk and crochet on Unix / Linux. The same tools can be used to convert them to different formats in order to be analyzed by more advanced tools.
Find a list of analytics tools below:

Table 7. Analyzing tools

Domain and IP address query tools	
DomainTools	<https://www.domaintools.com/>
Domain Dossier	<http://centralops.net/co/DomainDossier.aspx>
IP to ASN Mapping	<http://www.team-cymru.org/IP-ASN-mapping.html>
GeoLite2	<http://dev.maxmind.com/geoip/geoip2/geolite2/>
RIPEstat	<https://stat.ripe.net/>
E-mail header analysis tools	
Google Apps Messageheader	<https://toolbox.googleapps.com/apps/messageheader/>
MXToolbox	<http://mxtoolbox.com/EmailHeaders.aspx>
Network monitoring tools	
nfdump	<http://nfdump.sourceforge.net/>
nfsen	<http://nfsen.sourceforge.net/>
Network auditing tools	
nmap	<https://nmap.org/>
AutoScan-Network	<http://autoscan-network.com/>
Wireshark	<https://www.wireshark.org/>
AbuseHelper	<https://github.com/abusesa/abusehelper>
Vulnerability tools assessment	
Nessus	<http://www.tenable.com/products/nessus-vulnerabilityhttp://www.tenable.com/products/nessus-vulnerability-scannerscanner>
Metasploit	<https://www.metasploit.com/>
Vega	<https://subgraph.com/vega/index.en.html>

OWASP ZAP	<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>
SQLcheck	<http://www.softpedia.com/get/Internet/Servers/Database-Utils/SQLCheck.shtml>
Burp Suite	<https://portswigger.net/burp/>
Kali	<https://www.kali.org/>
Intrusion detection tools	
Snort	<https://www.snort.org/>
Tripwire	<https://sourceforge.net/projects/tripwire/>
Forensic tools	
Sleuth Kit	<http://www.sleuthkit.org/>
Autopsy	<http://www.sleuthkit.org/autopsy/>
Tcpxtract	<http://tcpxtract.sourceforge.net/>
EnCase	<https://www.guidancesoftware.com/encase-forensic>
FTK, Forensic Toolkit	<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
Malware analysis tools	
VirusTotal	<https://www.virustotal.com/>
Malware Domain List	<http://www.malwaredomainlist.com/>
Malware Hash Registry	<http://www.team-cymru.org/MHR.html>
MISP, Malware Information Sharing Platform	<https://mispriv.circl.lu/>
AlienVault Open Threat Exchange	<https://otx.alienvault.com/>

Malwr	<https://malwr.com/>
Hybrid Analysis	<https://www.hybrid-analysis.com/>
Honeypots	
honeyd	<http://www.honeyd.org/index.php>
WiFi tools	
inSSIDer	<http://www.metageek.com/products/inssider/>
Acrylic WiFi Scanner	<https://www.acrylicwifi.com/en/wlan-software/wlan-scanner-acrylichttps://www.acrylicwifi.com/en/wlan-software/wlan-scanner-acrylic-wifi-free/wififree/>
SIEM tools	
Splunk	<http://www.splunk.com/>
Encryption tools	
GnuPG	<https://www.gnupg.org/>
VeraCrypt	<https://veracrypt.codeplex.com/>
Incidenttracking tools	
RTIR	<https://bestpractical.com/>
OTRS	<https://www.otrs.com/>
Databases	
SQLite	<https://www.sqlite.org/>
MySQL	<https://www.mysql.com/>
PostgreSQL	<https://www.postgresql.org/>

Appendix D: Information Sources

To receive incident notifications, there are several forums that distribute reliable information to the security community, and most of this news is free. Find a list of resources below:

Incident notifications		
APWG, Anti- Phishing Working Group	<http://apwg.org/>	▪ Phishing
PhishTank	<http://www.phishtank.com>	▪ Phishing
Dark-H	<http://dark-h.org>	▪ Web defacements
Mirror-Zone	<http://mirror-zone.org>	▪ Web defacements
Zone-H	<http://zone-h.org>	▪ Web defacements
Zone-HC	<http://zone-hc.com>	▪ Web defacements
Shadowserver	<https://www.shadowserver.org>	▪ Botnet ▪ Open DNS resolver ▪ Open proxy server ▪ etc.
Team Cymru	<http://www.teamcymru.org/services.html>	▪ Botnet ▪ Brute force ▪ DDoS ▪ Malware URL ▪ Open DNS resolver ▪ Open proxy server ▪ Phishing ▪ Scanning

To find contact information on teams that have been involved in an attack, you can rely on the following resources:

Contact Information for CSIRTs	
FIRST, Forum of Incident Response and Security Teams	<https://www.first.org/>
APCERT, Asia Pacific CERT	<http://www.apcert.org/>
Trusted Introducer	<https://www.trusted-introducer.org/>
AfricaCERT	<http://www.africacert.org>
Latin American CSIRTs	<http://www.lacnic.net/en/web/lacnic/csirts>
OIC-CERT, Organisation of the Islamic Cooperation CERT	<http://www.oic-cert.org/>
NatCSIRT, National CSIRTs	<http://www.cert.org/incident-management/national-csirts/nationalhttp://www.cert.org/incident-management/national-csirts/national-csirts.cfmcsirts.cfm>

Appendix E: Legislation for drafting security policies

[1] http://cesk.gov.al/legjislacioni/index.html
[2] http://www.idp.al/legjislacion/
[3] http://www.plus.al/download/Kodi-i-sjelljes-07-02-2013.pdf
[4] http://cesk.gov.al/wp-content/uploads/2016/04/REGEUR.pdf
[5] https://gdpr-info.eu/
[6] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/currentrisk/laws-regulation/corporate-governance/directive-2002-19-ec
[7] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/currentrisk/laws-regulation/corporate-governance/directive-2002-22-ec
[8] https://www.princeton.edu/~markus/teaching/Eco467/10Lecture/Basel2_last.pdf
[9] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[10] https://www.echr.coe.int/Documents/Convention_ENG.pdf
[11] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/currentrisk/laws-regulation/rm-ra-standards/bs-7799-3
[12] https://www.iso.org/isoiec-27001-information-security.html
[13] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[14] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/currentrisk/risk-management-inventory/rm-ra-tools/t_ebios.html