REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 1088 Prot   Tiranë më 18.12.2024

URDHËR

Nr.458 datë. 18.12.2024

PËR
"MIRATIMIN E RREGULLORES MBI PROCEDURAT E MENAXHIMIT TË INCIDENTEVE TË SIGURISË KIBERNETIKE, KUNDËRMASAT, PLAYBOOKS DHE MASAT MBROJTËSE TË NATYRËS SË PËRGJITHSHME"

Në zbatim të shkronjës "k", të nenit 13, pikës 3 dhe 4 të nenit 22 të ligjit nr.25/2024 "Për sigurinë kibernetike",

URDHËROJ

1. Miratimin e rregullores "Mbi procedurat e menaxhimit të incidenteve të sigurisë kibernetike, kundërmasat, playbooks dhe masat mbrojtëse të natyrës së përgjithshme" sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, CSIRT-et sektoriale, si dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTORI I PËRGJITHSHËM

IGLI TAFA

REPUBLIKA E SHQIPËRISË - KËSHILLI I MINISTRAVE - AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

REPUBLIC OF ALBANIA
NATIONAL AUTHORITY FOR CYBER SECURITY

Regulation on Procedures for the Management of Cybersecurity Incidents, Countermeasures, and Playbooks

TABLE OF CONTENTS

List of Figures

List of Tables

1. Introduction

In accordance with Law No. 25/2024 “On Cybersecurity”, the entities responsible for cybersecurity incident management are the National CSIRT, the Sectoral CSIRT, and the operator-level CSIRT.

The National CSIRT, exercises the following competences within the framework of incident management:

- Monitors, analyzes, and manages cyber threats, vulnerabilities, and incidents at the national level, and provides technical assistance to critical and important information infrastructures upon request by information infrastructure operators.
- Handles cybersecurity incidents in cooperation with operators of critical and important information infrastructures and delivers concrete solutions based on the policies and measures defined under this law; it also cooperates with relevant law enforcement institutions when cybercrime elements are suspected.
- Collects and analyzes data through digital investigations and provides dynamic risk and incident analysis, as well as situational awareness regarding the current state of cybersecurity.
- Analyzes incidents and prepares incident-specific response measures, communicating them to Sectoral CSIRTs and CSIRTs established within operators of critical and important information infrastructures.
- Analyzes incidents to identify their root cause and coordinates activities with operators, Sectoral CSIRTs, and international and governmental institutions, as deemed appropriate.
- Responds to any information infrastructure, in accordance with security procedures, to actively support the resolution of incidents.
- Coordinates with the State Police and any competent institution to preserve and enable the collection of evidence when cybercrime elements or other related criminal offenses are suspected within information infrastructures.

Sectoral CSIRT exercises the following competences within the framework of incident management:

- Ensures the enhancement of staff capacities through periodic training and certification programs, in accordance with the sectors it covers.
- Where applicable, provides assistance to operators of information infrastructures and makes available the necessary information that may facilitate the effective handling of incidents.
- Notifies the National CSIRT immediately upon identifying an incident and also informs it in the event of the prompt resolution of an incident occurring within the infrastructures under its administration.

The Operator-Level CSIRT exercises the following competences within the framework of incident management:

- Monitors networks and information systems within its critical or important information infrastructure for cybersecurity incidents or potential cyberattacks.

- Identifies and categorizes incidents, and assesses their scope and the damage caused.
- Handles incidents and provides concrete solutions based on the policies and measures defined under this law, and cooperates with the relevant law enforcement institutions when elements of cybercrime or other related criminal offenses are suspected.
- Prevents the recurrence of similar incidents by implementing preventive measures.
- Prepares and submits incident reports to the National CSIRT in accordance with the format and deadlines established by this law and by the regulation approved by order of the Director General of the Authority.
- Maintains and preserves the chronology of all incident-related evidence in compliance with the provisions of Law No. 25/2024 “On Cybersecurity” and the applicable legislation on the protection of personal data.
- Reports to the National CSIRT and the Sectoral CSIRT any cybersecurity incident occurring within its infrastructures.

1.1 Object and purpose

The purpose of this regulation is to define the procedures and steps to be followed for the prevention, identification, registration, categorization, prioritization, analysis, recovery, and reporting of cybersecurity incidents, with the aim of ensuring effective response, resolution, and minimization of their impact on information infrastructures.

1.2 Responsible entities

This regulation details the implementation of the steps outlined in Section 1.1 of this regulation by defining the duties and responsibilities of the National CSIRT, the Sectoral CSIRT, and the Operator-Level CSIRT in managing cybersecurity incidents.

1.3 Definitions

The terms defined in this regulation shall have the same meaning as those defined in Law No. 25/2024 “On Cybersecurity,” as outlined below:

“Cybersecurity Incident” means any event that compromises the availability, authenticity, integrity, or confidentiality of data that is stored, transmitted, or processed, or of services provided or accessible through information networks and systems.

“Cybersecurity Incident Handling” refers to all necessary procedures for the prevention, identification, analysis, response, and recovery from a cybersecurity incident.

“Cyber Threat” means any event or potential action that may damage, disrupt, or negatively impact information networks and systems for their users and other parties.

“Vulnerability” is a weakness, sensitivity, or flaw in ICT products or services that can be exploited by a cyber threat.

“Playbooks” are guides that outline well-defined procedures to be followed for managing each category of cybersecurity incident.

2. Cybersecurity incident management cycle

1. Cybersecurity incident management proceeds through several phases, which are detailed schematically in Annex 1 of this regulation. The process of handling a cybersecurity incident consists of:

   a) Preparation and development of human, technological, and process capacities;
   b) Detection of the cybersecurity incident;
   c) Identification of the cybersecurity incident;
   d) Initiation of communication and coordination processes with infrastructures, international partners, etc.;
   e) Recording of the cybersecurity incident;
   f) Categorization of the cybersecurity incident;
   g) Prioritization of the cybersecurity incident;
   h) Analysis of the cybersecurity incident;
   i) Isolation, removal, and restoration of services/data;
   j) Support for the isolation, removal, and restoration of services/data;
   k) Post-incident activities.

2. The process of handling a cybersecurity incident involves the National CSIRT, the Sectoral CSIRT, and the Operator-Level CSIRT (operators of critical and important information infrastructures).

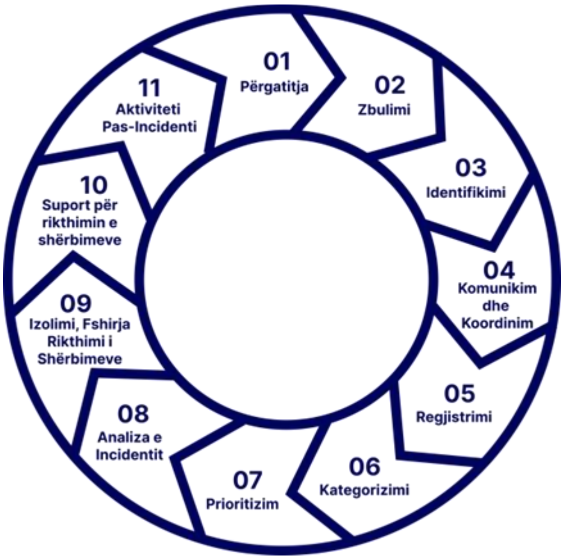

Figure 1: Cyber Incident Management Cycle

Phase	Description
Preparation	It includes the development of security policies, the formation of cybersecurity incident response teams (CSIRTs), the development of response strategies, the definition of communication workflows, the implementation of documentation systems, the provision of necessary tools, and the training of the team to ensure readiness in the event of incidents.
Detection of the cyber incident	It includes the processes and technologies for monitoring networks and systems to identify suspicious activities, through the use of monitoring tools, traffic analysis, and cyber threat intelligence, with the aim of detecting potential security breaches.
Identification of the cyber incident	It involves confirming that a suspicious activity constitutes a cybersecurity incident. Incident identification is carried out by analyzing alarms and suspicious activities to determine whether they are genuine and persistent.
Initiation of the communication and coordination process with infrastructures, International Partners, etc.	It includes a series of critical activities aimed at ensuring a synchronized and coordinated response to the incident. This phase is essential to guarantee that all relevant parties, including critical and important information infrastructures, international partners, and others, are properly informed and effectively engaged.
Registration of the cyber incident	It involves documenting all relevant information regarding the incident, including the time of occurrence, the nature of the incident, the affected systems, and the actions taken up to that point.
Incident categorization	It involves categorizing the incident based on its type and significance, with the aim of planning actions for the handling and resolution of the cybersecurity incident, in accordance with the regulation approved by order of the General Director of the Authority on “Cybersecurity Incident Categorization.”
Prioritization of the cyber incident	It involves assessing the significance and impact of the incident by considering factors such as infrastructure impact, scope of propagation, and potential risk. Based on this assessment, a task force is designated to take actions to respond to the incident and to analyze it, in accordance with the regulation approved by order of the Gerneral Director of the Authority on “Cybersecurity Incident Categorization.”
Cyber incident analysis	It involves a detailed investigation of the incident to understand its cause, profile, behavior, and the damage caused. This phase helps in developing strategies to prevent similar incidents in the future.
Isolation, Removal, and Restoration of the Service / Data	It includes actions to stop the spread of the incident, cleanse the affected systems, and restore services and data to their normal state. This involves the use of tools and techniques to eliminate threats and repair the damage caused.
Support for Isolation, Removal, and Restoration of the Service / Data	It includes the assistance provided by the National CSIRT to infrastructure operators to stop the spread of the incident, cleanse the affected systems, and restore services and data to their normal state.

Post-incident activity	It involves reviewing the incident response to identify potential improvements in security processes and policies, through lessons learned, updating documentation, and developing strategies to prevent similar incidents in the future, as well as refreshing the training program.

Table 1: Phases of the incident management cycle

2.1 Preparation in developing human, technological, and process capacities

The preparation phase for developing human, technological, and process capacities includes the following steps:

1. **Creation of Security Policies**

   Security policies consist of the following processes:

   a) Development of comprehensive security policies based on well-recognized international security standards such as the ISO 2700x series or NIST 800 series.

   b) Conducting risk assessments and security questionnaires to identify and document potential security risks and vulnerabilities.

2. **Formation of the Cybersecurity Incident Response Team (CSIRT)**
   In this step, a Cybersecurity Incident Response Team (CSIRT) is designated, with clearly defined roles and responsibilities.

3. **Incident Response Training**
   In this step, regular training sessions and simulation exercises are conducted to ensure team readiness. Additionally, the preparation phase is reviewed, and newly identified threats are documented as they are discovered.

4. **Development of Response Strategies**
   In this step, response strategies are developed that prioritize the risks based on the significance of their impact.

5. **Determination of Cyber Incident Communication Flows**
   At this stage, a detailed communication plan is developed to inform infrastructures, stakeholders, and law enforcement authorities about cyber incidents.Contacts for all members of the response team are defined, and secure, encrypted communication channels are ensured.

6. **Maintaining a Register of Cyber Incidents**
   This step includes maintaining a register to document cyber incidents, which is an essential component of incident response. This register ensures that all actions and details related to incidents are documented in a structured and clear manner. Maintaining this register helps in managing and resolving current incidents, but also provides a valuable resource for the analysis and improvement of security policies and procedures in the future.

7. **Provision of Tools and Resources for Cyber Incident Response**
   In this phase, the availability of necessary tools and solutions for incident response is ensured. Recommended tools are detailed in Annex 2 of this regulation.

8. **Access Control**
   Access Control is a key component in the management and protection of systems and data within an infrastructure during and after a cyber incident. Access control involves implementing security measures and protocols to ensure that only authorized individuals have access to sensitive resources.

2.2 Detection of the cyber incident

This phase is transitional and essential to determine whether the detection concerns an incident or the so-called “false-positive”.

The discovery process includes the following steps:

1. **Monitoring:** The use of tools and technologies to monitor networks and systems for any suspicious or unusual behavior that may indicate a security breach.
2. **Alarms:** Configuration of alarms that are triggered when suspicious activities are detected, immediately notifying the security teams.
3. **Notifications:** Information about a cyber incident may come from several channels, such as:
   a. Incident Reporting Platform;
   b. E-mail;
   c. Official letter from the infrastructures,
   d. Social networks such as: Telegram channel, Facebook, Instagram, etc.;
   e. Various media;
   f. From national or international partners,
   g. The telephone, the dedicated number at the National CSIRT
4. **Traffic Analysis:** Analysis of core network traffic, network perimeter, of end-user systems and server or in the cloud to identify unexpected patterns or changes that may indicate the presence of a threat.
5. **Use of Intelligence for Threats:** The use of data from external sources to determine whether there are any new data or information regarding current threats that may impact the infrastructure.

2.3 Identification of the cyber incident

1. The third phase of the cyber incident management cycle is the identification of the incident. Identification can be carried out by the National CSIRT, the Sectoral CSIRT, the infrastructure itself / the Operator-Level CSIRT, or by automated systems managed by the relevant structure in **AKSK** and also with the infrastructure operators.
   ➢ In the event of identification of the incident by the National CSIRT, or by the infrastructure operator itself, the respective structure in the **AKSK** (SOC T1) and the Operator-Level CSIRT, according to the categorization of the incident, in order to handle the incident, execute the specific Playbook, as referred to in Annex 3 of this regulation.

2. The identification of the Incident is carried out by:
   a) Systems and Employees:
      - Employees are trained to identify and report suspicious activities.

- All systems must have appropriate monitoring and alarm mechanisms.

b) Automated Identification: Automated systems (e.g., SIEM) managed by the relevant structures at AKSK or/and at the operators of the infrastructures are established and maintained in order to continuously monitor and identify potential incidents.

2.4 Initiation of the Communication and Coordination Process with operators of critical and important information infrastructures, international partners, etc.

This phase involves a series of critical activities aimed at ensuring a synchronized and coordinated response to the incident. This phase is important to guarantee that all stakeholders, including operators of critical and important information infrastructures, international partners, and other important organizations, are informed and effectively engaged. The main steps that occur during this phase are:

1. **Identification of Stakeholders**: In this step, all entities that need to be informed and involved in the incident response are identified. These may include operators of critical and important information infrastructures, international partners, as well as other governmental, independent, or private infrastructures that may have an interest or responsibility in incident management.
2. **Establishment of communication channels**: Once the stakeholders have been identified, the necessary communication channels are opened to ensure that information is distributed securely. These may include communications via secure email, dedicated telephone lines, and platforms for sharing classified information.
3. **Response Coordination**: In this step, the various teams involved begin to coordinate their efforts. This includes sharing important information regarding the incident, assigning specific responsibilities to each party, and planning joint actions to address the incident.
4. **Information Sharing**: At this stage, updated information is shared regarding the nature of the incident, its potential impact, and the measures taken up to that point. The information must be shared securely to avoid any risk of compromising the data.
5. **Monitoring and review of coordination**: In continuation of communication and coordination, it is essential that the effectiveness of these processes is continuously monitored. The response plans should be reviewed and updated as necessary, based on the information and feedback received from stakeholders.
6. **Documentation and reporting**: At the end of this phase, all actions undertaken and decisions made must be documented in detail to ensure a clear trace of the communication and coordination that has been carried out. This is necessary for post-incident analysis and to draw lessons for the future.

This phase ensures that all key stakeholders are engaged and informed in order to undertake synchronized and coordinated measures, which is essential for effective incident management.

2.5 Incident registration

The fifth phase of cyber incident management is the registration of the incident.

In the case of identification of the incident by the National CSIRT (SOC T1), the registration of the incident is performed by SOC T1 in the 30th (thirty) minute after the identification of the incident. In other cases, the registration of the incident is carried out by the relevant structures for the Protection, Management, and Response to Cyber Incidents at the AKSK.

In the case of incident identification by the Operator-Level CSIRT the registration of the incident is carried out at the 30th (thirtieth) minute after the identification of the incident.

In each case of incident identification by the CSIRT at the operator or the National CSIRT, the incident is registered in the registers according to the formats of Annexes III and IV of the regulation “On the Categorization of Cybersecurity Incidents” approved by order of the General Director of the Authority.

2.6 Categorisation

After the registration of the incident, the process of *triage*, which includes categorization, prioritization, correlation, and assignment for addressing (*assign for handling)* of the incident.

The categorization of the incident is carried out according to the provisions of Article 6 of the regulation “On the Categorization of Cybersecurity Incidents”, approved by order of the General Director of the Authority.

2.7 Incident Prioritization

At this stage, the prioritization of the cyber incident is carried out based on the categorization and impact of this cyber incident. The prioritization of incidents is done according to the provisions of Article 7 of the regulation “On the Categorization of Cybersecurity Incidents”, approved by order of the Gerneral Director of the Authority.

After categorisation and prioritisation, correlation with other ongoing incidents or with incidents that have occurred previously is carried out.

Finally, a ticket is created (planner / *HIVE* / internal order) to designate the responsible sectors that will address the incident according to the management cycle.

2.8 Incident analysis

The incident analysis is carried out by the National CSIRT and the CSIRT at the operator and consists of examining all available information and accompanying evidence related to a cyber incident that has occurred. The purpose of the incident analysis is to identify its cause, the extent of the damage, the nature of the incident, and possible response strategies.

The Analysis and Response Task Force, which is established pursuant to the provisions of Article 6 and Table 1 of the regulation “Për kategorizimin e incidenteve të sigurisë kibernetike” and in accordance with *ticket* created at the stage of *triage-t*, may use artifact analysis to better understand the incident and the affected systems. The incident analysis is based on the incident report sent from the infrastructure to **the National CSIRT**. The Task Force assesses whether the isolation of the affected devices has been fully carried out and provides recommendations for further isolation.

The analysis of artifacts consists of collecting, preserving, documenting, and deeper analyzing of log file copies, copies of malicious files, etc.

The analysis process includes tracing how the attacker gained access to the system or network, which systems were used to gain access, what the origin of the attack is and which systems or networks were used to carry out the cyberattack, checking for data leaks on the Dark web, checking whether the victim has branches or headquarters in the Balkans/EU/USA, etc., and if so, communicating with the relevant structures for Cyber Incident Protection, Management and

Response regarding data leaks in these branches. This may also include identifying the attacker when possible.

The incident analysis process may require cooperation with law enforcement agencies, regulatory authorities, internet service providers, or other interested parties.

2.9 Isolation, Deletion and Restoration of the Service/Data

When the incident is identified by the CSIRT at the operator, after the categorization of the incident according to the provisions of the regulation "Për kategorizimin e incidenteve të sigurisë kibernetike" as well as the application of the relevant playbook according to Annex 3 of this Regulation, immediate measures are taken to **isolation** of the end devices and affected systems quickly to prevent further damage.

The CSIRT at the operator, after analyzing the incident, carries out, either independently or in cooperation with the National CSIRT, the cleanup of incident components in the affected systems, such as deleting malicious files, disabling user accounts, etc., according to the category of the incident. Additionally, actions are taken to eliminate cyber threats by deactivating infected systems, scanning for malware, and addressing vulnerabilities.

2.10 Support for Isolation, Deletion, and Restoration of Service/Data

The Sectoral CSIRT provides technical assistance for critical and important information infrastructures to the operators of the respective sector, as well as makes available the necessary information and provides concrete solutions for the incident.

The National CSIRT/Analysis and Response Task Force analyses and manages cyber threats, vulnerabilities, and incidents at the national level, and provides technical assistance for critical and important information infrastructures upon request from the operators of information infrastructures.

Additionally, the Task Force handles cyber incidents in cooperation with operators of critical and important information infrastructures and provides concrete solutions based on the policies and measures set forth in the applicable legislation, as well as cooperates with the relevant law enforcement institutions when there is suspicion of elements of cybercrime.

All artifacts accompanying the incident analysis are stored securely and kept for future reference in the event of a similar incident.

2.10.1 Incident Response (Containment)

The incident response procedure varies according to the different categories of reported incidents. The specific response steps are defined in the Playbooks outlined in Annex 3 of this Regulation.

1. Upon identification of an incident, and in accordance with the Cybersecurity Incident Playbooks, support is provided for the **containment** of affected endpoints. Affected systems are promptly isolated to prevent further damage. Examples include disconnecting infected devices, segmenting compromised network segments, and shutting down routers associated with infected networks.
2. A **forensic examination** is subsequently conducted to assess the state of compromised systems. Specialized tools such as Forensic Tool Kit (FTK) are employed to collect and analyze evidence.
3. ***Forensic* backup copies** of compromised systems are created to collect evidence for future investigations. The National CSIRT takes and preserves copies of incident logs, whether identified or reported, in accordance with the regulation issued by the Director General of the Authority on "Procedures and timelines for retaining logs of identified or reported cybersecurity incidents."
4. Long-term mitigation strategies are implemented, such as applying security patches, disabling vulnerable ports, or redirecting network traffic to clean backup systems. This step is intended to restore operational continuity by remediating the affected systems.

Isolation Phase Checklist

The National CSIRT/Incident Analysis and Response Task Force, together with the Sectoral CSIRT, provides guidance to the Operator's CSIRT in developing a containment checklist that includes the following key questions:

- Can the cybersecurity incident be effectively isolated?
- Have all compromised systems and devices been isolated?
- Are all owners of the affected systems fully aware of the incident?
- Has coordination been established with system owners and security managers to determine the necessary follow-up actions?

Throughout this phase of Incident Response, Indicators of Compromise (**IOCs**) and Indicators of Attack (**IOAs**) are identified to update all IT and security assets and controls. Firewall/WAF/proxy rules, access control lists (**ACLs**), and blocking mechanisms remain enforced. SIEM rules, use cases, dashboards, alert creation, tuning, and modification, as well as endpoint detection and response (**EDR**) rules, signatures, and blacklist/whitelist entries are continuously updated. Ongoing threat investigation through analysis of discovered IOCs continues to determine subsequent remediation steps. Malware analysis, classification, and eradication from affected systems are performed to establish the root cause and to update IT/security assets and vendors with intelligence on IOAs and IOCs. Open-source intelligence (OSINT), threat intelligence, and threat analysis are also leveraged during this phase to further support investigation and the remediation of vulnerabilities.

2.10.2 Cleaning up phase of Affected Systems/Networks

Once the incident has been analyzed, the National CSIRT/Incident Analysis and Response Task Force, upon request from the infrastructure operator, assists in cleansing the affected systems by removing incident components such as malicious files, disabling compromised user accounts,

and other actions depending on the incident category. Cyber threats are further eliminated by deactivating infected systems, conducting malware scans, and remediating vulnerabilities, with the objective of ensuring that all weaknesses are fully addressed and properly documented.
System Cleansing Activities include:

- Deactivation of infected systems to strengthen the network against ongoing or persistent attacks.
- Comprehensive scanning of compromised systems to detect traces of malware and unpatched vulnerabilities.
- Remediation of vulnerabilities within clean backup copies of compromised systems to ensure they are hardened before reintegration.

Checklist for Cleaning Phase

The National CSIRT / Analysis and Response Task Force, during the incident cleaning phase, assists the Operator’s CSIRT in developing the following checklist of questions:
Can the compromised assets be reinforced to withstand similar cyberattacks?

- Have the compromised assets been fully cleansed?
- Have the response teams documented their remediation efforts?
- Have all vulnerabilities that led to the cyber incident been addressed?

2.10.3 Service and Data Restoration Post-Incident

After the cleansing of the affected systems/networks has been completed, recovery of the system and its restoration to operational status may proceed where possible. The recovered data must be stored on a clean system, which should remain isolated from the rest of the network. It must also be ensured that the backup used for data and system recovery is clean.

In some cases, restoring the system to operational status may require additional time even after the incident has been resolved, as a criminal investigation may have been initiated. If communication experts are involved in the incident, they must ensure that the information they convey is up to date.

Systems are restored to their pre-compromise state by using clean backup copies. In addition, monitoring is performed for suspicious activities, and security patches are applied to address the vulnerabilities that caused the intrusion. The objective is to return the systems to their condition prior to compromise. The steps include:

- Replacing the targeted environments with clean backup copies.
- Monitoring the restored systems for abnormal activity indicative of malware infections.

Recovery Phase Checklist

- Have the compromised systems been replaced with clean backup copies?
- Have the vulnerabilities that caused the intrusion in the restored systems been addressed?
- Have the restored systems been monitored for suspicious activity?

2.10.4 Cyber Incident Report

After the data recovery process, the Operator’s CSIRT prepares a detailed report in accordance with Article 23(5) of Law No. 25/2024 “On Cybersecurity” regarding the incident, in which the essential elements are highlighted with the purpose of documenting the incident, analyzing its causes and consequences, as well as identifying important lessons that may help prevent future incidents.

This report not only provides a clear overview of the nature of the incident, including the attack methods, actions conducted by the attackers, and the vulnerabilities identified in the systems, but also recommends specific measures to enhance the cybersecurity resilience of the infrastructure.

Furthermore, the report serves as a communication tool with stakeholders, informing them about the identified risks and the protective measures taken to mitigate them, as well as to build trust and transparency between the National CSIRT and the infrastructures.

The Operator’s CSIRT is obliged to submit, within one month after the notification of the incident, a Final Cyber Incident Report to the National CSIRT, in accordance with Article 23(5) of Law No. 25/2024 “On Cybersecurity.”

The Cyber Incident Report is essential not only for closing the incident management cycle but also serves as a key instrument for continuously improving cybersecurity strategies and strengthening protection against future threats.

The Cyber Incident Report form must be submitted as an official document and sent to the following email address: soc@aksk.gov.al

2.11 Post-Incident Activity

1. Lessons Learned

At this stage, it is important to fully document the incident and conduct a post-incident analysis within two weeks from the time it is recorded. The objective is to identify areas requiring improvement and establish an optimized response process for similar future incidents. This phase includes:

- Reviewing the entire incident response sequence.
- Convening response teams and stakeholders to discuss the event, how it was managed, and how the response phase can be improved.
- Refreshing training topics and, if deemed appropriate by AKSK, retraining operators.

2. Creation of a Strategy for Response to Future Incidents

Immediately after the incident has been closed and services have returned to operational status, infrastructures must update response strategies based on lessons learned. They must return to the preparedness phase to document new response strategies and improve future responses.

3. Incident Report

The incident report is the stage where post-incident actions are consolidated, such as reporting findings to internal and external groups, personnel, and stakeholders. In this phase, all submissions are tracked, a technical report detailing the root cause is generated, and an executive summary is prepared. Actions are taken according to every recommendation for strengthening IT/Security assets (e.g., updates to Firewall and EDR rules and signatures), including updates to procedural documentation and guidelines.

Checklist of the Lessons Learned Phase

- Have all meeting participants reviewed the complete incident response report?
- Have areas for improvement been identified?
- Has an optimized response process been documented based on the identified areas for improvement?
- Has the optimized response document been used to update or create a response strategy for similar future cyber incidents?

Incidents that do not need to be reported are those cybersecurity incidents as defined in Article 11 of the Regulation "Për kategorizimin e incidenteve të sigurisë kibernetike"

ANNEX 1: Cyber incident management scheme

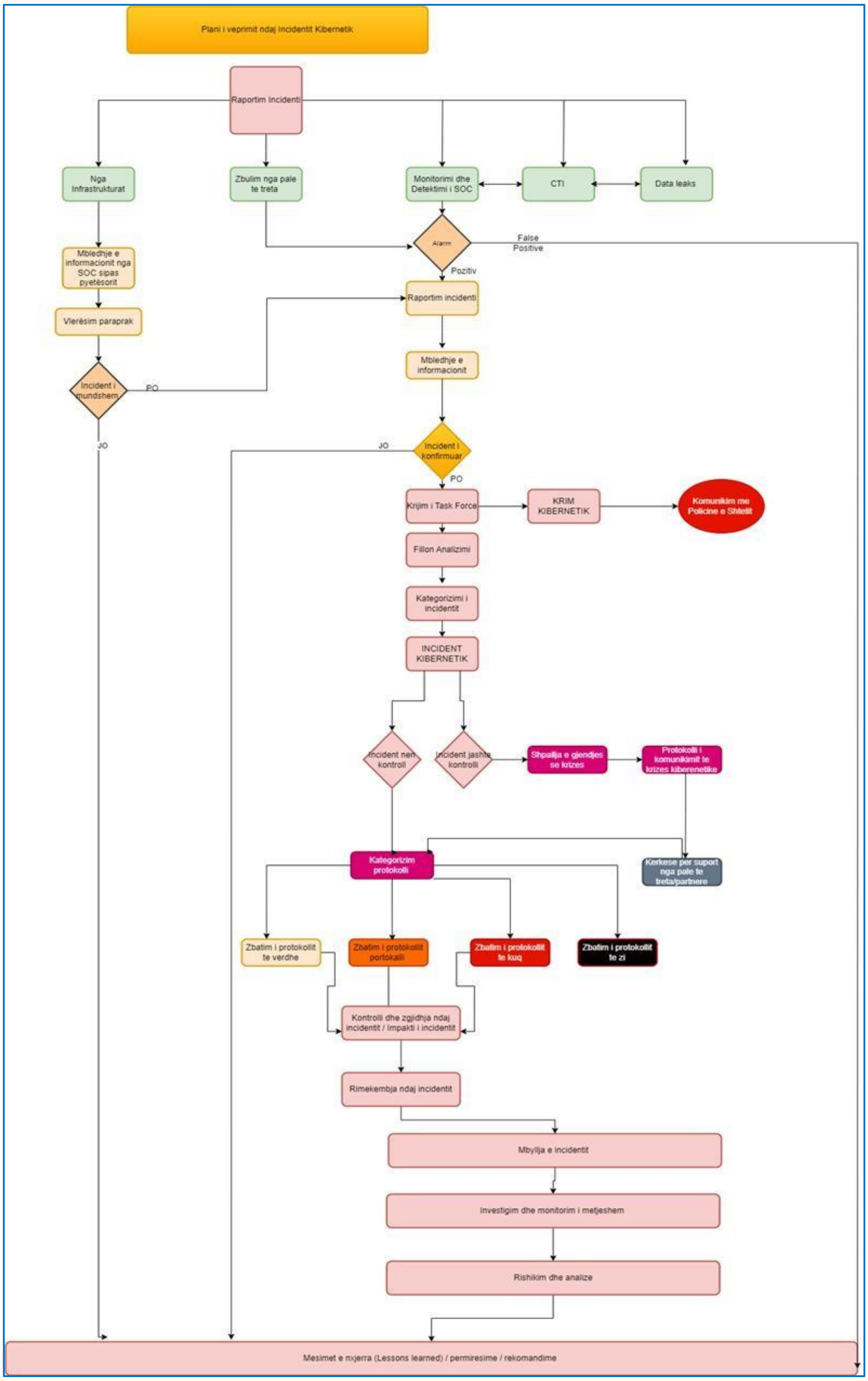
Plani i veprimit ndaj Incidentit Kibernetik
Raportim Incidenti
Nga Infrastrukturat
Zbulim nga pale te treta
Monitorimi dhe Detektimi i SOC
CTI
Data leaks
Alarm
False Positive
Pozitiv
Mbledhje e informacionit nga SOC sipas pyetësorit
Vlerësim paraprak
Incident i mundshem
PO
JO
Raportim incidenti
Mbledhje e informacionit
JO
Incident i konfirmuar
PO
Krijim i Task Force
KRIM KIBERNETIK
Komunikim me Policine e Shtetit
Fillon Analizimi
Kategorizimi i incidentit
INCIDENT KIBERNETIK
Incident nen kontroll
Incident jashte kontrolli
Shpallja e gjendjes se krizes
Protokolli i komunikimit te krizes kiberenetike
Kategorizim protokolli
Kerkese per suport nga pale te treta/partnere
Zbatim i protokollit te verdhe
Zbatim i protokollit portokalli
Zbatim i protokollit te kuq
Zbatim i protokollit te zi
Kontrolli dhe zgjidhja ndaj incidentit / Impakti i incidentit
Rimekembja ndaj incidentit
Mbyllja e incidentit
Investigim dhe monitorim i metjeshem
Rishikim dhe analize
Mesimet e nxjerra (Lessons learned) / permiresime / rekomandime

Figure 2: Cyber Incident Cyber Management Scheme

Note: In accordance with Law No. 25/2024 "On Cybersecurity," any incident suspected of containing elements of cybercrime will immediately involve the State Police. This ensures that all necessary legal and investigative measures are taken without delay to address and mitigate the impact of such incidents.

ANNEX 2: Recommended tools for monitoring and analysis of incidents

Recommended tools for monitoring and analysis [1]

Tools for log analysis:

1. **ELK Stack (ElasticSearch + Logstash + Kibana):** Log analysis (SIEM)
2. **Security Onion:** Log analysis (SIEM)
3. **Wireshark:** Network log analysis
4. **NetworkMiner:** Network log analysis
5. **Sharrë motorike:** Analysis of Windows logs
6. **Sysinternals Suite:** Analysis of Windows logs
7. **Event Log Explorer:** Analysis of Windows logs
8. **ZUI:** Zeek, Network log analysis
9. **RITA (Real Intelligence Threat Analytics):** Analysis of Zeek logs

Some of the tools for Malware Analysis and Reverse Engineering:

1. **Ghidra:** Inxhinieri e kundërt
2. **REMnux:** Malware analysis and reverse engineering
3. **Cuckoo.cert:** Malware analysis
4. **x64dbg (X64Debugger):** Malware analysis and reverse engineering
5. **Floss:** Malware analysis and reverse engineering
6. **CAPA:** Malware analysis and reverse engineering
7. **DetectItEasy:** Malware analysis and reverse engineering
8. **PE-Bear:** Malware analysis and reverse engineering
9. **MD5SUM:** Malware analysis - for finding the HASH of files
10. **Strings:** Malware analysis - for the exfiltration of strings from malicious files
11. **Binwalk:** Malware analysis - for identifying the characteristics of malicious files
12. **Radare2:** Malware analysis - for identifying the characteristics and instructions of malicious files

[1] This list is not restrictive for the use of other tools for monitoring and analysis

Some of the tools for Security Threat Intelligence Exchange and Management:

1. **MISP Server:** Exchange and management of security threat information (Threat Intelligence Platform).
2. **Abuse.ch:** Platform for sharing information about malware and threats.

Some of the tools for Vulnerability/Network Scanning and Discovery:

1. **Nikto (Kali Linux):** Web Vulnerability Scanner.
2. **Nmap:** Network scanning and for host/service discovery (Network Scanner).
3. **Spamhaus:** List for spam blocking and detection of misdirected IP addresses (Spam & Threat Intelligence).

ANNEX 3: Cyber Incident Playbooks

Cyber incident playbooks are standardized operational guidelines, developed in accordance with the legal and regulatory framework, which define the steps for managing and addressing cyber incidents according to their category and nature. These guidelines are grounded in national and international cybersecurity standards, ensuring a coordinated response across infrastructures. The National CSIRT ensures compliance with the relevant legislation and provides technical and operational support to sectoral CSIRTs and operator-level CSIRTs.

1) Abusive Content

Abusive content refers to digital materials that are unlawful, harmful, or inappropriate. This includes cases such as:

Spam: The use of electronic messaging systems to send unsolicited messages, which may be distributed for malicious purposes. The most widely known form is email spam.

Exploitation and online harassment: The harassment or bullying of individuals through the internet.

Hate speech: Material that promotes violence or hatred against individuals or groups based on gender, belief, race, etc.

Child abuse: Materials that focus on the exploitation or abuse of minors.

Terrorist content: Materials containing images, videos, or text promoted by terrorist groups.

Disinformation or fake news: False information intended to mislead.

1.1 Preparation

National CSIRT

a) Drafts policies and procedures for the identification and response to abusive content.
b) Develops and maintains threat intelligence platforms that include indicators of abusive content.
c) Conducts regular training sessions for CSIRT analysts on detecting and handling incidents involving abusive content.
d) Ensures legal and regulatory compliance regarding the monitoring of abusive content and the response to it.
e) Designates the individuals responsible for managing the incident, defining their specific roles and responsibilities in incident management.

Sectoral CSIRT

a) Provides sector specific guidance for managing incidents related to abusive content.
b) Establishes communication channels within the sector for reporting and discussing potentially abusive content.
c) Conducts regular training for sectoral CSIRT personnel on issues related to abusive content.
d) Identifies key assets and platforms within the sector that may be targeted with abusive content (such as social media, forums, messaging platforms, cloud service providers,
e) email services, etc.).
f) Coordinates with the operator's CSIRT to establish a monitoring team for the early

detection of abusive content.

CSIRT at the Operator

a) Implements systems for monitoring and filtering abusive content, with the purpose of detecting it.
b) Trains staff to recognize and report abusive content.
c) Develops and enforces policies regarding user-generated content on platforms managed by the operator.
d) Creates a list of trusted contacts for reporting and escalating incidents involving abusive content.

1.2 Discovery

National CSIRT

a) Monitors the national network and social platforms for indicators of abusive content, using anomaly detection tools and threat intelligence to identify the distribution of malicious content.
b) Utilizes platforms integrated with Artificial Intelligence and machine learning to automate the process of detecting abusive content.
c) Correlates reports and data from various information sources and identifies incidents related to abusive content.

Sectoral CSIRT

a) Shares findings and discoveries related to abusive content with the National CSIRT and the operator's CSIRT.
b) Monitors sectoral networks for traffic and content anomalies, including unexpected user activities or unauthorized attempts to distribute abusive content.

CSIRT at the operator

a) Uses tools to monitor systems and networks to detect abnormal activities or suspicious content, such as unauthorized communications, unexpected file changes, or unauthorized attempts to upload content to internal platforms.
b) Configures automated systems that immediately issue alerts when attempts to distribute abusive content is identified or when signs of unauthorized activity are detected in critical information assets.
c) Maintains logs and data related to detected abusive content activities for further analysis and specialized incident response.
d) Systematically scans content across internal and external platforms to identify abusive material that may have been uploaded or distributed without authorization.
e) Immediately reports any detected attempts to disseminate abusive content to the National CSIRT and the sectoral CSIRT, providing details on the nature and source of the content**.**

1.3 Incident identification

National CSIRT

a) Confirms abusive content through data analysis and the collection of information from intelligent systems.
b) Identifies the scope and potential impact of abusive content on critical and important

information infrastructures.

c) Notifies the relevant sectoral CSIRTs and the operator's CSIRT regarding the identification of abusive content.

Sectoral CSIRT

a) Coordinates with the operator's CSIRT regarding abusive content reported directly by the operator and assesses the impact of the incident on sectoral assets.
b) Provides detailed information to the National CSIRT for further analysis.
c) Works in coordination with the operator's CSIRT to evaluate the scope and impact of the incident.

CSIRT at the operator

a) Identifies and reports incidents of abusive content to the National CSIRT and the sectoral CSIRT.
b) Provides detailed information for further analysis, including the source of the information and its impact.
c) Determines whether the content has been distributed internally or externally to their systems.
d) Identifies immediate measures to be taken, such as blocking the content, filtering data, or isolating unauthorized users to prevent further impact of abusive content.
e) Assists in the identification process by sharing logs and related data.

1.4 Communication and coordination

National CSIRT

a) Establish communication channels between the national CSIRT, the sectoral CSIRT, and the CSIRT at the operator.
b) Communicates with law enforcement authorities to ensure more effective coordination in resolving the issue.
c) Provides regular updates and guidance to all relevant stakeholders during the incident.
d) Coordinates actions for incident response through a unified mitigation approach.

Sectoral CSIRT

a) Leverages preliminary information provided by operators and reports it to the National CSIRT.
b) Coordinates directly with operators to ensure the timely and accurate sharing of critical incident-related information, thereby enhancing the effectiveness of the operational response.
c) Holds regular coordination meetings with operators and relevant stakeholders to align response actions and continuously update protection and mitigation strategies throughout the incident.

CSIRT at the Operator Level

a) It is coordinated with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate protection measures.
b) They inform the national and sectoral CSIRT in real time about any significant developments related to the incident and share the updated traffic logs for further analysis.

1.5 Registration

National CSIRT

a) Registers the incident in the incident management platform.
b) It coordinates with the sectoral CSIRT and the one at the operator in gathering the necessary information and to ensure that the incident is fully documented.

Sectoral CSIRT

a) Coordinates with the CSIRT at the affected operator to register the incident in the incident management platform provided by the National CSIRT, and ensures that all affected operators are involved in the process by contributing additional details.
b) Collects and forwards incident-related data to the National CSIRT, ensuring the centralization of information.

CSIRT at the operator Level

a) Documents the steps taken in the management of the incident related to abusive content.
b) Registers the incident in the incident management system in accordance with the procedures defined in the regulation on the categorization of cybersecurity incidents.
c) Reports the incident to the national CSIRT and the sectoral CSIRT.

1.6 Incident categorization

National CSIRT

a) Categorizes the incident as "abusive content" based on its nature, once it has been confirmed as such.
b) Classifies the incident according to its impact on national security, public safety and
c) social stability.
d) Notifies the Sectoral CSIRT and the operator-level CSIRT of the categorization and the subsequent steps to be taken.

Sectoral CSIRT

a) Coordinates with the operator-level CSIRT regarding the categorization of the incident as abusive and communicates this categorization within the sector.
b) Assists in determining the specific nature of the abusive content (e.g., hate speech, disinformation, illegal content).

CSIRT at the Operator Level

a) Categorizes the incident as abusive content and reports it to the National CSIRT and the Sectoral CSIRT.
b) Provides information about the nature and potential impact of the content.
c) Takes immediate measures to mitigate the impact and prevent further spread of the incident.

1.7 Incident prioritization

National CSIRT

a) Assesses the criticality of abusive content based on the impact that such content has on the public and on national security.
b) Prioritizes the incident based on the dissemination of the content, the audience, and the

criticality of the affected services.

c) Coordinates the management of the incident based on the content with the highest impact.

Sectoral CSIRT

a) Cooperates with the operator-level CSIRT in assessing the impact of the incident on the sector's critical services.
b) Coordinates with the operator-level CSIRT to prioritize the incident, focusing on high-impact areas in order to ensure a coordinated incident response.

CSIRT at the Operator Level

a) Assesses the impact of abusive content on public trust.
b) Prioritizes incident response measures by focusing on the criticality of the incident.
c) Reports prioritization decisions to the National CSIRT and the Sectoral CSIRT, based on accurate analysis and well-reasoned justification.

1.8 Incident analysis

National CSIRT

a) Conducts a detailed analysis to understand the origin, intent, and potential impact of the abusive content.
b) Cooperates with international partners and intelligence agencies to gather additional information, including the source and intent of the abusive content.
c) Shares the results of the analysis with the Sectoral CSIRT and the operator-level CSIRT to support future incident response efforts.

Sectoral CSIRT

a) Assists the operator-level CSIRT in identifying vulnerabilities exploited by attackers to disseminate abusive content and recommends mitigation strategies to prevent similar incidents in the future.
b) Assists the operator-level CSIRT in analyzing the dissemination methods and intent of the abusive content to determine whether it was distributed with the aim of damaging reputation, spreading panic, or disseminating false information.
c) Provides the National CSIRT with the operators' analysis data in order to explain the situation and the scope of the incident.

CSIRT at the operator Level

a) Analyzes the incident at the operational level to understand how the abusive content was disseminated and to assess its impact.
b) Analyzes the dissemination paths of the abusive content by identifying users, IP addresses, applications, or services that may have been used for this purpose.
c) Analyzes the source and abusive content to identify potential techniques used by malicious actors, with the aim of improving system protection in the future.
d) Cooperates with the National CSIRT and the Sectoral CSIRT by sharing data and analytical findings.
e) Uses the findings to support and improve future incident response activities.

1.9 Containment and Eradication

National CSIRT

a) Provides support to infrastructure operators for the isolation and removal of identified abusive content components.
b) Provides guidance on isolating identified abusive content, including methods to block its dissemination across national networks.
c) Cooperates with competent institutions to remove abusive content from national systems and platforms, ensuring its complete elimination.

Sectoral CSIRT

a) Coordinates with the operator-level CSIRT to implement protective measures to isolate systems affected by abusive content, including cooperation with the responsible institution for blocking source IP addresses, filtering traffic, and preventing access to abusive content within sectoral networks.
b) Coordinates with the operator-level CSIRT for the removal of abusive content.
c) Monitors the situation to prevent the reappearance of the content after it has been removed.

CSIRT at the operator

a) Immediately isolates any system affected by abusive content by interrupting access for unauthorized users and blocking traffic containing abusive content.
b) Follows the guidance of the National CSIRT and the Sectoral CSIRT for the isolation and removal of abusive content, ensuring that all necessary steps are taken to prevent further dissemination.
c) For the implementation of specific isolation and removal measures, the operator-level CSIRT carries out the following actions:
   i. Blocks malicious IP addresses: Updates firewall configurations and IDS/IPS systems to block any IP addresses identified as sources of abusive content.
   ii. Removes content from internal platforms: Identifies and deletes all instances of abusive content.
   iii. Restricts access for compromised users: Deactivates user account(s) involved in the dissemination of abusive content by changing credentials and enforcing access control rules and policies.
   iv. Uses automated tools: Employs automated tools to scan for and remove abusive content that may have been disseminated across internal or external systems.
d) Verifies that the abusive content has been fully removed and reports the status to the respective National CSIRT and Sectoral CSIRT teams.

1.10 Restoration of services/data

National CSIRT

a) Provides assistance in restoring operational services, platforms, and systems to normal operation.
b) Coordinates with the operator-level CSIRT and the Sectoral CSIRT to ensure that all affected services are fully restored to operational status.
c) Monitors systems after restoration and implements measures to prevent future incidents.

Sectoral CSIRT

a) Provides support to infrastructure operators during the service recovery phase within their respective sectors, prioritizing services based on the level of impact.
b) Supports operators in restoring normal operations and in rebuilding public trust.
c) Communicates the recovery status to the National CSIRT and relevant third parties.

CSIRT at the operator

a) Restore services based on those with the highest impact.
b) Verifies the integrity and functionality of the restored services.
c) Reports the progress of service recovery and any identified issues to the National CSIRT and the Sectoral CSIRT.

1.11 Post-incident activity

National CSIRT

a) Prepares a detailed report on the abusive content, the actions taken to manage the incident, and the conclusions drawn.
b) Conducts a post-incident review to identify lessons learned and areas requiring further improvement.
c) Shares the reports with the Sectoral CSIRT and the CSIRT at operators of critical and important information infrastructure in order to enhance future incident response.

Sectoral CSIRT

a) Drafts, for the specific sector, a report on the impact of the incident and the steps taken for incident management and conclusions.
b) Participates in the post-incident review process, contributing sector-specific knowledge.
c) Disseminates lessons learned within the sector to improve future detection and response capabilities.

CSIRT at the operator

a) Drafts a final report regarding the impact of the incident, the measures taken, as well as the restoration of services.
b) Participates in the lessons learned process and records the factors that contribute to a faster incident response in the future.
c) Implements the recommendations to improve protection against incidents relating to content
d) abusive in the future.

2) Malicious Code

By malicious code, or '*Malicious Code / Malware*,' we mean any program or script designed to negatively affect a computer, server, or computer network. *Malware* can enter a victim's computer in various ways. It may take the form of executable code, a script, an application, or similar software.

Malware may include: computer viruses, worms, trojans, spyware, rootkits, botnets, keystroke loggers (keyloggers), ransomware, cryptocurrency mining malware, malicious code targeting mobile devices, etc.
How can we identify their characteristics?

	Nature	Damage
Virus	A program that replicates itself and whose code is injected in a highly complex manner into legitimate programs.	Dissemination,corruption as and the destruction of data.
Worm	One program that spreads by itself through network or other transfer media.	High speed of spread and the potential for mass destruction.
Trojan	A hidden program within a regular program or application by caused damages when executed.	Destruction of data, dissemination of confidential information.
Spyware	A program that secretly collects information about a user's activity without their knowledge.	Restriction of privacy, theft of sensitive information.
Rootkit	A group of tools and techniques that hide the activity of a program or user in operating system level.	Ensuring the sustainability of *malware* in the infected system, the difficulty of detection.
Dialler	A program that creates telephone connections (usually with high rates) without the user's knowledge, using modems to do so making expensive phone calls.	It may result in high telephone bills and in the misuse of the victim's financial resources.
Ransomware	A type of malware that encrypts the victim's data and demands payment (often in the form of cryptocurrencies) for to return him them.	Loss of access to critical data, financial expenses for the payment of compensation or for efforts to recover the data without payment.
Wiper	A type of malware that is designed to destroy data by deleting it irreversibly from disk of the victim.	Irreversible loss of data, which may cause serious disruption to the operations of an infrastructure or an individual.

Table 2: Characteristics of Malicious Codes

2.1 Preparation

National CSIRT

a) Develops and maintains plans for incident response, such as malicious codes.Constantly updates indicators of compromise in cases of incidents involving malicious code.
b) Conducts trainings *Table-Top-Exercise* (TTX) for CSIRT analysts on malicious codes, their detection and response.
c) Ensures that the means and systems for detecting malicious software (*malware*) are

implemented at the national level.

d) Defines the persons who will manage the incident by determining for each their roles and responsibilities in the management of the incident.

Sectoral CSIRT

a) Provides guidance to the sector to respond to malicious code incidents.

b) Ensures that the specific sector is equipped with protective systems such as antivirus, *anti-malware* etc., as updated.

c) Conducts training focused on the relevant sector and stimulates exercises on the detection and management of incidents related to malicious codes.

d) Identifies and secures critical assets at the sectoral level which may be targeted by malicious code.

CSIRT at the operator

a) Implements and maintains protective systems for endpoint devices for critical and important infrastructure systems.

b) Carries out program updates to avoid vulnerabilities that may be exploited by malicious code.

c) Trains the staff with best practices to avoid infections with malicious code, such as awareness about attacks *phishing.*

d) Applies policies and procedures for:

i. User privileges

ii. Passwords

iii. The use of programs, downloading and execution of files on the device.

e) Keeps backup copies of the systems (*backups*) on a continuous basis, to restore services in the event of an incident.

2.2 Discovery

National CSIRT

a) Monitors the national network for abnormal activities that provide indications of malicious code.

b) Uses advanced tools and techniques to detect threats or anomalies, and testing environments for the identification of malicious code.

c) Cross-checks the data with various sources of information such as the sectoral CSIRT and the operator’s CSIRT to further identify the possible spread of the infection.

Sectoral CSIRT

a) Assists the CSIRT at the operator with the aim of implementing tools for detecting, analyzing, and monitoring malicious code.

b) Shares critical alerts and notifications with the National CSIRT and other Sectoral CSIRTs in order to coordinate the incident response.

CSIRT at the operator

a) Use endpoint detection and response (EDR) tools to monitor for signs of malicious code on systems.

b) Monitors any attempts for network connections resulting from malicious code. Looks for IPs that establish communications with the system using tools or commands such as: **Task Manager => Performance => Resource monitor**, **tcpview** (Sysinternals Suite), the command **netstat -ano** for the systems ***Windows***. For the systems ***Linux*** use **netstat -tulpn** and **netstat -tupn**, or any other tool or command that the operator possesses for monitoring malicious activities.

c) Monitors for suspicious processes through **Task Manager** or **Procexp (**Sysinternals Suite**)** in the systems ***Windows*** and with the commands **htop** or **ps -ef** in the systems ***Linux***

d) Monitors for any file created or modified by malware (primarily in the TEMP directory for the . format.**exe**, **ps1**, **vbs** etc. for the systems *Windows* – in the directory **tmp** for files **.py**, **sh** for the systems *Linux*).

e) Use Thor Lite for Yara Rules or implement Yara Rules manually in *Firewall*, for detecting other malicious files in the system.

f) Marks the discovered IPs and files as indicators of compromise (IoCs).

g) Checks for added users, via the command **lusrmgr.msc** (***Windows***) or the cat /etc/passwd command (***Linux***), as well as for domain users, the user tree is viewed in *Active Directory*.

h) Immediately reports any discovery of malicious code to the national and sectoral CSIRT.

2.2.1 Detection of ransomware cases

National CSIRT

a) Continuously monitors traffic to detect known behaviors of *ransomware*, such as data encryption and increased requirements for traffic with external services.
b) Uses advanced detection systems and intelligent platforms that assist in identifying cases of *ransomware* as well as communications with control servers (C2).
c) Monitors log-in activities through the (RDP) protocol or programs with remote connection
d) distance (teamviewer, anydesk, etc.) to detect anomalies that may be related to ransomware.
e) Monitors for occurrences such as massive compromise of files or processes attempting to encrypt data.

Sectoral CSIRT

a) Uses tools to detect attempts to encrypt data.
b) Uses techniques such as *honeypot* in the sector to stimulate vulnerable systems, in order to detect abnormal activities on the network.
c) It is coordinated with the CSIRT at the operator for the exchange of indicators of compromise (IOC) related to the latest ransomware.

CSIRT at the operator

a) Monitors systems for any sudden attempt at file encryption or sudden deletion of backup copies (*backups*), using endpoint detection and response (EDR) management tools.
b) Checks for changes in system services, such as the deactivation of critical security services (*antivirus, firewall*).
c) It checks for the creation of new unexpected files with names such as **"README.txt"** or
d) "DECRYPT_INSTRUCTIONS.html,".
e) Monitors network connections for any attempt to communicate with IP addresses or domains that serve as ransomware control servers (C2).
f) Monitors for any file created or modified by malware.
g) Uses **Thor Lite** for **Yara Rules** or implements Yara Rules manually in *Firewall*, for the detection of other malicious files in the system
h) Marks the IPs and files discovered as indicators of compromise **(IoCs).**

2.3 Incident identification

National CSIRT

a) Confirms the presence of malicious code through in-depth analysis, leveraging national intelligence resources.
b) Identifies the scope and potential impact of the incident on all critical and important information infrastructures.
c) Notifies the sectoral CSIRT and the CSIRT at the operator to identify the malicious code incident.

Sectoral CSIRT

a) It is coordinated with the CSIRT at the operator regarding the reporting of the malicious code incident.
b) Provides information about the incident to the national CSIRT for further analysis.
c) Assists the operators in finding the origin and entry point of the malicious code.

CSIRT at the operator

a) Identifies and documents the incident, including the type of malicious code and the affected systems.
b) Preserves the affected system(s) for further analysis, including:
   i. Logs (event logs, audit logs, logs from security systems, etc.),
   ii. a clone of the compromised instance.
   iii. copies of the malicious file in a password-protected zip folder (if system cloning is not possible).
c) Use the command **"Get-FileHash"** in **PowerShell** (Windows) or "**sha256sum**" (Linux) to obtain the SHA-256 hash value of the detected malicious file.
d) Checks for the presence of malicious programs/scripts/codes that are being executed immediately after the start of the system:
   i. The values of registers such as:
      - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
      - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
   ii. **Autoruns/Autoruns64** (Sysinternals Suite), **Run > shell:startup**, **Task Manager Startup** and the programmed tasks (***Task Scheduler***) for systems ***Windows*** and commands **crontab -l**, **ls /etc/cron.*** for the systems *Linux*
e) Reports the incident to the national and sectoral CSIRT with detailed information such as logs or a preliminary impact assessment.
f) Shares the data with the national or sectoral CSIRT in the context of the incident identification process.

2.3.1 Identification for ransomware cases

National CSIRT

a) Verifies the presence of ransomware through in-depth analyses of the information and data made available by the CSIRT at the operator and the sectoral CSIRT, as well as uses national security intelligence to identify the attacker and the attack vector.
b) Processes incident reports submitted by the sectoral CSIRT and the one at the operator, creating a map of the possible spread of ransomware in critical and important infrastructure at the national level.
c) Notifies the sectoral CSIRT and the CSIRT at the operator regarding the identification of the ransomware variant, including the indicators of compromise (IoCs) to facilitate protective measures.

Sectoral CSIRT

a) Collects and provides accurate information to the national CSIRT, including data on the type of ransomware and the method of distribution within the sector.
b) Works closely with operators to identify the initial point of infection and the methods used to circumvent security measures.

CSIRT at the operator

a) Documents the incident by identifying the type of ransomware, the initial signs of infection, and the affected systems.
b) Ensures the preservation of evidence, including:
   i. Collection of important logs from the affected systems.
   ii. The creation of a clone of the compromised instance for further analysis, ensuring that the original system remains intact.
   iii. The retention of the ransomware file in a compressed and password-protected folder,
c) Reports detailed data on the incident, including logs, a copy of the instance, copies of the identified files, and a preliminary assessment of the impact on the national and sectoral CSIRT.

2.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national CSIRT, the sectoral CSIRT, and the CSIRT at the operator.
b) Communicates with law enforcement authorities for more efficient coordination in solving the problem.
c) Provides periodic updates and guidance to all relevant parties during the incident.
d) Coordinates incident response actions by following a unified approach to mitigate the incident.

Sectoral CSIRT

a) Uses the preliminary information provided by the operators and reports it directly to the national CSIRT.
b) Coordinates directly with the operators to ensure that critical information about the incident is shared as quickly and accurately as possible in order to optimize the operational response.
c) Holds regular meetings with operators and other sectoral CSIRTs to harmonize actions and update defense strategies during the incident.

CSIRT at the operator

a) Coordinates with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate protective measures.
b) Inform the national and sectoral CSIRT in real time about any significant developments related to the incident and share updated traffic logs for further analysis.

2.5 Registration

National CSIRT

a) Registers the incident in the incident management platform along with the details regarding the incident.
b) Coordinates with the sectoral CSIRT and CSIRT at the operator in gathering the necessary information about the incident.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator affected by the incident for the purpose of registering the incident in the management platform enabled by the national CSIRT and ensures that all affected operators are included in the registration process.
b) Collects and sends the data on the incident to the national CSIRT, centralizing the information.

CSIRT at the operator

a) Documents the steps taken for the management of the incident and records it in the incident management platform in accordance with the definitions of the regulation for the categorization of cybersecurity incidents.
b) Reports the incident to the national and sectoral CSIRT.

2.6 Categorization of the incident

National CSIRT

a) Categorizes the incident as malicious code or *ransomware* based on the analysis and detection of the threat.
b) Classifies the incident according to its impact on national security, public security, and critical infrastructure.
c) Notifies the CSIRT sectoral and CSIRT at the operator about the categorization and provides the necessary recommendations.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator regarding the categorization of the incident as malicious code or *ransomware* and the impacts that this incident has on their systems as well as communicates it within the relevant sector.
b) Helps in determining the specific nature of the malicious code (e.g., virus, worm, trojan, etc).

CSIRT at the operator

a) Categorizes and reports the incident as malicious code or ransomware, ensuring that the details are also documented.
b) Take immediate measures to mitigate the impact and prevent the further spread of the malicious activity.

2.7 Prioritization of the incident

National CSIRT

a) Assesses the criticality of the malicious code based on the potential impact and disruption of services at the national level.
b) Prioritizes the response to the incident based on the severity and extent of the impact for all critical and important information infrastructures.
c) Coordinates incident management based on the content with the highest impact.

Sectoral CSIRT

a) Assesses the impact of the incident based on the sector-specific services and prioritises them.
b) Coordinates with the operator's CSIRT in order to prioritize the incident, ensuring that the incident response is aligned.
c) Assists the CSIRT at the operator with the aim of reducing the level of threats in the sector's operational services.

CSIRT at the operator

a) Assesses the impact of malicious code on operational services with a focus on critical services.
b) Prioritizes measures over incident response and initially restores the most critical systems and those with the highest risk level.
c) Reports decisions on the prioritization of the incident to the national and sectoral CSIRT based on accurate analyses and reasoning.

2.8 Analysis of the incident

National CSIRT

a) Carries out the forensic analysis of indicators and all data made available by the CSIRT near the operator or the CSIRT-sectoral, in order to understand the origin, behavior or potential impact that the malicious code may have.
b) Cooperates with international partners and experts in cybersecurity by gathering more information about malicious codes.
c) Shares the results of the analysis with the sectoral CSIRT and the operator's CSIRT to assist in responding to future incidents.

Sectoral CSIRT

a) Assists the CSIRT at the operator in the detailed analysis of the incident related to malicious code.
b) Analyzes the vulnerabilities of the sector exploited to implement the malicious code.
c) Makes available to the national CSIRT and the CSIRT at the operator data that serve to further understand the situation.

CSIRT at the operator

a) Analyzes the incident at an operational level to understand what the entry point is, how the malicious code was distributed, and which systems were affected.
b) Analyzes the activity of the compromised user and checks if there is any lateral movement in the network.
c) Distributes detailed analysis with CSIRT-the national and sectoral level by assisting in the understanding of the incident.
d) Uses the findings to improve future protection against similar incidents.

2.8.1Analysis for ransomware cases

National CSIRT

a) Conducts an analysis by comparing with previous cases of ransomware, in order to understand if this attack contains any new element that requires special treatment.

b) Uses controlled environments **(sandbox)** to execute and analyze the ransomware, by studying its behavior, encryption mechanisms, and method of spreading within the system.
c) Identifies all files and processes created by ransomware, using the memory analysis technique (***memory forensics***, *made available by the operators*) to extract the binary files and encrypted data created by the malware.
d) Checks if there is a key to make the files accessible again.
e) It is coordinated with international partners in order to reach a solution to the incident.
f) Shares the results of the analysis with the sectoral CSIRT and the CSIRT at the operator to assist in preventing similar incidents in the future.

Sectoral CSIRT

a) Prepares a detailed analysis report for the relevant sector based on reports from operators with the aim of determining the impact and spread of ransomware, a report which is shared with the national CSIRT and the one at the operator.
b) Analyzes logs and network activities in the sector to determine the initial attack vector and the spread of ransomware in the infrastructure.
c) Analyzes messages where ransom is requested for the ransomware***shënim për shpërblim***) to identify the variant and to gather further information regarding the methods of contact and the objectives of the attackers.

CSIRT at the operator

a) Analyzes the activities of users and processes during the incident to identify which users were compromised and whether the ransomware managed to obtain high privileges in the system.
b) Prepare a detailed report on the impact of ransomware on its systems, including deactivated services and operational disruptions, and shares this information with the national CSIRT.
c) Performs disk analysis to identify sectors modified or encrypted by ransomware and to assess the possibility of data recovery from backups or data recovery tools.

2.9 Containment and Eradication

National CSIRT

a) Provides guidance and technical support to remove the malicious code identified at the national level.
b) Coordinates with the sectoral CSIRT and the one at the operator to ensure cyber resilience strategies for the protection of systems and services across all sectors.
c) Assists the CSIRT at the operator in the deletion process, ensuring that the malicious code is completely removed from all affected systems.

Sectoral CSIRT

a) Takes steps for the rapid isolation of affected systems within the sector, based on prioritization, in order to prevent further spread of ransomware.
b) Assists the CSIRT at the operator by ensuring that the deletion process is effective.
c) Monitors the situation to prevent the re-emergence of malicious code after it has been removed.

CSIRT at the operator

a) Immediately isolates systems containing the malicious code, avoiding lateral movement.
b) Blocks all indicators of compromise identified during analysis or reported by the national or sectoral CSIRT.

c) Follow the procedures provided by the national and sectoral CSIRT, ensuring that the systems are cleansed of malicious codes.
d) Verifies that the malicious code has been deleted and reports the status to the relevant national and sectorial CSIRT teams.

2.9.1 Isolation and deletion for ransomware cases

National CSIRT

a) Immediately requires the isolation of affected systems from the national network as soon as a ransomware attack is identified, in order to prevent lateral movement in critical and important information infrastructure.
b) Coordinates with sectoral CSIRTs and those at operators to implement joint isolation strategies, including interruption of communications with command and control (C2) servers and blocking of known attacker IP addresses.
c) Requests the deactivation of compromised users and to restrict access only to authorized personnel for analysis and system recovery.
d) Maintains an inventory of all isolated systems, documenting the time of isolation and following procedures for the security of digital evidence for further analysis.

Sectoral CSIRT

a) Assists the CSIRT at the operator in fulfilling the instructions of the national CSIRT for isolating systems in the sector, in order that any compromised system is disconnected from the sectoral network to prevent the spread of ransomware.
b) Assists the CSIRT at the operator regarding the use of network security tools such as antivirus, EDR, and a specific ransomware scanner to create restricted zones (*zona karantine*) where the affected systems will be placed for further analysis, disconnecting all connections to the external network.
c) Assists the CSIRT at the operator to analyze isolated systems in order to determine if selective deletion of compromised files is possible or if a full system restore from backups is necessary.

CSIRT at the operator

a) Immediately isolates the affected systems as soon as ransomware activity is detected, by disconnecting all network connections and disabling user access to prevent further spread.
b) Use security tools (firewall, EDR) to block traffic to and from IP addresses or domains known as command and control (C2) servers of ransomware.
c) Deletes files identified as compromised.
d) Creates a clone of the affected system prior to deletion in order to preserve digital evidence for further analysis, documenting all changes made during the isolation and deletion process.
e) Documents all isolation and deletion actions and reports them to the national and sectoral CSIRT, including details of the deleted files.

2.10 Restoration of services / data

National CSIRT

a) Assists the sectoral CSIRT and the one at the operator in restoring to normal condition
b) critical services after the incident.
c) Coordinations with the sectoral CSIRT and CSIRT at the operator so that all affected

services are restored to operational status.
d) Monitors the systems after their restoration by ensuring stability and to avoid incidents in the future.

Sectoral CSIRT

a) Assists the CSIRT at the operator in the restoration of services according to the respective sectors by prioritizing services based on those that have been most affected.
b) Communicates the status of recovery and the issues encountered to the national CSIRT and third parties.

CSIRT at the operator

a) Restores the services affected by malicious code activity, following the steps of the recovery plan.
b) For *ransomware* cases if decryption is impossible, backup copies are restored, ensuring that they are not infected.
c) Verifies the integrity and functionality of the restored services before resuming normal operations
d) Reports the progress of the restoration of services and any issues to the national CSIRT and the sectoral CSIRT.

2.11 Post-incident activity

National CSIRT

a) Drafts a detailed report regarding the malicious code, incident response actions, and
b) results.
c) Conducts a post-incident analysis to draw lessons to identify which areas are most in need of improvement.
d) Shares reports with the sectoral CSIRT and the CSIRT at the operator in order to improve response to future incidents.

Sectoral CSIRT

a) Drafts a report for the specific sectors on the impact of the incident, the steps taken for incident management, and the conclusions.
b) Participates in the post-incident review process, contributing sector-specific expertise.
c) Shares reports and lessons learned within the sector to improve response to incidents in the future.

CSIRT at the operator

a) Drafts a final report with information on the impact of the incident and the restoration of services.
b) Participates in the lessons learned process by identifying what could have been done better during the incident response.
c) Applies the recommendations to improve the protection regarding incidents involving malicious codes.

3) Collection of information

By information gathering we will mean the active and passive attempts that malicious actors undertake to collect sensitive data or to identify weaknesses in the system. The techniques used for information gathering include **social engineering**, where attackers attempt to deceive personnel in order to extract confidential data, **network scanning**, where malicious actors conduct analysis of the network and services to identify vulnerabilities and open ports. A passive method for gathering information is through **OSINT tools (*Open Source Intelligence*)** which allows attackers to collect data from social networks, public databases, and other open sources

3.1 Preparation

National CSIRT

a) Develops and maintains policy and guidelines on activities for collection of the information.
b) Implements advanced tools and technologies that perform continuous vulnerability scanning and detection.
c) Conducts regular trainings on the ethical and legal aspects regarding scanning and social engineering activities.
d) Creates a centralized system for the collection of data, ensuring their secure storage.
e) Determines the persons who will manage the incident by specifying for each their roles and responsibilities in incident management.

Sectoral CSIRT

a) Creates an inventory of information that is public and related to the sector, such as IP addresses, domains, published contacts and used applications, data that malicious actors may exploit.
b) Assists the CSIRT at the operator in the implementation of monitoring systems for social engineering activities, such as phishing attempts and other scams, to identify and alert about threats targeting the collection of information.
c) Trains the sector's personnel to recognize advanced information gathering techniques employed by malicious actors, such as network scanning and social engineering.
d) Tests and strengthens access controls to internal information resources to prevent malicious actors and unauthorized persons from accessing sensitive information.
e) Creates a database with indicators of compromise (IoCs), such as scanning IPs that are related to information gathering activities.

CSIRT at the operator

a) Drafts and implements internal policies to protect sensitive data and restrict information that is publicly accessible, including details such as the internal network IP, contacts, and internal systems.
b) Identifies and controls all information published by the infrastructure, including websites, social networks, and public documents, in order to reduce data that could be used by malicious actors for the purpose of information gathering.
c) Conducts regular training for staff to recognize social engineering tactics, such as *phishing* and *vishing* (phishing via phone), and to instruct them on the ways to immediately report these attempts to the security team.
d) Implements protection measures for access to internal systems and services, using multi-factor authentication (MFA) and restricting access for unauthorized persons, in order to minimize the possibility for malicious actors to collect information.
e) Regularly scan their network and systems to identify and address vulnerabilities that could be exploited by attackers for information gathering.

3.2 Detection

National CSIRT

a) Monitors national-level traffic to identify scanning activities from unknown or suspicious IPs, which are analyzed through intelligent platforms.

b) Carries out continuous research on the internet to find sensitive information that could be exploited by malicious actors and reports them directly to the operator's CSIRT and the sectoral one.

c) Coordinates with other national and international institutions to identify the sources of information gathering efforts and to share indicators of compromise (IoCs).

d) Correlates the scan data with different information sources such as intelligence platforms.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator with the aim of implementing the necessary mechanisms in the relevant sector regarding the detection of scanning activity which may target critical systems.

b) Distributes indicators of scans detected by the CSIRT at the operator to the national CSIRT and other sectoral CSIRTs.

c) Has a proactive approach to monitoring and analyzing scans to understand potential threats.

CSIRT at the operator

a) Uses network monitoring tools to detect unauthorized or suspicious activity related to scanning or attempts at social engineering.

b) Immediately reports scanning activities to the national CSIRT and the sectoral CSIRT.

c) Implements internal tools to monitor network traffic and to identify multiple DNS, ARP requests, or other activities that may indicate an attempt to intercept traffic within the infrastructure.

d) Collects information on suspicious activities and immediately shares it with the sectoral CSIRT for a coordinated response and to assist in determining the extent of the attempted information gathering.

e) Keeps logs and data related to malicious activity for further investigation.

3.3 Incident identification

National CSIRT

a) Confirms the presence of information gathering activity as part of a potential security incident through initial analysis after the detection of malicious activity.

b) Analyzes and evaluates reports of phishing and social engineering activities reported by the CSIRT at the operator and sectoral levels, in order to identify new tactics that may be used for information gathering

c) Identifies the extent and impact primarily on all critical and important information infrastructures.

d) Notifies the sectorial CSIRT and the CSIRT at the operator regarding the identified incident and its impact.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator regarding the reporting of the incident classified as "information gathering" carried out by the operator itself, to determine whether it poses a threat to their assets on a broader scale.

b) Coordinates with the CSIRT at the operator to assess the impact of the scanning within the relevant sector.

c) Provides detailed information about the incident to the national CSIRT for further analysis.

CSIRT at the operator

a) Identifies and documents the incident, including the source of the attack, the users and targeted systems, and the user's privilege level.

b) Analyzes system and network logs to identify sources of suspicious activity, such as: IP addresses attempting to gather information through port scanning.

c) Views the content of suspicious messages in the email and identify whether we have an incident or attempt of social engineering and it determines the objectives of the malicious actors based on the recipient of the messages.

d) Monitors the logs of servers and applications to identify whether any service has been used to collect information from outside, such as multiple requests for information from a single IP address.

e) Collects and documents the identified information, including IP addresses, techniques used, and suspicious files, and reports them immediately to the national and sectoral CSIRT for further analysis and coordination.

3.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national CSIRT, the sectoral CSIRT, and the one attached of the operator.

b) Provides updates and guidance from time to time to all relevant parties during the incident.

c) Coordinates actions in response to the incident by following a unified approach for mitigating the incident.

Sectoral CSIRT

a) Utilizes the preliminary information provided by the operators and reports it directly to the national CSIRT.

b) Coordinates directly with the CSIRT at the operator to ensure that the Critical information regarding the incident must be shared in the shortest possible time and with accuracy to optimize the operational response.

c) Holds regular meetings with operators and other sectoral CSIRTs to harmonize actions and update defense strategies during the incident.

CSIRT at the operator

a) Coordinates with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate protective measures.

b) Informs the national and sectoral CSIRT in real time about any significant developments related to the incident and share updated traffic logs for further analysis.

3.5 Registration

National CSIRT

a) Registers the incident in the incident management platform and ensures that the affected operators are included in this process by assisting with additional details.

b) Coordinates with the sectoral CSIRT and CSIRT at the operator in gathering the necessary information regarding the incident based on documentation.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator affected by the incident for the purpose of recording the incident in the incident management platform.
b) Coordinates with the operators of the infrastructures affected by the incident with the aim of involving them in the incident registration process.
c) Collects and sends the data concerning the incident to the national CSIRT, thereby centralising the information.

CSIRT at the operator

a) Documents the scanning incident and findings based on the data collected.
b) Registers the incident in accordance with the provisions of the regulation on the categorization of the cybersecurity incident.
c) Reports the incident to the national CSIRT and the sectoral CSIRT.

3.6 Categorisation of the incident

National CSIRT

a) Categorizes the information gathering incident as scanning, social engineering, OSINT, etc., based on the nature, scope, and potential impact on national security.
b) Classifies the incident according to its impact and the intent behind the information gathering and the targeted systems.
c) Notifies the CSIRT sectoral and that near of the operator on the categorization and gives the necessary recommendations.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator regarding the categorization of the scanning incident within the sector, based on its impact and the collected data.
b) Assists in determining the scanning activity and its importance for the operational services of the sector.

CSIRT at the operator

a) Categorises the information gathering incident as scanning, social engineering, OSINT.
b) Reports on the meeting activity of the information, by ensuring all relevant information leads to the categorisation of the incident.
c) Follows the established procedures for incident management based on its categorization.
d) Implements immediate measures to address any vulnerability identified through
e) the activity of information gathering.

3.7 Prioritization of the Incident

National CSIRT

a) Assesses the importance of the information gathering activity based on its potential to identify or exploit vulnerabilities in national systems.
b) Prioritizes incident response, focusing on those incidents that may lead to security breaches.
c) Coordinates with the sectoral CSIRT and CSIRT at the operator to ensure that the most

critical incidents are addressed immediately.

Sectoral CSIRT

a) Assesses the impact of the scanning activity on the specific critical services of the sector and prioritizes based on criticality.
b) Coordinates with the CSIRT at the operator with the aim of prioritizing the incident, ensuring that the incident response is aligned.
c) Focuses on mitigating threats by paying attention to critical services affected by scanning.

CSIRT at the operator

a) Assesses the impact of information gathering activity on operational processes and prioritizes response actions to the incident according to the importance of the services.
b) Ensures that the vulnerabilities identified through scanning are addressed immediately.
c) Reports prioritization decisions to the national and sectoral CSIRT, based on precise justifications.

3.8 Analysis of the incident

National CSIRT

a) Conducts a thorough analysis of the scanning activity, focusing on the source, purpose, and potential impact.
b) Cooperates with international partners and intelligence agencies to collect
c) additional information regarding the indicators identified during the analysis phase.
d) Shares the analysis results with the sectoral CSIRT and the CSIRT at the operator in order to assist in future incident responses.

Sectoral CSIRT

a) Conducts a sector-level analysis on information-gathering activities, utilizing the information made available by the operators and the threat intelligence platform.
b) Provides assistance in analyzing the sources that malicious actors have exploited to collect information and suggests strategies for eliminating this information from those sources.
c) Makes available to the national CSIRT data that serve to further understand the situation.

CSIRT at the operator

a) Analyzes the activity of information gathering at the operational level, focusing on how it can impact critical systems.
b) Shares the findings with the national and sectoral CSIRT to help the latter better understand the scanning incident, social engineering, etc.
c) Uses the findings to improve security measures and to prevent the exploitation of identified vulnerabilities.

3.9 Containment and Eradication

National CSIRT

a) Provides guidance and support for reducing the impact from activities identified as “information gathering”.
b) Coordinates with the sectoral CSIRT and that at the operator to ensure strategies for
c) cyber resilience in all sectors.
d) Leads efforts to address any information exposed by the information gathering activity,

ensuring the elimination of such information.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator in order to apply protective measures across the entire sector to prevent the exploitation of the collected information.
b) Collaborates with the operators to avoid possible threats related to malicious activity.
c) Monitors the situation to ensure that measures have been taken regarding all exposed information.

CSIRT at the operator

a) Immediately isolates the devices and systems identified as compromised from the network to prevent further spread of information gathering activities and to protect sensitive data.
b) Blocks IP addresses, domains, and other suspicious resources that have been used for information gathering, using the rules of protective systems such as: the firewall and IDS/IPS to prevent any further communication with malicious actors.
c) Actively monitors isolated systems for ongoing suspicious activity, such as repeated attempts at communication, ensuring that the isolation has been effective.
d) Documents all actions undertaken during the isolation and deletion phase, including blocked IP addresses, deleted files, and deactivated accounts, and shares this information with the national and sectoral CSIRT for a coordinated response and further analysis.
e) Follows the procedures provided by the national and sectoral CSIRT for the elimination of exposed sensitive information, ensuring that all necessary steps are taken.

3.10 Restoration of services / data

National CSIRT

a) Assists in the restoration of all affected services to normal operation.
b) Coordinates with the sectoral CSIRT and the CSIRT at the operator to ensure that all affected services are fully restored to operational status.
c) Monitors the systems during and after recovery to ensure stability and to prevent future incidents.

Sectoral CSIRT

a) Assists operators in the recovery of specific sector services by prioritizing the most critical affected systems.
b) Communicates the recovery status and ongoing situation to the national CSIRT and stakeholders.

CSIRT at the operator

a) Restores the services affected by the scanning activity, following the incident response plans.
b) Verifies the integrity and functionality of the restored services before resuming normal operations.
c) Reports the progress of recovery and any challenges to the national and sectoral CSIRT for further assistance.

3.11 Post-incident activity

National CSIRT

a) Drafts a report describing the incident for information gathering, the actions of
b) incident response and the results.
c) Reviews the activity after the incident to draw lessons learned and to identify areas in need of improvement.
d) Updates the response plan based on the lessons learned.
e) Distributes the report to the sectoral CSIRT and to the one at the operator in order to increase overall preparedness.

Sectoral CSIRT

a) Prepares a report for the sector describing the impact of the scanning activity, the incident response steps, and the recovery efforts.
b) Participates in the post-incident review process, contributing sector-specific knowledge and recommendations.
c) Disseminates lessons learned within the sector to improve the plan for responding to incidents in the future.

CSIRT at the operator

a) Drafts a final report with detailed information on the impact, response, and recovery of the malicious activity.
b) Engages in the lessons learned process, identifying what can be improved for similar incidents in the future.
c) Applies the recommendations to strengthen protection and to improve the activities of
d) future scans.

4) Attempts at intervention

Attempts at unauthorized access in the field of cybersecurity are ongoing signs of efforts to penetrate the systems of an information infrastructure or an individual's devices. These attempts come from unauthorized individuals or groups aiming to gain illegal access to sensitive data, cause damage, or exploit resources unlawfully. Attempts at interference take various forms such as: *email phishing, brute-force,* injection of malicious code (SQLi, XSS), etc.

4.1 Preparation

National CSIRT

a) Develops and maintains policies and procedures for detection and response against attempts at interference.
b) Implements advanced security technologies, including intrusion detection systems (IDS) and intrusion prevention systems (IPS), across all national networks.
c) Conducts ongoing training for CSIRT analysts to identify and respond to attempts at intervention.
d) Collaborates with global cybersecurity organizations to stay informed about the latest intervention tactics and techniques.
e) Determines the responsible persons for the response of the incident and determines the roles and responsibilities of each.

Sectoral CSIRT

a) Assists infrastructure operators through sector-specific guidelines for monitoring and preventing interference attempts.

b) Ensures that the sectoral networks are equipped with up-to-date IDS/IPS technology.
c) Conducts training for the sectoral CSIRT teams and those at the operator to identify signs of intrusion attempts.
d) Cooperates with the CSIRT within the operator to develop a plan for responding to incidents such as attempted intrusions.

CSIRT at the operator

a) Implements and maintains security systems that monitor network traffic for signs of intrusion attempts.
b) Trains the staff to recognize suspicious activities and to report possible attempts to interfere with systems.
c) It provides the operator's staff with best security practices, such as restricting access by users with low privileges, ensures that passwords meet standards, regularly applies updates, in order to reduce the risk of successful breaches.
d) Regularly reviews and updates security configurations to address new threats.

4.2 Discovery

National CSIRT

a) Continuously monitors national networks for indicators of intrusion attempts, such as unauthorized access attempts, unusual traffic, and abnormal system behavior.
b) Uses threat intelligence sources and anomaly detection tools to identify potential interference attempts.
c) Cooperates with the sectoral CSIRT and the one at the operator to increase capacities for
d) the detection of interference attempts by sharing information and data between the parties.

Sectoral CSIRT

a) Cooperates with the CSIRT at the operator for the purpose of implementing mechanisms for detecting and identifying intervention attempts targeting the critical infrastructure.
b) Notifies the national CSIRT and other sectoral CSIRTs of identified intervention attempts in order to ensure a coordinated response.

CSIRT at the operator

a) Uses network monitoring tools to detect attempts of unauthorized interference.
b) Monitors for multiple attempts to gain access to protocols such as: smb, ssh, ftp, http/https, rdp, etc.
c) Performs internal scans to identify systems or services that may have known vulnerabilities that may be exploited by malicious actors.
d) Monitors the activity of users to identify their abnormal behaviors, such as attempts to access outside working hours or attempts to gain access to folders for which they are not authorized to use.
e) Reports immediately any detected attempt of interference to the national and sectoral CSIRT.
f) Retains logs and data related to detected intrusion attempts for the purpose of further investigation.

4.3 Incident identification

National CSIRT

a) Categorizes as a cyber incident, through analysis of the collected data, the attempts for intervention.
b) Verifies the extent and possible impact of the attempted interference in terms of national security for critical and important infrastructures.
c) Notifies the sectoral CSIRT and the one at the operator regarding the attempts of intervention and its possible consequences.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator regarding the intervention effort reported by them and assesses its impact on the specific assets of the sector.
b) Coordinates with the operators to determine the scope of the attempted intervention within the sector.
c) Provides detailed information about the incident to the national CSIRT for further analysis.

CSIRT at the operator

a) Identifies and documents the attempted intervention, including the source, method, and which services or users are targeted.
b) Verifies the level of privileges that the user has over which access is being attempted.
c) In the attacks *phishing*, the sender's IP, the file or the link is identified (*link*) which may be part of the email and are considered as indicators of compromise.
d) Identifies IPs that attempt to inject malicious code into systems or services, in order to gain unauthorized access.
e) Analyses the behaviour of personnel to identify whether there are insiders hiding behind the attempts.
f) Identifies whether attempts to gain access originate from a supply chain attack which initially affects third-party operators that provide services to critical or important infrastructures.
g) Reports the incident to the national and sectoral CSIRT, providing all relevant data and the initial analysis.
h) Assists in identifying the purpose that intervention efforts have and their impact possible in the operational services.

4.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national CSIRT, the sectoral CSIRT, and the CSIRT at the operator.
b) Provides updates and guidance from time to time to all relevant parties during the incident.
c) Coordinates actions for responding to the incident by following a unified approach to its mitigation.

Sectoral CSIRT

a) Utilizes preliminary information provided by the operators and reports it directly to the national CSIRT.
b) Coordinates directly with the operators to ensure that critical information regarding
c) The incident should be communicated as quickly and accurately as possible in order to optimize the operational response.
d) Holds regular meetings with operators and other sectoral CSIRTs to harmonize actions and update defense strategies during the incident.

CSIRT at the operator

a) Coordinates with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate protective measures.
b) Informs the national and sectoral CSIRT in real time about any significant development related to the incident and share the updated traffic logs for further analysis.

4.5 Registration

National CSIRT

a) Records as an incident any attempts at interference in the incident management platform,
b) ensuring that all collected data are recorded.
c) Coordinates with the sectoral CSIRT and that at the operator to collect additional information and to ensure that the incident is fully documented.

Sectoral CSIRT

a) Assists the CSIRT at the operator in registering the incident in the incident management platform and ensures that the affected operators are included in this process by assisting with additional details.
b) Sends the collected information and incident details to the national CSIRT to centralise the information.

CSIRT at the operator

a) Documents intervention attempts and any initial findings based on the data collected.
b) Ensures the registration of the incident according to the provisions in the regulation on the categorisation of cyber incidents.
c) Reports the incident to the national CSIRT and the sectoral CSIRT with all relevant details.

4.6 Categorization of incidents

National CSIRT

a) It categorizes as an incident the attempted interference based on its nature, scope, and impact
b) possible to national security.
c) Classifies the incident according to its severity, taking into account the potential impact on the targeted systems.
d) Notifies the sectoral CSIRT and the one at the operator for categorization and provides instructions on how to respond to the incident.

Sectoral CSIRT

a) It is coordinated with the CSIRT at the operator regarding the categorization of the scanning incident within the sector, based on its impact and the data collected.
b) It helps to determine the nature of the "attempted interference" and its significance for sectoral operations.

CSIRT at the operator

a) Attempts at interference are categorized as incidents.
b) Follows the established procedures for incident management based on its categorisation.
c) Implements immediate measures to mitigate any possible harm caused by the attempted

interference.

4.7 Prioritization of the incident

National CSIRT

a) Assesses the criticality that intervention efforts have, based on their potential to compromise sensitive data or disrupt critical services.
b) Prioritizes incident response, focusing on those incidents that may lead to
c) security breaches in critical systems or services.
d) Coordinates with the sectoral CSIRT and CSIRT at the operator to ensure that the most critical incidents are addressed immediately.

Sectoral CSIRT

a) Assesses the impact of attempts at interference in the sector's critical services and prioritizes them as needed.
b) Coordinates with the CSIRT at the operator for the prioritization of the incident, in order to coordinate and synchronize the response to the incident.
c) Assists the CSIRT at the operator in mitigating the most critical threats identified through the incident.

CSIRT at the operator

a) Assesses the impact of attempted interference in operational processes and prioritizes response actions as needed.
b) Ensures that any potential damage or compromise of data is managed and addressed immediately.
c) Reports decisions for prioritization to the national and sectoral CSIRT, providing analysis and justification.

4.8 Analysis of the incident

National CSIRT

a) Conducts a detailed analysis of the attempted intervention, understanding the origin, method, techniques of malicious actors, or the potential impact on national security.
b) Defines indicators of compromise, such as suspicious IPs, hashes of infected files,
c) Harmful URLs based on the data made available by the sectoral CSIRT and that at the operator.
d) Cooperates with international partners and intelligence agencies to gather additional information that assists in responding to the incident.
e) Shares the results of the analysis with the sectoral CSIRT and the one at the operator for this purpose assisted in responding to incidents in the future.

Sectoral CSIRT

a) Assists the CSIRT at the operator in analyzing the intrusion attempt, utilizing the collected information and threat intelligence.
b) Assists the CSIRT at the operator in identifying vulnerabilities exploited by the intrusion attempt and suggests strategies for mitigating the vulnerabilities.
c) Makes available to the national CSIRT and to the operator's CSIRT analyses and data that serve to further understand the situation.

CSIRT at the operator

a) Analyzes the attempt to intervene at the operational level, focusing on how it may impact critical systems and data.
b) Shares the findings with the national and sectorial CSIRT to contribute to a broader understanding of the intervention incident.
c) Implements the findings to improve security measures and to prevent further attempts at interference.

4.9 Containment and Eradication

National CSIRT

a) Provides guidance and support for mitigating the impact of interference attempts.
b) Coordinates efforts with the sectoral CSIRT and the one at the operator to ensure that cyber resilience strategies are implemented across all sectors.
c) Addresses the weaknesses exposed by the attempted intervention, and provides recommendations to reduce the number of these weaknesses.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator for the purpose of taking preventive measures across the entire sector to prevent further exploitation of vulnerabilities.
b) Works closely with the operators to ensure the reduction of vulnerabilities exploited for attempted interference.
c) Monitors the situation to ensure that all identified weaknesses have been addressed and the incident is fully resolved.

CSIRT at the operator

a) Immediately addresses any weakness identified as a “tampering attempt” such as:
    i. If attacks are detected on ports known as, for example: 21, 22, 3389, filter the traffic for these ports to eliminate possible attacks.
    ii. After you have identified the above IP from which these attempts originate, block them.
    iii. Limit login attempts, for example: a maximum of 5 attempts, and then the user must wait 5 minutes.
    iv. If there are doubts about authentication, take steps to increase the protection of the account and the system. This may include adjusting security policies, using *note-changes*, up to the freezing of accounts in suspicious cases.
b) Follows the preventive and mitigation procedures provided by the CSIRTs, ensuring that all necessary steps are taken such as:
    i. Changing passwords for users or services where access has been attempted.
    ii. Application of updates or taking measures on systems that have vulnerabilities
        a. known that lead to compromise.
c) Verifies how effective the preventive measures have been, the mitigation of weaknesses, and reports the status to the national and sectoral CSIRT.

4.10 Restoration of services / data

National CSIRT

a) Assists in the recovery of services affected by the attempted interference.
b) Coordinates with the sectorial CSIRT and the CSIRT at the operator to ensure that all

affected services are fully recovered.

c) Monitors the systems during and after recovery to ensure stability and to prevent future incidents.

Sectoral CSIRT

a) Assists in the restoration of sectoral services, by prioritizing the most critical affected services or systems.
b) Supports operators in restoring services to full operational capacity.
c) Communicates the recovery status and any ongoing issues to the national CSIRT and relevant third parties.

CSIRT at the operator

a) Recovers the services affected by the “intervention attempts”, by following the recovery plans set out in the incident management plan.
b) Verifies the integrity and functionality of the recovered services before normal operations are resumed.
c) Reports the progress of recovery and any issues during the process to the national and sectoral CSIRT for further assistance.

4.11 Post-incident activity

National CSIRT

a) Drafts a detailed report regarding the intervention efforts, response actions to the incident and the results.
b) Conducts post-incident review to identify lessons learned and areas where further improvement is needed.
c) Disseminates the reports with the sectoral CSIRT and critical infrastructure operators and important for improving the response to incidents in the future.

Sectoral CSIRT

a) Prepares a report for the sector on the impact of the incident, the steps taken to manage the incident, and the conclusions.
b) Participates in the post-incident review process, providing specific recommendations for the sector.
c) Disseminates reports and lessons learned within the sector to improve the response to incidents in the future.

CSIRT at the operator

a) Drafts a final report providing detailed information on the impact of the incident, the response to it, and the recovery.
b) Participates in the lessons learned process, by identifying operational improvements and updating response plans.
c) Implements recommendations to strengthen protection and improve detection for future attacks such as attempted intrusions.

5) Interventions

5.1 Preparation

National CSIRT

a) Develops and maintains policies and procedures for detection and response against bypassing authentication.
b) Implements advanced security controls such as multi-factor authentication (MFA), strong password policies, and continuous reviews in national systems.
c) Conducts regular training for CSIRT analysts on recognizing and responding to authentication bypass techniques.
d) Collaborates with cybersecurity organizations to exchange intelligence and remain informed about emerging authentication bypass techniques.
e) Designates the individuals responsible for managing the incident by defining each person's roles and responsibilities in incident management.

Sectoral CSIRT

a) Coordinates activities with the operator's CSIRT by providing guidance to the relevant sector to ensure authentication mechanisms are implemented in accordance with international standards.
b) Coordinates with infrastructure operators for the purpose of implementing multi-factor authentication across the entire sector and regularly updates access controls.
c) Trains the sectoral teams of the CSIRTs for the identification, mitigation, and avoidance of authentication bypass.

CSIRT at the operator

a) Applies and maintains strong authentication mechanisms, including MFA, strong passwords, and ongoing access reviews.
b) Trains the staff on safe authentication practices and the importance of reporting
c) suspicious activities.
d) Implements monitoring tools to detect unusual access activities or failed entry attempts.
e) Regularly reviews and updates access policies and authentication configurations.

5.2 Discovery

National CSIRT

a) Monitors the national network for authentication bypass activities, such as unusual login patterns, repeated failed login attempts, or access from different locations.
b) Leverages anomaly detection tools and threat intelligence to identify potential authentication bypass activities.
c) Uses intelligent platforms to record the data that have been leaked and forwards them to the relevant CSIRTs in order to prevent unauthorized access.
d) Cooperates with the sectoral CSIRTs and those near the operators to improve detection capacities through shared knowledge and data.

Sectoral CSIRT

a) Use sector-specific tools to detect attempts to bypass authentication targeting systems, services, or access to critical areas.
b) Shares information on detected authentication bypass activities with the national CSIRT and other sectoral CSIRTs to ensure a coordinated response.
c) Assists operators with the aim of continuous monitoring for vulnerabilities that may be exploited to bypass authentication in services provided through the public internet

interface.

d) It is coordinated with the CSIRT at the operators for the purpose of monitoring the systems of authentication for unusual activities that may indicate signs of bypassing authentication.

CSIRT at the operator

a) Monitors networks and systems to detect unauthorized access attempts and other signs of authentication bypass.
b) Monitors for unusual behavior from authenticated users such as:
   i. frequent authentications;
   ii. authentication outside working hours;
   iii. use of services where the user is not authorized.
c) Searches the system for the presence of files such as **.exe**, **.vbs**, **.ps1** (*windows*) , **.py, .sh** (*linux*) mainly in the directorate **tmp.**
d) Request for scheduled tasks: task scheduler (*windows*) and commands **crontab -l**, **ls /etc/cron.*** in *Linux.*
e) Monitors for accounts created in the system by using commands such as: lusrmgr.msc (Windows) and the command cat /etc/passwd (Linux), etc. For domain users, it checks the user tree in *Active Directory*.
f) Immediately reports to the national and sectoral CSIRT as soon as bypassing of authentication is detected.
g) Keeps logs and data related to the bypassing of authentication for further analysis.

5.3 Identification of the incident

National CSIRT

a) Identifies the authentication bypass incident through analysis of the collected data.
b) Identifies the scope and potential impact of the incident on national security and on all critical and important infrastructures.
c) Notifies the sectoral CSIRT and the operator's CSIRT about the incident identified as an authentication bypass and its potential impacts.

Sectoral CSIRT

a) It coordinates with the CSIRT at the operator regarding the authentication bypass reported by the operators and assesses its impact on the specific assets of the sector.
b) Coordinates with the operators to determine the level of risk posed by circumvention of authentication within the sector.
c) Provides detailed incident information to the national CSIRT for an in-depth analysis.

CSIRT at the operator

a) Identifies and documents authentication bypass incidents, including the method, origin, and potential intent.
b) Identifies the user privileges that have been accessed in an unauthorized manner.
c) Applies Yara Rules to detect malicious files.
d) Identifies the IPs with which the systems communicate. Programs such as may be used. **Wireshark**, **Task Manager => Performance => Resource monitor**, **tcpview** (Sysinternals Suite), command **netstat -ano** (Windows cmd), for systems **Linux** use **netstat -tulpn** and **netstat -tupn**, or **lsof -i.**
e) Use the "Get-FileHash" command in PowerShell (Windows) or "sha256sum" (Linux) to obtain the SHA-256 hash value of the detected malicious file.
f) Reports the incident to the national and sectoral CSIRT, providing all relevant data and the

initial analysis.

g) It helps in identifying the purpose of bypassing authentication and the potential impact on infrastructure services.

5.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national CSIRT, the sectoral CSIRT, and that attached to the operator.
b) Provides updates and guidance from time to time to all relevant parties during the incident.
c) Coordinates actions for responding to the incident by following a unified approach for its mitigation.

Sectoral CSIRT

a) Utilizes the preliminary information provided by the operators and reports it directly to the national CSIRT.
b) It is coordinated directly with the operators to ensure that critical information about the incident is shared as quickly as possible and accurately, in order to optimize the operational response.
c) Conducts regular meetings with operators and other sectoral CSIRTs to coordinate actions and update defense strategies during incidents.

CSIRT at the operator

a) It coordinates with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate protective measures.
b) Informs the national and sectoral CSIRT in real time about any significant developments related to the incident and shares the updated traffic logs for further analysis.

5.5 Registration

National CSIRT

a) Registers the incident in the incident management platform together with the details regarding the incident.
b) Coordinates with the sectoral CSIRT and that at the operator in collecting the necessary information regarding the incident in order to achieve full documentation.

Sectoral CSIRT

a) Assists the CSIRT at the operator in registering the incident on the incident management platform and ensures that the affected operators are included in this process by providing additional details.
b) Collects and forwards incident data to the national CSIRT, centralizing the information.

CSIRT at the operator

a) Documents the actions taken during incident management and records them in accordance with the provisions of the cyber incident categorization regulations.
b) Reports the incident to the national CSIRT and the sectoral CSIRT.

5.6 Categorization of the Incident

National CSIRT

a) It categorizes the bypassing of authentication as an incident based on the nature, scope, and possible impact on national security.
b) Classifies the incident according to its severity, taking into account the potential damage and the targeted systems.
c) Notifies the sectoral CSIRT and the operator's CSIRT regarding the categorization of the incident and provides instructions for incident management actions.

Sectoral CSIRT

a) It is coordinated with the CSIRT at the operator regarding the categorization of the incident as authentication bypass within the sector, based on the impact and the data collected.
b) It helps in determining the nature of the bypass and its significance or impact on sectoral operations.

CSIRT at the operator

a) Categorizes and reports authentication bypass attempts.
b) Follows the established procedures for incident management based on its categorization.
c) Implements immediate measures to prevent the damage caused by attempts to bypass authentication.

5.7 Prioritization of the Incident

National CSIRT

a) Assesses the criticality of authentication bypass based on its potential to compromise sensitive data or disrupt critical services.
b) Prioritizes incident response by focusing on those incidents that may lead to significant security breaches.
c) It is coordinated with the sectoral CSIRTs and those at the operator to ensure that the most critical incidents are handled with priority.

Sectoral CSIRT

a) Assesses the impact of attempts to interfere with the sector’s critical services and prioritises them as needed.
b) Coordinates with the operator’s CSIRT to prioritize and synchronize the response to the incident.
c) Cooperates with the CSIRT at the operators with the aim of mitigating the most critical threats identified through the incident.

CSIRT at the operator

a) Assesses the impact of bypassing authentication on operational processes and prioritizes response actions as needed.
b) Ensures that any potential damage or data breach is managed and addressed immediately.
c) Reports prioritization decisions to the national and sectoral CSIRTs, providing analyses and justifications.

5.8 Incident Analysis

National CSIRT

a) Conducts a complete analysis of the incident classified as authentication bypass, focusing on its origin, method, and potential impact on national security.
b) Cooperates with international partners and intelligence agencies to gather additional information.
c) Communicates analytical findings to sectoral and operator CSIRTs to facilitate sector-specific incident responses and enhance future preventive actions.

Sectoral CSIRT

a) Assists the CSIRT at the operator in analyzing authentication bypass, using the collected information and threat intelligence.
b) Assists the CSIRT at the operator in identifying vulnerabilities exploited by authentication bypass and suggests strategies to reduce vulnerabilities.
c) Ensures the distribution of the analysis report to the national CSIRT for clarification of the situation.

CSIRT at the operator

a) Analyzes the bypass of authentication at the operational level, focusing on how it can affect critical systems and data.
b) Downloads the memory (memory dump) using tools such as FTK or alternatives, with the purpose of in-depth analysis by the relevant authorities.
c) Keeps evidence by creating a snapshot of the system’s current state.
d) Shares the findings with the national and sectoral CSIRT to contribute to a broader understanding of the incident.
e) Utilizes findings to enhance security measures and prevent further bypass attempts.

5.9 Containment and Eradication

National CSIRT

a) Provides guidelines and support for reducing the impact of circumvention authentication.
b) Coordinates efforts with sectoral CSIRTs and the one at the operator to ensure that response strategies are implemented across all sectors.
c) Addresses any weaknesses exposed by bypassing authentication, ensuring the reduction and prevention of similar cases in the future.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator for the purpose of taking preventive measures throughout the sector to prevent further exploitation of vulnerabilities.
b) Works closely with operators to ensure the reduction of vulnerabilities for intervention attempts.
c) Monitors the situation to ensure that all identified vulnerabilities have been addressed and the incident has been fully resolved.

CSIRT at the operator

a) Immediately addresses any weakness identified by authentication.
b) Deactivates compromised users.
c) Follows the preventive and mitigation procedures provided by the national and sectoral CSIRT, ensuring that all necessary steps are taken.

5.10 Restoration of services / data

National CSIRT

a) Assists in the restoration of any service affected as a result of bypassing authentication.
b) It is coordinated with the sectorial CSIRT and the CSIRT at the operator to ensure that all affected services are fully recovered.
c) Monitors the systems during and after recovery to ensure stability and to prevent future incidents.

Sectoral CSIRT

a) Helps in the restoration of sectoral services, by prioritizing the most critical affected services or systems.
b) Supports operators in restoring services to full operational capacity.
c) Communicates the status of recovery and any ongoing issues to the national CSIRT and the affected third parties.

CSIRT at the operator

a) Restore the services affected by the incident, following the drafted recovery plans. The steps that may be applied are:
    i. restoration of systems through backups (*backups*);
    ii. changing passwords for users;
    iii. the application of multi-factor authentication (MFA).
b) Verifies the integrity and functionality of the recovered services before they resume normal operations.
c) Reports the progress of recovery and any issues encountered during the recovery process to the national and sectoral CSIRT.
d) Monitors the traffic for suspicious activities that continue even after the restoration of the service.

5.11 Post-incident activity

National CSIRT

a) Draft a comprehensive report regarding the bypassing of authentication, incident response actions, and results.
b) Conducts a post-incident review to identify lessons learned and areas requiring further improvement.
c) Distributes the reports to the sectoral CSIRT and the CSIRT at the operator in order to improve incident response in the future.

Sectoral CSIRT

a) Prepares a sector-specific report detailing the impact of the incident, the actions taken to manage it, and the conclusions.
b) Participates in the post-incident review process, providing specific recommendations for the sector.
c) Disseminates reports and lessons learned within the sector to improve the response to future incidents.

CSIRT at the operator

d) Drafts a final report providing detailed information on the incident’s impact, the response actions taken, and the recovery process.

e) Participates in the lessons-learned process by identifying operational improvements and updating response plans.
f) Draws conclusions regarding the changes that need to be applied to increase the level of security in order to avoid incidents in the future such as:
   i. Network segmentation
   ii. Firewall configuration
   iii. Application security
   iv. Procedure for updating systems or applications
g) Implements the recommendations to strengthen protection and improve detection for future attacks such as unauthorized authentication.

6) Mass Attacks

The main characteristics of a DDoS attack are:
Distribution: Malicious actors use a compromised network of devices, which are infected with *malware* or *botnet* to send a large amount of traffic at once to a specific service or network. This traffic is distributed in such a way as to make it difficult to stop.
Objective is not to allow the service or network to be used normally. This interruption of service aims to damage infrastructure operations, impact reputation, damage data integrity, or distract from other attacks that may occur simultaneously.

6.1 Preparation

National CSIRT

a) Drafts and maintains specific policies and procedures for the detection of and response to volumetric attacks, otherwise known as DDoS (distributed denial-of-service) attacks.
b) Implements and regularly updates solutions for protection against DDoS, such as traffic filtering and rate limiting systems across all national networks.
c) Conducts regular training for the analysts of the national CSIRT on identifying and responding to volumetric attack scenarios.
d) Cooperates with the responsible authorities in order to liaise with internet service providers (ISPs) and cloud service providers to enable a prompt response to volumetric attacks.
e) Assigns accountable individuals to manage the incident and clearly establishes their roles and responsibilities for the incident response.

Sectoral CSIRT

a) Assists infrastructure operators through sector-specific guidelines for protection against volume attacks, ensuring compliance with national strategies.
b) Assists infrastructure operators in implementing measures to prevent volumetric attacks at entry points and critical segments of the network.
c) Conducts training for sectoral CSIRT teams and those at the operator on detection and mitigation of volumetric attacks, including the identification of high-risk events.
d) Collaborates with the operator's CSIRT to conduct continuous testing of the relevant sector's network in order to assess cyber resilience against volumetric attacks.

CSIRT at the operator

a) Implements protection measures against volumetric attacks, including traffic filtering and rate limiting.

b) Trains the staff to understand the signs of mass attacks and to report them immediately.
c) Applies the load balancing technique (*load balance*) to distribute the traffic volume and to reduce the impact of the attack.
d) Regularly updates firewall configurations and applies rules in IDS/IPS protection systems regarding the latest threats related to volumetric attacks.

6.2 Detection

National CSIRT

a) Continuously monitors national networks for signs of volumetric attacks, such as sudden increases in network traffic.
b) Use intelligence sources for threats and anomaly detection tools to identify potential activities of volumetric attacks.
c) Collaborates with the sectoral CSIRT and the operator’s CSIRT to share detection data and enhance overall situational awareness.

Sectoral CSIRT

a) Cooperates with the CSIRT at the operator for the purpose of implementing specific tools to detect volumetric attacks targeting critical infrastructure.
b) Assists operators in deploying additional tools or adjusting configurations to improve attack detection when threat levels increase.
c) Shares detected attempts of volumetric attacks with the national CSIRT and other sectoral CSIRTs to coordinate incident response efforts.

CSIRT at the operator

a) Use network monitoring tools to detect increases or abnormal traffic values that may indicate a volumetric attack (DDoS).
b) Configures automatic systems that notify in cases when traffic levels exceed predetermined limits.
c) Immediately reports any detected attempts of volumetric attacks to the national and sectoral CSIRTs.
d) Retains logs and data related to detected volumetric attacks for further analysis and response.

6.3 Identification of the incident

National CSIRT

a) It confirms the presence of a volumetric attack through in-depth analysis, utilizing national intelligence resources.
b) It coordinates with sectoral CSIRTs to synchronize identification data and to create a complete overview of the attack on a national scale.
c) Notifies the relevant sectoral CSIRTs and the operator CSIRTs about the identified volumetric attack and its potential impacts.

Sectoral CSIRT

a) Coordinates with operators regarding volumetric attacks they have reported and assesses their impact on sector assets.
b) Coordinates with operators to determine the scale of a volumetric attack within the sector.
c) Provides detailed information about the incident to the national CSIRT for a complete analysis.

CSIRT at the operator

a) Identifies and documents the volumetric attack, including the source, method, and possible targets based on the analysis of traffic and logs.
b) Identifies the affected systems, and the extent of the attack to other systems, if any.
c) Reports the incident to the national and sectoral CSIRT, providing all relevant data and the initial analysis.
d) Identifies the purpose of the attack and its possible impact on operational services.

6.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national CSIRT, the sectoral CSIRT, and the CSIRT at the operator.
b) Communicates with competent national authorities to block IPs identified as malicious following completed analyses.
c) Provides updates and guidance from time to time to all relevant parties during the incident.
d) Coordinates incident response actions by following a unified approach to mitigation.

Sectoral CSIRT

a) Utilises the preliminary information provided by the operators and reports it directly to the national CSIRT.
b) It is coordinated directly with the operators to ensure that critical information regarding the incident is shared as quickly and accurately as possible in order to optimize the operational response.
c) Conducts regular meetings with operators and other sectoral CSIRTs to harmonize actions and update defense strategies during an incident.

CSIRT at the operator

a) Coordinates with other departments internally, ensuring all relevant stakeholders are aware of changes and take protective measures.
b) Inform the national and sectoral CSIRT in real time about any important developments related to the incident and share updated traffic logs for further analysis.

6.5 Registration

National CSIRT

a) Records the volumetric attack as an incident in the national incident management system, ensuring
b) that all collected data are registered.
c) Coordinates with the sectorial CSIRT and the CSIRT at the operator to gather additional information and to ensure that the incident is fully documented.

Sectoral CSIRT

a) Coordinates with the operator's CSIRT affected by the incident to record the volumetric attack in the incident management platform, based on documentation.
b) Coordinates with the CSIRT at the operator with the aim that all affected operators are included in the registration process.
c) Sends the information and details of the incident collected to the national CSIRT in order

to centralize the information.

CSIRT at the operator

a) Documents the volume attack and any initial findings based on the collected data.
b) Ensures the proper registration in the incident management system according to the provisions in the regulation for the categorization of cyber incidents.
c) Reports the incident to the national CSIRT and the sectoral CSIRT with all relevant details.

6.6 Categorization of the Incident

National CSIRT

a) Classifies the volumetric attack as a cyber incident through analysis of network traffic data and other indicators.
b) Categorizes the volumetric attack based on its nature, scope, and potential impact on national security.
c) Classifies the incident according to its severity, taking into account the possible disruption of critical services.
d) Notifies the sectoral CSIRT and the one at the operator for categorisation and provides guidance for the appropriate response actions.

Sectoral CSIRT

a) Coordinates with the operator's CSIRT regarding the categorization of the volumetric attack within the sector, based on impact and collected data.
b) Assists in determining the specific nature of the volumetric attack and its significance for sector operations.

CSIRT at the operator

a) Categorizes and reports the volumetric attack, ensuring that all information assists in the categorization of the incident.
b) Follows the established procedures for incident management based on its categorization.
c) Implements immediate measures to mitigate any damage caused by the volumetric attack.

6.7 Prioritization of the Incident

National CSIRT

a) Assesses the significance of the volumetric attack based on its potential to disrupt critical services or compromise national security.
b) Prioritizes incident response, focusing on those incidents that may lead to significant disruptions.
c) Coordinates with the sectoral CSIRT and the one at the operator to ensure that the most critical incidents are handled promptly.

Sectoral CSIRT

a) Assesses the impact of the volumetric attack on the sector's critical services and assists the operator's CSIRT in prioritizing and coordinating the response as needed.
b) Coordinates with the operator's CSIRT to mitigate the highest-risk threats identified through the volumetric attack.

CSIRT at the operator

a) Assesses the impact of the volumetric attack on operational processes and prioritizes response actions to the attack as needed.
b) Ensures that any possible interruption of services is managed and addressed immediately.
c) Reports the prioritization decisions to the sectoral CSIRT and the national CSIRT, based on analyses and reasoning.

6.8 Incident Analysis

National CSIRT

a) Conducts a comprehensive analysis of the volumetric attack, focusing on its origin, method, and potential impact on national security.
b) Cooperates with international partners and intelligence agencies to gather additional information.
c) Distributes the analysis results to sectoral CSIRTs and operator CSIRTs to support a faster incident response and prevent similar attacks in the future.

Sectoral CSIRT

a) Assists the operator's CSIRT in analyzing the attack affecting the sector, utilizing collected information and threat intelligence.
b) Assists the CSIRT at the operator in identifying the vulnerabilities exploited by the attack and suggests mitigation strategies.
c) Makes analysis data available to the national CSIRT and the operator's CSIRT to provide insight into the scope and nature of the attack.

CSIRT at the operator

a) Analyzes the volumetric attack at the operational level, focusing on its impact on critical systems and services, including performance degradation or partial disruption.
b) Analyzes the nature of the attack to determine whether its primary objective is to serve as a diversion from a more sophisticated attack or to directly disrupt operational services.
c) Collects and analyses logs for the identification of malicious IPs, and categorises these IPs as indicators of compromise (IOC).
d) Analyzes the ports and services targeted by malicious actors in order to identify possible vulnerabilities and main objectives of volumetric attacks.
e) Shares the findings with the CSIRTs to contribute to a broader understanding of the attack.
f) Implements findings to enhance security measures and prevent further volumetric attacks.

6.9 Containment and Eradication

National CSIRT

a) Provides guidance and support for mitigating the impact of identified volumetric attacks.
b) Coordinates with sectoral CSIRTs and operator CSIRTs to ensure that mitigation strategies are implemented across all sectors.
c) Leads efforts to address weaknesses revealed by the volumetric attack, aiming to reduce risk and prevent similar incidents in the future.

Sectoral CSIRT

a) Coordinates with operator CSIRTs to implement protective measures and prevent further disruptions caused by the volumetric attack.
b) Works closely with operators to ensure effective mitigation of the attack's impact.

c) Monitors the situation to verify that all identified vulnerabilities have been addressed and the incident has been fully resolved.

CSIRT at the operator

a) Immediately addresses identified weaknesses resulting from the volumetric attack.

b) Follow the mitigation procedures provided by the national and sectoral CSIRT, ensuring that all necessary steps have been taken. Depending on the services affected, the following measures are suggested:

i. Cases when packets use ports **TCP** we are dealing with **SYN** Flood.
   a. Configure the Firewall, IDS, and IPS by filtering traffic from IPs that initiate bulk traffic.

ii. Cases when packets use ports **UDP** we are dealing with **UDP** Përmbytje.
   a. Limit the number of incoming UDP packets;

iii. **DNS Reflection** (It uses an open DNS resolver to load the server during the DNS response process).
   a. Such cases are used to generate high bandwidth traffic, where the solution in this case is to contact **ISP**, in order to migrate our IP to DDoS protection.
   b. In case the DDoS attack is exploiting a system vulnerability to create a DDoS attack without generating high bandwidth, it should be configured **DNS filter**.

iv. **NTP** uses open NTP servers.
   a. If the NTP version is lower than 4.2.7, an upgrade to 4.2.7+ is recommended.
      i. If an upgrade is not possible, it is recommended to do so **disable monlist and implementation of Ingress Filtering.**
   b. Use NTP filtering.

v. **SSDP** uses UPnP (Universal Plug and Play) to cause DDoS
   a. Blocking of traffic on port 1900.

vi. **XML-RPC** exploits XML-RPC requests that contain data structure and loaded information by consuming server resources.
   a. Implementation of *Rate-Limiting* and request filtering for XML requests
   b. Use the IP Whitelist or Blacklist for those IPs you want to allow or not.

vii. Other recommendations:
   a. If you are seeing a lot of incoming traffic (incoming requests) in **webserver logs**, or **filled bandwidth**, this may indicate an attack that is attempting to block your online service. Isolate your critical assets, identify the services that are exposed on the internet and the vulnerabilities of these services.

c) Verifies the effectiveness of containment and mitigation efforts and reports the status to the national CSIRT.

6.10 Restoration of Services / Data

National CSIRT

a) Assists in restoring services or systems affected by the volumetric attack back to normal operations.

b) Coordinates with the sectoral CSIRT and the operator’s CSIRT to ensure that all affected services are fully recovered.

c) Assists the operator’s CSIRT in monitoring systems during and after recovery to ensure stability and prevent future incidents.

Sectoral CSIRT

a) Assists in the recovery of sector-specific services, prioritizing the most critical affected

services and systems.
b) Supports operators in restoring services to full operational capacity.
c) Communicates the recovery status and any ongoing issues to the National CSIRT and other third parties involved in the incident.

CSIRT at the operator

a) Recovers services affected by the volumetric attack, following the established recovery plans.
b) Verifies the integrity and functionality of recovered services before resuming normal operations.
c) Documents and reports recovery progress and any issues to the National and Sectoral CSIRT for further support.

6.11 Post-incident activity

National CSIRT

Drafts a detailed report on the volumetric attack, incident response actions, and outcomes.

a) Conducts a post-incident review to identify lessons learned and improve detection and response capabilities against attacks.
b) Shares the report with the sectoral CSIRT and the operator's CSIRT to enhance overall preparedness.

Sectoral CSIRT

a) Prepares a report for the sector describing the impact of the volumetric attack, the incident response actions, and the recovery efforts.
b) Participates in the post-incident review process, contributing with knowledge and sector-specific recommendations.
c) Shares the lessons learned within the sector to improve detection and response capabilities in the future.

CSIRT at the operator

a) Drafts a final report providing detailed information on the impact of the volumetric attack, the response, and the recovery.
b) Participates in the lessons-learned process, identifying operational improvements and updating response plans.
c) Implements the recommendations to strengthen defenses and improve future detection of volumetric attacks.

7) Security of information content

Information Content Security includes the measures and practices implemented to protect the confidentiality, integrity, and availability of information and data within an organization. This involves a wide range of strategies, technologies, policies, and procedures designed to protect sensitive information from unauthorized access, unauthorized distribution, modification, and destruction. In cases where there are breaches of authorization in accessing or modifying information, the following steps are followed:

7.1 Preparation

National CSIRT

a) Drafts and maintains specific policies and procedures for detecting and responding to information content security incidents.
b) Regularly implements and updates technological solutions for information content security, such as data filtering and information classification.
c) Conducts regular training for national CSIRT analysts on best practices for protecting information content and responding to incidents.
d) Cooperates with the sectoral CSIRT and the operator’s CSIRT to enable a quick and coordinated response to information security incidents.
e) Appoints responsible personnel to follow up on the incident and defines their roles and responsibilities.

Sectoral CSIRT

a) Assists the operator’s CSIRT through sector-specific guidance for protecting information content, ensuring compliance with national policies.
b) Assists the operator’s CSIRT in implementing tools for protecting information content at the network entry points and the sector’s critical systems.
c) Provides training for both the sectoral CSIRT teams and the operator’s CSIRT teams on identifying and responding to incidents affecting information content security.
d) Assists the operator’s CSIRT in conducting regular system testing to assess cyber resilience against information content incidents.

Operator’s CSIRT

a) Implements protective measures for information content, including encryption, access control, and data classification techniques.
b) Trains staff to identify signs of information content security incidents and to report them immediately.
c) Regularly updates security configurations and applies rules in IDS/IPS protection systems related to the latest threats to information content.
d) Applies information management techniques to prevent unauthorized access and protect critical data.

7.2 Detection

National CSIRT

a) Continuously monitors the national network for signs of information content security incidents, such as unauthorized access or unexpected data changes.
b) Uses threat intelligence sources and anomaly detection tools to identify potential activities affecting information content.
c) Cooperates with the sectoral CSIRT and the operator’s CSIRT to share detection data and enhance the ability to respond to the situation.

Sectoral CSIRT

a) Cooperates with the operator’s CSIRT on the implementation of specific tools to detect incidents targeting critical information content.
b) Assists the operator’s CSIRT in using additional tools or changing configurations to better detect threats to information content.
c) Shares findings regarding information content security incidents with the National CSIRT

and affected operators to coordinate the incident response.

Operator's CSIRT

a) Uses monitoring tools to detect suspicious activities that may indicate an information content security incident.
b) Configures automated systems to issue alerts when information is accessed by unauthorized individuals.
c) Immediately reports any detected attempts or incidents affecting information content security to the National and Sectoral CSIRT.

7.3 Incident Identification

National CSIRT

a) Confirms the content security incident through the analysis of logs, system data, and other indicators.
b) It is coordinated with the sectoral CSIRT and the one at the operator in order to synchronize the identification data and to create a complete overview of the incident at the national level.
c) Notifies the sectoral CSIRT and the one at the operator regarding the identified incident and
d) possible impacts.

Sectoral CSIRT

a) Coordinates with the operator's CSIRT to verify the reported incident and assesses its impact on sector assets.
b) Coordinates with operators to determine the scope of the incident within the sector.
c) Provides detailed incident information to the National CSIRT for further in-depth analysis.

Operator's CSIRT

a) Identifies and documents the incident, including its source, method, and possible objectives based on log and system activity analysis.
b) Identifies files accessed, modified, or deleted in an unauthorized manner.
c) Identifies indicators of compromise such as IP addresses, domains, hashes, emails, etc.
d) Identifies affected systems and reports the incident to the National and Sectoral CSIRTs, providing all relevant data and initial findings such as the time of detection and the number of affected systems.
e) Maintains records for further analysis. Creates forensic copies of affected systems to preserve them for deeper investigations.

7.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the National CSIRT, the Sectoral CSIRT, and the Operator's CSIRT to ensure a unified response.
b) Communicates with competent authorities for cooperation in resolving incidents affecting information content at the national level.
c) Provides continuous updates and guidance to all relevant parties throughout the incident.

Sectoral CSIRT

a) Coordinates directly with operators' CSIRTs to ensure that information about the incident is shared in a timely manner to optimize response.
b) Holds regular meetings with operators and other sectoral CSIRTs to coordinate defense actions and strategies.

Operator's CSIRT

a) Coordinates with other departments within the infrastructure, ensuring that all parties are aware of the situation and take appropriate protective measures.
b) Provides real-time updates to the Sectoral and National CSIRT on any significant developments and shares updated logs for analysis.

7.5 Registration

National CSIRT

a) Registers the incident in the national incident management system, ensuring that all collected data is preserved.
b) Coordinates with the Sectoral CSIRT and the Operator's CSIRT to gather additional information and ensure that the incident is fully documented.

Sectoral CSIRT

a) Coordinates with the affected operator's CSIRT to register the incident in the management platform provided by the National CSIRT and ensures that the affected operators are included in this process by contributing additional details.
b) Sends incident data to the National CSIRT to centralize the information.

Operator's CSIRT

a) Documents the incident and any initial findings based on the collected data.
b) Ensures the registration of the incident in the incident management system according to the provisions of the cybersecurity incident categorization regulation.
c) Reports the incident to the National and Sectoral CSIRT with all relevant details (logs).

7.6 Incident Categorization

National CSIRT

a) Categorizes the information content security incident based on its nature, scope, and potential impact on national security.
b) Classifies the incident according to its severity, taking into account the possible disruption of critical services, loss of sensitive information, and damage to national reputation.
c) Notifies the Sectoral CSIRT and the Operator's CSIRT about the categorization and provides guidance on appropriate response actions

Sectoral CSIRT

a) Coordinates with the Operator's CSIRT regarding the categorization of the information content security incident within the sector, based on its impact and collected data.
b) Assists in determining the specific nature of the incident and its importance for sectoral operations.

Operator's CSIRT

a) Categorizes and reports the incident, ensuring that all information supports the categorization based on the impact on the system and information content.

b) Follows established procedures for incident management according to its categorization, including immediate measures to secure information.

c) Implements immediate measures to mitigate any damage caused by the incident and to prevent its spread.

7.7 Incident Prioritization

National CSIRT

a) Assesses the importance of the information content security incident based on its potential to disrupt critical services, compromise sensitive data, and affect national security.

b) Prioritizes the response to incidents, focusing on those that could cause significant damage to information content or national security.

c) Coordinates with the Sectoral CSIRT and the Operator's CSIRT to ensure that the most critical incidents are addressed promptly and their impact minimized.

Sectoral CSIRT

a) Assesses the impact of the information content security incident on the sector's critical services and prioritizes accordingly.

b) Coordinates with the Operator's CSIRT on prioritization, ensuring that they take immediate measures to mitigate the incident's impact on their operations.

c) Assists the Operator's CSIRT in avoiding high-risk threats that affect the sector's critical information content.

Operator's CSIRT

a) Assesses the impact of the information content security incident on operational processes and prioritizes response actions based on its risk level.

b) Ensures that any potential service disruption is managed and addressed immediately, preserving the integrity of the information content.

c) Reports prioritization decisions to the National and Sectoral CSIRTs, based on accurate analyses and justifications.

7.8 Incident Analysis

National CSIRT

a) Conducts a comprehensive analysis of the incident, focusing on its source, method, and impact on the national security of information.

b) Cooperates with international partners and intelligence agencies to gather additional information.

c) Analyzes and distributes indicators of compromise across all critical and important information infrastructures.

d) Shares the analysis results with the Sectoral CSIRT and the Operator's CSIRT to support a faster response to the incident.

Sectoral CSIRT

a) Assists the Operator's CSIRT in conducting the analysis for the affected sector, leveraging collected information and threat intelligence.

b) Assists the Operator's CSIRT in identifying exploited vulnerabilities and suggests strategies for improving security at the sectoral level.

c) Provides the National CSIRT and the Operator’s CSIRT with detailed findings from the analysis to deliver in-depth information about the incident.

Operator's CSIRT

a) Analyzes the incident at the operational level, highlighting its impact on critical systems and information content.
b) Analyzes whether the incident originated from insiders within the infrastructure.
c) Examines logs to identify the entry point and all indicators contributing to system compromise.
d) Collects and analyzes logs to identify malicious sources and shares the results with the CSIRTs.
e) Investigates for malicious programs that may be present in the system, specifically searching in the **%TEMP%** directory on Windows or **/tmp** on Linux.=

7.9 Containment and Eradication

National CSIRT

a) Provides guidance and support for isolating and mitigating the impact of information content security incidents.
b) Coordinates efforts with the Sectoral CSIRT and the Operator’s CSIRT to ensure that cyber resilience, isolation, and eradication strategies are applied across all sectors.
c) Addresses any weaknesses identified from the incident, ensuring reduction and prevention of similar cases in the future.
d) Cooperates with affected operators to stop unauthorized access and to erase compromised content from systems and other national resources.

Sectoral CSIRT

a) Assists the Operator’s CSIRT in implementing protective measures to isolate affected systems and networks, including blocking unauthorized access to information content.
b) Works closely with operators to ensure effective mitigation of the incident’s impact and removal of harmful content from systems (malicious files, modified content, malicious code, etc.
c) Monitors the situation to ensure that all identified weaknesses are addressed and that the incident is fully isolated and eradicated.
d) Assists the Operator’s CSIRT in analyzing the techniques used by malicious actors to develop preventive measures and update policies on information content security.

Operator's CSIRT

a) Immediately isolates any system affected by the incident, including cutting off unauthorized access to critical information content.
b) Follows the guidance provided by the National and Sectoral CSIRT for isolation and mitigation of the incident, ensuring all necessary steps are taken to prevent its spread.
    - **Monitors traffic** for suspicious activity.
    - **Checks if Syslog is configured**:
        - If yes, analyzes logs to determine when information was accessed and which user last modified it.
        - If not, uses PowerShell commands to identify recently modified files in a specific path. Function (Get-Date).AddDays(-30) checks for files modified in the last 30 days, -Filter *.exe checks for .exe file types.

Windows:

```
Get-ChildItem -Path C:\ -Recurse -File -Force -Filter *.exe | Where-Object { $_.LastWriteTime -gt (Get-Date).AddDays(-30) -and $_.PSIsContainer -eq $false}
```

Linux:

```
find / -type f -name "*.sh" -mtime -30
find / -type f -name "*.py" -mtime -30
```

- **When unauthorized access is internal**, the person owning the computer/instance is questioned to clarify the access details.
- **Analyzes Windows Event Viewer logs** for “Successful Login” to determine who accessed information and when:
  - Logon Type 2 – Local or console login
  - Logon Type 3 – Shared directory login
  - Logon Type 10 – RDP login
- **Analyzes DLP or log server data** to understand distribution methods, such as USB usage, CD-ROMs, or web browser history to identify potential sources of information leakage.
  Event Viewer → System Logs → Filter events by EventID 2002 (USB Connect/Disconnect).
- **If insider access occurred**, a meeting is held with the involved staff to gather further details.

c) Implements measures to erase or neutralize compromised content from all systems and resources, using encryption, classification, and secure data deletion tools.

d) Verifies the effectiveness of isolation and eradication efforts and reports the status to the National and Sectoral CSIRTs. Depending on the type of incident, the following measures are suggested:

   i. **Unauthorized data access**: Enforce strict access controls and change compromised credentials to isolate the incident.

   ii. **Unexpected data modification**: Restore data from secure backups and monitor to prevent further changes.

   iii. **Misinformation content**: Identify and remove dangerous content and block sources spreading the compromised information.

7.10 Service/Data Recovery

National CSIRT

a) Assists in restoring the affected information.

b) Monitors systems during and after recovery to ensure stability and to prevent future incidents.

Sectoral CSIRT

a) Assists in the recovery of compromised information content and supports operators in the full restoration of content.

b) Communicates the recovery status and any ongoing issues to the National CSIRT and affected third parties.

Operator's CSIRT

a) Recovers affected information content, following the recovery plan.

b) Verifies the integrity of the recovered information.

c) Documents and reports recovery progress to the National and Sectoral CSIRTs.

7.11 Post-Incident Activity

National CSIRT

a) Drafts a detailed report on the incident and the actions undertaken.
b) Conducts a post-incident review to identify lessons learned and to improve efforts for preventing similar incidents in the future.
c) Shares the report with the Sectoral CSIRT and the Operator’s CSIRT to enhance preparedness for responding to such incidents in the future.

Sectoral CSIRT

a) Prepares a sectoral report describing the impact and the recovery efforts.
b) Participates in the post-incident review process, contributing sector-specific knowledge and recommendations.
c) Disseminates lessons learned within the sector to improve future responses to such incidents.

Operator's CSIRT

a) Drafts a final report providing detailed information on the incident’s impact, the response, and the recovery.
b) Participates in the lessons-learned process, identifying areas for improvement to ensure faster responses in future incidents.
c) Implements the recommendations to strengthen protection and improve future detection of information content security incidents.

8) Fraud

Fraud generally refers to any malicious activity aimed at deceiving individuals or infrastructures for personal, financial, or espionage purposes. This includes phishing attacks, identity theft, financial fraud, or any other fraudulent practice used to unlawfully obtain money, information, or assets. Fraudulent activities often exploit security vulnerabilities, manipulate human psychology, or use social engineering tactics. The main characteristic of fraud in these categories is the intent to deceive and gain something of value through various means.

8.1 Preparation

National CSIRT

a) Drafts policies and procedures for detecting and responding to threats such as computer fraud (e.g., fake websites, phishing, and social engineering).
b) Implements advanced systems for threat detection, including technologies such as honeypots, honey tokens, and decoy systems.
c) Trains CSIRT analysts to identify and respond to computer fraud tactics, including how to manage and interpret false positives.
d) Cooperates with international cybersecurity organizations to stay informed about emerging computer fraud techniques.
e) Designates the individuals responsible for incident response, clearly defining their roles and responsibilities.

Sectoral CSIRT

a) Assists the operator's CSIRT by providing sector-specific guidelines for identifying and mitigating attacks such as computer fraud, while ensuring alignment with national strategies."
b) Assists the operator's CSIRT in implementing sector-specific technologies for detecting computer fraud. These include fake data, credentials, and services designed to attract and identify malicious actors.
c) Conducts periodic training sessions for both sectoral CSIRT teams and the operator's CSIRT, using computer fraud scenarios tailored to their specific needs.
d) Monitors and supports the operator's CSIRT on an ongoing basis, ensuring that relevant systems are regularly updated to strengthen protection against computer fraud attacks.

CSIRT at the operator

a) Implements and maintains technologies for the prevention of computer fraud, by setting up fake systems, and creating fake data within the operational environment.
b) Trains staff to understand computer fraud and the importance of reporting suspicious activities.
c) Regularly updates security configurations to ensure they remain effective against new threats.

8.2 Detection

National CSIRT

a) Continuously monitors national networks for computer fraud activities, such as interactions with honeypots or unexpected access to fraudulent systems (*honeypots*).
b) Utilizes advanced intelligent tools for detecting threats and anomalies to identify potential computer fraud attacks.
c) Cooperates with sectoral CSIRTs and the CSIRT at the operator to increase detection capacities by sharing data on detected computer fraud activities.

Sectoral CSIRT

a) Assists the operator's CSIRT in implementing sector-specific tools to detect interactions with computer fraud assets, such as honeypots and fake data.
b) Provides the operator's CSIRT with advice and policies to prevent unauthorized access and fraud attempts, including:
c) Impersonation of staff by malicious actors via email;
d) Infected USBs;
e) Interception, etc.
f) Shares information on detected computer fraud activities with the national CSIRT and other sectoral CSIRTs to enable a coordinated response..
g) Supports the operator's CSIRT in monitoring sectoral networks for suspicious activities that may indicate computer fraud attempts.

CSIRT at the operator

a) Uses network monitoring tools to detect unauthorized attempts to access or interact with fraud-detection systems, which may indicate a potential incident."
b) Monitors systems for unusual or suspicious user activities that may indicate potential security incidents.
c) Immediately reports any detected computer fraud activity to the national and sectoral

CSIRTs.

d) Stores the logs and the data related to the activities identified for detailed analysis.

8.3 Incident identification

National CSIRT

a) Confirms computer fraud activity as an incident after analyzing the collected data.

b) Identifies the extent and impact of the incident on national security as well as on all critical and important infrastructure

c) Notifies the relevant sectoral CSIRTs and operators about the identified computer fraud activity and its potential implications.

Sectoral CSIRT

a) Coordinates with the operator's CSIRT to verify reported computer fraud activity and assess its impact on the sector's specific assets.

b) Works with operators to determine the scale of computer fraud activity within the sector.

c) Provides detailed information about the incident to the national CSIRT to enable a more comprehensive analysis.

CSIRT at the operator

a) Identifies and documents computer fraud activity, including the techniques used, the source, and the targeted assets.

b) Identifies indicators of compromise (IOCs).

c) Reports the incident to the national and sectoral CSIRTs, providing all relevant data and the results of the initial analysis.

d) Identifies the purpose of the computer fraud activity and its potential impact on systems or services.

8.4 Communication and Coordination

National CSIRT

a) Establishes secure communication channels between the national CSIRT, the sectoral CSIRT, and the operator's CSIRT.

b) Provides timely updates and guidance to all relevant parties throughout the incident.

c) Coordinates response actions by applying a unified approach to incident mitigation

Sectoral CSIRT

a) Utilizes preliminary information provided by operators and reports it directly to the national CSIRT.

b) Coordinates directly with operators to ensure that critical incident information is shared quickly and accurately, optimizing the operational response.

c) Holds regular meetings with operators and sectoral CSIRTs to harmonize actions and update defense strategies throughout the incident.

CSIRT at the operator

a) Coordinates with other departments within the infrastructure to ensure that all relevant parties are informed of the situation and take appropriate protective measures.

b) Informs the national and sectoral CSIRTs in real time about any significant developments related to the incident and shares updated traffic logs for further analysis.

8.5 Registration

National CSIRT

a) Records the incident in the National incident management platform and ensures that all data collected is safe and saved.
b) It is coordinated with sectoral CSIRTs and Cyber Team at the operator in order to gather additional information and ensure that the incident is fully documented.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator affected by the incident in order to register the incident on the management platform provided by the national CSIRT and ensures that the affected operators are involved in this process by assisting with additional details.
b) Sends data on the incident to the national CSIRT to centralize the information.

CSIRT at the operator

a) Documents the incident and any initial findings based on the data collected.
b) Ensures the recording of the incident in the incident management system according to the definitions in the cybersecurity incident categorization regulation.
c) Reports the incident to the national and sectoral CSIRT and with all relevant details (logs).

8.6 Categorization the incident

National CSIRT

a) It categorises the activity of computer fraud based on the nature, scope, and impact that the incident has on national security.
b) Classifies the incident according to its severity, taking into account the potential damage and the systems or services targeted.
c) Notifies the sectoral CSIRT and that of the operator for categorization and provides guidance on the appropriate incident response actions.

Sectoral CSIRT

a) Coordinates with the operator's CSIRT regarding the categorization of the content security incident within the sector, based on the impact and data collected
b) Assists in determining the specific nature of the incident and its significance to sector operations.

CSIRT at the operator

a) Categorizes and reports the incident, ensuring that all information leads to the categorization of the incident based on the impact on the system and the content of the information.
b) Follows established procedures for managing the incident based on its categorization, including immediate measures to secure the information.
c) Implements immediate measures to mitigate any damage caused by the incident and to prevent its spread.

8.7 Prioritization of incident

National CSIRT

a) Assesses the significance of the information content security incident based on its potential to disrupt critical services, compromise sensitive data, and impact national security.
b) Prioritizes incident response, focusing on those incidents that could lead to significant harm to information content or national security.
c) Coordinates with the sectoral and operator CSIRTs to ensure that the most critical incidents are handled expeditiously and their impact is reduced.

Sectoral CSIRT

a) Assesses the impact of the information content security incident on the sector's critical services and prioritizes as necessary.
b) Coordinates with the operator's CSIRT on prioritization, ensuring that they take immediate action to mitigate the impact of the incident on their operations.
c) Assists the operator's CSIRT in order to avoid high-risk threats that affect the sector's critical information content.

CSIRT at the Operator

a) Assesses the impact of the information content security incident on operational processes and prioritizes response actions according to its risk.
b) Ensures that any potential service disruption is managed and addressed promptly, while maintaining the integrity of the information content.
c) Reports prioritization decisions to the national and sectoral CSIRT, based on accurate analysis and reasoning.

8.8 Incident Analysis

National CSIRT

a) Conducts a thorough analysis of the incident, focusing on its source, method, and impact on national information security.
b) Collaborates with international partners and intelligence agencies to gather additional information.Analyzes and disseminates indicators of compromise across all critical and important information infrastructures.
c) Distributes analysis results to the sectoral CSIRT and the operator's CSIRT to assist in the fastest response to the incident.

Sectoral CSIRT

a) Assists the operator's CSIRT in conducting analysis for the affected sector, using the collected information and threat intelligence.
b) Assists the operator's CSIRT in identifying exploited vulnerabilities and suggests strategies for improving security at the sector level.
c) Makes available to the national and operator CSIRT details from the analysis carried out in order to provide detailed information about the incident.

CSIRT at the operator

a) It analyzes computer fraud activity at the operational level, focusing on how it can impact critical systems and services.
b) Analyzes the activity of users and the technique used by malicious actors that led to the incident regarding:
   i. If we are dealing with payments.
      a. Communicates with third parties (banks) in order to obtain the necessary

support for stopping or reversing the payment.
        b. Analyzes how the payment was reached.

ii. Email Phishing.
    a. Analyses through *email header* the source of the content of the message (email);
    b. Analyzes the content of the email;
    c. Analyzes annexes;
    d. Analyzes connections (*link*);
    e. Analyzes DNS;
    f. Analyzes internet traffic;

iii. Fraud by telephone (Vishing).
    a. Contacts the competent authorities (the police), to obtain details regarding the call made

iv. Social engineering.
    a. Interviews persons who have been deceived through social engineering

v. Malicious attack;
    a. Analyzes the source of the attack (exploited vulnerable services) ;
    b. Checks for malicious programs (malware, spyware, etc.);

vi. He/she analyses the information collected in order to document it afterwards.

vii. Copyright theft.
    a. It analyses the source from which these documents have been taken;
    b. Analyzes who the publisher of the materials is;
    c. Collects evidence as *screenshot*, url, schedules, video, etc., which serve for documentation;
    d. Contacts law enforcement authorities for further measures.

c) Shares the findings with the CSIRTs to contribute to a deeper understanding of the incident.
d) Implements the findings for improving security measures and preventing attempts further for computer fraud.

8.9 Containment and Eradication

National CSIRT

a) Provides guidance and support for the isolation and mitigation of the impact of information content security incidents.
b) Coordinates efforts with the sectoral CSIRT and the operator CSIRT to ensure that cyber resilience, isolation and deletion strategies are implemented across all sectors.
c) Addresses any vulnerabilities identified by the incident, ensuring the reduction and prevention of similar incidents in the future.
d) Collaborates with affected operators to prevent unauthorized access and to delete compromised content from other national systems and resources.

Sectoral CSIRT

a) Assists the CSIRT at the operator in implementing protective measures throughout the sector to prevent future incidents.
b) Works closely with operators to reduce computer fraud activities as much as possible.
c) Monitors the situation to ensure that all identified vulnerabilities have been addressed and the incident has been fully resolved.

CSIRT at the operator

a) Immediately addresses any weakness identified through computer fraud activity.
b) Follows the procedures provided by the CSIRTs (national and sectoral) to contain and

reduce malicious activities, ensuring that all necessary steps are taken.

c) Verifies the effectiveness of efforts to deter and mitigate malicious activities and
d) reports the status to the CSIRTs.

8.10 Restoration of services / data

National CSIRT

a) Assists in restoring any service affected by computer fraud activity to normal operations.
b) Coordinate with the sectoral CSIRT and that at the operator to ensure that all affected services are fully recovered.
c) Monitors systems during and after recovery to ensure stability and prevent future incidents.

Sectoral CSIRT

a) Assists the CSIRT at the operator with the aim of recovering specific sectoral services, prioritizing the most critical affected services or systems.
b) Assists operators in restoring services to full operational capacity.
c) Communicates the recovery status and any ongoing issues to the national CSIRT and third parties.

CSIRT at the operator

a) Recovers the services affected by the computer fraud activity, by following the drafted recovery plans.
b) Verify the integrity and functionality of the restored services before resuming normal operations.
c) Reports recovery progress and any issues during recovery to the national and sectoral CSIRT for further assistance.

8.11 Post-incident activity

National CSIRT

a) Draft a comprehensive report detailing the incident of computer fraud, the actions of
b) incident response and results.
c) Reviews the situation after the incident to identify lessons learned and areas for improvement, with the aim of responding to the incident in the shortest possible time.
d) Distributes the report with The sectoral CSIRT and that at the operator to increase overall preparedness.

Sectoral CSIRT

a) Prepare a report on the impact of the computer fraud incident, the incident response actions, and the recovery steps.
b) Participates in the post-incident review process, contributing sector-specific knowledge and recommendations.
c) Disseminates lessons learned within the sector to improve detection and incident response capabilities in the future.

CSIRT at the operator

a) Drafts the final report, providing detailed information on the impact of the computer fraud incident, the response, and the recovery.
b) Participates in the lessons learned process, identifying improvements and updating

response plans.

c) Implements the recommendations to strengthen protection and to improve detection in possible future attacks related to computer fraud activities.

9) Weaknesses

Weaknesses refer to the vulnerabilities that systems may possess, which can be exploited by malicious actors to gain unauthorized access. Such vulnerabilities often stem from outdated software, misconfigurations in applications or network infrastructure, and zero-day flaws, where the weaknesses are still unknown. These vulnerabilities can also be identified through security scans and penetration testing.

9.1 Preparation

National CSIRT

a) Centralized vulnerability scanning tools are implemented to assess national networks and systems

b) Continuously trains the CSIRT analysts on vulnerability assessment techniques, the use of tools, and new vulnerabilities.

c) Cooperates with international security cyber organisations to receive timely updates on newly discovered vulnerabilities.

d) Continuously shares information with the sectoral CSIRT and the one at the operator regarding the latest vulnerabilities identified in technology.

e) Determines the persons to be involved in the incident response, roles, and responsibilities for addressing vulnerabilities.

Sectoral CSIRT

a) Provides specific guidance to the sector for regularly conducting assessments of vulnerabilities, ensuring compliance with national strategies.

b) Assists the CSIRT at the operator in the implementation of technologies and tools for vulnerability assessment adapted to the specific needs of the sector.

c) Trains sectoral teams on the importance of vulnerability assessments and the use of assessment tools.

d) Prioritises and addresses vulnerabilities based on the sector's critical assets.

CSIRT at the operator

a) Conducts regular scans for the assessment of vulnerabilities within the infrastructure.

b) Trains the staff on the importance of vulnerability management and how to respond to them.

c) Ensures that all systems are up to date and *patch*-are regularly updated to mitigate known vulnerabilities.

d) Inventories the assets and assesses them for vulnerabilities, including software, hardware devices, and network devices.

9.2 Detection

National CSIRT

a) Scans networks and systems national for vulnerabilities by using means to
b) automated and manual techniques.
c) Correlates data from various sources, including sectoral reports and threat intelligence, in order to detect and assess potential vulnerabilities.
d) Monitors for any new vulnerability that may affect national security and all critical and important infrastructure.

Sectoral CSIRT

a) Shares the discovered vulnerabilities with the national CSIRT and other sectoral CSIRTs for a coordinated response.
b) Assists the CSIRT at the operator in monitoring the network and specific sector systems for new vulnerabilities that may arise due to environmental changes or software updates.

CSIRT at the operator

a) Uses automated tools to perform periodic scans of the infrastructure to detect possible vulnerabilities in the systems and applications used.
b) Monitors the network for suspicious activities by malicious actors, and identifies attempts to exploit existing vulnerabilities.
c) Reports immediately any discovered vulnerability to the national CSIRT and the sectoral CSIRT for specialized analysis.
d) Keeps logs and documents all discovered vulnerabilities, including the origin of the attack, their type and status for audit, compliance and reference purposes future.

9.3 Identification of the incident

National CSIRT

a) Confirms vulnerabilities through the analysis of the identified weaknesses to
b) determine the level of risk for exploitation, especially if they are being actively exploited.
c) Assesses the risk based on the potential impact of vulnerabilities on national security and all critical and important infrastructures.
d) It is coordinated with international cybersecurity partners and intelligence sources to verify whether the identified vulnerability is part of a larger global threat.
e) Notifies the relevant sectoral CSIRT and the one at the operator regarding the identified vulnerabilities and any possible attempt to exploit them.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator regarding vulnerabilities reported by them and assesses their impact on the specific assets of the sector.
b) Coordination is carried out with the operators to identify the actors and indicators that exploit the vulnerabilities.
c) Provides detailed information on vulnerabilities to the national CSIRT for a comprehensive analysis.

CSIRT at the operator

a) Identifies and documents vulnerabilities, including details on their potential impact and the affected systems.
b) Reports the identified vulnerabilities to the national and sectoral CSIRT, providing all relevant data and the initial analysis.
c) It analyzes the internal traffic to identify IPs that attempt or exploit vulnerabilities for malicious purposes, classifying them as indicators of compromise.

d) Identifies the risk posed by vulnerabilities and their potential for exploitation.
e) Disseminates indicators of compromise with the national and sectoral CSIRT.

9.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national CSIRT, the sectoral CSIRT, and the CSIRT at the operator.
b) Provides updates and guidance from time to time to all relevant parties during the incident.
c) Coordinates actions for responding to the incident by following a unified approach to its mitigation.

Sectoral CSIRT

a) Utilizes preliminary information provided by operators and reports it directly to the national CSIRT.
b) It is directly coordinated with the operators to ensure that critical information regarding the incident is shared as quickly and accurately as possible in order to optimize the operational response.
c) Holds regular meetings with operators and other sectoral CSIRTs to harmonize actions and update defense strategies during the incident.

CSIRT at the operator

a) It is coordinated with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate protection measures.
b) They promptly inform the national and sectoral CSIRT of any significant developments related to the incident and share updated traffic logs for further analysis.

9.5 Registration

National CSIRT

a) Records the identified vulnerabilities in the national incident management system, ensuring that all collected data is registered.
b) It is coordinated with sectoral CSIRTs and the one near the operator to collect additional information and to ensure that the vulnerabilities are fully documented.

Sectoral CSIRT

a) It is coordinated with the CSIRT at the affected operator in order to register the incident on the incident management platform enabled by the national CSIRT.
b) It is coordinated with the operators of the infrastructures affected by the incident in order for them to be involved in the registration process.
c) Sends information and details regarding the identified vulnerabilities to CSIRT-the national authority to obtain the necessary recommendations for the elimination of weaknesses.

CSIRT at the operator

a) Documents the incident that exploits the operator's vulnerabilities and any findings based on detection and identification.
b) Records the incident in the incident management system according to the provisions in the regulation on the categorisation of cybersecurity incidents.

c) Reports the exploited vulnerabilities to the sectoral CSIRT and the national CSIRT with all relevant details.

9.6 Categorization of the Incident

National CSIRT

a) Categorizes the identified vulnerabilities based on their severity, scope, and potential impact on national security.
b) Classifies vulnerabilities according to their likelihood of exploitation, taking into consideration the affected systems and data.
c) Notifies the sectoral CSIRT and the operator's CSIRT of the categorization and provides guidance for the remediation of the vulnerabilities.

Sectoral CSIRT

a) Coordinates with the operator's CSIRT regarding the categorization of vulnerabilities within the sector, based on their impact and the data collected.
b) Assists in determining the specific nature of the vulnerabilities and their significance for sectoral operations.

CSIRT at the operator

a) Categorizes and reports exploited vulnerabilities, ensuring that all relevant information contributes to the proper categorization of the incident.
b) Follows established procedures for the management of vulnerabilities, based on their categorization.
c) Implements immediate measures to mitigate any exploitation of the identified vulnerabilities.

9.7 Incident Prioritization

National CSIRT

a) Assesses the significance of identified vulnerabilities based on their potential to compromise sensitive data or disrupt critical services.
b) Prioritizes the mitigation of vulnerabilities, focusing on those that pose the highest risk to national security.
c) Coordinates with sectoral CSIRTs and the operator's CSIRT to ensure that the most critical vulnerabilities are addressed promptly.

Sectoral CSIRT

a) Assesses the impact of identified vulnerabilities on the sector's critical services and prioritizes them as needed.
b) Coordinates with the operator's CSIRT on incident prioritization, ensuring that the necessary steps for incident management are followed.
c) Emphasizes the remediation of vulnerabilities affecting critical systems or services.

Operator's CSIRT

a) Assesses the impact of identified vulnerabilities on operational processes and prioritizes mitigation actions as needed.
b) Ensures that any vulnerability with the highest likelihood of exploitation and the greatest impact is addressed immediately to prevent potential compromise.

c) Reports prioritization decisions to the National CSIRT and the Sectoral CSIRT, accompanied by the necessary justifications.

9.8 Incident Analysis

National CSIRT

a) Conducts a comprehensive analysis of identified vulnerabilities, focusing on their origin, potential impact, and any patterns that may present broader risks.
b) Collaborates with international partners and intelligence agencies to gather additional information on vulnerabilities.
c) Shares the results of the analysis with the Sectoral CSIRT and the Operator's CSIRT to support faster incident response and future prevention.

Sectoral CSIRT

a) Assists the Operator's CSIRT in analyzing identified or reported vulnerabilities classified as cybersecurity incidents.
b) Assists the Operator's CSIRT in analyzing the key factors that led to the exploitation of vulnerabilities, as well as the indicators related to the incident.
c) Shares the analysis data with the National CSIRT.

Operator's CSIRT

a) Analyzes vulnerabilities at the operational level, focusing on their root cause and the way they were exploited.
b) Shares findings with the National CSIRT and the Sectoral CSIRT to contribute to a broader understanding of the situation.
c) Applies the findings to strengthen security measures and prevent similar vulnerabilities in the future.

9.9 Containment and Eradication

National CSIRT

a) Provides guidance and support for mitigating the impact of identified vulnerabilities.
b) Coordinates efforts with the Sectoral CSIRT and the Operator's CSIRT to ensure that cybersecurity resilience strategies are applied across all sectors.
c) Addresses any vulnerability that could be exploited, in order to prevent future exploitation attempts.

Sectoral CSIRT

a) Coordinates with the Operator's CSIRT to implement protective measures across the sector to prevent the exploitation of identified vulnerabilities.
b) Works closely with operators to ensure the effective mitigation of vulnerabilities.
c) Monitors the situation to ensure that all identified vulnerabilities have been addressed and that systems are fully secured.

Operator's CSIRT

a) Immediately addresses any identified vulnerability that could potentially be exploited.
b) Follows the mitigation and remediation procedures provided by the CSIRTs, ensuring that all necessary steps are undertaken.
c) Verifies the effectiveness of the remediation efforts and reports the status to the National

CSIRT and the Sectoral CSIRT.

9.10 Restoration of the services / data

National CSIRT

a) Assists in restoring any service affected by the exploitation of identified vulnerabilities back to normal operations.
b) Coordinates with the Sectoral CSIRT and the Operator's CSIRT to ensure that all affected services are fully recovered.
c) Monitors systems during and after recovery to ensure stability and to prevent future incidents.

Sectoral CSIRT

a) Assists the CSIRT at the operator in the recovery of specific sectoral services, by prioritizing the most critical and affected areas.
b) Assists the CSIRT with the operator in restoring services to full operational capacity.
c) Communicates the recovery status and any ongoing issues to the national CSIRT and interested stakeholders.

Operator's CSIRT

a) Restores services affected by identified vulnerabilities, following established recovery plans.
b) Takes measures for systems classified as "unsupported" (end-of-life), such as hardening or network micro-segmentation.
c) Verifies the integrity and functionality of recovered services before normal operations resume.
d) Reports on the progress of service recovery and any outstanding issues to the Sectoral CSIRT and the National CSIRT.

9.11 Post-Incident Activity

National CSIRT

a) Prepares a report detailing the identified vulnerabilities, incident response actions, and outcomes.
b) Reviews post-incident activities to extract lessons learned and identify areas requiring improvement for future vulnerability assessments.
c) Shares analysis reports with the Sectoral CSIRT and the Operator's CSIRT to enhance overall preparedness.

Sectoral CSIRT

a) Participates in the post-incident review process, contributing sector-specific knowledge and recommendations.
b) Participates in the post-incident review process, contributing sector-specific knowledge and recommendations.
c) Shares the lessons learned within the sector to improve future vulnerability assessments and response capabilities.

Operator's CSIRT

a) Prepares a final report providing detailed information on the impact of vulnerabilities, the response, and the recovery.

b) Participates in the lessons-learned process, identifying operational improvements and updating response plans.

c) Implements the recommendations to strengthen defenses and enhance future vulnerability assessments.

10) Cryptomining

Cryptocurrency mining is the process of using computers to verify and record transactions on a blockchain network to earn cryptocurrencies, a process known as cryptomining. Cryptomining is considered a cyber incident when carried out illegally or without the knowledge of the users of a system. This occurs when attackers install unauthorized programs to use the processing power of victims' computers to generate cryptocurrencies, such as Bitcoin, Etherium, etc. This type of attack, known as "cryptojacking", can slow down systems, consume energy resources, and damage devices. Key features include the covert use of CPU or GPU resources, the use of hidden codes in websites or applications, and high-power consumption, without the consent of the user.

10.1 Preparation

National CSIRT

a) Develops policies and procedures for detecting and responding to threats such as cryptocurrency mining, including unauthorized cryptomining and cryptojacking.

b) Implements advanced security controls, using anomaly detection systems and behavioral analysis tools, to identify cryptomining activities.

c) Conducts regular training for CSIRT analysts on the latest cryptomining techniques, tools, and trends in cryptocurrency mining.

d) Collaborates with international cybersecurity organizations to stay informed on the latest cryptomining threats.

e) Determines who will be involved in incident response, roles, and responsibilities for addressing vulnerabilities.

Sectoral CSIRT

a) Provides sector-specific guidance on identifying and mitigating cryptomining threats, ensuring alignment with national strategies.

b) Implements tailored monitoring technologies and tools to detect abnormal CPU/GPU/RAM usage and other signs of cryptomining within the sector.

c) Trains sectoral CSIRT teams on recognizing cryptomining indicators and appropriate response protocols.

d) Create policies to allow only highly privileged users to download or execute files or scripts.

e) Regularly update security configurations for the sector to prevent unauthorized cryptomining activities.

CSIRT of the operator

a) Implements security measures to prevent cryptomining, including endpoint protection, regular patching, and system hardening.

b) Trains staff on the risks associated with cryptomining, including the impact on system performance and power consumption.

c) Regularly monitors system performance and resource usage to detect signs of unauthorized cryptomining.

d) Establishes protocols for the rapid escalation of cryptomining incidents to appropriate CSIRTs.

10.2 Detection

National CSIRT

a) Continuously monitors the national network for signs of cryptomining activity, such as unusual CPU/GPU/RAM usage or unexplained increases in power consumption.
b) Uses threat intelligence sources and behavioral analysis tools to identify cryptomining activity.
c) Collaborates with sectoral and operator CSIRTs to share any data discovered to raise awareness of cryptomining threats.

Sectoral CSIRT

a) Implements specific monitoring tools based on sector needs to detect cryptomining activities (abnormal use of computing resources or unusual network traffic).
b) Distributes detected cryptomining activities to the national CSIRT and other sectoral CSIRTs to coordinate the incident response process.
c) Assists the operator-based CSIRT in monitoring sector-specific systems and networks for signs of cryptomining, including unauthorized software installations or unusual system behavior.

CSIRT of the operator

a) Uses monitoring tools on end-systems to detect unauthorized cryptomining software or abnormal resource consumption.
b) Monitors system behavior for CPU consumption above normal rates. The operator may use the commands **sudo top (*Linux*) or *Task Manager*** (***Windows*)** for the detection of activities that affect CPU load.
c) Check RAM usage, and processes that consume a lot of memory via commands **sudo free -h (Linux)** and via **Task Manager > Performance (Windows)**
d) Check space on disk through **This PC** (**Windows**) and **sudo df -h** (**Linux)**
e) Check bandwith if there is increased traffic on your network via monitoring programs
f) Monitors for pop-up ads outside the browser, redirection to harmful websites or installation of add-ons without the user's approval.
g) Immediately reports any detected cryptomining activity to the national and sectoral CSIRT
h) Stores logs and data related to detected cryptomining activities for further analysis and response.

10.3 Identification of the incident

National CSIRT

a) Confirms cryptomining activity as a cybersecurity incident through analysis of collected data and system behavior.
b) Identifies the scope and potential impact of cryptomining activity on national security and all critical and important infrastructures.
c) Notifies the relevant sectoral and operator-based CSIRTs about the identified cryptomining activity and its potential implications.

Sectoral CSIRT

a) Coordinates with the operator-based CSIRTs on the cryptomining activity reported by them and assesses its impact on sector-specific assets.
b) Coordinates with operators to determine the extent of cryptomining activity within the sector.
c) Provides detailed information about the incident to the national CSIRT for further analysis.

CSIRT of the operator

a) Identifies and makes the report for the cryptomining activity, including the technique, source, and potential targets.
b) Identifies the indicators**: IP, domain, hashes** of malicious files.
c) Reports the incident to the national and sectoral CSIRT, providing all relevant evidence and initial analysis.

10.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national CSIRT, the sectoral CSIRT and the CSIRT near the operators.
b) Provides updates and guidance from time to time to all relevant parties during the incident.
c) Coordinates the response to the incident by following a unified approach to its mitigation.

Sectoral CSIRT

a) Utilize the preliminary information provided by the operators and duly report it to the national CSIRT.
b) Coordinates directly with the operators to ensure that critical information about the incident is shared in a timely and accurate manner to optimize the operational response.
c) Holds regular meetings with the operators and other sectoral CSIRTs to harmonize actions and update protection strategies during the incident.

CSIRT at the operator

a) Coordinates with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate protective measures.
b) Informs the national and sectoral CSIRT in real time of any significant developments related to the incident and shares updated traffic logs for further analysis.

10.5 Registration

National CSIRT

a) Records the incident in the incident management platform and ensures that affected operators are involved in this process by assisting with additional details.
b) Coordinates with the sectoral and operator-based CSIRT to gather additional information and ensure that the incident is fully documented.

Sectoral CSIRT

a) Coordinates with the operator-based CSIRT affected by the incident to register the crypto-mining incident within the incident management platform, ensuring that all collected data is recorded.
b) Coordinates with the operator-based CSIRT to ensure that all affected operators are

involved in the registration process.

c) Sends the collected information and incident details to the national CSIRT to centralize the information.

CSIRT at the operator

a) Documents the cryptomining incident and any initial findings based on the collected data.
b) Ensures proper recording in the incident management system as defined in the regulation on the categorization of cybersecurity incidents.
c) Reports the incident to the sectoral and national CSIRT with all relevant details.

10.6 Categorization of the incident

National CSIRT

a) Categorizes cryptomining activity based on its nature, scope, and potential impact on national security.
b) Classifies the incident according to its severity, taking into account the potential damage to system performance and energy consumption.
c) Notifies the sectoral and operator CSIRT of the categorization and provides guidance on appropriate response actions.

Sectoral CSIRT

a) Coordinates with the operator CSIRT regarding the categorization of the cryptomining incident within the sector, based on its impact and the data collected.
b) Assists in determining the specific nature of the cryptomining and its significance to sectoral operations.

CSIRT at the operator

a) Categorizes and reports the cryptomining incident, ensuring that all available information assists in the categorization of the incident.
b) Follows established procedures for incident management based on its categorization.
c) Implement immediate measures to mitigate any harm caused by cryptomining activity.

10.7 Prioritization of the incident

National CSIRT

a) Assesses the impact of cryptomining activity based on its potential to increase infrastructure costs (high electricity consumption), disrupt critical services, or compromise system performance.
b) Prioritizes incident response, giving priority to incidents that could lead to significant operational disruption.
c) Coordinates with the sectoral and operator-based CSIRTs to ensure that the most critical incidents are handled expeditiously.

Sectoral CSIRT

a) Assesses the impact of cryptomining activity on sectoral critical services and prioritizes as necessary.
b) Coordinates with the operator-based CSIRT on prioritization, in order to synchronize incident response.
c) Assists the operator-based CSIRT in order to mitigate the most imminent and severe threats

identified through the cryptomining incident.

CSIRT at the operator

a) Assesses the impact of cryptomining activity on operational processes and prioritizes response actions as necessary.
b) Ensures that any potential service disruption or performance degradation is managed and addressed promptly.
c) Reports prioritization decisions to the national and sectoral CSIRT, providing analysis and justification.

10.8 Analysis of the incident

National CSIRT

a) Conducts a thorough analysis of cryptomining activity, focusing on the source, method, and potential impact on national security.
b) Collaborates with international partners and intelligence agencies to gather additional information and details on cryptomining techniques.
c) Analyzes and disseminates indicators of compromise across all critical and important infrastructures.
d) Distributes the post-analysis report to the sectoral and operator-based CSIRT to assist in reducing response times and in efforts to prevent similar incidents in the future.Sectoral CSIRT
e) Assists the operator-based CSIRT in analyzing the incident using information collected from operator reports and threat intelligence platforms and looks for indicators of compromise across the sector, with the aim of avoiding the incident.
f) Analyzes how the system was compromised to be used for generating cryptocurrencies and suggests strategies for taking measures from the incident.
g) Share details from the analysis performed to operators and the national CSIRT to provide detailed information about the incident.

CSIRT at the operator

a) Analyzes cryptomining activity at an operational level, focusing on how it can affect critical systems and services.
    - E.g.: Devices start to operate more slowly than usual, because they use maximum computer resources. This leads to delays in executing commands and difficulty executing several programs in parallel.
    - Sudden increase in energy costs.
    - Monitor the CPU, if it works at 80-90% when you have not executed any program, it is an indication that your computer may be infected.
    - Devices infected with cryptocurrency generators tend to overheat as they use a lot of CPU, can reduce battery life, and in specific cases can damage devices.
    - Pop-up ads appear outside the browser, redirect to malicious websites, install plugins without user consent.
b) Share findings with CSIRTs to contribute to a broader understanding of the incident identified as cryptomining.
c) Analyze logs to find the entry point, and all indicators that affect the compromise of the system.
d) Implement findings to improve security measures and prevent similar cryptomining incidents.

10.9 Containment and Eradication

National CSIRT

a) Provides guidance and support to mitigate the impact of identified cryptomining activities.
b) Coordinates efforts with the sectoral and operator CSIRT to ensure that cyber resilience strategies are implemented across sectors.
c) Assists information infrastructure operators in the process of removing all indicators of cryptomining activity.

Sectoral CSIRT

a) Assists the operator CSIRT in taking preventive measures across the sector to avoid further cryptomining activities.
b) Coordinates with operators to ensure the effective elimination of cryptomining software or scripts and to restore affected systems.
c) Monitors the situation to ensure that all identified indicators are addressed and the incident is fully resolved.

CSIRT at the operator

a) Isolates affected systems and the network to which these systems communicate.
b) Follow the procedures for eliminating indicators of compromise provided by the national and sectoral CSIRTs, ensuring that all necessary steps are taken.
c) Block all indicators on protective devices and continuously monitor traffic for the presence of these indicators on other systems.
    i. It is important to isolate the file that generates the cryptocurrencies, so that it does not spread on the network. For this, you should perform periodic scans of the devices.
    ii. Update your antivirus and scan the entire device to identify and delete the file.
    iii. Some cryptocurrencies generators operate in the browser and place scripts in the cache or cookies. You should delete browser data, images, files and cookies.
    iv. Reset all browser configurations and manually install only the plugins that you need.
    v. Temporarily disconnect from the internet to interrupt communication.
    vi. Use only trusted antiviruses.
    vii. Activate and configure a firewall to block unauthorized access.
    viii. Avoid untrusted links, download programs only from trusted sites, do not download attachments from unknown senders and always check the URL before clicking.
d) Verify the effectiveness of the measures taken and report the status to the CSIRTs.

10.10 Data and Service Restore

National CSIRT

a) Assists in restoring any service affected by cryptomining activity to normal operations.
b) Coordinates with sectoral and operator-based CSIRTs to ensure that all affected services are fully recovered.
c) Monitors systems during and after recovery to ensure stability and prevent future incidents.

Sectoral CSIRT

a) Assists operator-based CSIRT in recovering sectoral services, prioritizing the most critical and affected services or systems.

b) Supports operator-based CSIRT in restoring services to full operational capacity.
c) Communicates the recovery status and any ongoing issues to the national CSIRT and interested stakeholders. Operator-based CSIRT

CSIRT at the operator

a) Initiates the recovery process for services affected by cryptomining activity, following established recovery plans:
    i. Using antivirus products that protect the system from cryptocurrency mining and keep them updated.
    ii. Checks websites for cryptocurrency mining codes, as this can damage their reputation when customers become victims. To this end, website administrators should regularly check for suspicious changes to the website or any changes to the server.
    iii. ***Disabling JavaScript*** when opening suspicious or unknown websites.
    iv. Disable macros in Microsoft Word unless necessary.
    v. Use of updated versions of web browsers.
    vi. Stay up to date with cryptocurrency mining news, trends and threats, to be able to identify them in advance.
b) Verify the integrity and functionality of restored services before resuming normal operations.
c) Reports recovery progress and any challenges to the national and sectoral CSIRT for further assistance.

10.11 Post-incident activity

National CSIRT

a) Prepares a detailed report on the cryptomining incident, response actions, and results.
b) Reviews post-incident activities to learn lessons and identify areas for improvement from preparation to restoration of services and data.
c) Distributes analysis reports to sectoral and operator-based CSIRs to increase overall preparedness.

Sectoral CSIRT

a) Prepares a sector-specific report describing the cryptomining incident, response actions, and recovery efforts.
b) Participates in the post-incident review process, contributing sector-specific knowledge and recommendations.
c) Shares lessons learned within the sector to improve detection and response time to similar incidents in the future.

CSIRT at the operator

a) Drafts a final report providing detailed information on the impact of the cryptomining incident on the operator's systems and operations, response, and recovery.
b) Participates in the lessons learned process, identifying operational improvements and updating response plans.
c) Implements recommendations to strengthen defenses and improve future detection of cryptomining activities.

11) Data breach

A data breach is a cyber incident in which sensitive information has been compromised or disclosed without proper authorization.

In this situation, an attacker or a group of attackers has gained unlawful access to the systems or in the database of an infrastructure and has managed to copy, transfer, or publish the stolen information.

This category of incident affects personal data, financial data, and the integrity of an organization, and also requires an immediate response to prevent further damage and to identify the source and consequences of the data breach.

11.1 Preparation

National CSIRT

a) Drafts and maintains policies and procedures for detecting and responding to data leakage incidents.
b) Use intelligent platforms that assist in identifying data breaches for all critical and important information infrastructures in national networks.
c) Regularly trains CSIR analysts on identifying information gathering techniques
d) data (*exfiltration*), including the latest methods used by malicious actors.
e) Ensures that the means and systems for detecting and preventing data exfiltration (DLP, IDS/IPS) are implemented and functional at the national level.
f) Cooperates with international cybersecurity organisations to stay informed about new exfiltration threats and best practices for detecting and protecting against such attacks.
g) Determines the persons who will manage the incident and defines their roles and responsibilities.

Sectoral CSIRT

a) Provides guidance to the sector for protection against data exfiltration, ensuring compliance with national strategies.
b) It is coordinated with the CSIRT at the operator with the aim of using monitoring tools such as (DLP/IDS/IPS) adapted to detect unusual data transfers, unauthorized access, and potential exfiltration activities.
c) Trains sectoral CSIRT teams on recognizing the signs of data exfiltration and the steps to be taken for incident response.
d) Identifies and secures the sector's most critical assets, which may be targeted for data leakage.
e) Coordination is carried out with the operators for the regular updating of the security configurations for the protection devices (firewall) regarding the latest threats related to data acquisition.

CSIRT at the operator

a) Implements strong access controls, encryption, and deploys protective systems such as DLP to prevent unauthorized data exfiltration.
b) Trains staff on the risks related to data exfiltration, including the importance of compliance with data security policies.
c) Regularly monitors data transfers and network traffic to detect unusual activities that may indicate exfiltration attempts.
d) Applies policies and procedures for:
    i. User privileges in accessing data.

    ii. Encryption of sensitive data.
    iii. The secure transfer of data.

e) Keeps backup copies of critical data to restore services in case of a data breach incident.

11.2 Detection

National CSIRT

a) Continuously monitors national networks for signs of data exfiltration, such as large or unusual data transfers, unauthorized access, or the use of non-standard communication channels.
b) Use intelligence sources for threats and behavioral analysis tools to identify possible exfiltration activities.

Sectoral CSIRT

a) It is coordinated with the CSIRT at the operator with the aim of using sector-specific monitoring tools to detect exfiltration activities, such as data flows or unauthorized access to sensitive information.
b) Shares identified exfiltration activities with the national CSIRT and other sectoral CSIRTs for coordinated response efforts.
c) Assists the CSIRT at the operator in monitoring systems and networks specific to the sector for signs of data leakage, including unauthorized installations of software or unusual system behavior.

CSIRT at the operator

a) Use tools to monitor endpoints and the network to detect unauthorized data transfers or suspicious activities that may indicate exfiltration.
b) Implements and uses **YARA Rules** to detect suspicious files that connect communications with malicious actors and lead to data breaches.
c) Monitors the actions of insider persons with access to critical data, by checked for unusual behavior, such as:
    i. Transfer of data to external devices (USB, removable disks).
    ii. Accessing data outside working hours or from unusual locations.
    iii. Changing user privileges without proper authorization.
d) Immediately reports any detected exfiltration activity to the national CSIRT and the sectoral CSIRT.
e) Retain the logs and data related to the detected exfiltration activities for analysis and incident response.

11.3 Incident identification

National CSIRT

a) Confirms the presence of a data leak through in-depth analysis, utilizing national intelligence sources.
b) Identifies the scope and possible impact of exfiltration of the of data in critical and important infrastructures throughout the country.
c) Notifies the sectoral CSIRT and the one at the operator about the data breach incident and the possible consequences.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator regarding the reporting of the data leakage incident made by the operators and assesses its impact on the assets of the sector.
b) It is coordinated with the operators to determine the amount of data that has been leaked within the sector.
c) Provides detailed information about the incident to the CSIRT-national level for an in-depth analysis.

CSIRT at the operator

a) Identifies unusual activities by insiders including, but not limited to:
   i. The large-scale transfer of data to mobile devices (USB, external drives) or cloud platforms.
   ii. Accessing data outside of working hours or from unusual locations.
   iii. The creation or modification of user privileges without documented authorization.
b) For any unusual activity detected, the operator must initiate an internal investigation to identify the possible source of the leakage and implement immediate measures to prevent further exfiltration.
c) Identifies and documents the exfiltration activity, including the method, source, and possible targets.
d) Identifies unusual activities from external sources including, but not limited to:
   i. Unusual traffic on the network, especially towards unknown IPs or suspicious domains.
   ii. Accessing internal resources from external IP addresses at unusual times.
   iii. Attempts to transfer data to external destinations without authorization.
e) Reports the incident to the national CSIRT and it **sectoral, by** provided all relevant data and the initial analysis.
f) Verifies whether the leak occurred through different channels (email, cloud, etc.) and reports to the national and sectoral CSIRT with detailed information.
g) Identifies the purpose of the exfiltration activity and its potential impact on operations.

11.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national CSIRT, the sectoral CSIRT, and the CSIRT at the operator.
b) Provides updates and guidance from time to time to all relevant parties during the incident.
c) Regularly notifies the CSIRT at the operator regarding data breaches identified through intelligent systems and in-depth research *dark web.*
d) Coordinates actions in response to the incident by following a unified approach to its mitigation.

Sectoral CSIRT

a) Utilizes the preliminary information provided by the operators and reports it directly to the national CSIRT.
b) It is coordinated directly with the operators to ensure that critical information regarding
c) The incident should be separated as quickly and accurately as possible in order to optimize the operational response.
d) Holds regular meetings with operators and other sectoral CSIRTs to harmonize actions and update defense strategies during the incident.

CSIRT at the operator

a) Coordinates with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate response measures.
b) They inform the national and sectoral CSIRT in real time about any important development related to the incident and share the updated traffic logs for further analysis.

11.5 Registration

National CSIRT

a) Registers the incident in the incident management platform, along with the details of
b) data breach.
c) It is coordinated with CSIRT-the sectoral one and the one at the operator in order to collect the necessary information and to ensure that the incident is fully documented.

Sectoral CSIRT

a) It is coordinated with the CSIRT at the operator affected by the incident for the purpose of registering the incident on the management platform enabled by the national CSIRT and ensures that the affected operators are included in this process by assisting with additional details.
b) Sends the collected information to the national CSIRT in order to centralize the information.

CSIRT near the operator

a) Documents the exfiltration incident and any initial findings based on the data collected.
b) Ensures the proper registration in the incident management system according to the provisions of the regulation on the categorisation of cybersecurity incidents.
c) Reports the incident to the national CSIRT and the sectoral CSIRT with all relevant details.

11.6 Categorisation of the Incident Incident categorisation

National CSIRT

a) Categorizes the incident as a "data breach" based on the threat analysis and the type of compromised data.
b) Classifies the incident according to its severity and its impact on national security, citizens' privacy, and the functionality of critical infrastructure.
c) Notifies the sectoral CSIRT and the one at the operator’s for the categorization and provides the necessary recommendations for appropriate response actions.

Sectoral CSIRT

a) It is coordinated with the CSIRT at the operator regarding the categorization of the incident and communicates it within the respective sector.
b) Ensures that operators follow the established procedures for managing data breaches
c) data.
d) It helps in determining the exact nature of the incident and the compromised data.

CSIRT at the operator

a) Categorizes and reports the incident and ensures that all information assists in its categorization.
b) Follows the established procedures for incident management based on its categorization.
c) Implements immediate measures to mitigate the impact of the data breach.

11.7 Prioritization of the incident

National CSIRT

a) Assesses the significance of the leaked information based on its potential impact on the national infrastructure.
b) Prioritizes incident response, focusing on those cases that have a high potential to cause damage to critical systems or services.
c) It is coordinated with CSIRT-at the sectoral level and at the operator, to ensure that the most critical incidents are handled promptly.

Sectoral CSIRT

a) Assesses the impact of the activity on the sector's critical services and prioritizes as necessary.
b) Coordinates with the CSIRT at the operator for the prioritisation of the incident, ensuring appropriate coordination for the response to the data breach.
c) Assists the CSIRT at the operator with the aim of mitigating the highest impact threats based on the assessment of critical services.

CSIRT at the operator

a) Assesses the impact of the data breach on operational services and prioritises response actions according to its risk level.
b) Ensures that any possible interruption of services is managed and addressed immediately.
c) Reports prioritization decisions to the national CSIRT and the sectoral CSIRT, based on accurate analyses and reasoning.

11.8 Incident Analysis

National CSIRT

a) Performs forensic analysis to understand the origin, method of execution, and impact of the data breach.
b) Cooperates with international partners and intelligence agencies to gather more information on the techniques and tools used for data exfiltration.
c) Shares the results of the analysis with CSIRT-sectoral one and that at the operator assisted in preventing similar incidents in the future.

Sectoral CSIRT

a) Assists the CSIRT at the operator in analyzing the exfiltration activity, utilizing the information collected from intelligent threat platforms or information made available by the operators.
b) Assists the CSIRT at the operator in identifying the exploited vulnerabilities that led to the data breach and suggests strategies to mitigate the impact.
c) Ensures the distribution of the analysis report to the national CSIRT to clarify the situation.

CSIRT at the operator

a) Analyzes exfiltration activity at the operational level, focusing on how it can impact critical systems and services.
b) Collects and analyzes logs to trace suspicious activities and identifies the methods used for data exfiltration.

c) Analyzes the logs from critical systems and network devices for signs of compromise, including:
   i. Attempts to access data without authorization;
   ii. Processes that create hidden connections to unknown IPs;
   iii. Modification of data or copying of sensitive files;

d) Analyzes for suspicious processes in the system to identify possible applications used for data exfiltration

e) Shares the findings with CSIRT-the sectoral and national one to contribute to a broader understanding of the exfiltration incident.

f) Utilises the findings to improve security measures and to prevent further attempts at exfiltration.

11.9 Containment and Eradication

National CSIRT

a) Provides guidance and support for mitigating the impact of activities identified as resulting in data leakage.

b) Coordinates the response with CSIRT-the sectoral one and that with the operator to ensure that the cybersecurity resilience strategies are implemented by all sectors.

c) Addresses any vulnerability exploited by the exfiltration activity, ensuring the reduction and prevention of similar cases in the future.

d) Distributes to the CSIRT at the operators the indicators of compromise (IP/files/url) derived from the analysis of data collected by the operators and the sectoral CSIRT.

Sectoral CSIRT

a) Coordinates with the CSIRT at the operator with the aim of implementing protective measures throughout the sector to prevent further exfiltration activities.

b) Works closely with operators to ensure the eradication of the threat from the systems and to restored the affected systems.

c) Monitors the situation to ensure that all identified weaknesses have been addressed and the incident has been fully resolved.

CSIRT at the operator

a) Isolate all systems based on prioritization, in order to prevent further data exfiltration.

b) Deactivates users who are engaging in suspicious activity.

c) Blocks communications with malicious IPs identified through analyses and reported by CSIRT the national one and the sectoral one.

d) Follows the procedures made available by the CSIRT-the national and the sectoral one for the deletion of compromise indicators, or the deletion of the system.

e) Verifies that the activity is no longer present in the system and reports the status to the CSIRT national and sectoral.

11.10 Restoration of services / data

National CSIRT

a) Assists in the restoration of any service affected by the exfiltration activity to normal operations.

b) It is coordinated with CSIRT-sectoral one and that with the operator to ensure that all affected services are fully recovered.

c) Monitors systems during and after recovery to ensure that malicious activity has been eradicated and to prevent its recurrence in the future.

Sectoral CSIRT

a) Assists in the restoration of sectoral services, prioritizing the most critical affected services or systems.
b) Supports operators in restoring services to full operational capacity.
c) Communicates the recovery status and any ongoing issues to CSIRT-the national level and the stakeholders.

CSIRT at the operator

a) Restore the services affected by the exfiltration activity, following the established recovery plans.
b) Reactivates deactivated users by first changing their password.
c) Verifies the integrity and functionality of the recovered services before resuming normal operations.
d) Reports the progress of recovery and any issues encountered during the restoration of services to the national and sectoral CSIRT for further assistance.

11.11 Post-incident activity

National CSIRT

a) Draft a comprehensive report detailing the exfiltration incident, response actions, and outcomes.
b) Reviews activities after the incident to draw lessons and identify areas that need improvement in order to avoid similar cases of data breaches.
c) Distributes the final report to the sectoral CSIRT and to the one at the operator increased overall preparedness.

Sectoral CSIRT

a) Prepares a report for the specific sector and describes the impact of the exfiltration incident, the response actions, and the recovery efforts.
b) Participates in the post-incident review process, contributing sector-specific knowledge and recommendations.
c) Disseminates lessons learned within the sector to improve future detection and response capabilities.

CSIRT at the operator

a) Drafts a final report providing detailed information on the impact of the exfiltration incident, the response, and the recovery.
b) Participates in the lessons learned process, by identifying operational improvements and updating response plans.
c) Implements the recommendations to strengthen protection and improve future detection of exfiltration activities.

12) Others

Others include information security incidents that do not fall under the previously mentioned categories. This may cover special or unusual incidents such as system failures, incidents caused by natural disasters, incidents related to third parties, etc.

12.1 Preparation

National CSIRT

a) Drafts policies and guidelines for managing unusual incidents, including system failures or chain incidents resulting from third-party compromise.
b) Ensures that all sectoral CSIRTs and CSIRTs at the operator maintain a detailed business continuity plan for cases of system failure within their infrastructure.
c) Organizes training and exercises on "Other" incident scenarios to enhance response and recovery time for service restoration.
d) Designates the personnel responsible for managing the incident and defines their roles and responsibilities.

Sectoral CSIRT

a) Drafts procedures for monitoring the performance of third-party services and critical systems within the sector.
b) Coordinates with the CSIRT at the operator to implement systems that provide alerts for potential system failures and unusual events.
c) Coordinates with operators to establish a response plan aimed at minimizing the impact of incidents, such as third-party service disruptions or system malfunctions.

CSIRT at the operator

a) Develops and maintains an up-to-date inventory of hardware and software components dependent on third parties.
b) Prepares a recovery plan for system failures and incidents related to external providers.
c) Collaborates and establishes agreements with third-party suppliers to ensure rapid response in case of incidents.

12.2 Detection

National CSIRT

a) Utilizes intelligent systems to notify of service outages at third-party companies operating at the national level.
b) Analyzes reports from sectoral CSIRTs and CSIRTs at the operator to determine if the incident represents a broader national-level issue.

Sectoral CSIRT

a) Assists the CSIRT at the operator in monitoring the performance of critical services and
b) applications to detect early signs of system failure.
c) Assists the CSIRT at the operator in deploying monitoring tools to identify when third-party services become unavailable or operate below expected standards.

CSIRT at the operator

a) Monitors systems and applications to detect any unexpected failures or errors that could impact infrastructure operations.
b) Regularly reviews third-party supplier relations to identify notifications of outages or potential problems.

c) Configures alerts to detect hardware failures and other issues affecting normal operations.

12.3 Incident Identification

National CSIRT

a) Analyzes system data and reports from sectoral CSIRTs and CSIRTs at the operator to determine the nature of the incident and potential impact on critical infrastructures.
b) Assesses whether the problem is related to internal system failures, third-party malfunction, or incidents caused by natural disasters.

Sectoral CSIRT

a) Reviews and verifies reports of system failures or third-party incidents from operators
b) Analyzes system logs to identify causes and impact of the incident within the sector.
c) Collects data from operators to assess how the incident's impact may propagate across the sector.

CSIRT at the operator

a) Identifies the source of the problem, such as hardware or software errors, or third-party supplier disruptions.
b) Analyzes system logs and third-party reports to understand the incident's root causes.
c) Verifies the functionality of equipment and systems to identify affected components.

12.4 Communication and Coordination

National CSIRT

a) Establishes communication channels between the national, sectoral, and operator-level CSIRTs.
Provides timely updates and guidance to all relevant parties during the incident.
b) Coordinates actions for incident response following a unified approach for mitigation.

Sectoral CSIRT

a) Uses preliminary information provided by operators and reports it to the national CSIRT.
b) Coordinates directly with operators to ensure that critical incident information is shared promptly and accurately, optimizing operational response.
c) Holds regular meetings with operators and other sectoral CSIRTs to align actions and update defensive strategies during the incident.

CSIRT at the operator

a) Coordinates with other departments within the infrastructure, ensuring that all relevant parties are aware of the situation and take appropriate response measures.
b) Provides real-time updates to the national and sectoral CSIRTs regarding any significant developments and shares updated traffic logs for further analysis.

12.5 Incident Registration

National CSIRT

a) Registers the incident in the incident management platform along with all relevant details.
b) Coordinates with sectoral CSIRTs and CSIRTs at the operator to gather necessary

information and ensure full documentation of the incident.

Sectoral CSIRT

a) Assists the CSIRT at the operator in registering the incident in the sector's incident management platform and ensures that affected operators are included in the process by providing additional details.
b) Transmits the collected information to the national CSIRT for centralization.

CSIRT at the operator

a) Documents the exfiltration incident and any initial findings based on collected data.
b) Registers the incident in the incident management system according to cybersecurity incident categorization regulations.
c) Reports the incident to the national and sectoral CSIRTs with all relevant details.

12.6 Incident Categorization

National CSIRT

a) Categorizes the incident based on its nature and impact, such as system failure, third-party incident or natural disaster.
b) Assesses the potential impact on national infrastructure and assigns a risk level. Updates the incident register with the defined category and risk rating.

Sectoral CSIRT

a) Assists the CSIRT at the operator in categorizing the incident and communicates this within the relevant sector.
b) Ensures operators follow established procedures for managing data breaches.
c) Supports in determining the exact nature of the incident and the systems affected.

CSIRT at the operator

a) Categorizes and reports the incident, ensuring that all information supports proper classification.
b) Assesses the impact on operational processes and infrastructure data security.
c) Follows established procedures for incident management based on classification.
d) Implements immediate measures to mitigate the impact of data breaches.

12.7 Incident Prioritization

National CSIRT

a) Evaluates the importance of affected systems and prioritizes based on potential national
b) infrastructure impact.
c) Prioritizes incident response, focusing on cases where service disruption has a high impact on infrastructure reputation.
d) Coordinates with sectoral CSIRTs and CSIRTs at the operator to ensure that the most critical service incidents are addressed quickly.

Sectoral CSIRT

a) Evaluates the impact on critical sector services and prioritizes accordingly.
b) Coordinates with CSIRTs at the operator to ensure synchronized response to data breaches.
c) Assists CSIRTs at the operator in mitigating the highest-impact threats based on the

criticality of services.

CSIRT at the operator

a) Prioritizes the incident based on its impact on business operations and client services.
b) Allocates necessary resources to resolve the incident, starting with the most sensitive systems/services.
c) Notifies the national and sectoral CSIRTs regarding prioritization levels and response priorities.

12.8 Incident Analysis

National CSIRT

a) Analyzes all data and reports collected from sectoral CSIRTs and CSIRTs at the operator to understand the root causes of the incident.
b) Collaborates with international partners to adopt and apply best practices for handling the incident at a national level.

Sectoral CSIRT

a) Analyzes operator-provided data on the incident, focusing on key factors that led to system
b) failures, service outages, or natural disaster impacts.
c) Reviews external factors such as power supply issues, room temperature, or physical equipment damage.
d) Assists operators in identifying weaknesses in operational and technical processes that enabled the incident and analyzes its effects within the sector.
e) Shares analytical information and recommendations with sector operators to accelerate service restoration.
f) Informs the national CSIRT of any significant findings during analysis.

CSIRT at the operator

a) Analyzes the incident at the operational level, identifying the root cause and circumstances leading to system failure or service outage.
b) Assesses the impact on daily operations and long-term effects, and identifies mitigation measures.
c) Shares full findings with the national and sectoral CSIRTs to enable a synchronized and faster response.
d) Implements necessary improvements to prevent similar incidents in the future and strengthens disaster response planning.

12.9 Containment and Eradication

National CSIRT

a) Coordinates with sectoral CSIRTs and CSIRTs at the operator to isolate the source of the incident, particularly when originating from third parties.
b) Provides technical guidance for isolating affected systems and shutting down endangered services, considering national operational impacts.
c) Takes measures to block further access from internal or external sources that could cause recurrence.
d) Prepares a report on containment measures and shares it with sectoral and operator-level CSIRTs to support eradication and recovery efforts.

Sectoral CSIRT

a) Coordinates with CSIRTs at the operator to implement immediate measures for isolating affected systems within the sector, disconnecting from third parties until resolution.
b) Provides detailed guidance to operators for properly isolating affected devices, systems, and networks.
c) Collaborates with operators to identify components requiring full eradication to eliminate the incident and restore operations.
d) Shares results of the containment and eradication phase with the national CSIRT to ensure coordinated and effective measures.

CSIRT at the operator

a) Conducts rapid isolation of affected systems to prevent further spread within internal infrastructure.
b) Suspends all affected services and ensures network and device isolation to mitigate additional risks.
c) Documents all containment and eradication measures and reports outcomes to the national and sectoral CSIRTs for knowledge sharing and future security improvements.

12.10 Service/Data Recovery

National CSIRT

a) Supports the restoration of any service affected by exfiltration to normal operations.
b) Coordinates with sectoral and operator-level CSIRTs to ensure full recovery of all affected services.
c) Monitors systems during and after restoration to ensure that malicious activity has been eliminated and to prevent recurrence.

Sectoral CSIRT

a) Assists in restoring sector-level services, prioritizing the most critical ones.
b) Supports operators in fully restoring operational service capacity.
c) Communicates recovery status and any ongoing issues to the national CSIRT and stakeholders.

CSIRT at the operator

a) Activates the Business Continuity Plan (BCP).
b) Activates backups for service restoration.
c) Verifies the integrity and functionality of restored services before resuming normal operations.
d) Reports recover progress and any arising issues to the national and sectoral CSIRTs for further support.

12.11 Post-Incident Activity

National CSIRT

a) Drafts a comprehensive report detailing the incident, response actions, and outcomes.
b) Reviews post-incident activities to identify lessons learned and highlight areas for improvement to avoid recurrence.
c) Shares the final report with sectoral and operator-level CSIRTs to enhance overall

preparedness.

Sectoral CSIRT

a) Prepares a sector-specific report describing the incident’s impact, response actions, and recovery efforts.
b) Assists the CSIRT at the operator in the post-incident review process, contributing sector-specific knowledge and recommendations.
c) Disseminates lessons learned across the sector to strengthen future detection and response capabilities.

CSIRT at the operator

a) Drafts a final report providing detailed information on the incident’s impact, response, and recovery.
b) Participates in lessons-learned exercises, identifying operational improvements and updating response plans.
c) Implements recommendations to strengthen defenses and improve detection of future similar incidents.