INTERNATIONAL STANDARD

ISO/IEC 27035-3

First edition
2020-09

Information technology — Information security incident management —

Part 3:
Guidelines for ICT incident response operations

Technologies de l'information — Gestion des incidents de sécurité de l'information —

Partie 3: Lignes directrices relatives aux opérations de réponse aux incidents TIC

Reference number
ISO/IEC 27035-3:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO 27035 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

An information security incident can involve ICT or not. For example, information that spreads unintentionally through the loss of paper documents can very well be a serious information security incident, which requires incident reporting, investigation, containment, corrective actions and management involvement. This type of incident management is often carried out, for example, by the Chief Information Security Officer (CISO) within the organization. Guidance on the management of such information security incidents can be found in ISO/IEC 27035-1. This document, however, only considers incident response operations for ICT-related incidents, and not for information security incidents related to paper documents or any other non-ICT incidents. Whenever the term "information security" is used in this document, it is done so in the context of ICT-related information security.

The organizational structures for information security vary depending on the size and business field of organizations. As various and numerous incidents occur and are increasing (such as network incidents, e.g. intrusions, data breaches and hacking), higher concerns about information security have been raised by organizations. A secure ICT environment set up to withstand various types of attacks (such as DoS, worms and viruses) with network security equipment such as firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) should be complemented with clear operating procedures for incident handling, along with well-defined reporting structures within the organization.

To ensure confidentiality, integrity and availability of information and to handle incidents efficiently, capabilities to conduct incident response operations is required. For this purpose, a computer security incident response team (CSIRT) should be established to perform tasks such as monitoring, detection, analysis and response activities for collected data or security events. These tasks may be assisted by artificial intelligence tools and techniques.

This document supports the controls of ISO/IEC 27001:2013, Annex A, related to incident management.

Not all steps in this document are applicable since it depends on the particular incident. For example, a smaller organization may not use all guidance in this document but can find it useful for organization of their ICT-related incident operations especially if operating their own ICT environment. It can also be useful for smaller organizations that have outsourced their IT operations to better understand the requirements and execution of incident operations that they should expect from their ICT supplier(s).

This document is particularly useful to organizations providing ICT services that involve interactions between organizations of incident operations in order to follow the same processes and terms.

This document also provides a better understanding on how incident operations relates to the users/customers in order to define when and how such interaction needs to take place, even if this is not specified.

Information technology — Information security incident management —

Part 3: **Guidelines for ICT incident response operations**

1 Scope

This document gives guidelines for information security incident response in ICT security operations. This document does this by firstly covering the operational aspects in ICT security operations from a people, processes and technology perspective. It then further focuses on information security incident response in ICT security operations including information security incident detection, reporting, triage, analysis, response, containment, eradication, recovery and conclusion.

This document is not concerned with non-ICT incident response operations such as loss of paper-based documents.

This document is based on the “Detection and reporting” phase, the “Assessment and decision” phase and the “Responses” phase of the “Information security incident management phases” model presented in ISO/IEC 27035-1:2016.

The principles given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the provisions given in this document according to their type, size and nature of business in relation to the information security risk situation.

This document is also applicable to external organizations providing information security incident management services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27035-1, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

ISO/IEC 27035-2, *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

ISO/IEC 27043, *Information technology — Security techniques — Incident investigation principles and processes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27037, ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27043 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
asset
anything that has value to an individual, an organization or a government

[SOURCE: ISO/IEC 27032:2012, 4.6]

3.2
computer security incident response team
CSIRT
team of security experts to support the handling of information security incidents

[SOURCE: ISO/IEC 27019:2017, 3.2]

3.3
investigation
systematic or formal process of inquiring into or researching, and examining facts or materials associated with a matter

Note 1 to entry: A similar definition can be found in ISO/IEC 27042:2015, 3.10.

[SOURCE: ISO/IEC 27050:2017, 3.17, modified — Note 1 to entry has been added.]

3.1.4
response
incident response
action taken to protect and restore the normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs

[SOURCE: ISO/IEC 27039:2015, 2.24]

4 Abbreviated terms

ASCII	American standard code for information interchange
CPU	central processing unit
DNS	domain name system or domain name service
DDoS	distributed denial of service
DoS	denial of service
ENISA	European Union agency for network and information security
FAT	file allocation table file system
FAT32	32-bit file allocation table file system
FIRST	forum of incident response and security teams
HPFS	high performance file system
HR	human resources
ICT	information and communication technology

IDS	intrusion detection system
IoC	indicators of compromise
IP	internet protocol
IPS	intrusion prevention system
ISP	internet service provider
IT	information technology
MD5	message digest 5 algorithm
NIST	national institute for standards and technology
NTFS	windows networking technology file system
OS	operating system
PoC	point of contact
SHA	secure hashing algorithm
SIEM	security information and event management system
URL	universal resource locator
WAF	web application firewall
XML	extended mark-up language

5 Overview

5.1 General

ISO/IEC 27035-1 covers the following five main phases for information security incident management:

- Plan and prepare;
- Detection and reporting;
- Assessment and decision;
- Responses;
- Lessons learnt.

ISO/IEC 27035-2 covers two of these five phases in detail, i.e. "Plan and prepare" and "Lessons learnt".

This document covers the remaining three phases in detail. These three remaining phases are collectively referred to as incident response operations, which are the focus in this document.

5.2 Structure of this document

The provisions in this document are based on the "Detection and reporting", "Assessment and decision" and "Responses" phases of the “Information security incident management phases” model presented in ISO/IEC 27035-1. Collectively, these phases are known as the incident response operation process.

The phases within the incident response operation process (which are "Detection and reporting", "Assessment and decision" and "Responses" as stipulated in ISO/IEC 27035-1) include the following:

- operations for incident identification;
- operations for incident assessment and qualification;
- operations for threat intelligence gathering;
- operations for incident containment, eradication and recovery;
- operations for incident analysis;
- operations for incident reporting.

The scope for incident response is defined in ISO/IEC 27035-1. Incident response operations should be seen as a business process that enables an organization to remain in business. Specifically, an incident response operation process is a collection of procedures aimed at identifying, responding to and investigating potential security incidents in a way that minimizes their impact and support rapid recovery.

ISO/IEC 27035-1 shows the five phases of information security incident management as Plan and prepare, Detection and reporting, Assessment and decision, Responses and Lessons learnt. As mentioned before, this document focuses on an incident response operation process. This process can be characterized by a lifecycle of incident response operations which is represented by the inner phases (detection, notification, triage, analysis, response, and reporting). These are represented in more detail in Figure 1.

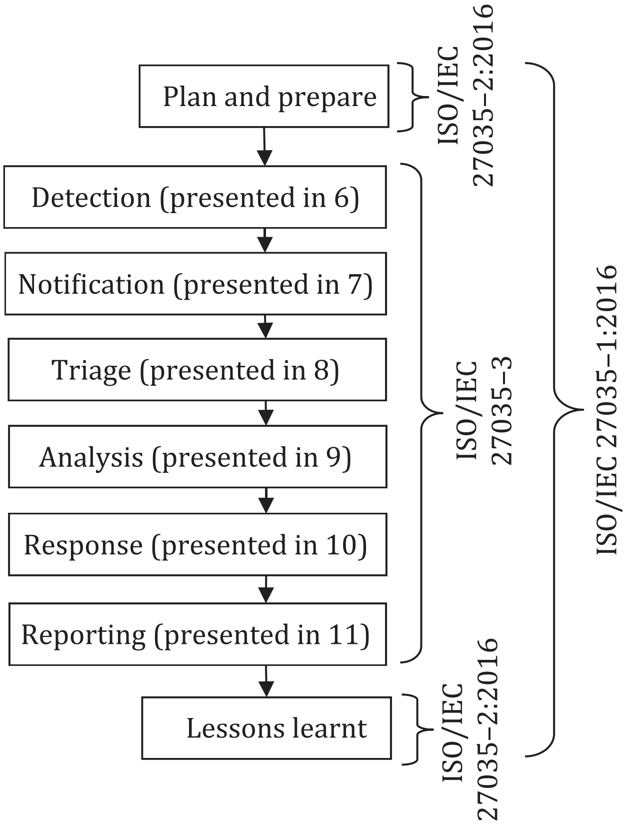
Plan and prepare
Detection (presented in 6)
Notification (presented in 7)
Triage (presented in 8)
Analysis (presented in 9)
Response (presented in 10)
Reporting (presented in 11)
Lessons learnt
ISO/IEC 27035–2:2016
ISO/IEC 27035–3
ISO/IEC 27035–2:2016
ISO/IEC 27035–1:2016

Figure 1 — Lifecycle of incident response operations

The lifecycle of incident response operations (detection, notification, triage, analysis, response, and reporting) can be mapped to the five phases of information security incident management of

ISO/IEC 27035-1 (Plan and prepare, Detection and reporting, Assessment and decision, Responses and Lessons learnt) as shown in Table 1.

Table 1 — Mapping of the five phases of information security incident management in ISO/IEC 27035-1 to the lifecycle of incident response operations in this document

Five phases of information security incident management in ISO/IEC 27035-1	Lifecycle of ICT incident response operations in this document
Plan and prepare	(None – covered in detail by ISO/IEC 27035–2)
Detection and reporting	— Detection (presented in Clause 7, which links to ISO/IEC 27035-1:2016, 5.3) — Notification (presented in Clause 8, which links to ISO/IEC 27035-1:2016, 5.3)
Assessment and decision	— Triage (presented in Clause 9, which links to ISO/IEC 27035-1:2016, 5.4) — Analysis (presented in Clause 10, which links to ISO/IEC 27035-1:2016, 5.4)
Responses	— Response (presented in Clause 11, which links to ISO/IEC 27035-1:2016, 5.5) — Reporting (presented in Clause 12, which links to ISO/IEC 27035-1:2016, 5.3)
Lessons learnt	(None – covered in detail by ISO/IEC 27035-2)

NOTE The notion of reporting appears only once in ISO/IEC 27035-1:2016, 5.3. However, during the entire lifecycle of incident response operations (as portrayed in this document), the notion of reporting appears twice: once in Clause 7 and once in Clause 11. However, both instances of reporting map to ISO/IEC 27035-1:2016, 5.3. To clarify, there are two distinct instances (occurrences) of reporting that take place during the entire lifecycle of incident response operations as portrayed in this document. The first occurrence of reporting involves the recording or registration of the fact that an incident has indeed occurred (as presented in Clause 7). The second occurrence of reporting involves the recording of the outcome of the entire lifecycle of incident response operations (as presented in Clause 11). In summary, the first occurrence reports to (notifies) a PoC that an incident has indeed occurred, while the second occurrence reports on the outcome of the entire lifecycle of incident response operations.

6 Common types of attacks

Incidents can happen in various ways and it is not practical to define all the incidents and prepare the response manual for each type of incident. However, there are common attack types/sources that an organization often encounter and should therefore be prepared to handle, such attacks efficiently. Criteria should be set for security incidents according to the importance (priority) of information and information systems, impact of each incident, damage scale, alarm ranking and its severity. See Annex A for examples of such criteria.

The following is a non-exhaustive list of common attack types/sources that can be used as the basis for defining incident handling procedures:

- external/removable media: an attack executed from removable media (e.g. flash drive, CD) or a peripheral device;
- attrition: an attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g. a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures);
- web: an attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware);

- e-mail: an attack executed via an email message or attachment (e.g. exploit code disguised as an attached document or a link to a malicious website in the body of an email message);
- supply chain interdiction: an antagonistic attack on hardware or software assets utilizing physical implants, Trojans or backdoors, by intercepting and modifying an asset in transit from the vendor or retailer;
- impersonation: an attack involving replacement of something benign with something malicious (e.g. spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation);
- improper usage: any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories (e.g. a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system);
- loss or theft of equipment: the loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token;
- other: an attack that does not fit into any of these categories.

NOTE See the NIST Computer Security Incident Handling Guide[1] for more incident classification guidelines and attack vectors.

An incident comprises one or multiple related information security events that can harm an organization's assets or compromise its operations, where an information security event comprise one or multiple occurrences indicating a possible breach or failure of information security controls.

7 Incident detection operations

7.1 Point of contact

Incident detection operations require that there be a point of contact (PoC) to receive information, an established methodology for the team to detect information security events. Detection is important because it starts the incident response operations.

The PoC is the organizational function or role serving as the coordinator or focal point of incident operation activities. An information security event is reported by the "User/Source" in some way, as shown in ISO/IEC 27035-1:2016, Figure 4. The main purpose of the PoC is to ensure that an event is reported as soon as possible to the organization so that the event can be handled efficiently. A critical success factor is that the PoC possesses the skills to determine whether an event indeed is an ICT-related event and that the PoC is able to describe the event.

An event should then be further handled by a PoC and then transferred into incident response operations. The organization of a PoC can be different depending on the size and structure of the organization as well as the nature of the business. This can affect how incident operations are informed of the event.

There are three different main scenarios for the PoC:

a) no formal PoC exists;

b) single PoC for all types of events irrespective of the number of geographic locations;

c) multiple PoCs depending on the nature of the event and geographic locations.

[1] This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products can be used if they are applicable.

Regardless of which of the above PoC situation exists, the incidents have specific operations which are covered in this document.

NOTE Information security events that exist, which are determined as incidents according to ISO/IEC 27035-1, can either be ICT-related or non–ICT-related. Examples of non–ICT-related information security events include lost paper document(s), a physical break-in to the organization's premises resulting in the theft of physical document(s), breach of policy or security rules, etc. This document focuses only on ICT-related incidents.

Examples of incidents or events that the PoC receives can be found in Annex A.

7.2 Monitoring and detection

Information security events can be detected internally by a person or by information security technologies such as an IDS, or can be reported from external sources of information. Information security events can be detected by various means and can be categorized into the following three means:

— technical:

  a) intrusion detection and prevention systems (IDPSs);

  b) endpoint security tools such as anti-virus software;

  c) security log analyzer tools or security information and event management systems (SIEMs);

— people: internal or external users, including non-IT or security-related staff, or customers;

— organizational:

  a) IT department, including network operations centre and security operations centre, IT help desk;

  b) managed service providers (including ISPs, telecommunication service providers, and suppliers);

  c) CSIRTs;

  d) other units and staff that may detect anomalies during their daily work;

  e) mass media (newspaper, television, etc.); and

  f) websites (public security information websites, websites by security researchers, defacement archive websites, etc.).

As the first step, the organization:

— monitors the security events in order to detect incidents; and/or

— receives a list of the security events from the monitoring site (or domain) of the organization and/or PoC.

As soon as the event is registered through detection and/or notification, the monitoring team verifies whether the case is a potential incident using the collected information. After verifying that the security event(s) is/are real, the monitoring team makes a decision on incident occurrence, and its initial severity such as incident type, the importance of the damaged system, alarm level, etc. (see Annex A). It performs the following tasks in order to monitor and detect an event:

a) monitoring:

  1) monitoring security events from the target organization continuously;

  2) monitoring by the console (e.g. security device does not support inter-operation);

  3) monitor public information for indicators of compromise and threat intelligence;

4) reinforce and/or alter rules set of the monitoring system while any intrusion is in progress;

b) detecting:

1) identify security events by collecting, analysing and qualifying the events;

2) performing incident correlation (also known as retrospective analysis) and adequate triage on the events mentioned above. initiate and perform case management. incident response playbooks may also be utilized.

7.3 Common ways detection is performed

7.3.1 Monitoring public sources to look for potential reports (and threats)

Monitoring public sources includes gathering information from public sources that is relevant to the organization or CSIRT work. This information is used to keep up to date with ongoing security-related activities, to provide information on new vulnerabilities, attack types, mitigation strategies and security tools, and to provide insight, perspective and context for ongoing activity. These services involve looking at available security resources such as mailing lists, web sites, articles or news reports that are available publicly for free or from a commercial service for a fee.

Staff performing technology watch functions can include actual CSIRT staff, network operations staff, other systems and network administrators, or even outsourced contractors. Information sought and passed on can include new vulnerabilities, new attack types and threats, new recommendations and solutions for preventing incidents, or general political, social or sector-related information that can have relevance to any ongoing or potential malicious activity.

The following are examples of proactive detection of network security incidents:

- client side honeypot (both high and low interaction);
- server side honeypot (both high and low interaction);
- sandbox;
- intrusion detection system (IDS)/intrusion prevention system (IPS):
- netflow;
- darknet (no interaction);
- passive DNS monitoring;
- antivirus;
- spamtrap;
- firewall;
- web application firewall (WAF);
- application logs.

Different threat feeds tend not to overlap so it is important to acquire one that is targeted to the business needs and type of ICT process being protected or informed by the threat feed[1]. The following are examples of thread feeds that organizations can subscribe to:

- DNS-BH Malware domain blocklist;
- MalwareURL;
- DShield;

- Google safe browsing alerts;
- Team Cymru;
- Shadowserver.

NOTE Also see the ENISA document on detection and the FIRST CSIRT Services Framework for more examples of proactive detection of network security incidents and thread feeds that organizations can subscribe to[2].

7.3.2 Validation of external source data

The following process steps are used to implement situational awareness.

- Identify the trust levels or trustworthiness of data sources. Ensure that data sourced is trusted.
- Identify information requirements. Requirements development.
    - Determine criteria for monitoring related to severity, relevancy and priority.
    - The trust levels or trustworthiness of data sources should be identified first and ensure that data sourced is trusted.
    - Train the public monitors and data collectors.
    - Establish PoC list of who to contact with different types of information.
- Determine sensors to be deployed and data to be collected or monitored.
    - Indicators of compromise (IoC) (i.e. IP addresses, email subject lines, etc.).
    - Techniques, tactics and procedures (TTPs) of attackers. Examples include methods of social engineering, malicious document execution (i.e. PDFs and GIFs).
    - Open source threat intelligence.
    - Subscription service threat intelligence.
    - Network performance data.
        - Bandwidth usage of network(s).
        - Flow records collection.
        - Full packet capture.
    - Host data (i.e. disk usage, software inventory/patch-level, event logs).
    - Application data (i.e. email spam filtered, DNS resolutions).
- Actively monitor key sensors.
- Actively monitor threat feeds.
- Actively monitor for reported vulnerabilities.
    - Subscribe to vendor and security related mailing lists.
    - Maintain a list of vendor advisory sites to be periodically reviewed.

[2] This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products can be used if they are applicable.

  - Proactively search for additional sites to monitor.

- Actively monitor for ongoing security incidents or suspicious activity, this feeds situational awareness.

  - Identify news, political, government, economic sites for review.

  - Identify security and incident response sites or team sites for review or subscriptions.

- Create procedures for notifying key personnel of information that is relevant.

  - Vulnerability reports that can have a high impact.

  - Widespread incidents.

  - Current events that may provide insight into ongoing events.

- Develop a knowledge management system to store information and allow it to be searchable.

7.3.3 Proactive detection

Proactive detection refers to devices, people and/or mechanisms that are actively searching for vulnerabilities that can potentially be security events. This may include searching for indicators of threat activity seen by others. Examples of proactive detection methods include, but are not limited to, the following:

- vulnerability scanning;

- proactive activities of hunting teams actively searching for events;

- log correlation;

- penetration testing;

- proactive network monitoring, which can include alerting, trend reporting and providing proactive updates to software/firmware;

- proactive detection using software systems like intrusion prevention systems.

7.3.4 Reactive methods

Reactive detection refers to devices, people and/or mechanisms that are not actively searching for incidents but that, in the course of their daily duties/responsibilities/tasks, produce some signal of a possible incident that should be reported to the CSIRT. Sources of reactive detection include, but are not limited to, the following:

- reports or alerts from users;

- rule-based alerts which are triggered by software systems such as intrusion detection systems, file integrity monitoring systems;

- reactive network monitoring using data mining utilities;

- complaints or suggestions from users of the products or applications, which can include the business logic vulnerabilities, the hijacking of the network traffic of a specific website, and other security scenarios that are hard to be identified by the CSIRT.

8 Incident notification operations

8.1 Overview

Incident reporting is used for all types of events for the purpose of incident communication. Figure 2 shows that incident reporting consists of three phases that can be described as:

1) incident notification operation: the detected ICT security event, that is a potential incident, is reported (event reporting) from the source (people, external organization notice or system alert) to the PoC;

2) internal incident reporting: depending on the characteristics of the incident, various types of internal reporting take place as part of the incident reporting (see Clause 12);

3) external incident reporting: the organization can need to report certain types of incidents to external parties outside the organization (such as for regulatory purposes), to authorities or to other identified parties (such as suppliers, customers etc.). This can form part of the incident operation but can also be separated depending on how the incident management is structured and the characteristics of the incident (see Clause 12).

Reporting within incident operations is focused on handling the incident and determining the kind of reporting that is needed – including escalation – as necessary. However, it should also consider the reporting that is to be made in order to report it as part of the ICT security procedures. Depending on the categorization and classification of the incident, preparation of external reporting can also be necessary as part of the incident operation. The initial event reporting involves the notification or alerting of CSIRT staff about security events.

NOTE Incident notification operations differ from incident reporting operations in that incident notification operations involve the events taken before the formal reporting of an event. The difference is also explained in the Note in 5.2. Incident notification operations eventually trigger incident reporting operations. Incident reporting operations are covered in Clause 12.

Notification of security events can originate from a user source to the PoC, that assesses the event and, if the PoC considers it to be a possible incident, the CSIRT is contacted. Notification of security incidents can also originate as a result of monitoring and detection activities directly conducted by the CSIRT.

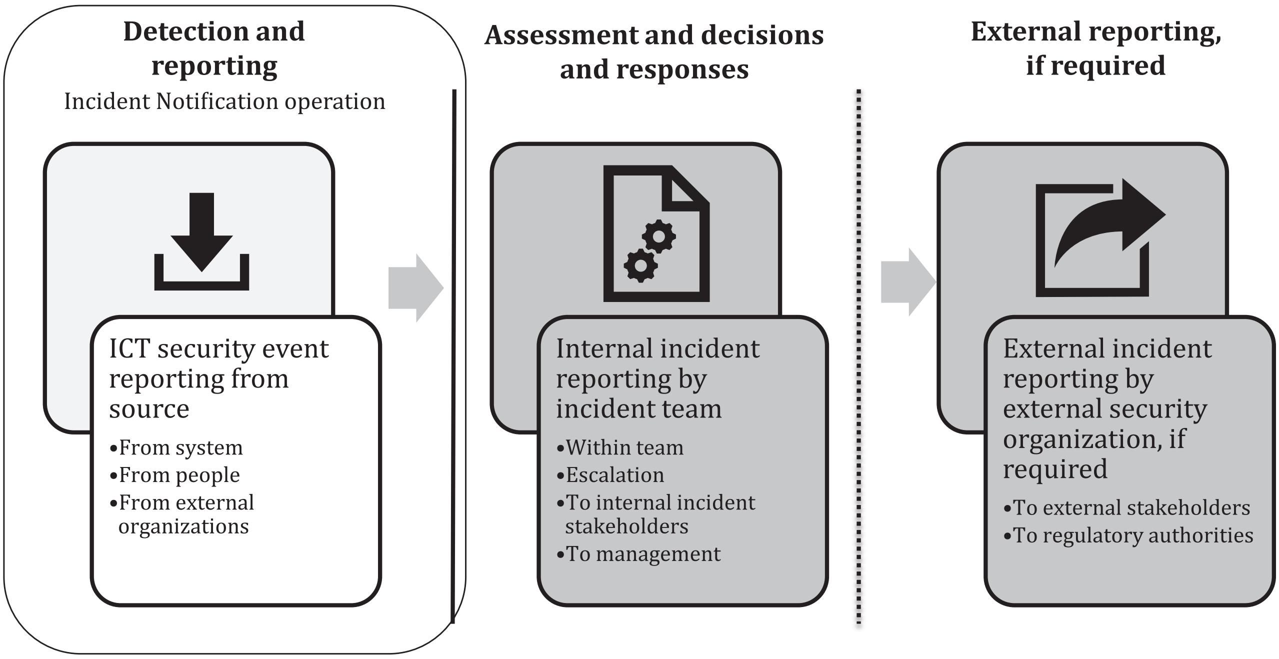
Detection and reporting
Incident Notification operation
ICT security event reporting from source
•From system
•From people
•From external organizations
Assessment and decisions and responses
Internal incident reporting by incident team
•Within team
•Escalation
•To internal incident stakeholders
•To management
External reporting, if required
External incident reporting by external security organization, if required
•To external stakeholders
•To regulatory authorities

Figure 2 — Internal incident notification and reporting

Reporting within incident operations depends on the information security event and whether the nature of the event is determined to be an incident that needs to be reported externally. The process starts with internal incident notification operation. Incident notification operations can differ in the following possible cases:

- a single PoC exists in the organization;
- multiple PoC exist in the organization.

See 8.3 for different PoC structures and how that can affect notifications.

8.2 Immediate incident notification

8.2.1 Incident reporting forms

Reporting forms can be used for suspicious events, incidents, vulnerabilities, and other event types for the team to investigate. The use of a reporting form helps sites to provide the appropriate information, organize the information they provide and understand how to make a request/report. The use of a reporting form helps the CSIRTs to prioritize reports, obtain the information needed in one interaction and set expectations of sites using the form. For examples of incident reporting forms, please refer to ISO/IEC 27035-2.

NOTE The requirements and procedures for external reporting is determined as part of plan and prepare (ISO/IEC 27035-2).

8.2.2 Critical information that incident reports should (ideally) contain

The incident report should contain Indicators of Compromise (IoCs). An IoC is an artifact observed on a network or in an operating system that, with high confidence, indicates an intrusion. Typical IoCs are virus signatures and IP addresses, MD5/SHA hashes of malware files or URLs or domain names of botnet command and control servers.

For example, an MD5 hash can be created to signify the integrity of a data block or string. The resulting hash uniquely identifies that particular block or string of data. If the original block or string of data is illegally changed by as little as a single text character, and if a new hash value is computed for that particular block or data, this re-computed hash value differs completely from the original hash value, indicating that the integrity of the original data has been altered, either deliberately or inadvertently.

8.2.3 Methods to receive reports

Two main methods to receive reports exist: via a CSIRT team email address or via a hotline or helpdesk. Regarding the CSIRT team email address, a standard email address should be used to communicate with the CSIRT team. Ensure that this is the address that is published for constituents to send reports or requests for information. Communications should use the appropriate channel based on a need-to-know basis. Also, the confidentiality aspect of the information that is being reported should be considered, taking into account the organization's classification and handling rules as well as their access controls.

Regarding the hotline or helpdesk, each CSIRT should decide how to provide their hotline service. Many teams do not have a formal CSIRT hotline but use an already existing organizational helpdesk number to receive computer security incident reports and requests. Issues relating to the location of a hotline service (i.e. within a CSIRT and parent organization), staffing schedules, operation hours and service level agreements should be identified and documented in relevant policies and procedures.

A CSIRT hotline can be:

- part of the CSIRT and has a special CSIRT number;
- part of a general Helpdesk and has a general Helpdesk number;
- part of an IT or infrastructure team and has a general number;

- part of a security team and has a general security number;
- a third party answering service or message centre.

A CSIRT can staff its hotline with dedicated personnel or resource, shared responsibility or external staff. The CSIRT should have procedures for when the hotline is very busy. The CSIRT hotline hours of operation can be 24/7/365, business hours only or specified hours only. CSIRTs should distribute information related to their service availability.

Whoever answers the hotline should know the level of service they are expected to provide. For example, they should gather information only, provide technical assistance or some mix of the two. The CSIRT constituents should be made aware of the level of technical services available through the hotline.

8.2.4 Considerations for escalation

If the PoC has the ability to estimate that the incident is serious by using scales or classifications of an incident (see Annex A), this should follow notification to several roles (including CSIRT manager) specified for such incidents to enable escalation for possible early activation of continuity plans and crises teams.

If the PoC is uncertain, advice on escalation should be immediately sourced from the CSIRT manager that determines what to do.

In the case that the notification alarm[3] level is identified as "Serious" or "Alert", the CSIRT manager should be notified and a report registered. The CSIRT manager verifies the case and checks whether it is indeed considered "Serious" or "Alert". Using emergency contacts, the related staff members and/or organizations can be alerted. In the case that the alarm level is identified as "Cautious", the CSIRT manager should be notified, who should request that the necessary actions be taken by response teams according to the direction or discretion of the manager. In the case that the alarm level is identified as "Concerned", notify the CSIRT manager and monitoring teams and/or staff directly to take proper responses.

NOTE Verify incident notifier information (organization, name, contact, etc.), damaged system (host name, IP etc.), detailed description of the incidents, incident detected date/time, post–response, attack types, etc.

Procedures for handling false reports should be created. False reports would include angry reports, spam reports and malicious reports.

8.3 PoC structure

8.3.1 Incident response operation notification if a single PoC exists

If a single PoC is formalized, all events should trigger and send a notification to the PoC. Normally, the PoC then handles all types of events, i.e. not only information security events, but can be related to quality, health and safety, etc. which can fall outside the scope of information security. The wide variation of events often requires that the single PoC has a second line of expertise and one of these should focus on ICT-related events. For ICT-related incident response operations, the single PoC should:

- have high availability;
- use skills to be able to determine what an ICT-related information security event or incident can be;
- have a clear understanding of who to contact next;
- have the task of recording all initial data about the event.

A single PoC can exist in smaller organizations in a quite informal manner. In a larger organization, the PoC should be highly structured and formalized and some kind of incident system support should

[3] For a full list of alarms, see A.2.

be considered. The system support should enable easy delegation and can also involve categorization and reporting. A distinctive definition and clear chain of responsibility contacts are key elements for incident response operations.

8.3.2 Incident response operation notification if multiple PoCs exist

In case of multiple PoCs, these PoCs may each be responsible for a primary type of event that should be notified to them. For example, ICT-related events go to an ICT-related PoC such as Helpdesk. Health and safety goes to an HR-related PoC, etc. From an information security point of view, having multiple PoCs can create problems, as non–ICT-related as well as ICT-related information security events can be sent to the wrong PoCs. In such a case, certain incidents may not reach the intended PoC. A multiple PoC structure may be used in larger or medium-sized organizations and an evaluation of their relative effectiveness should be regularly reviewed. If a multiple PoC structure is used by the organization, it is essential that:

- a clear definition of information security events and incidents are determined that distinguishes ICT-related information security events;
- a high awareness of the personnel exists of which events should be notified to which PoC;
- each PoC should be aware of the domain of the other PoCs so that events can easily be transferred to the relevant PoC if the PoC was not duly informed, especially for events that can be ICT-related;
- a common system support for all PoCs should be used;
- the system should have an instant alert ability that enables a quick initiation of the incident response operation, regardless of which PoC it is notified to;
- all PoCs should have the ability to record the initial data of an event.

9 Incident triage operations

9.1 Overview

By analysing and eventually identifying the root cause after collecting the data for an attack type and evidence, the spread of damage can be blocked, a prevention policy can be established, and quick and effective recovery of the system should be followed. This practice is known as triage. Triage is the process of sorting, categorizing, correlating, prioritizing and assigning incoming events, incident reports, vulnerability reports and other general information requests. It can be compared to triage in a hospital where patients who need to be seen immediately are treated with a higher priority and, thus, are separated from those who are still able to wait for assistance.

Triage is an essential element of any incident management capability, particularly for any established CSIRT. The purpose of triage is to understand what is being reported throughout the organization. It serves as the vehicle by which all information flows into a single PoC, allowing for an enterprise view of ongoing activity and a comprehensive correlation of all reported data. Furthermore, triage allows for an initial assessment of an incoming report and queues it, based on a certain priority, for further handling. It also provides a venue for beginning the initial documentation and data entry of a report or request if this has not already been done in the detection phase.

9.2 How triage is conducted

The triage process involves the following stages:

- determination of incident severity is based on the business impact to the constituency, the hosts involved, the activity/attack method used, the timing of “attacks” and reference number(s);
- correlation with other reports: correlation is looking at how many reports relate to one particular incident. This can help determine the scope and severity of the activity;

- prioritization: if the event is not part of an ongoing incident then, after it is categorized, it is passed to the Prioritize stage. Certain categories of events can actually have their own predefined priorities. Often, it can take additional analysis to determine the priority. Prioritization decision criteria can involve the following:
  - level of danger to human life;
  - reputational impact;
  - operations stoppage or damage;
  - protecting sensitive information;
  - limiting financial loss;
  - maintaining infrastructure integrity;
  - threat to CSIRT systems;
  - threat to critical infrastructure;
  - type of activity;
  - scope of activity;
  - relationship to other ongoing security-related and non-security related activity;
- assignment: if information is notable or suspicious, it is assigned to someone in the Analysis process and passed on to that process. It should be noted that the categorization and priority, as well as the assignment, may be changed when the event is analysed in the Respond process.

The following sources of information can assist analysts performing triage:

- public (external) sources;
- internal sources, perhaps from other incident reports;
- threat intelligence sources: using knowledge about the type of incident or attack (internally or externally);
- common description: if it has been identified as an attack, search if there is a common description (externally). Also see common attack types in Clause 5;
- organizational priorities defined by standard scoring processes or matrixes for scoring;
- know-errors or problem databases.

NOTE 1 Threat intelligence can be arranged as part of plan and prepare (ISO/IEC 27035-2) to be used during triage.

NOTE 2 ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043 and ISO/IEC 27050 provide more detailed information on the digital evidence and investigative process.

10 Incident analysis operations

10.1 Overview

Incident analysis is defined as the series of analytical steps taken when trying to ascertain what is the cause and effect of an incident. There are different types of technical analysis that can be conducted when handling an incident. Examples include, but are not limited to, the following:

- system analysis – the process of acquiring, preserving, and analysing system artifacts (e.g. log files or registry information) that help determine the cause of the incident and develop courses of action;

- network analysis – the process of collecting, examining, and interpreting network traffic to identify and respond to events that violate the security policy or posture of the resources attached to the network, or the network infrastructure and used to support computer security incident investigations;
- malware analysis – the process of identifying, analysing and characterizing reported software artifacts (e.g. signatures of viruses, worms, Trojan horses, etc.) suspected of being adversarial tradecraft to help with in-depth mitigation actions and strategies, counterintelligence activities, and law enforcement activities;
- forensic analysis – for information regarding computer forensics technology and methodology, please refer to ISO/IEC 27037 and ISO/IEC 27043.

The above set of names for "analysis categories" is an example. Often, there are not clear lines of separation between these. For example, a person analysing a system using system analysis can discover malware traces on the system. The same is true for a person performing network analysis. The level, or depths, of analysis conducted can often depend on the context of the analysis request or mission of the organization. For instance, some organizations can be tasked with recovering from a compromise and wish to determine the extent of the damage. This can differ greatly from analysis required to support a law enforcement investigation where data preservation and chain of custody should be strictly managed.

When conducting the analysis, known knowledge can be useful. Such known knowledge can be gathered by the organization from threat intelligence in order to better prepare response to incidents or attacks. Such knowledge can also originate from external sources or even from cooperation with other organizations. Threat intelligence can include the identification of potential malicious parties that want to harm the organization due to the way such parties act. If an attack occurs, it would be useful to determine the type of attack during analysis. Determining the attack type often reveals more detail of the type of incident, such as what specific malware can have been utilized during the attack. It can be useful for the organization, as part of their threat intelligence gathering, to regularly stay informed about threats using indicators of compromise (IoC).

Table 2 shows examples of typical information that would be of analytical value to an incident investigation. These examples are not complete or exhaustive.

Table 2 — Examples of analysis information

Item		Analysis description
Computer Systems	Desktop system	Verify system and process time/status, network information, user/group, sharing information, login information.
		Rootkit (process, network, hidden registry check).
		Registry analysis, auto execution, event/log analysis, file system created time, intrusion method analysis, Internet temporary files.
		Detected malicious codes and/or hacking programs.
	Server system	System information (e.g. operating system type, version, usage, services), process information, open files and ports, network information, accessed users.
		Password file, log file, root kit, hacking-related files.
Network		Data collection for each incident types (use of illegal resources, DoS, data loss and modification, exposed information).
		Packet, traffic statistics, decoded packet.
		Attack patterns, cause of overload.
Database		Use of the default password, remote access.
		Access permission and/or authorization, access control list.

NOTE Threat intelligence including knowledge about indicators of compromise (IoC) can be arranged as part of plan and prepare (ISO/IEC 27035-2) to be used during analysis.

10.2 Purpose of analysis

An analysis attempts to discover the full impact of an incident within an organization. This includes the threat and vulnerability information which can be used by the CSIRT team to plan its next course of action (response and recovery). An analysis is used to determine answers to critical questions about information such as:

- what is the problem?
- who is affected?
- how wide-spread is the problem?
- how serious is the problem?
- what fixes, workarounds, and mitigation strategies can be provided as a response?

The following is a list of examples of common file types with some general notes on analysing them.

- Binaries. Most files in applications like word processors, audio recorders, or video editing software, are binary files. Binary file analysts often want to extract the contents of such files. Digital forensics experts have to identify traces of suspicious activities in them, such as dissecting binaries to understand the capabilities of malware. They often have to reverse engineer binary files in order to accomplish this.
- Executable files are the most common file type that is used by malware, like viruses, as their hosts. Malware can attach themselves in various ways to executable files by means of "infections". Analysts need to inspect such file types in much the same way as explained in the binary file type above. A common file analysis utility used to analyse this and many of the other file types listed here, is known as a hex editor.
- ASCII encoded files. This kind of files is text-based files that can be easily read by any text editor. This file type is the most commonly indexed file, i.e. it is usually used to make a full text index so that, when investigated, an investigator can effectively search for certain text search strings in order to find any potential evidence within it.
- Archives. One of the main reasons for analysing archive files is to gather any potential evidence since archive files often contain backed-up documents that can hold sensitive information. Archives are also much larger in size and can potentially hold key evidence.
- Log files are one of the files that digital forensic investigators starts with when doing their analysis. Log files contain a plethora of crucial information such as date and timestamps, who accessed what objects, from where were these objects accessed, activities that were executed, etc.
- Like archives, document files may contain lots of content that may have evidential value, such as business secrets, electronic communications, intellectual property and almost any kind of information that would be printable but stored in electronic format.
- Spreadsheets are similar to document files. However, the main reason spreadsheets are to be part of the analysis is because they often contain financial information.
- Metadata is not applicable to a single file type, but to almost all other file types that exist. Metadata is often sought after when analysts want to investigate meta events that were recorded in a file, such as last date and time accessed, updated, copied, moved and by which user or process these actions have been effected.
- Similar to metadata, network traffic is also not bound to a particular file type. There are many reasons that calls for network traffic to form part of an analysis. For example, network traffic can be used to determine unusual file transfers, the source and destination of malicious packets/traffic, responsible processes, and devices or users.

- Packet capture is strongly connected to analysing network traffic. In fact, the main difference between analysing network traffic and capturing packets is that, when capturing traffic, a copy of the network traffic is made in order to conduct a later analysis on the network traffic whereas, in the case of network traffic analysis, the latter is conducted in a live fashion as opposed to a post-mortem fashion when doing packet capture.
- Source code of applications constitute the way in which programs eventually execute after they have been compiled and run. Analysts often want to figure out why a certain program behave the way it does. This helps to identify software bugs and vulnerabilities that are often exploited by malware. By analysing the source code, these bugs can be identified and fixed so that the applications may not be prone to malware exploits.

10.3 Intra-incident analysis

Intra-incident analysis deals with what happens with a very specific incident. Common types of intra-incident analyses involve the analysis of network traces, system data, file system data, malicious code and log files. The following is a list of common types of data that can be of interest during the analysis of these types of intra-incident analyses.

- Network data. One reason for analysing network data is due to performance issues affecting the network such as the traffic load over time (number of packets/bytes/connections) and the traffic load by protocol or IP address. Another reason for analysing network data is to determine the status of certain components such as:
  - connection attempts, failures, and duration;
  - connection by user or host;
  - which network interfaces are enabled, disabled, produced errors;
  - which listening service ports are active;
  - whether network probes and scans are/were conducted;
  - whether a system was actually compromised or not. Network trace data is less likely to be modified by a successful adversary, whereas on a compromised system the adversary can relatively easily alter the system's log data in order to hide the adversary's traces.
- System data. One reason for analysing system data is to determine performance issues that affect the system. These can include determining the resource use over time for resources such as CPU, memory and disk usage as well as determining which errors (if any) were reported by hardware. Another reason for analysing system data is to determine the status of certain components or events in a system such as:
  - current system status – when shutdowns and restarts occurred;
  - file system status such as the partitions on the file system, the file system mount-points (which files are currently open, how much free space is available, what size certain files are, etc.);
  - successful and failed logins that occurred;
  - what escalated user privileges took place.
- Process data. Understanding and capturing process status is one of the most granular types of logging. Process logging can reveal applications behaving erratically or out of standard operations parameters. One reason for analysing process data is to determine performance issues that are affecting the process(es). This can include determining the resources used over time or determining the top 10 resource-consuming processes. Another reason for analysing process data is to determine the status of a process such as:
  - who the user is/was that executed the process;

  - start/exit time and duration of a process;
  - arguments and file names associated with the process;
  - associated applications with the process.

- File system data analysis involves a combination of system and network analysis. A large number of file systems exists that all have unique properties. File systems are mostly dictated by the particular operating system providers. Some of the most common file systems in use today are NTFS, FAT, FAT32, HPFS, etc. These systems store most of the data that is used by computing devices. Hence, they are a source of ample potential evidence.

- Artifact/malicious code analysis attempt to analyse four different categories:

  - attack surface analysis: attack surface analysis is about mapping out what parts of a system need to be reviewed and tested for security vulnerabilities. The point of attack surface analysis is to understand the risk areas in an application, to make developers and security specialists aware of what parts of the application are open to attack and to find ways of minimizing this. This kind of analysis is usually done in advance, similar to threat modelling. Attack surface analysis and threat modelling should be performed as part of overall risk management processes before incidents occur;

  - comparative code analysis is the item-by-item comparison of two or more comparable pieces of code. Changes in the code of a program over several versions can be presented together to detect the emerging trends in the program's operations and results. For example, malware can infect a certain program, injecting its code into the program. This can change the program code significantly and can be detected by comparative code analysis;

  - runtime analysis is a tool that estimates and anticipates the increase in runtime of an algorithm as its size increases. A program can take seconds, hours or even years to finish executing, depending on which algorithm it implements. Runtime analysis can often detect the working of malware that is present in a system;

  - reverse engineering is the process of taking a software program's binary code and recreating it so as to trace it back to the original source code. It is being widely used by analysts when the source code of a program – especially malware – is not available. Reverse engineering a malware program in order to reveal the source code, can help an analyst to understand its logic so that appropriate action can be taken to either prevent future exploits or simply to understand what the malware program exactly executed.

- Software environment analysis involves the analysis of how different software applications behave together on a system. Analysts often like to investigate how software that co-exist on a single system interact and influence each other. Such an analysis would help to determine what software has what influence over security incidents.

- In a single incident, there can be certain situations that have trivial or subtle relationships. Such relationships can prove to be useful in determining the root cause of an incident. For example, an incident can have occurred when a storage drive shut down unexpectedly and this incident needs to be investigated. It turned out that the drive's power saving mode kicked in due to prolonged system idle time. This, in turn, caused performance issues when the system suddenly had to handle a burst of incoming network transfer requests. In this example, there is a relationship between the chain of events that happened to cause this performance degradation.

10.4 Inter-incident analysis

Inter-incident analysis involves the analysis of relationships and issues between a certain incident and the occurrence of one or more other incidents. Therefore, inter-incident analysis attempts to analyse similarities and relationships between the various incidents in order to obtain intelligence of the incidents. Inter-incident analysis also involves the correlation between different incidents in a time chain, which can help to identify the potential advanced persistent threats (APTs).

The modus operandi of conducting inter-incident analysis is similar to that of an intra-incident analysis. The only difference is that relationships are sought between several incidents in the case of inter-incident analysis as opposed to investigating within a certain incident in the case of intra-incident analysis.

10.5 Analysis tools

There are several analysis tools that already exist on the market today. However, this document does not promote any of them. Rather, the most common types of analysis tools and some examples are listed here (not an exhaustive list) and briefly described. It is recommended that other sources are also consulted for an updated list.

- General file analysis tools. These include file editors (e.g. hex editors), integrated development environment tools (IDEs), file viewers (e.g. type, cat, more, less), etc.
- Binary and executable file analysis tools. These include file information (metadata) tools (e.g. file, gfile, file properties), ASCII string viewers (e.g. strings and most other text viewers), debuggers and disassemblers/decompilers (e.g. IDA-Pro, Boomerang).
- Archive and media file analysis tools. These include media identification tools (e.g. PeID), (un) compressors (e.g. uncompress, bunzip2, gzip) and unpackers (e.g. tar, unzip, shar, stuffit, 7zip).
- Event viewers (SIEM) tools. With these tools, the analyst can view system, security and application event logs. They can also export the logs into a common delimited text file and then use an application like Excel or a Perl script to parse the information. Some sites set the log files to go to a centralized share; this may introduce some security issues into the process.
- Log file analysis tools. These include, for example, shell or Perl scripts to extract information, sort commands with options for creating unique lists or to total counts, and GNU tools such as “grep” or “awk” commands to pull out data matching a string.
- Forensics analysis tools. For information of digital forensics technology and methodology, please refer to ISO/IEC 27037 and ISO/IEC 27043.
- New and advanced tools appear frequently on the software market. Some of them are commercially available and others are freeware.
- There are various tools for viewing different types of network data, for example:
  - packet capture: tcpdump, wireshark;
  - network flow: SiLK, Argus;
  - passive DNS: nmsg;
  - network configuration and SNMP data: Nagios;
  - NIDPS alerts: Bro, Snort, integrated into SIEM.

10.6 Storing evidence and analysis results

The evidence of an incident should be preserved safely for the future reference, and the collected data (such as log files, process information, network connection status, file contents, malware, database, etc.) should be written to an image (such as a database dump, history file, screen shot, disk image, picture, etc.). The evidence should be preserved by means of enforcing rigorous chain of custody. See ISO/IEC 27037 for details on data preservation and chain of custody.

If an information security event is determined to be a significant incident (using the organization's pre-determined severity scale), the CSIRT manager should be informed directly. Information and other evidence collected at this stage can need to be used in the future for disciplinary or legal proceedings.

A person undertaking the information collection and assessment tasks should be trained in the requirements for collection and preservation of evidence (see ISO/IEC 27035-2).

11 Incident containment, eradication and recovery operations

11.1 Overview

The main purpose of an incident response is to contain, eradicate and recover from an incident. The primary objectives for the response process are:

- halt or minimize attack effects or damage while maintaining operational mission continuity;
- ensure the effective and timely recovery of systems in a way that prevents similar incidents from occurring again;
- strengthen the organizations' defensive posture and operational readiness;
- ensure that response activities occur in a manner that protects any data according to its level of sensitivity;
- support rapid, complete attack characterization;
- develop and implement courses of action (COAs);
- remediate or mitigate the activity;
- recover systems to normal operational level;
- improve infrastructure and incident handling processes.

11.2 Conducting the response for containment, eradication and recovery

11.2.1 Containment description

While an intruder has unauthorized access to a system, the system cannot be properly analysed or restored. Containment provides a reasonable security solution until such time that sufficient information has been collected to address the vulnerabilities and the damage. It should be noted that some containment actions can be taken during the preliminary response phase of an incident handling life cycle. More containment steps can be warranted following in depth analysis, which can identify more affected systems or malicious activities. Containment steps can be executed iteratively with the steps in the detection and analysis phase.

11.2.2 Containment goals

The containment goals are to prevent an intruder from:

- accessing or exfiltration of data or other information;
- destroying valuable evidence and tampering with systems while they are being analysed;
- using systems to attack other systems, protecting the organizational components from liability.

11.2.3 Common containment strategies

The following common containment strategies can be used.

- Implement (firewall) blocks. Gateway IP and port blocks are used to prevent the spread of compromise from an identified external system or attack vectors. Sample firewall blocks include IP addresses that host malicious code, malware, spyware, unauthorized software, mail relays, phishing and spam originators, or known hostile IP addresses and hosts. Mail blocks include filtering for attachments, subject lines and senders. Examples include spam, phishing, worms and other mail attachment attacks containing malicious code. Proxy firewall blocks are dependent on the content filtering solution of the component managing the proxy application.URL and domain blocks are used to prevent access to unauthorized or malicious websites or hosts.

- Disconnection (isolation, removal). Disconnecting a system that has been infected from the local network area can help prevent infections of the rest of the network. Disconnecting the system from the Internet or any other public networks can help to prevent inbound access, outbound traffic or data exfiltration. Disconnecting or isolating the affected network host and/or segment from the rest of the network can help to prevent further contamination or containing malicious activity to a system or logical network segment. This allows attached systems to still function but not spread malicious activity to the rest of the infrastructure. In some cases, this can be relevant to monitor malicious activity while limiting an adversary's ability to attack other systems.

- Shut down. If it is determined that allowing the system to function will destroy data or applications on the system, and with management's approval, the system should be shut down as a containment measure. If it is determined that a particular server, such as an email or web server, requires to be shut down until problems can be eliminated or to contain the spread of malicious code, the specific server should be shut down. Be advised that, in addition to destroying non-volatile data, shutting down a server can adversely affect multiple users and critical operations or services. This decision should be made in coordination with the business manager and data owners. If sufficient analysis has been performed to correctly limit the scope of an intrusion to specific services, these services can be disabled (especially if no patch is available). Be advised that this can destroy volatile data and affect critical operations.

- Routing changes. Eliminate the attacker's route into the environment by preventing the attacker from accessing nearby resources that can be targets. Block the transmission mechanisms for the malicious code between infected systems.

- Account disabling. Disable user accounts that can have been used in the attack.

- Consider other containment strategies presented by NIST SP 800-61: NIST Computer Security Incident Handling Guide.

11.2.4 Issues associated with containment

Any changes to compromised systems, including containment actions, can destroy information required to assess the cause of an intrusion. Ensure that all necessary data for analysis is completely collected before making any system changes. Also, collect and protect all evidence that can be needed in a subsequent investigation before performing any containment actions.

11.3 Eradication

11.3.1 Eradication description

Eradication is the elimination of components of the incident such as malicious code, compromised accounts and passwords, or other compromised systems and information. The goal of eradication is to permanently remove digitally stored data from some form of media either effectively or actually.

11.3.2 Eradication strategies

The following eradication strategies can be used:

- hard disk reformatting;

- use media wiping tools to completely erase the hard disk;

- firmware flashing;

- physical destruction.

11.3.3 Issues associated with eradication

The following issues can arise during the course of eradication:

- inadvertent destruction of data;
- inadvertent destruction of media;
- firmware flashing issues.

11.4 Recovery

11.4.1 Recovery description

Recovery is the restoration of a service, data or system to its normal operational state. The recovery may be part of an overall business continuity planning for the whole organization (see ISO 22301) or an ICT specific plan for continuity and recovery which is further described in ISO/IEC 27031.

Subclause 11.4 describes ICT recovery in brief while ISO/IEC 27031 covers it in detail.

11.4.2 Recovery strategies

The following recovery strategies can be used:

- rebuild systems from clean backups;
- rebuild systems from scratch;
- change accounts and passwords;
- harden against re-occurrence;
- apply system updates and patches;
- business continuity recovery from a hot or warm site, if the recovery state is hardened against the incident.

11.4.3 Issues associated with recovery

The following issues can arise during the course of recovery:

- incomplete backups were made and, hence, not all data can be recovered;
- lack of time or other resources;
- credential and/or policy management issues;
- patch management issues;
- network connectivity issues;
- recovery images or installations are susceptible to an ongoing hot or warm incident.

12 Incident reporting operations

12.1 Overview

Incident notification operations trigger incident reporting operations. Incident notification operations are covered in Clause 8.

Incident reporting is an important part of incident assessment and decisions for coordinating correct responses. It is an essential part of incident operations that the reporting channels and formats are established in order to get quick responses to an incident. Furthermore, organizations analyse incidents to uncover issues or problems that place its clients and other clients at risk.

Depending on the context and the characteristics of the incident, reporting can be necessary to make to external parties aware. External parties can be stakeholders such as customers, suppliers, etc., in a supply chain, but can also include individuals. There can also be cases where external reporting should be made to external authorities (see Figure 3). Reporting of an incident internally depends on the ICT security incident characteristics (type of incident and its severity). The incident characteristics and the context of the organization can also require external reporting. If external incident reporting is made it is essential that the procedures and roles for the reporting is established so that the incident operation can focus on handling the incident.

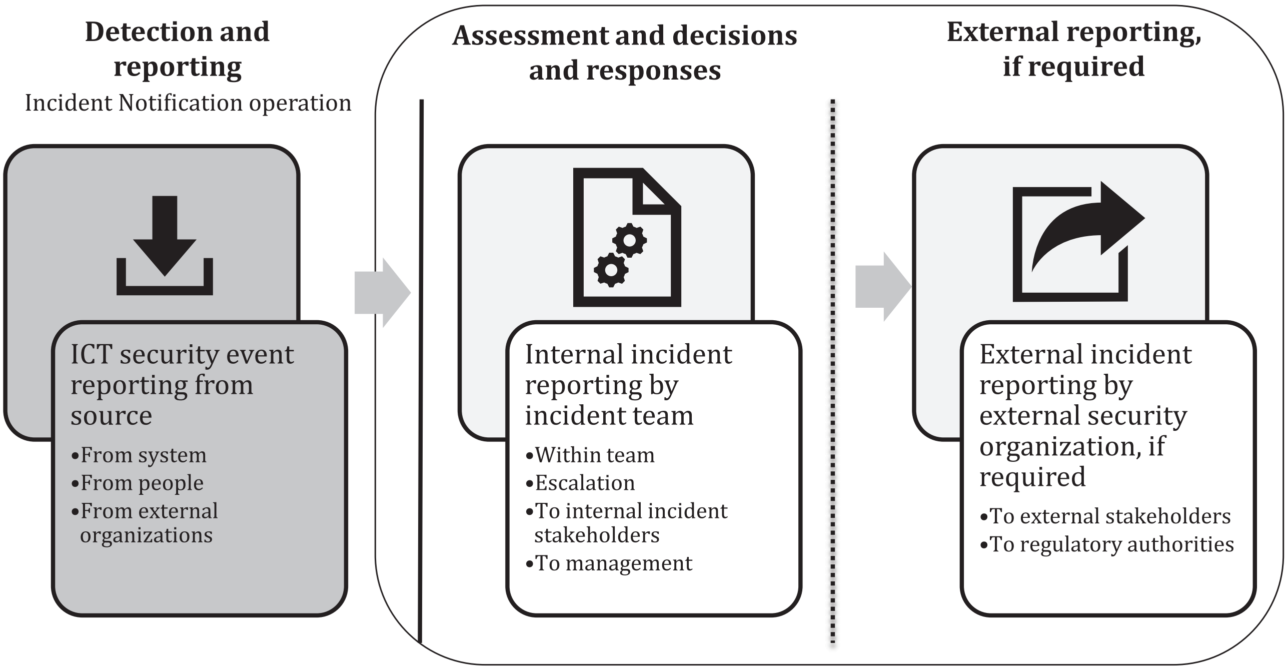
Detection and reporting
Incident Notification operation
Assessment and decisions and responses
External reporting, if required
ICT security event reporting from source
•From system
•From people
•From external organizations
Internal incident reporting by incident team
•Within team
•Escalation
•To internal incident stakeholders
•To management
External incident reporting by external security organization, if required
•To external stakeholders
•To regulatory authorities

Figure 3 — External incident reporting

12.2 How to establish reporting

Incident reporting guidelines should be used to define what constitutes an incident to be reported by the organization. This can include categories of incidents and priorities associated with incident types. There can be several different reports of an incident that the CSIRT needs to initiate. The team can be able to provide technical assistance in responding to the incident but needs a decision to be made by management to act on the response or put the organization in touch with other sites involved in the same activity. The reports also allow the CSIRT to collect and distribute better information about incident-related activities throughout the organization.

The following requirements and guidance should be followed for reporting:

- provide the definition of an incident for the organization;
- provide an explanation for why an individual or group should have a report;
- identify to whom or where the report should be sent;
- provide an explanation of how to report;
- provide a description of what critical information should be included in a report;

- provide an explanation of when to report.

The guidelines can be used to explain:

- who and why they should receive the reports, for example, entities that should receive the report may include the CISO, CEO or some other group or function depending on the characteristics and severity of the incident;
- when a response from the report is required;
- the exact method and procedures for submitting the information via a form, via email or via phone calls;
- contact information;
- if and when external reporting should be made and, if so, how external reporting should be made;
- time and date of report;
- timeframe and date of activity;
- systems affected (e.g. OS version, patch level and purpose);
- brief description of problem or activity;
- any time requirements for submitting reports;
- what critical information should be included in each report.

It is important to use an incident taxonomy in order for the organization to avoid misunderstandings and in order to perform the correct response and make the correct decisions. If external reporting is made, this can also have an impact on the taxonomy and guidelines (see 12.3).

The internal reporting of an incident is also a base for lessons learnt and this should also be considered when creating the guidelines.

NOTE The guidelines are established as part of plan and prepare (ISO/IEC 27035-2).

12.3 How to establish external reporting, if required

External reporting of an incident, if required, should be established and formed with the objective of minimizing the incident operations. The interaction between incident operation and internal reporting, in case of external reporting, should be form of the incident reporting guidelines.

There can be several occasions why and when external reporting is necessary, such as:

- the organization is a supplier and the customers need to be informed of an incident according their contract;
- the incident can affect individuals that need to be informed;
- the incident can be related to crime and, hence, law enforcement should be involved;
- there are regulatory requirements of incident reporting to authorities;
- an external CERT function exists;
- the incident is of such nature and severity that media is informed.

External reporting of an incident may be handled by the CSIRT but, often, this should be handled by other roles. For larger organizations, this can include roles such as:

- the CISO, in terms of reporting to authorities;

- a communications officer, if there is a risk of media interest;
- the customer responsible for reporting the incident, if there is a service that has been affected by the incident;
- any other individual role, if individuals have been affected, as this can have legal implications.

Specific requirements by authorities can exist regarding what incidents to report and when to report them (time frames). Certain taxonomy such as incident types or attack types can also be set. When determining the internal reporting (see 12.2), external requirements should be considered in order to align the guidelines for efficient report handling.

12.4 Information sharing

Information on incidents that occurred should be shared. Reports can be received from other CSIRT teams. The CSIRT team should also report important information that they have received to other teams. Subclause 12.4 includes a short explanation of each data schema, its structure and function, and references to any other International Standards regarding them. An example list of incident data schemas is provided below:

- STIX (XML);
- incident object description and exchange format (IODEF) – (RFC 5070 and possibly RFC 6545);
- VERIS Framework;
- Facebook Threat Exchange (JSON);
- CRITs Data Model (JSON);
- SES-CIF Data Model (JSON);
- ISO references to any structured data schema described above.

Communities for sharing should be created to facilitate threat exchanges, for example, communities (INFRAGUARD), ISACs, etc. More examples (some are commercial) are Open Threat Exchange, RedSky Alliance, Soltra Edge, HITRUST ALLIANCE, CrowdStrike Intelligence Exchange, MSISAC, HPFeeds/HPFriends, Facebook Threat Exchange, REN-ISAC, etc.

12.5 Other reporting considerations

The organization can have a list of high-priority constituents or constituents requiring special considerations. The priority list can include:

- sponsors;
- high-ranking officials;
- other CSIRTs;
- vendors who are currently working with you on a vulnerability analysis;
- vendors whose products are affected by a new attack type;
- other “regulars” (e.g. noted security experts, regular incident or vulnerability reporters, etc.).

The organization's priority list should be a dynamic document that can be easily updated. This is necessary as the people on the list change due to staff turnover, change in sponsorship or priority of incident activity.

12.6 Types of reports

The following types and examples of reports can be created.

- Internal reporting.
  - Report from a customer claiming that they have found a security flaw in operating system software used at their site.
  - Report from a customer claiming that they have an active computer security intrusion on a host at their site.
  - Report containing a partially completed incident reporting form from a customer.
  - Report of a user’s system being compromised and a Trojan horse program being installed.
  - Report of a user sending money for an item won on an online auction and not receiving the merchandise.
  - Report that a laptop has been stolen that contained customer records and credit card numbers.
- External reporting.
  - Posting forwarded from a user community containing an exploit script for a software security flaw.
  - Report of a site’s mail server crashing due to the receipt of large amounts of email with self-propagating worm in attachment.
- Indicator sharing.
  - Request to be added to your CSIRT advisory mailing list.
  - Request for recommendations on web security.
  - Passing of structured indicator information.

12.7 Methods for storing reports and analysts' knowledge

Develop a knowledge management system or database for storing and is searchable for information. The following advice on storage architectures is proposed:

- hot storage: hot storage for data that is accessed on a regular basis, providing quick and responsive read, write and other functionality;
- cool storage: cool storage is optimized for less-frequently accessed data and has a minimum storage period of one month;
- archive: best suited to long-term retention of data.

Annex A
(informative)

Example of the incident criteria based on information security events and incidents

A.1 Information security events and incidents

A.1.1 Fundamental incident criteria

For all the incidents that can cause damage and interferences to running services, the incident criteria are determined based on the type, impact, system priority, damage scale, etc.

Incident criteria should be established as appropriate for an organization based on Tables A.1 to A.4.

Table A.1 — Example of fundamental incident criteria

Category	Description	Reference
Importance of Information	"Moderate", "Important", "Very important"	Table A.4
Impact of the incident type	"Moderate" or beyond	Table A.2
Intrusion damage scale	"Moderate" or beyond	Table A.3
User definition	Security event is detected by user-defined rule set	Other than integrated analysis, ESM, and TMS, etc.

A.1.2 Impacts according to each incident type

Table A.2 — Example of impacts according to each incident

Incident types	Impact			
	Low	Moderate	Important	Very important
Information gathering	x			
Simple intrusion trials	x			
Security policy violation	x	x		
Causing traffic network	x	x		
Attack trials		x		
Website incidents		x		
Website forgery		x	x	
Worms and viruses		x	x	
DoS	x	x	x	
Damage resource		x	x	
Exposed information		x	x	
System destruction			x	x
Network failure			x	x

A.1.3 Damage scale of incidents

Table A.3 — Example of damage scale of incident

Criteria	Description of damage scale
Very important	— The credit rating of the monitoring organization is expected to be lowered. — Core services are stopped. — Financial loss is fatal.
Important	— Core services are jammed. — Large amount of sensitive information is exposed. — Financial loss is considerable.
Moderate	— The impact to core services is partial. — Information leakage is minor. — Financial loss is minor.
Low	Impact to core services is potentially possible.

A.1.4 Importance of the information/system

Table A.4 — Example of information/system importance

Criteria	Description
Very important	Operate majority tasks, Core tasks are processed through the information system (core tasks are jammed in case of incident).
Important	Core tasks are partially processed through the information system (core tasks are partially jammed in case of incident).
Moderate	Few core tasks are processed through the information system (impact is low in case of incident).
Low	No core task is processed through the information system (no impact is applied in case of incident).

A.2 Incident alarm level

Incident alarm level, as shown in Table A.5, is classified into four levels: Concerned (blue), Cautious (yellow), Alert (orange), and Serious (red). Normal is exempted.

Table A.5 — Examples of incident alarm level

Criteria	Description
Serious (red)	The incidents has spread out over the entire country.
Alert (orange)	Incident is verified to impact numerous organizations network/system failures and/or spread out to other organizations.
Cautious (yellow)	Incident is verified to impact several organization network/system failures and/or their vulnerability is increased.
Concerned (blue)	— The damage possibility is increased by worms, viruses, and hacking trials. — System's damage is concerned by the spread of overseas attacks. — The damage is verified similar vulnerability causes by exposed vulnerabilities.

Bibliography

[1] Metcalf L., Spring J.M. Blacklist ecosystem analysis: Spanning Jan 2012 to Jun 2014. *ACM Workshop on Information Sharing and Collaborative Security*. 2015, 13-22, ISBN: 978-1-4503-3822-6

[2] ISO/IEC 22301, *Societal security — Business continuity management systems — Requirements*

[3] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[4] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[5] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[6] ISO/IEC 27041, *Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*

[7] ISO/IEC 27042:2015, *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*

[8] ISO/IEC 27050:2017, *(all parts), Information technology — Security techniques — Electronic discovery*

[9] National Institute of Standards and Technology. NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide [online]. Paul Cichonski, Thomas Millar, Tim Grance, Karen Scarfone. August 2012 [viewed 2019-06-18]. Available at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[10] Internet Engineering Task Force. (IETF). RFC 5070: The Incident Object Description Exchange Format [online]. Edited by R. Danyliw, J. Meijer and Y. Demchenko. December 2007 [viewed 2019-06-18]. Available at https://www.rfc-editor.org/rfc/rfc5070.txt

[11] Internet Engineering Task Force. (IETF). RFC 6545: Real-time Inter-network Defense (RID) [online]. Edited by K. Moriarty. April 2012 [viewed 2019-06-18]. Available at https://www.rfc-editor.org/rfc/rfc6545.txt

[12] RiskAnalytics. DNS-BH Malware domain blocklist [online]. [viewed 2019-06-18]. Available at https://www.malwaredomains.com

[13] Malware U.R.L. [online]. [viewed 2019-06-18]. Available at https://www.malwareurl.com/index.php

[14] DShield. Internet Storm Centre [online]. [viewed 2019-06-18]. Available at https://www.dshield.org

[15] Google. Safe Browsing Alerts for Network Administrators [online]. [viewed 2019-06-18]. Available at https://www.google.com/safebrowsing/alerts/

[16] Team Cymru. [online]. [viewed 2019-06-18]. Available at http://www.team-cymru.com

[17] Shadowserver. [online]. [viewed 2019-06-18]. Available at https://www.shadowserver.org

[18] European Union Agency for Network and Informatrion Security. A good practice guide of using taxonomies in incident prevention and detection [online]. December 2016 [viewed 2019-06-18]. Available at https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection. ISBN: 978-92-9204-194-6. DOI: 10.2824/780536

[19] Forum of Incident Response and Security Teams. Computer Security Incident Response Team (CSIRT) Services Framework, Version 1.1.1 [online]. [viewed 2019-06-18]. Available at https://www.first.org/education/csirt_services_framework

ICS 35.030

Price based on 31 pages