ETSI GS ISI 007 V1.1.1 (2018-12)

GROUP SPECIFICATION

Information Security Indicators (ISI); Guidelines for building and operating a secured Security Operations Center (SOC)

Disclaimer

The present document has been produced and approved by the Information Security Indicators (ISI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/ISI-007

Keywords
cyber defence, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Information Security Indicators (ISI).

The present document is included in a series of 9 ISI 00x specifications. These 9 specifications are the following (see figure 1 summarizing the various concepts involved in event detection and interactions between all parts):

- ETSI GS ISI 001-1 [1] addressing (together with its associated guide ETSI GS ISI 001-2 [2]) information security indicators, meant to measure application and efficacy of preventative measures.

- ETSI GS ISI 002 [3] addressing the underlying event classification model and the associated taxonomy.

- ETSI GS ISI 003 [i.1] addressing the key issue of assessing an organization's maturity level regarding overall event detection (technology/process/ people) in order to weigh event detection results.

- ETSI GS ISI 004 [i.2] addressing demonstration through examples how to produce indicators and how to detect the related events with various means and methods (with a classification of the main categories of use cases/symptoms).

- ETSI GS ISI 005 [i.3] addressing ways to produce security events and to test the efficacy of existing detection means within organization (for major types of events), which is a more detailed and a more case by case approach than ETSI GS ISI 003 one [i.1] and which can therefore complement it.

- ETSI GS ISI 006 [i.4] addressing another engineering part of the series, complementing ETSI GS ISI 004 [i.2] and focusing on the design of a cybersecurity language to model threat intelligence information and enable detection tools interoperability.

- **ETSI GS ISI 007 (the present document) addressing comprehensive guidelines to build and operate a secured SOC, especially regarding the architectural aspects, in a context where SOCs are often real control towers within organizations.**

- ETSI GS ISI 008 [i.5] addressing and explaining how to make SIEM a whole approach which is truly integrated within an overall organization-wide and not only IT-oriented cyber defence.

Figure 1 summarizes the various concepts involved in event detection and the interactions between the specifications.

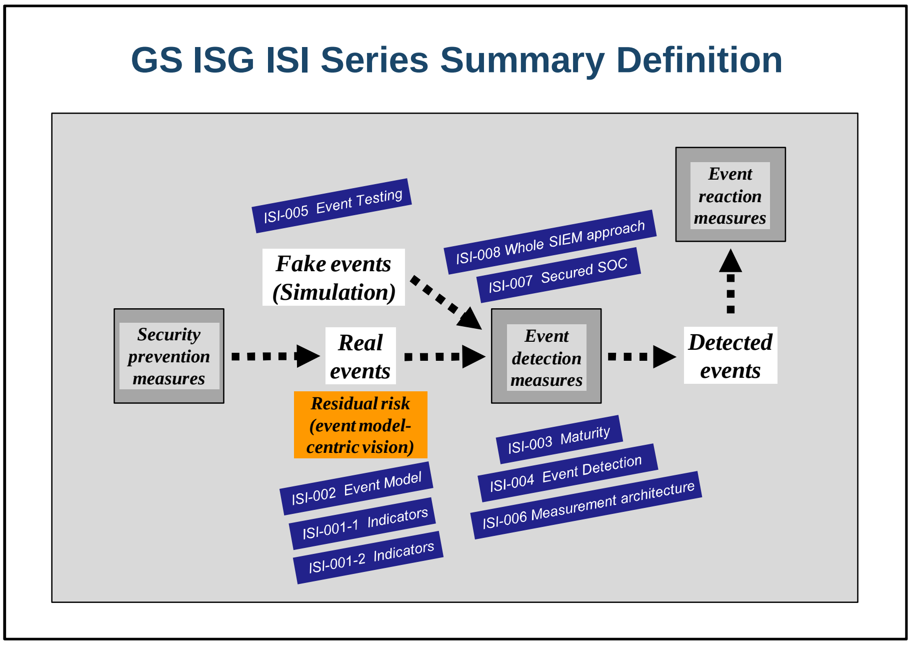

Figure 1: Positioning the 9 GS ISI against the 3 main security measures

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The growing interconnection of networks and the requirements of dematerialization leave information systems vulnerable to cyber-attacks. The points of interconnection with external networks and, in particular, with the Internet, are all access points an external attacker can attempt to exploit to enter and remain inside an information system in order to steal, alter or destroy its information assets. And addressing often very dangerous internal threats is also necessary.

Furthermore, new regulations and laws make it more and more mandatory to detect and report to authorities security incidents. This is in particular the case with the **Network and Information Security (NIS) Directive [**i.10**]**, for which the present document can be a strong basis for the implementation of Articles 14 and 16. For this purpose, it addresses a secured way to use cyber threat intelligence to detect security incidents, which is an important issue to be dealt with in the NIS Directive.

The use of security incident detection systems contributes to the protection of information systems from the threats of cyber-attacks. Human, technical and organizational resources can be concentrated within a cyber security operations center (CyberSOC or SOC), generally dedicated to the detection of and response to security incidents. Depending on the challenges, needs and resources of the commissioning entity, this center can be internal, outsourced dedicated or even shared. In this latter case, the pooling of resources can have positive effects, such as the sharing of information on threats and detection rules.

When the provision of the detection service is compliant with the state-of-the-art, and is precisely adapted to the needs of the commissioning entity, it helps to prevent severe security incidents (by detecting vulnerabilities or non-conformities - see ETSI GS ISI 001-1 [1] or ETSI GS ISI 002 [3]) or, when such incidents occur, to limit their consequences by making it possible to take rapid remediation actions that can be carried out by the commissioning entity's security incident response teams (located either in a CERT or in the SOC itself).

However, the concentration and pooling of detection capabilities make the cyber security operations center a prime target for attackers. Therefore, special attention should be paid to protecting its information system.

The purpose of the present document is to provide guidelines to build and operate a **secured SOC**, through a list of functional, organizational and technical requirements. Furthermore, it covers **security incident detection** up to incident reporting to the commissioning entity **without entering the incident response field**.

It can also be used, in the interest of adopting best practices, independently of any regulatory framework.

1 Scope

The present document covers the 2 types of security incident detection services: internal and external.

The requirements can be implemented at 2 different levels: basic level (partial compliance), advanced level (full compliance).

The present document is structured as follows (after clauses 2 and 3 respectively dedicated to references and terms, symbols and abbreviations):

- **Clause 4** describes the activities to which the present document relates.
- **Clause 5** presents the requirements applicable to service providers (either internal or external) operating a SOC.

NOTE: These requirements, labelled with lowercase letters (a, b, c, etc.), stem from requirements of a similar reference framework published by ANSSI [i.12], so that their labelling is aligned with them, meaning that not present letters correspond to discarded or not relevant requirements.

- **Annex A** presents the tasks and skills expected from the service provider's employees.
- **Annex B** presents the recommendations for the commissioning entities when contracting with security incident detection providers.
- **Annex C** defines the basic and partial level of implementation of the requirements.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS ISI 001-1: "Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture".

[2] ETSI GS ISI 001-2: "Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1".

[3] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model A security event classification model and taxonomy".

[4] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of Practice for information security controls".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS ISI 003: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".

[i.2] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[i.3] ETSI GS ISI 005: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".

[i.4] ETSI GS ISI 006: "Information Security Indicators (ISI); An ISI-compliant Measurement and Event Management Architecture for Cyber Security and Safety

[i.5] ETSI GS ISI 008: "Information Security Indicators (ISI); Description of an Overall Organization-wide Security Information and Event Management (SIEM) Approach".

[i.6] ISO 27035-1:2016: "Information technology - Security techniques - Information security incident management -- Part 1: Principles of incident management".

[i.7] ISO 27035-2:2016: "Information technology - Security techniques - Information security incident management -- Part 2: Guidelines to plan and prepare for incident response".

[i.8] ANSSI: "Guide d'hygiène informatique".

NOTE: Available at https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/ for an up-to-date version.

[i.9] The Center for Internet Cybersecurity: "Critical Security Controls for Effective Cyber Defense Version 7".

NOTE: Available at https://www.cisecurity.org/critical-controls.cfm.

[i.10] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

NOTE: Available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[i.11] ISO 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.12] ANSSI (The French Networks and Information Security Agency): "Security incident detection service providers - Requirements reference document".

NOTE: Available at https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v1.0_en.pdf.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS ISI 001-2 [2] and the following apply:

NOTE: They are primarily taken from the ISO 27000 [i.11] and ISO 27035 [i.6] and [i.7] standards.

administrator: member of the detection service with privileged rights enabling them to ensure the smooth running of the detection service devices

collection source: equipment within the information system that generates events related to the security of the information

collector: device enabling the centralization of security events originating from various collection sources

EXAMPLE: Syslog server, SIEM solution collector.

NOTE: In the context of this service, local collectors are collectors installed in the commissioning entity's information system, and central collectors are collectors used for centralizing events and located in the service provider's information system.

commissioning entity: entity using a security incident detection service

context of a security incident: event related to a security incident, along with all information analysed and produced during its qualification

EXAMPLE: Qualification analysis report(s).

detection rule: list of technical elements allowing identifying an incident based on one or more events

NOTE: A detection rule can be formed by one or more markers, one or more signatures or a behavioural rule based on abnormal behaviour. A detection rule can originate from the vendor of the technical analysis tools used for the detection service, the service provider itself (monitoring of new incidents, a rule used for another commissioning entity with its agreement, etc.), a partner, a specialized supplier, or it can have been created specifically for the commissioning entity.

efficacy: level of achievement of planned activities and the expected results

information system: organized set of resources (hardware, software, personnel, data and procedures) for processing and communicating information

investigation: process designed to collect and analyse all technical, functional or organizational elements of the information system in order to qualify a suspicious situation as a security incident and to understand the intrusion set and the scope of a security incident within an information system

operator: member of the detection service in charge of operating the service, i.e. performing the detection-related tasks constituting the service on behalf of the commissioning entity

probe or detection system: technical device designed to identify abnormal, suspicious or malicious activity within the supervised perimeter

NOTE: The purpose of a probe is to generate security events; it is considered to be a collection source within the security incident detection service.

qualified service: security incident detection service provided to a commissioning entity in compliance with the reference document

qualifying a security incident: determining the nature and criticality of a security incident

reporting: act of informing the commissioning entity of the occurrence of a security incident jeopardizing its information system

security of an information system: all technical and non-technical controls that make it possible for an information system to manage events that could compromise the availability, integrity or confidentiality of the data being handled or transmitted and the related services that this system provides or makes available

service agreement: written agreement between a commissioning entity and a service provider for the performance of the service

NOTE: When the service provider is a private entity, the service agreement includes the contract form.

service provider: entity providing a security incident detection service in compliance with the present document

state-of-the-art: set of publicly accessible best practices, technologies and reference documents (and the information that can be inferred from them) relating to information systems security

NOTE: These documents can be made available on the Internet by the information systems security community, or distributed by reference or regulatory entities.

subcontracting: operation through which the service provider entrusts to another entity all or part of the execution of a contract concluded with the commissioning entity

supervised perimeter: all or part of the commissioning entity's information system, which is object of the security incident detection service

third party: person or organization that is recognized as independent from the service provider and the commissioning entity

3.2 Symbols

For the purposes of the present document, the symbols given in ETSI GS ISI 001-2 [2] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ISI 001-2 [2] and the following apply:

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (France)
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
IS	Information System
ISI	Information Security Indicators
NIS	Network and Information Security
SLA	Service Level Agreement
SOC	Security Operations Center

4 General Description of the Security Incident Detection Service provided by the SOC

4.1 Activities of the security incident detection service

The security incident detection service is composed of three distinct activities:

- Incident management, meaning all of the technical and organizational means for identifying and qualifying a security incident on the basis of collected events. Storing and capitalizing on security incidents in order to improve the service is also part of this activity.

- Event management, meaning all technical and organizational means for ensuring the collection and storage of security events.

- Reporting management, meaning all technical and organizational means making it possible to inform the commissioning entity about detected security incidents and to store these reports.

Reaction and remediation activities are beyond the scope of this service.

4.2 Architecture of the detection service information system

The present document does not impose any specific architecture on the detection service's information system. Several implementation methods are possible. In particular, according to the type of detection service (internal or external), the different zones presented in this clause can be hosted in different entities or organisms, provided that the requirements of the present document are complied with.

Figure 2 is a simplified representation of a typical architecture for a security incident detection service information system, provided for informational purposes only.

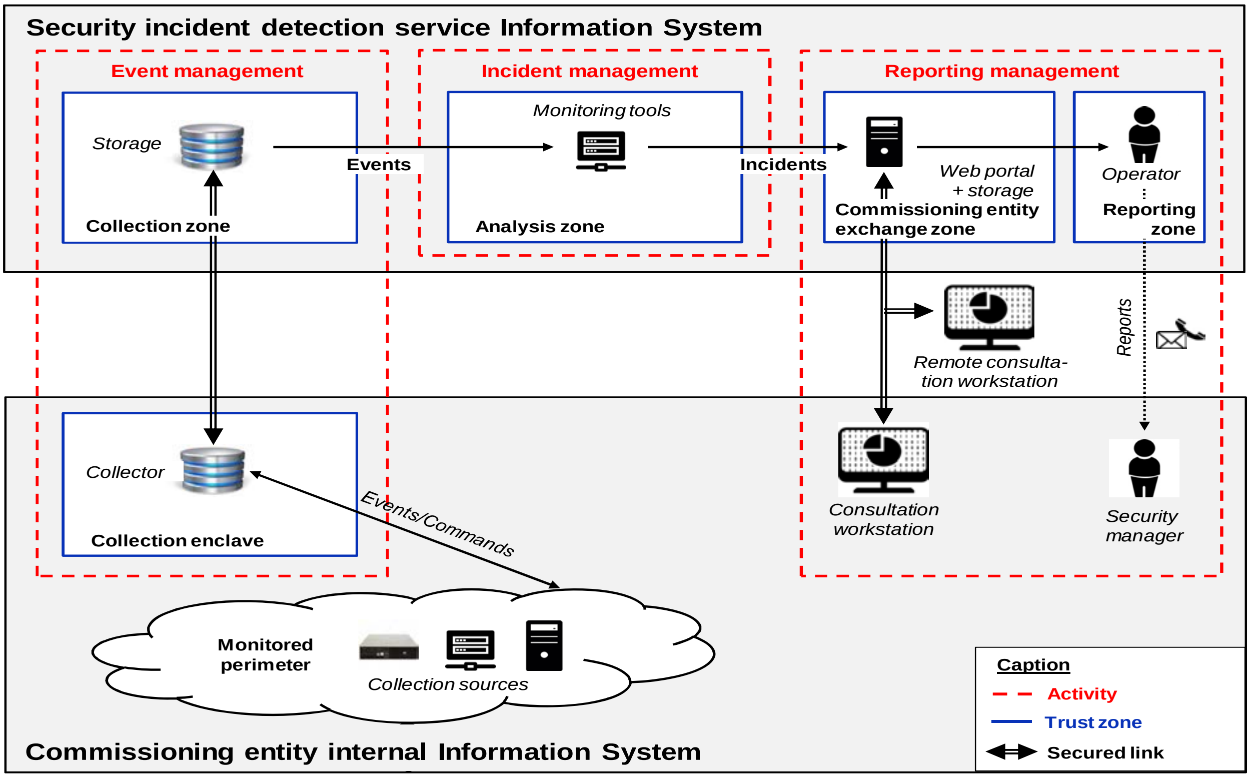

Figure 2: Simplified representation of a typical architecture for a security incident detection service information system

The information system of a detection service is organized into trust zones, partitioned using filtering, authentication and access control mechanisms. The trust zones in the information system of the detection service are the following:

- collection zone(s) (one or more), comprising all devices involved in the collection process, including the central collectors and the systems for storing events and, where necessary, background information;
- analysis zone(s), comprising all devices involved in the analysis process, including the technical tools for analysing security incidents;
- reporting zone(s), comprising commissioning entity's reporting systems, in particular messaging systems;
- commissioning entity exchange zone(s), comprising all devices enabling the commissioning entity to view the details of information on the reported incidents, in particular the web portal, and to provide, where applicable, the information necessary to qualify the incident;
- administration zone(s), comprising all administration tools and administration workstations;
- update zone(s), comprising all devices involved in the process of downloading updates for detection service devices;

- operations zone(s), comprising the operators' workstations;
- exchange zones, which are separate for administrators and operators, comprising all devices enabling the external transfer of the security incident detection service information system files.

Furthermore, a specific zone, which is external to the detection service information system, should be set up within the commissioning entity's internal information system, hereinafter referred to as "enclaves" (due to interaction with the latter). *At a minimum*, one collection enclave should be put in place to host the detection service collection devices deployed within the commissioning entity. In particular, the collection enclave contains one or more local collectors, the role of which is to centralize security events arising within the supervised perimeter.

4.3 Scope of application of the present document's requirements

Clause 5.1 lists the general requirements relating to the service provider's legal obligations, including its duties vis-à-vis the commissioning entity, its guarantees, etc.

Clause 5.2 lists the requirements relating to the activities of the security incident detection service:

- Requirements regarding the incident management activity, including skills of the operators, features of the tools used, implementation of the detection rules, etc.
- Requirements regarding the event management activity, including the sources of collection, the centralization of events on a collector, etc.
- Requirements regarding the reporting management activity, including the means of reporting, the consultation of incident tickets, etc.

Clause 5.3 lists the requirements relating to the protection of information, including encryption, filtering between trust zones, separation of roles between administrators and operators, etc.

Clause 5.4 lists the requirements relating to the organization of the service provider and the governance of the service, including the establishment of a code of ethics and recruitment, the content of the operational and strategic committee meetings, etc.

Clause 5.5 lists the requirements relating to the quality and level of service, including the nature of the indicators to be monitored, the content of the service agreement established between the service provider and the commissioning entity, etc.

5 Requirements to be met by the service provider operating the Security Operations Center (SOC)

5.1 General requirements

a) The service provider should be an entity or part of an entity that has a legal personality so that it can be held legally responsible for the services that it provides.

b) The service provider should comply with the laws and regulations in force where the SOC data are stored and processed by the analysis tool.

c) The service provider should describe the organization of the security incident detection activity that it provides to the commissioning entity.

d) The service provider has, in its professional capacity, a duty to advise the commissioning entity.

f) The service provider should obtain professional liability insurance covering any damages caused to the commissioning entity and especially to its information system during the provision of the service.

g) The service provider should ensure that the consent of the commissioning entity has been obtained prior to any disclosure of information obtained or produced during the provision of the service.

h) The service provider should ensure that the information it provides, including advertising, is neither false nor misleading.

i) The service provider should provide sufficient evidence that the way in which it operates, especially in terms of its financial operations, is not liable to compromise its impartiality or the quality of its performance with respect to the commissioning entity or to cause conflicts of interest.

k) The service provider should possess valid licences for the tools (software and hardware) used to provide the service.

l) The service provider should ask the commissioning entity to notify it of any specific legal or regulatory requirements to which it is subject, especially those related to its sector of activity.

m) The provider service should inform the commissioning entity when the commissioning entity is required to report a security incident to a government authority (in the country where the commissioning entity's information system is attacked) and should assist it in this process if the commissioning entity asks it to do so.

n) The service provider should establish a service agreement with the commissioning entity. The service agreement should comply with the requirements of clause 5.5.3 and should be formally approved, in writing, by the commissioning entity before the service is performed.

5.2 Activities of the security incident detection service

5.2.1 Incident management

a) The service provider should establish with the commissioning entity a list of feared incidents and the impacts and consequences associated with them based on the results of a risk assessment prepared by the commissioning entity (at least for monitored critical application software), and on statistical state-of-the-art figures associated to the ETSI GS ISI 001 part 1 [1] and part 2 [2]. The service provider should recommend to the commissioning entity to update its risk assessment in the event of a change in its infrastructure.

c) The service provider should take into account the list of security incidents and their origins in annex B of the ISO 27035-2 [i.7], as well as that of the ETSI GS ISI 001-1 [1] and ETSI GS ISI 002 [3].

d) The service provider should develop and implement with the commissioning entity an analysis strategy that makes it possible to detect all the incidents on the feared incident list (see requirement 5.2.1.a). This strategy could also include other approaches, for example based on behavioural analysis and threat hunting. The analysis strategy should be reviewed with the commissioning entity during the operational committee meetings defined in clause 5.4.3.

f) The analysis strategy should include a precise description of the implementation of the detection rules for detecting security incidents based on the collected events.

g) The service provider should create detection rules based on:

- the list of security incidents that are feared by the commissioning entity;
- knowledge bases acquired from vendors and information systems security companies;
- internal knowledge bases derived from the expertise of the service provider:
  - the monitoring and qualifying of vulnerabilities, with priority given to those relating to the execution of arbitrary code, locally or remotely;
  - the monitoring and qualification of command control protocols;
  - the monitoring of the modes of operation for attacks and malicious code;
- contextual elements specific to the commissioning entity;
- security incidents detected with any other commissioning entities.

h) The service provider should develop and implement a marking policy for detection rules. This policy should define, for each detection rule:

- a unique identifier for the detection rule, linking various tools and associated knowledge bases;
- a detection rule version number;
- the owner of the detection rule, meaning the entity that owns the rights on the detection rule;
- the author of the detection rule, meaning the entity that created the detection rule;
- the source of the detection rule, meaning the entity that is the source of the information enabling the creation of the detection rule and which is not necessarily the owner or author of the detection rule (for example, a partner, a supplier, the commissioning entity, etc.);
- the creation date of the detection rule;
- the date of the last modification made to the detection rule;
- the terms for the distribution of the detection rule, such as "unrestricted distribution", "may be distributed within a community but not publicly", "may be distributed internally subject to need-to-know", "may be distributed to named individuals and may not be redistributed" or in the form of TRAFFIC LIGHT PROTOCOL (TLP) or others, in accordance with the agreements set out with the sources of the detection rule;
- whether or not it is possible to conduct open-source searches depending on the level of sensitivity and the methods of distribution;
- the description of the behaviour that the rule aims to detect:
    - ▪ the description of the threat;
    - ▪ where applicable, the descriptions and identifiers (e.g. CVE) of vulnerabilities for which exploitations or exploitation attempts have been detected by the rule;
    - ▪ the phases of attack detected by the rule, such as: reconnaissance, initial infiltration, interaction with command and control infrastructure, privilege escalation, lateral movements, exfiltration, etc.;
    - ▪ any other information necessary for the description of the behaviour targeted by the rule;
- the descriptive elements for the implementation of the rule in technical analysis tools:
    - ▪ the method for event analysis and for the triggering of the detection rule;
    - ▪ any potential operational restrictions related to technical criteria;
- analysis and qualification instructions to be followed by the operator in the event that the detection rule is triggered.

i) The service provider should establish and keep up to date, for each commissioning entity, a list of all detection rules that have been implemented or that are being implemented as part of the service. This list should specify, for every rule identified by its identifier and its version number:

- the date(s) on which the detection rule was included in the technical analysis tools;
- if the service provider has conducted an *a posteriori* analysis with this detection rule (see requirement 5.2.1.dd) and the date of this analysis, if applicable;
- the date(s) on which the detection rule was withdrawn from the technical analysis tools in use.

This list should make it possible to establish a historical record of detection rules, allowing for the identification of rules that were active at a given time, or over a given period. A detection rule that has been withdrawn from the technical analysis tools in use should therefore be marked as withdrawn and should not be deleted from this list.

NOTE: The case in which modifications have been made to a detection rule solely for sub-perimeters of the supervised perimeter should be specified in the list.

j) The service provider should send to the commissioning entity, *at a minimum* once a month, a detection rule status report that presents:

- the number of detection rules created, modified or withdrawn from the analysis tools in use;
- the identifier, version number, and description of each rule that has been created, modified or withdrawn from the analysis tools in use;
- the reason for the creation, modification or withdrawal of the security rule (e.g. creation, modification or withdrawal at the request of the commissioning entity, etc.).

m) The service provider should implement in the technical analysis tools in use all of the detection rules identified in the list set out in requirement 5.2.1.i) except for the rules marked as withdrawn.

n) The service provider should independently add new detection rules to the technical analysis tools in use.

q) Following an addition of this type, the service provider should update the documentary record and provide information about the details of the additions that have been made in order to ensure the monitoring and the traceability of such additions.

r) The service provider should qualify the detected security incidents in order to assess their veracity (true/false positive, proven incident or not) and criticality (functional impacts, informational impacts, etc.).

s) The service provider should establish with the commissioning entity a criticality scale associated with the feared security incidents, taking into account the risk assessment and especially the threats, the assets, the potential impacts and their level of criticality.

t) The service provider should use the criticality scale for information security incidents in annex C of the ISO 27035-2 [i.7].

As part of the qualification of a security incident, the service provider can be called upon to carry out open-source searches, especially on the Internet, based on information collected or taken from analyses (cryptographic fingerprints, names of malicious files or of malware, character chains contained in malware, domain names, IP addresses, etc.).

Open-source searches using information collected or taken from analyses can draw the attacker's attention. Thus, it is important that the service provider exercises the utmost caution when carrying them out. Thus, it should take into account the marking of detection rules indicating the possibility of carrying out such a search, or not (see requirement 5.2.1.h).

The service provider should define a methodology for open-source searches based on information collected or taken from analyses. It should specify which types of information can be searched and the associated conditions.

v) The service provider should be able to integrate the results of the tests for vulnerabilities and intrusions carried out by the commissioning entity on its information system In particular, this could translate into:

- the creation of detection rules associated with identified vulnerabilities;
- the development of knowledge bases on existing vulnerabilities to improve diagnosis, whether through technical analysis tools (correlation) or operators (capitalization and use of background knowledge on the supervised IS).

w) The service provider should create a ticket for each security incident detected and make it available to the commissioning entity. *At a minimum*, the security incident ticket should contain the following elements:

- the date of creation of the ticket and the various operations carried out on said ticket (traceability of actions);
- the date and time when the security incident was detected;
- the effective date of the event or events having led to the security incident;
- the description of the security incident;
- the criticality of the security incident;

- the description of the impact of the security incident for the commissioning entity;
- the identifiers and version numbers of the detection rules that were triggered;
- the equipment having generated and collected the events of the incidents;
- the identifiers of events that made it possible to detect the incident;
- the risk resulting from the incident.

x) The service provider should define the format of the security incident tickets together with the commissioning entity.

y) The service provider should use the security incident ticket format set out in ETSI GS ISI 002 [3] and ISO 27035-2 [i.7].

z) The service provider should have a tool for managing the security incident tickets.

aa) The service provider should link each security incident ticket to its context (associated events and qualification analysis report(s)) and store these elements centrally, whether the security incidents are in the process of being qualified, are proven or closed.

bb) The service provider should implement and keep up to date a centralized, chronological record for each commissioning entity identifying all detected security incidents.

cc) The service provider should implement a process to manage the storage capacity of security incident tickets and their context allowing to monitor its evolution and to be able to adapt it to ensure their retention for the duration of the service, subject to compliance with legislation and regulations in force on the concerned territory (see requirement 5.1.b).

dd) The analysis strategy should ensure that for each detection rule that is created or modified, the service provider conducts an *a posteriori* analysis, meaning an analysis of all events that have been stored for a period of time determined together with the commissioning entity in the analysis strategy.

This requirement does not apply to detection rules requiring types of events that are not yet present in the event storage systems.

The service provider should be able to search, *at a minimum*, for the following types of:

- files: fingerprint (MD5, SHA1, SHA256), name fingerprint, access path, size, extension, magic number;
- public IP addresses;
- domains for the following protocols: HTTP, SMTP and DNS;
- URL;
- user-agent;
- e-mail fields: source domain, destination domain, subject fingerprint, timestamp;
- X509 certificate fields: fingerprint, issuer, date of validity, subject, extensions, host name, timestamp.

It is recommended that the service provider be able to search for combinations of these indicators of compromise.

ee) The service provider should be able, upon request of the commissioning entity, to conduct an analysis on the set of events that have been stored for the previous six months.

5.2.2 Event management

a) The service provider should develop, together with the commissioning entity, and implement a collection strategy based on the list of feared security incidents (see requirement 5.2.1.a). The collection strategy should be reviewed with the commissioning entity at the operational committee meetings defined in clause 5.4.3.

b) The collection strategy should identify the list of collection sources, collectors, events to be collected, describe the collection methods (protocols, applications, security properties, etc.), and identify the frequency of collection.

c) The service provider should be, *at a minimum*, capable of collecting events from the following collection sources:

- security equipment: network firewalls, application firewalls, encrypters, probes, antivirus software, VPN concentrators, SSL gateways, proxies, reverse proxies;
- network equipment: routers, switches, equipment generating netflow data, DNS servers, load balancers, time servers;
- infrastructure servers: authentication, directories, software distribution, remote management, supervision, virtualization, file servers, backups, mail, print;
- business servers: web servers, databases, application servers, collectors;
- workstations: main operating systems, security applications;
- mobile devices through mobile fleet management servers (Mobile Devices Management).

d) The service provider should be able to collect events arising from the equipment comprising the industrial information systems: industrial programmable automatons, industrial firewalls, industrial switches and industrial routers.

f) The service provider should, in an independent manner, develop its collection capacity (collection sources and events collected), in connection with the list of feared incidents.

g) In the event of difficulty or inability to implement the collection of one or more events from a collection source, the service provider should warn the commissioning entity as soon as possible, and provide the detailed reasons for the failure. The maximum period between the decision to implement the collection and the report of the implementation failure to the commissioning entity should be defined in the service agreement.

h) The service provider should exercise its duty to advise the commissioning entity in respect of the development, implementation and review of the collection strategy. In this capacity, it should advise the commissioning entity on the development and review of the logging policy (collection sources, types of events to be logged, retention periods, standardization of information, synchronization of time sources, etc.) and on the deployment of logging devices on the supervised perimeter within the commissioning entity's information system.

i) The service provider should recommend to the commissioning entity that it integrates in the collection strategy the deployment of probes at each of the interconnections of the supervised perimeter, and in particular the interconnections with:

- the Internet;
- third-party information systems (partners, subcontractors, etc.);
- the commissioning entity's other information systems more vulnerable or with a lower security classification or sensitivity level.

n) The events from collection sources should be centralized on one or more collectors located in the collection enclave described in requirements in clause 5.3.14.

NOTE: For the sake of simplicity, for the remainder of the present document, it is assumed that there is only one collector.

o) The collection enclave collector should make it possible to carry out an initial filtering of events in order to only transmit to the collection zone and to the analytical tools those events that are relevant to the detection service and identified in the collection strategy.

r) The collector should be able to detect saturation and loss of communication events that would prevent it from transmitting the security events to the detection service and to delay the transmission of the events to the analysis tools if necessary. The service provider should guarantee the storage capacity of the collector in the service agreement. The evolution of the collector's storage capacity should be monitored and presented to the commissioning entity at the operational committee meetings defined in clause 5.4.3.

s) The service provider should have a centralized view of all the events collected, including the association of each event with the collector from which it came.

t) The system clocks of the collectors should be synchronized with a single time source (see requirement 5.3.9.l).

u) The service provider should index all of the collected events and be able to perform searches among the collected events.

v) The service provider should be able to locate and provide any collected event whatsoever upon request by the commissioning entity.

w) The service provider should put in place a process for managing the handling and storage capacity of events enabling the service provider to monitor its development and to be able to modify it as necessary and to ensure their storage for at least six months (see requirement 5.2.1.ee), subject to compliance with legislation and regulations in force within the concerned territory (see requirement 5.1.b).

5.2.3 Reporting management

a) The service provider should have one or more secured information channels available for the commissioning entity, notably for reporting (see requirement 5.2.3.b) and the exchange of detailed information (see requirement 5.2.3.l).

b) The service provider should have at least two reporting methods available: a nominal method and a secondary method. The secondary communication method should be tested at least every six months and every time a modification is made to the security incident detection service information system. For example, reporting methods can consist of:

- email;
- short text message (SMS);
- telephone.

c) The service provider should develop, together with the commissioning entity, and implement a security incident reporting strategy enabling it to notify the commissioning entity in the event that a security incident is detected. The reporting strategy should be reviewed with the commissioning entity at the operational committee meetings defined in clause 5.4.3.

d) The reporting strategy should identify, *at a minimum*, the list of security incidents to be reported, the format, the content, the time limit, and the level of sensitivity or classification of the reports, as well as the persons to be notified, particularly with respect to the security incident and its level of criticality.

e) The service provider should exercise its duty to advise the commissioning entity in the development, implementation and review of the reporting strategy. In this capacity, it should advise the commissioning entity on people to be notified and the reporting methods.

f) The service provider should recommend to the commissioning entity that it includes specific reports in the reporting strategy in the occurrence that major security incidents within its information system are detected.

h) The service provider should centralize all the reports in a report storage system. The following information should be stored:

- date and time of the report;
- reporting method;
- recipient(s) of the report; and
- content of the report, including in particular the incident ticket number.

NOTE: The above information relating to reports can be included in incident tickets.

j) The service provider should put in place and keep up to date a centralized and chronological record by a commissioning entity referencing all of the reports carried out for the commissioning entity. In particular, the report should include: date and time of the report, reporting method, recipient(s) of the report, content of the report including, in particular, the incident ticket number.

k) The service provider should put in place a process for managing the storage capacity for the reports enabling the service provider to monitor its development and to be able to modify it to ensure their retention for the duration of the service, subject to compliance with legislation and regulations in force within the concerned territory (see requirement 5.1.b).

l) The service provider should provide the commissioning entity with:

- a web portal that enables it to view and update the status of security incidents and actions undertaken;
- a storage device enabling the commissioning entity to:
  - retrieve the context of security incidents (associated events and qualification analysis report(s)) concerning it;
  - where necessary, deposit background information necessary for operators to qualify an incident;
  - get access to security indicators.

5.3 Information protection

5.3.1 Information systems security policy

a) The service provider should develop a risk analysis and the associated risk treatment plan covering the full scope of the security incident detection service.

c) The service provider should review the risk assessment and the associated risk treatment plan *at a minimum* once a year and in the event of any structural changes to the detection service, particularly those concerning its hosting, infrastructure or architecture.

e) The service provider should develop and implement an information systems security policy based on the risk assessment.

5.3.2 Levels of sensitivity or classification

b) The service provider should apply information technology hygiene to the security incident detection service information system, based on common reference frameworks such as the French "Guide d'hygiène informatique" [i.8], the US "CIS Critical Security Controls for Effective Cyber Defense" [i.9] or standards such as the ISO/IEC 27002 [4].

5.3.3 Territoriality of the service

a) The service provider should host the data related to the security incident detection service exclusively within the European Union. In the event that some collection sources are located outside of the European Union, the events originating from these sources will be transmitted to a collector located within the European Union.

5.3.4 Security review

a) The service provider should document and implement a security review plan defining the scope and the frequency of security reviews in accordance with the management of change, policies, and the results of the risk assessment.

b) This security review plan should verify the correct implementation of the information security and protection mechanisms for which the service provider is responsible. This security review plan should include, *at a minimum*:

- the review of logical and physical access controls implemented to protect the devices of the detection service;
- the review of privileges and access rights to the security incident detection service. This review should include the review of administrator and operator accounts *at a minimum* once a month.

c) The service provider should review the security review plan periodically and in the case of any structural changes to the detection service, particularly those concerning its hosting, infrastructure or architecture.

e) The security review plan should include a three-year audit programme including, in particular:

- audits of the configuration of servers and network equipment included in the scope of the detection service. These audits are conducted by sampling and should include all types of equipment and servers present in the information system of the service;
- penetration tests of the service information system (particular attention is required on interconnections);
- if the service benefits from internal developments, audits of the source code concerning the implemented security functions as well as high-risk features (ex: input/output).

f) The audit programme should include at a minimum one external audit per year.

h) The service provider should update the risk treatment plan (see requirement 5.3.1.a) in order to integrate the results of the audits.

i) The service provider should communicate the results of the audits to its management team. The results of the audits should be formally approved in writing by the service provider's management team.

5.3.5 Physical security

a) The service provider should develop and keep up to date the list of persons authorized to access the premises hosting the security incident detection service.

b) The service provider should implement mechanisms enabling it to ensure that only authorized persons can access the premises hosting the security incident detection service.

c) The service provider should implement mechanisms enabling it to log the accesses to the premises hosting the security incident detection service, while ensuring the integrity of the access logs.

5.3.6 Service continuity

a) The service provider should develop and implement for the security incident detection service a service continuity plan, which should address risks regarding its availability. This plan should include several distinct components, including at a minimum the following components:

- system backups;
- configuration backups;
- data backups.

b) The service provider should test the service continuity plan once a year at a minimum.

5.3.7 Service detection service (SOC of SOC)

a) The service provider should implement, for its own account, a security incident detection service, hereinafter referred to as the "service detection service", dealing with the information system of the security incident detection service.

b) The service provider should, on the basis of the risk assessment (see requirement 5.3.1.a), develop a collection strategy, an analysis strategy and a reporting strategy as part of the service detection service.

h) The service provider should develop a process for managing the security incidents of the service. This process should include a report to the commissioning entities upon the occurrence of a security incident on the security incident detection service. The report should specify the nature of the security incident and the measures taken by the service provider to respond to it.

5.3.8 Partitioning of the service information system

a) The service provider should use the security incident detection service information system in circumstances where the sharing of services of various security levels does not lower the security level of the highest level service information system.

b) The service provider should divide the security incident detection service information system into multiple trust zones into which all of the devices involved in the detection service are located:

- collection zone(s) (one or more), comprising all of the devices involved in the collection process, including the central collectors and the systems for storing events and, where necessary, background information;
- analysis zone(s), comprising all of the devices involved in the analysis process, including the technical tools for analysing security incidents;
- reporting zone(s), comprising the commissioning entity's reporting systems, in particular its messaging systems;
- commissioning entity exchange zone(s), comprising all of the devices enabling the secure exchange of information with the commissioning entity, in particular the web portal;
- administrative zone(s), comprising all of the administrative tools and administrators' workstations;
- update zone(s), comprising all of the devices involved in the process of downloading updates for detection service devices;
- operations zone(s), comprising the operators' workstations;
- exchange zones, that are separate for administrators and operators, comprising the devices enabling the transfer of files from and to the security incident detection service information system.

c) The service provider should put in place measures to ensure the partitioning between the different trust zones, in particular by using mechanisms for filtering, authentication and access control.

d) The service provider should create and keep up to date the reference flow matrix for the security incident detection system, together with the associated filtering policy, authorizing only those flows that are strictly necessary for the operation of the security incident detection service.

e) The service provider should implement IP encryption and authentication solutions between these trust zones as soon as the information exchanged between these zones passes through transport networks that are not dedicated to the detection service.

f) The service provider should create and keep up to date a detailed description of the architecture of the security incident detection service information system. This description should identify all of the information system devices and the trust zones of the detection service.

g) The service provider should partition between the commissioning entities:

- the storage and handling systems for events and associated background information;
- the security incident storage and handling systems, the technical analysis tools and the security incident ticket management tools;
- the reports, the web portal and the messaging system.

This partitioning should be achieved through logical access control mechanisms *at a minimum*, and implemented in accordance with the specific operational requirements (rights, privileges, authentication, etc.).

5.3.9 Administration and operation of the service

a) The administrators should manage the security incident detection service devices through dedicated administrative workstations, hosted in the administration zone and separated from the operator workstations.

b) The administration of the security incident detection service devices should be allowed only from the administration zone via the network interfaces of the devices dedicated to administration.

c) The service provider should log each access to the security incident detection service devices and the actions performed.

d) The service provider should put in place a centralized directory that is dedicated to the authentication of administrators and operators of the service, enabling, in particular, authentication on their workstations as well as on all of the detection service devices.

The solution implemented should ensure a strict logical partitioning of administrator and operator populations within the centralized directory, for authentication, authorization and management of identities.

e) The service provider should put in place controls to ensure that administrators manage the security incident detection service devices using administrative accounts dedicated to these tasks and accessible only to administrators.

f) The administrators should not have administrative rights on their administration workstations.

g) The service provider should implement controls to ensure that the administrators and operators can access only those resources that are relevant to their tasks (see annex A).

h) The service provider should apply controls depriving operators of administrative rights on the detection service devices, including on their own workstations.

i) The workstations of administrators and operators should be connected directly exclusively to the security incident detection information system.

In the event of a need to access the Internet or other information systems (the service provider's internal information system, for example), administrators and operators should access them through a special gateway with a special protocol (see requirement 5.3.15.a).

j) The service provider should put in place an exchange zone for transferring files with the outside of the detection service information system as part of the administration or operation of the detection service.

l) The service provider should host within the administration zone a reference time server to ensure that all of the clocks used by the detection service devices are synchronized.

5.3.10 Interconnections with the service information system

a) The only authorized interconnections with the security incident detection service are those with:

- the commissioning entity's information system:
  - for the collection of events and background information via the collection enclave;
  - for the administration of collection devices;
  - for the operation of collection devices;
  - for the sending of non-sensitive information via a non-secured channel, in particular the reporting of security incidents;
  - for the sending of sensitive information via a secured channel, in particular the reporting of full and detailed information related to security incidents;
- the remote administration and operation workstations (see clause 5.3.16) via specific gateways;

- the remote consultation workstations via a specific gateway (see clause 5.3.16);
- the update servers for downloading updates of security incident detection service devices via an update zone (see clause 5.3.11);
- the Internet gateway enabling access with the outside (see clause 5.3.15).

b) The service provider should filter flows at all interconnections with the security incident detection service information system using filtering solutions.

c) The flows at interconnections with the security incident detection service should be encrypted using IPsec VPN encryption and authentication solutions.

The only exceptions to this requirement, subject to the observance of the requirements of clauses 5.3.11 and 5.3.12, are the interconnections with:

- the update servers for downloading updates of security incident detection service devices via the update zone (see clause 5.3.11);
- the commissioning entity's information system for the sending of non-sensitive information, in particular security incident reporting (see clause 5.3.12).

e) The service provider should protect the confidentiality, integrity and authenticity of all information exchanged between the security incident detection service information system and the commissioning entity's information system.

5.3.11 Update zone

a) The service provider can implement an update zone containing one or several relay station(s) connected to a dedicated Internet gateway to enable the downloading of updates of the security incident detection service devices.

NOTE: The term "update" also covers updates from official sources of reference documents used by the detection service devices.

EXAMPLE: Threat monitoring and analysis tools.

b) The service provider should conduct a manual, offline update of the security incident detection service devices that cannot be updated via a relay station.

The following requirements only apply when an update zone has been put in place:

c) The service provider should implement a whitelist filter to ensure that the relay station(s) will only download official updates for the security incident detection service devices from the vendor's official update sources.

d) The service provider should ensure the authenticity and integrity of updates downloaded from authorized update sources.

e) The service provider should configure the filtering solutions (see requirement 5.3.10.b) so that they only allow flows initiated from the relay station(s) to the Internet gateway.

5.3.12 Reporting zone

b) The filtering device (see requirement 5.3.10.b) at the interconnection of the detection service's information system, between the outside of the service information system and the reporting zone, should only authorize flows issued from the reporting zone for the sending of non-sensitive information.

EXAMPLE: Security incident reporting.

5.3.13 Commissioning entity exchange zone

a) The service provider should set up a commissioning entity exchange zone comprising *at a minimum* of:

- a Web portal allowing the viewing and updating of the status of security incidents and the actions undertaken;
- a storage device enabling the commissioning entity to be provided with the context of security incidents detected within its supervised perimeter (associated events and qualification analysis report(s)), enabling the commissioning entity to deposit, if it wishes, information necessary for the qualification of an incident, and enabling the commissioning entity to get access to security indicators.

NOTE: The malicious content analysis tools can be shared between the commissioning entity exchange zone and the collection zone.

For malicious content analysis tools, the service provider should plan for specific handling of files that are encrypted or that cannot be analysed.

The service provider should log the timestamp, the name and the cryptographic fingerprint of all files processed by the malicious content analysis tools.

b) The service provider should dedicate one virtual machine per commissioning entity in order to host an instance of the Web portal and of the storage device for security incidents and reports.

c) The service provider should put in place a directory dedicated to the authentication of the commissioning entity in devices hosted in the commissioning entity exchange zone. The service provider should authenticate the commissioning entity using:

- registered accounts and at least two factors for the authentication of a person in respect of a machine;
- mutual authentication for machine-to-machine authentication.

The service provider should maintain a list of accounts that are authorized to access this zone, together with their associated privileges.

e) The service provider should implement controls to ensure that the commissioning entity can access only those resources that are relevant to its service.

f) The service provider should apply controls depriving the commissioning entity of administrative or operating rights on the detection service devices.

g) The service provider should implement a web application firewall to filter queries to the web portal.

h) The filtering device (see requirement 5.3.10.b) between the commissioning entity exchange zone and the commissioning entity's internal information system should prohibit all flows, save for:

- those between said commissioning entity exchange zone and the consultation enclave within the commissioning entity's internal information system, solely enabling the consultation and updating of the status of incidents and actions undertaken via the web portal and the secure exchange of information between these two zones;
- those between said commissioning entity exchange zone and remote consultation workstations (see requirement 5.3.16.l) solely enabling the consultation and updating of the status of incidents and actions undertaken via the web portal and the secure exchange of information with these workstations.

5.3.14 Collection enclave within the commissioning entity's information system

a) All of the security incident detection service devices that are interconnected with the supervised perimeter (in particular, the collectors) should be positioned within one or more collection enclaves within the commissioning entity's internal information system.

NOTE: For the sake of simplicity, for the remainder of the present document it is assumed that there is only one collection enclave.

b) With the commissioning entity, the service provider should define in the service agreement the responsibilities applicable to the ownership of devices hosted in the collection enclave.

c) The service provider should set out in the service agreement the following responsibilities regarding the administration and operation of the devices hosted in the collection enclave:

- the commissioning entity should be responsible for the administration of the filtering device between this collection enclave and the commissioning entity's internal information system, if any (see requirement 5.3.14.l);

- the service provider should be responsible for the administration and the operation of all other devices hosted in the collection enclave, including the filtering device between this collection enclave and the equipment used for the IPsec encryption and authentication of flows exchanged with the service provider's information system.

e) Information technology hygiene should be applied to the collection enclave, based on common reference frameworks such as the French "Guide d'hygiène informatique" [i.8], the US "CIS Critical Security Controls for Effective Cyber Defense" [i.9] or standards such as the ISO/IEC 27002 [4].

i) The service provider should manage and operate the devices hosted in the collection enclave from the administration and operation zones of its security incident detection service's information system respectively (see requirement 5.3.8.b).

j) The service provider should not under any circumstances have rights on the filtering device between the collection enclave and the commissioning entity's internal information system, if any (see requirement 5.3.14.l).

l) The partitioning of the collection enclave should be performed by:

- a filtering device between this enclave and the information system of the service provider's security incident detection service;

- a filtering device between this enclave and the commissioning entity's internal information system (only for the advanced and full level of implementation).

m) For the advanced and full level of implementation, the filtering device between this collection enclave and the commissioning entity's internal information system should prohibit all flows except those with the supervised perimeter and enabling:

- collection sources hosted on the supervised perimeter to exchange events with this zone;

- some devices within this zone to send command actions to other detection devices on the supervised information system;

- where applicable, the commissioning entity's centralized reference documents) to automatically deposit background information files pertaining to its own information system on the relay station.

EXAMPLE: Configuration management database.

p) An intermediate collector should be implemented under the responsibility of the commissioning entity when the collection sources cannot transmit the events directly to the collectors in the collection zone.

q) The filtering device between the collection enclave and the information system of the service provider's security incident detection service should block all flows except:

- those initiated from this collection enclave to the information system of the service provider's security incident detection service and that only enable the transmission of the events and background information files transferred by the commissioning entity from this enclave towards the collection zone. The service provider should limit as much as possible the number of flows permitting the events and files of this enclave to be transmitted to the detection service information system;

- those initiated from this collection enclave to the information system of the service provider's security incident detection service and that enable to get access to some stored security events, provided cyber risks are mastered by the service provider and accepted by the commissioning entity;

- those enabling the service provider to manage the devices hosted in this collection enclave from the administration zone (see requirement 5.3.8.b);
- those permitting the service provider to operate the devices hosted in this collection enclave from the operation zone (see requirement 5.3.8.b);
- those enabling the updating of the collection enclave's devices from the update zone (see requirement 5.3.8.b).

r) A relay station can be set up in the collection enclave to enable the automatic transmission of background information from the commissioning entity's internal information system.

5.3.15 External access

a) The service provider should implement a special gateway with a special secured protocol to let administrators and operators access to the Internet or other information systems.

EXAMPLE: The service provider's internal information system.

c) All flows exiting the gateway to the Internet should pass through a proxy service followed by a separate output towards the Internet than that used by the commissioning entity's information system.

f) The service provider should timestamp and log the open-source searches carried out.

h) The gateway logs should feed the internal security incident detection service's analysis tools.

i) The collection of the gateway logs should be carried out through one of the security incident detection service's operation exchange zones.

j) The filtering device between the Internet or other information systems and the gateway (see requirement 5.3.10.b) should block all flows except:

- those initiated from the gateway to the proxy service;
- those enabling the gateway to transmit event logs to the internal security incident detection service's operation exchange zone.

5.3.16 Remote access

a) In the case of remote access to the security incident detection service's information system, the service provider should put in place:

- *at a minimum* an administration and operations gateway for the detection service devices;
- where applicable, a gateway dedicated to remote access by the commissioning entity to the commissioning entity exchange zone, which is separate from the administration and operation gateway(s).

b) In the event that access to the commissioning entity exchange zone through remote consultation workstations is authorized, the service provider, together with the commissioning entity, should set out in the service agreement the responsibilities relating to:

- the ownership of remote consultation workstations;
- the management and updating of these devices;
- compliance with the security measures defined in requirement 5.3.16.l.

f) In the event of use of a unique gateway for remote access by administrators and operators, the service provider should implement a solution ensuring the strict separation of:

- administration flows from remote administration workstations to the administration zone;
- operation flows from remote operation workstations to the operation zone.

g) The flows between remote workstations and gateways should be encrypted using IPsec VPN encryption and authentication solutions.

h) The administrators, operators and users of remote consultation workstations should authenticate with a minimum of two factors.

j) Remote workstations should be hardened, configured so that they are only able to communicate exclusively with the dedicated remote access gateway through an encrypted and authenticated IPsec VPN connection, permit only the use of removable media that is authorized by the information systems security policy, and have their entire disks encrypted with an encryption solution.

k) The service provider should make provisions for mechanisms to update and manage remote workstations in the event that it supplies these workstations to the commissioning entity and manages them.

l) The service provider should configure the filtering solutions (see requirement 5.3.10.b) so that they only allow flows:

- initiated from the remote administration workstations to the administration zone (see requirement 5.3.8.b);
- initiated from the remote operation workstations to the operation zone (see requirement 5.3.8.b);
- initiated from the remote consultation workstations to the commissioning entity exchange zone (see requirement 5.3.8.b);
- initiated from the administration zone (see requirement 5.3.8.b) to the remote workstations to manage the workstations that it supplies and manages;
- initiated from the remote workstations to the update zone (see requirement 5.3.8.b) to update the workstations that it supplies and manages.

5.4 Organization of the service provider operating the SOC and Governance

5.4.1 Code of ethics and recruitment

a) The service provider should verify the training, qualifications, and employment references of candidates for the detection service and the truthfulness of their curriculum vitae prior to hiring them.

b) The service provider should require applicants to provide proof that they do not have a criminal record.

d) The service provider should have a code of ethics incorporated into its internal regulations, stipulating, in particular, that:

- the services are performed with loyalty, discretion and impartiality;
- employees use only those methods, tools and techniques that have been approved by the service provider;
- employees undertake to not disclose information to a third party, even if anonymized and decontextualized, which has been obtained or generated as part of the service, without the commissioning entity's formal written authorization;
- employees undertake to alert the service provider to all clearly illegal content discovered during the provision of the service;
- employees undertake to comply with the concerned legislation and regulations in force and with best practices related to their activities.

e) The service provider should ensure that all of its employees sign the code of ethics referred to in the previous requirement prior to performing the service.

f) The service provider should ensure the compliance with the code of ethics and makes provision for disciplinary sanctions for operators, administrators and experts of the detection service who have breached the security rules or the code of ethics.

g) The service provider should develop and implement a plan for raising the awareness of its employees with respect to information system security and the security measures associated with it, as well as to the concerned legislation and regulations in force relating to the security incident detection service.

5.4.2 Organization and management of competencies

a) The service provider should have a team that:

- ensures the performance of, at a minimum, the tasks described in annex A;
- has the skills associated with these tasks.

b) The service provider should define and formally document the exhaustive list of:

- administrator roles for its security incident detection service and associated tasks;
- operator roles for its security incident detection service and associated tasks.

This list should include *at a minimum* the roles of analyst operator and infrastructure administrator (see annex A).

The service provider should prove the compatibility between different operator roles and different administrator roles, in particular with regards to the resources accessed, according to the principles of least privilege and need-to-know.

c) The service provider should employ a sufficient number of employees and may use subcontracting (see clause 5.5.3.7 entitled "Subcontracting") to ensure that the service provided is a qualified service in all respects.

d) The service provider should create and implement a training plan designed for the use of the detection service team and which is adapted to its tasks.

e) The service provider should write and make available to employees guides about the operation and administration of the security incident detection service devices.

f) The service provider should put in place an on-call system enabling it to mobilise a part of its team outside working hours.

g) The service provider should have within its service a CERT or should subscribe to such a service.

i) The service provider should provide the commissioning entity with a remote support service that allows in particular:

- the commissioning entity to declare a suspected or confirmed security incident to the service provider;
- the service provider to help the commissioning entity to resolve production problems related to the devices managed by the service provider;
- the service provider to assist and advise the commissioning entity.

j) The service provider should make the support service accessible via a telephone number or email address.

l) The service provider should appoint a person to serve as an operational point of contact for the commissioning entity. This person is the main contact point with respect to the operational functioning of the security incident detection service and the monitoring of detected security incidents. The service provider should inform the commissioning entity of any change to the person serving as the operational point of contact for the security incident detection service.

m) The commissioning entity should appoint a person to serve as an operational point of contact for the security incident detection service.

n) The persons serving as operational points of contacts should participate in the operational and strategic committee meetings defined in clause 5.4.3.

5.4.3 Operational and strategic committees

5.4.3.1 Operational committee

a) The service provider should put in place and chair an operational committee meeting, in the presence of the commissioning entity, once per quarter *at a minimum*.

c) The operational committee should discuss, *at a minimum*, the following topics:

- an overall assessment of the security incident detection service:
    - a review of the operational indicators (see clause 5.5.1) according to a review cycle for each indicator, agreed upon with the commissioning entity;
    - a review of the detected security incidents;
    - a review of the collection, analysis and reporting strategies;
    - a review of the list of detection rules (see requirement 5.2.1.i);
    - a review of the detection rule status updates (see requirement 5.2.1.j);
- the scope of the security incident detection service:
    - a review of the commissioning entity's context;
    - a review of changes affecting the commissioning entity's information system;
    - a presentation of the evolution of any projects impacting the scope of the service;
    - a review of the list of feared security incidents;
- possible improvements to the security incident detection service:
    - a review of the quality indicators (see clause 5.5.1) according to a review cycle for each indicator, agreed upon with the commissioning entity;
    - an analysis of the operational evolutions in the security incident detection service (evolution of tools, modifications of operational processes, etc.);
    - a presentation of the detection rules that have been created, modified or withdrawn.

d) The service provider should write a report after each operational committee meeting and send it to the commissioning entity for approval. This report should contain *at a minimum* the list of the participants, the decisions taken at the committee meeting and the associated action plan.

e) The service provider should protect the operational committee's report, in particular as regards confidentiality, taking into consideration the level of sensitivity or of classification of its content.

f) The service provider should store and archive operational committee media and associated reports in a specific space within the detection service's infrastructure, with a logical partitioning of data, *at a minimum*, between commissioning entities.

5.4.3.2 Strategic committee

a) The service provider should put in place and chair a strategic committee meeting, in the presence of representatives from the commissioning entity's senior management team, *at a minimum* once a year.

c) The strategic committee should address *at a minimum* the following topics:

- a review of the strategic indicators (see clause 5.5.1);

- a review of the service agreement;
- a review of the reversibility plan;
- a summary presentation of the efficacy of the detection service;
- a review and predictions of threats.

d) The service provider should write a report after each strategic committee meeting and send it to the commissioning entity for approval. This report should contain *at a minimum* the list of the participants and the decisions taken at the committee meeting.

e) The service provider should protect the strategic committee report, in particular as regards confidentiality, taking into consideration the level of sensitivity and of classification of its content.

f) The service provider should store and archive strategic committee media and associated reports in a specific space within the detection service's infrastructure, with a logical partitioning of data, *at a minimum*, between commissioning entities.

5.5 Quality and level of Service

5.5.1 Quality of service

b) The service provider should develop and implement a knowledge capitalization process for the detected security incidents in order to continually improve the efficacy of its detection service.

c) The service provider should define, with the commissioning entity, the operational and strategic indicators for the security incident detection service, by relying notably on the ETSI GS ISI 001-1 [1].

e) The service provider should put in place, *at a minimum*, the following operational activity indicators:

- Management of the detection service supporting infrastructure:
  - ▪ the fill rate of the incident storage systems;
  - ▪ the remaining capacity of the incident storage systems;
  - ▪ the availability rate of the detection service technical devices:
    - commissioning entity exchange zone's web portal;
    - collection enclave collector;
    - system for sending incident reports;
    - technical analysis tools;
    - etc.
- Management of the security of interconnections of the detection service IS:
  - ▪ the number of failed and successful authentication attempts as well as the associated detailed list concerning:
    - access to the commissioning entity exchange zone;
    - access from the remote operation workstations;

      access from the remote administration workstations.
- Management of detection capabilities:
  - ▪ the number of security alerts detected per month;
  - ▪ the number of confirmed incidents following a qualification per month;

    - the number of detection rules implemented in the technical analysis tools;
    - the number of detection rules created, modified or withdrawn per month, by origin of the request (monitoring activity, requested by the commissioning entity, etc.);
    - the classification of the 20 most triggered detection rules.
  - Incident management:
    - the number of new incident tickets opened per month;
    - the number of security incident tickets closed per month;
    - the number of open tickets accumulated per month;
    - the minimum, average, and maximum time between the creation and the closure of a ticket;
    - the number of incidents created according to the criticality of the incident.
  - Event management:
    - the number of events not recognized and therefore not taken into account by the technical analysis tools;
    - the rate of events not recognized and therefore not taken into account by the technical analysis tools;
    - the number of collection sources per type of source equipment;
    - the number of collectors;
    - the number of events collected per day and per month;
    - the number of events collected by collector per day and per month;
    - the number of events sent to the storage system per day and per month;
    - the fill rate of each of the event storage systems, including the collectors in the enclave;
    - the remaining capacity of each of the event storage systems, including the collectors in the enclave;
    - the holding capacity of collectors if communication is not possible (for example, when the network link is broken) with the superior collector (in volume and in time).
  - Reporting management:
    - the number of accounts authorized to access the web portal and able to access the commissioning entity's information;
    - the number of web portal access accounts created per month;
    - the number of web portal access accounts deleted per month.

f) The service provider should put in place, *at a minimum*, the following operational efficacy indicators:

  - Management of detection capacities:
    - the average time taken to update the detection rules following a request by the commissioning entity;
    - the average time taken to search for an indicator of compromise, during an *a posteriori* search, in the storage system, by type of indicator of compromise.
  - Incident management:
    - the average time taken to qualify incidents, by type of incident and level of criticality.

- Event management:
    - the minimum, average, and maximum time between the generation of an event by the collection source and its storage in the event storage systems.
- Reporting management:
    - the minimum, average, and maximum time between the detection of a security event and the reporting of an associated incident, by level of criticality.

g) The service provider should put in place, *at a minimum*, the following strategic indicators:

- Management of the security of interconnections of the detection service IS:
    - the evolution of the number of abnormalities and incidents observed concerning the various external accesses to the detection service IS.
- Management of the detection service supporting infrastructure:
    - the monthly evolution of the availability rate of the detection service's technical devices:
        - commissioning entity exchange zone web portal;
        - collection enclave collector;
        - system for sending incident reports;
        - technical analysis tools;
        - etc.
- Management of detection capabilities:
    - the deviations identified in relation to the various SLAs set out.
- Incident management:
    - the evolution of the average time taken to handle incident tickets, by criticality, per month;
    - the evolution of the number of open accumulated incident tickets, by criticality, per month;
    - the number of confirmed incidents per month within the scope of the commissioning entity's detection service.
- Event management:
    - the evolution of the collection coverage rate of the logs for the equipment identified in the collection strategy.

h) The service provider should establish and keep up to date a process for measuring the indicators which describes, for each of the described operational and strategic indicators, the methods and means used by the service provider to measure the indicator.

5.5.2 Reversibility

a) The service provider should develop, with the commissioning entity, a reversibility plan for the security incident detection service enabling the restoration of service by the commissioning entity or another service provider.

b) The reversibility plan should contain, *at a minimum*, the following elements:

- a comprehensive inventory of the information and material to be restored;
- the duration of the reversibility;
- the people involved and the actions that each of them is required to perform;

- the formats of the information to be restored;
- the means of restoration.

The service provider should be able, if the commissioning entity so requests, to restore the stored security events, together with the specific detection rules, to the commissioning entity of the service.

c) The duration of the reversibility should be *at a minimum* of three months.

e) The service provider should maintain the security incident detection service in operational condition during the implementation of the reversibility plan.

f) The service provider should destroy all information relating to the commissioning entity at the end of the execution of the reversibility plan, with the exception of information that the commissioning entity has authorized it to retain (see requirement 5.5.3.4.a).

5.5.3 Service agreement

5.5.3.1 Terms of delivery of the service

a) The service agreement should:

- describe the scope and objectives of the service to be provided, the security incident detection service, including in particular the event, incident, and reporting management activities;
- describe the technical and organizational measures implemented by the service provider as part of the performance of the service;
- describe the location of storage and data processing, as well as the location of the operation and administration of the detection service;
- define the deliverables expected as part of the performance of the service, the intended recipients, and their level of sensitivity or classification, together with the associated modalities;
- describe the methods of communication between the service provider and the commissioning entity that will be used in providing the service;
- define the rules of ownership of the elements protected by intellectual property, such as the deliverables, the tools and the detection rules specifically developed by the service provider as part of the provision of the service;
- describe the process of registering and handling complaints concerning the service made by the commissioning entity or by third parties, as well as the procedures for filing a complaint.

5.5.3.2 Organization of the service

a) The service agreement should:

- stipulate that the service provider appoint a contact person for the commissioning entity, who will be in charge of ensuring the operational monitoring of the service;
- stipulate that the service provider and the commissioning entity specify the names, roles, responsibilities, rights and need to know of the individuals involved in the provision of the service. This clause is particularly important if there is a security incident that should not be made public;
- stipulate that the service provider does not involve employees who do not have a contractual relationship with it, did not sign the code of ethics or who have been the subject of a criminal offense;
- stipulate whether the service provider allows remote access by administrators or operators to the security incident detection service's information system.

5.5.3.3 Responsibilities

a) The service agreement should:

- stipulate that the service provider inform the commissioning entity in the event of any deficiency in the service agreement;
- stipulate that the service provider inform the commissioning entity in the event that a security incident is detected on the security incident detection service's information system, and the maximum time permitted to transmit the information following an incident;
- stipulate that the service provider perform only those actions that are strictly in line with the objectives of the service;
- stipulate that the commissioning entity possess all of the ownership rights and access rights required for the scope of the service (information systems, physical media, etc.) or that it has obtained the agreement of any third party, including its service providers or partners, whose information systems are included within the scope of the service;
- stipulate that the commissioning entity meet all of the legal requirements necessary for the service and in particular those relating to the collection and analysis of information;
- define the responsibilities and the precautions to be observed by all parties regarding the potential risks related to the service, especially with regard to the confidentiality of the information collected and analysed and the availability and integrity of the commissioning entity's information system;
- stipulate that the service provider have professional liability insurance covering any damage caused to the commissioning entity and in particular to its information system as a result of its service, specifying the coverage of the insurance and including the insurance certificate;
- define the responsibilities between the service provider and the commissioning entity with respect to the collection enclaves within the commissioning entity's information system, in accordance with requirements 5.3.14.b and 5.3.14.c;
- stipulate that the service provider have in place a change management procedure for its own information system;
- stipulate that the service provider have in place a process for the continuous improvement of the efficacy of its detection service, based on, in particular, the operational indicators set out in clause 5.5.1.

5.5.3.4 Confidentiality and information protection

a) The service agreement should:

- identify the level of sensitivity or classification of the security incident detection service implemented by the service provider;
- identify the level of sensitivity or classification of the supervised perimeter;
- stipulate that the service provider only collect and analyse the information that is strictly required for the smooth operation of the service;
- stipulate that the service provider not disclose any information relating to the service to third parties without the formal written authorization of the commissioning entity;
- specify the clauses relating to the ethical requirements of the service provider and include the service provider's code of ethics;

- specify the terms of access, storage, transmission, reproduction, destruction and restoration of the information collected and analysed by the service provider. If necessary, the service provider should define the terms, in collaboration with the commissioning entity, in accordance with the types of information:
    - stipulate that the service provider may, except in the case of a formal written refusal by the commissioning entity, retain certain types of information related to the service, and that it specifies these types of information (e.g. detection: rules, malware, attack scenarios, indicators of compromise, etc.);
    - stipulate that the service provider anonymize and decontextualize (deleting any information that could be used to identify the commissioning entity, any information of a personal nature, etc.) all of the information that the commissioning entity authorizes it to retain or to transmit to a third party;
    - stipulate that the service provider, except in the event of written formal refusal by the commissioning entity, transmit to a local information security authority the anonymized and decontextualized information, together with their level of sensitivity and their conditions of use;
    - stipulate that the service provider should protect the data transmitted to a third party, in confidentiality, in accordance with the level of sensitivity or classification;
    - stipulate that the service provider destroy all information about the commissioning entity at the end of the service or at the term of the retention period, whichever comes first, with the exception of information that the commissioning entity has authorized it to retain;
- define the frequency with which the service provider shall test the backup and restoration plan of the security incident detection service.

5.5.3.5 Reversibility

a) The service agreement should specify the terms of implementing a reversibility plan for the service: duration, implementation, any additional costs, etc. (see clause 5.5.2).

5.5.3.6 Laws and regulations

a) The service agreement should:

- specify the governing law for the service agreement;
- specify the technical and organizational measures implemented by the service provider in order to comply with applicable legislation, in particular those concerning:
    - personal data;
    - breach of trust;
    - confidentiality of private correspondence;
    - medical confidentiality;
    - invasion of privacy;
    - fraudulent access to or maintenance in an information system;
    - professional secrecy;
- specify any specific regulatory and legal requirements to which the commissioning entity is subject and, in particular, those relating to its sector of activity;
- establish the measures to be put in place by the service provider in the context of judicial, civil or arbitration proceedings. In this case, it is recommended to have recourse to a legal expert;

- define the retention period for information related to the service, and in particular for the collected events and the detected security incidents. If necessary, distinctions in retention periods may be made based on the different types of information. The minimum retention period, in accordance with European legislation and regulations in force, should be:
    - six months for collected events;
    - the entire duration of the service for security incidents and for the associated context (associated events and qualification analysis report(s)) and reports.

5.5.3.7 Subcontracting

a) The service agreement should specify that the service provider may subcontract, where necessary, all or part of the service to another service provider, provided that:

- there is a service agreement between the service provider and the subcontractor;
- the use of subcontracting is known to, and has been formally accepted in writing by, the commissioning entity;
- the subcontractor complies with the requirements of the present document.

5.5.3.8 Service level

a) The service agreement should:

- define the operational and strategic indicators used to measure the service level of the service;
- define the operating hours for the security incident detection service;
- stipulate that the service provider should hold operational and strategic committee meetings in the presence of the commissioning entity;
- specify the objectives and the frequency of these committee meetings;
- identify, for the service provider and the commissioning entity, the level of human resources dedicated to managing the detection rules and, in particular, their creation and modification;
- define the frequency with which the service provider transmits the detection rule status report to the commissioning entity;
- stipulate that the service provider should make a support service available to the commissioning entity and the hours during which this support service will be in operation;
- specify the type of support service (phone, email, etc.), its availability, and the level of sensitivity or classification of information that can be exchanged;
- specify the level of competence of the employees who are on call, in accordance with the needs of the commissioning entity and in the event that on-call services are put in place.

Annex A (informative): Tasks and skills of the service provider's SOC's employees

A.1 Analyst operator

A.1.1 Tasks

- identifying, analysing and qualifying the security incidents;
- supporting the investigation teams in handling the incidents.

A.1.2 Skills

- knowledge of protocols and network architectures;
- log analysis experience (systems or applications);
- knowledge of information systems' security;
- network traffic analysis skills;
- mastery of the business functionalities of detection service devices, including searching for events in the event storage systems.

A.2 Infrastructure administrator

A.2.1 Tasks

- managing the technical infrastructure devices of the security incident detection service;
- maintaining the technical infrastructure devices of the security detection service in operational conditions;
- updating and maintaining the technical infrastructure devices of the security incident detection service in secure condition.

A.2.2 Skills

- command of security incident detection service devices, particularly those related to event, incident and reporting management.

A.3 Architecture expert

A.3.1 Tasks

- designing and maintaining an architecture for the detection service;
- integrating or developing and maintaining the components of the detection service;
- integrating or developing and maintaining new correlation engines.

A.3.2 Skills

- operation of probes and event log correlation tools knowledge;
- mastery of common protocols for the operation of the services;
- good knowledge of the most common applications and their security (web servers, mail servers, database servers, DNS servers, proxies, firewalls, etc.);
- good knowledge of the global network architecture and the security of its components (routers, switches, etc.).

A.4 Collection and log analysis expert

A.4.1 Tasks

- contributing to defining and reviewing the collection strategy;
- contributing to defining the commissioning entity's logging policy by type of equipment (operating systems, infrastructure services, network equipment, security equipment, etc.);
- providing support to infrastructure administrators in the deployment of detection systems (tests, maintaining the systems in operational condition, support for analysts using these systems, etc.);
- participating in the development and maintenance of event correlation mechanisms and rules.

A.4.2 Skills

- in-depth knowledge of system, network and applications event log analysis;
- knowledge of event log correlation tools and techniques;
- knowledge of log analysis or security monitoring systems (security information and event management - SIEM).

A.5 Detection expert

A.5.1 Tasks

- expanding internal knowledge bases with information on threats, vulnerabilities and malicious code;
- managing detection rules throughout their life cycle (conception, implementation, documentation, modification, disabling, etc.);
- ensuring the continuous improvement of service processes.

A.5.2 Skills

- knowledge of vulnerabilities;
- knowledge of command and control protocols;
- knowledge of operational modes of attacks and malicious codes;
- expertise in detection rules development tools.

A.6 Access rights manager

A.6.1 Tasks

- manage the creation and deactivation of accounts for the service's operation tools;
- manage the attribution, modification and removal of access rights to the service's operation tools.

A.6.2 Skills

- proficiency in administering he service's operation tools;
- knowledge of detection service roles and associated rights.

Annex B (informative): Recommendations for Commissioning Entities

B.0 Introduction

This annex lists recommendations for commissioning entities in relation to security incident detection services.

B.1 Before the start of the service

a) It is recommended that the commissioning entity appoint a person to serve as an internal operational point of contact responsible for being the main point of contact with the service provider with respect to the operational functioning of the security incident detection service and for monitoring the detected security incidents.

b) It is recommended that the commissioning entity retain an approved audit service provider for information system security to draw up the risk assessment for establishing the list of feared security incidents and associated impacts (see requirement 5.2.1.a) from which the collection, analysis and reporting strategies are developed.

c) It is recommended that the commissioning entity update its risk assessment each time that there is a change in its infrastructure or its services, and that it communicate these changes and their consequences to the service provider.

d) It is recommended that the commissioning entity identify in the service agreement any specific legal and regulatory requirements to which it is subject, including those related to its sector of activity.

e) It is recommended that the commissioning entity require to the service provider that the frequency of the operational committee meetings (see clause 5.4.3.1), which should be set out in the service agreement, be once a quarter.

f) It is recommended that the commissioning entity require to the service provider that the frequency of the strategic committee meetings (see clause 5.4.3.2), which should be set out in the service agreement, be once a year.

g) It is recommended that the commissioning entity require to the service provider that the frequency of the detection rule status updates (see requirement 5.2.1.j), which should be set out in the service agreement, be once a month.

h) It is recommended that the commissioning entity choose the strategic and operational indicators which should be set out in the service agreement and which make it possible to measure the service level of the provided service among the ETSI GS ISI 001-1 [1] indicators.

i) It is recommended that the commissioning entity use ETSI GS ISI 002 [3] to define the format and content of the security incident tickets.

j) It is recommended that the commissioning entity require the service provider to include in the collection strategy (see requirement 5.2.2.a) the deployment of probes at each of the interconnections of its information system, and, in particular, those interconnections with:

- the Internet;
- third-party information systems (partners, subcontractors, etc.);
- the commissioning entity's other information systems with a lower or more vulnerable security classification or sensitivity level.

l) It is recommended that the commissioning entity:

- synchronize the collection sources hosted on its information system with a single time source;
- develop and implement an event logging policy.

m) It is recommended that the commissioning entity put in place a crisis management process in case of the detection of a major security incident within its information system.

n) It is recommended that the commissioning entity require the service provider to integrate into the reporting strategy (see requirement 5.2.3.f) specific reports in the event that major security incidents within its information system are detected.

o) It is recommended that the commissioning entity apply information technology hygiene to access the Web portal, based on common reference frameworks such as the French "Guide d'hygiène informatique" [i.8], the US "CIS Critical Security Controls for Effective Cyber Defense" [i.9] or standards such as the ISO/IEC 27002 [4].

B.2 During the provision of the service

a) It is recommended that the commissioning entity regularly transmit to the service provider, throughout the whole of the period that the service is provided, all of the information needed for the service provider to create new detection rules specific to the commissioning entity's needs.

b) To this end, the commissioning entity may, in particular, submit the results of tests for vulnerabilities and intrusions conducted on its information system.

c) It is recommended that the commissioning entity inform the service provider of any evolution of its information system that could impact the efficacy of the security incident detection service.

d) It is recommended that the commissioning entity put in place a change management process enabling it to continuously inform the service provider of any changes to its supervised information system (configuration, settings, software versions, etc.).

Annex C (informative): Definition of the basic level of implementation

Table C.1 describes the basic level of implementation of the present document (subset).

Table C.1

Requirement	Basic level (Subset)
Clause 5.1	
a, b, c	X
d	
f, g, h, i, k	X
l, m	
n	X
Clause 5.2.1	
a, c	X
d, f	
g	X
h, i, j, m, n	
q	X
r, s, t	
v, w	X
x	X
y, z, aa, bb, cc, dd, ee	X
Clause 5.2.2	
a, b, c	X
f	
g	X
h	
i, n, o, r, s, t	X
u, v	
w	X
Clause 5.2.3	
a	X
b	
c, d, e, f, h, j, k	X
l	
Clause 5.3.1	
a, c, e	X
Clause 5.3.2	
b	X
Clause 5.3.3	
a	X
Clause 5.3.4	
a, b, c, e, f, h, i	X
Clause 5.3.5	
a, b	X
c	
Clause 5.3.6	
a, b	X
Clause 5.3.7	
a, c, h	
Clause 5.3.8	
a, b, c, d, e, f, g	X
Clause 5.3.9	
a, b, c	X
d	
e	X
f, g	
h, i, j, l	X
Clause 5.3.10	
a, b, c, e	X

Requirement	Basic level (Subset)
Clause 5.3.11	
a, b, c, d, e	
Clause 5.3.12	
b	
Clause 5.3.13	
a, b, c, e, f, g, h	
Clause 5.3.14	
a, b, c, e, i, j	X
l, m, p, q, r	
Clause 5.3.15	
a, c, j	X
f, h, i	
Clause 5.3.16	
a, f, g, h, j, l	X
b	
Clause 5.4.1	
a, b, d, e, f, g	X
Clause 5.4.2	
a, b, c, d, e	X
f	
g, i, j, l, m, n	X
Clause 5.4.3.1	
a, c, d, e, f	
Clause 5.4.3.2	
a, c, d, e, f	X
Clause 5.5.1	
b, c, e	X
h	
Clause 5.5.2	
a, b, c, d, e, f	X
Clause 5.5.3	
1a, 2a, 3a, 4a, 5a, 6a, 7a, 8a	X

Annex D (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Gerard Gaudin, G²C, Chairman of ISG ISI

Other contributors:
Herve Debar, Institut Telecom, Vice-Chairman of ISG ISI

Arnaud Fillette, Thales, Secretary of ISG ISI

And in alphabetical order:

Jan deMeer, SmartSpaceLabs.eu

Axel Rennoch, Fraunhofer Fokus

Philippe Saadé, ESI-Group

Julien Saugeot, BNP Paribas

History

Document history		
V1.1.1	December 2018	Publication