Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

**Prime Minister**

**The French Networks and Information Security Agency**

*Agence nationale de la sécurité des systèmes d'information*

# Security incident detection service providers
*Prestataires de détection des incidents de sécurité*

# Requirements reference document
*Référentiel d'exigences*

*Version 2.0 dated 21 December 2017*

*This document is a courtesy translation of the initial French document "Prestataires de detection des incidents de sécurité – référentiel d'exigences", available at https://ssi.gouv.fr. In case of conflicts between these two documents, the latter is considered as the only reference.*

| VERSION HISTORY | | | |
|---|---|---|---|
| **DATE** | **VERSION** | **DOCUMENT HISTORY** | **AUTHOR** |
| 20/03/2014 | 0.1 | *Draft version presented in Working Group Meeting 1* | ANSSI |
| 16/04/2014 | 0.2 | *Draft version presented in Working Group Meeting 2* | ANSSI |
| 03/06/2014 | 0.3 | *Working version prepared for Working Group Meeting 3* | ANSSI |
| 25/06/2014 | 0.4 | *Working version prepared for Working Group Meeting 4* | ANSSI |
| 22/07/2014 | 0.5 | *Working version prepared for Working Group Meeting 5* | ANSSI |
| 05/09/2014 | 0.6 | *Working version prepared for Working Group Meeting 6* | ANSSI |
| 10/10/2014 | 0.7.4 | *Working version prepared for internal revisions by ANSSI* | ANSSI |
| 25/11/2014 | 0.8 | *Working version prepared for internal revisions by ANSSI* | ANSSI |
| 17/12/2014 | 0.9.1 | *Version published for public call for comments* | ANSSI |
| 06/10/2015 | 1.0 | *Revised version following the call for comments* | ANSSI |
| 10/02/2017 | 1.01 | *Working version prepared for Working Group Meeting 3 to review the reference document* | ANSSI |
| 10/05/2017 | 1.02 | *Working version prepared for Working Group Meeting 4 to review the reference document* | ANSSI |
| 08/06/2017 | 1.03 | *Working version prepared for internal revisions by ANSSI* | ANSSI |
| 21/12/2017 | 2.0 | *First applicable version.*<br>Principal modifications:<br>• Clarification of qualification procedures<br>• Clarification of information protection requirements<br>• Clarification of the scope of audits<br>• Addition of new communication possibilities<br>• Complete review of quality indicators | ANSSI |

Comments on this document should be sent to:

**Agence nationale de la sécurité des systèmes d'information**

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

qualification@ssi.gouv.fr

# CONTENTS

# I. Introduction

## I.1. Overview

### I.1.1. Context

The growing interconnection of networks and the requirements of dematerialisation 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 attacker can attempt to exploit in order to enter and remain inside an information system in order to steal, alter or destroy its information assets.

The use of security incident detection systems contributes to the protection of information systems from the threats of cyber-attacks. Human, technical and organisational resources can be concentrated within a cyber-security operations centre[1] dedicated to the security incidents detection. Depending on the challenges, needs and resources of the commissioning entity, this centre can be internal[2] or external[2]. In the latter, the pooling of resources can have positive effects, such as the sharing of information on threats and detection rules.

When a cyber-security operations centre is compliant with the "state of the art", particularly in terms of expertise and tooling, and is precisely adapted to the needs of the commissioning entity, it helps preventing severe security incidents or, when such incidents occur, to limit their consequences by making it possible to take rapid remediation actions that can be carried out by a qualified security incident response service provider (*Prestataire de réponse aux incidents de sécurité*—PRIS).

Concentrating and pooling detection capabilities make cyber-security operations centres a prime target for attackers. Therefore, special attention should be paid to protecting its infrastructure.

### I.1.2. Purpose of the document

This reference document lists the requirements applicable to a security incident detection service provider (*Prestataire de détection des incidents de sécurité*—PDIS), hereinafter referred to as "the service provider".

Its purpose is to enable the qualification of this category of service providers in accordance with the terms set out in section III.

It covers both types of security incident detection services: internal and external.

It provides assurance to the commissioning entity regarding the competences of the service provider and its staff, the quality of services for the security incident detection carried out and the confidence that the commissioning entity can place in the service provider, in particular with regard to confidentiality.

In particular, this reference document enables the qualification of providers likely to intervene, for the security incident detection, for sectors of critical importance concerned by the application of security rules provided for under the Military Planning Act (*Loi de programmation militaire*) [Author's note: A qualified incident detection service provider may help for the application of security rules from other frameworks such as the NIS[3] directive]. It can also be used, in the interest of adopting best practices, independently of any regulatory framework.

[1] Hereinafter referred to as the "security incident detection service".

[2] See section III.1 Approval methods

[3] EU Network and Information Security Directive, see EU 2016/1148

It does not exclude either the application of national laws and regulations e.g. on the protection of National defence secrets [IGI_1300], or the application of general rules imposed on service providers as professionals with particular regards to their duty to advise their commissioning entities.

### I.1.3. Document structure

Section I is the introduction to this reference document.

Section II describes the activities to which this reference document relates.

Section III presents the qualification methods, which attest to the compliance of the security incident detection service providers against applicable requirements.

Section IV presents the requirements applicable to service providers.

Appendix 1 presents references in terms of laws, regulations, standards and other documents cited in this reference document.

Appendix 2 presents the tasks and competences expected from the service provider's employees.

Appendix 3 presents the recommendations for the commissioning entities when contracting with security incident detection service providers.

Appendix 4 presents illustrative diagrams of architectures which comply with the reference document.

Appendix 5 presents the rules for using a feed aggregator

## I.2. Document identification

This reference document is named "Security incident detection service providers – requirements reference document" (*Prestataires de détection des incidents de sécurité – référentiel d'exigences*). It can be identified by its name, version number and date of update.

## I.3. Definitions and acronyms

### I.3.1. Acronyms

The acronyms used in this reference document are:

**ANSSI** The French Networks and Information Security Agency (*Agence nationale de la sécurité des systèmes d'information*)

**CERT-FR** The French national Computer Emergency Response Team (*Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*)[4]

**PASSI** Audit service provider for information system security (*Prestataire d'audit de la sécurité des systèmes d'information*)

**PDIS** Security incident detection service provider (*Prestataire de détection des incidents de sécurité*)

**PRIS** Security incident response service provider (*Prestataire de réponse aux incidents de sécurité*)

[4] http://www.cert.ssi.gouv.fr

### I.3.2. Definitions

The definitions below are primarily taken from the standards series [ISO27000] and especially [ISO27035] on the management of security incidents as well as the French national digital security strategy [STRAT_NUM].

**Administrator –** member of the detection service with privileged rights ensuring 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 centralisation of security events originating from various collection sources (example: syslog server, SIEM solution collector). In the context of this service, local collectors are all collectors installed in the information system of the commissioning entity, and central collectors are the collectors used for centralising 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. 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 specialised supplier, or it can have been created specifically for the commissioning entity.

**Efficacy** – the level of achievement of planned activities and the expected results.

**Event related to information security** – identified occurrence of a system, service or network status indicating a possible breach of information security, policy or a failure of security controls, or a previously unknown situation that can be relevant to information security.

**Information system** – organised 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 organisational 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. 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.

**Qualify a security incident** – determine the nature and severity of a security incident.

**Reporting** – act of informing the commissioning entity of the occurrence of a security incident jeopardising its information system.

**Risk related to information security** – scenario describing the effect of uncertainty on the activity and expressed as a combination of consequences of an event related to information security and the likelihood of its occurrence.

**Security incident** – single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and/or threatening information security.

**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. 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 this reference document.

**Severity of a security incident –** level of impact of the security incident affecting the information system of the commissioning entity.

**State of the art** – set of publicly accessible best practices, technologies and reference documents (and the information that that can be inferred from them) relating to the security of information systems. 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 another entity with all or part of the execution of a contract concluded with the commissioning entity.

**Supervised perimeter –** all or part of the information system of the commissioning entity, which is object of the security incident detection service.

**Third party** – person or organisation that is recognised as independent from the service provider and the commissioning entity.

**Vulnerability** – weakness of an asset or control that can be exploited by one or more threats.

# II. General description of the detection service

## II.1. Activities of the security incident detection service

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

- Incident management, meaning all technical and organisational means for identifying and qualifying a security incident on the basis of collected events. Storing and capitalising on security incidents in order to improve the service are also part of this activity;
- Event management, meaning all technical and organisational means for ensuring the collection and storage of security events;
- Notification management, meaning all technical and organisational 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. Those are handled by the security incident response service providers (PRIS).

## II.2. Architecture of the detection service information system

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

The diagram below is a simplified representation of a typical architecture for a security incident detection service, provided for informational purposes only. Appendix 4 presents more detailed representations.

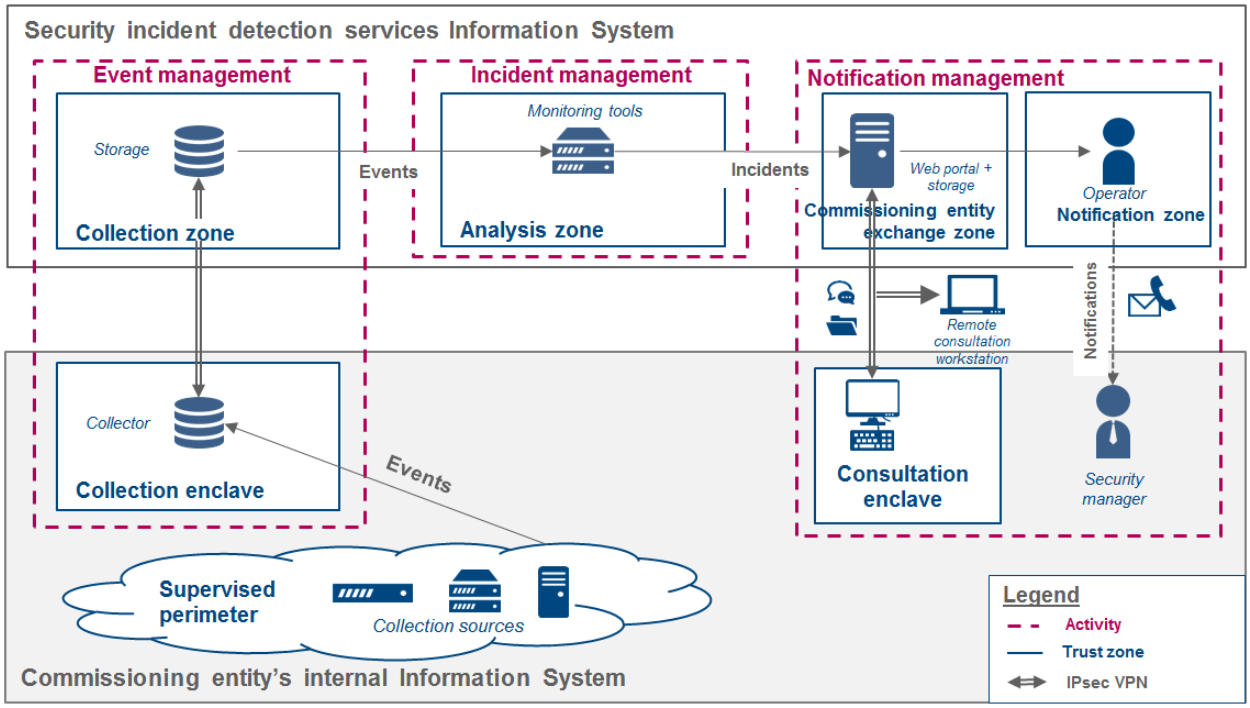



*Figure 1: Simplified representation of a typical architecture for a security incident detection service*

The information system of a detection service is organised 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;
- Notification zone(s), comprising all reporting systems of the commissioning entity, 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 separated for administrators and operators, comprising all devices enabling the external transfer of the security incident detection service information system files.

Furthermore, several specific zones, which are external to the information system of the detection service, shall be set up (due to interaction with the latter):

- Internet zone(s), comprising the workstations provided to detection service operators and administrators to access the Internet or other information systems than that of the service;
- Specific zones set up within the internal information system of the commissioning entity, hereinafter referred to as "enclaves". *At a minimum*, two enclaves shall be put in place:
    - A collection enclave to host the collection devices deployed by the detection service within the commissioning entity. In particular, the collection enclave contains one or more local collectors, the role of which is to centralise security events arising within the supervised perimeter;
    - A consultation enclave for the hosting of devices accessing the commissioning entity exchange zone.

A more detailed diagram, depicting all of these zones, and complying with the expected partitioning requirements, is provided in Appendix 4.

## II.3. Scope of application of the requirements of the reference document

Section IV.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.

Section IV.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 centralisation of events on a collector, etc.;
- Requirements regarding the notification management activity, including the means of reporting, the consultation of incident tickets, etc.

Section IV.3 lists the requirements relating to information protection, including encryption, filtering between trust zones, role separation between administrators and operators, etc.

Section IV.4 lists the requirements relating to the organisation of the service provider and the governance of the service, including the establishment of a code of ethics and recruitment, the content of operational and strategic committee meetings, etc.

Section IV.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.

# III. Qualification of security incident detection service providers

## III.1. Qualification methods

The reference document contains the requirements and recommendations for security incident detection service providers.

The qualification of a service provider is performed in accordance with the qualification process for a trusted service provider [QUAL_SERV_PROCESS] and attests to the compliance of the service provider with the requirements of the reference document.

Service providers shall comply with all requirements in order to obtain the qualification.

The recommendations of the reference document are provided as a matter of best practice and are not subject to verification.

This document also provides recommendations for commissioning entities in Appendix 3. These recommendations are not subject to verification in the qualification process.

*Note: All the legal references in this section are originated from French law.*

A security incident detection service is "internal" in the two following cases:[5]

- If it is provided exclusively to commissioning entities having a legal relationship, within the meaning of Articles L. 233-1 et seq. of the Commercial Code, with a legal entity and performed by a provider also having a legal relationship of the same nature with the same legal entity;
- If it is provided to commissioning entities belonging to the same administrative authority, within the meaning of Article I-1 of Order No. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and performed by a provider belonging to the same administrative authority.

Otherwise, the security incident detection service is considered as "external".

For internal security incident detection services, qualification is granted:

- In the 1st case, to the legal entity providing the detection service to which all commissioning entities of the detection service are legally linked, within the meaning of Articles L. 233-1 et seq. of the Commercial Code, or to one commissioning entity of the detection service in particular;
- In the 2nd case, to the administrative authority, within the meaning of Article I-1 of Order No. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities to which all commissioning entities of the detection service, as well as the provider itself, belong.

For external incident detection services:

- If the provider and any of its potential subcontractors implement all human, technical and organisational resources necessary for compliance with the reference document, and the commissioning entity only implements the security measures under its responsibility with regards to enclaves (section IV.3.14 and IV.3.15), qualification is granted to the provider.
- If all or part of the human, technical and organisational resources necessary for compliance with the requirements contained in the reference document is implemented by a commissioning entity[6], qualification is granted to the commissioning entity.

[5] Typical examples: a detection service created by a commissioning entity for its own individual use, or a detection service provided by a subsidiary of a group for the benefit of other subsidiaries of the same group.

[6] Save for the requirements on enclaves within the information system of the commissioning entity, for which the responsibilities are specifically set out in sections IV.3.14 and IV.3.15.

Whether the security incident detection service is internal or external, subcontractors that implement all or part of the human, technical and organisational resources necessary for compliance with the requirements of this reference document are assessed to ensure that they comply with the requirements placed upon them.

## III.2. Scope of the qualification

In order to be qualified, service providers shall meet all the requirements of this reference document.

In order to be qualified under Decree no. 2015-350 [D_2015_350], service providers shall comply with the requirements set out in [PDIS_LPM], in addition to the requirements defined in this reference document [PDIS_LPM].

Services that meet all the requirements of this reference document are considered to be qualified services according to the meaning of the reference document.

Services that meet all the requirements of this reference document and the additional requirements defined in [PDIS_LPM] are considered to be qualified services within the meaning of Decree No. 2015-350 [D_2015_350][PDIS_LPM].

Qualified service providers retain the ability to provide services outside of the scope for which they are qualified, but cannot, in this case, advertise those services as qualified.

A qualified security incident detection service can be combined with other complementary services (development, integration of security products, etc.) without losing the benefit of the qualification. A qualified security incident detection service provider can, for example, be qualified for other trust service provider categories (PASSI, PRIS).

## III.3. Warning

The use of non-qualified incident detection services, i.e. which do not fully comply with the requirements of this reference document, can potentially leave the commissioning entity vulnerable to certain risks, such as the leakage of confidential information, being compromised by another of the service provider's commissioning entities, and loss or unavailability of service. Accordingly, in the case of a non-qualified service, it is recommended that the commissioning entity request from its service provider a document listing all the requirements of this reference document that are not covered as part of its service, in order to understand the risks to which the commissioning entity is exposed.

# IV. Requirements to be met by the service provider

## IV.1. General requirements

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

b) The service provider shall comply with the laws and regulations in force within the national territory of France.

c) The service provider shall describe the organisation of the security incident detection activity it provides to the commissioning entity.

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

e) The service provider shall take responsibility for the activities it performs on behalf of the commissioning entity in connection with the service it provides, and in particular for any damages caused to the commissioning entity. In this respect, the service provider shall specify the types of damages involved and the terms under which the responsibilities are shared in the service agreement, taking into account any and all outsourced activities.

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

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

i) The service provider shall 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.

j) The service provider shall provide the service impartially, in good faith and with respect towards the commissioning entity, its employees and its infrastructure.

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

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

m) The service provider shall inform the commissioning entity when the commissioning entity is required to report a security incident to a government authority and shall provide assistance in this process if the commissioning entity asks for it.

n) The service provider shall establish a service agreement with the commissioning entity. The service agreement shall comply with the requirements of section IV.5.3 and shall be formally approved, in writing, by the commissioning entity before the service is performed.

## IV.2. Activities of the security incident detection service

### IV.2.1. Incident management

a) The service provider shall 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. The service provider shall recommend the commissioning entity to update its risk assessment in the event of a change in its infrastructure.

b) The service provider shall be able to take into account *at a minimum* the following categories of feared security incidents:

- Exploitation of a vulnerability;
- Privilege escalation;
- Data exfiltration;
- Viral propagation;
- Use of a persistence mechanism;
- Denial of service;
- Unauthorised access to a resource;
- Identity theft;
- Actions not complying with the security policy of the commissioning entity.

c) It is recommended that the service provider take into account the list of security incidents and their origins in Annex B of [ISO27035], as well as that of [ETSI_ISG_ISI].

d) The service provider shall 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 IV.2.1.a). The analysis strategy shall be reviewed with the commissioning entity during the operational committee meetings defined in section IV.4.3.

e) The service provider shall define, with the commissioning entity, the rules for the classification of security incidents within the meaning of [IGI_1300] and [II_901] and formalise these rules in the analysis strategy. These classification rules shall be reviewed, along with the analysis strategy, at the operational committee meetings defined in section IV.4.3.

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

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

- The list of security incidents that are feared by the commissioning entity;
- Knowledge bases acquired from vendors and specialist 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 and control protocols;
    - The monitoring of the modes of operation for attacks and malicious code;
- Contextual elements specific to the commissioning entity;
- Rules provided directly by the commissioning entity, previously assessed by the service provider (proper functioning in relation to the behaviour to detect, impact on performance, alert correction, usability of alerts produced, etc.);
- Security incidents detected with any other commissioning entities.

h) The service provider shall develop and implement a marking policy for detection rules. This policy shall 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 level of sensitivity or classification, within the meaning of [IGI_1300] and [II_901], of 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 shall 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 shall 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 shall specify, for every rule identified by its identifier and its version number:
- The date(s) on which the detection rule was implemented in the technical analysis tools;
- If the service provider has conducted an *a posteriori* analysis with this detection rule (see requirement IV.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 shall 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 shall therefore be marked as withdrawn and shall 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 shall be specified in the list.

j) The service provider shall 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.).

k) The service provider shall protect the detection rule status report, in particular as regards confidentiality, taking into consideration the level of sensitivity or the level of classification of the detection rules.

l) It is recommended that the service provider send the detection rule status report to the commissioning entity once a week.

m) The service provider shall implement in the technical analysis tools in use all of the detection rules identified in the list set out in requirement IV.2.1.i) except for the rules marked as withdrawn.

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

Following an addition of this type, the service provider shall 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.

o) The service provider shall, in the event that it is difficult or impossible to implement a detection rule, notify the commissioning entity as soon as possible, and specify the reasons for the failure to implement the rule. The maximum period between the decision to implement the detection rule and the report of failure of the implementation to the commissioning entity shall be defined in the service agreement.

p) For each commissioning entity, the service provider shall establish and keep up-to-date the list of rule additions in the technical analysis tools, by including the outcome of the implementation (implemented/failure) and the reasons for failure to implement, where applicable.

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

r) The service provider shall establish with the commissioning entity a severity 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 severity.

s) It is recommended that the service provider use the severity scale for information security incidents from Annex C of [ISO27035].

t) 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 exercise the utmost caution when carrying them out. Thus, it shall take into account the marking of detection rules indicating the possibility of carrying out such a search, or not (see IV.2.1 h).

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

u) The service provider shall use, wherever possible, internal information bases taken from open sources (RIPE bases, offline antiviral platforms, DNS resolution bases, etc.) in order to restrict internet searches as much as possible.

v) The service provider shall 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 (capitalisation and use of background knowledge on the supervised IS).

w) The service provider shall create a ticket for each security incident detected and make it available to the commissioning entity. *At a minimum*, the security incident ticket shall 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 level of classification of the incident [IGI_1300] [II_901]*;*
- The severity 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 shall define the format of the security incident tickets together with the commissioning entity.

y) It is recommended that the service provider use the security incident ticket format set out in [ETSI_ISG_ISI].

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

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

cc) The service provider shall 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 national territory (see requirement IV.1.b).

dd) The analysis strategy shall ensure that for each detection rule that is created or modified, the service provider conducts an *a posteriori* analysis, meaning an analysis of all of the 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 shall be able to search, *at a minimum*, for the following types of indicators of compromise:

- 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 shall 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.

### IV.2.2. Event management

a) The service provider shall develop, together with the commissioning entity, and implement a collection strategy based on the list of feared security incidents (see requirement IV.2.1.a). The collection strategy shall be reviewed with the commissioning entity at the operational committee meetings defined in section IV.4.3.

b) The collection strategy shall 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 shall be, *at a minimum*, capable of collecting events from the following collection sources:

- Security equipment: network firewalls, application firewalls, encrypters, probes including those qualified by ANSSI at the appropriate level, 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, virtualisation, 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.

d) It is recommended that the service provider be able to collect events arising from the equipment comprising the industrial information systems: industrial programmable automatons, industrial fire-walls, industrial switches and industrial routers.

e) The service provider shall be able, *at a minimum*, to handle logs for each collection source identified in requirement IV.2.2.c) of the events identified in Annex A of ANSSI's technical note on the implementation of a logging system [NT_JOURNAL].

f) The service provider shall, 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 shall 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 shall be defined in the service agreement.

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

i) The service provider shall recommend to the commissioning entity that it integrates 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 other information systems of the commissioning entity with a lower or more vulnerable security classification or sensitivity level.

j) The service provider shall recommend to the commissioning entity that it implement probes qualified by ANSSI at the appropriate level which will be used in accordance with the conditions of their qualification. These probes shall receive network traffic input feeds via TAP type equipment that is entirely passive and cannot be managed remotely.

k) It is recommended that TAP-type equipment which feed probes be qualified by ANSSI at the appropriate level and be used in accordance with the conditions of their qualification.

l) The service provider shall be able to operate probes receiving traffic via TAP type equipment that is entirely passive and cannot be managed remotely.

Note: If it wishes to use an intermediate feed aggregator between TAPs and the probe(s), the service provider shall dedicate the equipment to the aggregate function and comply with the rules on the use of a feed aggregator specified in Appendix 5.

m) It is recommended that the service provider be able to operate the probes dedicated to industrial information systems.

n) The events from collection sources shall be centralised on one or more collectors[7] located in the collection enclave described in requirement IV.3.15.

o) The collection enclave collector shall 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.

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

- The date(s) on which the filtering rule was introduced into the collectors;
- The date(s) on which the filtering rule was withdrawn from the collectors.

This list shall make it possible to establish a historical record of the filtering rules, enabling the identification of rules that were active at a given time or over a given period. A filtering rule that has

[7] For the sake of simplicity, for the remainder of this document, it is assumed that there is only one collector.

been withdrawn from collectors shall therefore be marked as withdrawn and shall 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 shall be specified in the list.

q) The service provider shall send to the commissioning entity, *at a minimum* once a month, a filtering rule status report that presents:

- The number of filtering rules created, modified or withdrawn from the collectors;
- The identifier and description of each rule that has been created, modified or withdrawn from the collectors;
- The reason for the creation, modification or withdrawal of the filtering rule (e.g.: creation, modification or withdrawal at the request of the commissioning entity, etc.).

It is recommended that the service provider send the filtering rule status report to the commissioning entity once a week.

r) The collector shall 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 shall guarantee the storage capacity of the collector in the service agreement. The evolution of the collector's storage capacity shall be monitored and presented to the commissioning entity at the operational committee meetings defined in section IV.4.3.

s) The service provider shall have a centralised 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 shall be synchronised with a single time source (see requirement IV.3.9.l).

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

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

w) The service provider shall 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 IV.2.1.ee), subject to compliance with legislation and regulations in force within the national territory (see requirement IV.1.b).

## IV.2.3. Notification management

a) The service provider shall have two information channels available for the commissioning entity:

- A notification channel (see requirement IV.2.3.b);
- A secure channel, in particular for the exchange of detailed information (see requirement IV.2.3. l).

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

- Email;
- Short text message (SMS);
- Telephone.

c) The service provider shall develop, together with the commissioning entity, and implement a security incident notification strategy enabling the provider to notify the commissioning entity in the event that a security incident is detected. The notification strategy shall be reviewed with the commissioning entity at the operational committee meetings defined in section IV.4.3.

d) The notification strategy shall 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 severity.

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

f) The service provider shall recommend to the commissioning entity that it include specific notifications in the notification strategy in the occurrence that major security incidents within its information system are detected.

g) The notifications shall contain only the following information: the identification number of the incident ticket.

The notifications shall not under any circumstances contain detailed information about the security incident, and especially about the collected events or the detection rules that detected the security incident, the part of the information system of the commissioning entity that was affected by the security incident, or the impact of the security incident.

h) The service provider shall centralise all the notifications in a notification storage system. The following information shall be stored: date and time of the notification, notification method, recipient(s) of the notification, content of the notification, including in particular the incident ticket number.

Note: The above information relating to notifications can be included in incident tickets.

i) The service provider shall be able to provide the security incident ticket and the associated background (associated events and analysis report(s)) at the origin of a notification.

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

k) The service provider shall put in place a process for managing the storage capacity for the notifications 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 national territory (see requirement IV.1.b).

l) The service provider shall 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.

## IV.3. Information protection

### IV.3.1. Information systems security policy

a) The service provider shall develop a risk assessment and the associated risk treatment plan covering the full scope of the security incident detection service. The assessment and the treatment plan shall be formally approved in writing by the management of the service provider.

b) The risk assessment shall include a list of feared incidents within the scope of the security incident detection service. This list shall include, *at a minimum*:

- Intrusion attempts on the detection service information system from one of its interconnections (see section IV.3.10);
- Rebound attempts between commissioning entities' information systems via the detection service information system ;
- Privilege escalation attempts by security incident detection service operators or administrators;
- The loss of communication with one or more of the items of equipment of the detection service;
- Viral infections arising from malware encountered in the context of the service.

c) The service provider shall 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.

d) The service provider shall make the risk treatment plan available to the commissioning entity upon request. The service provider shall indicate to the commissioning entity the safety conditions related to the transmission and storage of the risk treatment plan.

e) The service provider shall develop and implement an information systems security policy based on the risk assessment. This policy shall specify the levels of qualification or national qualification of the various pieces of equipment involved (levels considered "appropriate" in this reference document).

f) It is recommended that the service provider be certified [ISO27001] for the entirety of the scope of the security incident detection service.

### IV.3.2. Levels of sensitivity or classification

a) The service provider shall, *at a minimum*, comply with the rules established by ANSSI relating to protective measures for information systems treating sensitive unclassified defence information at the Restricted (*Diffusion Restreinte* [IGI_1300] [II_901], particularly for information identified as sensitive in the risk assessment (see requirement IV.3.1.a).

b) The service provider shall apply *at a minimum* the Standard Level of ANSSI's guide to information technology hygiene [HYGIENE] to the security incident detection service information system.

c) The detection service information system shall be accredited *at a minimum* at the Restricted level (*Diffusion Restreinte*) to supervise the information systems of the commissioning entities that are not classified defence.

d) The detection service information system shall be accredited *at a minimum* at the same classification level as the classified defence information systems of the commissioning entity. [IGI_1300].

e) It is recommended that the service provider use the process described in the [HOMOLOGATION] guide for accreditation of the security incident detection service information system.

f) It is recommended that the service provider have recourse to a qualified audit service provider for information system security (PASSI) to perform a qualified information security audit for the accreditation process.

### IV.3.3. Territoriality of the service

a) The service provider shall host and process 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 shall be transmitted to a collector located within the European Union.

b) The service provider shall operate and manage the security incident detection service exclusively from within the European Union.

### IV.3.4. Security review

a) The service provider shall 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 shall verify the correct implementation of the information security and protection mechanisms for which the service provider is responsible. This security review plan shall 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 shall include the review of administrator and operator accounts *at a minimum* once a month.

c) The service provider shall review the security review plan *at a minimum* once a year and in the case of any structural changes to the detection service, particularly those concerning its hosting, infrastructure or architecture.

d) The service provider shall include the list of feared security incidents (see requirement IV.3.1.b) in the security review plan in order to test these scenarios.

e) The security review plan shall 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 shall 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 shall include *at a minimum* one qualified audit per year conducted by a qualified audit service provider for information system security (PASSI). The appointed PASSI service providers and the service provider shall be legally independent from each other.

g) The service provider shall protect the results of the audits to, *at a minimum*, the same level of sensitivity or classification as the audited information system.

h) The service provider shall update the risk treatment plan (see requirement IV.3.1.a) in order to include the results of the audits.

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

### IV.3.5. Physical security

a) The service provider shall create and keep up to date the list of persons authorised to access the premises hosting the security incident detection service.

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

c) The service provider shall implement mechanisms enabling it to log the accesses to the premises hosting the security incident detection service.

d) The service provider shall define and implement controls enabling it to ensure the confidentiality and integrity of the access logs for the premises hosting the detection service using solutions nationally approved by ANSSI [CRYPTO_B1], [CRYPTO_B3] at the appropriate level and used in accordance with the conditions of their approval.

### IV.3.6. Backups

a) The service provider shall develop and implement a backup and restoration plan for the devices of the security incident detection service. The backup plan shall include several distinct components, including *at a minimum* the following components:

- System backups;
- Configuration backups;
- Data backups.

b) The service provider shall test the backup and restoration plan once a year *at a minimum*.

c) The service provider shall define and implement controls to ensure the confidentiality and integrity of the backups performed, at the same level as that for which the detection system was approved. The backup device shall be dedicated and located in an administration zone that provides for the partitioning of the backup activities, in compliance with the backup plan.

d) It is recommended that the service provider complies with all of the controls and recommendations regarding securing backups found in [ISO27002].

### IV.3.7. Service detection service

a) The service provider shall 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 shall comply with the requirements of section IV.3 for the service detection service, except for the requirements of IV.3.7.a) and the requirements of sections IV.3.13, IV.3.14 and IV.3.15.

c) The service provider shall, on the basis of the risk assessment (see requirement IV.3.1.a) and the associated list of feared security incidents (see requirement IV.3.1.b), develop a collection strategy, an analysis strategy and a notification strategy as part of the service detection service.

d) It is recommended that, depending on the results of the risk assessment and the list of associated feared security incidents, the service provider isolate the service detection service (separation of human, technical and organisational resources).

e) The service provider shall deploy one or more probes on the security incident detection service information system. These probes shall, in particular, make it possible to monitor each of the interconnections of the security incident detection service information system. These probes shall be collection sources for the service detection service.

f) The probes deployed by the service provider as part of the service detection service shall be qualified by ANSSI at the appropriate level and used in accordance with the conditions of their qualification.

These probes shall receive network traffic input feeds via TAP type equipment that is entirely passive and cannot be managed remotely.

Note: If it wishes to use an intermediate feed aggregator between Taps and the probe(s), the service provider shall dedicate the equipment to the aggregate function and comply with the rules on the use of a feed aggregator specified in Appendix 5.

g) It is recommended that the service provider sets up a transfer of the logs of its security incident detection system's devices towards a dedicated trust zone in accordance with the requirements of [NT_JOURNAL]. In this case, it is recommended that the dedicated trust zone implement access control prohibiting access by administrators and operators of the security incident detection service from the administration and operation zones respectively.

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

i) It is recommended that the service provider puts in place a crisis management process in the case of the detection of a major security incident within its detection service.

j) It is recommended that the service provider uses tools enabling it to conduct static or dynamic analysis of suspicious files.

k) If, for suspicious files, the service provider uses static or dynamic analysis tools which rely on resources hosted on the Internet, the service provider shall perform these operations outside of the security incident detection service information system

l) It is recommended that the service provider uses a qualified security incident response service provider (PRIS)[8] to perform the analysis of the suspicious files through a digital investigation service on a restricted perimeter for the analysis of malware. In this case, the security incident detection service provider shall ensure that the scope of the qualification of the security incident response service provider includes this type of service.

### IV.3.8. Partitioning of the service information system

a) The service provider shall dedicate the security incident detection service information system to the qualified services or use it in circumstances where the sharing of services does not lower the security level of the service information system. All other services shall be performed on an information system that is physically partitioned from the service information system.

b) The service provider shall 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;
- Notification zone(s), comprising the reporting systems of the commissioning entity, 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;

[8] The catalogue of qualified information security incident response service providers (PRIS) is published on ANSSI's website.

- 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, which 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 shall 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 shall create and keep up to date the reference flow matrix for the security incident detection system, together with the associated filtering policy, authorising only those flows that are strictly necessary for the operation of the security incident detection service.

e) The service provider shall 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. These IP encryption and authentication solutions shall be nationally approved by ANSSI at the appropriate level and used in accordance with the conditions of their approval.

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

g) The service provider shall 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 notifications, the web portal and the messaging system.

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

### IV.3.9. Administration and operation of the service

a) The administrators shall manage the security incident detection service devices through dedicated administrative workstations, hosted in the administration zone[9] and distinct from the operator workstations.

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

c) The service provider shall log each access to the security incident detection service devices and the actions performed[10].

[9] It is recommended that ANSSI's technical note on the secure administration of information systems be followed [NT_ADMIN].

[10] It is recommended that ANSSI's technical note on the implementation of a logging system be followed [NT_JOURNAL].

d) The service provider shall put in place a centralised 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 shall ensure a strict logical partitioning of administrator and operator populations within the centralised directory, for authentication, authorisation and management of identities.

e) The service provider shall 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 shall not have administrative rights on their administration workstations.

g) The service provider shall implement controls to ensure that the administrators and operators can only access those resources that are relevant to their tasks (see Appendix 2).

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

i) The workstations of administrators and operators shall be connected 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 shall have a separate workstation that is distinct from their normal workstation within a zone outside of the detection service information system, called "Internet zone" (see requirement IV.3.16.a).

j) The service provider shall 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. This exchange zone shall be separate for administrators and operators. The service provider shall meet the requirements for the exchange zone set out in the "Exchange system" (*Système d'échange*) section of the [NT_ADMIN] technical note.[NT_ADMIN]

Note: malicious content analysis tools can be shared between the exchange zone used by administrators and that used by operators.

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

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

k) All exchanges related to the detection service from administration or operations workstations shall be performed using encryption and authentication protocols that comply with ANSSI's requirements [CRYPTO_B1], [CRYPTO_B3].

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

m) The service provider shall ensure that its reference time service is synchronised by using a nominal channel and a stand-by channel, through the following channels:

- Via Internet: for this, the service provider shall set up a relay in the update zone;
- Via antenna, for this the service provider shall set up a dedicated antenna-type device (radio, GPS).

n) It is recommended that the time sources used by the service provider for any given commissioning entity are the same as those used by the commissioning entity itself.

o) The use of different time sources by the commissioning entity and the service provider can lead to issues in the sequencing of logs, particularly between the logs forwarded to the information system

via collectors and the logs forwarded by probes. The service provider shall be aware of the potential delta between the two sources.

### IV.3.10. Interconnections with the service information system

a) The only authorised interconnections with the security incident detection service are those with:
   - The information system of the commissioning entity:
     - For the collection of events and background information via the collection enclave;
     - For the administration of collection devices and, where necessary, consultation devices[11];
     - For the operation of collection devices;
     - For the sending of non-sensitive information via a non-secure channel, in particular the notification of security incidents;
     - For the exchange of sensitive information with the consultation enclave via a secure channel, in particular the exchange of information that is necessary for qualification, and interaction with the web portal for the follow-up of security incidents;
   - The remote administration and operation workstations (see IV.3.17) via specific gateways;
   - The remote consultation workstations via a specific gateway (see IV.3.17);
   - The update servers for downloading updates of security incident detection service devices via an update zone (see IV.3.11);
   - The Internet zone enabling the exchange of files with the outside through exchange zones (see IV.3.16).

b) The service provider shall filter flows at all interconnections with the security incident detection service information system using filtering solutions qualified by ANSSI at the appropriate level and used in accordance with the conditions for their qualification.

   Note: in addition, the interconnections of the detection service information system shall comply with the network partitioning requirements of Annex 2 of the Interministerial instruction on the protection of sensitive information systems [II_901] (see requirement IV.3.2.c).

c) The flows at interconnections with the security incident detection service shall be encrypted using IPsec encryption and authentication solutions nationally approved by ANSSI at the appropriate level and used in accordance with the conditions of their approval.

   The only exceptions to this requirement, subject to the observance of the requirements of sections IV.3.11 and IV.3.12, are the interconnections with:
   - The update servers for downloading updates of security incident detection service devices via the update zone (see IV.3.11);
   - The information system of the commissioning entity for the sending of non-sensitive information, in particular security incident reporting (see IV.3.12).

d) The equipment used to encrypt and authenticate interconnections shall be dedicated to qualified security incident detection services or used in circumstances in which the sharing of services does not reduce the security level of the detection service information system.

e) The service provider shall protect the confidentiality, integrity and authenticity of all information exchanged between the security incident detection service information system and the information

[11] Only if the commissioning entity authorises the service provider to manage one or more devices hosted in this zone (see requirement IV.3.14.b).

system of the commissioning entity using solutions nationally approved by ANSSI at the appropriate level and used in accordance with the conditions of their approval.

### IV.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 shall 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 shall 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 shall ensure the authenticity and integrity of updates downloaded from authorised update sources, and put in place certificates based on ANSSI's rules and recommendations on the management of keys used in [CRYPTO_B2] cryptographic mechanisms.[CRYPTO_B2]

e) The service provider shall configure the filtering solutions (see requirement IV.3.10.b) so that they only allow flows initiated from the relay station(s) to the Internet gateway.

### IV.3.12. Notification zone

a) When electronic messaging systems are used as part of the management of reports, these systems shall be dedicated to reporting activities in the context of qualified services or those which do not reduce the security level of the service information system, and shall be hosted in the notification zone.

b) The filtering device (see requirement IV.3.10.b) at the interconnection of the detection service information system , between the outside of the service information system and the notification zone, shall only authorise flows issued from the notification zone for the sending of non-sensitive information (example: security incident reporting).

### IV.3.13. Commissioning entity exchange zone

a) The service provider shall 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)), and enabling the commissioning entity to deposit, if it wishes, information necessary for the qualification of an incident.

   The service provider shall meet the requirements for the exchange zone set out in the "Exchange system" (*Système d'échange*) section of the [NT_ADMIN].

   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 shall plan for specific handling of files that are encrypted or that cannot be analysed.

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

b) The service provider shall dedicate one physical or 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 shall 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 shall 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 shall maintain a list of accounts that are authorised to access this zone, together with their associated privileges.

d) It is recommended that the service provider implement an authentication process for the commissioning entity exchange zone devices based on digital certificates issued by electronic certificate service providers qualified by ANSSI at a RGS *** level and therefore involving the use of cryptographic media qualified by ANSSI at an enhanced level.

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

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

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

h) The filtering device (see requirement IV.3.10.b) between the commissioning entity exchange zone and the internal information system of the commissioning entity shall prohibit all flows, save for:

- Those between said commissioning entity exchange zone and the consultation enclave within the internal information system of the commissioning entity, 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 IV.3.17.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;
- Those enabling the service provider to manage the devices hosted in the consultation enclave from the administration zone (see requirement IV.3.8.b) [12];
- Those enabling the updating of devices hosted in the consultation enclave from the update zone[12] (see requirement IV.3.8.b).

## IV.3.14. Consultation enclave within the information system of the commissioning entity

a) All devices able to access the commissioning entity exchange zone from the internal information system of the commissioning entity shall be placed within one or more[13] consultation enclaves within said information system.

b) With the commissioning entity, the service provider shall define in the service agreement the responsibilities applicable to:

[12] Only if the commissioning entity authorises the service provider to manage one or more devices hosted in this enclave (see requirement IV.3.14.b).

[13] For the sake of simplicity, for the remainder of this document it is assumed that there is only one consultation enclave.

- The ownership of the devices hosted in the consultation enclave;
- The management and updating of these devices;
- Compliance with the security controls set out in requirements IV.3.14.c) to IV.3.14.g).

c) The consultation enclave shall be accredited *at a minimum* at the Restricted level (*Diffusion Restreinte*) [IGI_1300] [II_901].

Note: The entity (service provider or commissioning entity) responsible for accreditation shall request that the other entity provide proof of the implementation of the measures which are incumbent upon the latter and include them in the accreditation file.

d) It is recommended that the service provider have recourse to an information system security audit service that has been qualified by a PASSI to carry out the audit for approval.

e) The workstations used by the commissioning entity to access the exchange zone shall be dedicated for this purpose and hosted in the consultation enclave (in the event of remote access to the commissioning entity exchange zone, the requirements of section IV.3.17 shall be complied with).

f) Consultation enclave workstation users shall not have administration rights on their workstations.

g) The partitioning of the consultation enclave shall be performed by:

- A filtering device between this enclave and the information system of the service provider's security incident detection service;
- Filtering and flow disruption devices between this enclave and the internal information system of the commissioning entity, in accordance with the network partitioning requirements of Annex 2 of the Interministerial instruction on the protection of sensitive information systems[II_901].

h) The filtering device between this consultation enclave and the internal information system of the commissioning entity shall block all flows except those initiated from the consultation enclave to the internal information system of the commissioning entity.

i) It is recommended that a nationally approved diode be placed at the interconnection between the consultation enclave and the internal information system of the commissioning entity, and used in accordance with the conditions for its approval, to ensure the unidirectional nature of flows from the consultation enclave to the internal information system of the commissioning entity.

## IV.3.15. Collection enclave within the information system of the commissioning entity

a) All of the security incident detection service devices that are interconnected with the supervised perimeter (in particular, the collectors) shall be positioned within one or more [14] collection enclaves within the internal information system of the commissioning entity.

b) With the commissioning entity, the service provider shall define in the service agreement the responsibilities applicable to:

- The ownership of devices hosted in the collection enclave;
- Compliance with the security controls defined in requirements IV.3.15.d) and IV.3.15.s).

c) The service provider shall 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 shall be responsible for the administration of the filtering device between this collection enclave and the internal information system of the commissioning entity (see IV.3.15.l);

[14] For the sake of simplicity, for the remainder of this document it is assumed that there is only one collection enclave.

- The service provider shall 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.

d) The collection enclave shall host only those devices that make it possible to ensure the provision of the security incident detection service, i.e.:

   - The devices involved in monitoring (probes, Taps, aggregators);
   - Event collection devices (local collectors);
   - The relay station enabling the transfer of the background information of the commissioning entity;
   - The filtering devices that ensure the partitioning of this enclave (see requirement IV.3.15.l);
   - The devices that make it possible to protect the confidentiality and authenticity of the information exchanged between the enclave and the security incident detection service information system.

e) The collection enclave shall be accredited *at a minimum* at the Standard Level of ANSSI's information technology hygiene guide [HYGIENE]. The approval procedure for this enclave shall include an information system security audit performed by a PASSI.

   Note: the entity (service provider or commissioning entity) responsible for approval shall request that the other entity provide proof of the implementation of the measures which are incumbent upon the latter and include them in the approval file.

g) It is recommended that the requirements of section IV.3.2 covering the protection of information within the service provider's security incident detection service be applied to this enclave.

h) The devices involved in the monitoring chain (probes, Taps and aggregators) shall be connected by a physically dedicated network link.

i) The service provider shall manage and operate the devices hosted in the collection enclave from the administration and operation zones of its security incident detection service information system respectively (see requirement IV.3.8.b).

j) The service provider shall not under any circumstances have rights on the filtering device between the collection enclave and the internal information system of the commissioning entity (see requirement IV.3.15.l).

k) The service provider shall apply the recommendations set out in ANSSI's technical note on the implementation of a logging system [NT_JOURNAL].

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

   - A filtering device between the enclave and the internal information system of the commissioning entity;
   - A filtering device between this enclave and the information system of the service provider's security incident detection service.

m) The filtering device between this collection enclave and the internal information system of the commissioning entity shall prohibit all flows except those initiated from the supervised perimeter towards this zone and enabling:

   - Collection sources hosted on the supervised perimeter to transfer events to this zone for a collector, save for command actions to software of the supervised information system;
   - Where applicable, the centralised reference documents of the commissioning entity (example: configuration management database) to automatically deposit background information files pertaining to its own information system on the relay station.

n) It is recommended that a nationally approved diode be placed at the interconnection between the collection enclave and the internal information system of the commissioning entity, and used in accordance with the conditions for its approval, to ensure the unidirectional nature of flows from the collection enclave to the internal information system of the commissioning entity.

o) The collectors shall be configured exclusively in listening mode for collection sources. No flow shall be initiated from the collectors to the collection sources.

p) It is recommended that an intermediate collector 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 shall 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 shall 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 enabling the service provider to manage the devices hosted in this collection enclave from the administration zone (see requirement IV.3.8.b);
- Those permitting the service provider to operate the devices hosted in this collection enclave from the operation zone (see requirement IV.3.8.b);
- Those enabling the updating of the collection enclave's devices from the update zone (see requirement IV.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 internal information system of the commissioning entity.

Where applicable, the relay station shall be configured exclusively in listening mode for the centralised reference documents of the commissioning entity. No flows are to be initiated by the relay station towards the internal information system of the commissioning entity.

The following requirement shall only apply when such a relay station has been put in place.

s) The service provider shall put in place an exchange system within its collection zone, enabling the transfer of files from the collection enclave's relay station to the detection service information system. The service provider shall meet the requirements for the exchange zone set out in the "Exchange system" (*Système d'échange*) section of the [NT_ADMIN].

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

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

The service provider shall set up the logging of the name and cryptographic fingerprint of all files passing through the malicious content analysis tools.

## IV.3.16. Internet zone within the service provider's information system

a) The service provider shall set up, outside of the detection service information system, an Internet zone containing dedicated workstations used by operators and administrators to access the Internet or other information systems (for example, the service provider's internal information system). The Internet zone shall be disconnected from the information system of the commissioning entities.

b) The workstations hosted in the Internet zone shall be physically dedicated to the Internet zone (dedicated to the access to other information systems than the detection service information system).

c) All flows exiting the Internet zone to the Internet shall pass through a proxy service followed by a separate output towards the Internet than that used by the information system of the commissioning entity.

d) It is recommended that the service provider carry out open-source searches, in particular on the Internet, from demarcated internet links (anonymous and dynamic IP with periodic change, no entry in who-is bases, etc.), so that the attacker cannot identify the service provider.

e) The Internet zone shall be accredited *at a minimum* at the Standard Level of ANSSI's guide to information technology hygiene [HYGIENE].

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

g) It is recommended that the service provider log each access to the devices hosted in the Internet zone as well as the actions carried out, and apply the recommendations set out in ANSSI's technical note on the implementation of a logging system [NT_JOURNAL].

h) It is recommended that the Internet zone logs are transferred to the internal security incident detection service analysis tools.

i) If the Internet zone logs are collected, such collection shall be carried out through one of the security incident detection service's operation exchange zones or through the implementation of a collection enclave, as is the case for a normal commissioning entity.

j) The filtering device between the Internet zone and the detection service information system (see requirement IV.3.10.b) shall block all flows except:

- Those initiated from the Internet zone to exchange zones and enabling the workstations hosted in the Internet zone to deposit or collect files in the exchange zones;
- If the Internet zone logs are collected, those enabling the devices hosted in the Internet zone to transmit event logs to the internal security incident detection service's exchange zone.

### IV.3.17. Remote access

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

- *At a minimum* an administration and operations gateway[15]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 authorised, the service provider, together with the commissioning entity, shall 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 controls defined in requirements IV.3.17.e) to IV.3.17.l).

c) It is recommended that separate administration and operation gateways be put in place.

d) The remote workstations used by administrators and operators shall be dedicated to the qualified services and to any service that is compliant with the requirements of section IV.3 – Information protection.

[15] In compliance with the technical note [NT_ADMIN].

e) The remote workstations used by the commissioning entity shall be dedicated to accessing the commissioning entity exchange zone.

f) In the event of use of a unique gateway for remote access by administrators and operators, the service provider shall 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 shall be encrypted using IPsec encryption and authentication solutions nationally approved by ANSSI at the appropriate level and used in accordance with the conditions of their approval.

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

i) It is recommended that, for remote access, the service provider implements an authentication process based on digital certificates issued by electronic certificate service providers qualified by ANSSI at a RGS *** level and therefore involving the use of cryptographic media qualified by ANSSI at an enhanced level.

j) Remote workstations shall be hardened, configured so that they are only able to communicate exclusively with the dedicated remote access gateway through an encrypted and authenticated IPsec connection, permit only the use of removable media that is authorised by the information systems security policy, and have their entire disks encrypted with an encryption solution nationally approved by ANSSI *at a minimum* at the Restricted level (*Diffusion Restreinte*) and used in compliance with the conditions of its approval.

k) The service provider shall 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 shall configure the filtering solutions (see requirement IV.3.10.b) so that they only allow flows:

- Initiated from the remote administration workstations to the administration zone (see requirement IV.3.8.b);
- Initiated from the remote operation workstations to the operation zone (see requirement IV.3.8.b);
- Initiated from the remote consultation workstations to the commissioning entity exchange zone (see requirement IV.3.8.b);
- Initiated from the administration zone (see requirement IV.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 IV.3.8.b) to update the workstations that it supplies and manages.

## IV.4. Organisation of the service provider and governance

### IV.4.1. Code of ethics and recruitment

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

b) The service provider shall require applicants to provide proof that they do not have a criminal record (“*bulletin n° 3 du casier judiciaire*”).

c) The operators, administrators and specialists in the detection service shall have a contractual relationship with the service provider or one of its subcontractors in the event the service provider subcontracts part of its activities.

d) The service provider shall 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 anonymised and decontextualized, which has been obtained or generated as part of the service, without the formal written authorisation of the commissioning entity;
- 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 national legislation and regulations in force and with best practices related to their activities.

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

### IV.4.2. Organisation and management of competences

a) The service provider shall have a team that:

- Ensures the performance of, *at a minimum*, the tasks described in Appendix 2;
- Has the skills associated with these tasks.

b) The service provider shall 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 shall include *at a minimum* the roles of analyst operator and infrastructure administrator (see Appendix 2).

The service provider shall 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 shall employ a sufficient number of employees and may use subcontracting (see section IV.5.3.7 entitled “Subcontracting”) to ensure that the service provided is a qualified service in all respects.

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

f) It is recommended that the service provider put in place an on-call system enabling it to mobilise a part of its team outside working hours.

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

h) It is recommended that the CERT be referenced by the French national CERT.

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

k) The service provider shall implement mechanisms enabling it to exchange information with the commissioning entity *at a minimum* at the Restricted (*Diffusion Restreinte*) level via the support service.

l) The service provider shall 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 shall inform the commissioning entity of any change to the person serving as the operational point of contact for the security incident detection service.

m) It is recommended that the commissioning entity 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 shall participate in the operational and strategic committee meetings defined in section IV.4.3.

## IV.4.3. Operational and strategic committees

### *IV.4.3.1. Operational committee*

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

b) It is recommended that the service provider hold an operational committee meeting once a month.

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

- An overall assessment of the security incident detection service:
  - A review of the operational indicators (see section IV.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 notification strategies;
  - A review of the list of detection rules (see requirement IV.2.1.i);
  - A review of the detection rule status updates (see requirement IV.2.1.j).
- The scope of the security incident detection service:
  - A review of the context of the commissioning entity;
  - A review of changes affecting the information system of the commissioning entity;
  - 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 section IV.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 shall write a report after each operational committee meeting and send it to the commissioning entity for approval. This report shall 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 shall 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 shall store and archive operational committee media and associated reports in a specific space within the detection service infrastructure, with a logical partitioning of data, *at a minimum*, between commissioning entities.

#### *IV.4.3.2. Strategic committee*

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

b) It is recommended that the service provider hold a strategic committee meeting twice a year.

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

- A review of the strategic indicators (see section IV.5.1);
- A review of the service agreement;
- A review of the reversibility plan;
- A summary presentation of the effectiveness of the detection service;
- A review and predictions of threats.

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

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

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

## IV.5. Quality and level of service

### IV.5.1. Quality of service

a) It is recommended that the service provider be [ISO9001] certified in respect of the scope of the security incident detection service.

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

c) The service provider shall define, with the commissioning entity, the operational and strategic indicators for the security incident detection service.

d) It is recommended that the service provider use the indicators proposed in [ETSI_ISG_ISI].

e) The service provider shall 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's relay station;
        - 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 capacities
    - 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 severity of the incident.

- Event management
  - The number of events not recognised and therefore not taken into account by the technical analysis tools;
  - The rate of events not recognised 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).
- Notification management
  - The number of accounts authorised to access the web portal and able to access the information of the commissioning entity,
  - The number of web portal access accounts created per month,
  - The number of web portal access accounts deleted per month.

f) The service provider shall 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 severity.
- 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.
- Notification management
  - The minimum, average, and maximum time between the detection of a security event and the reporting of an associated incident, by level of severity;

g) The service provider shall 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 technical devices of the detection service:
        - Commissioning entity exchange zone web portal;
        - Collection enclave's relay station;
        - Collection enclave collector;
        - System for sending incident reports;
        - Technical analysis tools;
        - Etc.
- Management of detection capacities
    - 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 detection service of the commissioning entity.
- Event management
    - The evolution of the collection coverage rate of the logs for the equipment identified in the collection strategy

h) The service provider shall 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.

### IV.5.2. Reversibility

a) The service provider shall 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 shall 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 shall 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 shall be *at a minimum* of three months.

d) It is recommended that the duration of the reversibility be six months.

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

f) The service provider shall 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 authorised it to retain (see requirement IV.5.3.4.a).

## IV.5.3. Service agreement

### *IV.5.3.1. Terms of delivery of the service*

a) The service agreement shall:

- 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 organisational 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.

### *IV.5.3.2. Organisation of the service*

a) The service agreement shall:

- 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 shall not be made public;
- Stipulate that the service provider collaborate with third parties mandated by the commissioning entity and specifically appointed by the latter. This clause shall, in particular, enable the service provider to work with a security incident response service provider mandated by the commissioning entity in the event of a suspected or confirmed security incident;
- 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 an entry in bulletin 3 of their criminal record;
- Stipulate whether the service provider allows remote access by administrators or operators to the security incident detection service information system.

### *IV.5.3.3. Responsibilities*

a) The service agreement shall:

- Stipulate that the service provider do not provide the service until receiving formal written approval of the service agreement by the commissioning entity;
- 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 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 information system of the commissioning entity;
- 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 and consultation enclaves within the information system of the commissioning entity, in accordance with requirements IV.3.14.b), IV.3.15.b) and IV.3.15.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 section IV.5.1.

### *IV.5.3.4. Confidentiality and information protection*

a) The service agreement shall:

- 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 authorisation 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 shall define the terms, in collaboration with the commissioning entity, in accordance with the types of information, and the service agreement shall:
    - 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 anonymise 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 authorises 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 the French national CERT the anonymised and decontextualized information, together with their level of sensitivity and their conditions of use;
    - Stipulate that the service provider shall 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 authorised it to retain;
- Define the frequency with which the service provider shall test the backup and restoration plan of the security incident detection service.

### *IV.5.3.5. Reversibility*

a) The service agreement shall specify the terms of implementing a reversibility plan for the service: duration, implementation, any additional costs, etc. (see section IV.5.2).

### *IV.5.3.6. Laws and regulations*

a) The service agreement shall:
    - Be written in French. The service provider shall provide a courtesy translation of the service agreement if the commissioning entity requests it;
    - Stipulate that the French version shall prevail, particularly in the context of a legal dispute;
    - Specify the governing law for the service agreement;
    - Specify the technical and organisational 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 [LOI_EJ];
- 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 French legislation and regulations in force, is:
    - 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.

b) It is recommended that the governing law for the service agreement be the French law.

c) If the governing law for the service agreement is the French law, the service provider shall specify, in the service agreement, the technical and organisational resources implemented to comply with the following texts:

- Personal data [LOI_IL];
- Breach of trust [CP_ART_314-1];
- Confidentiality of private correspondence [CP_ART_226-15];
- Medical confidentiality [CSP_ART_L1110-4];
- Invasion of privacy [CP_ART_226-1];
- Fraudulent access to or maintenance in an information system [CP_ART_323-1];
- Professional secrecy [CP_ART_226-13], where applicable without prejudice to the application of article 40, paragraph 2 of the Code of Criminal Procedure relating to reporting to a judicial authority.

#### *IV.5.3.7. Subcontracting*

a) The service agreement shall 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 this reference document.

#### *IV.5.3.8. Deliverables*

a) The service agreement shall specify that the deliverables of the service shall be in French, except at the formal written request of the commissioning entity.

#### *IV.5.3.9. Qualification of the service*

a) The service agreement shall state that:

- The service provided is a qualified service and shall include the service provider's proof of qualification;
- In accordance with the qualification process for trust service providers [QUAL_SERV_PROCESS], the commissioning entity may file a claim against the service provider to ANSSI;

- In accordance with the qualification process for trust service providers [QUAL_SERV_PROCESS], the commissioning entity authorises ANSSI and the assessment centre to audit the information system of the service provider's security incident detection service;
- In accordance with this reference document (see requirement IV.3.4.f), the commissioning entity authorises a qualified audit service provider for information system security (PASSI) to audit the information system of the service provider's security incident detection service as part of the audit plan.

b) When the service provider carries out a non-qualified service (see III.2), it shall explicitly state such in the service agreement and inform the commissioning entity of the risks of not requiring a qualified service.

### *IV.5.3.10. Service level*

a) The service agreement shall:
- 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 shall 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 shall 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.

# Appendix 1 Documentary references

## I. Codes, laws and regulations

| Reference | Document |
|---|---|
| [LOI_IL] | Law of 6 January 1978 on information technology, data files and civil liberties.<br>Available on http://www.legifrance.gouv.fr |
| [CP_ART_314-1] | Article 334-1 of the French penal code on the abuse of trust.<br>Available on http://www.legifrance.gouv.fr |
| [CP_ART_226-1] | Article 226-1 of the French penal code on the invasion of privacy.<br>Available on http://www.legifrance.gouv.fr |
| [CP_ART_226-13] | Article 226-13 of the French penal code concerning professional secrecy.<br>Available on http://www.legifrance.gouv.fr |
| [CP_ART_226-15] | Article 226-15 of the French penal code relating to confidentiality of correspondence.<br>Available on http://www.legifrance.gouv.fr |
| [CP_ART_323-1] | Article 323-1 of the French penal code on access or fraudulent maintenance in an automated data processing system.<br>Available on http://www.legifrance.gouv.fr |
| [CSP_ART_L1110-4] | Article L1110-4 of the French public health code relating to medical confidentiality.<br>Available on http://www.legifrance.gouv.fr |
| [IGI_1300] | French interministerial general instruction no. 1300 on the protection of the secrets of national defence, no. 1300 /SGDSN/PSE/PSD, 30 November 2011.<br>Available on http://www.legifrance.gouv.fr |
| [II_910] | French interministerial instruction on controlled items of information system security (ACSSI), no. 910/SGDSN/ANSSI, 22 October 2013.<br>Available on http://www.legifrance.gouv.fr |
| [II_901] | Interministerial instruction on the protection of sensitive information systems, no. 901/SGDSN/ANSSI, 28 January 2015.<br>Available on http://www.legifrance.gouv.fr |
| [D_2015_350] | Decree concerning the qualification of security products and trust service providers for the needs of national security, No. 2015-350, 27 March 2015.<br>Available on http://www.legifrance.gouv.fr |
| [LOI_EJ] | Law on legal experts, No. 71-498, 29 June 1971.<br>Available on http://www.legifrance.gouv.fr |

## II. Standards and technical documents

| Reference | Document |
|---|---|
| [PDIS_LPM] | Additional requirements applicable to service providers of security incident detection services under law no. 2013-1168 of 18 December 2013.<br>This document is marked *Diffusion Restreinte* and can be obtained from ANSSI. |
| [CRYPTO_B1] | Rules and recommendations concerning the choice and size parameters of cryptographic mechanisms, ANSSI, version 2.03.<br>Available on http://www.ssi.gouv.fr |
| [CRYPTO_B2] | Rules and recommendations concerning the management of keys used in cryptographic mechanisms.<br>Available on http://www.ssi.gouv.fr |
| [CRYPTO_B3] | Rules and recommendations concerning authentication mechanisms, ANSSI.<br>Available on http://www.ssi.gouv.fr |

| Reference | Document |
|---|---|
| [HOMOLOGATION] | Security accreditation in nine simple steps, ANSSI, current version.<br>Available on http://www.ssi.gouv.fr |
| [HYGIENE] | Guide to Information Technology Hygiene, ANSSI, current version.<br>Available on http://www.ssi.gouv.fr |
| [NT_JOURNAL] | Security recommendations for the implementation of a logging system, technical note no. DAT-NT-012/ANSSI/SDE/NP of 2 December 2013, ANSSI.<br>Available on http://www.ssi.gouv.fr |
| [NT_ADMIN] | Recommendations on the secure administration of information systems, technical note no. DAT-NT-22/ANSSI/SDE/NP of 20 February 2015, ANSSI<br>Available on http://www.ssi.gouv.fr |
| [ETSI_ISG_ISI] | ETSI ISI Indicator standards (ISI 001-1 and Guides 001-2), ISI Event Model (ISI-002), ISI Maturity (ISI-003), ISI Event Detection (ISI-004) – 5 standards on security incident detection.<br>Available on http://www.etsi.org |
| [ISO9001] | International standard ISO 9001:2008: Quality management systems – Requirements.<br>Available on http://www.iso.org |
| [ISO27000] | International standard ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary.<br>Available on http://www.iso.org |
| [ISO27001] | International standard ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements.<br>Available on http://www.iso.org |
| [ISO27002] | International standard ISO/IEC 27002:2013: Information technology – Security techniques – Code of best practice for information security management.<br>Available on http://www.iso.org |
| [ISO27005] | International standard ISO/IEC 27005:2011 – Information technology – Security techniques – Managing risks related to information security.<br>Available on http://www.iso.org |
| [ISO27035] | International standard ISO/IEC 27035:2011: Information technology – Security techniques – Managing information security incidents.<br>Available on http://www.iso.org |

## III. Other documentary references

| Reference | Document |
|---|---|
| [STRAT_NUM] | National digital security strategy, October 2015.<br>Available on http://www.ssi.gouv.fr |
| [QUAL_SERV_PROCESS] | Qualification process for a service, current version.<br>Available on http://www.ssi.gouv.fr |
| [GUIDE_ACHAT] | Buyer's guide to security products and qualified trust services, current version.<br>Available on http://www.ssi.gouv.fr |

# Appendix 2 Tasks and competences of the employees of the service provider

## I. Analyst operator

### I.1. Tasks

- Identifying, analysing and qualifying the security incidents;
- Supporting the investigation teams in handling the incidents.

### I.2. Competences

- Knowledge of protocols and network architectures;
- Log analysis experience (systems or applications);
- Knowledge of information systems' security;
- Network traffic analysis competences;
- Mastery of the analysis functionalities of detection service devices, including searching for events in the event storage systems.

## II. Infrastructure administrator

### II.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 conditions.

### II.2.Competences

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

## III. Architecture expert

### III.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.

### III.2. Competences

- 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.).

# IV. Collection and log analysis expert

## IV.1. Tasks

- Contributing to defining and reviewing the collection strategy;
- Contributing to defining the logging policy of the commissioning entity 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.

## IV.2. Competences

- 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).

# V. Detection expert

## V.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

## V.2. Competences

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

# VI. Access rights manager

## VI.1. Tasks

- Managing the creation and deactivation of accounts for the service operation tools;
- Managing the attribution, modification and removal of access rights to the service operation tools;

## VI.2. Competences

- Proficiency in administering he service operation tools;
- Knowledge of detection service roles and associated rights.

# Appendix 3 Recommendations for commissioning entities

This appendix lists ANSSI's recommendations for commissioning entities in relation to security incident detection services.

## I. Qualification

a) The commissioning entity may, when it is an administrative authority or an operator of critical importance, ask ANSSI to participate in defining the specifications covered by a tender or contract.

b) It is recommended that the commissioning entity choose its service provider from among those listed in the catalogue of qualified service providers published on ANSSI's website: the qualification of a security incident detection service provider demonstrates its compliance with all of the requirements of this reference document.

c) To receive the benefits of a qualified service, i.e. one that complies with all of the requirements of this reference document, the commissioning entity shall:

- Select the service provider from among those listed in the catalogue of qualified service providers published on ANSSI's website;
- Require the service provider to stipulate in the service agreement that the service provided is a qualified service.

Qualified service providers retain the ability to provide non-qualified services. Using a service provider from among those listed in the catalogue of qualified service providers is therefore a necessary condition but not a sufficient one for receiving a qualified service: the commissioning entity shall also require a qualified service.

d) It is recommended that the commissioning entity having recourse to a qualified service provider for the carrying out of a non-qualified service request the list of PDIS requirements that the service provider will not meet during said service.

e) It is recommended that the commissioning entity use the buyer's guide to security products and trust services [GUIDE_ACHAT], the purpose of which is to assist commissioning entities in making buying decisions during the tender process.

f) It is recommended that the commissioning entity asks the service provider to submit its proof of qualification. This certificate identifies, in particular, the activities for which the service provider is qualified and the expiry date of the qualification.

g) In accordance with the qualification process for trust service providers [QUAL_SERV_PROCESS], the commissioning entity may file a complaint with ANSSI against a qualified service provider if it considers that the service provider has not met one or more of the requirements of this reference document in providing a qualified service.

If, following investigation of the complaint, it is determined that the service provider has not complied with one or more of the requirements of this reference document in providing a qualified service, and depending on the severity of such breach, the service provider's qualification can be suspended or revoked, or the scope of its qualification can be reduced.

h) Qualification of a service provider does not attest to its capacity to access or hold classified defence information [IGI_1300] and is therefore not a substitute for a defence clearance.

It is possible for a commissioning entity to use a qualified service provider after ensuring that it has adequate defence clearances if necessary.

i) Qualification of a service provider does not attest to its capacity to access or hold controlled items of information system security (ACSSI) [II_910].

It is possible for a commissioning entity to use a qualified service provider after ensuring that the latter has, *at a minimum*, for service providers with ACSSI clearance, adequate ACSSI access clearance (DACSSI), or, for service providers without ACSSI clearance, certificates of ACSSI manipulation training.

# II. 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 a qualified audit service provider for information system security (PASSI)[16]to draw up the risk assessment for establishing the list of feared security incidents and associated impacts (see requirement IV.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 requirement 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 section IV.4.3.1), which shall be set out in the service agreement, be once a month.

f) It is recommended that the commissioning entity require to the service provider that the frequency of the strategic committee meetings (see section IV.4.3.2), which shall be set out in the service agreement, be twice 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 section IV.2.1.j), which shall be set out in the service agreement, be once a week.

h) It is recommended that the commissioning entity choose the strategic and operational indicators which shall be set out in the service agreement and which make it possible to measure the service level of the provided service among the indicators suggested by [ETSI_ISG_ISI].

i) It is recommended that the commissioning entity use [ETSI_ISG_ISI] 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 IV.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 other information systems of the commissioning entity with a lower or more vulnerable security classification or sensitivity level.

k) It is recommended that probes deployed at the interconnections of the information system of the commissioning entity be qualified by ANSSI at the appropriate level and used in accordance with the conditions for their qualification.

[16] The catalogue of qualified audit service providers for information system security (PASSI) is published on ANSSI's website.

l) It is recommended that the commissioning entity:

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

To do this, the commissioning entity may use ANSSI's technical note on the implementation of a logging system [NT_JOURNAL] and use the services of the security incident detection service provider (PDIS) or a qualified audit service provider for information system security (PASSI).

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 IV.2.3.c) specific reports in the event that major security incidents within its information system are detected.

# III. 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 needs of the commissioning entity.

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

b) 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.

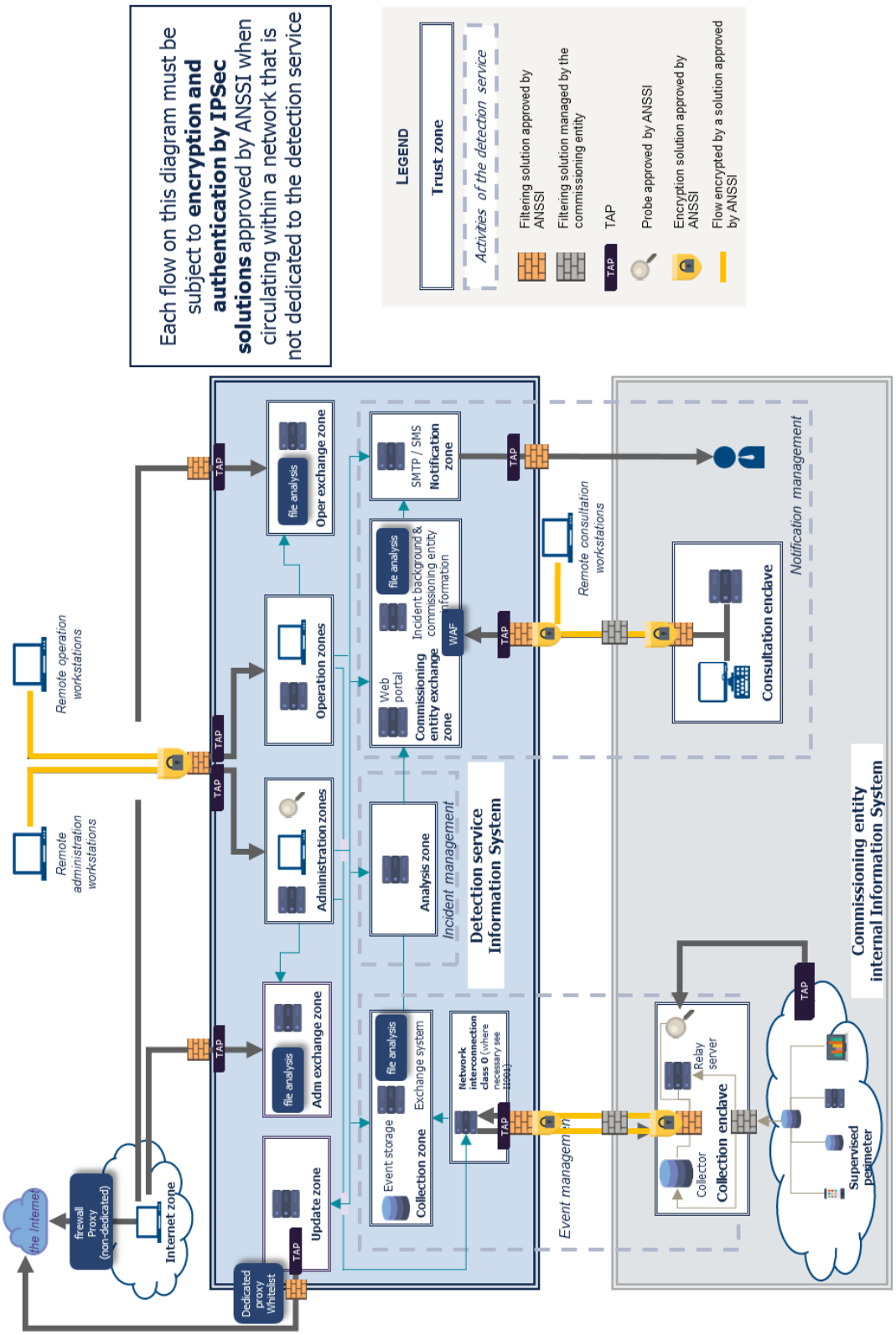
c) It is recommended that the commissioning entity put in place a change management process enabling it to continuously inform the service provider of any changes to its supervised information system (configuration, settings, software versions, etc.).

d) It is recommended that the commissioning entity use the qualified service of a qualified security incident response service provider (PRIS)[17] in the event of a suspected or confirmed security incident.

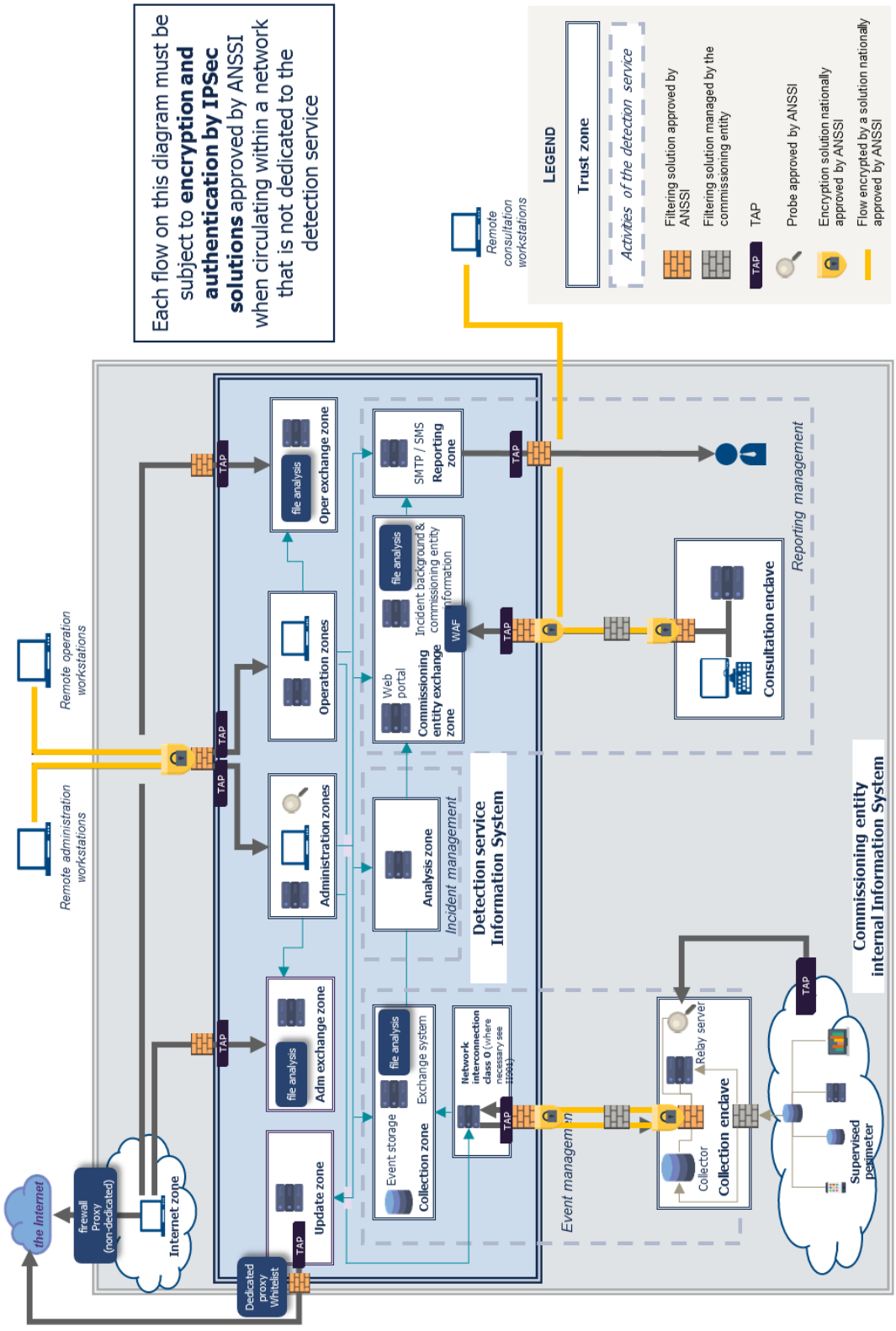
[17] The catalogue of qualified security incident response service providers (PRIS) is published on the ANSSI website.

# Appendix 4 Illustrative diagrams of PDIS-compliant architecture

The diagram below represents a possible example of compliant architecture for the detection service information system. This diagram is provided for illustrative purposes only and does not preclude the implementation of other architectures.




The following diagram, still provided for informational purposes only, highlights the fact that an internal detection service shall comply with the same requirements.


Each flow on this diagram must be subject to **encryption and authentication by IPSec solutions** approved by ANSSI when circulating within a network that is not dedicated to the detection service
LEGEND
Trust zone
Activities of the detection service
Filtering solution approved by ANSSI
Filtering solution managed by the commissioning entity
TAP
Probe approved by ANSSI
Encryption solution nationally approved by ANSSI
Flow encrypted by a solution nationally approved by ANSSI
Remote consultation workstations
Remote operation workstations
Remote administration workstations
the Internet
firewall Proxy (non-dedicated)
Internet zone
Dedicated proxy Whitelist
Update zone
Adm exchange zone
Administration zones
Oper exchange zone
Operation zones
Collection zone
Event storage
file analysis
Exchange system
Network interconnection class 0 (where necessary see ITSG)
Analysis zone
Commissioning entity exchange zone
Web portal
Incident background & commissioning entity information
WAF
SMTP / SMS
Reporting zone
Consultation enclave
Collection enclave
Collector
Relay server
Supervised perimeter
Incident management
Event management
Reporting management
Detection service Information System
Commissioning entity internal Information System
TAP

# Appendix 5 Rules concerning the use of a feed aggregator

The use of a feed aggregator between TAPs and a probe is authorised under the following conditions:

- The aggregator shall be used exclusively to ensure the aggregate function:
    - All other aggregator functions shall be disabled;
    - An equipment fulfilling TAP and aggregator functions is not authorised (dedicated equipment is necessary for each function);
- The aggregator shall be managed in the same manner and under the same security conditions as for the probes qualified by ANSSI;
- The aggregator's administration responsibilities shall be detailed in the service agreement;
- The aggregator shall be managed from the security incident detection service;
- The aggregator shall be supervised in order to identify potential package losses;
- Aggregator updates shall be carried out under the same conditions as for probes.

It is recommended that the aggregator be scaled to support the theoretical network capacity of each aggregated network.

If an aggregator is not used, a probe with multiple network interfaces and carrying out an aggregate function may be used.