TLP:CLEAR

PREMIER MINISTRE

*Liberté*
*Égalité*
*Fraternité*

**Prime Minister**

**French National Cyber Security Agency**

# Cyber security incident response service providers

# Requirements baseline

*Version 3.0 of 28 July 2024*

**Courtesy translation**

## TABLE OF CONTENTS

**I. Introduction ..... 5**

I.1. Overview ..... 5

*I.1.1. Context ..... 5*

*I.1.2. Purpose of the document ..... 5*

*I.1.3. Document structure ..... 6*

I.2. Document identification ..... 6

I.3. Acronyms and definitions ..... 6

*I.3.1. Acronyms ..... 6*

*I.3.2. Definitions ..... 6*

**II. Activities covered by the baseline ..... 10**

II.1. Search for indicators of compromise ..... 10

II.2. Digital investigation ..... 10

II.3. Malicious code analysis ..... 11

II.4. Investigation management and coordination ..... 11

**III. Qualification of service providers ..... 12**

III.1. Qualification procedures ..... 12

III.2. Qualification levels ..... 12

III.3. Scope of qualification ..... 13

III.4. Qualification for national security purposes ..... 13

**IV. Requirements applicable to the service provider ..... 14**

IV.1. General requirements ..... 14

IV.2. Personnel management ..... 14

IV.3. Protection of information ..... 15

**V. Requirements applicable to the service provider's staff ..... 17**

V.1. General knowledge and skills ..... 17

V.2. Specific knowledge and skills ..... 17

V.3. Experience ..... 17

V.4. Commitment ..... 17

**VI. Requirements applicable to the service ..... 18**

VI.1. Stage 1 – Pre-qualification of suitability to carry out the service ..... 18

VI.2. Stage 2 – Drawing up the service agreement ..... 18

*VI.2.1. Qualification ..... 18*

*VI.2.2. Terms and conditions of the service ..... 19*

*VI.2.3. Responsibilities ..... 19*

*VI.2.4. Confidentiality ..... 19*

*VI.2.5. Experts ..... 20*

*VI.2.6. Subcontracting ..... 20*

*VI.2.7. Project outline* ..... *20*

VI.3. Stage 3 - Understanding and initial stance ..... 20

VI.4. Stage 4 – Preparing the service ..... 22

*VI.4.1. Setting up the team* ..... *22*
*VI.4.2. Drawing up the project outline* ..... *22*
*VI.4.3. Special precautionary measures* ..... *23*
*VI.4.4. Opening meeting* ..... *24*

VI.5. Stage 5 – Performance of the service ..... 24

*VI.5.1. Collection* ..... *24*
VI.5.1.1. Preparation ..... 24
VI.5.1.2. Collection of technical information ..... 25
VI.5.1.3. Collection of event logs ..... 25
VI.5.1.4. Copy ..... 25
VI.5.1.5. Network flow collection ..... 25
*VI.5.2. Analysis* ..... *26*
VI.5.2.1. Search for indicators of compromise ..... 26
VI.5.2.2. System and network analysis ..... 27
VI.5.2.3. Analysis of malicious code ..... 27
VI.5.2.4. Open source research ..... 27
*VI.5.3. Steering and monitoring investigations* ..... *28*
*VI.5.4. Support for containment* ..... *29*

VI.6. Stage 6 – Feedback ..... 29

VI.7. Stage 7 – Drawing up the report ..... 29

*VI.7.1. Qualification* ..... *29*
*VI.7.2. Framework* ..... *30*
*VI.7.3. Executive summary* ..... *30*
*VI.7.4. Results* ..... *30*
*VI.7.5. Appendices* ..... *31*

VI.8. Stage 8 – Closing the service ..... 31

**Appendix 1 Bibliography ..... 33**

**Appendix 2 Tasks and skills expected of the service provider's staff ..... 35**

I. Knowledge of regulations ..... 35

II. Team leader ..... 35

*II.1. Tasks 35*
*II.2. Skills 36*

III. Investigation manager ..... 36

*III.1. Tasks 36*
*III.2. Skills 37*

IV. Systems analyst ..... 37

*IV.1. Tasks 37*
*IV.2. Skills 38*

V. Network analyst ..... 38

*V.1. Tasks 38*
*V.2. Skills 39*

VI. Malicious code analyst ..... 39

*VI.1. Tasks 39*
*VI.2. Skills 41*

**Appendix 3 Recommendations for clients ..... 42**
I. Before the service ..... 42
II. During the service ..... 44
III. After the service ..... 45
**Appendix 4 Requirements to be met by clients ..... 47**

# I. Introduction

## I.1. Overview

### I.1.1. Context

Information systems are changing, opening up more and more to the outside world and facing new threats. Despite the implementation of security measures, the risk of information systems being compromised is real.

Cyber security incident response service providers (PRIS) can be called in when a security breach is suspected, i.e. when a series of signs leads to a suspicion of malicious activity, or when a security breach is confirmed.

The security breaches covered by this baseline concern cyber attacks, the sources of which may be strategic, systemic, hacktivist or isolated.

Security incident response service providers make it possible to:

- search for traces of a possible compromise;
- confirm the malicious origin of a security breach;
- understand the security breach: date of initial compromise, chronology of the compromise, attacker's modus operandi, etc.;
- characterise the attacker: objectives, attack potential, associated threat, etc.
- identify the scope of the compromise;
- propose containment measures to limit the security breach.

The analysis report drawn up by the cyber security incident response service provider can be used to define and implement a remediation plan.

### I.1.2. Purpose of the document

This document constitutes the requirements baseline applicable to a cyber security incident response service provider (PRIS), hereinafter referred to as "the service provider".

Its purpose is to qualify a service provider in accordance with the procedures described in section III.

It provides the client of an incident response service with guarantees about the skills of the service provider and its staff, about the service provider's ability to provide a service that complies with the requirements of this baseline and to protect sensitive information and media to which it has access during the course of the service.

It can also be used as good practice outside any legal, regulatory or contractual requirements.

It does not replace the application of the legislation and regulations in force, in particular with regard to the protection of sensitive information (1) and classified information (2) or the obligations of service providers in their capacity as professionals, in particular their duty to advise their clients.

### I.1.3. Document structure

Section I gives an introduction to this baseline.

Section II describes the activities covered by this baseline.

Section III describes the qualification procedures for a service provider.

Section IV describes the requirements applicable to the service provider.

Section V describes the requirements applicable to the service provider's staff.

Section VI describes the requirements applicable to the service.

Appendix 1 gives the bibliography.

Appendix 2 describes the knowledge, skills and tasks of the service provider's staff.

Appendix 3 provides recommendations for clients before, during and after the service.

Appendix 4 describes the recommended prerequisites to be provided by clients.

## I.2. Document identification

This standard is called "Cyber security incident response service providers – Requirements baseline". It can be identified by its name, version number and date of update.

## I.3. Acronyms and definitions

### I.3.1. Acronyms

The acronyms used in this baseline are:

| | |
|---|---|
| **ANSSI** | French National Cyber Security Agency |
| **PACS** | Security support and consultancy service provider |
| **PASSI** | Cyber security audit service provider |
| **PDIS** | Cyber security incident detection service provider |
| **PRIS** | Cyber security incident response service provider |

### I.3.2. Definitions

The definitions used in this baseline are as follows, based in part on the standards (3) (4) (5) (6):

**Analyst** – individual who carries out research into indicators of compromise, system or network analysis, or malicious code.

**Individual attestation of competence** – document issued by an assessment centre following written and oral examinations, certifying that an analyst or investigation manager has the knowledge and skills expected under this baseline.

**Beneficiary** – legal entity whose information system is the subject of the service. The beneficiary may or may not be the client of the service.

**Client** – legal entity contracting a service provider to provide a qualified service. The client may or may not be the beneficiary of the service.

**Service agreement** – written agreement between the client and the service provider for the performance of the service.

**Containment** – all actions designed to contain a security breach. Some of the containment measures may disrupt the normal operation of the information system and are not intended to be extended beyond the resolution of the incident.

**Expert** – individual whom the service provider may call upon to carry out part of the service when specific knowledge and skills, outside the scope of the activities of the baseline and not held by the analysts or investigation managers, are required for the proper performance of the service. The expert may be internal or external to the service provider.

**Security breach** – one or more undesirable or unexpected information security events with a high probability of compromising an organisation's activities and/or threatening information security.

**Indicator of compromise** – combination of technical and contextual information indicating a compromise or attempted compromise, the presence of which can be identified from system and/or network analyses or malicious code.

**Command and control infrastructure** – all the communication tools and channels between the attacker and the compromised resources.

**Investigation** – process aimed at collecting and analysing information to confirm or deny the malicious origin of a security breach, to better understand the security breach and the attacker's modus operandi, to qualify the extent of the compromise and to propose containment measures.

**Hacktivist or isolated threat** – this threat is characterised by cyber attacks carried out by a lone individual or a hacktivist group with the aim of destabilising the system (for revenge, ideological motives, etc.). The methods used include denial-of-service attacks and data leaks in particular. Isolated threats also include individuals using unsophisticated tools or with privileged access within an entity, but with limited resources.

**Strategic threat** – this threat is characterised by persistent and targeted cyber attacks carried out or financed by a state. It requires considerable technical and organisational resources, as well as discretion. These attacks may be carried out for espionage, pre-positioning or destabilisation purposes.

**Systemic threat** – this threat is characterised by its ability to affect a large number of entities. It includes cyber crime, involving the use of mostly opportunistic cyber attacks. These attacks are generally carried out for financial gain and may take the form of ransomware or fraud. These threats are also represented by the proliferation of offensive tools and services available off-the-shelf or marketed by private companies. These services may be used for economic intelligence or industrial espionage, or to give certain states with limited resources access to offensive capabilities.

**Security measure** – measure enabling a security requirement to be met, preventing or reducing the occurrence of a risk of a breach of information security or reducing its severity.

**High level qualification** – level of qualification that, compared with a substantial level qualification, provides a greater guarantee of the service provider's competence, the trust that can be placed in it and its ability to protect the information and media relating to the service.

A high level service is recommended when the risks to the information system being serviced are high and/or when the intentional risk scenarios involve a strategic threat.

**Substantial level qualification** – level of qualification providing an initial level of guarantee particularly of the service provider's competence, the trust that can be placed in it and its ability to protect the information and media relating to the service. A substantial level service is recommended when the intentional risk scenarios affecting the information system being serviced involve a systemic, hacktivist or isolated threat.

**Project outline** – document drawn up and kept up to date by the service provider in consultation with the client, setting out the terms and conditions of the service. The project outline is generally drawn up after the service agreement has been signed.

**Investigation manager** – individual who manages and coordinates investigations on behalf of the service provider, i.e. actions aimed at guiding and coordinating the technical or organisational aspects of the service provided, in conjunction with the client, the beneficiary or any external entity involved in the service.

**Scope of the service** – the physical, logical and organisational environment of the information system that is the subject of the service.

**Stance** – a combination of the incident response approach, the level of discretion to be adopted with respect to the attacker, the resources to be committed and the schedule of activities.

**Attack potential** – measure of the effort required to attack an information system, expressed in terms of an attacker's expertise, resources and motivation.

**Service provider** – legal entity providing a qualified service, i.e. one that complies with the requirements of this baseline.

**Analysis report** – document drawn up by the incident response team presenting the results of the service and given to the client at the end of the service.

**Baseline** – this document.

**Team leader** – individual within the service provider's organisation responsible for the security breach response service. In particular, the team leader is responsible for putting together the security breach response team, ensuring that the skills of the analysts and investigation managers and, where applicable, the experts, are in line with the objectives, criteria, scope and activities of the service. The team leader is an analyst or an investigation manager.

**Information systems security** – safeguarding the security requirements, in particular the confidentiality, integrity and availability of information collected, stored, processed and distributed within an information system.

**Subcontracting** – operation whereby the service provider entrusts, under its responsibility, to a legal entity (the subcontractor) all or part of the performance of a contract concluded between the service provider and the client.

**Contingency supervision** – temporary device or configuration that can be deployed quickly and set up as part of the service. It supplements or replaces the supervision initially implemented, by relying on a temporary device or configuration for the continuous collection of logs and/or network flows from different sources**.** In particular, it provides a warning of potentially malicious activity.

**Information system** – organised set of resources (hardware, software, personnel, data, procedures, etc.) used to collect, store, process and distribute information.

**Target information system** – the information system that is the subject of the service.

**Third party** – individual or legal entity who is independent of the service provider, the client and the beneficiary.

**Vulnerability** – weakness in an information system or security measure that can be exploited by a threat.

# II. Activities covered by the baseline

The activities covered by this baseline are as follows:

- search for indicators of compromise (REC);
- digital investigation (INV);
- malicious code analysis (CODE);
- steering and coordination of investigations (PCI).

Where a requirement is applicable to only one activity, it is preceded by a reference in square brackets identifying that activity. For example, a requirement preceded by the reference "[REC]" applies exclusively to the activity of searching for indicators of compromise.

Where a requirement is applicable to several activities but is not applicable to all activities, it is preceded by a reference in square brackets identifying those activities. For example, a requirement preceded by the reference "[REC, INV]" applies exclusively to the search for indicators of compromise and digital investigation activities.

Where a requirement is not preceded by any reference in square brackets identifying an activity, then it is applicable to all activities.

The fully automated performance of an activity is not considered an activity within the meaning of the baseline.

The service provider may adapt steps 3 to 7 of the service described in section VI of this baseline, or even not carry out some of them, depending on how its understanding of the security breach or the security breach itself evolves.

## II.1. Search for indicators of compromise

The search for indicators of compromise consists in looking for traces of a compromise within an information system.

This activity may be carried out on its own, in conjunction with a malicious code analysis activity or as part of a managed or unmanaged digital investigation.

## II.2. Digital investigation

Digital investigation consists in collecting and analysing information and media collected from an information system in order to deny or confirm a compromise and, where necessary, identify the scope and chronology of the compromise, the attacker's modus operandi and its characterisation, particularly in terms of attack potential and objectives.

Digital investigation may involve system and/or network analysis.

This activity may be carried out on its own or in conjunction with a search for indicators of compromise or analysis of malicious code. When it is carried out in conjunction with an investigation management and coordination activity, it is said to be "managed"; otherwise it is "unmanaged".

## II.3. Malicious code analysis

Malicious code analysis consists in analysing malicious code to understand its behaviour, how it works and its impact.

This activity may be carried out on its own, in conjunction with a search for indicators of compromise or as part of a managed or unmanaged digital investigation.

## II.4. Investigation management and coordination

Investigation management and coordination is necessary in the case of serious or complex situations, in particular due to the nature, scale or seriousness of the security breach, which require several incident response activities to be carried out in a coordinated manner.

This activity involves carrying out several incident response activities simultaneously: searching for indicators of compromise, digital investigation and/or malicious code analysis.

# III. Qualification of service providers

## III.1. Qualification procedures

The qualification of a service provider is carried out in accordance with the service qualification process (7) and attests that the service provider complies with the requirements of this baseline.

The baseline contains requirements and recommendations applicable to service providers, their staff and the service provided.

Requirements must be met by service providers to obtain qualification.

Recommendations are given as good practices and are not subject to verification to obtain qualification.

The baseline also provides recommendations for clients in Appendix 3. These recommendations are not subject to verification to obtain qualification.

An organisation may apply for qualification of an internal security breach response service, i.e. a service used to meet all or part of its own needs. In this case, the qualification process and the requirements for obtaining qualification are strictly identical to those described in this baseline. The term "service provider" therefore refers to any organisation offering security breach response services on its own behalf or on behalf of other organisations.

A qualified service is one that complies with the approach described in section VI and whose activities, described in section II, are carried out by staff who comply with the requirements of section V and work for a qualified service provider who complies with the requirements of section IV. For each type of service, staff must comply with the expected skills profiles, in accordance with Annex Appendix 2.

The qualification does not replace registration on a list of digital investigation experts with a court of appeal and does not grant any rights associated with the status of expert.

## III.2. Qualification levels

There are two qualification levels for service providers: substantial and high.

Where a requirement is applicable to only one qualification level, it is preceded by a reference in square brackets identifying that level. Thus, a requirement preceded by the reference "[SUBSTANTIAL]" applies exclusively to the substantial level qualification and a requirement preceded by the words "[HIGH]" applies exclusively to the high level qualification.

Where a requirement is not preceded by a reference in square brackets identifying a qualification level, it applies to all qualification levels.

The requirements applicable to the high level qualification are, by default, recommendations for the substantial level qualification.

A service provider cannot obtain qualification for several activities at different qualification levels.

A service provider's high level qualification attests to its ability to carry out all the activities that establish its qualification at substantial level and at high level.

A service provider's substantial level qualification attests to its ability to carry out all the activities that establish its qualification at substantial level only.

Appendix 3 provides recommendations to clients on the choice of qualification level for the service.

## III.3. Scope of qualification

The scope of qualification consists of one or more activities described in section II and a qualification level described in section III.2.

The service provider may apply for qualification for one or more activities and for one qualification level.

In order to be qualified according to a scope of qualification, the service provider must satisfy all the requirements of the baseline applicable to the activities and the qualification level which constitute the scope of qualification.

The service provider may request qualification for a qualification level and for one or more response activities as specified below:

- REC + INV;
- REC + INV + PCI;
- REC + CODE + INV + PCI;
- CODE.

## III.4. Qualification for national security purposes

In addition to the requirements of this baseline for high level, service providers providing security breach response services for national security purposes must meet the requirements of the baseline (8).

Responding to incidents for national security purposes includes responding to incidents affecting critical information systems (SIIV) of operators of critical national infrastructures (OIV) and information systems handling information and media classified FR (2) EU (9) and NATO (10).

# IV. Requirements applicable to the service provider

## IV.1. General requirements

a) The service provider must be a legal entity.

b) The service provider must be subject to the law of a Member State of the European Union.

c) As a professional, the service provider has a duty to advise the client.

d) The service provider must obtain the client's consent before passing on any information or media relating to the service to third parties.

e) The service provider must provide proof that its organisation, the resources it uses to provide the service and the way it operates, particularly financially, are not likely to compromise its impartiality towards the client.

f) The service provider must provide the service impartially, in good faith and with respect for the client, its staff and its infrastructure.

g) The service provider must record and deal with complaints relating to qualified services lodged by clients, beneficiaries and, in general, all third parties.

h) The service provider must inform ANSSI without delay of any complaint lodged in relation to a qualified service and of the processing thereof.

## IV.2. Personnel management

a) Before any analyst or investigation manager is incorporated into its teams, the service provider must check their training, knowledge, skills and professional references, as well as the veracity of their curriculum vitae.

b) The service provider must ensure, before the start of each service, that the members of the team have the knowledge and skills associated with their activities in accordance with Appendix 2.

c) [HIGH] The service provider must only use analysts and investigation managers who have an individual certificate of competence to carry out the service.

The service provider may, with the client's agreement, include in the response team people who do not have an individual certificate of competence for the purposes of training or upgrading their skills. These people are present as observers and do not take part in performance of the service.

d) The service provider must ensure ongoing training for analysts and investigation managers in order to keep their knowledge and skills up to date in the field of security breach response, and in particular those required to carry out their tasks.

e) The service provider must enable analysts and investigation managers to monitor developments in order to keep their knowledge and skills up to date in the field of security breach response, and in particular those required to carry out their tasks.

f) The service provider is responsible for the methods and tools used by the response team and for their correct use during the service.

g) The service provider must make the analysts and investigation managers aware of the regulations in force within the European Union in the field of security breach response, and in particular those applicable to their tasks.

h) [HIGH] The service provider must ensure that no member of the response team has a criminal record that is incompatible with the performance of their tasks.

## IV.3. Protection of information

At the client's request, the service provider may process all or part of the information and media relating to the service on its own information system, that of the client or that of the beneficiary.

To obtain the high level qualification, the service provider must, in all cases, have an information system approved for the protection of information and media bearing the Restricted Distribution (diffusion restreinte) mark (1).

When carrying out a high level qualified service, the service provider must use its information system approved as Restricted Distribution (diffusion restreinte), whatever the marking of the information and media relating to the service.

When carrying out a substantial level qualified service, the service provider qualified at high level may choose to have, in addition to its Restricted Distribution (diffusion restreinte) information system, a second information system complying with the requirements of this section for substantial level. A service provider qualified to high level may, as part of a substantial level qualified service, at the client's request, process information and media relating to the service which do not bear the Restricted Distribution (diffusion restreinte) mark, either on its Restricted Distribution (diffusion restreinte) information system or on its second information system.

a) The service provider must draw up and keep up to date an assessment of the risks relating to its incident response activity.

b) It is recommended that the service provider use the method (11) to assess the risks relating to its incident response activity.

c) The service provider must protect the integrity and confidentiality of information and media relating to the service according to their marking and level of sensitivity.

d) The service provider must apply the principle of least privilege and limit access to information and media relating to the service to only those people who have the right and need to know.

e) The service provider may need to connect the same equipment (USB key, computer, etc.) to its approved information system and to the potentially compromised target information system. The service provider must implement appropriate security measures for this equipment in order to meet the operational requirements of the service and the security requirements of its approved information system. [HIGH] The service provider is not required to obtain security accreditation for this equipment for Restricted Distribution (diffusion restreinte) if the target information system is not approved as Restricted Distribution (diffusion restreinte).

f) The service provider must obtain security accreditation for its information system.

g) [HIGH] The service provider must obtain security accreditation for its information system for the protection of information and media marked as Restricted Distribution (diffusion restreinte).

h) It is recommended that the service provider implement the approach described in the guide (12) to obtain security accreditation for its information system.

i) The service provider must be able to use its information system to carry out the entire service.

j) [HIGH] The service provider must implement all the rules of the cyber hygiene guide (13) for the enhanced level on its Restricted Distribution (diffusion restreinte) information system.

k) [HIGH] The service provider must implement all the rules relating to the protection of information systems dealing with information and media bearing the Restricted Distribution (diffusion restreinte) mark as defined in (1) on its Restricted Distribution (diffusion restreinte) information system.

l) [HIGH] It is recommended that the service provider implement the recommendations of the guide (14) on its Restricted Distribution (diffusion restreinte) information system.

m) [SUBSTANTIAL] The service provider must implement all the rules of the cyber hygiene guide (13) for the standard level on its information system.

n) The service provider must carry out a periodic review of access rights to its information system.

o) [HIGH] The service provider must carry out a review of access rights to its information system every six months.

p) The service provider must have an offline information system to store all the information and media relating to the service for which it has received authorisation to retain from the client.

q) The service provider must implement specific security measures for the storage and handling of malicious code in order to avoid any contamination of its information system.

# V. Requirements applicable to the service provider's staff

## V.1. General knowledge and skills

a) Analysts, investigation managers and team leaders must possess the personal qualities described in section "7.2.2 Personal behaviour" of the standard (3).

b) [PCI] Team leaders and investigation managers must possess the personal qualities described in section "7.2.3.4 General competencies of the audit team leader" of the standard (3).

c) Analysts, investigation managers and team leaders must have good writing and summarising skills, and be able to convey relevant information tailored to the profiles of their contacts (management, technical departments, business and security managers, etc.).

## V.2. Specific knowledge and skills

a) Analysts, investigation managers and team leaders must, depending on their role, carry out the service in accordance with the requirements of section VI.

b) Depending on their role, analysts, investigation managers and team leaders must carry out the tasks described in Appendix 2.

c) Depending on their role, analysts, investigation managers and team leaders must have the knowledge and skills to respond to security breaches, particularly those described in Appendix 2.

d) [HIGH] [PCI] Investigation managers must be familiar with good practices for managing the security breaches described in the standards (4) (5).

e) [HIGH] Analysts and investigation managers must be familiar with good practices in the identification, collection, acquisition and preservation of evidence, as described in the standard (6).

## V.3. Experience

a) It is recommended that analysts, investigation managers and team leaders have received training in information systems security.

b) It is recommended that analysts, investigation managers and team leaders have at least one year's experience in security breach response.

## V.4. Commitment

a) Analysts, investigation managers and team leaders must have an employment contract with the service provider.

b) The service provider must have a contractual framework with experts.

# VI. Requirements applicable to the service

## VI.1. Stage 1 – Pre-qualification of suitability to carry out the service

a) It is recommended that the service provider ask the client to provide the information identified in Appendix 4 in order to carry out the pre-qualification.

b) The service provider must, on the basis of the information provided by the client, and in particular the description of the security breach, the objectives, the criteria, the scope, the response activities and any special terms and conditions of the service[1], do a preliminary qualification of suitability in order to make an impartial assessment of whether it is able to carry out the service in full, in part or not at all.

c) The service provider must inform the client of the conclusions of the preliminary qualification of suitability to carry out the service and, in particular, whether it considers that it is able to carry out the service in full, in part or not at all.

d) The service provider must only agree to provide the service if the conclusions of the preliminary qualification of suitability confirm that it is fully capable of providing the service.

## VI.2. Stage 2 – Drawing up the service agreement

a) The service provider must draw up a service agreement with the client.

When a rapid start to the service requires the service provider to access the target information system or information and media from the target information system in the absence of a service agreement or project outline, an agreement must be signed between the service provider and the client. The signatories of this agreement may be the legal representatives of the entities or any person able to bind the parties involved. This agreement must describe the scope and actions envisaged. It does not replace the drawing up of the service agreement or the project outline.

b) The service agreement must be signed by a legal representative of the service provider and a legal representative of the client, or any person who can bind the service provider and the client.

### VI.2.1. Qualification

The service agreement must:

a) specify that the service is qualified;

b) identify the qualification level of the service;

c) identify the incident response activities. When the service includes digital investigation, the service agreement must specify the type of analysis (system and/or network);

d) include the service provider's certificate of qualification;

[1] The choice of objectives, criteria, scope, response activities and any specific terms and conditions of the service is ultimately the responsibility of the client, although the service provider has a duty to advise on their relevance and consistency in its capacity as an information systems security professional.

e) [HIGH] specify that each analyst or investigation manager has an individual certificate of competence;

f) specify that the client may, in accordance with the service qualification process (7), submit a complaint to ANSSI when it considers that the service provider has not complied with one or more requirements of the baseline in the context of a qualified service, and highlight that in the event of a breach by the service provider, the service provider's qualification may be withdrawn, the scope of qualification reduced, or the service provider's level of recommendation downgraded.

### VI.2.2. Terms and conditions of the service

The service agreement must:

a) provide a general description of the approach, objectives, criteria, scope and activities of the response, as well as the terms and conditions of the service: prerequisites, milestones, deliverables, dates and locations of the service. This information can be specified and updated if necessary in the project outline;

b) specify that the law applicable to the service agreement is that of a Member State of the European Union, and specify which Member State;

c) specify the rules for ownership of elements protected by intellectual property such as the tools developed specifically by the service provider as part of the service and the deliverables of the service, in particular the analysis report;

d) specify that any amendment to the service agreement must be approved by a legal representative of the service provider and a legal representative of the customer, or any person who can bind the service provider and the customer.

### VI.2.3. Responsibilities

The service agreement must:

a) specify that the client has all ownership and access rights to the scope of the service or that it has obtained the agreement of any parties whose information systems fall within the scope of the service;

b) specify that the service provider must inform the client in writing without delay in the event of a breach of the service agreement;

c) specify that the client authorises the service provider to collect and analyse data from the target information system solely for the purposes of the service and in strict compliance with applicable laws and regulations;

d) describe the risks associated with the service, in particular those relating to compromising the availability of the target information system and the confidentiality of its data.

### VI.2.4. Confidentiality

The service agreement must:

a) specify that the service provider will only collect and analyse information and media that are strictly necessary for the proper performance of the service in accordance with the objectives, criteria, scope and activities of the service;

b) specify that the service provider will not divulge to or share with third parties any information or media relating to the service without the written authorisation of the client;

c) specify that, at the end of the service, the service provider shall return, delete or destroy all information and media relating to the service, with the exception of those for which it has received written authorisation to retain from the client;

d) specify that, at the end of the service, the service provider will store on an offline information system all the information and media relating to the service for which it has received written authorisation to retain from the client.

### VI.2.5. Experts

The service agreement must:

a) specify that the service provider may incorporate one or more experts into the response team to take part in carrying out certain activities where these require specific knowledge or skills that the analysts or investigation managers do not have, provided that:

   i. there is a documented contractual framework between the service provider and the experts;

   ii. the use of experts is accepted by the client;

   iii. the experts are duly supervised by the team leader.

### VI.2.6. Subcontracting

The service agreement must:

a) specify that the service provider may subcontract all or part of the response activities to a subcontracted service provider, provided that:

   i. the subcontracted service provider is qualified to the same qualification level for the subcontracted response activities;

   ii. the subcontracted service is qualified to the same level;

   iii. there is a contractual framework between the service provider and the subcontracted service provider;

   iv. the use of subcontractors is accepted by the client in the project outline.

### VI.2.7. Project outline

The service agreement must:

a) stipulate the drawing up a project outline and that it must be updated during the service;

b) indicate that the project outline meets the requirements set out in section VI.4.2.

## VI.3. Stage 3 - Understanding and initial stance

a) [REC, INV, PCI] The service provider must acquire an understanding of the target information system, in particular based on the information gathered during the preliminary qualification of suitability to carry out the service:

   i. mapping the target information system;

ii. architecture of the target information system;

iii. location of the target information system;

iv. means of supervising the target information system and, if necessary, detecting security breaches;

v. specific features and constraints of the target information system;

vi. interconnections of the target information system.

b) [HIGH] [PCI] The service provider must propose an initial stance to the client, identifying in particular:

i. the general approach to incident response adapted to the needs of the service;

ii. the major milestones of the service and the associated timetable;

iii. the response activities to be carried out;

iv. the information to be collected and analysed and the associated operating procedures;

v. the number of analysts and, if necessary, experts to be engaged;

vi. the level of discretion to adopt with respect to the attacker:

- high: the service provider carries out its activities without the possibility of detection by the attacker (copying disks on disconnected systems, gathering information on equipment inaccessible to the attacker, etc.). The activities carried out by the service provider do not expose knowledge about the attacker and do not hinder the attacker's operations, its means and channels of communication are not modified or suppressed,
- average: the service provider carries out its activities with a low probability of detection (collection of information confused with the normal activity of an administrator or user, security actions carried out by an administrator, etc.). The service provider's activities may partially or totally hinder the attacker's operations, but do not necessarily appear to be directed against it. Its means and channels of communication may be restricted (limiting bandwidth, configuration hardening, shutting down compromised workstations, etc.),
- weak: the service provider carries out its activities without worrying about the presence of the attacker. The service provider's activities may partially or totally hinder the attacker's operations, leaving it in no doubt as to the detection of its presence. The attacker's communication channels and resources can sometimes be blocked or suppressed.

c) [HIGH] [PCI] The investigation manager must submit the initial stance to the client's contact person for validation and at each review. The final choice of stance is the responsibility of the client.

d) [HIGH] [PCI] The investigation manager must revise the stance according to the results of the collection and analysis activities and the understanding of the incident.

## VI.4. Stage 4 – Preparing the service

### VI.4.1. Setting up the team

a) The service provider must appoint a team leader.

b) The team leader must put together a team of analysts and, where appropriate, investigation managers and experts with all the knowledge and skills required to carry out the service. The team leader may, if he has sufficient knowledge and skills, carry out the service alone.

c) The team leader must regularly reassess the profile and number of analysts and, if applicable, of investigation managers and experts to ensure that the service provider's commitment remains appropriate for the proper performance of the service.

d) [HIGH] Analysts and, where applicable, investigation managers must each have a valid individual certificate of competence for the activities entrusted to them.

### VI.4.2. Drawing up the project outline

a) The team leader must draw up the project outline in consultation with the response team and the client's contact person for the service.

The project outline must:

b) specify the objectives, criteria, scope and activities of the response, as well as the terms and conditions of the service: prerequisites, milestones, deliverables, dates and locations of the service, etc.;

c) identify the governing bodies for the service and specify their roles and frequency of meeting;

d) identify the name of the client's contact person, whose role is to manage the relationship with the service provider, ensure that the service is carried out properly and ensure that the service agreement and the project outline are complied with;

e) identify whether the client authorises the service provider to subcontract all or part of the service and, if so, identify the subcontracting service provider and the subcontracted response activities;

f) identify whether the client authorises the service provider to use experts;

g) identify the names and contact details of the members of the response team and specify for each of them their role (team leader, investigation manager, analyst or expert) and the response activities entrusted to them;

h) [HIGH] Attach individual certificates of competence for analysts and investigation managers;

i) identify the names, roles and responsibilities of the persons appointed by the client and involved in the service;

j) describe any arrangements for working with third parties (subcontractors, etc.);

k) identify rights and needs for information and media relating to the service;

l) identify the marking of information and media relating to the service according to their level of sensitivity[2];

m) identify the means of protecting information and media relating to the service according to their level of sensitivity and their marking[3];

n) specify the deliverables of the service and describe the applicable terms and conditions: content, form, language, etc.;

o) identify, for each item of information and media relating to the service, which will be retained, deleted or destroyed by the service provider or returned to the client, and specify the methods of retention, deletion, destruction and return;

p) identify any specific legal and regulatory requirements to which the client is subject, in particular those applicable to the target information system;

q) [HIGH] describe the method and resources for compiling and updating the register of information and media supplied to or collected by the service provider;

r) [HIGH] describe the method and resources used for compiling and updating the register of actions carried out by the service provider on the information and media collected and the target information system;

s) identify any specific requests the client may have, in particular any matters to which the client would like the service provider to pay particular attention. For example, there may be particular constraints to which the target system or the client may be subject;

t) be validated by the client's contact person and by the team leader, and updated each time during the service.

### VI.4.3. Special precautionary measures

a) The team leader must raise the client's awareness of the issues identified in Appendix 3, in particular:

   i. implementation of backup measures for the target information system;

   ii. setting up a crisis management system;

   iii. providing the service provider with a secure area dedicated to the service;

   iv. providing the service provider with a secure analysis environment that is disconnected from the target information system;

   v. setting up a secure means of communication, dedicated to the service and disconnected from the target information system;

[2] The choice of marking of information and media relating to the service is ultimately the responsibility of the client. However, as a professional in the field of information systems security, the service provider has a duty to advise the client and must propose suitable marking. Appendix 3 provides recommendations to clients on the marking of deliverables of the service, in particular the analysis report.

[3] The choice of means of protection of information and media relating to the service is ultimately the responsibility of the client. However, as a professional in the field of information systems security, the service provider has a duty to advise the client and must propose appropriate means of protection.

vi. implementation of security measures when the service requires the installation of tools or the execution of commands on the target system;

vii. implementation of emergency procedures, also known as "red button" procedures to quickly isolate the target information system if necessary.

b) The team leader must obtain the client's consent before carrying out any action that could lead to a malfunction or even a denial of service of the target information system.

### VI.4.4. Opening meeting

a) It is recommended that the team leader organise an opening meeting attended by at least the team leader, the analysts, the investigation manager and any experts, the client's contact person and the security and business managers of the target information system, in order to confirm their agreement to all the terms and conditions of the service, in particular the project outline, before the service is carried out.

## VI.5. Stage 5 – Performance of the service

In this section, the various operations may be carried out at the same time or successively, in the order deemed appropriate by the team leader and, where applicable, the investigation manager, for the proper performance of the service.

### VI.5.1. Collection

Collection is a fundamental stage that requires a methodical approach. It may be carried out by the service provider, the client, the beneficiary or a third party, in connected or disconnected mode. If collection is not carried out by the service provider, the latter must make the client aware of the risks of not complying with the requirements of this section.

#### *VI.5.1.1. Preparation*

a) [REC, INV] The service provider must identify the relevant system and network collection points to achieve the objectives of the service.

b) [REC, INV] The service provider must be able to carry out the following collection operations:

i. collection of technical information;

ii. collection of event logs;

iii. network flow collection.

c) [PCI] The service provider must develop and implement a collection approach that describes:

i. target information system equipment with relevant information to be collected;

ii. the relevant information to be collected: event logs, volatile memory, etc.;

iii. appropriate methods for collecting information: copying disks, copying volatile memories, etc.;

iv. the sequencing of collection operations.

d) [REC, INV, PCI] The service provider must, in collaboration with the client, identify the possible impacts of collection operations, in particular if they present a risk to the availability of the target information system.

#### *VI.5.1.2. Collection of technical information*

a) [REC, INV] The service provider must be able to collect information on the following equipment:
   i. system: backup servers, file servers, etc.;
   ii. network: proxy servers, DNS servers, routers, wireless access points, etc.;
   iii. security: firewalls, encryption, antivirus, network probes, etc.;
   iv. business: web servers, databases, etc.;
   v. administrative workstations;
   vi. user workstations: fixed or mobile computers, mobile phones, etc.

b) [REC, INV] The service provider must be able to collect technical information relating to:
   i. equipment configurations;
   ii. file systems;
   iii. programs (services, processes, etc.) that are running.

#### *VI.5.1.3. Collection of event logs*

a) [HIGH] [PCI] The service provider must be able to propose and implement a logging policy that meets the needs of the service.

b) [HIGH] [PCI] It is recommended that the service provider use the guide (15) as a basis for proposing and implementing the logging policy.

c) [REC, INV] The service provider must be able to collect event logs on the following equipment:
   i. network: proxy servers, DNS servers, routers, wireless access points, etc.;
   ii. security: firewalls, encryption, antivirus, network probes, etc.;
   iii. business: file servers, web servers, databases, etc.;
   iv. administrative workstations;
   v. user workstations: fixed or mobile computers, mobile phones, etc.

#### *VI.5.1.4. Copy*

a) [REC, INV] The service provider must be able to make copies of volatile and non-volatile memory media.

#### *VI.5.1.5. Network flow collection*

a) [REC, INV] The service provider must be able to collect network flows in order to:

i. analyse the communication protocol between a compromised resource and a command and control infrastructure;

ii. analyse the method used during the attacker's lateral movements;

iii. search for indicators of compromise.

### VI.5.2. Analysis

Analysis is a fundamental stage that requires a methodical approach. It can be carried out by the service provider on the target information system or offline.

#### *VI.5.2.1. Search for indicators of compromise*

a) [REC, INV] The service provider must have a regularly updated database of indicators of compromise[4].

b) [REC, INV] The service provider must comply with the conditions and restrictions of use applicable to indicators of compromise, in particular those marked [6], as the target information system must be considered to have been compromised a priori.

c) [REC, INV] The service provider must be able to search for indicators of compromise on the following equipment:

i. network: proxy servers, DNS servers, routers, wireless access points, etc.;

ii. security: firewalls, encryption, antivirus, network probes, etc.;

iii. business: file servers, web servers, databases, etc.;

iv. administrative workstations;

v. user workstations: fixed or mobile computers, mobile phones, etc.

d) [REC, INV] The service provider must analyse the information collected and be able to search for the following indicators of compromise:

i. file attributes: fingerprint, name, size, date, location, etc.;

ii. system artefacts: configuration parameters, Windows registry keys, etc.;

iii. network artefacts: IP addresses, URLs and domain names, etc.;

iv. memory artefacts: processes, services, etc.;

v. character strings;

vi. complex signatures: combination of indicators of compromise.

[4] Indicators of compromise may be derived from the service provider's threat monitoring, from the results of previous incident response services or from information provided by partners or the authorities.

[6] The marking may relate to a sensitivity level (e.g.: Restricted Distribution (diffusion restreinte)), classification level (e.g.: Secret) as well as to the methods of distribution or use. The TLP*(Traffic Light Protocol*) is an example of marking relating to distribution methods. The PAP*(Permissible Actions Protocol*) is an example of marking relating to terms of use.

e) [REC] Before launching a search for indicators of compromise, the service provider must check that the indicators of compromise sought are relevant to the objectives of the service.

f) [HIGH] [PCI] The service provider must be able to identify when a search for prior indicators of compromise art is necessary, and if so, to carry it out.

#### *VI.5.2.2. System and network analysis*

a) [INV] The service provider must analyse the information collected by looking for:

   i. traces of malicious activity: exploitation of vulnerabilities, elevation of privileges, information system reconnaissance, data exfiltration, etc.;

   ii. persistence mechanisms;

   iii. anomalies in relation to standard business and administration practices;

   iv. [REC] indicators of compromise.

#### *VI.5.2.3. Analysis of malicious code*

a) [CODE] The service provider must be able to carry out:

   i. an analysis of the malicious code using an online platform for analysing suspicious files;

   ii. static and dynamic analysis of malicious code;

   iii. reverse engineering of malicious code.

b) [HIGH] It is recommended that the service provider be able to perform malicious code analysis using an offline platform for analysing suspicious files.

#### *VI.5.2.4. Open source research*

As part of the analysis, the service provider may carry out open source research. Open source research, particularly on the Internet, may arouse the attention of an attacker, so it is important for the service provider to be extremely careful when carrying it out, especially if the level of discretion sought with respect to the attacker is high.

a) [HIGH] The service provider must define an open source research method which specifies the information that can be sought and the associated research methods, depending on the level of discretion sought with respect to the attacker.

b) [HIGH] It is recommended that the service provider use internal information databases when the level of discretion sought with respect to the attacker is high,.

c) [HIGH] When the level of discretion sought with respect to the attacker is high and open research, particularly on the Internet, is nevertheless necessary, it is recommended that the service provider use demarcated connections with no direct link to the service provider or the client.

### VI.5.3. Steering and monitoring investigations

a) [HIGH] [PCI] The service provider must provide the client with regular monitoring of the service, and in particular of the understanding of the incident, the stance and the next operations.

b) [HIGH] The team leader must keep an up-to-date record of all information and media collected, indicating:

   i. description of the information or medium collected;

   ii. date and time of collection of the information or medium;

   iii. method used to collect the information or medium;

   iv. level of sensitivity or classification of the information or medium.

c) [HIGH] [REC, INV, PCI] The team leader must keep an up-to-date log of each action carried out on the information and media collected and on the resources of the target information system, indicating:

   i. date and time of the action;

   ii. description of the action;

   iii. the information, medium or resource of the target information system on which the action was performed.

d) [INV, PCI] The team leader must keep an updated summary of the understanding of the security breach, indicating:

   i. whether the attacker is still present in the information system;

   ii. date of the initial compromise;

   iii. chronology of the main phases of the compromise;

   iv. the attacker's modus operandi for:

      - initially compromise the information system,
      - staying in the information system,
      - concealing its activities,
      - mapping the information system,
      - elevating its privileges,
      - controlling compromised resources,
      - collecting information,
      - exfiltrating information;

   v. characterisation of the attacker:

      - its estimated attack potential,
      - estimated level of threat: strategic, systemic, hacktivist or isolated,
      - its supposed objectives: theft of information, sabotage, etc.;

vi. scope of the security breach:

- initial vector of compromise,
- level of privilege obtained by the attacker,
- list of compromised resources and accounts, in particular those for administration.

### VI.5.4. Support for containment

a) [INV, PCI] The team leader must propose containment measures to the client in order to limit or slow down the attacker's actions. These measures must be re-evaluated regularly as understanding of the security breach or the security breach itself evolves.

b) [INV, PCI] The team leader must propose emergency measures, sometimes called "red button" procedures, to the client in order to quickly isolate the target information system if necessary. The decision to activate these procedures ultimately rests with the client.

## VI.6. Stage 6 – Feedback

a) [HIGH] The team leader must organise an "on-the-spot" debriefing at the end of each day to present to the client's contact person:

i. a progress report for the service;

ii. a summary of the results of the day's response activities;

iii. [INV, PCI] the understanding of the security breach;

iv. any difficulties encountered during the day: difficult collaboration or unavailability of the client's or beneficiary's staff, difficulty accessing the premises, the information system or documentation, etc.

b) As soon as the response activities have been completed and without waiting for the analysis report to be finalised, the team leader must inform the client of the findings and the initial conclusions of the service.

## VI.7. Stage 7 – Drawing up the report

a) The service provider must draw up an analysis report [7].

### VI.7.1. Qualification

The analysis report must:

a) specify that the service is qualified;

b) identify the qualification level of the service;

c) identify incident response activities;

d) [INV, PCI] specify whether the service involves network and/or system analysis;

[7] When several activities are carried out during the service, the choice of having one or more analysis reports rests with the client.

e) identify the names and contact details of the members of the response team and specify for each of them their role (team leader, investigation manager, network analyst, system analyst, malicious code analyst or expert) and the response activities carried out.

### VI.7.2. Framework

The analysis report must:

a) describe the objectives, criteria, scope and response activities as well as any special terms and conditions of the service;

b) identify the dates and locations of the service;

c) precisely identify (reference, version number, date, etc.) the documents on which the service provider relied to carry out the service.

### VI.7.3. Executive summary

a) The analysis report must include an executive summary.

The executive summary must:

b) be understandable by people who are not experts in information systems security;

c) summarise the understanding of the security breach: date of the initial compromise, chronology of the main phases of the compromise, modus operandi and characterisation of the attacker (objectives and threat level);

d) describe the scope of the security breach;

e) describe the critical risks associated with the security breach;

f) describe the main containment measures recommended to deal with critical risks;

g) describe any reservations relating to the results of the service: mismatch between objectives, criteria, scope, activities and workload, difficulties encountered during the service, sampling limitations, difficulty in collaborating with or unavailability of the client's or beneficiary's staff, difficulty in gaining access to the premises, information system or documentation, etc.

### VI.7.4. Results

The analysis report must:

a) [REC] identify the indicators of compromise sought;

b) [REC, INV, PCI] identify the elements collected and analysed;

c) detail the results of response activities;

d) [INV, PCI] detail the understanding of the security breach:

   i. whether the attacker is still present in the information system;

   ii. date of the initial compromise;

   iii. detailed chronology of the phases of the compromise;

   iv. the attacker's modus operandi for:

- initially compromise the information system,
- staying in the information system,
- concealing its activities,
- mapping the information system,
- elevating its privileges,
- controlling compromised resources,
- collecting information,
- exfiltrating information;

v. characterisation of the attacker:
   - its estimated attack potential,
   - estimated level of threat: strategic, systemic, hacktivist or isolated,
   - its supposed objectives: theft of information, sabotage, etc.;

vi. scope of the security breach:
   - initial vector of compromise,
   - level of privilege obtained by the attacker,
   - list of compromised resources and accounts, in particular those for administration.

e) [INV, PCI] describe the level of discretion adopted with respect to the attacker;

f) [INV, PCI] propose containment measures to limit the security breach;

g) identify the names and roles of the people with the client, the beneficiary and any third parties (subcontractors, etc.) with whom the service provider interacted to provide the service.

### VI.7.5. Appendices

The analysis report must include:

a) the project outline;

b) [HIGH] the register of information and media collected by the service provider;

c) [HIGH] the register of actions carried out by the service provider on the information and media collected and on the target information system.

## VI.8. Stage 8 – Closing the service

a) It is recommended that, once the analysis report has been submitted, the team leader organise a closing meeting attended by at least the team leader, the analysts, the investigation manager and any experts, the client's contact person, the client's management team and the security and business managers for the target information system. This meeting provides an opportunity to present the summary of the analysis report and answer any questions the client may have.

b) The service provider must return, delete or destroy any information or media relating to the service for which it has not obtained the client's consent to retain in the project outline.

c) The service provider must store offline the information and media relating to the service for which it has obtained the client's consent to retain in the project outline.

d) [HIGH] It is recommended that the service provider produce a record of the destruction, deletion or return of any information or media relating to the service for which it has not obtained the client's written consent to retain in the project outline. This report, which should be given to the client, should identify precisely the information or media destroyed, deleted or returned, the date and the method of destruction, deletion or return.

# Appendix 1 Bibliography

1. **Instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles, n° 901/SGDSN/ANSSI, version en vigueur.** ***Disponible sur https://www.legifrance.gouv.fr.***

**2.** ***Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, n° 1300/SGDSN/PSE/PSD, version en vigueur. Disponible sur https://www.legifrance.gouv.fr.***

**3.** ***Norme internationale ISO/IEC 19011 : Lignes directrices pour l'audit des systèmes de management, version en vigueur. Disponible sur https://www.iso.org.***

**4. Norme internationale ISO/IEC 27035-1 : Technologies de l'information – Gestion des incidents de sécurité de l'information. Partie 1 : Principes de la gestion des incidents, version en vigueur.** ***Disponible sur https://www.iso.org.***

**5. Norme internationale ISO/IEC 27035-2 : Technologies de l'information– Gestion des incidents de sécurité de l'information. Partie 2 : Lignes directrices pour planifier et préparer une réponse aux Incidents, version en vigueur.** ***Disponible sur https://www.iso.org.***

**6. Norme internationale ISO/IEC 27037 : Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques, version en vigueur.** ***Disponible sur https://www.iso.org.***

**7.** ***Processus de qualification d'un service, version en vigueur. Disponible sur https://www.cyber.gouv.fr.***

**8. Référentiel d'exigences applicables aux prestataires de réponse aux incidents de sécurité pour les besoins de la sécurité nationale, version en vigueur.** ***Document Diffusion Restreinte, il peut être obtenu auprès de l'ANSSI.***

**9. Instruction interministérielle n° 2102 sur la protection en France des informations classifiées de l'Union Européenne, n° 2102/SGDSN/PSD, version en vigueur. Disponible sur https://www.legifrance.gouv.fr.**

**10. Instruction interministérielle n° 2100 pour l'application en France du système de sécurité de l'Organisation du traité de l'Atlantique nord, version en vigueur. Disponible sur https://legifrance.gouv.fr.**

**11. Guide - Méthode de gestion de risques EBIOS Risk Manager.** ***Disponible sur https://www.cyber.gouv.fr.***

**12. Guide - L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur.** ***Disponible sur https://cyber.gouv.fr.***

**13.** ***Guide - Guide d'hygiène informatique, ANSSI, version en vigueur.*** **Disponible sur https://cyber.gouv.fr.**

**14. Guide – Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte – version en vigueur. *Disponible sur https://www.cyber.gouv.fr.***

**15. Guide - Recommandations de sécurité pour l'architecture d'un système de journalisation, ANSSI-PA-012/ANSSI/SDE, ANSSI, version en vigueur. *Disponible sur https://www.cyber.gouv.fr.***

**16. Loi relative à la programmation militaire, version en vigueur. *https://www.legifrance.gouv.fr.***

**17. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. *Disponible sur https://eur-lex.europa.eu.***

**18. Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. Disponible sur https://eur-lex.europa.eu.**

**19. Référentiel général de sécurité, version en vigueur. *Disponible sur https://legifrance.gouv.fr.***

**20. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. *Disponible sur https://eur-lex.***

**21. Guide - Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. *Disponible sur https://www.cyber.gouv.fr.***

**22. Instruction interministérielle n° 910 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, version en vigueur. Disponible sur https://www.legifrance.gouv.fr.**

**23. Guide - Crise d'origine Cyber, les clés d'une gestion opérationnelle et stratégique, ANSSI, version en vigueur. *Disponible sur https://www.cyber.gouv.fr.***

**24. Guide - Anticiper et gérer sa communication de crise cyber, ANSSI, version en vigueur. *Disponible sur https://www.cyber.gouv.fr.***

**25. Guide - Guides de remédiation d'incidents de sécurité, volet stratégique, volet opérationnel, volet technique – version en vigueur. *Disponible sur https://www.cyber.gouv.fr.***

**26. Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. *Disponible sur https://www.cyber.gouv.fr.***

# Appendix 2 Tasks and skills expected of the service provider's staff

This annex describes the knowledge, skills and tasks of the service provider's staff.

Knowledge of the regulations cited in section I is supplemented by the specific tasks and skills required for each staff profile described in the following sections of this appendix.

To qualify, the service provider must have the following profiles for each response activity:

| Activity | Profile(s) |
|---|---|
| REC | Network and/or systems analyst |
| INV | Network and/or systems analyst |
| CODE | Malicious code analyst |
| PCI | Investigation manager |

## I. Knowledge of regulations

Analysts and investigation managers must be familiar with the following regulations:

- protection of national defence secrets (2);
- protection of sensitive information systems (1);
- loi de programmation militaire (Critical Information Infrastructure Protection Law) (16) and in particular the provisions applicable to the critical information systems (SIIV) of operators of critical national infrastructures (OIV);
- European directives on network and information security (17) and (18);
- the General Security Baseline (19);
- the General Data Protection Regulation (20);
- protection of classified information of the North Atlantic Treaty Organisation (NATO) (10);
- protection of European Union (EU) classified information (9).

## II. Team leader

This section describes the tasks and skills of the team leader.

### II.1. Tasks

The team leader must be capable of carrying out the following tasks:

- defining and implementing an organisation appropriate to the objectives, criteria, scope and activities of the response;

- setting up and managing the incident response team, made up of analysts and, where applicable, experts and investigation managers;
- defining and managing service priorities;
- organising feedback meetings;
- organising the closing meeting for the service;
- checking the quality and validating the deliverables of the service, in particular the project outline and the analysis report, especially the executive summary.

### II.2. Skills

The team leader must have the following skills:

- summarising and presenting useful information to technical and non-technical staff;
- drafting deliverables tailored to different levels of audience (technical departments, management bodies, etc.).

## III. Investigation manager

This section describes the tasks and skills of the investigation manager.

### III.1. Tasks

The investigation manager must be capable of carrying out the following tasks:

- defining and managing service priorities, particularly in crisis situations;
- managing and monitoring the activities of the members of the incident response team;
- proposing and supporting the client in defining and implementing precautionary measures upstream of incident response actions;
- proposing and implementing a security breach response approach tailored to the objectives, criteria, scope and activities of the response;
- proposing an initial stance and revising it as necessary during the service;
- developing and maintaining an understanding of the security breach;
- maintaining an up-to-date status report on operations (collections, research, analyses) and compromises, and presenting the relevant information to each level (technical committee, strategic committee, etc.);
- supporting the client in assessing the business impact of the security breach;
- supporting the client in implementing solutions for collecting and analysing system and network events;
- helping the client to define and implement a system and network event logging policy;
- supporting the client in defining and implementing containment measures;
- writing the relevant parts of the analysis report, in particular the executive summary;
- taking part in feedback meetings;

- taking part in the closing meeting;

### III.2. Skills

The investigation manager must have in-depth skills in most of the following technical areas:

- the main malicious attacks and activities: exploitation of vulnerabilities, backdoors, *rootkits*, *botnets*, ransomware, command and control infrastructures, etc.;
- references for the representation of indicators of compromise: *Structured Threat Information eXpression*, *OpenIOC*, etc.;
- information system architectures, their vulnerabilities and their administration mechanisms;
- the main operating systems and virtualisation solutions, their vulnerabilities and how to secure them;
- network protocols and architectures, their vulnerabilities and security;
- applications, their vulnerabilities and security: office applications, web servers, databases, mail servers, software packages, etc.;
- analysis tools: system analysis (antivirus, memory, disks), log analysis (signature, network, system, application or network), static and dynamic program analysis.

## IV. Systems analyst

This section describes the tasks and skills of the systems analyst.

### IV.1. Tasks

The systems analyst must be capable of carrying out the following tasks:

- assimilating an overview of the information system in order to identify:
    - exploitable system vulnerabilities and associated attack paths;
    - end points requiring data collection (infrastructure servers, administration and user workstations, business servers, etc.);
- collecting and analysing a large volume of technical information (file system, configuration, system and application logs, etc.) from a wide range of IT systems;
- carrying out searches for indicators of compromise;
- making a physical/memory copy of terminals (workstations, mobile workstations, etc.), servers (infrastructure servers, application servers, etc.) and removable media (USB sticks, external disks, etc.) likely to have been part of an attack scenario and analysing them;
- supporting the client in implementing log collection and analysis solutions adapted to the target architecture, in order to track the attacker's activities;
- supporting the client in defining a system logging policy (types of events, retention times, etc.) for each type of equipment;
- supporting the client in developing rules for correlating system events;

- extracting indicators of compromise for analysis and monitoring purposes;
- analysing all the technical data collected (disk images, memory images, event logs, alerts, system, network and application traces, etc.) to determine the cause of the incident, the modus operandi of the attack, the vulnerabilities exploited, the extent of the compromise and the malicious activities;
- characterising files (binaries and documents) to identify their potential malicious nature (checking headers, checking via antivirus software, analysing performance in an isolated system, etc.);
- supporting the client in implementing containment measures;
- capitalising on the knowledge acquired, providing feedback and producing an analysis report.

### IV.2. Skills

The systems analyst must have in-depth skills in the following technical areas:

- operation, security and vulnerabilities of the main operating systems and the most widespread virtualisation solutions;
- applications and their vulnerabilities: office applications, Internet browsers, web servers, databases, mail servers, software packages, etc.;
- malicious attacks and activities: exploitation of vulnerabilities, backdoors, *rootkits*, *botnets*, command and control infrastructure, *obfuscation*, etc.;
- analysis tools: system analysis (artefacts, memory, disks, file system, boot sequence), log analysis (system, application or network), static and dynamic analysis of programs and documents, etc.;
- system, network and application event logs;
- collection solutions (including logging and copying);
- log analysis or security monitoring solutions (SIEM);
- network protocols and architectures, their vulnerabilities and security;
- low-level programming languages (C, assembler, etc.) and scripting languages (Python, Perl, PowerShell, etc.).

## V. Network analyst

This section describes the tasks and skills of the network analyst.

### V.1. Tasks

The network analyst must be capable of carrying out the following tasks:

- assimilating an overall view of the information system and its architecture, identifying potential infiltration/exfiltration points and the associated collection points (network components, security products, etc.);
- supporting the client in identifying the attacks to be detected;

- carrying out searches for indicators of compromise;
- supporting the client in implementing solutions for collecting and analysing network logs adapted to the target architecture for monitoring purposes;
- supporting the client in defining a network logging policy (types of events, retention times, etc.) for each type of equipment (interconnection nodes, Internet gateways, security equipment, etc.) (15) and in developing network event correlation rules;
- supporting the client in the design and implementation of cyber attack detection solutions and the development of event correlation rules;
- analysing and interpreting the technical information collected (logs, alerts): vulnerabilities exploited, attack paths, etc.;
- extracting indicators of compromise for analysis and monitoring purposes;
- characterising files (binaries and documents) to identify their potential malicious nature (checking headers, checking via antivirus software, analysing performance in an isolated system, etc.);
- supporting the client in implementing containment measures;
- capitalising on the knowledge acquired, providing feedback and producing an analysis report.

### V.2. Skills

The network analyst must have in-depth skills in the following technical areas:

- the overall architecture of a network, its vulnerabilities and security;
- classic network protocols (TCP/IP, routing mechanisms, IPsec and VPN) and the most common application protocols (HTTP, SMTP, LDAP, SSH, etc.);
- malicious attacks and activities: exploitation of vulnerabilities, backdoors, *rootkits*, *botnets*, command and control infrastructure, *obfuscation*, etc.;
- analysis of system, network and application event logs;
- mirroring of network equipment (physical or virtualised), in particular the implementation of TAPs (*Test Access Points*).
- log analysis or security monitoring solutions (SIEM);
- intrusion detection probes and event log correlation tools;
- programming and scripting languages (Python, Perl, PowerShell, etc.).

## VI. Malicious code analyst

This section describes the tasks and skills of the malicious code analyst.

### VI.1. Tasks

The malicious code analyst must be able to identify the following elements:

- the characteristics of the malicious code (cryptographic fingerprint, size of the malicious code, version of the target operating system concerned, characteristic elements, etc.), the family or category to which the malicious code belongs *(dropper*, *loader*, *Remote Access Trojan*, *bootkit*, etc.) as well as the reference to an analysis already carried out if it is a known variant;
- the context in which the malicious code was extracted. This should include a description of how the malicious code was initially detected and the location on the system from which it was extracted (e.g. file, memory, hardware, etc.);
- the malicious code execution phase (e.g. exploiting a vulnerability, downloading other malicious code, installing a *rootkit*, etc.);
- dependencies on the compromised environment (presence of a configuration file, use of a data file, memory copy in the case of in-memory execution, etc.);
- summary of the main functions of the malicious code (recovery of banking data, file exfiltration, recovery of technical data, etc.);
- technical capabilities of the malicious code, for example:
    - collection of technical data (system and/or network) or business data (files, keystrokes, passwords, etc.);
    - persistent execution: the malicious code executes again on the compromised system after completing its initial execution (system shutdown, ephemeral execution, etc.). Persistence can be implemented by the malicious code itself or via a second code. In most cases, this involves identifying an execution at operating system or user session start-up, an execution on a system event, an execution via a system reinfection, etc.;
    - propagation on the information system, via the network (e.g. exploitation of a vulnerability, use of an account with a stolen password, etc.) or via removable media (e.g. USB stick);
    - elevation of privileges (e.g. obtaining additional or even administrative privileges on the compromised system by exploiting vulnerabilities);
    - protection against collection (falsification of activities on a compromised system, deletion of logs, modification of file dates, etc.);
    - protection against analysis. This protection can be static (scrambling or encryption of code, complication of operation, etc.) or dynamic (detection of an antivirus or analysis environment, etc.);
    - the level of autonomy (e.g. use of a dedicated means of communication to control the code, existence of pre-programmed mechanisms and performance conditions, etc.) ;
    - data exfiltration or the installation of a command and control infrastructure. This involves identifying the means of data exfiltration (file sharing, email, proxy server, USB stick, etc.).

To do this, the analyst must carry out the following activities:

- characterise the malicious code in relation to antivirus databases;

- dynamically analyse code to extract behaviours;
- reverse engineer the code and its components;
- identify and extract indicators of compromise.

The code analyst must capitalise on the knowledge acquired, provide feedback and produce an analysis report.

It must propose detection and protection methods and extract indicators of compromise for monitoring purposes, in particular taking into account:

- the characteristics of the malicious code: cryptographic fingerprint, size, cryptographic routine, discriminating character string, etc;
- the activities of the malicious code on the information system: files created or modified, services performed, etc.;
- malicious code activities on the network: communication protocol, discriminating markers (HTTP UserAgent), IP addresses, command and control infrastructure server domain names, patterns, etc.

### VI.2. Skills

The malicious code analyst must have in-depth skills in the following technical areas:

- the main dynamic, behavioural (sandbox) and static code analysis tools and how to use them;
- how malicious code works: persistence, communication, protection (cryptography, *unpacking*, etc.);
- operation, security and vulnerabilities of the main operating systems and the most widespread virtualisation solutions;
- applications and their vulnerabilities: office applications, Internet browsers, web servers, databases, mail servers, software packages, etc.;
- reverse engineering tools and solutions (disassemblers, decompilers, etc.);
- malicious attacks and activities: exploitation of vulnerabilities, backdoors, *rootkits*, *botnets*, command and control infrastructure, etc.;
- network protocols and architectures, their vulnerabilities and security;
- low-level programming languages (C, assembler, etc.) and scripting languages (Python, Perl, PowerShell, etc.).

# Appendix 3 Recommendations for clients

This appendix lists ANSSI's recommendations for the clients of security breach response service providers.

## I. Before the service

a) When the client is an administrative authority or an operator of vital importance, it may ask ANSSI to take part in defining the specifications of a call for tenders or a contract for security breach response.

b) It is recommended that the client use the guide (21) to draw up the specifications for a call to tender or a contract for security breach response.

c) The client can consult the catalogue of qualified service providers on the ANSSI website. For each service provider, this catalogue sets out the activities for which it is qualified, the period of validity of the qualification, the level of qualification and the level of recommendation.

d) Qualified service providers retain the option of carrying out non-qualified services, but may not claim qualification for these services. If the client wishes to benefit from a qualified service, i.e. one that complies with the requirements of this baseline, it must ensure that the service agreement drawn up with the service provider explicitly states that the service is qualified.

e) An unqualified service, i.e. one that does not comply with the requirements of this baseline, exposes the client to certain risks, in particular compromising confidential information and the loss or unavailability of the information system that is the subject of the service. These risks can be reduced by using a qualified service provider. If, however, the client does not wish to use a qualified service, it is nevertheless recommended that they ask the service provider for a document identifying all the requirements of this baseline that have not been met as part of their service, in order to identify the risks to which they are exposed.

f) The client may, in accordance with the qualification process for a service (7), submit a complaint to ANSSI when it considers that the service provider has not complied with one or more requirements of this baseline in the context of a qualified service. Complaints may also be lodged directly with the qualified service provider, which is obliged to inform ANSSI without delay.

   If, after investigating the complaint, it is found that the qualified service provider has failed to comply with one or more requirements of this baseline in the context of a qualified service, the service provider's qualification may be withdrawn, the scope of qualification reduced, or the level of recommendation of the service provider downgraded in accordance with the qualification process for a service (7).

g) Unless the client is subject to a legal, regulatory or contractual obligation, the choice of qualification level for the service is the sole responsibility of the client. In this case, it is recommended that the qualification level of the qualified service be determined using a risk-based approach.

It is recommended that a high level service be carried out when the risks to the information system being serviced are high and/or when the intentional risk scenarios involve strategic threats. In other cases, a substantial level service should suffice.

For this reason, in the case of a high level qualified service, it is recommended that the client require of the service provider in the project outline that the analysis report bear the words Restricted Distribution (diffusion restreinte).

h) Where the information system to be provided is a national security system, the client must provide a service that is qualified for national security purposes, i.e. in addition to the requirements for high level of this baseline, it must comply with the requirements of the baseline (8).

i) The qualification of a service provider does not attest to its ability to access or hold classified information and therefore does not replace the clearance of a legal or natural person under the directive (2).

Where the service requires the service provider to access or hold classified information, the client must check that the service provider and its staff comply with the principles governing access to national defence secrets by natural and legal persons.

j) The qualification of a service provider does not attest to its ability to access or hold controlled items of information systems security (ACSSI) (22).

Where the service requires the service provider to access or hold controlled items relating to information systems security, the client must check that the service provider has the necessary DACSSI (Decisions on Access to ACSSI) for classified ACSSI or training certificates for the handling of ACSSI for unclassified ACSSI.

k) It is recommended that the client determine the objectives, scope and activities of the service using a risk-based approach.

l) It is recommended that the client ask the service provider to provide references for services carried out with objectives, scope and activities similar to those required by the client.

m) Because of the importance of rapid intervention by the service provider in the event of a security breach, it is recommended that the client draw up a service agreement with the service provider before any service is provided so that the service provider is not slowed down in its work by the stage of drawing up a service agreement.

n) It is recommended that the scope of the service cover the entire information system so that the service provider can identify the full scope of the compromise.

o) The service provider must propose a workload appropriate to the objectives, criteria, scope and activities, although the workload ultimately chosen is the sole responsibility of the client. The service provider will mention in the report any reservations regarding the service that may have an impact on the results of the service, particularly in the event of a mismatch between the workload on the one hand and the objectives, scope and activities on the other.

Because of its unpredictable and unplannable nature, a security breach response service is an iterative process requiring regular review of the approach to be adopted and, consequently, of the associated workload and resources (staff, budget, etc.). The workload,

duration and resources of the service may be revised during the course of the service depending on the understanding of the security breach or the security breach itself. An incident response service can last several weeks or even months.

p) In order to reduce the workload of the service and therefore its cost, while still meeting the objectives of the service, the service provider can propose that the client carry out sampling using a risk-based approach.

q) The client must appoint a contact person whose role is to draw up and keep up to date, in collaboration with the service provider, the project outline for the service. The contact person manages the relationship with the service provider and ensures that the service is carried out correctly, in compliance with the service agreement and the project outline.

It is recommended that the client's contact person have the means to engage the responsibility of the client and to respond rapidly to the service provider's requests.

r) It is recommended that the client have a cyber crisis management system in place. This system provides the client with a cyber crisis management governance system and the associated resources (organisation, policies, procedures, tools, etc.) so that it can provide a strategic and operational response during the crisis. It also includes crisis communication, legal and potentially insurance aspects.

It is recommended that the client call on a qualified consultancy and support service to prepare for cyber crisis management, provided by a qualified cyber security consultancy and support service provider (PACS) to design a cyber crisis management system, or to develop or review an existing system.

If the client does not have a pre-existing cyber crisis management system, then it is recommended that the client's contact person set up a project structure with the appropriate level of decision-making power to ensure a short, rapid and simplified decision-making chain for all the processes required for the successful performance of the service: purchasing, communication, etc. It is essential that the client's management is represented in this structure.

It is recommended that the client use the guide (23) to manage a cyber crisis and the guide (24) to manage crisis communications.

s) Filing a complaint with the competent authorities can facilitate international cooperation, in particular with companies providing outsourced services (e.g. email, data storage, social networks, etc.) in order to collect information relating to the security breach.

t) It is recommended that the client inform the service provider of all actions (administration, maintenance, etc.) planned or in progress on the information system so as not to disrupt the incident response service.

u) It is recommended that the client implement emergency procedures, sometimes called "red button" procedures, to quickly isolate the target information system if necessary.

## II. During the service

a) It is recommended that the client provide the service provider, from the start of the service, with the information identified in Appendix 4 to enable the service provider to

rapidly acquire an initial understanding of the target information system and the security breach.

b) It is recommended that the client provide the service provider with a secure, dedicated area for storing sensitive information and media relating to the service (safe, guarded room, etc.). This zone must comply with the regulatory constraints associated with the level of sensitivity or classification of the information and media stored.

c) It is recommended that the client provide the service provider with the technical resources (hardware, equipment, connections, etc.) required for the service, and that these resources constitute a secure analysis environment that is disconnected from the target information system.

d) It is recommended that the client implement a secure and dedicated means of communication for all exchanges relating to security breaches, both internally and externally, in particular with the service provider. It is recommended that these resources be disconnected from the target information system so as not to enable the attacker to obtain information relating to the service in progress.

e) In the case of a substantial level qualified service carried out by a service provider qualified to high level, it is recommended that the client, in the project outline, require the service provider to process all information and media relating to the service on its Restricted Distribution (diffusion restreinte) information system, regardless of the marking of this information and media.

f) It is recommended that the client trace and inform the service provider of all operations carried out on the target information system during the service (administration operations, backup, restoration, etc.) to enable the service provider to identify illegitimate actions carried out by the attacker.

g) It is recommended that, where the service requires a tool to be installed or a command to be executed on the target system, the client carry out these actions itself or, failing that, authorise the service provider to carry out these actions with dedicated accounts benefiting from the principle of least privilege and under the constant supervision of the client.

h) It is recommended that the client create accounts enabling the service provider to carry out collection operations. These accounts must be dedicated, benefit from the principle of least privilege and, as far as possible, be unmarked and respect the naming policy of the client so as not to attract the attention of the attacker.

## III. After the service

a) Based on the analysis report drawn up by the cyber security incident response service provider, it is recommended that the client draw up an action plan to remediate the security breach, using the guide (25) as a basis.

b) It is recommended that the client call on a qualified consultancy and support service to prepare for cyber crisis management, provided by a qualified cyber security consultancy and support service provider (PACS) to design a cyber crisis management system, or to develop or review an existing system.

a) It is recommended that the client call on the services of a qualified cyber security support and consultancy service provider (PACS) to support the client in restoring its information system, improving the level of security and thus limiting the occurrence of a new security breach.

b) It is recommended that the client call on a qualified audit service provided by a qualified cyber security audit service provider (PASSI) to check the level of security of the target information system once a remediation plan has been implemented.

c) It is recommended that the client call on a qualified security breach detection service provider (PDIS) to detect the occurrence of a new security breach as early as possible.

# Appendix 4 Requirements to be met by clients

Prior to carrying out the service, it is recommended that the client provide the service provider with information concerning:

- the organisation chart;
- the general organisation of the information system;
- information system architecture:
    - IP address ranges, network and security equipment, etc.;
    - output gateways to the Internet (web relays, *domain name system*, outgoing flows, messaging chain, etc.);
    - input gateways (VPN, nomads, incoming flows and remote access to messaging, telephony);
    - servers exposed to the Internet or to a third party (web server, application server, etc.);
    - network zone architecture and filtering;
    - information system interconnections;
- specific features of the information system (applicable regulations, SIIV, business and/or technical constraints, outsourcing, etc.) and its geographical location;
- the information system:
    - operating systems (administration workstations, user workstations, mobile workstations, infrastructure and business servers, etc.);
    - technologies used for business applications;
    - technologies used for infrastructure services;
    - specify whether the clocks of the information system equipment are synchronised (e.g.: *network time protocol* – NTP) and the different zones used (e.g.: *coordinated universal time* – UTC);
    - special features of systems (impossible to shut down or change configuration);
- the architecture of administration domains and the links between domains;
- logging policy, means of supervision and detection;
- technical freeze periods and current or planned projects for the information system;
- any steps already taken by the client:
    - methodology used to identify compromised elements;
    - chronology and nature of the analysis and containment measures already carried out;
    - measures taken by the client to detect or block the attacker;
- any initial results from understanding the security breach;

- any previous incident reports;
- any existing emergency procedures.