Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de réponse aux incidents de sécurité

Référentiel d'exigences

Version 2.0 du 2 août 2017

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
26/02/2014	0.1	*Version préliminaire interne ANSSI.*	ANSSI
29/04/2014	0.2	*Prise en compte des remarques SD COSSI, SD SDE, MRR.*	ANSSI
7/07/2014	0.3	*Prise en compte des remarques SD COSSI, SD SDE, MRR et validation pour publication.*	ANSSI
6/10/2015	1.0	*Version révisée suite à l'appel à commentaires et utilisée pour la phase expérimentale.*	ANSSI
02/08/2017	2.0	*Première version applicable.* Modifications principales : • Ajout des prestations de recherche d'indicateurs de compromission et d'investigation numérique sur périmètre restreint • Actualisation des compétences requises pour les analystes • Ajout du rôle d'analyste référent	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

qualification@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

L'interconnexion croissante des réseaux et les besoins de dématérialisation des processus ou des documents exposent les systèmes d'information à des risques de vol, de modification ou de destruction de données.

Lorsqu'une concordance de signaux permet de soupçonner une activité malveillante au sein d'un système d'information, il convient de faire appel à un prestataire de réponse aux incidents de sécurité afin de :

- définir une méthode de réponse aux incidents de sécurité adaptée au contexte ;
- rechercher, collecter et analyser des éléments issus du système d'information ;
- identifier le mode opératoire et l'objectif de l'attaquant ;
- qualifier l'étendue de la compromission ;
- aider à évaluer les risques et les impacts associés ;
- préconiser des mesures de remédiation.

Les incidents de sécurité concernés par ce référentiel sont les incidents ayant pour effet une compromission ou un sabotage ; il ne cible pas la réponse aux fraudes et attaques par saturation pouvant conduire à un déni de service[1].

Les types de prestations de réponse aux incidents de sécurité décrites dans ce référentiel sont :

- la recherche d'indicateurs de compromission ;
- l'investigation numérique sur périmètre restreint ;
- l'investigation numérique sur large périmètre.

I.1.2. Objet du document

Ce document constitue le référentiel d'exigences applicables à un prestataire de réponse aux incidents de sécurité (PRIS), ci-après dénommé « le prestataire ».

Il a vocation à permettre la qualification de cette famille de prestataires selon les modalités décrites au chapitre III.1.

Il permet au commanditaire d'une prestation de disposer de garanties sur les compétences du prestataire et de son personnel, sur la qualité des prestations de réponse aux incidents de sécurité réalisées à sa capacité à adopter une approche globale de l'incident de sécurité, une démarche d'analyse adaptée et sur la protection des informations sensibles dont le prestataire aura connaissance au cours de la prestation.

Ce référentiel permet notamment de qualifier les prestataires susceptibles d'intervenir, pour le traitement des incidents de sécurité, au profit des secteurs d'importance vitale concernés par l'application des règles de sécurité prévues au titre de la loi de programmation militaire. Il peut également être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire.

Il n'exclut ni l'application de la législation et de la réglementation nationale, en matière de protection du secret de la défense nationale [IGI_1300] par exemple, ni l'application des règles générales imposées aux prestataires en leur qualité de professionnels, notamment leur devoir de conseil vis-à-vis de leurs commanditaires.

[1] Des typologies des incidents de sécurité sont présentes dans l'annexe B de [ISO27035] et dans [ETSI_ISG_ISI].

I.1.3. Structure du présent document

Le chapitre I correspond à l'introduction du présent référentiel.

Le chapitre II présente les activités visées par le présent référentiel.

Le chapitre III présente les modalités de la qualification, qui atteste de la conformité des prestataires de réponse aux incidents de sécurité aux exigences qui leur sont applicables.

Le chapitre IV présente les exigences relatives aux prestataires.

Le chapitre V présente les exigences relatives aux analystes.

Le chapitre VI présente les exigences relatives au déroulement d'une prestation de réponse aux incidents de sécurité.

L'Annexe 1 présente les références des textes législatifs, réglementaires, normatifs et autres mentionnés dans le présent référentiel.

L'Annexe 2 présente les missions et compétences attendues des analystes du prestataire.

L'Annexe 3 présente des recommandations aux commanditaires de prestations de réponse aux incidents de sécurité.

L'Annexe 4 présente les prérequis à fournir par les commanditaires dans le cadre d'une prestation de réponse aux incidents de sécurité.

L'Annexe 5 illustre dans un schéma les étapes des trois types de prestations.

I.2. Identification du document

Le présent référentiel est dénommé « Prestataires de réponse aux incidents de sécurité – référentiel d'exigences ». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

I.3. Définitions et acronymes

I.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont :

ANSSI	Agence nationale de la sécurité des systèmes d'information
CERT-FR	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PDIS	Prestataire de détection d'incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité

I.3.2. Définitions

Les définitions ci-dessous s'appuient sur les normes de la suite [ISO27000] et notamment la norme [ISO27035] relative à la gestion des incidents de sécurité, la norme [ISO27037] relative à l'identification, la collecte, l'acquisition et la préservation de preuves numériques ainsi que sur la stratégie nationale pour la sécurité du numérique [STRAT_NUM].

Analyste – personne réalisant une activité d'analyse pour le compte d'un prestataire (pilotage technique, analyse système, analyse réseau, analyse de codes malveillants).

Analyste référent – analyste système, réseau ou de code malveillant responsable de l'équipe d'analyse pour une prestation de recherche d'indicateurs de compromission ou une investigation numérique sur périmètre restreint ; c'est le pendant du pilote requis pour une investigation sur large périmètre.

Commanditaire - entité faisant appel au service de réponse aux incidents de sécurité.

Convention de service – accord écrit entre un commanditaire et un prestataire pour la réalisation de la prestation. Dans le cas où le prestataire est un organisme privé, la convention inclut le contrat.

État de l'art – ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.

Évènement lié à la sécurité de l'information – occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une violation possible de la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité de l'information.

Incident de sécurité – un ou plusieurs évènement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et/ou de menacer la sécurité de l'information.

Indicateur de compromission – combinaison d'informations techniques représentatives d'une manifestation de compromission, dont la présence peut être identifiée à partir de l'analyse d'un système, d'un code malveillant ou de traces réseau.

Investigation – procédé visant à collecter et analyser tout élément technique, fonctionnel ou organisationnel du système d'information permettant de qualifier une situation suspecte en incident de sécurité et de comprendre le mode opératoire et l'étendue d'un incident de sécurité sur un système d'information.

Mesure de sécurité – ensemble des moyens techniques et non techniques de protection, permettant à un système d'information de réduire le risque d'atteinte à la sécurité de l'information.

Périmètre – environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, concerné par la prestation.

Posture – ensemble composé de la démarche de réponse à incident, du niveau de discrétion à adopter vis-à-vis de l'attaquant, des ressources à engager et du calendrier des activités.

Prestataire – organisme proposant une offre de service de réponse aux incidents de sécurité conforme au référentiel.

Rapport d'analyse – document de synthèse élaboré par l'équipe d'analyse et remis au commanditaire à l'issue de la prestation.

Référentiel – le présent document.

Responsable d'équipe d'analyse – personne responsable de la prestation en réponse aux incidents de sécurité et de la constitution de l'équipe d'analystes, en particulier de la complémentarité de leurs compétences. Il est chargé de définir, de proposer et de suivre une feuille de route, de coordonner, d'orienter et de contrôler les activités associées, ainsi que d'assurer la capitalisation des résultats. Dans le cas des prestations d'investigation numérique sur large périmètre, il doit également définir une posture et proposer des mesures de remédiation adaptées. Selon le type de prestation, le responsable de l'équipe d'analyse est soit un analyste référent, soit un pilote.

Sécurité de l'information – Préservation de la confidentialité, l'intégrité et la disponibilité de l'information

Sonde – dispositif technique destiné à repérer des activités anormales, suspectes ou malveillantes sur le périmètre supervisé. Une sonde est considérée comme une source de collecte dans le cadre d'un service de détection des incidents de sécurité.

Sous-traitance – opération par laquelle le prestataire confie sous sa responsabilité à une entité tout ou partie de l'exécution d'un contrat conclu avec le commanditaire.

Système d'information – ensemble organisé de ressources (matériel, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

Système d'information cible – système d'information concerné par la prestation. Il est inclus dans le périmètre,

Tiers – personne ou organisme reconnu comme indépendant du prestataire et du commanditaire.

Victime – organisme dont tout ou partie du système d'information fait l'objet d'un incident de sécurité d'origine malveillante ou d'une suspicion d'un tel incident. Le commanditaire de la prestation peut être ou non la victime.

Vulnérabilité – faiblesse d'un bien ou d'une mesure pouvant être exploitée par une menace ou un groupe de menaces.

II. Prestations et activités visées par le référentiel

Ce chapitre présente les différents types de prestations de réponse aux incidents et activités traitées dans le référentiel.

II.1. Types de prestations

II.1.1. Recherche d'indicateurs de compromission

La recherche d'indicateurs de compromission consiste en une recherche ciblée sur le périmètre de la prestation, une analyse des résultats afin d'identifier la présence des indicateurs de compromission et la recommandation d'une suite à donner.

II.1.2. Investigations numériques sur périmètre restreint

L'investigation numérique sur périmètre restreint consiste en une investigation sur des éléments collectés par le prestataire ou remis par le commanditaire. Elle est réalisée sur un périmètre de taille restreinte (un à une dizaine de postes) et se conclut par la recommandation d'une suite à donner. Le type d'analyse est toujours précisé pour ce type de prestation. C'est une combinaison des activités d'analyse : analyse système, analyse réseau et analyse de codes malveillants,

II.1.3. Investigations numériques sur large périmètre

L'investigation numérique sur large périmètre consiste en une investigation sur des éléments collectés par le prestataire ou remis par le commanditaire. Elle est réalisée sur un périmètre de grande taille. Elle s'appuie sur le déploiement d'une structure opérationnelle de réponse aux incidents et sur un processus itératif d'analyse. Elle couvre plusieurs étapes, de la compréhension initiale de l'incident à la préconisation de mesures de remédiation. Elle est souvent déclenchée à la suite d'une recherche d'indicateurs de compromission ou d'une investigation numérique sur périmètre restreint.

II.2. Activités

Les prestations de réponse aux incidents mettent en jeu plusieurs activités. Selon le type de prestation, les activités représentées sont différentes.

II.2.1. Pilotage technique

Le pilotage technique couvre la définition, le pilotage et le contrôle des activités techniques nécessaires au traitement d'un incident de sécurité, ainsi que la communication avec le commanditaire tout au long de la prestation. Le responsable de l'équipe d'analyse d'une prestation d'investigation numérique sur large périmètre est un pilote technique[2].

II.2.2. Analyse système

L'analyse système consiste à collecter des informations techniques sur des équipements (terminaux utilisateur, serveurs, périphériques, etc.) ou à l'échelle d'un système d'information puis à les analyser et en extraire des indicateurs de compromission. Elle a pour objectif d'identifier le périmètre d'une compromission et le mode opératoire d'un attaquant. Elle permet la préconisation de mesures de remédiation pour limiter une compromission, enrayer l'activité d'un attaquant et durcir la sécurité du système d'information cible de la prestation. Elle peut également intervenir en prévention par la recherche d'indicateurs de compromission sur différents types de systèmes.

[2] Comme défini au chapitre VI.5.1, pour les prestations de recherche d'indicateurs de compromission et d'investigation numérique sur périmètre restreint, le responsable d'équipe d'analyse est un analyste référent.

II.2.3. Analyse réseau

L'analyse réseau consiste à collecter des évènements réseau à partir de systèmes de journalisation, de supervision et de détection des incidents de sécurité, existants ou de circonstance, puis à les analyser et en extraire des indicateurs de compromission. Elle a pour objectif d'identifier le périmètre d'une compromission et le mode opératoire d'un attaquant. Elle permet la préconisation de mesures de remédiation pour limiter une compromission, enrayer l'activité d'un attaquant et durcir la sécurité du système d'information cible de la prestation. Elle peut également intervenir en prévention par la recherche d'indicateurs de compromission dans des journaux ou informations collectées à partir d'une source réseau.

II.2.4. Analyse de codes malveillants

L'analyse de codes malveillants consiste à identifier et analyser les codes malveillants pour comprendre leurs comportements, en extraire des indicateurs de compromission puis enfin à préconiser des mesures de remédiation pour limiter une compromission, enrayer l'activité d'un attaquant et durcir la sécurité du système d'information cible de la prestation.

III. Qualification des prestataires de réponse aux incidents de sécurité

III.1. Modalités de la qualification

Le référentiel contient les exigences et les recommandations à destination des prestataires de réponse aux incidents de sécurité.

La qualification d'un prestataire est réalisée conformément au processus de qualification d'un prestataire de service de confiance [QUAL_SERV_PROCESS] et permet d'attester de la conformité du prestataire aux exigences du référentiel.

Un organisme peut demander la qualification d'un service de réponse aux incidents de sécurité interne, c'est-à-dire un service utilisé pour répondre à tout ou partie de ses propres besoins en réponse aux incidents de sécurité. Dans ce cas, le processus de qualification ainsi que les exigences applicables pour obtenir la qualification sont strictement identiques à ceux définis dans le présent référentiel. Le terme « prestataire » désigne donc indifféremment un organisme offrant des prestations de réponse aux incidents de sécurité pour son propre compte ou pour le compte d'autres organismes.

Les exigences doivent être respectées par les prestataires pour obtenir la qualification.

Les recommandations sont données à titre de bonnes pratiques et ne font pas l'objet de vérification pour obtenir la qualification.

Le référentiel donne également des recommandations aux commanditaires dans l'Annexe 3. Ces recommandations ne font pas l'objet de vérification pour obtenir la qualification.

La qualification ne se substitue pas à l'inscription sur une liste d'experts en investigation numérique auprès d'une cour d'appel et n'accorde pas de droits afférents à la qualité d'expert.

III.2. Portée de la qualification

Pour être qualifié, un prestataire doit répondre à toutes les exigences du présent référentiel sur la portée choisie.

Pour être qualifié dans le cadre du décret n° 2015-350 [D_2015_350], un prestataire doit, en plus des exigences du présent référentiel, répondre aux exigences supplémentaires définies dans [PRIS_LPM].

Le prestataire de réponse à incidents peut demander la qualification pour tout ou partie des prestations décrites au chapitre II.1 :

- recherche d'indicateurs de compromission ;
- investigation numérique sur périmètre restreint ;
- investigation numérique sur large périmètre.

Pour chacun de ces types de prestations, plusieurs activités décrites au chapitre II.2 sont requises :

- recherche d'indicateurs de compromission : analyse système et analyse réseau ;
- investigation numérique sur périmètre restreint : analyse système, analyse réseau et/ou analyse de codes malveillants ;
- investigation numérique sur large périmètre : pilotage technique, analyse système, analyse réseau et analyse de codes malveillants.

Est considérée comme une prestation qualifiée au sens du référentiel, une prestation respectant une des démarches décrites au chapitre VI, dont les activités sont réalisées par un ou plusieurs analystes évalués individuellement et reconnus compétents pour ces activités, conformément au chapitre V et à l'Annexe 2 et travaillant pour un prestataire respectant les exigences du chapitre IV.

Est considérée comme une prestation qualifiée au sens du décret n° 2015-350 [D_2015_350], une prestation qualifiée au sens du référentiel et respectant les exigences supplémentaires définies dans [PRIS_LPM].

Les prestataires qualifiés gardent la faculté de réaliser des prestations en dehors du périmètre pour lequel ils sont qualifiés, mais ne peuvent, dans ce cas, se prévaloir de la qualification sur ces prestations.

Une prestation de réponse aux incidents de sécurité qualifiée peut être associée à la réalisation d'autres prestations complémentaires (audit, développement, intégration de produits de sécurité, supervision et détection, etc.) sans perdre le bénéfice de la qualification. Un prestataire de réponse aux incidents de sécurité qualifié peut notamment être qualifié pour d'autres familles de prestataires de services de confiance (PASSI, PDIS).

III.3. Avertissement

Une prestation de réponse aux incidents de sécurité non qualifiée, c'est-à-dire ne respectant pas intégralement les exigences du présent référentiel, peut potentiellement exposer le commanditaire à certains risques et notamment la fuite d'informations confidentielles, la compromission, la perte ou l'indisponibilité de son système d'information. Ainsi, dans le cas d'une prestation non qualifiée, il est recommandé au commanditaire d'exiger de la part de son prestataire un document listant l'ensemble des exigences de ce référentiel non couvertes dans le cadre de sa prestation, afin de connaître les risques auxquels il s'expose.

IV. Exigences relatives au prestataire de réponse aux incidents de sécurité

IV.1. Exigences générales

a) Le prestataire doit être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de sa prestation.

b) Le prestataire doit respecter la législation et la réglementation en vigueur sur le territoire national.

c) Le prestataire doit décrire l'organisation de son activité de réponse aux incidents de sécurité auprès du commanditaire.

d) Le prestataire doit, en sa qualité de professionnel, avoir un devoir de conseil vis-à-vis du commanditaire.

e) Le prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte du commanditaire dans le cadre de la prestation et en particulier les éventuels dommages causés au commanditaire.

f) Le prestataire doit souscrire une assurance professionnelle couvrant les éventuels dommages causés au commanditaire et notamment à son système d'information dans le cadre de la prestation.

   Le prestataire et le commanditaire peuvent préciser les types de dommages concernés et les modalités de partage des responsabilités au sein de la convention, en tenant compte de toutes les éventuelles activités sous-traitées. Le prestataire peut s'exonérer de tout ou partie de sa responsabilité s'il est avéré que le dommage éventuellement subi par le commanditaire résulte d'un défaut d'information de ce dernier.

g) Le prestataire doit s'assurer du consentement du commanditaire avant toute communication d'informations obtenues ou produites dans le cadre de la prestation.

h) Le prestataire doit garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses.

i) Le prestataire doit apporter une preuve suffisante que les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de ses prestations à l'égard du commanditaire ou de provoquer des conflits d'intérêts.

j) Le prestataire doit réaliser la prestation de manière impartiale, en toute bonne foi et dans le respect du commanditaire, de son personnel et de son infrastructure.

k) Le prestataire doit demander au commanditaire de lui communiquer les éventuelles exigences légales et réglementaires spécifiques auquel il est soumis et notamment celles liées à son secteur d'activité.

l) Le prestataire doit informer le commanditaire lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementale et doit l'accompagner dans cette démarche si ce dernier en fait la demande.

m) Le prestataire doit réaliser sa prestation dans le cadre d'un accord de non-divulgation[3] et d'une convention de réponse aux incidents de sécurité approuvée formellement et par écrit par le commanditaire, et conforme aux exigences du chapitre VI.2.

n) Le prestataire doit prévoir l'enregistrement et le traitement des plaintes portant sur sa prestation déposées par les commanditaires et les tiers (hébergeurs, sous-traitants, etc.).

[3] Pour les étapes de qualification préalable d'aptitude à la réalisation de la prestation (chapitre VI.1) et potentiellement de compréhension de l'incident de sécurité et de l'environnement (chapitre VI.3).

IV.2. Charte d'éthique

a) Le prestataire doit disposer d'une charte d'éthique prévoyant notamment que :

- les prestations sont réalisées avec loyauté, discrétion et impartialité ;
- les analystes ne recourent qu'aux méthodes, outils et techniques validés par le prestataire ;
- les analystes s'engagent à ne pas divulguer d'informations à un tiers, même anonymisés et décontextualisées, obtenues ou générées dans le cadre de leurs activités, y compris aux autres analystes du prestataire non concernés par la prestation, sauf autorisation formelle et écrite du commanditaire et du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques[4] (CERT-FR) ;
- les analystes signalent au commanditaire tout contenu manifestement illicite découvert durant la prestation ;
- les analystes s'engagent à respecter la législation et la réglementation nationale en vigueur ainsi que les bonnes pratiques liées à leurs activités.

b) Le prestataire doit faire appliquer la charte d'éthique.

IV.3. Gestion des ressources et des compétences

a) Le prestataire doit employer un nombre suffisant d'analystes et éventuellement recourir à des sous-traitants pour assurer totalement et dans tous leurs aspects les activités de réponse aux incidents de sécurité pour lesquelles il a établi des conventions avec des commanditaires. Le prestataire doit s'assurer, pour chaque prestation, que les analystes désignés disposent des qualités et des compétences requises. Chaque analyste doit disposer d'une attestation individuelle de compétence[5] pour les activités qu'il réalise et doit la présenter au commanditaire au début de toute prestation.

b) Le prestataire doit s'assurer du maintien à jour des compétences des analystes dans les activités pour lesquelles ils ont obtenu une attestation individuelle de compétence[6]. Pour cela, le prestataire doit disposer d'un processus de formation continue et permettre à ses analystes d'assurer une veille technologique.

c) Le prestataire doit, en matière de recrutement, procéder à une vérification des formations, compétences et références professionnelles des analystes candidats et de la véracité de leur *curriculum vitae*.

d) Le prestataire est responsable des méthodes, outils (logiciels ou matériels) et techniques utilisés par ses analystes et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration, etc.) pour la réalisation de la prestation. Pour cela, le prestataire doit assurer une veille technologique sur leur mise à jour et leur pertinence (efficacité et confiance).

e) Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation.

f) Le prestataire doit disposer d'une base d'indicateurs de compromission régulièrement mise à jour et intégrant les indicateurs de compromission :

- issus des prestations réalisées ;
- issus de sa veille technique sur les vulnérabilités et les codes malveillants ;
- transmis par des partenaires.

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

[5] Voir [QUAL_SERV_PROCESS].

g) Le prestataire doit mettre en place un processus de sensibilisation des analystes à la législation en vigueur sur le territoire français applicable à leurs missions.

h) Le prestataire doit s'assurer que les analystes ne font pas l'objet d'une inscription au bulletin n°3 du casier judiciaire.

i) Le prestataire doit élaborer un processus disciplinaire à l'intention des analystes ayant enfreint les règles de sécurité ou la charte d'éthique.

IV.4. Protection de l'information

a) Le prestataire doit protéger au minimum au niveau *Diffusion restreinte* [IGI_1300] [II_901] les informations sensibles relatives à la prestation, et notamment les documents transmis par le commanditaire, les informations collectées, les indicateurs de compromission, les constats, les mains courantes, les différents registres, la feuille de route et les rapports d'analyse.

b) Le prestataire doit respecter les règles établies par l'ANSSI et relatives aux mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau *Diffusion Restreinte*.

c) Le prestataire doit homologuer son système d'information au niveau *Diffusion Restreinte*.

d) Il est recommandé que le prestataire utilise la démarche décrite dans le guide [HOMOLOGATION] pour homologuer son système d'information.

e) Le prestataire doit appliquer le guide d'hygiène informatique de l'ANSSI [HYGIENE] sur le système d'information utilisé par le prestataire dans le cadre de ses prestations de réponse aux incidents de sécurité.

f) Le prestataire doit mettre en œuvre des mesures de protection spécifiques dans le cadre de la manipulation et du stockage des codes malveillants. Le prestataire doit assurer au minimum, sur les équipements et réseaux associés, un cloisonnement logique strict et une journalisation des évènements réseau.

g) Le prestataire doit mettre en place les mesures permettant d'assurer la confidentialité des indicateurs de compromission en fonction de leur niveau de sensibilité ou de classification et respecter les conditions d'utilisation associées.

V. Exigences relatives aux analystes

V.1. Aptitudes générales

a) Le pilote technique et les analystes référents doivent posséder les qualités personnelles identifiées au chapitre 7.2.3.4 de la norme [ISO19011].

b) L'analyste doit posséder les qualités personnelles identifiées au chapitre 7.2.2 de la norme [ISO19011].

c) Le pilote technique et les analystes référents doivent maîtriser la législation en vigueur sur le territoire français et applicable à leurs missions ainsi qu'à celles des analystes.

d) L'analyste système, l'analyste réseau et l'analyste de codes malveillants doivent être sensibilisés à la législation en vigueur sur le territoire français et applicable à leurs missions.

e) L'analyste doit disposer de qualités rédactionnelles et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible, en langue française.

f) L'analyste doit régulièrement mettre à jour ses compétences conformément aux processus de formation et de veille du prestataire (voir chapitre IV.3, paragraphe b)), par une veille active sur la méthodologie, les techniques et les outils utilisés dans le cadre de ses missions.

   Il est recommandé que l'analyste participe à l'évolution de l'état de l'art par une participation à des évènements professionnels de son domaine de compétence, à des travaux de recherche ou la publication d'articles.

V.2. Expérience

a) L'analyste doit avoir reçu une formation en technologies des systèmes d'information.

b) Il est recommandé que l'analyste justifie :

   - d'au moins deux années d'expérience dans le domaine de la sécurité des systèmes d'information ;
   - d'au moins une année d'expérience dans le domaine de la réponse aux incidents de sécurité.

V.3. Aptitudes et connaissances spécifiques aux activités de réponse aux incidents de sécurité

a) L'analyste doit maîtriser les bonnes pratiques en matière de gestion des incidents de sécurité décrites dans la norme [ISO27035].

b) L'analyste doit maîtriser les bonnes pratiques et la méthodologie de collecte et de préservation des preuves décrites dans la norme [ISO27037].

c) L'analyste doit réaliser la prestation conformément aux exigences du chapitre VI.

d) L'analyste doit assurer les missions selon son profil, telles que définies dans l'Annexe 2.

e) L'analyste doit disposer des compétences requises par son profil, telles que définies dans l'Annexe 2.

f) Il est recommandé que l'analyste soit sensibilisé à l'ensemble des autres activités pour lesquelles le prestataire demande la qualification.

V.4. Engagements

a) L'analyste doit avoir un contrat avec le prestataire.

b) L'analyste doit avoir signé la charte d'éthique élaborée par le prestataire (voir chapitre IV.2).

VI. Exigences relatives au déroulement d'une prestation de réponse aux incidents

Le prestataire peut réaliser trois types de prestations :

- recherche d'indicateurs de compromission ;
- investigation numérique sur périmètre restreint ;
- investigation numérique sur large périmètre.

Les exigences relatives au déroulement des prestations de réponse aux incidents de sécurité sont réparties selon différentes étapes. Selon leur type, les prestations se composent de la totalité ou d'un sous-ensemble des neuf étapes décrites dans ce chapitre. La succession des étapes pour chaque type de prestation est présentée dans le schéma de l'Annexe 5.

Les étapes et exigences du chapitre IV s'appliquent aux trois types de prestations, sauf si elles sont précédées d'un ou plusieurs identifiants entre crochets. Dans ce cas, elles ne s'appliquent qu'aux types de prestations indiqués par leur identifiant.

Les identifiants utilisés sont :

- REC pour la recherche d'indicateurs de compromission ;
- IPR pour l'investigation numérique sur périmètre restreint ;
- ILP pour l'investigation numérique sur large périmètre.

VI.1. Étape 1 - Qualification préalable d'aptitude à la réalisation de la prestation

[IPR, ILP] La qualification préalable d'aptitude à la réalisation de la prestation consiste pour le prestataire à évaluer s'il est en mesure de réaliser la prestation.

a) [IPR, ILP] Le prestataire doit signer un accord de non-divulgation avec le commanditaire afin d'assurer la confidentialité des informations que ce dernier lui transmet. Cet accord doit être signé par un représentant légal du commanditaire et du prestataire.

b) [IPR, ILP] Le responsable d'équipe d'analyse doit sensibiliser le commanditaire sur l'intérêt d'utiliser des moyens de communication sécurisés et dédiés avec le prestataire. Dans le cas d'une prestation [ILP], ces moyens doivent être déconnectés du système d'information compromis, afin de ne pas permettre à l'attaquant de suivre les opérations en cours (voir Annexe 3 III, paragraphe l).

c) [IPR] Le prestataire doit demander au commanditaire de lui fournir les informations de contexte sur la situation suspecte qui a conduit à la demande de prestation d'investigation.

   [ILP] Le prestataire doit demander au commanditaire de lui fournir les informations de contexte sur l'incident de sécurité et notamment celles identifiées dans l'Annexe 4.

d) [IPR] Le prestataire doit, sur la seule base des informations transmises par le commanditaire, évaluer de manière impartiale s'il est en mesure de réaliser la prestation en prenant en compte notamment les facteurs suivants : complexité du périmètre, complexité de la situation, types d'activités à réaliser[6], nombre d'analystes à engager, disponibilité des ressources en interne, etc.

[6] Conformément au chapitre III.2, un prestataire ne peut réaliser que les types de prestations pour lesquelles il dispose des compétences d'analyse requises.

[ILP] Le prestataire doit, sur la seule base des informations transmises par le commanditaire[7], évaluer de manière impartiale s'il est en mesure de réaliser la prestation en prenant en compte notamment les facteurs suivants : complexité du système d'information cible, complexité de l'incident de sécurité, périmètre de la compromission, types d'activités à réaliser, nombre d'analystes à engager, disponibilité des ressources en interne, etc.

e) [IPR, ILP] Le prestataire doit informer le commanditaire des résultats de la qualification préalable d'aptitude à la réalisation de la prestation. Il doit notamment indiquer sa capacité à répondre totalement, partiellement ou non à la prestation. Le cas échéant, il doit indiquer les activités envisagées et les ressources associées (nombre d'intervenants et durée de la prestation).

VI.2. Étape 2 - Établissement d'une convention

a) Le prestataire doit établir une convention de service avec le commanditaire avant l'exécution de la prestation.

b) La convention doit être signée par un représentant légal du commanditaire et du prestataire.

VI.2.1. Modalités de la prestation

La convention de service doit :

a) décrire le périmètre initial de la prestation, la démarche générale de réponse aux incidents de sécurité adaptée au type de prestation, les activités, les modalités de la prestation (objectifs, jalons, livrables attendus en entrée, prérequis, etc.) et les éventuelles limites de la prestation[8] ;

b) définir les livrables attendus en sortie, les réunions d'ouverture et de clôture, les publics destinataires, leur niveau de sensibilité ou de classification et les modalités associées ;

c) décrire les moyens techniques (matériel et outils) et organisationnels mis en œuvre par le prestataire dans le cadre de sa prestation ;

d) décrire les méthodes de communication qui seront employés lors de la prestation entre le prestataire et le commanditaire ;

e) préciser les moyens logistiques devant être mis à disposition du prestataire par le commanditaire (moyens matériels, humains, techniques, etc.) ;

f) définir les règles de titularité des éléments protégés par la propriété intellectuelle tels que les outils développés spécifiquement par le prestataire dans le cadre de la prestation, les indicateurs de compromission ou le rapport d'analyse ;

g) préciser les actions qui ne peuvent être menées sur le système d'information cible ou sur les informations collectées sans autorisation expresse du commanditaire et éventuellement accord ou présence du commanditaire, ainsi que les modalités associées (mise en œuvre, personnes présentes, durée, plage horaire, exécutant, description des données sensibles et des actions autorisées, etc.) ;

h) décrire le processus d'enregistrement et de traitement des plaintes par le commanditaire ou les tiers, ainsi que la marche à suivre pour le dépôt de plainte ;

i) [IPR, ILP] définir les moyens assurant la traçabilité entre le commanditaire et le prestataire des informations et supports matériels remis pour analyse.

[7] Durant la phase de qualification préalable d'aptitude à la réalisation de la prestation, le prestataire n'intervient pas sur le système d'information de la victime.

[8] Exemple : Pour une prestation IPR réalisée par un prestataire disposant d'analystes système et/ou réseau, le prestataire doit indiquer qu'il ne réalisera pas d'analyse de codes malveillants.

VI.2.2. Organisation

La convention de service doit :

a) préciser le nom du correspondant en charge, chez le commanditaire, de mettre en relation le prestataire avec les différents correspondants impliqués ;

b) préciser les noms, rôles, responsabilités ainsi que les droits et besoins d'en connaître des personnes désignées par le prestataire et le commanditaire. Cette exigence est d'autant plus importante si la prestation ou l'existence de l'incident de sécurité ne doit pas être divulguée ;

c) stipuler que le prestataire doit, le cas échéant, collaborer avec des prestataires tiers qui travaillent pour le compte du commanditaire (qui auront été spécifiquement désignés par le commanditaire) et distinguer clairement les responsabilités du prestataire tiers. Cette exigence doit notamment permettre au prestataire de collaborer avec un prestataire de détection d'incidents de sécurité ;

d) stipuler que le prestataire ne fait pas intervenir d'analystes n'ayant pas de relation contractuelle avec lui, n'ayant pas signé sa charte d'éthique ou ayant fait l'objet d'une inscription au bulletin n°3 du casier judiciaire.

VI.2.3. Responsabilités

La convention de service doit :

a) stipuler que le prestataire ne réalisera la prestation qu'après une approbation formelle et écrite du commanditaire ;

b) stipuler que le prestataire informe le commanditaire en cas de manquement à la convention ;

c) stipuler que le prestataire s'engage à ce que les actions réalisées dans le cadre de la prestation restent strictement en adéquation avec les objectifs de la prestation ;

d) stipuler que le commanditaire dispose de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.) ou qu'il a recueilli l'accord des éventuels tiers, et notamment de ses prestataires ou partenaires, dont les systèmes d'information entrent dans le périmètre de la prestation ;

e) stipuler que le commanditaire et le prestataire remplissent toutes les obligations légales et réglementaires nécessaires à la collecte et à l'analyse d'informations ;

f) stipuler que le commanditaire autorise provisoirement le prestataire, aux seules fins de réaliser la prestation, à accéder et se maintenir dans tout ou partie du périmètre et à effectuer des traitements sur les données hébergées, quelle que soit la nature de ces données, conformément aux réglementations de protection de ces types de données ;

g) stipuler que le commanditaire autorise provisoirement le prestataire à reproduire, collecter et analyser, aux seules fins de réaliser la prestation, des données appartenant au périmètre du système d'information cible;

h) définir les responsabilités et les précautions d'usage à respecter par l'ensemble des parties concernant les risques potentiels liés à la prestation, en matière de confidentialité des informations collectées et analysées ainsi qu'en matière de disponibilité et d'intégrité du système d'information ciblé ;

i) stipuler que le prestataire dispose d'une assurance professionnelle couvrant les éventuels dommages causés lors de la réalisation des activités d'analyse, le cas échéant, préciser la couverture de celle-ci et inclure l'attestation d'assurance.

VI.2.4. Confidentialité

La convention de service doit :

a) stipuler que le prestataire ne collecte et n'analyse que les informations strictement nécessaires au bon déroulement de la prestation ;

b) reprendre les modalités suivantes de divulgation à un tiers d'informations anonymisées et décontextualisées relatives à la prestation (informations et supports collectés, livrables, indicateurs de compromission, etc.):

- le commanditaire doit autoriser formellement et par écrit la divulgation ;
- le centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques[9] (CERT-FR) doit également autoriser formellement et par écrit la divulgation. Sans réponse de ce dernier et après un délai de 10 jours ouvrés, le prestataire disposant de l'autorisation du commanditaire peut procéder à la divulgation ;
- les informations divulguées à un tiers doivent être protégées en confidentialité, conformément à leur niveau de sensibilité ou de classification ;
- toute action de divulgation doit être accompagnée d'une information au centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR).

c) préciser les modalités d'accès, de stockage, de transport, de reproduction, de destruction et de restitution des informations et, le cas échéant, les supports matériels collectés et analysés par le prestataire. Si besoin, le prestataire doit définir, en collaboration avec le commanditaire, les modalités selon les types d'informations ou de supports matériels ;

d) stipuler que le prestataire peut, sauf refus formel et écrit du commanditaire, conserver certains types d'informations liées à la prestation une fois celle-ci terminée. Le prestataire devra identifier ces types d'informations dans la convention (ex : codes malveillants, scénarios d'attaque, indicateurs de compromission, etc.) ;

e) stipuler que le prestataire anonymise et décontextualise (suppression de toute information permettant d'identifier le commanditaire, de toute information à caractère personnel, etc.) l'ensemble des informations que le commanditaire l'autorise à conserver ;

f) stipuler que le prestataire détruit l'ensemble des informations relatives au commanditaire à l'issue de la prestation à l'exception de celles pour lesquelles il a reçu une autorisation de conservation de la part du commanditaire ;

g) stipuler que le prestataire, sauf refus formel et écrit du commanditaire, transmet au centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) ces éléments anonymisés et décontextualisés, ainsi que leur niveau de sensibilité ou de classification et leurs conditions d'utilisation.

VI.2.5. Lois et réglementations

La convention de service doit :

a) être rédigée en français. Le prestataire doit fournir une traduction de courtoisie de la convention de service si le commanditaire en fait la demande ;

b) stipuler que seule la version française fait foi, notamment dans le cadre d'un litige ;

c) stipuler que la législation applicable à la convention de service est la législation française ;

d) préciser les moyens techniques et organisationnels mis en œuvre par le prestataire pour le respect de la législation française applicable, notamment ceux concernant :

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

- les données à caractère personnel [LOI_IL],
- l'abus de confiance [CP_ART_314-1],
- le secret des correspondances privées [CP_ART_226-15],
- le secret médical [CSP_ART_L1110-4],
- l'atteinte à la vie privée [CP_ART_226-1],
- l'accès ou le maintien frauduleux à un système d'information [CP_ART_323-1],
- le secret professionnel [CP_ART_226-13], le cas échéant sans préjudice de l'application de l'article 40 alinéa 2 du Code de procédure pénale relatif au signalement à une autorité judiciaire ;

e) préciser les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire et notamment celles liées à son secteur d'activité ;

f) prévoir les mesures à mettre en place par le prestataire dans le cadre d'une affaire judiciaire, civile ou arbitrale. Dans ce cas, il est recommandé de faire appel à un expert judiciaire [LOI_EJ] ;

g) définir la durée de conservation des informations liées à la prestation et notamment les informations collectées et les incidents de sécurité détectés. Si besoin, une distinction de la durée de conservation peut être faite en fonction des types d'information. La durée minimale de conservation est de six mois sous réserve de la législation et de la réglementation française en vigueur.

VI.2.6. Sous-traitance

a) La convention doit préciser que le prestataire peut si nécessaire sous-traiter une partie des activités à un autre prestataire qualifié sur ces activités conformément aux exigences du référentiel qui lui sont applicables sous réserve que :
   - il existe une convention ou un cadre contractuel documenté entre le prestataire et le sous-traitant ;
   - le recours à la sous-traitance est connu et formellement accepté par écrit par le commanditaire.

b) La convention doit préciser que le prestataire peut si nécessaire faire intervenir un expert sur une partie des activités, pour des besoins ponctuels, sous réserve que :
   - il existe une convention ou un cadre contractuel documenté entre le prestataire et l'expert ;
   - le recours à un expert est connu et formellement accepté par écrit par le commanditaire ;
   - l'expert est encadré par le responsable de l'équipe d'analyse ;
   - le domaine d'expertise n'est pas une des activités décrite au chapitre II.2.

VI.2.7. Livrables

a) La convention doit préciser que tous les livrables de la prestation sont fournis en langue française sauf si le commanditaire en fait la demande formelle et écrite.

VI.2.8. Qualification

La convention de service doit :

a) indiquer que la prestation réalisée est :
   - soit une prestation qualifiée et inclure l'attestation de qualification du prestataire et des éventuels sous-traitants qualifiés ;
   - soit une prestation non qualifiée. Dans ce cas, le prestataire doit sensibiliser le commanditaire aux risques de ne pas exiger une prestation qualifiée.

b) indiquer que les analystes disposent d'une attestation individuelle de compétence pour les activités d'analyse.

VI.3. Étape 3 – Compréhension de la situation et de l'environnement

L'élaboration de la posture nécessite au préalable une phase de compréhension de l'incident de sécurité et de l'environnement et des risques associés.

a) [ILP] Le prestataire peut, dans certains cas d'urgence et avec l'accord du commanditaire, réaliser les phases de compréhension de l'incident de sécurité et de son environnement en l'absence de convention, sur la base d'un accord de non-divulgation signé par le prestataire et le commanditaire et à la condition que le prestataire n'intervienne pas sur le système d'information cible.

VI.3.1. Compréhension de la situation

a) [IPR, ILP] Les prérequis fournis et les échanges avec le commanditaire doivent permettre de réaliser une première compréhension de la situation. Dans le cas d'un incident de sécurité avéré, l'objectif est d'apprécier le caractère malveillant des éléments remontés par le commanditaire (voir chapitre VI.6.1). Si le caractère malveillant n'est pas avéré, les étapes suivantes peuvent être remises en question.

VI.3.2. Compréhension de l'environnement

a) Le prestataire doit acquérir une vision globale du système d'information cible. [IPR, ILP] Il doit ainsi demander au commanditaire des compléments d'informations techniques par rapport à ceux déjà transmis en phase de qualification préalable d'aptitude à la réalisation de la prestation (voir chapitre VI.1 et Annexe 4).

b) Le prestataire doit définir et mettre en œuvre une démarche pragmatique de compréhension du système d'information cible pour disposer d'une connaissance fidèle de l'existant.

c) Le prestataire doit identifier les contraintes géographiques associées au système d'information cible (ex. : réseau local, multi-sites, international, etc.).

d) Le prestataire doit demander au commanditaire de l'informer des spécificités et des contraintes du système d'information cible ;

e) Le prestataire doit identifier le(s) fuseau(x) horaire(s) utilisé(s) dans le système d'information cible et choisir le fuseau horaire de référence qui sera utilisé tout au long de la prestation ;

f) Le prestataire doit s'assurer que le commanditaire a identifié correctement toutes les dépendances et interconnexions du système d'information cible (partenaires, sous-traitants, etc.).

VI.4. Étape 4 – Élaboration de la posture initiale

a) [ILP] Le prestataire doit proposer au commanditaire une posture initiale identifiant notamment :

- le niveau de discrétion à adopter par le prestataire vis-à-vis de l'attaquant, en prenant en compte les risques liés à la situation :
    - élevé : le prestataire réalise ses activités sans possibilité de détection informatique par l'attaquant (copie de disques sur systèmes éteints, collecte d'informations sur des équipements inaccessibles par l'attaquant, etc.). Les activités réalisées par le prestataire n'entravent pas les opérations de l'attaquant, ses moyens et ses canaux de communication ne sont pas modifiés ou supprimés,
    - moyen : le prestataire réalise ses activités avec une faible probabilité de détection informatique (collecte d'informations confondues avec l'activité normale d'un administrateur ou utilisateur, actions de sécurisation réalisées par un administrateur, etc.). Les activités du prestataire entravent partiellement ou totalement les opérations de l'attaquant, mais n'apparaissent pas nécessairement dirigées contre lui, ses moyens et canaux de communication sont restreints (limitation de la bande passante, durcissement de la configuration, extinction de postes compromis, etc.),

- faible : le prestataire réalise ses activités sans se préoccuper de la présence de l'attaquant. Les activités du prestataire entravent partiellement ou totalement les opérations de l'attaquant et ne lui laissent aucun doute quant à la détection de sa présence. Les canaux de communication et moyens de l'attaquant sont bloqués ou supprimés ;

En cas de présence de l'attaquant sur le système, si aucun moyen ne permet de remédier rapidement et durablement à la compromission, il est recommandé que le prestataire adopte une démarche la plus discrète possible vis-à-vis de l'attaquant afin d'éviter d'éveiller ses soupçons et de l'amener à changer son mode opératoire au profit d'un mode plus furtif ;

- la démarche générale de réponse à incident et ses grandes étapes, en considération des spécificités et contraintes du système d'information cible et de l'incident ;
- les activités à réaliser, les informations à collecter, le nombre d'analystes à engager et le calendrier associé[10].

b) [ILP] Le prestataire doit établir sa posture en fonction de sa compréhension de l'incident de sécurité et de l'environnement.

c) [ILP] Le responsable d'équipe d'analyse doit définir et tenir à jour une feuille de route recensant l'intégralité des activités envisagées, en précisant les jalons associés.

d) [ILP] Le prestataire doit soumettre pour accord la posture initiale au commanditaire. La décision finale et la responsabilité de la posture initiale appartiennent au commanditaire.

VI.5. Étape 5 - Préparation de la prestation

VI.5.1. Mise en place de l'organisation

a) Le prestataire doit désigner un responsable d'équipe d'analyse afin de coordonner et suivre la prestation. Il est l'interlocuteur privilégié du commanditaire, et doit être désigné dans la convention :

- [REC] analyste référent (analyste système ou analyste réseau), choisi en fonction du contexte de la prestation ;
- [IPR] analyste référent (analyste système, réseau ou de code malveillant), choisi en fonction du contexte de la prestation ;
- [ILP] pilote technique.

b) Le responsable d'équipe d'analyse doit, dès le début de la préparation de la prestation, établir un contact avec le correspondant chez le commanditaire. Ce contact, formel ou informel, a notamment pour objectif de mettre en place les circuits de communication et de décision à respecter avec le commanditaire (voir Annexe 3 III, paragraphe d) et de préciser les modalités d'exécution de la prestation. Le responsable d'équipe d'analyse doit également obtenir du correspondant chez le commanditaire la liste des points de contact nécessaires à la réalisation de la prestation.

c) [ILP] Le responsable d'équipe d'analyse doit sensibiliser le commanditaire sur l'intérêt de mettre en place, si elle n'existe pas, une structure projet afin d'assurer le suivi de la prestation et d'arbitrer les décisions (voir Annexe 3 III, paragraphe d). Cette structure peut être rattachée à une cellule de crise déjà existante.

d) [ILP] Le responsable d'équipe d'analyse doit réaliser des points de synchronisation réguliers, de niveaux techniques ou stratégiques selon le besoin, avec le commanditaire.

e) [ILP] Le responsable d'équipe d'analyse doit sensibiliser le commanditaire sur l'intérêt d'élaborer un plan de communication relatif à l'incident de sécurité (voir Annexe 3 III, paragraphe f).

[10] Ces éléments définis dans la convention peuvent être revus lors de l'élaboration de la posture initiale et au cours de la prestation.

f) Le responsable d'équipe d'analyse doit sensibiliser le commanditaire sur l'intérêt de l'informer tout au long de la prestation des actions qu'il réalise sur le système d'information cible et qui pourraient affecter la prestation, en explicitant les risques associés (voir Annexe 3 III, paragraphe i).

VI.5.2. Mise en place des moyens opérationnels

VI.5.2.1. Gestion des ressources

a) Le responsable d'équipe d'analyse doit constituer une équipe d'analystes disposant des compétences nécessaires à la réalisation des activités définies :

- [REC, IPR] dans la convention de service ;
- [ILP] dans la posture.

b) Le responsable d'équipe d'analyse doit s'assurer que les analystes disposent d'une attestation individuelle de compétence[11] pour les activités qu'ils mènent.

Il peut, s'il dispose des compétences suffisantes et d'une attestation individuelle[12] de compétence, réaliser la prestation de réponse aux incidents de sécurité lui-même et seul.

Un analyste peut intervenir sur plusieurs types d'analyses s'il dispose des attestations individuelles de compétence associées.

Il peut également faire appel à de la sous-traitance dans les conditions définies dans la convention.

c) Le responsable d'équipe d'analyse doit constituer une équipe d'analystes dont le nombre et les compétences sont adaptés à la prestation et dans le cas d'investigation numérique sur large périmètre à la posture.

d) [IPR, ILP] Le responsable d'équipe d'analyse doit réévaluer régulièrement le profil et le nombre des analystes afin de s'assurer que l'engagement reste adapté à la prestation.

[ILP] La complexité de l'incident peut s'avérer en cours de prestation plus élevée que prévue dans la posture initiale (voir chapitre VI.6.2).

e) Le prestataire doit demander au commanditaire que lui soient fournis les privilèges nécessaires et suffisants pour réaliser les opérations de recherche ou de collecte, en respectant la politique de gestion des droits de appliquée sur le système d'information cible. Les comptes doivent être dédiés et démarqués. Le prestataire doit s'assurer que l'activité de ce compte est strictement conforme à celle attendue.

VI.5.2.2. Gestion des moyens logistiques et informatiques

a) Le responsable d'équipe d'analyse doit mettre en place et tenir à jour un registre centralisé, imputable et chronologique recensant pour chaque action réalisée par l'équipe d'analyse sur le système d'information cible :

- la date de l'action ;
- la description de l'action ;
- le motif de l'action ;
- le type de l'action (action manuelle, recherche réseau, déploiement de scripts, modification de fichiers, etc.) ;
- le système d'information et les fichiers concernés par l'action ;
- les noms des analystes ayant réalisé l'action.

[11] Voir [QUAL_SERV_PROCESS].

b) [IPR, ILP] Le responsable d'équipe d'analyse doit mettre en place et tenir à jour un registre centralisé recensant pour chaque information et support collecté:

- la date de collecte ou de remise de l'information ou du support ;
- les noms du cédant et de l'analyste prenant en compte les éléments ;
- le type d'information (technique ou métier) et le support de stockage associé ;
- le propriétaire légal de l'information ou du support ;
- le niveau de sensibilité ou de classification de l'information et du support associé.

c) Le responsable d'équipe d'analyse doit, en collaboration avec le commanditaire, définir les procédures et les clauses particulières associées aux informations et supports collectés :

- [IPR, ILP] remise et inventaire ;
- conditions de collecte, de transport, de traitement et de stockage ;
- conditions et limites de conservation ;
- obligations et modalités de destruction ou de restitution.

d) [ILP] Le responsable d'équipe d'analyse doit sensibiliser le commanditaire sur l'intérêt de lui mettre à disposition un environnement de travail et une zone sécurisée dédiée au stockage et à l'analyse des informations collectées et respectant les exigences réglementaires associées au niveau de sensibilité ou de classification de ces données (voir Annexe 3 III, paragraphe i). Cet environnement de travail doit être cloisonné du système d'information cible sur lequel des investigations sont en cours.

e) [ILP] Lorsque cela s'avère nécessaire, le responsable d'équipe d'analyse doit sensibiliser le commanditaire sur l'intérêt de lui mettre à disposition des moyens techniques (ex : équipements réseau, connexion Internet, etc.) pour mettre en place un environnement d'analyse sécurisé [HYGIENE] et déconnecté du système d'information cible (voir Annexe 3 III, paragraphe k).

f) Le prestataire doit utiliser des médias amovibles de stockage ou disques internes dédiés à la prestation. Ces médias peuvent être éventuellement fournis par le commanditaire puis restitués à la fin de la prestation.

VI.5.3. Mise en place de mesures de sauvegarde et de préservation

a) [ILP] Le responsable d'équipe d'analyse doit sensibiliser le commanditaire sur l'intérêt de sauvegarder et préserver les données, applications et équipements présents dans son système d'information et plus particulièrement sur le périmètre compromis et sur le périmètre analysé (voir Annexe 3 III, paragraphe c) afin de réduire les risques de sabotage pouvant atteindre la disponibilité ou intégrité des éléments du système d'information cible.

VI.5.4. Mise en place de procédures d'urgence

a) [ILP] Le responsable d'équipe d'analyse doit, en collaboration avec le commanditaire, définir des procédures d'urgence, parfois appelées procédures « bouton-rouge », permettant au commanditaire de réagir rapidement et conformément aux procédures d'urgence dans certains cas prédéfinis (ex. : exfiltration massive d'informations, sabotage, etc.). Les procédures d'urgence peuvent par exemple prévoir l'isolation complète d'un système d'information, l'isolation d'un système d'information vis-à-vis d'Internet, etc.

b) [ILP] Il est recommandé que le prestataire et le commanditaire soient en mesure de déclencher les procédures d'urgence en heures non ouvrées.

VI.6. Étape 6 - Exécution de la prestation

a) [ILP] La démarche de réponse doit s'appuyer sur un processus itératif d'adaptation constante de la posture initiale (voir chapitre VI.4).

b) La prestation ne doit débuter qu'après une réunion formelle d'ouverture au cours de laquelle les représentants habilités du prestataire et ceux du commanditaire confirment leur accord sur l'ensemble des modalités de la prestation.

c) La démarche doit comprendre au moins les phases suivantes :

- phase 1 : [ILP] révision de la compréhension de l'incident de sécurité et de l'environnement ;
- phase 2 : [ILP] révision de la posture ;
- phase 3 : collecte des informations ;
- phase 4 : analyse des informations collectées ;
- phase 5 : synthèse des analyses et capitalisation des indicateurs de compromission ;
- phase 6 : [ILP] révision des mesures de remédiation.

d) Pour chacune des phases, les missions définies par domaine de compétences doivent être respectées (voir Annexe 2).

VI.6.1. Phase 1 : révision de la compréhension de l'incident de sécurité et de l'environnement

a) [ILP] Le responsable d'équipe d'analyse doit maintenir à jour une synthèse du mode opératoire de l'attaquant et du périmètre concerné tout au long de la prestation :

- la (ou les) date(s) de compromission initiale(s) ;
- la chronologie générale des activités de l'attaquant, en précisant les différentes phases (reconnaissance, compromission initiale, interaction avec le contrôle commande, élévation de privilèges et déplacements latéraux, exfiltration, etc.) ;
- le périmètre précis de la compromission :
    - niveau de privilège obtenu par l'attaquant,
    - liste des machines compromises, comptes et domaines d'administration usurpés, etc.,
    - vecteur initial de compromission, vulnérabilités exploitées et outils utilisés,
    - matériel compromis (modification du système d'exploitation embarqué),
    - modifications logicielles sur le système d'information cible (ex : listes de contrôle d'accès, fichiers, etc.) ;
- les moyens de déplacement latéral :
    - vulnérabilités exploitées et outils utilisés,
    - techniques utilisées pour l'escalade de privilège sur le système d'information cible ;
- les moyens de communication utilisés par l'attaquant depuis l'extérieur,
    - moyens utilisés pour récupérer / collecter les données à exfiltrer,
    - moyens de persistance éventuels pour se maintenir sur le système,
    - moyens utilisés pour exécuter des commandes à distance sur des ressources internes,
    - moyen de communication physique ajouté par l'attaquant (carte sans-fil) ;
    - liste des équipements correspondants ;

- la liste des indicateurs de compromission ;
- les impacts métier pour le commanditaire :
    - risques associés à la compromission (ex. : exfiltration, destruction, etc.),
    - nature des éléments compromis, systèmes piégés ou détruits,
    - nature des données exfiltrées et champs d'intérêt,
    - etc.

b) [ILP] Afin de pouvoir compléter les résultats d'analyse de l'incident de sécurité, le prestataire peut être amené à réviser sa compréhension de l'environnement, par exemple pour apprécier le périmètre de compromission.

c) [ILP] Le prestataire doit présenter régulièrement et après toute découverte ou événement majeur (exfiltration en cours de données, sabotage, élargissement du périmètre de compromission, etc.) au commanditaire une synthèse de la compréhension de l'incident de sécurité afin de :

- caractériser la nature des informations ciblées afin de permettre au commanditaire d'évaluer la motivation présumée de l'attaquant (espionnage, intelligence économique, cybercriminalité, etc.) ;
- confirmer ou infirmer la présence active de l'attaquant dans le système d'information ;
- identifier le niveau de complexité de l'attaque (ex. : code malveillant spécifique ou générique) ;
- évaluer de manière plus précise le périmètre, les risques et l'impact de la compromission ;
- adapter la posture ;
- établir le plan d'action de remédiation associé au périmètre à assainir.

VI.6.2. Phase 2 : révision de la posture

a) [ILP] Le responsable d'équipe d'analyse doit réviser la posture à chaque nouvelle itération afin d'orienter les analyses, d'identifier les analyses à débuter, à poursuivre et à clôturer. En particulier, la présence active ou l'absence de l'attaquant sur le système d'information cible est de nature à modifier la posture initiale.

b) [ILP] Le responsable d'équipe d'analyse doit mettre à jour la feuille de route associée (voir chapitre VI.4).

c) [ILP] Le responsable d'équipe d'analyse doit, à chaque révision de la posture, assurer une restitution au commanditaire pour accord. La décision finale et la responsabilité de la posture initiale appartiennent au commanditaire.

VI.6.3. Phase 3 : collecte des informations

Cette étape a pour objectif de collecter les informations qui seront ensuite analysées.

La collecte des informations est réalisée par le prestataire, le commanditaire ou un tiers pour le compte du commanditaire. Dans tous les cas, la collecte est une étape fondamentale qui nécessite une approche méthodique. Si la collecte n'est pas réalisée par le prestataire, il doit sensibiliser le commanditaire aux risques de ne pas respecter les exigences du présent chapitre.

[REC] La phase 3 de collecte des informations est réalisée en vue d'une recherche hors ligne d'indicateurs de compromission. Dans le cas d'une recherche en ligne, aucune action de collecte préalable à l'analyse n'est nécessaire.

VI.6.3.1. Conditions de réalisation

a) La collecte des informations doit suivre une méthode dont les actions sont préalablement identifiées et dont la démarche est reproductible. Les analystes doivent réaliser la collecte des informations conformément à la méthode définie et [ILP] à la posture définie (voir chapitre VI.6.2) et peuvent notamment réaliser les opérations suivantes :

- collecte d'informations techniques ;
- copies physiques ;
- collecte de journaux d'évènements ;
- capture de flux.

b) [REC, IPR] Les analystes doivent collecter les informations permettant de rechercher les indicateurs de compromission à disposition de l'équipe d'analyse et pertinents pour la situation et l'environnement (voir chapitre VI.3).

[ILP] Les analystes doivent collecter les informations permettant de rechercher les indicateurs de compromission de l'incident capitalisés lors de la révision de la compréhension de la situation (voir chapitre VI.6.1) afin d'identifier l'étendue de l'éventuelle compromission.

c) [ILP] Le prestataire doit adapter la méthode de collecte à la posture préalablement convenue entre le prestataire et le commanditaire (voir chapitre VI.6.2). En particulier, si la méthode de collecte présente un risque pour la disponibilité du système d'information cible.

d) Les analystes ne doivent collecter que les informations strictement nécessaires au bon déroulement de la prestation conformément à la convention. Ils doivent mettre à disposition du commanditaire la liste des éléments qui seront collectés. Le commanditaire peut refuser la collecte de certains éléments. Néanmoins, les analystes doivent sensibiliser le commanditaire à l'importance de la collecte des éléments pour l'efficacité de la prestation.

e) Les analystes doivent s'accorder avec le commanditaire sur le déroulement des opérations de collecte (types d'éléments, périmètre, méthodes employées, calendrier, etc.).

f) Les analystes doivent identifier, en s'appuyant sur la phase de compréhension de l'environnement, les points de collecte système et réseau permettant de atteindre les objectifs de la prestation.

g) Les analystes doivent, au moment de la remise d'un support, remettre un document de prise en compte au cédant. Ce document doit présenter les informations associées à ce support, issues du registre centralisé, et être signé par l'analyste et le cédant.

h) Les analystes doivent assurer la préservation et la non-altération de tous les éléments récoltés au titre de la prestation.
Ainsi, ils doivent réaliser une vérification d'intégrité des éléments collectés, ou des éléments fournis par le commanditaire dès leur réception.

i) Les analystes doivent définir et mettre en place des moyens adaptés aux contraintes du commanditaire et assurant la collecte et la normalisation de volumes d'informations à l'échelle du système d'information cible.

VI.6.3.2. Collecte d'informations techniques

a) Les analystes doivent être en mesure de collecter des informations techniques sur les équipements suivants :

- serveurs d'infrastructure système (ex. : authentification, télédistribution, télégestion et prise de main à distance, sauvegarde, supervision, antivirus, virtualisation, serveurs de fichiers, etc.) ;
- serveurs d'infrastructure réseau (ex. : serveurs mandataire, serveurs DNS, etc.) ;
- équipements d'infrastructure réseau (ex. : concentrateur, routeur, point d'accès sans fil, etc.) ;

- équipements de sécurité (ex. : pare-feu, chiffreurs, etc.) ;
- postes d'administration et postes utilisateur (ex : Windows, Linux, etc.) ;
- serveurs métier (ex. : serveurs Web, base de données, etc.).

b) Les analystes doivent être en mesure de collecter des informations techniques portant notamment sur :
- les configurations des systèmes ;
- les entrées des systèmes de fichiers ;
- les systèmes en exécution (incluant mais ne se limitant pas à la mémoire, les connexions réseau, les données de configuration volatiles, etc.).

c) Le prestataire doit formaliser et tenir à jour une liste des types d'informations techniques requise à l'exigence VI.6.3.2 b) qu'il est en mesure de collecter par type d'équipement identifié à l'exigence VI.6.3.2 a). Lorsqu'il n'est pas en mesure de collecter un type information technique, le prestataire doit en préciser la raison dans la liste: type d'information technique non présent sur l'équipement ou raison technique.

VI.6.3.3. Copie physique

a) [REC] Dans le cas d'une recherche hors-ligne, les analystes doivent réaliser une copie physique des éléments nécessaires au bon déroulement de la prestation de recherche d'indicateurs de compromission (ex : disque dur et mémoire) des équipements inclus dans le périmètre de la prestation : serveurs, terminaux utilisateur, systèmes nomades (ordinateurs portables, ordiphones, etc.) et supports amovibles (clé USB, disque externe, etc.).

[IPR] Pour les équipements inclus dans le périmètre de la prestation, les analystes doivent réaliser une copie physique du disque dur et de la mémoire des équipements : serveurs, terminaux utilisateur, systèmes nomades (ordinateurs portables, ordiphones, etc.) et supports amovibles (clé USB, disque externe, etc.).

[ILP] Dans les cas jugés nécessaires (identification des activités de l'attaquant, collecte de codes non identifiés par ailleurs, identification des données exfiltrées, etc.), les analystes doivent réaliser, pour les équipements susceptibles d'avoir été compromis par l'attaquant, une copie physique de leur disque dur et de leur mémoire : serveurs, terminaux utilisateur, systèmes nomades (ordinateurs portables, ordiphones, etc.) et supports amovibles (clé USB, disque externe, etc.).

b) Le prestataire doit disposer de solutions adaptées à la copie physique de supports de données et à la copie mémoire des architectures rencontrées, afin d'en préserver l'intégrité.

VI.6.3.4. Collecte de journaux d'évènements

a) Les analystes doivent être en mesure de collecter des journaux d'évènements :
- sur les systèmes :
  - serveurs d'infrastructure système (ex. : authentification, télédistribution, télégestion et prise de main à distance, sauvegarde, supervision, anti-virus, virtualisation, serveurs de fichiers, etc.) ;
  - postes d'administration et postes utilisateur ;
  - serveurs métier (ex. : serveurs Web, base de données, etc.) ;
- sur les équipements réseau et de sécurité situés en périphérie ou au cœur du système d'information cible :
  - serveurs d'infrastructure réseau (ex. : serveurs mandataire, serveurs DNS, etc.) ;
  - équipements réseau (ex. : routeurs, VPN, journaux de flux de type Netflow, IPFIX, etc.) ;

- équipements de sécurité (ex. : pare-feu, sondes de détection, relais inverse, etc.).

b) [ILP] Le prestataire doit, en collaboration avec le commanditaire, définir et mettre en œuvre une politique de journalisation répondant au minimum aux besoins de la prestation. À ce titre, il est recommandé que le prestataire utilise la note technique de l'ANSSI en matière de journalisation [NT_JOURNAL] qui présente les types d'évènements à journaliser (authentification, gestion des comptes et des droits, accès aux ressources, modification des stratégies de sécurité, activité des processus, activité des systèmes, etc.).

VI.6.3.5. Capture de flux

a) Les analystes doivent être en mesure de capturer les flux afin de mener à bien la prestation. Ces captures peuvent, par exemple, permettre :

- d'analyser le protocole de communication entre une ressource compromise et un serveur de commande et de contrôle ;
- d'analyser la méthode de déplacement utilisée lors des mouvements latéraux de l'attaquant ;
- de rechercher des indicateurs de compromission.

b) Le responsable d'équipe d'analyse doit demander l'autorisation formelle et écrite du commanditaire préalablement à toute capture ou analyse de flux.

VI.6.3.6. Supervision de circonstance

a) [ILP] Le prestataire peut, si besoin, soutenir le commanditaire à la mise en place d'une supervision de circonstance s'appuyant sur une solution de collecte en continu des journaux issus de différentes sources (voir chapitre VI.6.3). À ce titre, il est recommandé que le prestataire utilise la note technique de l'ANSSI en matière de journalisation [NT_JOURNAL] qui propose des recommandations en matière d'architecture.

b) [ILP] Il est recommandé que le prestataire complète la supervision de circonstance par des sondes de détection d'intrusion qualifiées par l'ANSSI.

VI.6.4. Phase 4 : Analyse des informations

[IPR, ILP] Les phases 4.1 et 4.2 peuvent être réalisées en parallèle ou successivement, dans l'ordre jugé pertinent pour la prestation par le responsable d'équipe d'analyse.

VI.6.4.1. Objectifs

Le prestataire doit réaliser des opérations d'analyse avec pour objectifs :

- [REC] d'identifier la présence d'indicateurs de compromission dans le système d'information cible ;
- [IPR] d'identifier un potentiel incident de sécurité dans le système d'information cible ;
- [ILP] d'améliorer la compréhension de l'incident de sécurité affectant le système d'information cible (voir chapitre VI.6.1).

VI.6.4.2. Conditions de réalisation

a) Les opérations de recherche et d'analyse doivent suivre une méthode dont les actions sont préalablement identifiées et dont la démarche est reproductible.

b) Les analystes ne doivent rechercher et analyser que les informations strictement nécessaires au bon déroulement de la prestation conformément à la convention. Ils doivent mettre à disposition du commanditaire la liste des éléments qui seront recherchés et analysés. Le commanditaire peut refuser la recherche ou l'analyse de certains éléments. Néanmoins, les analystes doivent sensibiliser le

commanditaire à l'importance de la recherche et l'analyse des éléments pour l'efficacité de la prestation.

c) Les analystes doivent s'accorder avec le commanditaire sur le déroulement des opérations de recherche et d'analyse (types d'éléments, périmètre, méthodes employées, calendrier, etc.).

d) Les analystes doivent identifier, en s'appuyant sur la phase de compréhension de l'environnement, les points de recherche système et réseau permettant de atteindre les objectifs de la prestation.

e) Les analystes doivent assurer la préservation et la non-altération de tous les éléments récoltés et analysés au titre de la prestation.

f) Les analystes doivent définir et mettre en place des moyens adaptés aux contraintes du système d'information cible et assurant la recherche et la normalisation de volumes importants d'informations à l'échelle d'un système d'information.

g) Le responsable d'analyse doit mettre en place une main courante afin de permettre aux analystes de capitaliser les résultats de leurs analyses système, réseau et de codes malveillants.

VI.6.4.3. Phase 4.1 : recherche des indicateurs de compromission

Les recherches peuvent être réalisées directement sur le système d'information cible ou hors ligne sur des éléments collectés.

a) Les analystes doivent être en mesure de rechercher des indicateurs de compromission sur les équipements suivants :

- serveurs d'infrastructure système (ex. : authentification, télédistribution, télégestion et prise de main à distance, sauvegarde, supervision, antivirus, virtualisation, serveurs de fichiers, etc.) ;
- serveurs d'infrastructure réseau (ex. : serveurs mandataire, serveurs DNS, etc.) ;
- équipements d'infrastructure réseau (ex. : concentrateur, routeur, point d'accès sans fil, etc.) ;
- équipements de sécurité (ex. : pare-feu, chiffreurs, etc.) ;
- postes d'administration et postes utilisateur (ex : Windows, Linux, etc.) ;
- serveurs métier (ex. : serveurs Web, base de données, etc.).

b) Les analystes doivent être en mesure de rechercher les indicateurs de compromission des types suivants :

- Attributs de fichiers (empreinte cryptographique, nom, taille, date de compilation, localisation dans le système de fichiers, etc.) ;
- Artefact système (paramètre de configuration, clé de registre Windows, caractéristique d'un service, tube de communication, etc.) ;
- Artefact en mémoire (caractéristique d'un processus, d'un service, etc.) ;
- Adresse IP, URL, nom de domaine ;
- Chaîne de caractères ;
- Signature complexe (combinaison d'indicateurs de compromission).

c) Les analystes doivent être capables de normaliser dans un format unique les indicateurs de compromission qui leur sont transmis afin de pouvoir réaliser les recherches de façon cohérente.

d) Le prestataire doit formaliser et tenir à jour une liste des types d'indicateurs de compromission requis à l'exigence VI.6.4.3 a) qu'il est en mesure de rechercher par type d'équipement identifié à l'exigence VI.6.4.3 b). Lorsqu'il n'est pas en mesure de rechercher un type d'indicateur de compromission, le prestataire doit en préciser dans la liste la raison : type d'indicateur de compromission non présent sur l'équipement ou raison technique.

e) Les analystes doivent prendre en compte la sensibilité des indicateurs de compromission lors des recherches. Les recherches réalisées directement sur le système d'information cible ne peuvent employer que des indicateurs de compromission non sensibles. Les recherches réalisées hors ligne sur des éléments collectés peuvent employer des indicateurs de compromission sensibles voire de niveau *Diffusion Restreinte* [II_901].

[ILP] En particulier, l'environnement de travail doit être distinct du système d'information cible (cf. chapitre VI.5.2.2, paragraphe d).

f) Les analystes doivent réaliser l'analyse des résultats de recherche. Elle consiste en l'identification des résultats faux positifs et vrais positifs. Cette identification doit s'appuyer sur les éléments de contexte reçus lors de l'étape de compréhension de la situation et de l'environnement (voir chapitre VI.3), en particulier les pratiques d'administration[12].

VI.6.4.4. Phase 4.2 : recherche d'éléments d'intérêt - Analyse système et réseau

a) [IPR, ILP] Les analystes doivent analyser les informations collectées en supposant que ces dernières ne sont pas de confiance, car potentiellement modifiées par l'attaquant (ex. : modification du noyau du système d'exploitation, des logiciels, etc.).

b) [IPR, ILP] Les analyses doivent être réalisées autant que possible sur des copies des informations collectées. Avant toute opération d'analyse, l'analyste doit s'assurer de l'intégrité des copies effectuées.

c) [IPR, ILP] Le prestataire doit analyser les éléments collectés (voir chapitre VI.6.3) en recherchant ;

- une activité malveillante : exploitation d'une vulnérabilité, élévation de privilèges, reconnaissance du système d'information, exfiltration de données, etc. ;
- la présence d'un mécanisme de persistance ;
- les anomalies par rapport aux pratiques métier et d'administration sur le système d'information cible.

Cette étape d'analyse peut être combinée avec la phase 4.1 pour rechercher :

- [ILP] les indicateurs de compromission déjà connus de l'incident en cours de traitement ;
- les indicateurs de compromission génériques issus d'une base de connaissances du prestataire.

d) [ILP] Le responsable d'analyse doit mettre en place et tenir à jour un registre centralisé et chronologique référençant tous les évènements caractérisant les activités de l'attaquant dans le système d'information cible (date relative au système ayant été touché par l'évènement, date rapportée à la base de temps de référence).

VI.6.4.5. Phase 4.2 : recherche d'éléments d'intérêt - Analyse de codes malveillants

a) [IPR, ILP] Les missions à assurer en matière d'analyse de codes malveillants sont spécifiées en Annexe 2.

b) [IPR, ILP] L'analyste doit réaliser les analyses de codes malveillants nécessaires, pouvant nécessiter :

- une analyse du code sur une base hors ligne de plusieurs antivirus du marché ;
- une analyse dynamique du comportement du code malveillant ;
- une rétro-conception du code et de ses composants.

[12] Afin d'identifier si un usage malveillant d'un outil d'administration est réalisé, dans le cas d'outils pouvant être utilisés aussi bien par les administrateurs que par des attaquants (ex : psexec).

c) [IPR, ILP] Les objectifs poursuivis pour ces opérations d'analyse de code doivent demeurer en adéquation avec la réalisation de la prestation.

VI.6.4.6. Phase 4.2 : recherche d'éléments d'intérêt - Supervision de circonstance

a) [ILP] La solution de supervision de circonstance mise en œuvre lors de la phase de collecte doit permettre de détecter la présence de l'attaquant sur le système d'information cible en exploitant les indicateurs de compromission découverts lors des opérations d'analyse et, le cas échéant, de suivre aussi précisément que possible ses actions, ses déplacements voire ses changements de comportement.

VI.6.4.7. Recherches en sources ouvertes

Le prestataire peut être amené à réaliser des recherches en sources ouvertes, sur Internet notamment, à partir des résultats de recherches d'indicateurs de compromission, d'informations collectées ou issues des analyses (empreintes cryptographiques ou noms de fichiers ou de codes malveillants, chaînes de caractères contenues dans des codes malveillants, noms de domaines et adresses IP, etc.) et ainsi récupérer des informations nécessaires à l'enrichissement, voire à la poursuite de la prestation.

Les recherches en sources ouvertes à partir d'informations collectées ou issues des analyses peuvent éveiller l'attention [ILP] de l'attaquant. Il est donc important que le prestataire observe la plus grande prudence en les effectuant.

a) Le prestataire doit définir une méthodologie pour la recherche en sources ouvertes à partir d'informations collectées ou issues des analyses. Elle doit préciser, [ILP] en fonction du niveau de discrétion recherché vis-à-vis de l'attaquant (voir chapitre VI.4, paragraphe a), les types d'informations pouvant être recherchés et les modalités associées. Elle doit également prendre en compte la sensibilité et la confidentialité des indicateurs de compromission (voir chapitre IV.3).

b) Le prestataire doit horodater et conserver les résultats obtenus par recherche en source ouverte afin de limiter le nombre de recherches réalisées et afin de conserver un historique des résultats permettant d'en identifier les évolutions.

c) [ILP] Le prestataire doit utiliser des bases d'informations internes et précollectées issues de sources ouvertes (bases RIPE, plateformes antivirales hors ligne, bases de résolution DNS, etc.) afin de limiter au maximum les recherches sur Internet.

   [IPR] Il est recommandé que le prestataire utilise des bases d'informations internes et précollectées issues de sources ouvertes (bases RIPE, plateformes antivirales hors ligne, bases de résolution DNS, etc.) afin de limiter au maximum les recherches sur Internet.

d) Il est recommandé que le prestataire réalise les recherches en sources ouvertes à partir de liaisons Internet démarquées sans lien direct avec le prestataire ou le commanditaire (IP dynamique avec changement périodique, aucun enregistrement dans les bases whois, etc.) afin de ne pas permettre leur identification par l'attaquant.

VI.6.5. Phase 5 : synthèse des analyses, capitalisation et diffusion

a) Le responsable d'équipe d'analyse doit :
   - regrouper et synthétiser les résultats des analyses ;
   - [ILP] réviser la compréhension de l'incident de sécurité (voir chapitre VI.6.1) afin de :
     - affiner les scénarios d'attaque et le périmètre de compromission,
     - identifier d'éventuels nouveaux indicateurs de compromission ;
   - [ILP] réviser la posture (voir chapitre VI.6.2) afin de :
     - préparer la prochaine campagne de collecte (voir chapitre VI.6.3),

- affiner les prochaines analyses (voir chapitre VI.6.4.4).

b) [IPR, ILP] Le responsable d'équipe d'analyse est responsable de l'anonymisation et de la décontextualisation des nouveaux indicateurs de compromission obtenus lors de sa prestation pour pouvoir les réutiliser dans les prochaines analyses (adresses IP, noms de domaine, URL, empreintes cryptographiques ou noms de fichiers ou de codes malveillants, chaînes spécifiques contenues dans des codes malveillants, informations sur un processus ou un service, entrées dans la base de registre Windows, etc.).

c) Le responsable d'équipe d'analyse doit diffuser ces informations aux membres de son équipe d'analystes ainsi qu'aux parties ayant le besoin d'en connaître, en accord avec le commanditaire.

d) [REC] Le responsable d'équipe d'analyse doit exploiter les résultats des recherches afin de réduire le nombre de faux positifs des futures prestations de recherche d'indicateurs de compromission.

VI.6.6. Phase 6 : révision des mesures de remédiation

a) [ILP] Le responsable d'équipe d'analyse doit définir et tenir à jour un plan de remédiation identifiant :

- les mesures de durcissement du système d'information cible, visant d'une part à augmenter le niveau de sécurité et à réduire les risques d'une nouvelle compromission une fois le système d'information cible assaini ;
- les mesures d'assainissement du système d'information cible, visant à contenir et bloquer l'attaque en cours puis à supprimer les moyens utilisés par l'attaquant pour accéder au système d'information cible.

b) [ILP] Le responsable d'équipe d'analyse doit identifier dans le plan de remédiation les éventuels effets de bord associés à chacune des mesures de remédiation, via une analyse d'impact (risque d'appliquer une mesure de remédiation face au risque de ne pas l'appliquer).

c) [ILP] Le responsable d'équipe d'analyse doit ordonner dans le plan de remédiation les mesures de remédiation en prenant en compte leur importance, efficacité et difficulté de mise en place. Cet ordonnancement doit inclure au moins trois regroupements par échéance : court, moyen et long terme.

d) [ILP] Le prestataire doit soumettre pour accord le plan de remédiation au commanditaire. La décision finale et la mise en œuvre du plan de remédiation appartiennent au commanditaire.

VI.6.6.1. Mesures de durcissement initiales

a) [ILP] Le prestataire doit proposer des mesures de durcissement à appliquer avant l'assainissement du système d'information cible.

b) [ILP] Le prestataire doit proposer les mesures de durcissement en s'appuyant sur le guide d'hygiène informatique de l'ANSSI [HYGIENE].

c) [ILP] Le prestataire doit proposer au commanditaire d'adopter une stratégie de défense en profondeur et proposer des mesures de durcissement applicables à différents niveaux du système d'information cible (postes de travail, serveurs, relais, équipements réseau, équipements de sécurité, etc.). En particulier, les mesures de durcissement proposées par le prestataire doivent permettre :

- de détecter une nouvelle tentative de compromission afin d'en limiter les impacts ;
- d'empêcher une attaque selon le mode opératoire utilisé par l'attaquant ou du même niveau de complexité ;
- de combler les vecteurs de compromission les plus courants.

d) [ILP] Le prestataire doit adapter les mesures de durcissement au niveau de discrétion adopté vis-à-vis de l'attaquant.

À titre d'exemple, si le niveau de discrétion recherché vis-à-vis de l'attaquant est élevé ou moyen (voir chapitre VI.4, paragraphe a)) :

- les mesures de durcissement appliquées doivent pouvoir être interprétées par l'attaquant comme des opérations classiques d'administration ;
- les mesures de durcissement peuvent être appliquées sur l'ensemble du système d'information cible, à l'exception des ressources compromises et maîtrisées par l'attaquant ;
- les mesures de durcissement susceptibles d'éveiller l'attention de l'attaquant (ex. : restriction de certains privilèges, durcissement de la politique de filtrage, etc.) doivent être appliquées après l'assainissement.

e) [ILP] Le prestataire doit recommander au commanditaire de recourir à un prestataire de détection des incidents de sécurité qualifié (PDIS). Il doit lui transmettre le lien vers le catalogue des prestataires de détection des incidents de sécurité qualifiés[13].

VI.6.6.2. Mesures d'assainissement

a) [ILP] Le prestataire doit proposer des mesures d'isolation permettant d'empêcher toute action de l'attaquant visant à perturber ou empêcher l'application des mesures d'assainissement sur le système d'information cible.

Cette exigence vise à empêcher l'attaquant de réagir (ex. : exfiltration massive d'informations, sabotage, etc.) pendant l'application des mesures d'assainissement.

b) [ILP] Le prestataire doit proposer des mesures d'assainissement permettant de supprimer les moyens d'accès de l'attaquant au système d'information cible (changement de l'ensemble des secrets, suppression des comptes utilisés par l'attaquant, etc.) et d'assainir le système d'information cible (ex. : remplacer les machines compromises).

Le prestataire doit proposer des mesures d'assainissement prévoyant jusqu'à la réinstallation intégrale du cœur de confiance du système d'information cible, sur une échelle de temps réduite, par exemple sur un week-end, et en une seule fois. Il doit prendre en compte la nature et l'étendue de la compromission, ainsi que la complexité du système d'information cible et les impacts métier associés.

Le cœur de confiance comprend les services ayant des privilèges élevés sur les ressources d'un système d'information, notamment les services d'infrastructure (ex : authentification, contrôle d'accès, télédistribution, télégestion, prise de main à distance, supervision, anti-virus, etc.) et les postes d'administration associés.

L'application des mesures d'assainissement sur une période longue ou en plusieurs fois pourrait permettre à l'attaquant de compromettre à nouveau le système d'information cible.

VI.6.6.3. Mesures de durcissement post-assainissement

a) [ILP] Le prestataire doit proposer des mesures de durcissement à appliquer après l'assainissement du système d'information cible, afin de permettre à plus long terme de :

- garantir un niveau de sécurité en adéquation avec les besoins du commanditaire, notamment en matière de disponibilité, d'intégrité et de confidentialité;
- empêcher une nouvelle compromission ciblée employant des scénarios d'attaque courants ;
- détecter de nouvelles tentatives de compromission afin de permettre la limitation des impacts ;
- lever les restrictions temporaires mises en place après la phase d'assainissement.

[13] Le catalogue des prestataires de détection des incidents de sécurité qualifiés est publié sur le site de l'ANSSI.

b) [ILP] Le prestataire doit recommander au commanditaire de recourir à un prestataire d'audit de sécurité des systèmes d'information qualifié (PASSI) pour valider in fine l'efficacité des mesures effectivement mises en place. Il doit lui transmettre le lien vers le catalogue des prestataires d'audit de sécurité des systèmes d'information qualifiés[14].

VI.7. Étape 7 - Restitutions

a) [ILP] Le responsable d'équipe d'analyse doit présenter au commanditaire une synthèse à jour concernant :

- la compréhension de l'incident (voir chapitre VI.6.1) ;
- la posture adoptée (voir chapitre VI.6.2) ;
- les opérations en cours de réalisation et réalisées ;
- les mesures de remédiation proposées (voir chapitre VI.6.6).

b) Le responsable d'équipe d'analyse [ILP] doit assurer une restitution, [REC, IPR] assure une restitution à la demande du commanditaire :

- [ILP] quotidiennement, au référent désigné par le commanditaire (voir Annexe 3 II, paragraphe a) ;
- [ILP] à chaque révision de la posture ;
- à l'issue de la prestation, sans attendre que le rapport d'analyse soit achevé ;
- à la clôture de la prestation, après la livraison du rapport d'analyse, à la demande du commanditaire.

VI.8. Étape 8 - Élaboration du rapport d'analyse

a) Le prestataire doit, pour toute prestation, élaborer un rapport d'analyse et le transmettre au commanditaire.

b) Le prestataire doit mentionner explicitement dans le rapport d'analyse si la prestation réalisée est une prestation qualifiée et préciser les activités d'analyse (voir chapitre II) associées.

c) Le rapport d'analyse doit mentionner les noms et coordonnées des analystes, responsables d'équipe d'analyse et commanditaires de la prestation.

d) [REC] Le prestataire doit élaborer un rapport d'analyse présentant notamment :

- une synthèse, compréhensible par des non-experts, qui précise :
    - l'objectif de la recherche,
    - l'(es) indicateur(s) de compromission recherché(s),
    - le périmètre couvert par la recherche,
    - les résultats de la recherche,
    - la suite à donner à la recherche ;
- la description des recherches réalisées et de leurs résultats (voir chapitre VI.6.4) :
    - les modes opératoires,
    - les outils utilisés,
    - les vrais positifs;

[14] Le catalogue des prestataires d'audit de sécurité des systèmes d'information qualifiés est publié sur le site de l'ANSSI.

- la suite à donner à la recherche, incluant :
    - la justification de cette recommandation,
    - les différentes options possibles, le cas échéant,
    - lorsque la suite à donner indique de poursuivre avec une nouvelle prestation :
        - le type de prestation : une prestation d'investigation numérique sur périmètre restreint, en précisant le type d'analyse requise, ou d'investigation numérique sur large périmètre,
        - le périmètre de la prestation,
        - le niveau de discrétion requis.

[IPR] Le prestataire doit élaborer un rapport d'analyse présentant notamment :

- une synthèse, compréhensible par des non-experts, qui précise :
    - le contexte de l'investigation,
    - le périmètre concerné par l'investigation,
    - les résultats de l'investigation,
    - la suite à donner à l'investigation ;
- la description des analyses réalisées et de leurs résultats (voir chapitre VI.6.4.4) :
    - les éléments collectés et analysés,
    - le cas échéant :
        - les codes malveillants utilisés et leur analyse,
        - les méthodes de persistance,
        - les vulnérabilités exploitées,
        - les méthodes d'escalade de privilèges,
        - les méthodes de communication,
        - le vecteur initial de compromission ;
- la suite à donner à la recherche, incluant :
    - la justification de cette recommandation,
    - les différentes options possibles, le cas échéant,
    - lorsque la suite à donner indique de poursuivre avec une nouvelle prestation :
        - le type de prestation : une prestation complémentaire d'investigation numérique sur périmètre restreint, en précisant le type d'analyse requise, ou d'investigation numérique sur large périmètre,
        - le périmètre de la prestation,
        - le niveau de discrétion requis.

[ILP] Le prestataire doit élaborer un rapport d'analyse présentant notamment :

- une synthèse, compréhensible par des non-experts, qui précise :
    - le contexte de l'incident,
    - l'objectif de l'attaquant,
    - le périmètre concerné par l'attaque et le périmètre compromis,

    - les actions réalisées par l'attaquant ayant un impact fort pour le commanditaire (ex. : exfiltration de données, sabotage, suppression de données, etc.),
    - les étapes clés du mode opératoire de l'attaquant et la chronologie associée,
    - les mesures prises par le commanditaire pour remédier à l'incident ;
  - un ou plusieurs schémas récapitulatifs de l'attaque, si cela s'avère pertinent :
    - désignation des systèmes compromis,
    - horodatage des événements ;
  - la description des analyses réalisées et de leurs résultats (voir chapitreVI.6.4.4) :
    - les éléments collectés et analysés,
    - les codes malveillants utilisés et leur analyse,
    - les méthodes de persistance,
    - les vulnérabilités exploitées,
    - les méthodes d'escalade de privilèges,
    - les méthodes de communication,
    - le vecteur initial de compromission ;
  - la liste exhaustive des ressources et comptes compromis ;
  - les indicateurs de compromission ;
  - les mesures de remédiation, leur périmètre et leur séquencement de mise en œuvre.

e) [IPR, ILP] Le prestataire doit également transmettre :
  - le registre recensant toutes les actions réalisées sur le système (voir chapitre VI.5.2.2, paragraphe a) ;
  - le registre recensant toutes les informations et supports collectés au titre de la prestation (voir chapitre VI.5.2.2, paragraphe b).

f) Le prestataire doit mentionner dans le rapport d'analyse :
  - les réserves relatives à l'exhaustivité des résultats de la prestation (liées aux délais alloués, à la disponibilité des informations demandées, à la collaboration du commanditaire, etc.) ;
  - les sources d'information qui ont fait défaut (ex. : absence de journalisation sur un serveur particulier, mauvaise configuration de la journalisation, etc.) pour compléter les analyses et consolider une chronologie exhaustive de toutes les actions de l'attaquant ;
  - [IPR, ILP] les infractions législatives et/ou réglementaires qui découlent de l'incident (ex : violation de données à caractère personnel, de données *Diffusion Restreinte* [II_901], etc.).

VI.9. Étape 9 - Clôture de la prestation

a) Il est recommandé qu'une réunion de clôture de la prestation soit organisée avec le commanditaire suite à la livraison du rapport d'analyse, conformément au chapitre VI.7. Cette réunion permet de présenter la synthèse du rapport d'analyse, [ILP] de la chronologie des événements composant l'incident de sécurité, [ILP] des mesures de durcissement, [REC, IPR] de la suite à donner à la prestation et d'organiser un jeu de questions / réponses.

b) Le responsable d'équipe d'analyse doit, selon ce qui a été prévu dans la convention établie entre le prestataire et le commanditaire, réaliser l'effacement sécurisé des media du prestataire et détruire ou restituer, l'ensemble des informations collectées ou documents relatifs au système d'information cible.

c) Le responsable d'équipe d'analyse doit transmettre au commanditaire un procès-verbal de destruction ou de restitution, selon ce qui a été prévu dans la convention établie avec le prestataire. Le procès-verbal de destruction ou de restitution doit identifier les informations et supports détruits ou restitués ainsi que le mode de destruction ou de restitution.

d) La prestation est considérée comme terminée lorsque toutes les activités prévues ont été réalisées et que le commanditaire a reçu et attesté, formellement et par écrit, que le rapport d'analyse est conforme aux objectifs visés dans la convention.

VI.10. Cas des enquêtes judiciaires

Une enquête judiciaire est une action pénale, qui peut être déclenchée, à la demande ou non du commanditaire :

- antérieurement ou simultanément au démarrage de la prestation ;
- au cours de la prestation ;
- à la clôture ou postérieurement à la fin de la prestation.

Les objectifs des enquêteurs et du prestataire sont distincts, même si ils portent sur les mêmes faits.

a) Le prestataire doit, dans le cas d'une enquête judiciaire et conformément à la législation en vigueur sur le territoire français, assurer une collaboration pleine et entière avec le service enquêteur.

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[LOI_IL]	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_314-1]	Article 334-1 du Code pénal relatif à l'abus de confiance. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-1]	Article 226-1 du Code pénal relatif à l'atteinte à la vie privée. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-13]	Article 226-13 du Code pénal relatif au secret professionnel. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-15]	Article 226-15 du Code pénal relatif au secret des correspondances. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_323-1]	Article 323-1 du Code pénal relatif à l'accès ou au maintien frauduleux dans un système de traitement automatisé de données. Disponible sur http://www.legifrance.gouv.fr
[CSP_ART_L1110-4]	Article L1110-4 du Code de la santé publique relatif au secret médical. Disponible sur http://www.legifrance.gouv.fr
[IGI_1300]	Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale, n°1300 /SGDSN/PSE/PSD, 30 novembre 2011. Disponible sur http://www.legifrance.gouv.fr
[II_910]	Instruction interministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, 22 octobre 2013. Disponible sur http://www.legifrance.gouv.fr
[II_901]	Instruction interministérielle relative à la protection des systèmes d'information sensibles, n°901/SGDSN/ANSSI, 28 janvier 2015. Disponible sur http://www.legifrance.gouv.fr
[D_2015_350]	Décret relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de sécurité nationale, n° 2015-350, 27 mars 2015. Disponible sur http://www.legifrance.gouv.fr
[LOI_EJ]	Loi relative aux experts judiciaires, n° 71-498, 29 juin 1971. Disponible sur http://www.legifrance.gouv.fr

II. Normes et documents techniques

Renvoi	Document
[PRIS_LPM]	Exigences supplémentaires applicables aux prestataires d'audit de la sécurité des systèmes d'information dans le cadre de la loi n°2013-1168 du 18 décembre 2013. Document de niveau *Diffusion Restreinte*, il peut être obtenu auprès de l'ANSSI.
[ETSI_ISG_ISI]	Standards ETSI ISI Indicators (ISI 001-1 and Guides 001-2), ISI Event Model (ISI-002), ISI Maturity (ISI-003), ISI Event Detection (ISI-004) – 5 standards sur la détection des incidents de sécurité. Disponible sur http://www.etsi.org
[ISO19011]	Norme internationale ISO/IEC 19011:2011 : Lignes directrices pour l'audit des systèmes de management. Disponible sur http://www.iso.org

Renvoi	Document
[ISO27000]	Norme internationale ISO/IEC 27000:2014 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – vue d'ensemble et vocabulaire. Disponible sur http://www.iso.org
[ISO27035]	Norme internationale ISO/IEC 27035-1:2016 : Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information. Partie 1: Principes de la gestion des incidents Norme internationale ISO/IEC 27035-2:2016 : Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information. Partie 2 : Lignes directrices pour planifier et préparer une réponse aux incidents Disponible sur http://www.iso.org
[ISO27037]	Norme internationale ISO/IEC 27037 :2012 : Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques. Disponible sur http://www.iso.org
[NT_JOURNAL]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, note technique n° DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013, ANSSI. Disponible sur http://www.ssi.gouv.fr/journalisation
[NT_PASSE]	Recommandations de sécurité relatives aux mots de passe, note technique n° DAT-NT-001/ANSSI/SDE/NP du 5 juin 2012, ANSSI. Disponible sur http://www.ssi.gouv.fr/mots-de-passe
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HYGIENE]	Guide d'hygiène informatique – version en vigueur. Disponible sur http://www.ssi.gouv.fr/hygiene-informatique

III. Autres références documentaires

Renvoi	Document
[STRAT_NUM]	Stratégie nationale pour la sécurité du numérique, octobre 2015. Disponible sur http://www.ssi.gouv.fr
[QUAL_SERV_PROCESS]	Processus de qualification d'un service, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[GUIDE_ACHAT]	Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. Disponible sur http://www.ssi.gouv.fr

Annexe 2 Missions et compétences attendues du personnel du prestataire

Cette annexe présente, pour chaque profil d'analyste, les missions à assurer et les compétences requises.

I. Responsable d'équipe d'analyse

Cette partie décrit les missions et compétences du responsable d'une prestation (pilotes techniques et analystes référents). Celles qui concernent exclusivement les pilotes techniques sont précédées de l'identifiant ILP.

I.1. Missions

Le responsable d'équipe d'analyse doit assurer les missions suivantes :

- mettre en œuvre une organisation adaptée aux objectifs de la prestation (voir chapitre VI.5.1) ;
- structurer l'équipe d'analystes (compétences, effectif) ;
- assurer la définition, le pilotage et le contrôle des activités des analystes ;
- mettre en œuvre les moyens adaptés aux objectifs de la prestation (voir chapitre VI.5.2) ;
- définir et gérer les priorités, [ILP] en particulier en situation de crise ;
- définir une démarche permettant de comprendre :
    - [IPR] la situation, [ILP] l'incident de sécurité (voir chapitre VI.3.1) ;
    - l'environnement (voir chapitre VI.3.2) ;
- [ILP] définir et réviser la posture (voir chapitres VI.4 et VI.6.2) ;
- [ILP] maintenir à jour un état de la compréhension de l'incident de sécurité (voir chapitre VI.6.1) ;
- [ILP] maintenir à jour un état de la situation des analyses et de la compromission et présenter l'information utile à chaque échelon (comité technique, comité stratégique, etc.) ;
- [ILP] soutenir le commanditaire dans l'évaluation des impacts métier associés à l'incident de sécurité notamment en matière de confidentialité (ex. : données exfiltrées), d'intégrité et de disponibilité ;
- [ILP] préconiser les mesures nécessaires pour remédier à l'incident de sécurité, en limiter l'impact et réduire les risques d'une nouvelle compromission ;
- assurer et contrôler la synthèse des analyses, la capitalisation et la diffusion (voir chapitre VI.6.5) ;
- contrôler la qualité des productions ;
- valider les livrables.

I.2. Compétences

Le pilote technique doit avoir des compétences approfondies dans la plupart des domaines techniques suivants :

- les principales attaques et activités malveillantes : exploitation de vulnérabilités, portes dérobées, *rootkit*, *botnet*, rançongiciel, C&C, etc. ;
- la connaissance des normes de référence pour la représentation des indicateurs de compromission (STIX, OpenIOC, etc.) ;

- les architectures des systèmes d'informations d'envergure, leurs vulnérabilités et leurs mécanismes d'administration ;
- le fonctionnement, la sécurisation et les vulnérabilités des principaux systèmes d'exploitation (Microsoft, UNIX/Linux) et solutions de virtualisation ;
- les protocoles et architectures réseau, leurs vulnérabilités et leur sécurisation ;
- les applications et leurs vulnérabilités : application bureautique, navigateurs Internet, serveurs Web, bases de données, serveurs de messagerie, progiciels, etc. ;
- les outils d'analyse : analyse de systèmes (antivirus, mémoire, disques), analyse de journaux (signature, réseau, système, applicatif ou réseau), analyse statique et dynamique de programmes et documents, etc.
- la connaissance du présent référentiel (Chapitre VI) ;
- la connaissance des entités judiciaires impliquées dans le traitement d'un incident informatique.

Le responsable d'équipe d'analyse doit avoir les qualités suivantes :

- savoir piloter des équipes d'analystes ;
- [ILP] savoir définir et gérer les priorités, en particulier en situation de crise ;
- savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- savoir rédiger des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.).

II. Analyste système

II.1.Missions

L'analyste système doit assurer les missions suivantes :

- adopter une vision globale du système d'information afin d'identifier :
    - les vulnérabilités système exploitables et les chemins d'attaque associés,
    - les points d'extrémité nécessitant une collecte de données (serveurs d'infrastructure, poste d'administration et postes utilisateur, serveurs métier, etc.) ;
- recueillir à l'échelle du système d'information un volume important d'informations techniques (système de fichiers, configuration, journaux système et applicatifs, etc.) d'un large ensemble de systèmes informatiques et en assurer l'analyse ;
- réaliser la recherche d'indicateurs de compromission ;
- réaliser une copie physique / mémoire de terminaux (poste de travail, poste nomade, etc.), de serveurs (serveur d'infrastructure, serveur applicatif, etc.) et de supports amovibles (clé USB, disque externe, etc.) susceptibles d'avoir participé à un scénario d'attaque et en assurer l'analyse ;
- soutenir le commanditaire dans la définition d'une politique de journalisation système (types d'événements, durées de rétention, etc.) par type d'équipement ;
- soutenir le commanditaire dans le développement de règles de corrélation d'événements système ;
- soutenir le commanditaire dans la mise en place de solutions de collecte et d'analyse de journaux adaptées à l'architecture cible, afin de pouvoir suivre les activés de l'attaquant ;
- extraire des indicateurs de compromission à des fins d'analyse et de supervision ;

- qualifier l'ensemble des relevés techniques recueillis (images disques, images mémoire, journaux d'événements, alertes, traces système, réseau et applicatives) pour déterminer la cause de l'incident, le mode opératoire de l'attaque, les vulnérabilités exploitées, l'étendue de la compromission et les événements impactants ;
- réaliser la caractérisation des fichiers (binaires et documents) afin d'identifier leur potentiel caractère malveillant (vérification des en-têtes, vérification via logiciel antivirus, analyse d'exécution dans un système isolé, etc.) ;
- préconiser des mesures de remédiation pour limiter la compromission, enrayer l'activité de l'attaquant et assurer le durcissement de la sécurité du système d'information cible ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'analyse.

II.2.Compétences

L'analyste système doit disposer de compétences approfondies dans les domaines techniques suivants :

- le fonctionnement, la sécurisation et les vulnérabilités des principaux systèmes d'exploitation (Microsoft, UNIX/Linux) et solutions de virtualisation ;
- les applications et leurs vulnérabilités : application bureautique, navigateur Internet, serveur Web, base de données, serveurs de messagerie, progiciels, etc. ;
- les attaques et activités malveillantes : exploitation de vulnérabilités, portes dérobées, *rootkit*, *botnet*, C&C, etc. ;
- les outils d'analyse : analyse de systèmes (artefact Windows, mémoire, disques, système de fichiers dont NTFS et EXT3/4, séquence de démarrage), analyse de journaux (système, applicatif ou réseau), analyse statique et dynamique de programmes et documents, etc.
- les journaux d'événements système (événements Windows et journaux syslog), réseau et applicatifs ;
- les solutions d'analyse de journaux ou de supervision de la sécurité (SIEM) ;
- les protocoles et architectures réseau, leurs vulnérabilités et leur sécurisation ;
- les langages de programmation de bas niveau (C, assembleur, etc.) et langages de scripts (Python, Perl, PowerShell, etc.).

Il doit par ailleurs avoir les qualités suivantes :

- savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;
- savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

III. Analyste réseau

III.1. Missions

L'analyste réseau doit assurer les missions suivantes :

- adopter une vision globale du système d'information et de son architecture, identifier les points potentiels d'infiltration/exfiltration et les points de collecte associés (composants réseau, produits de sécurité, etc.) ;
- soutenir le commanditaire dans l'identification des attaques à détecter ;
- réaliser la recherche d'indicateurs de compromission ;

- soutenir le commanditaire dans la mise en place de solutions de collecte et d'analyse de journaux réseau adaptées à l'architecture cible, à des fins de supervision de circonstance ;
- soutenir le commanditaire dans la définition d'une politique de journalisation réseau (types d'événements, durées de rétention, etc.) par type d'équipement (nœuds d'interconnexion, passerelles Internet, équipements de sécurité, etc.) [NT_JOURNAL] et au développement de règles de corrélation d'événements réseau ;
- soutenir le commanditaire dans la conception et à la mise en place de solutions de détection d'attaques informatiques et au développement de règles de corrélation d'évènements ;
- analyser et interpréter les informations techniques collectées (journaux, alertes) : vulnérabilités exploitées, chemins d'attaque, etc. ;
- extraire des indicateurs de compromission à des fins d'analyse et de supervision ;
- réaliser la caractérisation des fichiers (binaires et documents) afin d'identifier leur potentiel caractère malveillant (vérification des en-têtes, vérification via logiciel antivirus, analyse d'exécution dans un système isolé, etc.) ;
- préconiser des mesures de remédiation pour limiter la compromission, enrayer l'activité de l'attaquant et assurer le durcissement de la sécurité du système d'information cible ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'analyse.

III.2. Compétences

L'analyste réseau doit avoir des compétences approfondies dans les domaines techniques suivants :

- l'architecture globale d'un réseau, ses vulnérabilités et sa sécurisation ;
- les protocoles réseau classiques (TCP/IP, mécanismes de routage, IPsec et VPN) et protocoles applicatifs les plus courants (HTTP, SMTP, LDAP, SSH, etc.) ;
- les attaques et activités malveillantes : exploitation de vulnérabilités, portes dérobées, *rootkit*, *botnet*, C&C, etc. ;
- l'analyse de journaux d'événements système, réseau et applicatifs ;
- les solutions d'analyse de journaux ou de supervision de la sécurité (SIEM) ;
- les sondes de détection d'intrusions et outils de corrélation de journaux d'événements ;
- les langages de programmation et de scripts (C, Python, Perl, PowerShell, etc.).

Il doit par ailleurs avoir les qualités suivantes :

- savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;
- savoir travailler en équipe (partage de connaissances, collaboration technique et entraide) ;
- être sensibilisé à la réglementation applicable aux opérations qu'il met en œuvre, notamment les textes référencés au chapitre Annexe 1.

IV. Analyste de codes malveillants

IV.1. Missions

L'analyste de codes malveillants doit savoir identifier les éléments suivants :

- les caractéristiques du code malveillant (empreinte cryptographique, taille du code malveillant, version du système d'exploitation cible concerné, éléments caractéristiques, etc.), la famille ou la

catégorie à laquelle appartient le code malveillant (*dropper*, *loader*, RAT, *bootkit*, etc.) ainsi que la référence à une analyse déjà réalisée s'il s'agit d'une variante connue ;

- le contexte d'extraction du code malveillant. Il convient notamment de décrire comment le code malveillant a été initialement détecté et l'emplacement du système d'où il a été extrait (ex. : fichier, mémoire, matériel, etc.) ;
- la phase d'exécution du code malveillant (ex. : exploitation d'une vulnérabilité, téléchargement d'un autre code malveillant, installation de *rootkit*, etc.) ;
- les dépendances vis-à-vis de l'environnement compromis (présence d'un fichier de configuration, utilisation d'un fichier de données, copie de la mémoire dans le cas d'une exécution en mémoire, etc.) ;
- la synthèse des fonctionnalités principales du code malveillant (récupération de données bancaires, exfiltration de fichiers, récupération de données techniques, etc.) ;
- les capacités techniques du code malveillant, par exemple :
    - la capture des données techniques (système et/ou réseau) ou des données métier (fichiers, frappes du clavier, mots de passe, etc.) ;
    - la persistance d'exécution, le code malveillant s'exécute une nouvelle fois sur le système compromis après avoir terminé son exécution initiale (extinction du système, exécution éphémère, etc.). La persistance peut être mise en place par le code malveillant de manière autonome ou via un deuxième code. Dans la plupart des cas, il s'agit d'identifier une exécution au démarrage du système d'exploitation ou d'une session utilisateur, une exécution sur un événement système, une exécution via une réinfection du système, etc. ;
    - la propagation sur le système d'information, par le réseau (ex. : exploitation d'une vulnérabilité, utilisation d'un compte avec un mot de passe subtilisé, etc.) ou par support amovible (ex. : clé USB) ;
    - l'escalade de privilèges (ex. : obtenir des privilèges supplémentaires, voire d'administration, sur le système compromis via l'exploitation de vulnérabilités) ;
    - la protection contre la collecte (falsification des activités sur un système compromis, effacement de journaux, modification des dates de fichiers, etc.) ;
    - la protection contre l'analyse. Il peut s'agir de protection statique (brouillage ou chiffrement du code, complication du fonctionnement, etc.) ou dynamique (détection d'un antivirus ou d'un environnement d'analyse, etc.) ;
    - le niveau d'autonomie (ex. : utilisation d'un moyen de communication dédié pour commander le code, existence de mécanismes préprogrammés et de conditions de réalisation, etc.) ;
    - l'exfiltration de données. Il s'agit d'identifier les moyens d'exfiltration de données (partage de fichiers, messagerie, serveur mandataire, clé USB, etc.).

Pour ce faire, l'analyste doit réaliser les activités suivantes :

- caractériser le code malveillant par rapport à des bases antivirales ;
- analyser dynamiquement le code pour en extraire les comportements ;
- réaliser une rétro-conception du code et de ses composants ;
- identifier et extraire des indicateurs de compromission.

L'analyste de code doit capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'analyse.

Il doit proposer des méthodes de détection et de protection, extraire des indicateurs de compromission à des fins de supervision et de remédiation, pouvant notamment prendre en compte :

- les caractéristiques du code malveillant : empreinte cryptographique, taille, routine cryptographique, chaîne de caractères discriminante ;
- les activités du code malveillant sur le système d'information : fichiers créés ou modifiés, services exécutés, etc. ;
- les activités du code malveillant sur le réseau : protocole de communication, marqueurs discriminants (UserAgent HTTP), adresses IP, noms de domaines de serveurs de commande et de contrôle, motifs, etc.

IV.2. Compétences

L'analyste de codes malveillants doit disposer de compétences approfondies dans les domaines techniques suivants :

- les principaux outils d'analyse dynamique, comportementale (bac-à-sable) et statique de code et leur utilisation ;
- le fonctionnement des codes malveillants : persistance, communication, protection (cryptographie, unpacking, etc.) ;
- le fonctionnement, la sécurisation et les vulnérabilités des principaux systèmes d'exploitation (Microsoft, UNIX/Linux) et solutions de virtualisation ;
- les applications et leurs vulnérabilités : application bureautique, navigateur Internet, serveur Web, base de données, serveurs de messagerie, progiciels, etc. ;
- les attaques et activités malveillantes : exploitation de vulnérabilités, portes dérobées, *rootkit*, *botnet*, C&C, etc. ;
- les protocoles et architectures réseau, leurs vulnérabilités et leur sécurisation ;
- les langages de programmation de bas niveau (C, assembleur, etc.) et langages de scripts (Python, Perl, PowerShell, etc.).

Il doit par ailleurs avoir les qualités suivantes :

- savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;
- savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

Annexe 3 Recommandations aux commanditaires

Cette annexe liste les recommandations de l'ANSSI à l'intention des commanditaires de prestations de réponse aux incidents de sécurité.

I. Qualification

a) Le commanditaire peut, lorsqu'il est une administration ou un opérateur d'importance vitale, demander à l'ANSSI de participer à la définition du cahier des charges faisant l'objet d'un appel d'offres ou d'un contrat.

b) Il est recommandé que le commanditaire choisisse son prestataire dans le catalogue des prestataires qualifiés publié sur le site de l'ANSSI, la qualification d'un prestataire attestant de sa conformité à l'ensemble des exigences du présent référentiel.

c) Pour bénéficier d'une prestation qualifiée, c'est-à-dire conforme à l'ensemble des exigences du présent référentiel, le commanditaire doit :

- identifier le type de prestation PRIS adaptée à son besoin ;
- choisir le prestataire dans le catalogue des prestataires qualifiés publié sur le site de l'ANSSI, qualifié pour réaliser le type de prestation attendue et ;
- exiger du prestataire de stipuler dans la convention de service que la prestation réalisée est une prestation qualifiée.

En effet, un prestataire qualifié garde la faculté de réaliser des prestations non qualifiées. Le recours à un prestataire issu du catalogue des prestataires qualifiés est donc une condition nécessaire mais pas suffisante pour bénéficier d'une prestation qualifiée, le commanditaire doit donc également exiger une prestation qualifiée.

d) Il est recommandé que le commanditaire qui recourt à un prestataire qualifié pour la réalisation d'une prestation non-qualifiée demande la liste des exigences PRIS que le prestataire ne respectera pas lors de la prestation.-

e) Il est recommandé que le commanditaire utilise le guide d'achat des produits de sécurité et des services de confiance [GUIDE_ACHAT] qui a pour vocation à accompagner la fonction achat des commanditaires lors des appels d'offres.

f) Il est recommandé que le commanditaire demande au prestataire de lui transmettre son attestation de qualification. Cette attestation identifie notamment les activités pour lesquelles le prestataire est qualifié et la date de validité de la qualification.

g) Il est recommandé que le commanditaire demande au prestataire de lui transmettre les attestations individuelles de compétence de chaque analyste intervenant dans le cadre de la prestation.

h) Le commanditaire peut, conformément au processus de qualification des prestataires de service de confiance [QUAL_SERV_PROCESS], déposer auprès de l'ANSSI une réclamation contre un prestataire qualifié pour lequel il estime que ce dernier n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée.

S'il s'avère après instruction de la réclamation que le prestataire n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée, et selon la gravité, la qualification du prestataire peut être suspendue retirée ou sa portée de qualification réduite.

i) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des informations classifiées de défense [IGI_1300] et par conséquent ne se substitue pas à une habilitation de défense.

Il est possible pour un commanditaire de recourir à un prestataire qualifié après s'être assuré que ce dernier dispose des habilitations de défense adéquates si nécessaire.

j) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des articles contrôlés de la sécurité des systèmes d'information (ACSSI) [II_910].

k) Il est possible pour un commanditaire de recourir à un prestataire qualifié après s'être assuré que ce dernier dispose au minimum des décisions d'accès aux ACSSI (DACSSI) adéquates pour les ACSSI classifiés ou des attestations de formation à la manipulation des ACSSI pour les ACSSI non classifiés.

l) Du fait de l'importance d'une intervention rapide du prestataire en cas d'incident de sécurité, il est recommandé que le commanditaire établisse une convention avec le prestataire en amont de toute prestation afin que le prestataire ne soit pas ralenti dans la réponse à incident par l'étape d'établissement de la convention.

m) Une prestation d'investigation numérique sur large périmètre, par sa nature imprévisible et non-planifiable, est une démarche itérative nécessitant une révision régulière de la posture à adopter et par conséquent des moyens associés (ressources humaines, budget, disponibilités, etc.). La durée de la prestation peut être révisée dans le temps en fonction de la compréhension de l'incident de sécurité et de son environnement et peut durer ainsi plusieurs semaines, voire plusieurs mois.

n) Il est recommandé que le commanditaire demande au prestataire de lui fournir des références : références clients, participation à des programmes de recherche, etc.

II. Avant la prestation

a) Il est recommandé que le commanditaire désigne en son sein un référent opérationnel chargé d'être l'interlocuteur privilégié avec le prestataire.

b) Il est recommandé que le commanditaire fasse appel à un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié[15] pour élaborer l'analyse de risques permettant d'établir la liste des incidents de sécurité redoutés et des impacts associés à partir desquelles les stratégies de collecte, d'analyse et de notification sont élaborées et mises en application par un prestataire de détection d'incidents de sécurité (PDIS) qualifié[16].

c) Il est recommandé que le commanditaire mette en place un processus de gestion de crise mis en œuvre en cas de détection d'un incident de sécurité majeur au sein de son système d'information.

d) Il est recommandé que le périmètre de l'analyse porte sur l'ensemble du système d'information afin que le prestataire puisse identifier le périmètre global de la compromission.

e) Le dépôt d'une plainte peut permettre de faciliter la coopération internationale, en particulier avec les entreprises fournissant des services externalisés (ex. : messagerie, stockage de données, réseaux sociaux, etc.) afin de collecter des informations liées à l'incident.

III. Pendant la prestation

a) Il est recommandé que le commanditaire fournisse au prestataire, dès le début de la prestation, les éléments identifiés en Annexe 4.

b) Il est recommandé que le commanditaire désigne en son sein un référent de confiance chargé de la gestion des relations avec le prestataire et des modalités de réalisation des activités d'analyse (horaires des interventions, autorisations, etc.).

[15] Le catalogue des prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés est publié sur le site de l'ANSSI.

[16] Le catalogue des prestataires de détection d'incidents de sécurité (PDIS) qualifiés est publié sur le site de l'ANSSI.

c) Il est recommandé que le commanditaire prenne les mesures de sauvegarde nécessaires à la protection de son système d'information et des données associées préalablement et au cours de la prestation. Cette démarche doit être réalisée en collaboration avec le prestataire afin de ne pas gêner les activités d'analyse, notamment les équipes informatiques du commanditaire ne doivent pas porter atteinte à l'intégrité des traces d'activités malveillantes.

d) Il est recommandé que le commanditaire mette en place une structure projet capable de définir les objectifs, le dispositif et le cadre de la prestation. Elle doit en assurer le suivi et réaliser les arbitrages associés. Cette structure doit avoir le bon niveau de décision. Il est recommandé que le commanditaire mette en place avec le prestataire une chaîne de décision courte et simplifiée des processus nécessaires au bon déroulement de la prestation, en particulier un comité stratégique et un processus d'achat rapide pour répondre aux besoins immédiats. Les contacts techniques utiles pour la bonne réalisation de la prestation doivent être communiqués au prestataire.

e) Il est recommandé que le commanditaire mette en place une cellule pour gérer une éventuelle crise induite par l'incident de sécurité et que le prestataire soit intégré à cette cellule.

f) Il est recommandé que le commanditaire définisse un plan de communication associé au traitement de l'incident de sécurité. Il doit définir les exigences que doit respecter le prestataire dans le cas où l'incident est divulgué au personnel de l'entité concernée ou au grand public. Il est notamment précisé le niveau de confidentialité à adopter par le prestataire vis-à-vis de l'incident de sécurité (communication aux exploitants, aux sous-traitants, etc.).

g) Il est recommandé, afin d'éviter toute dénonciation de vol ou d'abus de confiance, que le commanditaire évite de remettre au prestataire des matériels dont il n'est pas le titulaire mais tout de même utilisés à des fins professionnelles (BYOD[17]) en l'absence du titulaire du matériel ou sans son accord explicite.

h) Il est recommandé que le commanditaire trace toutes les modifications qu'il effectue sur le système d'information cible durant la prestation afin de pouvoir identifier les actions illégitimes sur le réseau pendant la prestation.

i) Il est recommandé que le commanditaire informe le prestataire, tout au long de la prestation, des actions qu'elle réalise sur le système d'information cible (opérations d'administration, sauvegardes, etc.) et qui pourraient affecter la prestation.

j) Il est recommandé que le commanditaire mette à disposition du prestataire une zone sécurisée et dédiée pour le stockage d'éléments sensibles (coffre-fort, salle surveillée, etc.). Cette zone doit respecter les contraintes réglementaires associées au niveau de sensibilité ou de classification des données stockées.

k) Il est recommandé que le commanditaire mette à disposition du prestataire les moyens techniques (ex : équipements réseau, connexion Internet, etc.) dont il a besoin pour sa prestation, et que ces moyens constituent un environnement d'analyse sécurisé et déconnecté du système d'information cible.

l) Il est recommandé que le commanditaire mette en œuvre des moyens de communication sécurisés et dédiés pour tous les échanges en rapport avec l'incident de sécurité, en interne et avec le prestataire. Il est recommandé que ces moyens soient déconnectés du système d'information compromis afin de ne pas permettre à l'attaquant de suivre les opérations en cours.

m) Il est recommandé que le commanditaire ait la capacité à révoquer un analyste.

[17] *Bring Your Own Device* (Apporter Votre Equipement personnel de Communication).

IV. Après la prestation

a) La définition et la mise en place de mesures de remédiation doivent, au même titre que la prestation, faire l'objet d'une structure projet : identification des traitants, identification des personnes requises (notamment les administrateurs), gestion des liens entre actions, planification des actions, etc.

b) Il est recommandé que le commanditaire fasse appel à un prestataire d'audit en sécurité des systèmes d'information (PASSI) qualifié et lui transmette le lien vers le catalogue des prestataires d'audit de sécurité des systèmes d'information qualifiés[18] pour :

   - enrichir les mesures de remédiation proposées par le prestataire de réponse aux incidents de sécurité (durcissement du système, confinement et blocage de l'attaque, assainissement) ;
   - contrôler la mise en place et la pertinence des mesures de remédiation proposées.

   Le cas échéant, il est recommandé que le PASSI réalise sa prestation en collaboration étroite avec le prestataire.

c) Il est recommandé que le commanditaire mette en place une organisation et des moyens de détection des incidents de sécurité ou fasse appel à un prestataire de détection des incidents de sécurité qualifié (PDIS)[19], si tel n'est pas déjà le cas.

d) Il est recommandé que le commanditaire mette en place une organisation de gestion des incidents de sécurité informatique, s'appuyant sur les bonnes pratiques de [ISO27035] (planification et préparation, détection et notification, qualification et arbitrage, traitement, amélioration continue).

[18] Le catalogue des prestataires d'audit de la sécurité des systèmes d'information qualifiés est publié sur le site de l'ANSSI.

[19] Le catalogue des prestataires de détection des incidents de sécurité qualifiés est publié sur le site de l'ANSSI.

Annexe 4 Prérequis à fournir par les commanditaires

Le commanditaire doit créer des comptes permettant au prestataire de réaliser les opérations de collecte. Ces comptes doivent avoir les privilèges nécessaires et suffisants pour réaliser la prestation. Ils doivent être dédiés, démarqués et respecter la politique de nommage du commanditaire sans éveiller l'attention d'un éventuel attaquant. Il est recommandé que ces comptes soient désactivés après chaque utilisation. Ils doivent faire l'objet d'une supervision spécifique. La politique de mot de passe doit respecter les recommandations de l'ANSSI [NT_PASSE].

Préalablement à la réalisation de la prestation, il est recommandé que le commanditaire mette à disposition du prestataire les informations concernant :

- l'organigramme de l'organisation ;
- l'organisation générale du système d'information ;
- l'architecture du système d'information :
    - plages d'adresses IP, équipements réseau et sécurité, etc. ;
    - passerelles de sortie avec Internet (relais Web, DNS, chaîne de messagerie, etc.) ;
    - passerelles d'entrées (VPN, nomades, accès distant à la messagerie, téléphonie) ;
    - serveurs exposés à Internet ou à un tiers (serveur web, serveur applicatif, etc.) ;
    - architecture des zones réseau et filtrage ;
    - dépendances et interconnexions du système d'information ;
- les spécificités et les contraintes du système d'information (réglementation applicable, SIIV, contraintes métier et/ou techniques, sous-traitance, etc.) ainsi que la localisation géographique ;
- le système d'information :
    - systèmes d'exploitation (postes d'administration, postes utilisateurs, postes nomades, serveurs d'infrastructure et métier, etc.) ;
    - technologies employées pour les applications métier ;
    - technologies employées pour les services d'infrastructure ;
    - préciser si les horloges des équipements du système d'information sont synchronisés (NTP) et les différentes zones utilisées (GMT, Paris) ;
    - particularités de systèmes (impossibilité de les arrêter ou d'en modifier la configuration) ;
- l'architecture des domaines d'administration et des liens entre les domaines ;
- la politique de journalisation, les moyens de supervision et de détection ;
- les périodes de gel technique et les projets en cours ou prévus pour le système d'information ;
- les éventuelles démarches déjà entreprises par le commanditaire :
    - méthodologie employée pour la recherche des éléments compromis ;
    - chronologie et nature des actions d'analyse et de remédiation déjà réalisées ;
    - mesures engagées par le commanditaire afin de détecter, voire bloquer l'attaquant ;
- les éventuels premiers résultats de la compréhension de l'incident de sécurité (voir chapitre VI.6.1) ;
- les éventuels rapports d'incidents précédents.

Annexe 5 Étapes des trois types de prestations