Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Première ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de réponse aux incidents de sécurité

Référentiel d'exigences

Version 2.1 du 14 février 2023

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
14/02/2023	2.1	*Version pour appel à commentaires.* Modifications principales : • Répartition des exigences selon deux niveaux d'assurance [ELEVE] et [SUBSTANTIEL] • Simplification des notions d'activités et de prestations • Allègement des exigences générales • Allègement des attendus relatifs à la convention de service • Ajout de la notion de « Note de cadrage » • Mise à jour des exigences métiers • Transformation des activités IPR et ILP et clarification des périmètres des activités visées par le référentiel	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

commentaires-passipdispris@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 augmente l'exposition des systèmes d'information aux 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.

Les incidents de sécurité présentés par ce référentiel concernent à la fois les cyberattaques de masse (rançongiciel, attaques par opportunité) et les cyberattaques ciblées (attaques étatiques, gouvernementales).

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

- la recherche d'indicateurs de compromission ;
- l'investigation numérique ;
- le pilotage de l'investigation et/ou d'analyse;
- l'analyse de code malveillant.

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, sur la capacité organisationnelle et technique du prestataire à proposer une réponse aux incidents de sécurité conformément aux diverses exigences du référentiel, sur une démarche adaptée aux contraintes de la prestation et sur la protection des informations sensibles dont le prestataire aura connaissance au cours de la prestation.

Le présent référentiel contient des exigences applicables aux prestataires de réponse aux incidents de sécurité (PRIS), afin d'offrir un niveau d'assurance en fonction des risques et des profils d'attaquants. Les niveaux d'assurance couverts par le présent référentiel sont décrits dans le chapitre III.2.

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 ne se substitue ni à l'application de la législation et de la réglementation en vigueur, notamment en matière de protection des informations sensibles [II_901] et de protection du secret de la défense nationale

[IGI_1300], ni à l'application des règles générales imposées aux prestataires en leur qualité de professionnels, notamment leur devoir de conseil vis-à-vis de leurs commanditaires.

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 et aux pilotes.

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 et des pilotes 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.

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[2]
OIV	Opérateur d'importance vitale
PACS	Prestataire d'accompagnement et de conseil en sécurité
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
PSSI	Politique de sécurité des systèmes d'informations
RETEX	Retour d'Expérience

[2] http://cert.ssi;gouv.fr

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 (analyse système, analyse réseau, analyse de codes malveillants).

Bénéficiaire – entité bénéficiant du service de réponse aux incidents. Il peut s'agir d'un organisme dont tout ou partie d'un ou de plusieurs systèmes d'information fait l'objet d'un incident de sécurité d'origine malveillante ou d'une suspicion d'un tel incident. Le bénéficiaire de la prestation peut être ou non le commanditaire de la prestation.

Commanditaire - entité faisant appel au service de réponse aux incidents de sécurité. Le commanditaire de la prestation peut être ou non le bénéficiaire de la prestation.

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 publiquement accessible 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.

Expert – personne physique liée contractuellement avec le prestataire. L'expert est reconnu par le responsable de prestation comme ayant une ou plusieurs compétences spécifiques, nécessaires à l'appréhension du périmètre de la prestation et à l'exécution de certaines tâches nécessitant de telles compétences ou la maitrise d'un domaine d'expertise, et non nécessairement détenues par les analystes ou pilotes.

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 et contextuelles représentatives d'une manifestation ou d'une tentative 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 – Mise en œuvre de 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.

Pilote : personne réalisant une activité de pilotage, c'est-à-dire les actions visant à orienter et coordonner techniquement ou de manière organisationnelle la prestation fournie, conjointement avec le bénéficiaire ou toute entité externe impliquée dans la prestation. Le pilote adapte ses propositions en fonction des contraintes imposées (délais, environnement, contexte, …).

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.

Potentiel d'attaque – mesure de l'effort à fournir pour attaquer un service, exprimée en termes d'expertise, de ressources et de motivation d'un attaquant. L'annexe B.4 du document [CC_CEM] fournit des indications relatives au calcul d'un potentiel d'attaque (« high », « moderate », « enhanced-basic », « basic »).

Prestataire – entité 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.

Renseignement sur la menace ou *Threat Intelligence* : ensemble des processus d'identification et d'analyse des cybermenaces.

Responsable d'équipe– personne responsable de la prestation en réponse aux incidents de sécurité et de la constitution de l'équipe d'analystes et de pilotes, 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. Selon le type de prestation, le responsable de l'équipe peut être un analyste ou un pilote.

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

Sous-traitance – opération par laquelle le prestataire confie sous sa responsabilité à une entité (le sous-traitant) 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, du commanditaire et du bénéficiaire.

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

II. Activités visées par le référentiel

Ce chapitre présente les différentes activités de réponse aux incidents traitées dans le référentiel.

Les activités couvertes par ce référentiel sont les suivantes :

- recherche d'indicateurs de compromission (REC);
- investigation numérique (INV);
- pilotage d'investigation et d'analyse (PIA) ;
- analyse de code malveillant (CODE) ;

Les activités REC, INV, PIA, CODE permettent la transition vers d'autres activités, dont les objectifs sont :

- d'enrayer l'activité d'un attaquant pour limiter une compromission ;
- de durcir la sécurité du système d'information cible de la prestation ;
- de préconiser ou d'accompagner aux mesures de remédiation imminentes lors d'un incident.

Ces objectifs ne sont pas traités dans le cadre de cette version du référentiel. Il est recommandé d'utiliser les guides de remédiation d'incidents de sécurité [G_REM] pour la délivrance des activités de remédiation.

II.1. Recherche d'indicateurs de compromission

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

Cette activité peut faire partie d'une activité d'investigation numérique.

II.2. Investigation numérique

L'investigation numérique consiste en une analyse des éléments collectés par le prestataire ou remis par le commanditaire, le bénéficiaire ou un tiers. L'investigation numérique a pour objectif d'identifier le périmètre d'une compromission et le mode opératoire d'un attaquant. Elle se conclut par des résultats d'analyses et des recommandations d'une suite à donner. Le type d'investigation et d'analyse est toujours précisé pour ce type d'activité : système (à partir d'équipements tels que des terminaux utilisateur, serveurs, périphériques, etc) et/ou réseau (à partir de systèmes de journalisation, de supervision, de détection des incidents de sécurité, etc).

Cette activité peut être complétée par une activité d'analyse de code malveillant.

Cette activité peut être encadrée ou non par une activité de pilotage d'investigation et d'analyse.

II.3. Analyse de codes malveillants

L'analyse de codes malveillants vise à identifier et analyser les codes malveillants pour comprendre leurs comportements, identifier l'ampleur de la compromission, consolider son périmètre et extraire des indicateurs de compromission. Elle se conclut par des résultats d'analyses et des recommandations d'une suite à donner.

Cette activité peut être encadrée ou non par une activité de pilotage d'analyse.

II.4. Pilotage d'investigation et d'analyse

Le pilotage d'investigation et d'analyse peut intervenir dans le cadre d'une investigation numérique ou d'une analyse de code malveillant.

Le pilotage d'investigation et d'analyse couvre, en relation avec les analystes, les éléments suivants nécessaires au traitement d'un incident de sécurité :

- la définition et le cadrage (posture technique, temps, moyens) des activités techniques d'investigation et d'analyse ;

- le pilotage, le contrôle et le suivi des activités techniques d'investigation et d'analyse tout au long de la prestation ;
- la synchronisation de ces éléments avec le commanditaire tout au long de la prestation.

Le pilote d'investigation et d'analyse doit prendre en compte les capacités (techniques et humaines) disponibles en interne (bénéficiaire) et externe (prestataire) et pouvoir adapter la posture au besoin.

Cette activité est nécessaire :

- lorsque le bénéficiaire n'a pas/plus la capacité interne (compétences, disponibilité) pour assurer cette fonction ;
- lorsque la complexité de l'incident (périmètre, sophistication) ou ses impacts imposent un suivi dédié car elles engendrent potentiellement plusieurs changements d'orientation/priorisation ;
- lorsque les éléments d'entrée (contexte techniques) et les attendus ne sont pas clairement spécifiés par le commanditaire ou le bénéficiaire.

Dans le cas contraire, les investigations numériques ou analyses de code malveillant sont dites « non pilotées », le commanditaire assurant les orientations et le suivi des actions.

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 souhaitée, conformément au chapitre III.2.

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

La portée de qualification prend en compte un niveau d'assurance tels que décrits ci-dessous ainsi qu'une activité ou combinaison d'activités.

Les deux niveaux d'assurance visés par le référentiel sont les suivants :

- le niveau d'assurance élevé. Le service vise à résister et répondre à des attaques de potentiel élevé, modéré et élémentaire amélioré (voir la définition de potentielle d'attaque) ;
- le niveau d'assurance substantiel. Le service vise à résister et répondre à des attaques de potentiel élémentaire.

Pour être qualifié, un prestataire doit répondre à toutes les exigences du présent référentiel sur la portée choisie, aux exceptions suivantes :

- les exigences et recommandations identifiées par le préfixe [SUBSTANTIEL] ne sont applicables que pour le niveau d'assurance substantiel ;
- les exigences et recommandations identifiées par le préfixe [ELEVE] ne sont applicables que pour le niveau d'assurance élevé.

La qualification de niveau élevé permet d'attester de l'aptitude du prestataire à effectuer des prestations de niveau élevé et substantiel.

Les exigences de niveau d'assurance élevé sont par défaut des recommandations pour le niveau d'assurance substantiel.

Tout bénéficiaire soumis à des obligations légales notamment s'il est identifié comme étant opérateur d'importance vitale ou obligations afférentes à la loi de programmation militaire [LOI_LPM] doit faire appel dans ce cadre, à un prestataire de niveau d'assurance élevé et possédant la mention LPM. Pour obtenir

cette mention, le prestataire de niveau élevé doit en plus des exigences du présent référentiel, répondre aux exigences supplémentaires définies dans [PRIS_LPM].

Dans le cas où le bénéficiaire de la prestation n'est soumis à aucune obligation règlementaire, le choix du niveau ainsi que du prestataire est de la responsabilité du commanditaire. Ce choix doit notamment découler d'une analyse de risque permettant d'identifier le niveau de menace auquel il est soumis.

Le prestataire de réponse aux incidents peut demander la qualification pour tout ou partie des activités décrites au chapitre 0. Toutefois, la qualification d'un prestataire de réponse aux incidents ne portant que sur les activités de recherche d'indicateurs de compromission (REC) et de pilotage d'investigation et d'analyse n'est pas autorisée (PIA), de telles activités étant jugées insuffisantes si menées seules.

Les activités ou combinaisons d'activités à prendre en compte dans la portée de qualification sont les suivantes :

- REC + INV
- REC + INV + PIA
- CODE

Un prestataire peut cumuler plusieurs activités ou combinaisons d'activités, dans ce cas, il doit répondre à l'ensemble des exigences sur l'activité ou les activités choisie(s).

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 ou pilotes 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. Pour les besoins de la loi de programmation militaire, une prestation est considérée comme qualifiée si elle respecte en plus 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, PACS, etc.).

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 sur la portée cible, peut potentiellement exposer le commanditaire ou le bénéficiaire 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 de demander au 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. Le prestataire est tenu d'accéder favorablement à cette demande.

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 être soumis au droit d'un État membre de l'Union Européenne et respecter les droits et règlements qui lui sont applicables.

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

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

e) Le prestataire doit apporter une preuve suffisante que son organisation, ses moyens mis en œuvre pour délivrer la prestation et les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du commanditaire ou de provoquer des conflits d'intérêts.

f) 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.

g) Le prestataire doit informer le commanditaire lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementale (par exemple dans le cadre de la loi de programmation militaire ou de la directive NIS[4]) et doit l'accompagner dans cette démarche si ce dernier en fait la demande.

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

i) Des mesures de sécurité doivent être mises en place pour protéger les informations relatives à la prestation à toutes les étapes. Le prestataire doit protéger en confidentialité ces informations, notamment lors de la phase de qualification préalable d'aptitude à la réalisation de la prestation (voir chapitre VI.1). Ces mesures doivent tenir compte du niveau de sensibilité ou de classification de ces informations.

IV.2. Gestion des ressources et des compétences

a) Le prestataire doit s'assurer, pour chaque prestation, que les analystes et/ou pilotes désignés ont les qualités et les compétences requises. Chaque analyste ou pilote de l'équipe doit disposer d'une attestation individuelle de compétence[7] pour les activités qui lui sont affectées au cours de la prestation.

b) Le prestataire doit d'assurer du maintien à jour des compétences des analystes et pilotes dans les activités pour lesquelles ils ont obtenu une attestation individuelle de compétence. Pour cela, le prestataire doit disposer d'un processus de formation continue et permettre à ses analystes et pilotes d'assurer une veille technologique[8].

---

[4] Directive *Network Information Security*, résultant de la coopération entre les Etats membres de l'Union Européenne et portant sur les aspects politiques et opérationnels de la cybersécurité.

[7] Voir [QUAL_SERV_PROCESS].

[8] Le prestataire peut par exemple mettre en place une formation en continue, des modules d'auto-formation, des séminaires internes, s'abonner à des revues spécialisées, contracter avec un ou plusieurs CERT, disposer d'un accès à une ou plusieurs bases de vulnérabilités offrant un certain niveau de garantie en matière de couverture et de réactivité ou toute autre méthode lui permettant d'assurer l'évolutivité de ses compétences ainsi que celles de son personnel.

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

d) Le prestataire est responsable des méthodes et outils utilisés par ses analystes et pilotes et de leur bonne utilisation 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 justifier, au travers des analystes et des pilotes évalués au titre de la qualification du prestataire, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités citées en Annexe 2.

f) Le prestataire doit mettre en place un processus de sensibilisation des analystes et des pilotes à la réglementation en vigueur sur le territoire de l'Union Européenne et applicable à leurs missions.

g) Le prestataire doit s'assurer que les analystes et les pilotes ne font pas l'objet d'une inscription, qui ne soit incompatible avec l'exercice de leurs fonctions, au bulletin n°3 du casier judiciaire français ou un extrait de casier judiciaire étranger pour les candidats résidant hors du territoire français.

IV.3. Protection de l'information

Dans le cadre de la réalisation de la prestation, le prestataire est amené à utiliser différents moyens informatiques. Dans ce cas, plusieurs scénarios sont envisageables, illustrés ci-dessous :

- le bénéficiaire ou le commanditaire fournit l'ensemble des moyens et équipements à utiliser dans le cadre de la prestation. Dans ce cas, le prestataire a un devoir de conseil vis-à-vis de la protection des informations relatives à la prestation. Ces moyens sont tracés dans la note de cadrage (voir chapitre VI.2.5) ;
- le prestataire utilise tout ou partie de son système d'information. Pour les prestations de niveau [ELEVE], le prestataire doit disposer d'un système d'information de niveau *Diffusion Restreinte* et effectuer par défaut les activités identifiées comme étant des activités de rédaction (traitement des documents métier reçus ou élaboration de nouveaux documents) sur le système d'information de niveau au minimum *Diffusion Restreinte*).

Dans ce dernier cas, le prestataire conjointement avec le commanditaire détermine la sensibilité des livrables et documents résultant de ces activités : le marquage *Diffusion Restreinte* n'étant pas automatiquement appliqué. Cette mesure est souhaitée afin d'assurer un niveau de protection sur les informations du commanditaire et du bénéficiaire tout en permettant de répondre à l'urgence de la mission.

Pour les données classifiées [IGI_1300], des moyens adaptés doivent être utilisés.

a) Le prestataire doit respecter les prescriptions de l'[IGI_1300] et de l'[II_901] sur les systèmes d'information de niveau *Diffusion Restreinte* pour ses systèmes d'information traitant les informations sensibles relatives à la prestation.

   [ELEVE] Au minimum, le prestataire doit disposer d'un système d'information ou de dispositifs permettant de traiter des informations sensibles de niveau *Diffusion Restreinte*.

b) [ELEVE] Par défaut, sauf demande explicite du commanditaire de la prestation, les activités de rédaction (traitement des documents métier reçus ou élaboration de nouveaux documents) doivent être effectuées sur le système d'information de niveau *Diffusion Restreinte* relatif au service de réponses aux incidents.

c) Il est recommandé aux prestataires d'utiliser le guide [G_SIDR] pour la sécurisation de leurs systèmes d'information de niveau *Diffusion Restreinte*.

d) Le système d'information ou les dispositifs utilisés dans le cadre de leur prestation doivent avoir fait l'objet d'une homologation au niveau adéquat et par conséquent, d'une appréciation des risques. Si le prestataire souhaite utiliser un système d'information déjà homologué, notamment au niveau *Diffusion Restreinte*, pour d'autres prestations, telles que celles relatives aux référentiels [PASSI], [PACS], ce dernier doit assurer une protection du besoin d'en connaitre des informations relatives aux prestations.

[ELEVE] Particulièrement, le prestataire doit :

i. mettre en place un cloisonnement au moins logique du système d'information entre les différentes activités au sens des différents référentiels [PASSI], [PACS], etc. ;

ii. mettre en place un cloisonnement au moins logique du système d'information entre les différentes prestations effectuées (pour le compte de différents commanditaires, affaires) ;

iii. effectuer une revue, au moins tous les 6 mois, des droits associés aux mécanismes de cloisonnement.

e) Il est recommandé que le prestataire utilise la démarche décrite dans le guide [G_HOM] pour homologuer son système d'information et ses dispositifs utilisés dans le cadre de la prestation.

f) [ELEVE] Le prestataire doit appliquer au minimum le *Niveau Renforcé* du guide d'hygiène informatique de l'ANSSI [G_HYG] sur le système d'information ou les dispositifs utilisés par le prestataire dans le cadre de sa prestation.

[SUBSTANTIEL] Le prestataire doit appliquer au minimum le *Niveau Standard* du guide d'hygiène informatique de l'ANSSI [G_HYG] sur le système d'information ou les dispositifs utilisés par le prestataire dans le cadre de sa prestation.

g) En tenant compte du contexte de la prestation, de l'analyse de risque et de la sensibilité du système d'information concerné, le prestataire doit sensibiliser le commanditaire sur le risque de compromission d'information par un attaquant lors de la prestation (voir Annexe 3 III, paragraphe l). Le prestataire doit convenir avec le commanditaire des moyens et mesures adaptées à la situation et aux risques :

i. les méthodes de communication qui seront employées lors de la prestation entre le prestataire, le commanditaire et le bénéficiaire (par exemple : canal chiffré à l'état de l'art). La transmission de documents techniques doit être protégée par un chiffrement logiciel additionnel indépendant du chiffrement natif du protocole de communication, sauf demande du commanditaire.

ii. les moyens logistiques devant être mis à disposition du prestataire par le commanditaire et le bénéficiaire (par exemple : moyens matériels, humains, techniques, etc.) ;

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

iv. les mesures pourront être réévaluées conjointement en cas d'évolution de la situation.

h) 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 système et réseau.

i) 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 et de diffusion associées.

V. Exigences relatives aux analystes et aux pilotes

V.1. Aptitudes générales

a) Le pilote technique et le responsable d'équipe 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) Les analystes et pilotes doivent disposer de qualités rédactionnelles, de rigueur et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible.

d) Les analystes et les pilotes doivent régulièrement mettre à jour leurs compétences conformément aux processus de formation et de veille du prestataire (voir chapitre IV.2, paragraphe b)), par une veille active sur la méthodologie, les techniques et les outils utilisés dans le cadre de leurs missions.

Il est recommandé que les analystes et pilotes participent à l'évolution de l'état de l'art par une participation à des évènements professionnels de leur domaine de compétence, à des travaux de recherche ou la publication d'articles.

V.2. Expérience

a) Il est recommandé que les analystes et les pilotes aient reçu une formation en technologies des systèmes d'information.

b) Il est recommandé que les analystes justifient :

- 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) Les analystes et les pilotes doivent maîtriser les bonnes pratiques en matière de gestion des incidents de sécurité décrites dans la norme [ISO27035].

b) Les analystes et les pilotes doivent maîtriser les bonnes pratiques et la méthodologie de collecte et de préservation des preuves décrites dans la norme [ISO27037].

c) Les analystes et les pilotes doivent réaliser la prestation conformément aux exigences du chapitre VI.

d) Les analystes et les pilotes doivent assurer les missions selon leur profil, telles que définies dans l'Annexe 2.

e) Les analystes et les pilotes doivent disposer des compétences requises par leur profil, telles que définies dans l'Annexe 2.

f) Il est recommandé que les analystes et les pilotes soient sensibilisés à l'ensemble des autres activités pour lesquelles le prestataire demande la qualification.

V.4. Engagements

a) Les analystes et pilotes doivent avoir un contrat avec le prestataire.

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

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.

Les étapes et exigences du chapitre IV s'appliquent à toutes les activités, sauf si elles sont précédées d'un ou plusieurs identifiants entre crochets. Dans ce cas, elles ne s'appliquent qu'aux types d'activités indiquées par leur identifiant.

Les identifiants utilisés sont :

- REC pour la recherche d'indicateurs de compromission ;
- INV pour l'investigation ;
- PIA pour le pilotage de l'investigation et/ou d'analyse ;
- CODE pour l'analyse de code source.

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

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) [REC, INV, PIA]. 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.

b) Il est recommandé que le prestataire demande au commanditaire de lui fournir les informations de contexte sur l'incident de sécurité et notamment celles identifiées dans l'Annexe 4.

c) 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, nombre d'analystes et de pilotes à engager, disponibilité des ressources en interne, etc.

d) 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.

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.

Lorsqu'une intervention rapide est requise et justifiée, un accord sur le périmètre et le type d'action envisagé est un prérequis à toute intervention qui impliquerait d'accéder au système d'information. Cet accord doit être signé par des représentants légaux ou toutes personnes en mesure d'engager les parties impliquées.

b) La convention de service doit être signée par le prestataire et le commanditaire. Elle doit être signée par des représentants légaux ou toute personne pouvant engager le prestataire et le commanditaire. Dans le cas où le commanditaire n'est pas le bénéficiaire de la prestation, celui-ci atteste de l'accord du bénéficiaire pour démarrer la prestation. Toute modification de la convention de service doit être soumise à acceptation du commanditaire.

VI.2.1. Modalités de la prestation

La convention de service doit :

a) indiquer que la prestation réalisée est une prestation qualifiée et inclure l'attestation de qualification du prestataire ;

b) identifier et appliquer le droit d'un Etat membre de l'Union Européenne ;

c) décrire le périmètre de la prestation, la démarche générale de réponse à l'incident de sécurité, les activités et les modalités de la prestation (objectifs, jalons, etc.) ;

d) indiquer que les analystes et pilotes disposent d'une attestation individuelle de compétence pour les activités de la prestation et inclure ces attestations ;

e) préciser que le prestataire peut faire intervenir un expert sur une partie de la prestation pour des activités nécessaires à la qualité globale de la prestation et motivées par un besoin de compétences spécifiques non couverts par les analystes et pilotes, sous réserve que :

   i. il existe une convention ou un cadre contractuel documenté entre le prestataire et l'expert ;

   ii. le recours est connu et formellement accepté par écrit par le commanditaire ;

   iii. l'expert est dûment encadré par le responsable d'équipe de la prestation.

   Dans ce cas, l'expert ne se substitue pas à un analyste ou pilote disposant ou non d'une attestation de compétence.

f) préciser les prérequis attendus en entrée du commanditaire. Il est recommandé d'utiliser l'Annexe 4 ;

g) préciser les livrables attendus, les réunions d'ouverture et de clôture éventuelles, les publics destinataires, le niveau de sensibilité ou de classification des systèmes impactés ;

h) 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 bases de connaissance ou le rapport de prestation ;

i) préciser les traitements qui ne peuvent être menés sur les informations collectées sans autorisation expresse du commanditaire et éventuellement accord ou présence de celui-ci, ainsi que les modalités associées (mise en œuvre, personnes présentes, durée, plage horaire, exécutant, description des données sensibles et des actions autorisées, etc.) ;

j) spécifier que le prestataire ne recourt pas à des analystes ou pilotes n'ayant pas de relation contractuelle avec lui, n'ayant pas obtenu une attestation individuelle de compétence ou ayant fait l'objet d'une inscription au bulletin n°3 du casier judiciaire français ou extrait de casier judiciaire étranger pour les candidats résidant hors du territoire français ;

k) préciser les modalités (contenu, forme, langue, etc.) de rédaction des livrables produits par le prestataire au titre de la prestation.

VI.2.2. Responsabilités

La convention de service doit :

a) spécifier que le prestataire informe le commanditaire en cas de manquement à la convention et réciproquement ;

b) spécifier 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 parties impliquées, et notamment de ses prestataires ou partenaires, dont les systèmes d'information entrent dans le périmètre de la prestation ;

c) spécifier que le commanditaire, avec accord du bénéficiaire, 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 ;

d) spécifier que le commanditaire, avec accord du bénéficiaire, 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.

VI.2.3. Confidentialité

La convention de service doit :

a) indiquer que le prestataire ne divulgue ou ne partage aucune information relative à la prestation à des tiers, sauf autorisation écrite du commanditaire ;

b) indiquer que le prestataire met en place une liste des informations transmises aux tiers autorisés ; cette dernière précise pour chaque information le tiers auquel elle a été transmise. Cette liste est maintenue à jour et mise à disposition du commanditaire lorsque ce dernier en fait la demande ;

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

- le centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques[12] (CERT-FR) doit également autoriser formellement et par écrit le partage. Sans réponse de ce dernier et après un délai de 10 jours ouvrés, le prestataire disposant de l'autorisation du commanditaire et du bénéficiaire peut procéder au partage;
- les informations partagées à un tiers doivent être protégées en confidentialité, conformément à leur niveau de sensibilité ou de classification ;
- toute action de partage doit être accompagnée d'une information au centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR).

d) spécifier que le prestataire, sauf refus formel et écrit du commanditaire ou du bénéficiaire, transmet au centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) les éléments anonymisés et décontextualisés (voir VI.2.3.c), ainsi que leur niveau de sensibilité ou de classification et leurs conditions d'utilisation ;

e) indiquer que le prestataire détruit l'ensemble des informations relatives à la prestation à l'issue de la prestation ou à la date d'échéance de la durée de conservation, au premier terme échu, à l'exception de celles pour lesquelles il a reçu une autorisation écrite de conservation de la part du commanditaire. Le cas échéant les modalités de conservations (par exemple anonymisation, décontextualisation, durée) doivent être approuvées par le commanditaire.

VI.2.4. Sous-traitance

La convention de service doit :

a) préciser que le prestataire peut sous-traiter une partie des activités à un autre prestataire qualifié conformément aux exigences du référentiel qui lui sont applicables sous réserve que :
   i. il existe une convention ou un cadre contractuel documenté entre le prestataire et son sous-traitant ;
   ii. le recours à la sous-traitance est connu et formellement accepté par écrit par le commanditaire
   iii. le prestataire respecte les exigences du référentiel sur l'activité cible.

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

VI.2.5. Note de cadrage

a) La convention de service doit imposer l'élaboration d'une note de cadrage. Cette note de cadrage doit être validée par le correspondant de la prestation chez le commanditaire et le responsable d'équipe chez le prestataire au début de la prestation.

b) La note de cadrage doit :

i. préciser le nom du correspondant de la prestation chez le commanditaire ou le bénéficiaire ;

ii. préciser les noms, rôles, responsabilités ainsi que les droits et besoin d'en connaître des personnes désignées par le prestataire et le commanditaire ;

iii. le cas échant, prévoir et prendre en compte les modalités de collaboration avec les prestataires tiers concernés (sous-traitants du commanditaire, etc.) ;

iv. spécifier les instances de gouvernance de la prestation mises en place et leur fréquence de réunion (réunions, comités de pilotage, etc.).

v. spécifier les modalités et moyens utilisés lors de la prestation conformément à l'exigence IV.3.e). Dans le cas où des dispositifs ou système d'information non *Diffusion Restreinte* sont utilisés ; ceux-ci doivent être identifiés dans la note de cadrage afin d'en assurer une traçabilité ;

vi. identifier les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le système d'information cible ; préciser, le cas échéant, les exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire et notamment celles liées à son secteur d'activité.

c) [INV, CODE, PIA] spécifier les moyens assurant la traçabilité entre le bénéficiaire et le prestataire des informations et supports matériels remis pour analyse ;

d) La note de cadrage doit être mise à jour tout au long de la prestation.

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.

VI.3.1. Compréhension de la situation

a) [INV, PIA] Les prérequis fournis et les échanges avec le commanditaire et le bénéficiaire 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 les parties impliquées (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) [REC, INV, PIA] Il est recommandé que le prestataire définisse et mette en œuvre une démarche pragmatique de compréhension du système d'information cible pour disposer d'une connaissance fidèle de l'existant, notamment :

i. la vision globale du système d'information cible ;

ii. les contraintes géographiques associées au système d'information cible (par exemple : réseau local, multi-sites, international, etc) ;

iii. les spécificités et contraintes du système d'information cible ;

iv. le(s) fuseau(x) horaire(s) utilisé(s) dans le système d'information cible et celui qui sera utilisé dans le cadre de la prestation ;

v. les dépendances et interconnexions du systèmes d'information cible (partenaires, sous-traitants, etc).

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

a) [PIA] Le pilote d'investigation et d'analyse doit proposer au commanditaire une posture initiale identifiant notamment :

i. 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 déconnectés, collecte d'informations sur des équipements inaccessibles par l'attaquant, etc.). Les activités réalisées par le prestataire n'exposent pas la connaissance sur l'attaquant et 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 peuvent entraver partiellement ou totalement les opérations de l'attaquant, mais n'apparaissent pas nécessairement dirigées contre lui, ses moyens et canaux de communication peuvent être 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 peuvent entraver 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 peuvent parfois être bloqués ou supprimés.

Les exceptions ou cas notables allant à l'encontre du niveau de discrétion et pouvant rendre perceptible les actions du prestataire, doivent faire l'objet d'une validation du commanditaire.

ii. 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 ;

iii. les activités à réaliser, les informations à collecter, le nombre d'analystes à engager et le calendrier associé.

b) [PIA] Le pilote d'investigation et d'analyse doit établir sa posture en fonction de sa compréhension de l'incident de sécurité et de l'environnement.

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

d) [PIA] Le pilote d'investigation et d'analyse 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 afin de coordonner et suivre la prestation. Il est l'interlocuteur privilégié du commanditaire et du bénéficiaire ;

b) Le responsable d'équipe doit, dès le début de la préparation de la prestation, établir un contact avec le correspondant chez le bénéficiaire. 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 (voir IV.3.e)). Le responsable d'équipe doit également obtenir du correspondant chez le bénéficiaire la liste des points de contact nécessaires à la réalisation de la prestation.

c) Le prestataire 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) Le prestataire 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).

e) Le prestataire 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 doit constituer une équipe disposant des compétences nécessaires à la réalisation des activités et doit s'assurer que ceux-ci disposent d'une attestation de compétence pour les activités qu'ils mènent. Le nombre et les compétences doivent être adaptées à la prestation.

Le responsable d'équipe peut, s'il dispose des compétences suffisantes et d'une attestation individuelle de compétence, réaliser la prestation de réponse aux incidents de sécurité lui-même et seul. Il peut également faire appel à de la sous-traitance dans les conditions définies dans la convention.

Un analyste peut intervenir sur plusieurs types d'analyses et/ou d'une activité de pilotage s'il dispose des attestations individuelles de compétence associées.

b) [REC, INV, PIA] Le responsable d'équipe doit réévaluer régulièrement le profil et le nombre d'analystes et de pilotes afin de s'assurer que l'engagement reste adapté à la prestation.

[PIA] 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).

c) 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 d'accès 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) [ELEVE] [REC, INV, PIA] Le responsable d'équipe doit mettre en place et tenir à jour un registre centralisé, imputable et chronologique recensant pour chaque action réalisée 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.) ;
- la réalisation de l'action (effectuée, partiellement effectuée, échec de réalisation, le cas échéant, les limites et motifs de l'échec) ;
- le système d'information et les fichiers concernés par l'action ;

- les noms des analystes ou pilotes ayant réalisé l'action.

[SUBSTANTIEL] Cette exigence est une recommandation pour le niveau de garantie substantiel.

b) [ELEVE] [REC, INV, PIA] 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.

[SUBSTANTIEL] Cette exigence est une recommandation pour le niveau de garantie substantiel.

c) [ELEVE] [REC, INV, PIA] Le responsable d'équipe doit, en collaboration avec le commanditaire, définir les procédures et les clauses particulières associées aux informations et supports collectés :

- 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) Le prestataire 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 à leur niveau de sensibilité ou de classification (voir Annexe 3 III, paragraphe i).

e) Le prestataire lorsque cela s'avère nécessaire, 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 [G_GHI] 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. Modalités et préparations des bases de connaissances

Les indicateurs de compromission peuvent provenir :

- d'une activité de veille sur la menace (par exemple provenant des processus de renseignement sur la menace s'ils existent) ;
- d'une activité de veille technique (par exemple sur les vulnérabilités et les codes malveillants) ;
- d'indicateurs provenant d'une compromission antérieure d'une même organisation (issus d'un précédent incident) ou d'une organisation différente (capitalisation de prestations) ;
- de partage provenant de partenaires extérieurs (agences nationales, réseaux de partage tel que l'InterCERT France, etc).

a) [REC, INV, PIA] Le prestataire doit disposer d'une base d'indicateurs de compromission régulièrement mise à jour et savoir prendre en compte les indicateurs spécifiquement transmis dans le cadre de l'incident.

VI.5.4. Mise en place de mesures de sauvegarde et de préservation

a) Le prestataire 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.5.5. Mise en place de procédures d'urgence

a) [PIA] Le pilote d'investigation et 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.

   Si des procédures sont déjà existantes, notamment suite à la prestation d'un prestataire d'accompagnement et de conseil en sécurité (PACS), le pilote d'investigation et d'analyse doit en prendre connaissance et les exploiter au mieux selon le contexte de la prestation.

b) [PIA] 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

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

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

b) [ELEVE] [PIA] Le pilote d'investigation et d'analyse doit maintenir à jour une synthèse du mode opératoire de l'attaquant et du périmètre concerné tout au long de la prestation :

   i. la (ou les) date(s) de compromission initiale(s) ;

   ii. 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.) ;

   iii. 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.) ;

   iv. les moyens de déplacement latéral :

      - vulnérabilités exploitées et outils utilisés ;
      - techniques utilisées pour l'escalade de privilège sur le système d'information cible ;

   v. les moyens d'interconnexion 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 ;
- moyens de communication physiques ajoutés par l'attaquant (cartes sans-fil) ;
- liste des équipements correspondants ;
- la liste des indicateurs de compromission.

c) [PIA] 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 :

i. caractériser la nature des informations ciblées afin de permettre au commanditaire d'évaluer la motivation présumée de l'attaquant (espionnage, intelligence économique, cybercriminalité, etc.) ;

ii. confirmer ou infirmer la présence active de l'attaquant dans le système d'information ;

iii. identifier le niveau de complexité de l'attaque (ex. : code malveillant spécifique ou générique) ;

iv. évaluer de manière plus précise le périmètre, les risques et l'impact de la compromission ;

v. adapter la posture ;

vi. établir le plan d'action de remédiation associé au périmètre à assainir. Il est recommandé de s'aider des guides [G_REM] pour établir ce plan d'action de remédiation.

d) Dans le cas avéré d'un incident de sécurité, le prestataire doit proposer des mesures d'endiguements (mesures conservatoires permettant de limiter ou ralentir les actions de l'attaquant) et évaluer avec le commanditaire les mesures nécessaires à la protection du système d'information. Ces mesures doivent être réévaluées régulièrement.

e) 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.

VI.6.2. Phase 2 : révision de la posture

a) [PIA] Le pilote d'analyse et d'investigation 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) [PIA] Le pilote d'analyse et d'investigation doit mettre à jour la feuille de route associée (voir chapitre VI.4).

c) [PIA] Le pilote d'analyse et d'investigation 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 peut être effectuée :

- par le prestataire, le commanditaire, le bénéficiaire ou un tiers;
- à chaud, ou à froid sur le système cible ;
- au travers de copies ou non ;

- connecté (en ligne) ou déconnecté du système cible.

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.

VI.6.3.1. Conditions de réalisation

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

   [PIA] 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) [PIA] Si la collecte est effectuée par un tiers, par le commanditaire ou le bénéficiaire, le prestataire doit les orienter sur les méthodes de collecte à réaliser (copie disque, copie mémoire, utilisation d'un outil de collecte, utilisation d'une solution de type EDR, etc). La méthode de collecte doit être adaptée à la posture préalablement convenue entre le prestataire et le bénéficiaire, en particulier si la méthode de collecte présente un risque pour la disponibilité du système d'information cible.

d) [REC, INV, PIA] Le prestataire ne doit collecter que les informations nécessaires au bon déroulement de la prestation. Le prestataire doit mettre à disposition du commanditaire la liste des éléments qui seront collectés. Le commanditaire peut refuser la collecte de certains éléments.

   Néanmoins, le prestataire doit sensibiliser le commanditaire à l'importance de la collecte des éléments pour l'efficacité de la prestation.

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

f) [REC, INV, PIA] Les analystes doivent identifier, les points de collecte système et réseau permettant d'atteindre les objectifs de la prestation.

g) [REC, INV, PIA] 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, 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 et analysés au titre de la prestation.

i) [PIA] Les analystes doivent définir et mettre en place des moyens adaptés aux contraintes du bénéficiaire 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) [REC, INV] 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.) ;
- service externalisé largement répandu (ex. technologies relatives à l'informatique en nuage).

b) [REC, INV] 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) [ELEVE] [REC, INV] 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

a) [REC] Dans le cas d'une recherche déconnecté, hors-ligne, les analystes doivent réaliser une copie 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.).

[INV] Pour les équipements inclus dans le périmètre de la prestation, les analystes doivent réaliser une copie 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.).

[PIA] 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 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) [ELEVE] [REC, INV] Le prestataire doit disposer de solutions (notamment en termes d'outillages et de procédures d'exploitation) 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.) ;
  - sur des infrastructures de services externalisées (ex : serveurs d'informatique en nuage).

b) [ELEVE] [PIA] 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 [G_LOGS] 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) [INV] 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.

VI.6.3.6. Supervision de circonstance

a) [ELEVE] [PIA] 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 [G_LOGS] qui propose des recommandations en matière d'architecture.

VI.6.4. Phase 4 : Analyse des informations

[INV, PIA] 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.

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 ;
- [INV] d'identifier un potentiel incident de sécurité dans le système d'information cible ;
- [PIA] d'améliorer la compréhension de l'incident de sécurité affectant le système d'information cible
- [CODE] de comprendre le comportement des codes malveillants et d'en extraire des indicateurs de compromission.

VI.6.4.2. Conditions de réalisation

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

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

d) [REC, INV, PIA] 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.

e) [REC, INV, PIA, CODE] Le responsable d'équipe 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. La recherche d'indicateur de compromission peut s'appuyer :

- sur des outils existants au sein de l'entreprise (*Security Operation Center*, solution *Endpoint Detection and Response*, antivirus, etc) ;
- sur un outil externe dédié prenant en charge des fonctionnalités de recherche de marqueurs (ex : ORC/fastFind, etc). Celui-ci doit être adapté aux moyens d'administration et de déploiement existants ou compatibles dans l'organisation/entreprise (GPO, SCCM, …). La centralisation des résultats doit également être adaptée aux capacités existantes du système d'information cible.

De plus, une attention particulière doit être portée par le prestataire sur la pertinence des indicateurs de compromission afin qu'ils soient adaptés au contexte de la prestation.

a) [REC] Avant le lancement de la recherche, le prestataire doit vérifier :
   i. la pertinence des indicateurs de compromissions utilisés afin d'éviter au maximum les faux positifs ;
   ii. la performance de la méthode de recherche prévue.

La performance de la méthode de recherche doit être adaptée au contexte de la prestation afin de limiter les impacts relatifs aux perturbations du ou des systèmes d'informations du commanditaire ainsi qu'aux perturbations afférentes aux moyens utilisés par le prestataire dans le cadre de sa prestation.

b) [REC, INV] S'il existe, les analystes doivent prendre en compte le marquage des indicateurs de compromission lors des recherches (modalité de diffusion et en particulier les modalités d'utilisation). 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]

c) [ELEVE] [REC, INV] 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.) ;
- infrastructures de services externalisées (ex : serveurs d'informatique en nuage).

d) [REC, INV] 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).

e) [REC, INV] Les analystes doivent être capables de normaliser les indicateurs de compromission qui leur sont transmis afin de pouvoir réaliser les recherches de façon cohérente.

f) [ELEVE] [REC, INV] 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 d). 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.

g) Les indicateurs de compromission issus des investigations et des analyses doivent faire l'objet d'un marquage permettant de préciser :

i. leur sensibilité ou classification, au sens [IGI_1300] et [II901] ;
ii. leurs modalités de diffusion (ex. : TLP Traffic Light Protocol) ;
iii. leurs modalités d'utilisation (ex. : PAP Permissible Actions Protocol).

Il est recommandé d'utiliser le double marquage TLP : PAP tel que décrit dans [CERT-FR TLP:PAP].

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

a) [REC, INV] 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) [REC, INV] 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) [REC, INV] 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 :

- [PIA] 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) [REC, INV] Le responsable d'équipe doit mettre en place et tenir à jour un document référençant chronologiquement tous les évènements caractérisant les activités de l'attaquant (date relative au système ayant été touché par l'évènement, date rapportée à la base de temps de référence, vecteurs, etc).

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

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

b) [CODE] L'analyste doit réaliser les analyses de codes malveillants nécessaires, notamment :

- 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.

c) [CODE] 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) [ELEVE] [PIA] 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 de l'attaquant. Il est donc important que le prestataire observe la plus grande prudence en les effectuant.

a) [ELEVE] Le prestataire doit définir une méthodologie pour la recherche en sources ouvertes à partir d'informations collectées ou issues des analyses. Elle doit préciser, en fonction du niveau de discrétion recherché vis-à-vis de l'attaquant les types d'informations pouvant être recherchés et les modalités associées. Elle doit également prendre en compte le niveau de sensibilité et classification, les modalités d'utilisation des indicateurs de compromission (notamment les éventuels marquages PAP).

b) [ELEVE] 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) [ELEVE] Le prestataire doit, autant que possible, utiliser des bases d'informations internes et pré-collectées 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) [ELEVE] 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) [REC, INV] Les analystes doivent réaliser systématiquement l'analyse des résultats de recherche, d'investigation et d'analyse. Les analystes doivent vérifier la pertinence des indicateurs de compromissions issus des investigations, des analyses et des recherches afin d'éviter les faux-positifs lors de leurs exploitations ou des suites à donner. Cette analyse doit s'appuyer sur :

   i. 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 ;

   ii. une ou plusieurs phases d'échanges avec le commanditaire sur les éventuels faux-positifs.

Cette qualification pour l'activité REC, et INV, permettra d'établir si l'indicateur de compromission identifié correspond à une activité malveillante. Une investigation numérique pilotée ou non pourra alors être engagée si des analyses complémentaires sont nécessaires pour déterminer le périmètre de la compromission.

e) Le responsable d'équipe doit :

- regrouper et synthétiser les résultats des analyses ;
- [PIA] 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 et accompagner le commanditaire à leurs capitalisations ;
- [PIA] 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).

f) [ELEVE] [REC, INV] Le responsable d'équipe est responsable de l'anonymisation et de la décontextualisation des nouveaux indicateurs de compromission obtenus lors de sa prestation pour le compte du commanditaire. La politique de partage de ces indicateurs de compromission est de la responsabilité du commanditaire.

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

h) [PIA] Le prestataire doit pouvoir formaliser les éléments issus des investigations, des recherches et des analyses afin d'alimenter un éventuel plan de remédiation. Il est possible de s'aider des guides [G_REM] pour établir ce plan d'action de remédiation.

VI.7. Étape 7 - Restitutions

a) [PIA] Le pilote d'investigation et 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

b) Le responsable d'équipe doit assurer une restitution lors de découverte notable.

c) [PIA] En complément, le responsable d'équipe doit assurer une restitution à chaque révision de la posture.

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 associées (voir chapitre II).

c) [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;
- la suite à donner à la recherche, incluant :
    - la justification des recommandations,
    - 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 pilotée ou non, en précisant le type d'analyse requise, une analyse de code),
        - le périmètre de la prestation,
        - le niveau de discrétion requis.

[INV] 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 des recommandations,
    - les différentes options possibles, le cas échéant,
    - lorsque la suite à donner indique de poursuivre avec une nouvelle prestation :
        - le type de prestation (investigation complémentaire, une investigation pilotée, une analyse de code, etc),
        - le périmètre de la prestation,
        - le niveau de discrétion requis.

[PIA] 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,
- 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 ;
- la suite à donner à la recherche, incluant :
    - la justification des recommandations,
    - les différentes options possibles, le cas échéant,
    - lorsque la suite à donner indique de poursuivre avec une nouvelle prestation :
        - le type de prestation (investigation complémentaire, une investigation pilotée, une analyse de code, etc),
        - le périmètre de la prestation,

- le niveau de discrétion requis.

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

- une synthèse, compréhensible par des non-experts, qui précise :
  - l'objectif de l'analyse,
  - l'(es) indicateur(s) de compromission recherché(s),
  - le périmètre couvert par l'analyse,
  - succinctement le comportement du ou des codes malveillant ;
  - les résultats de l'analyse,
  - la suite à donner à l'analyse;
- la description des analyses réalisées et de leurs résultats (voir chapitre VI.6.4) :
  - les modes opératoires,
  - les outils utilisés,
  - les vrais positifs;
- le comportement du ou des codes malveillants en fonction de l'environnement ;
- la suite à donner à la recherche, incluant :
  - la justification des recommandations,
  - les différentes options possibles, le cas échéant,
  - lorsque la suite à donner indique de poursuivre avec une nouvelle prestation :
    - le type de prestation (recherche d'indicateur de compromission, une investigation numérique pilotée ou non, une analyse de code complémentaire)
    - le périmètre de la prestation.

d) [ELEVE] [PIA] 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).

e) 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, durées de rétention de certains journaux trop courte, etc.) pour compléter les analyses et consolider une chronologie exhaustive de toutes les actions de l'attaquant.

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 et le bénéficiaire suite à la livraison du rapport d'analyse, conformément au chapitre VI.7. Cette réunion permet de présenter la synthèse du rapport d'analyse, [PIA] de la chronologie des événements composant l'incident de sécurité, de la suite à donner à la prestation et d'organiser un jeu de questions / réponses.

b) Le responsable d'équipe 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 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 s'ils portent sur les mêmes faits.

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

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[IGI_1300]	Instruction générale interministérielle n°1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale. Disponible sur https://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 https://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 https://www.legifrance.gouv.fr
[D_2015_350]	Décret n°2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. Disponible sur https://www.legifrance.gouv.fr
[LOI_LPM]	Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. Disponible sur https://www.legifrance.gouv.fr

II. Normes et documents techniques

Renvoi	Document
[CC_CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[ISO19011]	Norme internationale ISO/IEC 19011: Lignes directrices pour l'audit des systèmes de management, version en vigueur Disponible sur https://www.iso.org
[ISO27000]	Norme internationale ISO/IEC 27000 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – vue d'ensemble et vocabulaire, version en vigueur. Disponible sur https://www.iso.org
[ISO27035]	Norme internationale ISO/IEC 27035-1 : Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information. Partie 1 : Principes de la gestion des incidents, version en vigueur. Norme internationale ISO/IEC 27035-2 : 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, version en vigueur. Disponible sur https://www.iso.org
[ISO27037]	Norme internationale ISO/IEC 27037 : Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques, version en vigueur. Disponible sur https://www.iso.org
[PRIS_LPM]	Exigences supplémentaires applicables aux prestataires de réponses aux incidents dans le cadre de la loi n°2013-1168 du 18 décembre 2013, ANSSI, version en vigueur. Document Diffusion Restreinte, il peut être obtenu auprès de l'ANSSI.

Renvoi	Document
[G_LOGS]	Guide - Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, ANSSI-PA-012/ANSSI/SDE, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_AUTH-MULTI-MDP]	Guide - Recommandations de sécurité relatives aux mots de passe, ANSSI-PG-078, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_HOM]	Guide - L'homologation de sécurité en neuf étapes simples, ANSSI - version en vigueur. Disponible sur http://www.ssi.gouv.fr
[G_HYG]	Guide d'hygiène informatique, ANSSI – version en vigueur. Disponible sur http://www.ssi.gouv.fr
[G_SIDR]	Guide – Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte – version en vigueur. Disponible sur http://www.ssi.gouv.fr
[G_REM]	Guides de remédiation d'incidents de sécurité, volet stratégique, volet opérationnel, volet technique – version en vigueur. Disponible sur http://www.ssi.gouv.fr

III. Autres références documentaires

Renvoi	Document
[STRAT_NUM]	Stratégie nationale pour la sécurité du numérique, octobre 2015. Disponible sur https://www.ssi.gouv.fr
[QUAL_SERV_PROCESS]	Processus de qualification d'un service, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[GUIDE_ACHAT]	Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[CERT-FR _TLP :PAP]	Politique de partage et d'utilisation des informations à caractère opérationnel. Disponible sur https://www.cert.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

Cette partie décrit les missions et compétences du responsable d'équipe. Le responsable d'équipe peut être un analyste si la prestation ne fait pas appel à un pilote d'investigation et d'analyse. Dans le cas contraire, il est recommandé à ce que le responsable d'équipe soit un pilote d'investigation et d'analyse.

I.1. Missions

Le responsable d'équipe 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 ;
- définir une démarche permettant de comprendre :
    - la situation ;
    - l'environnement (voir chapitre VI.3.2) ;
- 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 responsable d'équipe d'analyse doit avoir les qualités suivantes :

- savoir piloter des équipes d'analystes ;
- 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. Pilote d'investigation et d'analyse

Le pilote d'investigation et d'analyse doit répondre à l'ensemble des attendus du Responsable d'équipe (Annexe 2, Chapitre I). Le pilote d'investigation et d'analyse possède un profil technique.

II.1.Missions

Le pilote d'investigation et d'analyse doit assurer les missions suivantes, en complément des missions présentées en chapitre I de cette Annexe :

- gérer les priorités, en particulier en situation de crise ;
- définir une démarche permettant de comprendre :
    - la situation, l'incident de sécurité (voir chapitre VI.3.1) ;

    - l'environnement (voir chapitre VI.3.2) ;
- définir et réviser la posture (voir chapitres VI.4 et VI.6.2) ;
- maintenir à jour un état de la compréhension de l'incident de sécurité (voir chapitre VI.6.1) ;
- 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.) ;
- 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 ;
- préconiser les mesures nécessaires pour remédier à l'incident de sécurité, en limiter l'impact et réduire les risques d'une nouvelle compromission.

II.2.Compétences

Le pilote d'investigation et d'analyse doit avoir des compétences approfondies énoncées en chapitre I.2 de cette Annexe.

Le pilote d'investigation et d'analyse 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 pilote d'investigation et d'analyse doit avoir les qualités suivantes :

- savoir piloter des équipes d'analystes ;
- 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.).

III. Analyste système

III.1. Missions

L'analyste système doit assurer les missions suivantes :

- assimiler 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.

III.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).

IV. Analyste réseau

IV.1. Missions

L'analyste réseau doit assurer les missions suivantes :

- assimiler 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.) [G_LOGS] 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.

IV.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.

V. Analyste de codes malveillants

V.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.

V.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[18] 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[19].

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.).

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

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

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

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[20]) 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.

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.

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

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[21] 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)[22], 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).

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

[22] 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 [G_AUTH-MULTI-MDP].

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.

Le prestataire doit protéger ces informations conformément à leur niveau de sensibilité ou de classifications éventuels.