Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de réponse aux incidents de sécurité

Référentiel d'exigences

Version 0.3 du 7 juillet 2014

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
7/7/2014	0.3	*Prise en compte des remarques SD COSSI, SD SDE, MRR et validation pour publication.*	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

qualification@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

L'interconnexion croissante des réseaux et les besoins de dématérialisation des processus ou des documents exposent les systèmes d'information à des risques de vol, de modification ou de destruction de données. Ainsi, les points d'interconnexion avec l'extérieur, en particulier les accès Internet associés à la messagerie ou des téléservices, sont autant d'accès qu'un attaquant peut tenter d'utiliser pour s'introduire au sein même du système d'information, pour dérober, dénaturer ou encore détruire son patrimoine informationnel.

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 ;
- collecter et analyser des éléments issus du système d'information ;
- identifier le mode opératoire de l'attaquant ;
- qualifier l'étendue de la compromission ;
- évaluer les risques et les impacts associés ;
- préconiser des mesures de remédiation.

Un prestataire de réponse aux incidents de sécurité doit être capable d'intervenir dans le traitement d'une attaque ciblée et de grande ampleur.

I.1.2. Objet du document

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

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

Il permet aux commanditaires de disposer de garanties sur les compétences du prestataire et de ses analystes, sur la qualité des activités de réponse aux incidents de sécurité réalisées, sur la capacité du prestataire à adopter une approche globale de l'incident de sécurité et une démarche d'analyse adaptée.

Il peut également être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire.

Il n'exclut ni l'application des règles générales imposées aux prestataires en leur qualité de professionnel et notamment leur devoir de conseil vis-à-vis de leurs clients, ni l'application de la législation nationale.

I.1.3. Structure du document

Le chapitre II présente les activités visées par le référentiel.

Le chapitre III présente les modalités de la qualification.

Le chapitre IV décrit les exigences relatives au prestataire.

Le chapitre V décrit les exigences relatives aux analystes.

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

L'Annexe 1 présente les compétences et les missions à assurer par les analystes.

L'Annexe 2 présente des recommandations à l'intention des commanditaires de prestations de réponse aux incidents de sécurité.

L'Annexe 3 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 « Prestataire 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
CRI	Correspondant réponse à incident
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PRIS	Prestataire de réponse aux incidents de sécurité

I.3.2. Définitions

Les définitions ci-dessous s'appuient sur 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.

Analyse d'un incident de sécurité – procédé visant à collecter et analyser tout élément technique du système d'information permettant de comprendre le mode opératoire et l'étendue d'une compromission d'un système d'information.

Analyste – personne réalisant une prestation d'analyse pour le compte d'un prestataire (responsable d'équipe d'analyse, analyse système, analyse réseau, analyse de codes malveillants).

Commanditaire – organisme ou personne pour le compte desquels la prestation est réalisée.

Convention – accord écrit entre un commanditaire et un prestataire pour la réalisation de l'activité de réponse aux incidents. Dans le cas où le prestataire est un organisme privé, la convention est le contrat.

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

Évènement de sécurité – occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une faille possible dans 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.

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

Indicateur de compromission – combinaison d'informations techniques représentatives d'une manifestation de compromission, qui peuvent être identifiées à partir de l'analyse d'un système, d'un code malveillant ou de traces réseau.

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

Prestataire de réponse aux incidents de sécurité – organisme ayant les compétences et les capacités pour réaliser des prestations d'investigation numérique d'incidents de sécurité touchant des systèmes d'information et définir des mesures de remédiation adaptées.

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

Référentiel – le présent document.

Responsable d'équipe d'analyse – personne responsable de la prestation en réponse aux incidents de sécurité et de la constitution de l'équipe d'analystes, en particulier de la complémentarité de leurs compétences. Il est chargé de définir, de proposer et de suivre une feuille de route, de coordonner, d'orienter et de contrôler les activités d'analyse associées, ainsi que d'assurer la capitalisation des résultats. Il doit également définir une posture et proposer des mesures de remédiation adaptées.

Sécurité d'un système d'information – ensemble des moyens techniques et non techniques de protection, permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles.

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

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

II. Activités visées par le référentiel

Ce chapitre présente les différentes activités traitées dans le Référentiel.

II.1. Pilotage technique

Le pilotage technique couvre la définition, le pilotage et le contrôle des activités techniques nécessaires au traitement d'un incident de sécurité. Cette activité est assurée par le responsable de l'équipe d'analyse.

II.2. Analyse système

L'analyse système consiste à collecter des informations techniques sur des équipements (terminaux utilisateur, serveurs, périphériques, etc.) ou à l'échelle d'un système d'information puis à les analyser en vue notamment d'identifier le périmètre de la compromission et le mode opératoire de l'attaquant puis enfin à préconiser des mesures de remédiation pour limiter la compromission, enrayer l'activité de l'attaquant et durcir la sécurité du système d'information de la victime.

II.3. Analyse réseau

L'analyse réseau consiste à collecter des évènements réseau à partir de systèmes de journalisation, de supervision et de détection des incidents de sécurité, existants ou de circonstance, puis à les analyser en vue notamment d'identifier le périmètre de la compromission et le mode opératoire de l'attaquant puis enfin à préconiser des mesures de remédiation pour limiter la compromission, enrayer l'activité de l'attaquant et durcir la sécurité du système d'information de la victime.

II.4. Analyse de codes malveillants

L'analyse de codes malveillants consiste à identifier et analyser les codes malveillants pour comprendre leurs comportements, en extraire des indicateurs de compromission[1] et proposer des mesures de remédiation.

[1] Voir glossaire.

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.

Les exigences doivent être respectées par les prestataires dans le but d'obtenir la qualification. Les recommandations sont données à titre de bonnes pratiques et ne font pas l'objet d'une quelconque vérification en vue de la qualification.

La qualification est réalisée conformément à [PROCESS_QUALIF_PSCO] et permet d'attester de la conformité du prestataire aux exigences du Référentiel.

Les exigences du chapitre IV relatives au prestataire sont vérifiées lors d'un audit du siège[2] du prestataire.

Les exigences du chapitre V relatives aux analystes sont vérifiées lors d'évaluations individuelles des analystes. La qualification est notamment accordée au regard des compétences des analystes qui réaliseront les prestations, définies en Annexe 1.

Les exigences VI relatives au déroulement de la prestation sont vérifiées lors des observations sur site. Le respect des missions est par ailleurs évalué conformément à l'Annexe 1.

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

Un prestataire peut demander la qualification :

Portée 1. pour toutes les activités définies au chapitre II ;

Portée 2. pour les activités de pilotage technique, d'analyse système et d'analyse réseau ;

Portée 3. pour seulement l'activité d'analyse de codes malveillants décrite au chapitre II.4.

Seuls les prestataires qualifiés pour les portées 1 et 2 peuvent répondre à une demande de prestation de réponse aux incidents de sécurité qualifiée. Ils doivent s'appuyer sur un autre prestataire qualifié s'ils ne disposent pas des ressources suffisantes ou des compétences pour réaliser l'intégralité de la prestation.

Les prestataires qualifiés pour la portée 3 ne peuvent intervenir qu'au titre de sous-traitant d'un prestataire qualifié pour les portées 1 ou 2.

Est considérée comme une prestation qualifiée au sens du Référentiel, une prestation respectant la démarche décrite au chapitre VI, dont les activités sont réalisées par un ou plusieurs analystes évalués individuellement et reconnus compétents pour ces activités, conformément au chapitre V et à l'Annexe 1 et travaillant pour un prestataire qualifié pour ces mêmes activités.

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.

[2] Le siège correspond au lieu de travail habituel des analystes. Il peut s'agir du siège social ou d'établissements externes.

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 toutes ses activités de réponse aux incidents de sécurité.

b) Le prestataire doit décrire l'organisation de son activité de réponse aux incidents au bénéfice du commanditaire.

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

d) Le prestataire doit respecter la législation en vigueur sur le territoire français.

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

f) Le prestataire doit assumer la responsabilité de la prestation qu'il réalise pour le compte du commanditaire et, en particulier, des dommages éventuellement causés au cours des activités de réponse aux incidents de sécurité.

   Le prestataire et le commanditaire peuvent préciser les modalités de partage des responsabilités au sein de la convention. Le prestataire peut s'exonérer de tout ou partie de sa responsabilité s'il est avéré que le dommage éventuellement subi par le commanditaire résulte d'un défaut d'information de ce dernier.

   Il est recommandé que le prestataire garde, notamment, la responsabilité des actions qu'il effectue lors de la prestation de son propre fait.

g) Le prestataire doit apporter les éléments concourant à la preuve qu'il a évalué les risques résultant de ses activités de réponse aux incidents de sécurité et qu'il a pris des dispositions appropriées pour couvrir ces risques. Il doit mettre à disposition du commanditaire ces éléments de preuve.

h) Il est recommandé que le prestataire souscrive une assurance professionnelle couvrant les dommages éventuellement causés aux systèmes d'information de la victime.

i) Le prestataire doit s'assurer du consentement du commanditaire avant toute communication vers un tiers d'informations relatives aux prestations de réponse aux incidents de sécurité, que ces informations soient obtenues lors de la prestation ou non.

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

k) Le prestataire doit s'engager à ce que la prestation soit réalisée en toute impartialité.

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

m) Le prestataire doit réaliser la prestation de manière loyale, en toute bonne foi et dans le respect du commanditaire, de son personnel et de ses infrastructures.

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

n) Le prestataire doit informer la victime lorsque cette dernière est tenue de déclarer l'incident de sécurité à une instance gouvernementale et doit l'accompagner dans cette démarche si cette dernière en fait la demande.

IV.2. Charte d'éthique

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

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

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

c) Les analystes doivent signer la charte d'éthique préalablement à la réalisation d'une prestation.

IV.3. Gestion des ressources et des compétences

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

Des analystes débutants peuvent, au titre de leur formation et de leur montée en compétence, être incorporés à l'équipe d'analystes. Ils doivent cependant respecter la charte d'éthique du prestataire ainsi que l'ensemble des obligations contractuelles, réglementaires ou légales imposées aux analystes. Les analystes débutants doivent être intégrés à l'équipe au titre d'observateur. Le commanditaire doit en être tenu informé et donner son accord.

b) Le prestataire doit s'assurer du maintien à jour des compétences des analystes dans les activités pour lesquelles ils ont obtenu une attestation individuelle de compétence[2]. Pour cela, le prestataire doit disposer d'un processus de formation continue et permettre à ses analystes d'assurer une veille technologique.

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

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

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

[5] Voir [PROCESS_QUALIF_PSCO].

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

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

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

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

h) Le prestataire doit sensibiliser les analystes à la législation en vigueur sur le territoire français applicable à leurs missions.

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

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

IV.4. Protection de l'information

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

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

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

d) 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 *a minima* un cloisonnement logique strict et une journalisation des évènements réseau. Il est recommandé de mettre en œuvre un cloisonnement physique.

V. Exigences relatives aux analystes

V.1. Aptitudes générales

a) Le responsable d'équipe d'analyse doit posséder les qualités personnelles identifiées au chapitre 7.2.3.4 de la norme [ISO19011].

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

c) Le responsable d'équipe d'analyse doit maîtriser la législation en vigueur sur le territoire français et applicable à ses missions ainsi qu'à celles des analystes.

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

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

f) L'analyste doit mettre régulièrement à jour ses compétences par une veille active sur la méthodologie, les techniques et les outils utilisés dans le cadre de ses missions.

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

V.2. Expérience

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

b) Il est recommandé que l'analyste justifie :

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

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

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

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

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

d) L'analyste doit assurer les missions selon son profil, telles que définies dans l'Annexe 1.

e) L'analyste doit disposer des compétences requises par son profil, telles que définies dans l'Annexe 1.

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

V.4. Engagements

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

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

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

Les exigences relatives au déroulement d'une prestation de réponse aux incidents de sécurité sont réparties selon les étapes suivantes :

- étape 1 : qualification préalable d'aptitude à la réalisation de la prestation ;
- étape 2 : établissement d'une convention ;
- étape 3 : compréhension de l'incident de sécurité et de l'environnement ;
- étape 4 : élaboration d'une posture initiale ;
- étape 5 : préparation de la prestation ;
- étape 6 : exécution de la prestation ;
- étape 7 : restitutions ;
- étape 8 : élaboration du rapport d'analyse ;
- étape 9 : clôture de la prestation.

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) Le responsable d'équipe d'analyse doit sensibiliser la victime sur l'intérêt d'utiliser des moyens de communication sécurisés et dédiés avec le prestataire, dans tous les cas déconnectés du système d'information compromis, afin de ne pas permettre à l'attaquant de suivre les opérations en cours (voir Annexe 2, paragraphe l).

b) Le prestataire doit signer un accord de non-divulgation avec la victime afin d'assurer la confidentialité des informations que cette dernière lui transmet en l'absence de convention signée (voir chapitre VI.2).

c) Le prestataire doit demander à la victime de lui fournir les informations de contexte sur l'incident de sécurité et notamment celles identifiées dans l'Annexe 3.

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

e) Le prestataire doit informer la victime des résultats de la qualification préalable d'aptitude à la réalisation de la prestation. Il doit notamment indiquer sa capacité à répondre totalement, partiellement ou non à la prestation. Le cas échéant, il doit indiquer les activités envisagées et les ressources associées.

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

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

a) Une convention doit être établie entre le prestataire et le commanditaire avant l'exécution de la prestation.

VI.2.1. Modalités de la prestation

La convention établie entre le prestataire et le commanditaire doit :

a) décrire le périmètre initial de la prestation, la démarche générale, les activités et les modalités de la prestation (objectifs, jalons, livrables attendus en entrée, prérequis, etc.) ;

b) préciser les livrables attendus en sortie, les réunions de clôture, les publics destinataires, leur niveau de sensibilité et les modalités associées ;

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

d) prévoir une traçabilité entre le commanditaire et le prestataire des informations et supports matériels remis pour analyse ;

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

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

VI.2.2. Organisation

La convention établie entre le prestataire et le commanditaire doit :

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

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

c) stipuler que le prestataire doit, le cas échéant, collaborer avec des prestataires tiers qui travaillent pour le compte de la victime et qui auront été spécifiquement désignés par le commanditaire ;

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

VI.2.3. Responsabilités

La convention établie entre le prestataire et le commanditaire doit prévoir que :

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

b) le commanditaire autorise provisoirement le prestataire, aux seules fins de réaliser la prestation, d'accéder et de se maintenir dans tout ou partie du périmètre et d'effectuer des traitements sur les données hébergées, quelle que soit la nature de ces données ;

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

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

e) le commanditaire garantit disposer de l'ensemble des droits sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.) ou d'avoir recueilli l'accord des éventuels tiers, et notamment de ses prestataires ou de ses partenaires, dont les systèmes d'information entreraient dans le périmètre ;

f) le commanditaire remplit toutes les obligations légales nécessaires à la collecte et à l'analyse des données.

La convention établie entre le prestataire et le commanditaire doit préciser :

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

h) si le prestataire dispose d'une assurance couvrant les dommages éventuellement causés lors de la réalisation des activités d'analyse et, le cas échéant, la surface de couverture de celle-ci et l'attestation d'assurance.

VI.2.4. Confidentialité

La convention établie entre le prestataire et le commanditaire doit prévoir :

a) un engagement du prestataire à ne collecter et à n'analyser que les informations strictement nécessaires au bon déroulement de la prestation ;

b) la non-divulgation à un tiers par le prestataire de toute information, même décontextualisée, relative à la prestation (informations et supports matériels collectés, livrables, etc.), sauf autorisation formelle et écrite du commanditaire et du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques[7] (CERT-FR) ;

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

d) que le prestataire puisse, sauf refus formel et écrit du commanditaire, conserver certains types d'informations liées à la prestation une fois celle-ci terminée. Le prestataire devra identifier ces types d'informations dans la convention (ex : codes malveillants, scénarios d'attaque, indicateurs de compromission, etc.). Le prestataire doit s'engager à anonymiser et à décontextualiser ces informations (suppression de toute information permettant d'identifier la victime, de toute information à caractère personnel, etc.) ;

e) que le prestataire, sauf refus formel et écrit du commanditaire, transmette au centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques[7] (CERT-FR) ces éléments anonymisés et décontextualisés, ainsi que leur niveau sensibilité et leurs conditions d'utilisation.

VI.2.5. Juridique

La convention établie entre le prestataire et le commanditaire doit :

a) préciser les clauses relatives à l'éthique du prestataire et inclure la charte d'éthique (voir chapitre IV.2) ;

b) préciser les exigences en matière de respect de la législation nationale applicable, notamment :

- le secret professionnel [CP_ART_226-13], sans préjudice de l'application de l'article 40 alinéa 2 du Code de procédure pénale relatif au signalement à une autorité judiciaire,
- l'abus de confiance [CP_ART_314-1],

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

- le secret des correspondances privées [CP_ART_226-15],
- l'atteinte à la vie privée [CP_ART_226-1],
- l'accès ou le maintien frauduleux à un système d'information [CP_ART_323-1] ;

c) préciser les exigences spécifiques au contexte juridique du secteur d'activité de la victime ;

d) prévoir le cas échéant les exigences à respecter par le prestataire dans le cadre d'une affaire judiciaire, civile ou arbitrale.

VI.2.6. Sous-traitance

a) La convention établie entre le prestataire et le commanditaire doit 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 :
   - il existe une convention ou un cadre contractuel documenté entre le prestataire et son sous-traitant ;
   - le recours à la sous-traitance est connu et formellement accepté par écrit par le commanditaire.

VI.2.7. Livrables

a) La convention établie entre le prestataire et le commanditaire doit préciser que tous les documents produits par le prestataire au titre de la prestation sont au moins fournis en langue française.

VI.2.8. Qualification

La convention établie entre le prestataire et le commanditaire doit :

a) indiquer que la prestation réalisée est une prestation qualifiée et inclure l'attestation de qualification[8] du prestataire ;

b) indiquer que les analystes disposent d'une attestation individuelle de compétence[8] pour les activités d'analyse et inclure ces attestations.

VI.3. Étape 3 – Compréhension de l'incident de sécurité et de l'environnement

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

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

VI.3.1. Compréhension de l'incident de sécurité

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

[8] Voir [PROCESS_QUALIF_PSCO].

VI.3.2. Compréhension de l'environnement

a) Le prestataire doit adopter une vision globale du système d'information concerné. Il doit ainsi demander à la victime des compléments de cartographie par rapport à ceux déjà transmis en phase de qualification préalable d'aptitude à la réalisation de la prestation (voir chapitre VI.1, Annexe 3).

b) Le prestataire doit définir et mettre en œuvre une démarche de compréhension du système d'information compromis pour mettre en évidence les éventuels écarts entre la cartographie fournie par la victime et l'architecture réellement mise en place.

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

d) Le prestataire doit demander à la victime de l'informer des spécificités et des contraintes du système d'information ;

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

VI.4. Élaboration de la posture initiale

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

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

  En cas de présence de l'attaquant sur le système, si aucun moyen ne permet de remédier rapidement et durablement à la compromission, il est recommandé que le prestataire adopte une démarche la plus discrète possible vis-à-vis de l'attaquant afin d'éviter d'éveiller ses soupçons et de l'amener à changer son mode opératoire au profit d'un mode plus furtif.
- la démarche générale et ses grandes étapes, en considération des spécificités et contraintes du système d'information ;
- les activités à réaliser, les informations à collecter, le nombre d'analystes à engager et le calendrier associé[9].

b) Le prestataire doit adapter sa posture en fonction de la compréhension de l'incident de sécurité et de l'environnement.

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

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

d) Le prestataire doit soumettre pour accord la posture initiale à la victime. La décision finale et la responsabilité de la posture initiale appartiennent à la victime.

VI.5. Étape 4 - Préparation de la prestation

VI.5.1. Mise en place de l'organisation

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

b) Le responsable d'équipe d'analyse doit sensibiliser la victime sur l'intérêt de désigner en son sein un référent chargé des relations entre le prestataire et la victime (voir Annexe 2, paragraphe a).

c) Le responsable d'équipe d'analyse doit identifier et si besoin définir les circuits de communication et de décision à respecter avec le commanditaire (voir Annexe 2, paragraphe d). Il doit également obtenir du commanditaire la liste des points de contact nécessaires à la réalisation de la prestation.

d) Le responsable d'équipe d'analyse doit sensibiliser la victime 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 2, paragraphe d). Cette structure peut être rattachée à une cellule de crise déjà existante.

e) Le responsable d'équipe d'analyse doit réaliser des points de synchronisation réguliers, de niveaux techniques ou stratégiques selon le besoin, avec le commanditaire et la victime.

f) Le responsable d'équipe d'analyse doit sensibiliser la victime sur l'intérêt d'élaborer un plan de communication relatif à l'incident de sécurité (voir Annexe 2, paragraphe f).

g) Le responsable d'équipe d'analyse doit sensibiliser la victime sur l'intérêt de l'informer tout au long de la prestation des actions qu'elle réalise sur le système d'information et qui pourraient impacter la prestation (voir Annexe 2, paragraphe i).

VI.5.2. Mise en place des moyens opérationnels

VI.5.2.1. Gestion des ressources

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

b) Le responsable d'équipe d'analyse doit s'assurer que les analystes disposent d'une attestation individuelle de compétence[10] pour les activités qu'ils mènent.

Il peut, s'il dispose des compétences suffisantes et d'une attestation individuelle[7] de compétence, réaliser la prestation de réponse aux incidents de sécurité lui-même et seul.

Il peut incorporer à l'équipe d'analystes des analystes débutants, au titre de leur formation et de leur montée en compétence, en tant qu'observateurs, sous réserve du respect des obligations décrites au paragraphe IV.3 a).

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

c) Le responsable d'équipe d'analyse doit constituer une équipe d'analystes dont le nombre et les compétences sont adaptés à la posture.

[10] Voir [PROCESS_QUALIF_PSCO].

d) Le responsable d'équipe d'analyse doit réévaluer régulièrement le profil et le nombre des analystes afin de s'assurer que l'engagement reste adapté à la prestation, la complexité de l'incident pouvant s'avérer en cours de prestation plus élevée que prévue dans la posture initiale (voir chapitre VI.6.2).

e) Le prestataire doit obtenir les privilèges nécessaires et suffisants pour réaliser les opérations de collecte, en respectant la politique de gestion des droits de la victime. Les comptes doivent être dédiés, nominatifs. Le prestataire doit s'assurer que l'activité de ce compte est strictement conforme à celle attendue.

VI.5.2.2. Gestion des moyens logistiques et informatiques

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

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

b) Le responsable d'équipe d'analyse doit mettre en place, tenir à jour et partager avec la victime un registre centralisé recensant pour chaque information et support collecté et analysé :

- 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 et le support de stockage associé ;
- le propriétaire légal de l'information ou du support;
- le niveau de sensibilité de l'information et du support associé.

c) Le responsable d'équipe d'analyse doit, en collaboration avec la victime, 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 responsable d'équipe d'analyse doit sensibiliser la victime sur l'intérêt de lui mettre à disposition un environnement de travail et notamment une zone sécurisée dédiée au stockage et à l'analyse des informations collectées et respectant les exigences réglementaires associées au niveau de sensibilité de ces données (voir Annexe 2, paragraphe i). Cet environnement de travail doit être cloisonné du système d'information de la victime sur lequel des investigations sont en cours.

e) Le responsable d'équipe d'analyse doit sensibiliser la victime sur l'intérêt de lui mettre à disposition un environnement d'analyse sécurisé et déconnecté du système d'information compromis (voir Annexe 2, paragraphe k).

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

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

a) Le responsable d'équipe d'analyse doit sensibiliser la victime 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 2, paragraphe c).

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

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

b) Il est recommandé que le prestataire et la victime soient en mesure de déclencher les procédures d'urgence en heures non ouvrées.

VI.6. Étape 5 - Exécution de la prestation

a) Le responsable d'équipe d'analyse doit définir une démarche de réponse adaptée à l'étendue et à la complexité de l'incident de sécurité. Cette démarche doit donc s'appuyer sur un processus itératif d'adaptation constante de la posture initiale (voir chapitre VI.4).

b) La démarche doit comprendre au moins les étapes suivantes :

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

c) Pour chacune des étapes, les missions définies par domaine de compétences doivent être respectées (voir Annexe 1).

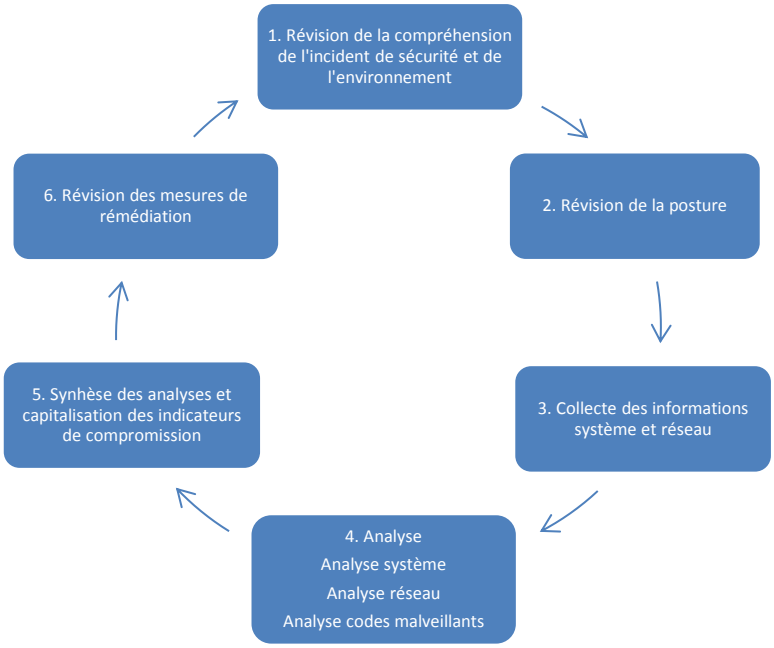

Figure 1: Étapes de l'exécution des prestations de réponse aux incidents de sécurité

VI.6.1. Révision de la compréhension de l'incident de sécurité et de l'environnement

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

- la date de compromission initiale ;
- la chronologie générale des activités de l'attaquant, en précisant les différentes phases (reconnaissance, infiltration initiale, interaction avec le contrôle commande, élévation de privilèges et déplacements latéraux, exfiltration, etc.) ;
- le périmètre précis de la compromission :
    - niveau de privilège obtenu par l'attaquant,
    - liste des machines compromises, comptes et domaines d'administration usurpés, etc.,
    - vecteur initial de compromission, vulnérabilités exploitées et outils utilisés,
    - modifications internes sur le SI (ACL, fichiers, etc.) ;
- les moyens de déplacement latéral :
    - vulnérabilités exploitées et outils utilisés,
    - techniques utilisées pour l'escalade de privilège sur le SI ;
- les moyens de communication utilisés par l'attaquant depuis l'extérieur,
    - moyens utilisés pour récupérer / collecter les données à exfiltrer,
    - moyens de persistance éventuels pour se maintenir sur le système,
    - moyens utilisés pour exécuter des commandes à distance sur des ressources internes,
    - liste des équipements correspondants ;
- la liste des indicateurs de compromission ;
- les impacts métier pour la victime et le commanditaire :
    - risques associés à la compromission (ex. : exfiltration, destruction, etc.),

- nature des éléments compromis, systèmes piégés ou détruits,
- nature des données exfiltrées et champs d'intérêt,
- etc.

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

c) Le prestataire doit présenter régulièrement au commanditaire une synthèse de la compréhension de l'incident de sécurité afin de :

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

VI.6.2. Révision de la posture

a) Le responsable d'équipe d'analyse doit réviser la posture à chaque nouvelle itération afin d'orienter les analyses, d'identifier les analyses à débuter, à poursuivre et à clôturer.

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

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

VI.6.3. Collecte des informations

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

a) La collecte des informations doit suivre une méthode dont les actions sont préalablement identifiées et dont la démarche est reproductible.

b) Les analystes doivent réaliser la collecte des informations conformément à la posture définie (voir chapitre VI.6.2) et peuvent notamment réaliser les opérations suivantes :

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

c) Les analystes doivent collecter les informations permettant de rechercher les indicateurs de compromission de l'incident capitalisés lors de la compréhension de l'incident de sécurité (voir chapitre VI.6.1) afin d'identifier l'étendue de la compromission.

d) Le prestataire doit adapter la méthode de collecte à la posture préalablement convenue entre le prestataire et le commanditaire (voir chapitre VI.6.2).

e) Le prestataire doit obtenir les privilèges nécessaires et suffisants pour réaliser les opérations de collecte, en respectant la politique de gestion des droits de la victime. Les comptes doivent être dédiés et démarqués.

f) Les analystes ne doivent collecter que les informations strictement nécessaires au bon déroulement de la prestation conformément à la convention.

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

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

i) Les analystes doivent tenir à jour le registre centralisé associé aux opérations réalisées sur le système d'information, conformément à l'organisation fixée en phase de préparation (voir chapitre VI.5.2.2, paragraphe a).

j) Les analystes doivent tenir à jour le registre centralisé associé aux opérations de collecte des informations et supports conformément à l'organisation fixée en phase de préparation (voir chapitre VI.5.2.2, paragraphe b).

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

l) Les analystes doivent assurer la préservation et la non-altération de tous les éléments récoltés au titre de l'investigation

m) Les analystes doivent définir et mettre en place des moyens adaptés aux contraintes de la victime et assurant la collecte et le formatage de volumes importants d'informations à l'échelle d'un système d'information.

VI.6.3.1. Collecte d'informations techniques

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

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

b) Les analystes doivent être en mesure de collecter des informations techniques portant notamment sur :

- les configurations des systèmes ;
- les entrées des systèmes de fichiers ;
- les systèmes en exécution.

VI.6.3.2. 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 compromis :
    - 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, etc.).

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

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

d) Il est recommandé que le prestataire complète la supervision de circonstance par des sondes de détection d'intrusion.

VI.6.3.3. Copie physique

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

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

VI.6.3.4. Capture de flux

a) Les analystes peuvent capturer les flux afin d'analyser le protocole de communication entre une ressource compromise et un serveur de commande et de contrôle.

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

VI.6.4. Analyse des informations collectées

a) Les analystes doivent analyser les informations collectées dans l'objectif d'améliorer la compréhension de l'incident de sécurité (voir chapitre VI.6.1).

VI.6.4.1. Analyse des informations collectées sur le système d'information

a) Les opérations d'analyses doivent s'appuyer sur une méthodologie reproductible entre analystes.

b) 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.).

c) Le prestataire doit analyser les éléments collectés (voir chapitre VI.6.3) en recherchant ;
- 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 ;

- 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 sur le système d'information.

d) Les opérations de recherches d'indicateurs de compromission issus d'une base de connaissances du prestataire doivent être réalisées sur un système d'information ayant un niveau de protection adapté au niveau de sensibilité des indicateurs de compromission. En particulier, le système doit être distinct du réseau de la victime (cf. chapitre VI.5.2.2 paragraphe d).

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

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

g) Le responsable d'équipe d'analyse doit informer sans attendre le commanditaire des constats pouvant manifestement présenter un intérêt majeur pour la protection de la victime : exfiltration en cours de données, sabotage, etc.

VI.6.4.2. Analyse de programmes malveillants

a) Les missions à assurer en matière d'analyse de programmes malveillants sont spécifiées en Annexe 1.

b) L'analyste doit réaliser les analyses de codes malveillants nécessaires, pouvant nécessiter :
- une analyse du code sur une base hors ligne de plusieurs antivirus du marché ;
- une analyse dynamique du comportement du code malveillant ;
- une rétro-conception du code et de ses composants.

c) Les objectifs poursuivis pour ces opérations d'analyse de code doivent demeurer en adéquation avec la réalisation de la mission.

VI.6.4.3. Supervision de circonstance

a) 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 et, le cas échéant, de suivre aussi précisément que possible ses actions, ses déplacements voire ses changements de comportement.

VI.6.4.4. Recherches en sources ouvertes

Le prestataire peut être amené à réaliser des recherches en sources ouvertes, sur Internet notamment, à partir 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) 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 (voir VI.4.a), les types d'informations pouvant être recherchés et les modalités associées.

b) Le prestataire doit notamment horodater les recherches réalisées et les résultats collectés.

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

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

VI.6.5. Synthèse des analyses, capitalisation et diffusion

a) Le responsable d'équipe d'analyse doit :

- regrouper et synthétiser les résultats des analyses ;
- 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 ;
- 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).

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

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

VI.6.6. Révision des mesures de remédiation

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

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

b) Le responsable d'équipe d'analyse doit identifier dans le plan de remédiation les éventuels effets de bord associés à chacune des mesures de remédiation.

c) Le prestataire doit soumettre pour accord le plan de remédiation à la victime. La décision finale et la responsabilité du plan de remédiation appartiennent à la victime.

VI.6.6.1. Mesures de durcissement

a) Le prestataire doit définir des mesures de durcissement à appliquer avant l'assainissement du système d'information.

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

c) Le prestataire doit adopter une stratégie de défense en profondeur et définir des mesures de durcissement applicables à différents niveaux du système d'information (postes de travail, serveurs,

relais, équipements réseau, équipements de sécurité, etc.). En particulier, les mesures de durcissement proposées par le prestataire doivent permettre :

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

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

À titre d'exemple, si le niveau de discrétion recherché vis-à-vis de l'attaquant est élevé ou moyen :

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

e) Le prestataire doit recommander à la victime de recourir à un prestataire de détection des incidents de sécurité qualifié. Il doit lui transmettre le lien vers le catalogue des prestataires de détection des incidents de sécurité qualifiés[11].

f) Le prestataire doit définir des mesures de durcissement à appliquer après l'assainissement du système d'information, afin de permettre à plus long terme de :

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

VI.6.6.2. Mesures d'assainissement

a) Le prestataire doit définir des mesures permettant d'empêcher tout accès de l'attaquant au système d'information pendant l'application des mesures d'assainissement.

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

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

Le prestataire doit définir des mesures d'assainissement prévoyant notamment la réinstallation intégrale du cœur de confiance du système d'information, sur une échelle de temps réduite, par exemple sur un week-end, et en une seule fois.

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

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

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

VI.7. Étape 6 - Restitutions

a) Le responsable d'équipe d'analyse doit présenter à la victime 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 ;
   - les mesures de remédiation proposées (voir chapitre VI.6.6).

b) Le responsable d'équipe d'analyse doit assurer une restitution :
   - quotidiennement, au référent désigné par la victime (voir Annexe 2, paragraphe a) ;
   - à chaque révision de la posture ;
   - à l'issue de la prestation, sans attendre que le rapport d'analyse soit achevé ;
   - à la clôture de la prestation, à la suite de la livraison du rapport d'analyse.

VI.8. Étape 7 - 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 que la prestation réalisée est une prestation qualifiée et préciser les activités d'analyse (voir chapitre II) associées.

c) Le prestataire doit élaborer un rapport d'analyse présentant notamment :
   - une synthèse, compréhensible par des non-experts, qui précise :
     - le rappel du contexte l'incident,
     - le périmètre concerné par l'attaque et le périmètre compromis,
     - les actions réalisées par l'attaquant ayant un impact fort pour la victime (ex. : exfiltration de données, etc.),
     - les mesures prises par la victime pour remédier à l'incident,
     - les étapes clés du mode opératoire de l'attaquant et la chronologie associée ;
   - un ou plusieurs schémas récapitulatifs de l'attaque :
     - désignation des systèmes compromis,
     - horodatage des événements ;
   - la description des analyses réalisées (cf. chapitre VI.6.1) :
     - 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,
     - le vecteur initial de compromission ;
   - la liste exhaustive des ressources et comptes compromis ;

- les indicateurs de compromission ;
- les mesures de remédiation, leur périmètre et leur séquencement de mise en œuvre.

d) 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 de la victime, etc.) ainsi que les sources d'information qui ont fait défaut (ex. : absence de journalisation sur un serveur particulier, etc.) pour compléter les analyses et consolider une chronologie exhaustive de toutes les actions de l'attaquant.

VI.9. Étape 8 - Clôture de la prestation

a) Le responsable d'équipe d'analyse doit organiser une réunion de clôture avec la victime suite à la livraison du rapport d'analyse, conformément au chapitre VI.7.

b) Le responsable d'équipe d'analyse doit demander à la victime de lui attester formellement et par écrit que le rapport d'analyse est conforme aux objectifs visés dans la convention.

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

d) Le responsable d'équipe d'analyse doit transmettre au commanditaire un procès-verbal de destruction ou de restitution, selon ce qui a été prévu dans la convention établie entre le prestataire et la victime. 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.

VI.10. Cas des enquêtes judiciaires

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

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

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

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

VII. Références documentaires

VII.1. Textes légaux

Renvoi	Document
[CP_ART_314-1]	Article 334-1 du Code pénal relatif à l'abus de confiance.
[CP_ART_226-1]	Article 226-1 du Code pénal relatif à l'atteinte à la vie privée.
[CP_ART_226-13]	Article 226-13 du Code pénal relatif au secret professionnel.
[CP_ART_226-15]	Article 226-15 du Code pénal relatif au secret des correspondances.
[CP_ART_323-1]	Article 323-1 du Code pénal relatif à l'accès ou au maintien frauduleux dans un système de traitement automatisé de données.
[LOI_IL]	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

VII.2. Normes et documents techniques

Renvoi	Document
[ISO19011]	Norme internationale ISO/IEC 19011 :2011: Lignes directrices pour l'audit des systèmes de management.
[ISO27035]	Norme internationale ISO/IEC 27035 :2011 : Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information.
[ISO27037]	Norme internationale ISO/IEC 27037 :2012 : Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques.
[NT_JOURNAL]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, note technique n° DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013, ANSSI. Disponible sur http://www.ssi.gouv.fr.
[HYGIENE]	Guide d'hygiène informatique – version en vigueur. Disponible sur http://www.ssi.gouv.fr.

VII.3. Autres références documentaires

Renvoi	Document
[PROCESS_QUALIF_PSCO]	Processus de qualification des prestataires de services de confiance – version en vigueur.

Annexe 1 Missions et compétences attendues pour chacun des domaines métier d'un prestataire de réponse aux incidents de sécurité

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

I. Responsable d'équipe d'analyse

I.1. Missions à assurer

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

- mettre en œuvre une organisation adaptée aux objectifs de la prestation (voir chapitre VI.5.1) ;
- structurer l'équipe d'analystes (compétences, effectif) ;
- assurer la définition, le pilotage et le contrôle des activités des analystes ;
- mettre en œuvre les moyens adaptés aux objectifs de la prestation (voir chapitre VI.5.2) ;
- définir et gérer les priorités, en particulier en situation de crise ;
- définir une démarche permettant de comprendre :
    - 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 la victime 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 ;
- assurer et contrôler la synthèse des analyses, la capitalisation et la diffusion (voir chapitre VI.6.5) ;
- contrôler la qualité des productions.

I.2. Compétences requises

Le responsable d'équipe 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*, C&C, 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 messageries, etc. ;
- les outils d'analyse : analyse de systèmes (mémoire, disques), analyse de journaux (système, applicatif ou réseau), analyse statique et dynamique de programmes et documents, etc.

Il doit par ailleurs 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 non technique ;
- savoir rédiger des documentations adaptées à différents niveaux d'interlocuteurs.

II. Analyste système

II.1.Missions à assurer

L'analyste système doit assurer les missions suivantes :

- adopter une vision globale du système d'information afin d'identifier :
    - les vulnérabilités système exploitables et les chemins d'attaque associés,
    - les points d'extrémité nécessitant une collecte de données (serveurs d'infrastructure, poste d'administration et postes utilisateur, serveurs métier, etc.) ;
- recueillir à l'échelle du système d'information un volume important d'informations techniques (système de fichiers, configuration, journaux système et applicatifs, etc.) d'un large ensemble de systèmes informatiques et en assurer l'analyse ;
- réaliser 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 la victime à la définition d'une politique de journalisation système (types d'événements, durées de rétention, etc.) par type d'équipement et au développement de règles de corrélation d'événements système ;
- soutenir la victime à 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 et l'étendue de la compromission ;
- 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 de la victime ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'analyse.

II.2.Compétences requises

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, etc. ;
- les attaques et activités malveillantes : exploitation de vulnérabilités, portes dérobées, *rootkit*, *botnet*, C&C, etc. ;
- les outils d'analyse : analyses statique et dynamique de programmes, analyse de systèmes de fichiers, analyse de journaux (système, applicatif ou réseau), etc. ;
- les journaux d'événements système, réseau et applicatifs ;
- 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 non technique ;
- savoir rédiger des rapports et des documentations ;
- savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

III. Analyste réseau

III.1. Missions à assurer

L'analyste réseau doit assurer les missions suivantes :

- adopter une vision globale du système et de son architecture, identifier les points potentiels d'infiltration/exfiltration et les points de collecte associés (composants réseau, produits de sécurité, etc.) ;
- soutenir la victime à 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 la victime à 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.) et au développement de règles de corrélation d'événements système ;
- soutenir la victime à 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 ;
- 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 de la victime ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'analyse.

III.2. Compétences requises

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) ;
- le fonctionnement de sondes de détection d'intrusions et d'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 non technique ;
- savoir rédiger des rapports et des documentations ;
- 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 VII.

IV. Analyste de codes malveillants

IV.1. Missions à assurer

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

- les caractéristiques du code malveillant (empreinte cryptographique, taille du code malveillant, 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, *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 du système de fichier, 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 ;

L'analyse 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, pouvant notamment prendre en compte :

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

IV.2. Compétences requises

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, 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 non technique ;
- savoir rédiger des rapports et des documentations ;
- savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

Annexe 2 Recommandations à l'intention des commanditaires

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

I. Avant la prestation

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 de ce référentiel.

c) Il est recommandé que le commanditaire demande au prestataire de lui transmettre son attestation de qualification. Cette attestation identifie notamment le périmètre de la qualification et la date de validité de la qualification.

d) 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.

e) Il est recommandé que le commanditaire vérifie que la convention établie entre lui et son prestataire mentionne explicitement que la prestation est qualifiée.

f) La qualification d'un prestataire n'atteste pas de sa capacité à accéder à des informations classifiées de défense et par conséquent ne se substitue pas à une habilitation de défense. Cependant, il est possible pour un commanditaire de faire intervenir un prestataire qualifié après s'être assuré que ce dernier dispose des habilitations défense adéquates.

g) Une prestation de réponse aux incidents de sécurité, 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.

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

i) 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.

II. Pendant la prestation

a) Il est recommandé que le commanditaire fournisse au prestataire, dès le début de la prestation, les éléments identifiés en Annexe 3.

b) Il est recommandé que le commanditaire désigne en son sein un référent 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 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 la victime 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[12]) en l'absence du titulaire du matériel ou sans son accord explicite.

h) Toutes les modifications effectuées sur le système d'information par la victime durant la prestation doivent être tracées afin de pouvoir identifier les actions illégitimes sur le réseau pendant la prestation.

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

k) Il est recommandé que le commanditaire mette à disposition du prestataire un environnement d'analyse sécurisé et déconnecté du système d'information compromis.

l) Il est recommandé que la victime 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.

III. Après la prestation

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

b) Il est recommandé que le commanditaire fasse appel à un prestataire d'audit en sécurité des systèmes d'information (PASSI) qualifié et lui transmettre le lien vers le catalogue des prestataires de détection des incidents de sécurité qualifiés[13] 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.

[12] *Bring Your Own Device*.

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

Le cas échéant, il est recommandé que le PASSI réalise sa prestation en collaboration étroite avec le prestataire de réponse aux incidents de sécurité.

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[14], si tel n'est pas déjà le cas.

d) Il est recommandé que la victime 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 reporting, qualification et arbitrage, traitement, amélioration continue).

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

Annexe 3 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 de la victime 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.

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

- 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) ;
    - dépendances et interconnexions du système d'information ;
- les spécificités et les contraintes du système d'information ainsi que la localisation géographique ;
- le système d'information :
    - systèmes d'exploitation (postes d'administration, poste utilisateur, 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) ;
- l'architecture des domaines d'administration et des liens entre les domaines ;
- la politique de journalisation, les moyens de supervision et de détection ;
- 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 traitement 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.