



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

Premier ministre

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

Prestataires de réponse aux incidents de sécurité

Référentiel d'exigences

Version 3.0 du 28 juillet 2024

TABLE DES MATIERES

- I. Introduction5**
- I.1. Présentation générale5
 - I.1.1. Contexte 5
 - I.1.2. Objet du document..... 5
 - I.1.3. Structure du document 6
- I.2. Identification du document6
- I.3. Acronymes et définitions6
 - I.3.1. Acronymes..... 6
 - I.3.2. Définitions 6
- II. Activités couvertes par le référentiel 10**
- II.1. Recherche d’indicateurs de compromission..... 10
- II.2. Investigation numérique 10
- II.3. Analyse de codes malveillants 11
- II.4. Pilotage et coordination des investigations 11
- III. Qualification des prestataires 12**
- III.1. Modalités de la qualification 12
- III.2. Niveaux de qualification 12
- III.3. Portée de la qualification 13
- III.4. Qualification pour les besoins de la sécurité nationale 13
- IV. Exigences applicables au prestataire 14**
- IV.1. Exigences générales..... 14
- IV.2. Gestion des personnels 14
- IV.3. Protection de l’information 15
- V. Exigences applicables aux personnels du prestataire..... 17**
- V.1. Connaissances et compétences générales..... 17
- V.2. Connaissances et compétences spécifiques..... 17
- V.3. Expérience..... 17
- V.4. Engagement 17
- VI. Exigences applicables à la prestation..... 18**
- VI.1. Étape 1 – Qualification préalable d’aptitude à la réalisation de la prestation 18
- VI.2. Étape 2 – Elaboration de la convention de service..... 18
 - VI.2.1. Qualification..... 18
 - VI.2.2. Modalités de la prestation..... 19
 - VI.2.3. Responsabilités 19
 - VI.2.4. Confidentialité..... 20
 - VI.2.5. Experts 20
 - VI.2.6. Sous-traitance 20

Prestataires de réponse aux incidents de sécurité – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	2/49

VI.2.7.	Note de cadrage.....	20
VI.3.	Étape 3 – Compréhension et posture initiale	21
VI.4.	Étape 4 – Préparation de la prestation.....	22
VI.4.1.	Constitution de l'équipe.....	22
VI.4.2.	Elaboration de la note de cadrage.....	22
VI.4.3.	Mesures de précaution particulières.....	23
VI.4.4.	Réunion d'ouverture	24
VI.5.	Étape 5 – Exécution de la prestation	24
VI.5.1.	Collecte.....	24
VI.5.1.1.	Préparation	24
VI.5.1.2.	Collecte d'informations techniques	25
VI.5.1.3.	Collecte de journaux d'évènements.....	25
VI.5.1.4.	Copie	26
VI.5.1.5.	Collecte de flux réseau	26
VI.5.2.	Analyse.....	26
VI.5.2.1.	Recherche d'indicateurs de compromission	26
VI.5.2.2.	Analyse système et réseau	27
VI.5.2.3.	Analyse de codes malveillants.....	27
VI.5.2.4.	Recherches en sources ouvertes.....	27
VI.5.3.	Pilotage et suivi des investigations	28
VI.5.4.	Soutien à l'endigement.....	29
VI.6.	Étape 6 – Restitution	29
VI.7.	Étape 7 – Élaboration du rapport.....	30
VI.7.1.	Qualification.....	30
VI.7.2.	Cadre.....	30
VI.7.3.	Synthèse managériale	30
VI.7.4.	Résultats	31
VI.7.5.	Annexes	32
VI.8.	Étape 8 – Clôture de la prestation	32
Annexe 1	Bibliographie	33
Annexe 2	Missions et compétences attendues du personnel du prestataire	35
I.	Connaissance de la réglementation.....	35
II.	Responsable d'équipe.....	35
II.1.	Missions.....	35
II.2.	Compétences.....	36
III.	Pilote d'investigation.....	36
III.1.	Missions.....	36
III.2.	Compétences.....	37
IV.	Analyste système	37
IV.1.	Missions.....	37
IV.2.	Compétences.....	38
V.	Analyste réseau	39
V.1.	Missions.....	39
V.2.	Compétences.....	39
VI.	Analyste de codes malveillants.....	40
VI.1.	Missions.....	40
VI.2.	Compétences.....	41

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	3/49

Annexe 3	Recommandations à l'attention des commanditaires.....	43
I.	Avant la prestation	43
II.	Pendant la prestation.....	46
III.	Après la prestation	47
Annexe 4	Prérequis à fournir par les commanditaires.....	48

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	4/49

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

Les systèmes d'information se transforment, s'ouvrent de plus en plus vers l'extérieur et font face à de nouvelles menaces. Malgré la mise en place de mesures de sécurité, le risque de compromission des systèmes d'information est réel.

Les prestataires de réponse aux incidents de sécurité (PRIS) peuvent être appelés lorsqu'un incident de sécurité est suspecté, c'est-à-dire lorsqu'une concordance de signaux permet de soupçonner une activité malveillante ou lorsqu'un incident de sécurité est avéré.

Les incidents de sécurité couverts par ce référentiel concernent les cyberattaques dont les sources peuvent être de nature : stratégique, systémique, hacktiviste ou isolée.

Les prestataires de réponse aux incidents de sécurité permettent de :

- rechercher les traces d'une éventuelle compromission ;
- confirmer l'origine malveillante d'un incident de sécurité ;
- comprendre l'incident de sécurité : date de compromission initiale, chronologie de la compromission, mode opératoire de l'attaquant, etc. ;
- caractériser l'attaquant : objectifs, potentiel d'attaque, menace associée, etc.
- identifier le périmètre de la compromission ;
- proposer des mesures d'endiguement destinées à circonscrire l'incident de sécurité.

Le rapport d'analyse élaboré par le prestataire de réponse aux incidents de sécurité peut être utilisé pour définir et mettre en œuvre un plan de remédiation.

I.1.2. Objet du document

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

Il a vocation à permettre la qualification d'un prestataire conformément aux modalités décrites au chapitre III.

Il permet au commanditaire d'une prestation de réponse aux incidents de disposer de garanties sur les compétences du prestataire et de ses personnels, sur la capacité du prestataire à réaliser une prestation conforme aux exigences du présent référentiel et à protéger les informations et supports sensibles auxquels il a accès au cours de la prestation.

Il peut également être utilisé à titre de bonnes pratiques en dehors de toutes exigences légales, réglementaires ou contractuelles.

Il ne se substitue ni à l'application de la législation et de la réglementation en vigueur notamment en matière de protection des informations sensibles (1) et classifiées (2) ni aux obligations des prestataires en leur qualité de professionnels notamment leur devoir de conseil vis-à-vis de leurs commanditaires.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	5/49

I.1.3. Structure du document

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

Le chapitre II décrit les activités couvertes par le présent référentiel.

Le chapitre III décrit les modalités de la qualification d'un prestataire.

Le chapitre IV décrit les exigences applicables au prestataire.

Le chapitre V décrit les exigences applicables aux personnels du prestataire.

Le chapitre VI décrit les exigences applicables à la prestation.

L'Annexe 1 présente la bibliographie.

L'Annexe 2 décrit les connaissances, compétences et missions des personnels du prestataire.

L'Annexe 3 fournit des recommandations à l'attention des commanditaires avant, pendant et après la prestation.

L'Annexe 4 décrit les prérequis recommandés à fournir par les commanditaires.

I.2. Identification du document

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

I.3. Acronymes et définitions

I.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont :

ANSSI	Agence nationale de la sécurité des systèmes d'information
PACS	Prestataire d'accompagnement et de conseil en sécurité
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PDIS	Prestataire de détection d'incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité

I.3.2. Définitions

Les définitions utilisées dans le présent référentiel sont les suivantes, elles s'appuient en partie sur les normes (3) (4) (5) (6) :

Analyste – personne physique réalisant une activité de recherche d'indicateurs de compromission, d'analyse système ou réseau, ou de codes malveillants.

Attestation individuelle de compétence – document délivré par un centre d'évaluation à l'issue d'examens écrits et oraux et attestant qu'un analyste ou un pilote dispose des connaissances et compétences attendues au titre du présent référentiel.

Bénéficiaire – personne morale dont le système d'information est l'objet de la prestation. Le bénéficiaire peut être ou non le commanditaire de la prestation.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	6/49

Commanditaire – personne morale faisant appel à un prestataire pour la réalisation d’une prestation qualifiée. Le commanditaire peut être ou non le bénéficiaire de la prestation.

Convention de service – accord écrit entre le commanditaire et le prestataire pour la réalisation de la prestation.

Endiguement – ensemble des actions destinées à contenir un incident de sécurité. Certaines des mesures d’endiguement peuvent perturber le fonctionnement habituel du système d’information et n’ont pas vocation à être prolongées au-delà de la résolution de l’incident.

Expert – personne physique à laquelle le prestataire peut faire appel pour réaliser une partie de la prestation lorsque des connaissances et compétences spécifiques, hors du périmètre des activités du référentiel et non détenues par les analystes ou pilotes, sont nécessaires pour la bonne exécution de la prestation. L’expert peut être un personnel interne ou externe au prestataire.

Incident de sécurité – un ou plusieurs événements de sécurité de l’information indésirables ou inattendus présentant une probabilité forte de compromettre les activités d’une organisation et/ou de menacer la sécurité de l’information.

Indicateur de compromission – combinaison d’informations techniques et contextuelles représentatives d’une compromission ou d’une tentative de compromission, dont la présence peut être identifiée à partir d’analyses système et/ou réseau ou de codes malveillants.

Infrastructure de commande et de contrôle – ensemble des outils et canaux de communication entre l’attaquant et les moyens compromis.

Investigation – procédé visant à collecter et analyser des informations pour confirmer ou d’infirmer l’origine malveillante d’un incident de sécurité, de mieux comprendre l’incident de sécurité et le mode opératoire de l’attaquant, de qualifier l’étendue de la compromission et de proposer des mesures d’endiguement.

Menace hactiviste ou isolée – cette menace s’illustre par la conduite d’attaques informatiques menées par un individu isolé ou un groupe hactiviste à des fins de déstabilisation (par vengeance, par motif idéologique, etc.). Les moyens mis en œuvre incluent notamment des attaques par déni de service ou des fuites de données. La menace isolée comprend également des individus utilisant des outils peu sophistiqués ou bénéficiant d’accès privilégiés au sein d’une entité, mais disposant de peu de moyens.

Menace stratégique – cette menace s’illustre par la conduite d’attaques informatiques persistantes et ciblées, menées ou financées par un État. Elle est caractérisée par des moyens techniques et organisationnels importants, ainsi qu’un effort de discrétion. Ces attaques peuvent être conduites notamment à des fins d’espionnage, de pré-positionnement ou de déstabilisation.

Menace systémique – cette menace s’illustre par sa capacité à affecter une large proportion d’entités. Elle inclut la menace cybercriminelle, caractérisée par la conduite d’attaques informatiques majoritairement opportunistes. Ces attaques sont généralement conduites à des fins lucratives et peuvent se matérialiser par des rançongiciels ou des fraudes. Ces menaces sont également représentées par la prolifération d’outils et de services offensifs disponibles sur étagère ou commercialisés par des entreprises privées. Ces services peuvent être utilisés dans des actions d’intelligence économique ou d’espionnage industriel ou permettre à certains États aux ressources limitées d’accéder à des capacités offensives.

Prestataires de réponse aux incidents de sécurité – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	7/49

Mesure de sécurité – mesure permettant de satisfaire une exigence de sécurité, d’empêcher ou réduire la survenance d’un risque d’atteinte à la sécurité de l’information ou d’en diminuer la gravité.

Niveau de qualification élevé – niveau de qualification permettant d’avoir, par rapport au niveau de qualification substantiel, une garantie renforcée notamment sur la compétence du prestataire, la confiance que l’on peut lui accorder et sa capacité à protéger les informations et supports relatifs à la prestation. Une prestation de niveau élevé est recommandée lorsque les risques qui pèsent sur le système d’information objet de la prestation sont élevés et/ou lorsque les scénarios de risque de nature intentionnelle impliquent une menace stratégique.

Niveau de qualification substantiel – niveau de qualification permettant d’avoir un premier niveau de garantie notamment sur la compétence du prestataire, la confiance que l’on peut lui accorder et sa capacité à protéger les informations et supports relatifs à la prestation. Une prestation de niveau substantiel est recommandée lorsque les scénarios de risque de nature intentionnelle qui pèsent sur le système d’information objet de la prestation impliquent une menace systémique, hacktiviste ou isolée.

Note de cadrage – document élaboré et tenu à jour par le prestataire en concertation avec le commanditaire et précisant les modalités de la prestation. La note de cadrage est généralement élaborée après la signature de la convention de service.

Pilote d’investigation – personne réalisant une activité de pilotage et de coordination des investigations pour le compte du prestataire, c’est-à-dire les actions visant à orienter et coordonner techniquement ou de manière organisationnelle la prestation fournie, conjointement avec le commanditaire, le bénéficiaire ou toute entité externe impliquée dans la prestation.

Périmètre de la prestation – environnement physique, logique et organisationnel du système d’information objet de la prestation.

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

Potentiel d’attaque – mesure de l’effort à fournir pour attaquer un système d’information exprimée en termes d’expertise, de ressources et de motivation d’un attaquant.

Prestataire – personne morale réalisant une prestation qualifiée c’est-à-dire conforme aux exigences du présent référentiel.

Rapport d’analyse – document élaboré par l’équipe de réponse aux incidents présentant les résultats de la prestation et remis au commanditaire à l’issue de la prestation.

Référentiel – le présent document.

Responsable d’équipe – personne physique au sein du prestataire responsable de la prestation de réponse aux incidents de sécurité. Le responsable d’équipe est notamment en charge de constituer l’équipe de réponse aux incidents de sécurité en veillant à l’adéquation des compétences des analystes et pilotes d’investigation et, le cas échéant des experts, avec les objectifs, critères, périmètre et activités de la prestation. Le responsable d’équipe est un analyste ou un pilote.

Prestataires de réponse aux incidents de sécurité – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	8/49

Sécurité d'un système d'information – préservation des besoins de sécurité, notamment la confidentialité, l'intégrité et la disponibilité, des informations collectées, stockées, traitées et distribuées au sein d'un système d'information.

Sous-traitance – opération par laquelle le prestataire confie, sous sa responsabilité, à une personne morale (le sous-traitant) tout ou partie de l'exécution d'un contrat conclu entre le prestataire et le commanditaire.

Supervision de circonstance – dispositif ou configuration temporaire, pouvant être déployé rapidement, et mis en place dans le cadre de la prestation. Elle complète ou remplace la supervision initialement mise en œuvre, en s'appuyant sur un dispositif ou une configuration temporaire de collecte en continu des journaux et/ou flux réseau issus de différentes sources. Elle permet notamment, d'alerter en cas d'activité potentiellement malveillante.

Système d'information – ensemble organisé de ressources (matériels, logiciels, personnels, données, procédures, etc.) permettant de collecter, stocker, traiter et distribuer l'information.

Système d'information cible – système d'information objet de la prestation.

Tiers – personne physique ou morale indépendante du prestataire, du commanditaire et du bénéficiaire.

Vulnérabilité – faiblesse d'un système d'information ou d'une mesure de sécurité pouvant être exploitée par une menace.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	9/49

II. Activités couvertes par le référentiel

Les activités couvertes par ce référentiel sont les suivantes :

- recherche d'indicateurs de compromission (REC) ;
- investigation numérique (INV) ;
- analyse de codes malveillants (CODE) ;
- pilotage et coordination des investigations (PCI).

Lorsqu'une exigence n'est applicable qu'à une seule et unique activité alors elle est précédée d'une mention entre crochets identifiant ladite activité. À titre d'exemple, une exigence précédée de la mention « [REC] » est applicable exclusivement à l'activité de recherche d'indicateurs de compromission.

Lorsqu'une exigence est applicable à plusieurs activités sans toutefois être applicable à l'ensemble des activités alors elle est précédée d'une mention entre crochets identifiant lesdites activités. À titre d'exemple, une exigence précédée de la mention « [REC, INV] » est applicable exclusivement aux activités de recherche d'indicateurs de compromission et d'investigation numérique.

Lorsqu'une exigence n'est précédée d'aucune mention entre crochets identifiant une activité alors elle est applicable à l'ensemble des activités.

La réalisation entièrement automatisée d'une activité ne représente pas une activité au sens du référentiel.

Le prestataire peut adapter les étapes 3 à 7 de la prestation décrites au chapitre VI du présent référentiel voire ne pas en réaliser certaines en fonction de l'évolution de la compréhension de l'incident de sécurité ou de l'incident de sécurité lui-même.

II.1. Recherche d'indicateurs de compromission

La recherche d'indicateurs de compromission consiste à rechercher les traces d'une compromission au sein d'un système d'information.

Cette activité peut être réalisée seule, conjointement à une activité d'analyse de codes malveillants ou dans le cadre d'une d'investigation numérique pilotée ou non pilotée.

II.2. Investigation numérique

L'investigation numérique consiste à collecter et analyser des informations et supports collectés au sein d'un système d'information afin d'infirmer ou de confirmer une compromission et, le cas échéant identifier le périmètre et la chronologie de la compromission, le mode opératoire de l'attaquant et sa caractérisation notamment en termes de potentiel d'attaque et d'objectifs.

L'investigation numérique peut impliquer des analyses système et/ou réseau.

Cette activité peut être réalisée seule, conjointement à une activité de recherche d'indicateurs de compromission ou d'analyse de codes malveillants. Lorsqu'elle être réalisée conjointement à une activité de pilotage et coordination des investigations est dite « pilotée » et « non pilotée » sinon.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	10/49

II.3. Analyse de codes malveillants

L'analyse de codes malveillants consiste à analyser des codes malveillants pour comprendre leur comportement, leur fonctionnement et leurs impacts.

Cette activité peut être réalisée seule, conjointement à une activité de recherche d'indicateurs de compromission, ou dans le cadre d'une d'investigation numérique pilotée ou non pilotée.

II.4. Pilotage et coordination des investigations

Le pilotage et la coordination des investigations est nécessaire dans le cas de situations graves ou complexes, notamment par la nature, l'ampleur ou la gravité de l'incident de sécurité qui nécessitent que plusieurs activités de réponse aux incidents doivent être réalisées de manière coordonnée.

Cette activité implique la réalisation simultanée de plusieurs activités de réponse aux incidents : recherche d'indicateurs de compromission, investigation numérique et/ou analyse de codes malveillants.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	11/49

III. Qualification des prestataires

III.1. Modalités de la qualification

La qualification d'un prestataire est réalisée conformément au processus de qualification d'un service (7) et permet d'attester de la conformité du prestataire aux exigences du présent référentiel.

Le référentiel contient des exigences et des recommandations applicables aux prestataires, à leurs personnels et à la prestation.

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

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

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

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

Est considérée comme une prestation qualifiée, une prestation respectant la démarche décrite au chapitre VI dont les activités décrites au chapitre II sont réalisées par le personnel respectant les exigences du chapitre V et travaillant pour un prestataire qualifié respectant les exigences du chapitre IV. Pour chaque type de prestation, le personnel doit respecter les profils de compétences attendus, conformément à l'Annexe 2.

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. Niveaux de qualification

Les prestataires peuvent se faire qualifier selon deux niveaux de qualification : substantiel ou élevé.

Lorsqu'une exigence n'est applicable qu'à un seul et unique niveau de qualification, alors elle est précédée d'une mention entre crochets identifiant ledit niveau. Ainsi, une exigence précédée de la mention « [SUBSTANTIEL] » est applicable exclusivement au niveau de qualification substantiel et une exigence précédée de la mention « [ELEVE] » est applicable exclusivement au niveau de qualification élevé.

Lorsqu'une exigence n'est précédée d'aucune mention entre crochets identifiant un niveau de qualification, alors elle est applicable à l'ensemble des niveaux de qualification.

Les exigences applicables au niveau de qualification élevé sont par défaut des recommandations pour le niveau de qualification substantiel.

Un prestataire ne peut pas obtenir la qualification pour plusieurs activités à des niveaux de qualification différents.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	12/49

La qualification d'un prestataire au niveau élevé atteste de son aptitude à réaliser l'ensemble des activités qui constituent sa portée de qualification au niveau substantiel et élevé.

La qualification d'un prestataire au niveau substantiel atteste de son aptitude à réaliser l'ensemble des activités qui constituent sa portée de qualification au niveau substantiel uniquement.

L'Annexe 3 fournit des recommandations aux commanditaires quant au choix du niveau de qualification de la prestation.

III.3. Portée de la qualification

La portée de qualification est constituée d'une ou plusieurs activités décrites au chapitre II et d'un niveau de qualification décrit au chapitre III.2.

Le prestataire peut demander la qualification pour une ou plusieurs activités et pour un niveau de qualification.

Pour être qualifié selon une portée de qualification, le prestataire doit satisfaire l'ensemble des exigences du référentiel applicables aux activités et au niveau de qualification qui constituent la portée de qualification.

Le prestataire peut demander la qualification pour un niveau de qualification et pour une ou plusieurs activités de réponse telles que précisées ci-dessous :

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

III.4. Qualification pour les besoins de la sécurité nationale

Les prestataires réalisant des prestations de réponse aux incidents de sécurité pour les besoins de la sécurité nationale doivent satisfaire, en sus des exigences du présent référentiel pour le niveau élevé, les exigences du référentiel (8).

La réponse aux incidents pour les besoins de la sécurité nationale comprend notamment la réponse aux incidents affectant les systèmes d'information d'importance vitale (SIIV) des opérateurs d'importance vitale (OIV) et les systèmes d'information traitant des informations et supports classifiés FR (2) UE (9) et OTAN (10).

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	13/49

IV. Exigences applicables au prestataire

IV.1. Exigences générales

- a) Le prestataire doit être une personne morale.
- b) Le prestataire doit être soumis au droit d'un État membre de l'Union Européenne.
- c) Le prestataire doit, en sa qualité de professionnel, avoir un devoir de conseil vis-à-vis du commanditaire.
- d) Le prestataire doit s'assurer du consentement du commanditaire avant toute communication à des tiers d'informations et supports relatifs à la prestation.
- e) Le prestataire doit apporter la preuve que son organisation, les moyens qu'il met en œuvre pour réaliser la prestation et les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité à l'égard du commanditaire.
- f) Le prestataire doit réaliser la prestation de manière impartiale, en toute bonne foi et dans le respect du commanditaire, de ses personnels et de ses infrastructures.
- g) Le prestataire doit enregistrer et traiter les plaintes relatives aux prestations qualifiées déposées par les commanditaires, les bénéficiaires et, de manière générale, l'ensemble des tiers.
- h) Le prestataire doit informer sans délai l'ANSSI de tout dépôt d'une plainte relative à une prestation qualifiée et du traitement de celle-ci.

IV.2. Gestion des personnels

- a) Le prestataire doit, avant toute incorporation d'un analyste ou d'un pilote dans ses équipes dans ses équipes, procéder à la vérification des formations, connaissances, compétences et références professionnelles, et de la véracité de leur curriculum vitae.
- b) Le prestataire doit s'assurer, avant le début de chaque prestation, que les membres de l'équipe, disposent des connaissances et compétences associées à leurs activités conformément à l'Annexe 2.
- c) [ELEVE] Le prestataire ne doit recourir qu'à des analystes et pilotes d'investigation disposant d'une attestation individuelle de compétence pour réaliser la prestation.

Le prestataire peut, avec l'accord du commanditaire, incorporer dans l'équipe de réponse, des personnes ne disposant pas d'attestation individuelle de compétence au titre de leur formation ou de leur montée en compétence. Ces personnes sont présentes en tant qu'observateurs et ne participent pas à la réalisation de la prestation.

- d) Le prestataire doit assurer la formation continue des analystes et pilotes d'investigation afin de maintenir à jour leurs connaissances et compétences en matière de réponse aux incidents de sécurité, et en particulier celles requises pour la réalisation de leurs missions.
- e) Le prestataire doit permettre aux analystes et aux pilotes d'investigation d'assurer une veille afin de maintenir à jour leurs connaissances et compétences en matière de réponse aux incidents de sécurité, et en particulier celles requises pour la réalisation de leurs missions.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	14/49

- f) Le prestataire est responsable des méthodes et outils utilisés par l'équipe de réponse ainsi que de leur bonne utilisation durant la prestation.
- g) Le prestataire doit sensibiliser les analystes et pilotes d'investigation à la réglementation en vigueur au sein de l'Union européenne en matière de réponse aux incidents de sécurité, et en particulier celle applicable à leurs missions.
- h) [ELEVE] Le prestataire doit s'assurer qu'aucun membre de l'équipe de réponse ne fait l'objet d'une inscription au casier judiciaire incompatible avec l'exercice de ses missions.

IV.3. Protection de l'information

Le prestataire peut, selon la demande du commanditaire, traiter tout ou partie des informations et supports relatifs à la prestation sur son système d'information, celui du commanditaire ou du bénéficiaire.

Pour obtenir la qualification au niveau élevé, le prestataire doit, dans tous les cas, disposer d'un système d'information homologué pour la protection d'informations et supports portant la mention Diffusion Restreinte (1).

Dans le cadre de la réalisation d'une prestation qualifiée de niveau élevé, le prestataire doit utiliser son système d'information homologué Diffusion Restreinte et ce quel que soit le marquage des informations et supports relatifs à la prestation.

Dans le cadre de la réalisation d'une prestation qualifiée de niveau substantiel, le prestataire qualifié au niveau élevé peut choisir de disposer, en plus de son système d'information homologué Diffusion Restreinte, d'un second système d'information respectant les exigences du présent chapitre pour le niveau substantiel. Ainsi le prestataire qualifié au niveau élevé peut, dans le cadre de la réalisation d'une prestation qualifiée de niveau substantiel, selon la demande du commanditaire, traiter les informations et supports relatifs à la prestation ne portant pas la mention Diffusion Restreinte soit sur son système d'information homologué Diffusion Restreinte soit sur son second système d'information.

- a) Le prestataire doit élaborer et tenir à jour une appréciation des risques relatifs à son activité de réponse aux incidents.
- b) Il est recommandé que le prestataire mette en œuvre la méthode (11) pour réaliser l'appréciation des risques relatifs à son activité de réponse aux incidents.
- c) Le prestataire doit protéger en intégrité et en confidentialité les informations et supports relatifs à la prestation selon leur marquage et leur niveau de sensibilité.
- d) Le prestataire doit appliquer le principe du moindre privilège et limiter l'accès aux informations et supports relatifs à la prestation aux strictes personnes ayant le droit et le besoin d'en connaître.
- e) Le prestataire peut être amené à connecter un même équipement (clé USB, ordinateur, etc.) à son système d'information homologué et au système d'information cible potentiellement compromis. Le prestataire doit mettre en œuvre des mesures de sécurité adaptées pour ces équipements afin de répondre aux besoins opérationnels de la prestation et aux besoins de sécurité de son système d'information homologué. [ELEVE] Il n'est pas exigé du prestataire qu'il homologue ces équipements Diffusion Restreinte si le système d'information cible n'est pas homologué Diffusion Restreinte.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	15/49

- f) Le prestataire doit homologuer son système d'information.
- g) [ELEVE] Le prestataire doit homologuer son système d'information pour la protection d'informations et supports portant la mention Diffusion Restreinte.
- h) Il est recommandé que le prestataire mette œuvre la démarche décrite dans le guide (12) pour homologuer son système d'information.
- i) Le prestataire doit être capable d'utiliser son système d'information pour réaliser la totalité d'une prestation.
- j) [ELEVE] Le prestataire doit mettre en œuvre l'ensemble des règles du guide d'hygiène informatique (13) pour le niveau renforcé sur son système d'information homologué Diffusion Restreinte.
- k) [ELEVE] Le prestataire doit mettre en œuvre l'ensemble des règles relatives à la protection des systèmes d'information traitant des informations et supports portant la mention Diffusion Restreinte définies dans (1) sur son système d'information homologué Diffusion Restreinte.
- l) [ELEVE] Il est recommandé que le prestataire mette en œuvre les recommandations du guide (14) sur son système d'information homologué Diffusion Restreinte.
- m) [SUBSTANTIEL] Le prestataire doit mettre en œuvre l'ensemble des règles du guide d'hygiène informatique (13) pour le niveau standard sur son système d'information.
- n) Le prestataire doit réaliser une revue périodique des droits d'accès sur son système d'information.
- o) [ELEVE] Le prestataire doit réaliser une revue des droits d'accès sur son système d'information tous les six mois.
- p) Le prestataire doit disposer d'un système d'information hors-ligne afin de conserver l'ensemble des informations et supports relatifs à la prestation pour lesquels il a reçu une autorisation de conservation du commanditaire.
- q) Le prestataire doit mettre en œuvre des mesures de sécurité spécifiques pour le stockage et la manipulation de codes malveillants afin d'éviter toute contamination de son système d'information.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	16/49

V. Exigences applicables aux personnels du prestataire

V.1. Connaissances et compétences générales

- a) Les analystes, pilotes d'investigation et responsable d'équipe doivent posséder les qualités personnelles décrites au chapitre « 7.2.2 Comportements personnels » de la norme (3).
- b) [PCI] Les responsables d'équipe et pilotes d'investigation doivent posséder les qualités personnelles décrites au chapitre « 7.2.3.4 Compétences générales du responsable d'une équipe d'audit » de la norme (3).
- c) Les analystes, pilotes d'investigation et responsables d'équipe doivent disposer de qualités rédactionnelles et de synthèse, et savoir restituer les informations pertinentes et adaptées aux profils de leurs interlocuteurs (direction, services techniques, responsables métier et sécurité, etc.).

V.2. Connaissances et compétences spécifiques

- a) Les analystes, pilotes d'investigation et responsables d'équipe doivent, selon leur rôle, réaliser la prestation conformément aux exigences du chapitre VI.
- b) Les analystes, pilotes d'investigation et responsables d'équipe doivent, selon leur rôle, assurer les missions décrites dans l'Annexe 2.
- c) Les analystes, pilotes d'investigation et responsables d'équipe doivent, selon leur rôle, disposer des connaissances et compétences en matière de réponse aux incidents de sécurité, particulièrement celles décrites dans l'Annexe 2.
- d) [ELEVE] [PCI] Les pilotes d'investigation doivent maîtriser les bonnes pratiques en matière de gestion des incidents de sécurité décrites dans les normes (4) (5).
- e) [ELEVE] Les analystes et pilotes d'investigation doivent maîtriser les bonnes pratiques en matière de d'identification, de collecte, d'acquisition et de préservation de preuves décrites dans la norme (6).

V.3. Expérience

- a) Il est recommandé que les analystes, pilotes d'investigation et responsables d'équipe aient reçu une formation en sécurité des systèmes d'information.
- b) Il est recommandé que les analystes, pilotes d'investigation et responsables d'équipe justifient d'au moins d'une année d'expérience dans le domaine de la réponse aux incidents de sécurité.

V.4. Engagement

- a) Les analystes, pilotes d'investigation et responsables d'équipe doivent avoir un contrat de travail avec le prestataire.
- b) Le prestataire doit avoir un cadre contractuel avec les experts.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	17/49

VI. Exigences applicables à la prestation

VI.1. Étape 1 – Qualification préalable d’aptitude à la réalisation de la prestation

- a) Il est recommandé que le prestataire demande au commanditaire de lui fournir les informations identifiées dans l’Annexe 4 afin de réaliser la qualification préalable d’aptitude.
- b) Le prestataire doit, en se fondant sur les informations communiquées par le commanditaire et notamment la description de l’incident de sécurité, les objectifs, les critères, le périmètre, les activités de réponse et les éventuelles modalités particulières de la prestation¹, réaliser une qualification préalable d’aptitude afin d’évaluer de manière impartiale s’il est en mesure de réaliser pleinement, partiellement ou non la prestation.
- c) Le prestataire doit informer le commanditaire des conclusions de la qualification préalable d’aptitude à la réalisation de la prestation et notamment s’il estime être en mesure de réaliser pleinement, partiellement ou non la prestation.
- d) Le prestataire ne doit accepter de réaliser prestation que si les conclusions de la qualification préalable d’aptitude confirment qu’il est en mesure de réaliser pleinement la prestation.

VI.2. Étape 2 – Elaboration de la convention de service

- a) Le prestataire doit établir une convention de service avec le commanditaire.

Lorsqu’un démarrage rapide de la prestation nécessite que le prestataire accède au système d’information cible ou à des informations et supports issus du système d’information cible en l’absence de convention de service ou de note de cadrage, un accord doit être signé entre le prestataire et le commanditaire. Les signataires de cet accord peuvent être les représentants légaux des entités ou toute personne en mesure d’engager les parties impliquées. Cet accord doit décrire le périmètre et les actions envisagées, il ne se substitue pas à l’élaboration de la convention de service ou de la note de cadrage.

- b) La convention de service doit être signée par un représentant légal du prestataire et un représentant légal du commanditaire, ou toute personne pouvant engager le prestataire et le commanditaire.

VI.2.1. Qualification

La convention de service doit :

- a) préciser que la prestation est qualifiée ;
- b) identifier le niveau de qualification de la prestation ;

¹ Le choix des objectifs, critères, périmètre, activités de réponse et éventuelles modalités particulières de la prestation revient in fine au commanditaire cependant le prestataire a, en sa qualité de professionnel en matière de sécurité des systèmes d’information, un devoir de conseil sur leur pertinence et leur cohérence.

Prestataires de réponse aux incidents de sécurité – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	18/49

- c) identifier les activités de réponse aux incidents. Lorsque la prestation comporte l'activité d'investigation numérique, la convention de service doit préciser le type d'analyse (système et/ou réseau) ;
- d) inclure l'attestation de qualification du prestataire ;
- e) [ELEVE] préciser que chaque analyste ou pilote dispose d'une attestation individuelle de compétence ;
- f) préciser que le commanditaire peut, conformément au processus de qualification d'un service (7), déposer auprès de l'ANSSI une réclamation lorsqu'il estime que le prestataire n'a pas respecté une ou plusieurs exigences du référentiel dans le cadre d'une prestation qualifiée, et rappeler qu'en cas de manquement du prestataire, la qualification du prestataire peut être retirée, la portée de qualification réduite, ou le niveau de recommandation du prestataire dégradé.

VI.2.2. Modalités de la prestation

La convention de service doit :

- a) décrire de manière générale la démarche, les objectifs, les critères, le périmètre et les activités de réponse, ainsi que les modalités de la prestation : prérequis, jalons, livrables, dates et lieux d'exécution de la prestation. Ces informations pourront être précisées et mises à jour si besoin dans la note de cadrage ;
- b) préciser que le droit applicable à la convention de service est celui d'un État membre de l'Union européenne et préciser lequel ;
- c) préciser 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 et les livrables de la prestation, en particulier le rapport d'analyse ;
- d) préciser que toute modification de la convention de service doit être soumise à l'acceptation d'un représentant légal du prestataire et d'un représentant légal du commanditaire, ou toute personne pouvant engager le prestataire et le commanditaire.

VI.2.3. Responsabilités

La convention de service doit :

- a) préciser que le commanditaire dispose de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation ou qu'il a recueilli l'accord des éventuelles parties dont les systèmes d'information entrent dans le périmètre de la prestation ;
- b) préciser que le prestataire informe le commanditaire par écrit et sans délai en cas de manquement à la convention de service ;
- c) préciser que le commanditaire autorise le prestataire à collecter et analyser des données du système d'information cible aux seules fins de la prestation et dans le strict respect des lois et réglementations applicables ;
- d) décrire les risques relatifs à la prestation, en particulier ceux concernant les atteintes à la disponibilité du système d'information cible et à la confidentialité de ses données.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	19/49

VI.2.4. Confidentialité

La convention de service doit :

- a) préciser que le prestataire ne collecte et n'analyse que les informations et supports strictement nécessaires à la bonne exécution de la prestation en adéquation avec les objectifs, critères, périmètre et activités de la prestation ;
- b) préciser que le prestataire ne divulgue ou ne partage aucune information ou support relatif la prestation à des tiers, sauf autorisation écrite du commanditaire ;
- c) préciser que le prestataire, à l'issue de la prestation, restitue, efface ou détruit l'ensemble des informations et supports relatifs à la prestation à l'exception de ceux pour lesquels il a reçu une autorisation écrite de conservation du commanditaire ;
- d) préciser que le prestataire, à l'issue de la prestation, conserve sur un système d'information hors-ligne l'ensemble des informations et supports relatifs à la prestation pour lesquels il a reçu une autorisation écrite de conservation du commanditaire.

VI.2.5. Experts

La convention de service doit :

- a) préciser que le prestataire peut incorporer dans l'équipe de réponse un ou plusieurs experts pour participer à la réalisation de certaines activités lorsque ces dernières requièrent des connaissances ou des compétences spécifiques dont les analystes ou pilotes d'investigation ne disposent pas sous réserve que :
 - i. il existe un cadre contractuel documenté entre le prestataire et les experts ;
 - ii. le recours aux experts est accepté par le commanditaire ;
 - iii. les experts sont dûment encadrés par le responsable d'équipe.

VI.2.6. Sous-traitance

La convention de service doit :

- a) préciser que le prestataire peut sous-traiter tout ou partie des activités de réponse à un prestataire sous-traitant sous réserve que :
 - i. le prestataire sous-traitant est qualifié pour les activités de réponse sous-traitées au même niveau de qualification ;
 - ii. la prestation sous-traitée est qualifiée au même niveau de qualification ;
 - iii. il existe un cadre contractuel entre le prestataire et le prestataire sous-traitant ;
 - iv. le recours à la sous-traitance est accepté par le commanditaire dans la note de cadrage.

VI.2.7. Note de cadrage

La convention de service doit :

- a) prévoir l'élaboration d'une note de cadrage et sa mise à jour durant la prestation ;
- b) indiquer que la note de cadrage respecte les exigences énoncées au chapitre VI.4.2.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	20/49

VI.3. Étape 3 – Compréhension et posture initiale

- a) [REC, INV, PCI] Le prestataire doit, notamment grâce aux informations recueillies lors de la qualification préalable d'aptitude à la réalisation de la prestation, acquérir une compréhension du système d'information cible :
- i. la cartographie du système d'information cible ;
 - ii. l'architecture du système d'information cible ;
 - iii. la localisation du système d'information cible ;
 - iv. les moyens de supervision, et le cas échéant de détection des incidents de sécurité, du système d'information cible ;
 - v. les spécificités et contraintes du système d'information cible ;
 - vi. les interconnexions du système d'information cible.
- b) [ELEVE] [PCI] Le prestataire doit proposer au commanditaire une posture initiale identifiant notamment :
- i. la démarche générale de réponse aux incidents adaptée aux besoins de la prestation ;
 - ii. les grands jalons de la prestation et le calendrier associé ;
 - iii. les activités de réponse à réaliser ;
 - iv. les informations à collecter et analyser et les modes opératoires associés ;
 - v. le nombre d'analystes et le cas échéant d'experts à engager ;
 - vi. le niveau de discrétion à adopter vis-à-vis de l'attaquant :
 - o élevé : le prestataire réalise ses activités sans possibilité de détection par l'attaquant (copie de disques sur systèmes déconnectés, collecte d'informations sur des équipements inaccessibles par l'attaquant, etc.). Les activités réalisées par le prestataire n'exposent pas la connaissance sur l'attaquant et n'entravent pas les opérations de l'attaquant, ses moyens et ses canaux de communication ne sont pas modifiés ou supprimés,
 - o moyen : le prestataire réalise ses activités avec une faible probabilité de détection (collecte d'informations confondues avec l'activité normale d'un administrateur ou utilisateur, actions de sécurisation réalisées par un administrateur, etc.). Les activités du prestataire peuvent entraver partiellement ou totalement les opérations de l'attaquant, mais n'apparaissent pas nécessairement dirigées contre lui, ses moyens et canaux de communication peuvent être restreints (limitation de la bande passante, durcissement de la configuration, extinction de postes compromis, etc.),
 - o faible : le prestataire réalise ses activités sans se préoccuper de la présence de l'attaquant. Les activités du prestataire peuvent entraver partiellement ou totalement les opérations de l'attaquant et ne lui laissent aucun doute quant à la détection de sa présence. Les canaux de communication et moyens de l'attaquant peuvent parfois être bloqués ou supprimés.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	21/49

- c) [ELEVE] [PCI] Le pilote d’investigation doit soumettre pour validation la posture initiale au correspondant de la prestation au sein du commanditaire et à chaque révision. Le choix définitif de la posture est de la responsabilité du commanditaire.
- d) [ELEVE] [PCI] Le pilote d’investigation doit réviser la posture en fonction des résultats des activités de collecte et d’analyse et de la compréhension de l’incident.

VI.4. Étape 4 – Préparation de la prestation

VI.4.1. Constitution de l’équipe

- a) Le prestataire doit désigner un responsable d’équipe.
- b) Le responsable d’équipe doit constituer une équipe composée d’analystes et, le cas échéant, de pilotes d’investigation et d’experts disposant de toutes les connaissances et compétences requises pour mener la prestation. Le responsable d’équipe peut, s’il dispose des connaissances et compétences suffisantes, réaliser la prestation seul.
- c) Le responsable d’équipe doit réévaluer régulièrement le profil et le nombre des analystes et, le cas échéant, de pilotes d’investigation et d’experts afin de s’assurer que l’engagement du prestataire reste adapté à la bonne exécution de la prestation.
- d) [ELEVE] Les analystes et, le cas échéant, les pilotes d’investigation doivent chacun disposer d’une attestation individuelle de compétence en vigueur pour les activités qui leur sont confiées.

VI.4.2. Elaboration de la note de cadrage

- a) Le responsable d’équipe doit élaborer la note de cadrage en concertation avec l’équipe de réponse et le correspondant de la prestation au sein du commanditaire.

La note de cadrage doit :

- b) préciser les objectifs, les critères, le périmètre et les activités de réponse, ainsi que les modalités de la prestation : prérequis, jalons, livrables, dates et lieux d’exécution de la prestation, etc. ;
- c) identifier les instances de gouvernance de la prestation et préciser leurs rôles et fréquences de réunion ;
- d) identifier le nom du correspondant de la prestation au sein du commanditaire dont le rôle est de gérer la relation avec le prestataire, de veiller à la bonne exécution de la prestation, et de s’assurer que la convention de service et la note de cadrage sont respectées ;
- e) identifier si le commanditaire autorise le prestataire à sous-traiter tout ou partie de la prestation et, le cas échéant, identifier le prestataire sous-traitant et les activités de réponse sous-traitées ;
- f) identifier si le commanditaire autorise le prestataire à recourir à des experts ;
- g) identifier les noms et les coordonnées des membres de l’équipe de réponse et préciser pour chacun d’eux leur rôle (responsable d’équipe, pilote, analyste ou expert) et les activités de réponse qui leur sont confiées ;

Prestataires de réponse aux incidents de sécurité – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	22/49

- h) [ELEVE] annexer les attestations individuelles de compétence des analystes et pilotes d'investigation ;
- i) identifier les noms, rôles, et responsabilités des personnes désignées par le commanditaire et intervenant dans le cadre de la prestation ;
- j) décrire, le cas échéant, les modalités de collaboration avec les tiers (sous-traitants, etc.) ;
- k) identifier les droits et besoins d'en connaître des informations et supports relatifs à la prestation ;
- l) identifier le marquage des informations et supports relatifs à la prestation selon leur niveau de sensibilité² ;
- m) identifier les moyens de protection des informations et supports relatifs à la prestation selon leur niveau de sensibilité et leur marquage³ ;
- n) préciser les livrables de la prestation et décrire les modalités applicables : contenu, forme, langue, etc. ;
- o) identifier pour chaque information et support relatif à la prestation lesquels seront conservés, effacés ou détruits par le prestataire ou restitués au commanditaire, et préciser les modalités de conservation, effacement, destruction et restitution ;
- p) identifier, le cas échéant, les exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire, en particulier celles applicables au système d'information cible ;
- q) [ELEVE] décrire la méthode et les moyens permettant d'élaborer et de tenir à jour le registre des informations et supports remis au prestataire ou collectés par ce dernier ;
- r) [ELEVE] décrire la méthode et les moyens permettant d'élaborer et de tenir à jour le registre des actions réalisées par le prestataire sur les informations et supports collectés et le système d'information cible ;
- s) identifier, le cas échéant, les demandes spécifiques du commanditaire notamment les sujets pour lesquels il souhaite que le prestataire ait une attention particulière. Il peut s'agir par exemple de contraintes particulières auxquelles pourraient être soumis le système cible ou le commanditaire ;
- t) être validée par le correspondant de la prestation au sein du commanditaire et par le responsable d'équipe et à chaque mise à jour durant la prestation.

VI.4.3. Mesures de précaution particulières

- a) Le responsable d'équipe doit sensibiliser le commanditaire sur les thèmes identifiés en Annexe 3 et notamment :

² Le choix du marquage des informations et supports relatifs à la prestation revient in fine au commanditaire cependant le prestataire a, en sa qualité de professionnel en matière de sécurité des systèmes d'information, un devoir de conseil et doit proposer au commanditaire un marquage adapté. L'Annexe 3 fournit des recommandations aux commanditaires sur le marquage des livrables de la prestation notamment le rapport d'analyse.

³ Le choix des moyens de protection des informations et supports relatifs à la prestation revient in fine au commanditaire cependant le prestataire a, en sa qualité de professionnel en matière de sécurité des systèmes d'information, un devoir de conseil et doit proposer au commanditaire des moyens de protection adaptés.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	23/49

- i. la mise en place de mesures de sauvegarde du système d'information cible ;
 - ii. la mise en place d'un dispositif de gestion de crise ;
 - iii. la mise à disposition du prestataire d'une zone sécurisée dédiée à la prestation ;
 - iv. la mise à disposition du prestataire d'un environnement d'analyse sécurisé et déconnecté du système d'information cible ;
 - v. la mise en place de moyens de communication sécurisés, dédiés à la prestation et déconnectés du système d'information cible ;
 - vi. la mise en place de mesures de sécurité lorsque la prestation nécessite l'installation d'outils ou l'exécution de commandes sur le système cible ;
 - vii. la mise en place de procédures d'urgence, aussi appelées procédures « bouton-rouge » afin d'isoler rapidement le système d'information cible en cas de besoin.
- b) Le responsable d'équipe doit obtenir l'accord du commanditaire pour la réalisation de toute action pouvant entraîner un dysfonctionnement voire un déni de service du système d'information cible.

VI.4.4. Réunion d'ouverture

- a) Il est recommandé que le responsable d'équipe organise une réunion d'ouverture à laquelle participent a minima le responsable d'équipe, les analystes, le pilote d'investigation et les experts le cas échéant, le correspondant de la prestation au sein du commanditaire ainsi que les responsables sécurité et métier du système d'information cible afin de confirmer, préalablement à l'exécution de la prestation, leur accord sur l'ensemble des modalités de la prestation, en particulier la note de cadrage.

VI.5. Étape 5 – Exécution de la prestation

Dans ce chapitre, les différentes opérations peuvent être réalisées en même temps ou successivement, dans l'ordre jugé pertinent par le responsable d'équipe et, le cas échéant le pilote d'investigation, pour la bonne exécution de la prestation.

VI.5.1. Collecte

La collecte est une étape fondamentale qui nécessite une approche méthodique. Elle peut être réalisée par le prestataire, le commanditaire, le bénéficiaire ou un tiers, en mode connecté ou déconnecté. Si la collecte n'est pas réalisée par le prestataire, celui-ci doit sensibiliser le commanditaire aux risques de ne pas respecter les exigences du présent chapitre.

VI.5.1.1. Préparation

- a) [REC, INV] Le prestataire doit identifier les points de collecte système et réseau pertinents pour atteindre les objectifs de la prestation.
- b) [REC, INV] Le prestataire doit être capable de réaliser les opérations de collecte suivantes :
- i. collecte d'informations techniques ;
 - ii. collecte de journaux d'évènements ;
 - iii. collecte de flux réseau.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	24/49

- c) [PCI] Le prestataire doit élaborer et mettre en œuvre une démarche de collecte qui décrit :
 - i. les équipements du système d'information cible porteurs d'informations pertinentes à collecter ;
 - ii. les informations pertinentes à collecter : journaux d'évènements, mémoire volatile, etc. ;
 - iii. les méthodes appropriées de collecte des informations : copie de disques, copie de mémoires volatiles, etc. ;
 - iv. le séquençage des opérations de collecte.
- d) [REC, INV, PCI] Le prestataire doit, en collaboration avec le commanditaire, identifier les impacts éventuels des opérations de collecte, en particulier si elles présentent un risque pour la disponibilité du système d'information cible.

VI.5.1.2. Collecte d'informations techniques

- a) [REC, INV] Le prestataire doit être capable de collecter les informations sur les équipements suivants :
 - i. système : serveurs de sauvegarde, serveurs de fichiers, etc. ;
 - ii. réseau : serveurs mandataires, serveurs DNS, routeurs, points d'accès sans fil, etc. ;
 - iii. sécurité : pare-feu, chiffreurs, antivirus, sondes réseau, etc. ;
 - iv. métier : serveurs Web, base de données, etc. ;
 - v. postes d'administration ;
 - vi. postes utilisateur : ordinateurs fixes ou nomades, téléphones portables, etc.
- b) [REC, INV] Le prestataire doit être capable de collecter les informations techniques portant sur :
 - i. les configurations des équipements ;
 - ii. les systèmes de fichiers ;
 - iii. les programmes (services, processus, etc.) en exécution.

VI.5.1.3. Collecte de journaux d'évènements

- a) [ELEVE] [PCI] Le prestataire doit être capable de proposer et de mettre en œuvre une politique de journalisation répondant aux besoins de la prestation.
- b) [ELEVE] [PCI] Il est recommandé que le prestataire s'appuie sur le guide (15) pour proposer et mettre en œuvre la politique de journalisation.
- c) [REC, INV] Le prestataire doit être capable de collecter les journaux d'évènements sur les équipements suivants :
 - i. réseau : serveurs mandataires, serveurs DNS, routeurs, points d'accès sans fil, etc. ;
 - ii. sécurité : pare-feu, chiffreurs, antivirus, sondes réseau, etc. ;
 - iii. métier : serveurs de fichiers, serveurs Web, base de données, etc. ;

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	25/49

- iv. postes d'administration ;
- v. postes utilisateur : ordinateurs fixes ou nomades, téléphones portables, etc.

VI.5.1.4. Copie

- a) [REC, INV] Le prestataire doit être capable de réaliser des copies de support de mémoires volatiles et non volatiles.

VI.5.1.5. Collecte de flux réseau

- a) [REC, INV] Le prestataire doit être capable de collecter des flux réseau afin de :
 - i. analyser le protocole de communication entre une ressource compromise et une infrastructure de commande et de contrôle ;
 - ii. analyser la méthode utilisée lors des mouvements latéraux de l'attaquant ;
 - iii. rechercher des indicateurs de compromission.

VI.5.2. Analyse

L'analyse est une étape fondamentale qui nécessite une approche méthodique. Elle peut être réalisée par le prestataire sur le système d'information cible ou hors ligne.

VI.5.2.1. Recherche d'indicateurs de compromission

- a) [REC, INV] Le prestataire doit disposer d'une base d'indicateurs de compromission régulièrement mise à jour⁴.
- b) [REC, INV] Le prestataire doit respecter les conditions et restriction d'utilisation applicables aux indicateurs de compromission notamment ceux bénéficiant d'un marquage⁶, le système d'information cible devant être considéré comme étant a priori compromis.
- c) [REC, INV] Le prestataire doit être capable de rechercher des indicateurs de compromission sur les équipements suivants :
 - i. réseau : serveurs mandataires, serveurs DNS, routeurs, points d'accès sans fil, etc. ;
 - ii. sécurité : pare-feu, chiffreurs, antivirus, sondes réseau, etc. ;
 - iii. métier : serveurs de fichiers, serveurs Web, base de données, etc. ;
 - iv. postes d'administration ;
 - v. postes utilisateur : ordinateurs fixes ou nomades, téléphones portables, etc.

⁴ Les indicateurs de compromission peuvent notamment être issus d'une veille sur la menace faite par le prestataire, de résultats de précédentes prestations de réponse aux incidents ou communiqués par des partenaires ou des autorités.

⁶ Le marquage peut être relatif à un niveau de sensibilité (p. ex. : Diffusion Restreinte), de classification (p. ex. : Secret) ainsi qu'à des modalités de diffusion ou d'utilisation. Le TLP (*Traffic Light Protocol*) est un exemple de marquage relatif à des modalités de diffusion. Le PAP (*Permissible Actions Protocol*) est un exemple de marquage relatif à des modalités d'utilisation.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	26/49

- d) [REC, INV] Le prestataire doit analyser les informations collectées et être capable de rechercher les indicateurs de compromission suivants :
 - i. attributs de fichiers : empreinte, nom, taille, date, localisation, etc. ;
 - ii. artefacts système : paramètres de configuration, clés de registre Windows, etc. ;
 - iii. artefacts réseau : adresses IP, URL et noms de domaine, etc. ;
 - iv. artefacts mémoire : processus, services, etc. ;
 - v. chaînes de caractères ;
 - vi. signatures complexes : combinaison d'indicateurs de compromission.
- e) [REC] Le prestataire doit, avant le lancement de la recherche d'indicateurs de compromission, vérifier que les indicateurs de compromission recherchés sont pertinents par rapport aux objectifs de la prestation.
- f) [ELEVE] [PCI] Le prestataire doit être capable d'identifier lorsqu'une recherche d'indicateurs de compromission d'antériorité est nécessaire, et le cas échéant, la réaliser.

VI.5.2.2. Analyse système et réseau

- a) [INV] Le prestataire doit analyser les informations collectées en recherchant :
 - i. les traces d'activité malveillante : exploitation de vulnérabilités, élévation de privilèges, reconnaissance du système d'information, exfiltration de données, etc. ;
 - ii. les mécanismes de persistance ;
 - iii. les anomalies par rapport aux pratiques usuelles métier et d'administration ;
 - iv. [REC] des indicateurs de compromission.

VI.5.2.3. Analyse de codes malveillants

- a) [CODE] Le prestataire doit être capable de réaliser :
 - i. une analyse du code malveillant à l'aide d'une plateforme en ligne d'analyse de fichiers suspects ;
 - ii. une analyse statique et dynamique du code malveillant ;
 - iii. une rétroconception du code malveillant.
- b) [ELEVE] Il est recommandé que le prestataire soit capable de réaliser une analyse du code malveillant à l'aide d'une plateforme hors ligne d'analyse de fichiers suspects.

VI.5.2.4. Recherches en sources ouvertes

Le prestataire peut, dans le cadre de l'analyse, réaliser des recherches en sources ouvertes. Les recherches en sources ouvertes, notamment sur Internet, peuvent éveiller l'attention de l'attaquant, il est donc important que le prestataire observe la plus grande prudence en les réalisant a fortiori si le niveau de discrétion recherché vis-à-vis de l'attaquant est élevé.

- a) [ELEVE] Le prestataire doit définir une méthode de recherche en sources ouvertes qui précise, en fonction du niveau de discrétion recherché vis-à-vis de l'attaquant, les informations pouvant être recherchées et les modalités de recherche associées.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	27/49

- b) [ELEVE] Il est recommandé que le prestataire, lorsque le niveau de discrétion recherché vis-à-vis de l’attaquant est élevé, utilise des bases d’informations internes.
- c) [ELEVE] Il est recommandé que le prestataire, lorsque le niveau de discrétion recherché vis-à-vis de l’attaquant est élevé et que des recherches ouvertes, notamment sur Internet, sont néanmoins nécessaires, utilise des liaisons démarquées sans lien direct avec le prestataire ou le commanditaire.

VI.5.3. Pilotage et suivi des investigations

- a) [ELEVE] [PCI] Le prestataire doit assurer au commanditaire un suivi régulier de la prestation, et en particulier de la compréhension de l’incident, de la posture et des prochaines opérations.
- b) [ELEVE] Le responsable d’équipe doit tenir à jour un registre recensant pour chaque information et support collecté :
 - i. la description de l’information ou du support collecté ;
 - ii. la date et l’heure de la collecte de l’information ou du support ;
 - iii. la méthode de collecte de l’information ou du support ;
 - iv. le niveau de sensibilité ou de classification de l’information ou du support.
- c) [ELEVE] [REC, INV, PCI] Le responsable d’équipe doit tenir à jour un registre recensant pour chaque action réalisée sur les informations et supports collectés et sur les ressources du système d’information cible :
 - i. la date et l’heure de l’action ;
 - ii. la description de l’action ;
 - iii. l’information, le support ou la ressource du système d’information cible sur lequel l’action a été réalisée.
- d) [INV, PCI] Le responsable d’équipe doit tenir à jour une synthèse de la compréhension de l’incident de sécurité décrivant :
 - i. si l’attaquant est toujours présent dans le système d’information ;
 - ii. la date de compromission initiale ;
 - iii. la chronologie des principales phases de la compromission ;
 - iv. le mode opératoire de l’attaquant pour :
 - compromettre initialement le système d’information,
 - se maintenir dans le système d’information,
 - dissimuler ses activités,
 - cartographier le système d’information,
 - élever ses privilèges,
 - contrôler les ressources compromises,
 - collecter des informations,

Prestataires de réponse aux incidents de sécurité – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	28/49

- exfiltrer des informations ;
- v. la caractérisation de l'attaquant :
 - o son potentiel d'attaque estimé,
 - o le niveau de menace estimé : stratégique, systémique, hacktiviste ou isolé,
 - o ses objectifs supposés : vol d'informations, sabotage, etc. ;
- vi. le périmètre de l'incident de sécurité :
 - le vecteur initial de compromission,
 - le niveau de privilège obtenu par l'attaquant,
 - la liste des ressources et comptes compromis, en particulier ceux d'administration.

VI.5.4. Soutien à l'endiguement

- a) [INV, PCI] Le responsable d'équipe doit proposer au commanditaire des mesures d'endiguement afin de limiter ou de ralentir les actions de l'attaquant. Ces mesures doivent être réévaluées régulièrement en fonction de l'évolution de la compréhension de l'incident de sécurité ou de l'incident de sécurité lui-même.
- b) [INV, PCI] Le responsable d'équipe doit proposer au commanditaire des mesures d'urgence, parfois appelées procédures « bouton-rouge », afin d'isoler rapidement le système d'information cible en cas de besoin. La décision d'activer ces procédures revient in fine au commanditaire.

VI.6. Étape 6 – Restitution

- a) [ELEVE] Le responsable d'équipe doit organiser une restitution dite « à chaud » à la fin de chaque journée afin de présenter au correspondant de la prestation au sein du commanditaire :
 - i. un état d'avancement de la prestation ;
 - ii. une synthèse des résultats des activités de réponse de la journée ;
 - iii. [INV, PCI] la compréhension de l'incident de sécurité ;
 - iv. les éventuelles difficultés rencontrées durant la journée : collaboration difficile ou indisponibilité du personnel du commanditaire ou du bénéficiaire, difficulté d'accès aux locaux, au système d'information ou à la documentation, etc.
- b) Le responsable d'équipe doit, dès la fin des activités de réponse et sans attendre que le rapport d'analyse soit achevé, informer le commanditaire des constats et des premières conclusions de la prestation.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	29/49

VI.7. Étape 7 – Élaboration du rapport

a) Le prestataire doit élaborer un rapport d'analyse⁷.

VI.7.1. Qualification

Le rapport d'analyse doit :

- a) préciser que la prestation est qualifiée ;
- b) identifier le niveau de qualification de la prestation ;
- c) identifier les activités de réponse aux incidents ;
- d) [INV, PCI] préciser si la prestation concerne une analyse réseau et/ou une analyse système ;
- e) identifier les noms et coordonnées des membres de l'équipe de réponse et préciser pour chacun d'eux leur rôle (responsable d'équipe, pilote d'investigation, analyste réseau, analyste système, analyste de codes malveillants ou expert) et les activités de réponse réalisées.

VI.7.2. Cadre

Le rapport d'analyse doit :

- a) décrire objectifs, les critères, le périmètre, les activités de réponse ainsi que les éventuelles modalités particulières de la prestation ;
- b) identifier les dates et lieux de la prestation ;
- c) identifier de manière précise (référence, numéro de version, date, etc.) les documents sur lesquels le prestataire s'est fondé pour réaliser la prestation.

VI.7.3. Synthèse managériale

a) Le rapport d'analyse doit présenter une synthèse managériale.

La synthèse managériale doit :

- b) être compréhensible par des personnes non expertes en sécurité des systèmes d'information ;
- c) synthétiser la compréhension de l'incident de sécurité : date de la compromission initiale, chronologie des principales phases de la compromission, mode opératoire et caractérisation de l'attaquant (objectifs et niveau de menace) ;
- d) décrire le périmètre de l'incident de sécurité ;
- e) décrire les risques critiques associés à l'incident de sécurité ;
- f) décrire les principales mesures d'endiguement recommandées pour traiter les risques critiques ;

⁷ Lorsque plusieurs activités sont menées durant la prestation, le choix d'avoir un ou plusieurs rapports d'analyse revient au commanditaire.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	30/49

- g) décrire les éventuelles réserves relatives aux résultats de la prestation : inadéquation entre les objectifs, les critères, le périmètre, les activités et la charge, difficultés rencontrées durant la prestation, limite de l'échantillonnage, collaboration difficile ou indisponibilité du personnel du commanditaire ou du bénéficiaire, difficulté d'accès aux locaux, au système d'information ou à la documentation, etc.

VI.7.4. Résultats

Le rapport d'analyse doit :

- a) [REC] identifier les indicateurs de compromission recherchés ;
- b) [REC, INV, PCI] identifier les éléments collectés et analysés ;
- c) détailler les résultats des activités de réponse ;
- d) [INV, PCI] détailler la compréhension de l'incident de sécurité :
 - i. si l'attaquant est toujours présent dans le système d'information ;
 - ii. la date de compromission initiale ;
 - iii. la chronologie détaillées des phases de la compromission ;
 - iv. le mode opératoire de l'attaquant pour :
 - compromettre initialement le système d'information,
 - se maintenir dans le système d'information,
 - dissimuler ses activités,
 - cartographier le système d'information,
 - élever ses privilèges,
 - contrôler les ressources compromises,
 - collecter des informations,
 - exfiltrer des informations ;
 - v. la caractérisation de l'attaquant :
 - o son potentiel d'attaque estimé,
 - o le niveau de menace estimé : stratégique, systémique, hacktiviste ou isolé,
 - o ses objectifs supposés : vol d'informations, sabotage, etc. ;
 - vi. le périmètre de l'incident de sécurité :
 - le vecteur initial de compromission,
 - le niveau de privilège obtenu par l'attaquant,
 - la liste des ressources et comptes compromis, en particulier ceux d'administration.
- e) [INV, PCI] décrire le niveau de discrétion adopté vis-à-vis de l'attaquant ;
- f) [INV, PCI] proposer des mesures d'endiguement afin de circonscrire l'incident de sécurité ;

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	31/49

- g) identifier les noms et fonctions des personnes au sein du commanditaire, du bénéficiaire et des éventuels tiers (sous-traitants, etc.) avec qui le prestataire a interagi pour réaliser la prestation.

VI.7.5. Annexes

Le rapport d'analyse doit annexer :

- a) la note de cadrage ;
- b) [ELEVE] le registre des informations et supports collectés par le prestataire ;
- c) [ELEVE] le registre des actions réalisées par le prestataire sur les informations et supports collectés ainsi que sur le système d'information cible.

VI.8. Étape 8 – Clôture de la prestation

- a) Il est recommandé que, suite à la remise du rapport d'analyse, le responsable d'équipe organise une réunion de clôture à laquelle participent a minima le responsable d'équipe, les analystes, le pilote d'investigation et les experts le cas échéant, le correspondant de la prestation au sein du commanditaire, la direction du commanditaire ainsi que les responsables sécurité et métier du système d'information cible. Cette réunion permet de présenter la synthèse du rapport d'analyse et de répondre aux éventuelles questions du commanditaire.
- b) Le prestataire doit procéder à la restitution, à l'effacement ou à la destruction des informations ou supports relatifs à la prestation pour lesquels il n'a pas obtenu l'accord de conservation du commanditaire dans la note de cadrage.
- c) Le prestataire doit conserver hors ligne les informations et supports relatifs à la prestation pour lesquels il a obtenu l'accord de conservation du commanditaire dans la note de cadrage.
- d) [ELEVE] Il est recommandé que le prestataire produise un procès-verbal de destruction, d'effacement ou de restitution des informations ou supports relatifs à la prestation pour lesquels il n'a pas obtenu l'accord écrit de conservation du commanditaire dans la note de cadrage. Ce procès-verbal, remis au commanditaire, devrait identifier de manière précise les informations ou supports détruits, effacés ou restitués, la date et le mode de destruction, d'effacement ou de restitution.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	32/49

Annexe 1 Bibliographie

1. Instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles, n° 901/SGDSN/ANSSI, version en vigueur. *Disponible sur <https://www.legifrance.gouv.fr>.*
2. *Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, n° 1300/SGDSN/PSE/PSD, version en vigueur. Disponible sur <https://www.legifrance.gouv.fr>.*
3. *Norme internationale ISO/IEC 19011 : Lignes directrices pour l'audit des systèmes de management, version en vigueur. Disponible sur <https://www.iso.org>.*
4. Norme internationale ISO/IEC 27035-1 : Technologies de l'information – Gestion des incidents de sécurité de l'information. Partie 1 : Principes de la gestion des incidents, version en vigueur. *Disponible sur <https://www.iso.org>.*
5. Norme internationale ISO/IEC 27035-2 : Technologies de l'information– Gestion des incidents de sécurité de l'information. Partie 2 : Lignes directrices pour planifier et préparer une réponse aux Incidents, version en vigueur. *Disponible sur <https://www.iso.org>.*
6. Norme internationale ISO/IEC 27037 : Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques, version en vigueur. *Disponible sur <https://www.iso.org>.*
7. *Processus de qualification d'un service, version en vigueur. Disponible sur <https://www.cyber.gouv.fr>.*
8. *Référentiel d'exigences applicables aux prestataires de réponse aux incidents de sécurité pour les besoins de la sécurité nationale, version en vigueur. Document Diffusion Restreinte, il peut être obtenu auprès de l'ANSSI.*
9. Instruction interministérielle n° 2102 sur la protection en France des informations classifiées de l'Union Européenne, n° 2102/SGDSN/PSD, version en vigueur. *Disponible sur <https://www.legifrance.gouv.fr>.*
10. Instruction interministérielle n° 2100 pour l'application en France du système de sécurité de l'Organisation du traité de l'Atlantique nord, version en vigueur. *Disponible sur <https://legifrance.gouv.fr>.*
11. Guide - Méthode de gestion de risques EBIOS Risk Manager. *Disponible sur <https://www.cyber.gouv.fr>.*
12. Guide - L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. *Disponible sur <https://cyber.gouv.fr>.*
13. *Guide - Guide d'hygiène informatique, ANSSI, version en vigueur. Disponible sur <https://cyber.gouv.fr>.*
14. Guide – Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte – version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
15. Guide - Recommandations de sécurité pour l'architecture d'un système de journalisation, ANSSI-PA-012/ANSSI/SDE, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
16. Loi relative à la programmation militaire, version en vigueur. *<https://www.legifrance.gouv.fr>.*

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	33/49

17. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. *Disponible sur <https://eur-lex.europa.eu>.*
18. Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. *Disponible sur <https://eur-lex.europa.eu>.*
19. Référentiel général de sécurité, version en vigueur. *Disponible sur <https://legifrance.gouv.fr>.*
20. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. *Disponible sur <https://eur-lex>.*
21. Guide - Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
22. Instruction interministérielle n° 910 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, version en vigueur. *Disponible sur <https://www.legifrance.gouv.fr>.*
23. Guide - Crise d'origine Cyber, les clés d'une gestion opérationnelle et stratégique, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
24. Guide - Anticiper et gérer sa communication de crise cyber, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
25. Guide - Guides de remédiation d'incidents de sécurité, volet stratégique, volet opérationnel, volet technique – version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
26. Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	34/49

Annexe 2 Missions et compétences attendues du personnel du prestataire

Cette annexe décrit les connaissances, compétences et missions des personnels du prestataire.

Les connaissances de la réglementation citées en chapitre I sont complétées par les missions et compétences spécifiques requises pour chaque profil de personnel décrites aux chapitres suivants de la présente annexe.

Pour être qualifié, le prestataire doit disposer par activité de réponse des profils suivants :

Activité	Profil(s)
REC	Analyste réseau et/ou analyste système
INV	Analyste réseau et/ou analyste système
CODE	Analyste de codes malveillants
PCI	Pilote d'investigation

I. Connaissance de la réglementation

Les analystes et pilotes d'investigation doivent connaître les réglementations suivantes :

- la protection du secret de la défense nationale (2) ;
- la protection des systèmes d'informations sensibles (1) ;
- la loi de programmation militaire (16) et particulièrement les dispositions applicables aux systèmes d'information d'importance vitale (SIIV) des opérateurs d'importance vitale (OIV) ;
- les directives européennes relatives à la sécurité des réseaux et de l'information (17) et (18) ;
- le référentiel général de sécurité (19) ;
- le règlement général sur la protection des données (20) ;
- la protection des informations classifiées de l'Organisation du traité de l'Atlantique nord (OTAN) (10) ;
- la protection des informations classifiées de l'Union européenne (UE) (9).

II. Responsable d'équipe

Ce chapitre décrit les missions et compétences du responsable d'équipe.

II.1. Missions

Le responsable d'équipe doit être capable d'assurer les missions suivantes :

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	35/49

- définir et mettre en œuvre une organisation adaptée aux objectifs, critères, périmètre et activités de réponse ;
- constituer et gérer l'équipe de réponse aux incidents composée d'analystes, et le cas échéant d'experts et de pilotes d'investigation ;
- définir et gérer les priorités de la prestation ;
- organiser les réunions de restitution à chaud ;
- organiser la réunion de clôture de la prestation ;
- contrôler la qualité et valider les livrables de la prestation, notamment la note de cadrage et le rapport d'analyse, en particulier la synthèse managériale.

II.2. Compétences

Le responsable d'équipe doit disposer des compétences suivantes :

- synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- rédiger des livrables adaptés à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.).

III. Pilote d'investigation

Ce chapitre décrit les missions et compétences du pilote d'investigation.

III.1. Missions

Le pilote d'investigation doit être capable d'assurer les missions suivantes :

- définir et gérer les priorités de la prestation, en particulier en situation de crise ;
- piloter et contrôler les activités des membres de l'équipe de réponse aux incidents ;
- proposer et accompagner le commanditaire dans la définition et la mise en œuvre de mesures de précaution en amont des actions de réponse aux incidents ;
- proposer et mettre en œuvre une démarche de réponse aux incidents de sécurité adaptée aux objectifs, critères, périmètre et activités de réponse ;
- proposer une posture initiale et la réviser en tant que de besoin durant la prestation ;
- élaborer et tenir à jour la compréhension de l'incident de sécurité ;
- maintenir à jour un état de la situation des opérations (collectes, recherche, analyses) et de la compromission et présenter l'information utile à chaque échelon (comité technique, comité stratégique, etc.) ;
- accompagner le commanditaire dans l'évaluation des impacts métier associés à l'incident de sécurité ;
- accompagner le commanditaire dans la mise en place de solutions de collecte et d'analyse d'événements système et réseau ;

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	36/49

- accompagner le commanditaire dans la définition et la mise en œuvre d'une politique de journalisation des événements système et réseau ;
- accompagner le commanditaire dans la définition et la mise en œuvre de mesures d'endiguement ;
- rédiger les parties du rapport d'analyse qui le concernent, en particulier la synthèse managériale ;
- participer aux réunions de restitution à chaud ;
- participer à la réunion de clôture de la prestation ;

III.2. Compétences

Le pilote d'investigation 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*, rançongiciels, infrastructures de commande et de contrôle, etc. ;
- les références pour la représentation des indicateurs de compromission : *Structured Threat Information eXpression*, *OpenIOC*, etc. ;
- les architectures des systèmes d'information, leurs vulnérabilités et leurs mécanismes d'administration ;
- les principaux systèmes d'exploitation et solutions de virtualisation, leurs vulnérabilités et leur sécurisation ;
- les protocoles et architectures réseau, leurs vulnérabilités et leur sécurisation ;
- les applications, leurs vulnérabilités et leur sécurisation : applications bureautiques, serveurs Web, bases de données, serveurs de messagerie, progiciels, etc. ;
- les outils d'analyse : analyse système (antivirus, mémoire, disques), analyse de journaux (signature, réseau, système, applicatif ou réseau), analyse statique et dynamique de programmes.

IV. Analyste système

Ce chapitre décrit les missions et compétences de l'analyste système.

IV.1. Missions

L'analyste système doit être capable d'assurer les missions suivantes :

- assimiler une vision globale du système d'information afin d'identifier :
 - o les vulnérabilités système exploitables et les chemins d'attaque associés ;
 - o les points terminaux nécessitant une collecte de données (serveurs d'infrastructure, postes d'administrations et postes utilisateur, serveurs métier, etc.) ;

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	37/49

- recueillir à l'échelle du système d'information un volume important d'informations techniques (système de fichiers, configuration, journaux système et applicatifs, etc.) d'un large ensemble de systèmes informatiques et en assurer l'analyse ;
- réaliser la recherche d'indicateurs de compromission ;
- réaliser une copie physique / mémoire de terminaux (poste de travail, poste nomade, etc.), de serveurs (serveur d'infrastructure, serveur applicatif, etc.) et de supports amovibles (clé USB, disque externe, etc.) susceptibles d'avoir participé à un scénario d'attaque et en assurer l'analyse ;
- soutenir le commanditaire dans la mise en place de solutions de collecte et d'analyse de journaux adaptées à l'architecture cible, afin de pouvoir suivre les activités de l'attaquant ;
- soutenir le commanditaire dans la définition d'une politique de journalisation système (types d'événements, durées de rétention, etc.) par type d'équipement ;
- soutenir le commanditaire dans le développement de règles de corrélation d'événements système ;
- extraire des indicateurs de compromission à des fins d'analyse et de supervision ;
- analyser l'ensemble des relevés techniques recueillis (images disques, images mémoire, journaux d'événements, alertes, traces système, réseau et applicatives, ...) pour qualifier la cause de l'incident, le mode opératoire de l'attaque, les vulnérabilités exploitées, l'étendue de la compromission et les activités malveillantes ;
- réaliser la caractérisation des fichiers (binaires et documents) afin d'identifier leur potentiel caractère malveillant (vérification des en-têtes, vérification via logiciel antivirus, analyse d'exécution dans un système isolé, etc.) ;
- soutenir le commanditaire sur les mesures d'endiguement à mettre en place ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'analyse.

IV.2. Compétences

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

- le fonctionnement, la sécurisation et les vulnérabilités des principaux systèmes d'exploitation et solutions de virtualisation les plus répandues ;
- les applications et leurs vulnérabilités : application bureautique, navigateur Internet, serveur Web, base de données, serveurs de messagerie, progiciels, etc. ;
- les attaques et activités malveillantes : exploitation de vulnérabilités, portes dérobées, *rootkit*, *botnet*, infrastructure de commande et de contrôle, *obfuscation*, etc. ;
- les outils d'analyse : analyse de systèmes (artefacts, mémoire, disques, système de fichiers, séquence de démarrage), analyse de journaux (système, applicatif ou réseau), analyse statique et dynamique de programmes et documents, etc. ;
- les journaux d'événements système, réseau et applicatifs ;

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	38/49

- les solutions de collectes (notamment journalisation et copie) ;
- les solutions d'analyse de journaux ou de supervision de la sécurité (SIEM) ;
- les protocoles et architectures réseau, leurs vulnérabilités et leur sécurisation ;
- les langages de programmation de bas niveau (C, assembleur, etc.) et langages de scripts (Python, Perl, PowerShell, etc.).

V. Analyste réseau

Ce chapitre décrit les missions et compétences de l'analyste réseau.

V.1.Missions

L'analyste réseau doit être capable d'assurer les missions suivantes :

- assimiler une vision globale du système d'information et de son architecture, identifier les points potentiels d'infiltration/exfiltration et les points de collecte associés (composants réseau, produits de sécurité, etc.) ;
- soutenir le commanditaire dans l'identification des attaques à détecter ;
- réaliser la recherche d'indicateurs de compromission ;
- soutenir le commanditaire dans la mise en place de solutions de collecte et d'analyse de journaux réseau adaptées à l'architecture cible, à des fins de supervision de circonstance ;
- soutenir le commanditaire dans la définition d'une politique de journalisation réseau (types d'événements, durées de rétention, etc.) par type d'équipement (nœuds d'interconnexion, passerelles Internet, équipements de sécurité, etc.) (15) et au développement de règles de corrélation d'événements réseau ;
- soutenir le commanditaire dans la conception et à la mise en place de solutions de détection d'attaques informatiques et au développement de règles de corrélation d'évènements ;
- analyser et interpréter les informations techniques collectées (journaux, alertes) : vulnérabilités exploitées, chemins d'attaque, etc. ;
- extraire des indicateurs de compromission à des fins d'analyse et de supervision ;
- réaliser la caractérisation des fichiers (binaires et documents) afin d'identifier leur potentiel caractère malveillant (vérification des en-têtes, vérification via logiciel antivirus, analyse d'exécution dans un système isolé, etc.) ;
- soutenir le commanditaire sur les mesures d'endiguement à mettre en place ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'analyse.

V.2. Compétences

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

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	39/49

- 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*, infrastructure de commande et de contrôle, *obfuscation*, etc. ;
- l'analyse de journaux d'événements système, réseau et applicatifs ;
- mises en miroir d'équipements réseaux (physiques ou virtualisés) et notamment l'implémentation de TAP – *Test Access Point*.
- les solutions d'analyse de journaux ou de supervision de la sécurité (SIEM) ;
- les sondes de détection d'intrusions et outils de corrélation de journaux d'événements ;
- les langages de programmation et de scripts (Python, Perl, PowerShell, etc.).

VI. Analyste de codes malveillants

Ce chapitre décrit les missions et compétences de l'analyste de codes malveillants.

VI.1. Missions

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

- les caractéristiques du code malveillant (empreinte cryptographique, taille du code malveillant, version du système d'exploitation cible concerné, éléments caractéristiques, etc.), la famille ou la catégorie à laquelle appartient le code malveillant (*dropper*, *loader*, *Remote Access Trojan*, *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 (p. ex. : fichier, mémoire, matériel, etc.) ;
- la phase d'exécution du code malveillant (p. ex. : exploitation d'une vulnérabilité, téléchargement d'un autre code malveillant, installation de *rootkit*, etc.) ;
- les dépendances vis-à-vis de l'environnement compromis (présence d'un fichier de configuration, utilisation d'un fichier de données, copie de la mémoire dans le cas d'une exécution en mémoire, etc.) ;
- la synthèse des fonctionnalités principales du code malveillant (récupération de données bancaires, exfiltration de fichiers, récupération de données techniques, etc.) ;
- les capacités techniques du code malveillant, par exemple :
 - o la collecte des données techniques (système et/ou réseau) ou des données métier (fichiers, frappes du clavier, mots de passe, etc.) ;
 - o 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

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	40/49

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 (p. ex. : exploitation d'une vulnérabilité, utilisation d'un compte avec un mot de passe subtilisé, etc.) ou par support amovible (p. ex. : clé USB) ;
- l'élévation de privilèges (p. ex. : obtenir des privilèges supplémentaires, voire d'administration, sur le système compromis via l'exploitation de vulnérabilités) ;
- la protection contre la collecte (falsification des activités sur un système compromis, effacement de journaux, modification des dates de fichiers, etc.) ;
- la protection contre l'analyse. Il peut s'agir de protection statique (brouillage ou chiffrement du code, complication du fonctionnement, etc.) ou dynamique (détection d'un antivirus ou d'un environnement d'analyse, etc.) ;
- le niveau d'autonomie (p. 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 ou la mise en place d'une infrastructure de commande et contrôle. 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 antivirusales ;
- analyser dynamiquement le code pour en extraire les comportements ;
- réaliser une rétro-conception du code et de ses composants ;
- identifier et extraire des indicateurs de compromission.

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

Il doit proposer des méthodes de détection et de protection, extraire des indicateurs de compromission à des fins de supervision, 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 d'infrastructure de commande et de contrôle, motifs, etc.

VI.2. Compétences

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

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	41/49

- 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 et solutions de virtualisation les plus répandues ;
- les applications et leurs vulnérabilités : application bureautique, navigateur Internet, serveur Web, base de données, serveurs de messagerie, progiciels, etc. ;
- les outils et solutions de rétro-ingénierie (désassembleurs, dé-compilateurs, etc.) ;
- les attaques et activités malveillantes : exploitation de vulnérabilités, portes dérobées, *rootkit*, *botnet*, infrastructure de contrôle et de commande, 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.).

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	42/49

Annexe 3 Recommandations à l'attention 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 autorité administrative ou un opérateur d'importance vitale, demander à l'ANSSI de participer à la définition du cahier des charges d'un appel d'offres ou d'un contrat en matière de réponse aux incidents de sécurité.
- b) Il est recommandé que le commanditaire utilise le guide (21) pour rédiger le cahier des charges d'un appel d'offres ou d'un contrat en matière de réponse aux incidents de sécurité.
- c) Le commanditaire peut consulter le catalogue des prestataires de services qualifiés sur le site de l'ANSSI. Ce catalogue présente pour chaque prestataire les activités pour lesquelles il est qualifié, la période de validité de la qualification, le niveau de qualification et le niveau de recommandation.
- d) Les prestataires qualifiés gardent la faculté de réaliser des prestations non qualifiées mais ne peuvent dans ce cas se prévaloir de la qualification sur ces prestations. Le commanditaire doit donc, s'il souhaite bénéficier d'une prestation qualifiée, c'est-à-dire conforme aux exigences du présent référentiel, s'assurer que la convention de service établie avec le prestataire indique explicitement que la prestation est qualifiée.
- e) Une prestation non qualifiée, c'est-à-dire ne respectant pas les exigences du présent référentiel, expose le commanditaire à certains risques, notamment la compromission d'informations confidentielles, la perte ou l'indisponibilité du système d'information objet de la prestation. Le recours à une prestation qualifiée permet de réduire ces risques. Si toutefois le commanditaire ne souhaite pas recourir à une prestation qualifiée, il est néanmoins recommandé qu'il demande au prestataire un document identifiant l'ensemble des exigences du présent référentiel non satisfaites dans le cadre de sa prestation afin de connaître les risques auxquels il s'expose.
- f) Le commanditaire peut, conformément au processus de qualification d'un service (7), déposer auprès de l'ANSSI une réclamation lorsqu'il estime que le prestataire n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée. La réclamation peut également être déposée directement auprès du prestataire qualifié qui a l'obligation d'en informer sans délai l'ANSSI.

S'il s'avère, après instruction de la réclamation, que le prestataire qualifié n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée, la qualification du prestataire peut être retirée, la portée de qualification réduite, ou le niveau de recommandation du prestataire dégradé conformément au processus de qualification d'un service (7).

- g) Sauf si le commanditaire est soumis à une obligation légale, réglementaire ou contractuelle, le choix du niveau de qualification de la prestation relève exclusivement du commanditaire. Dans ce cas, il est recommandé que le niveau de qualification de la prestation qualifiée soit déterminé à l'aide d'une approche par les risques.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	43/49

Il est recommandé qu’une prestation de niveau élevé soit réalisée lorsque les risques qui pèsent sur le système d’information objet de la prestation sont élevés et/ou lorsque les scénarios de risque de nature intentionnelle impliquent des menaces stratégiques. Dans les autres cas, une prestation de niveau substantiel devrait suffire.

De ce fait, dans le cadre d’une prestation qualifiée au niveau élevé, il est recommandé que le commanditaire exige du prestataire dans la note de cadrage que le rapport d’analyse porte la mention Diffusion Restreinte.

h) Lorsque le système d’information objet de la prestation relève de la sécurité nationale, le commanditaire doit réaliser une prestation qualifiée pour les besoins de la sécurité nationale, c’est-à-dire conforme, en sus des exigences pour le niveau élevé du présent référentiel, aux exigences du référentiel (8).

i) La qualification d’un prestataire n’atteste pas de sa capacité à accéder ou à détenir des informations classifiées et par conséquent ne se substitue pas à l’habilitation d’une personne morale ou physique au titre de l’instruction (2).

Lorsque la prestation requiert que le prestataire accède ou détienne des informations classifiées, le commanditaire doit vérifier que le prestataire et son personnel respectent les principes régissant l’accès des personnes morales et physiques au secret de la défense nationale.

j) La qualification d’un prestataire n’atteste pas de sa capacité à accéder ou à détenir des articles contrôlés de la sécurité des systèmes d’information (ACSSI) (22).

Lorsque la prestation requiert que le prestataire accède ou détienne des articles contrôlés de la sécurité des systèmes d’information, le commanditaire doit vérifier que le prestataire dispose des décisions d’accès aux ACSSI (DACSSI) pour les ACSSI classifiés ou des attestations de formation à la manipulation des ACSSI pour les ACSSI non classifiés.

k) Il est recommandé que le commanditaire détermine les objectifs, périmètre et activités de la prestation en utilisant une approche par les risques.

l) Il est recommandé que le commanditaire demande au prestataire de lui fournir des références de prestations réalisées dont les objectifs, périmètre et activités sont proches de ceux souhaités par le commanditaire.

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

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

o) Le prestataire doit proposer une charge adaptée aux objectifs, critères, périmètre et activités cependant la charge in fine retenue relève exclusivement du commanditaire. Le prestataire mentionnera dans le rapport les éventuelles réserves quant à la prestation pouvant avoir un impact sur les résultats de la prestation notamment en cas d’inadéquation entre la charge d’une part et les objectifs, périmètre et activités d’autre part.

Prestataires de réponse aux incidents de sécurité – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	44/49

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 de la charge et des moyens associés (personnels, budget, etc.). La charge, la durée et les moyens de la prestation peuvent être révisés au cours de la prestation en fonction de la compréhension de l'incident de sécurité ou de l'incident de sécurité lui-même. Une prestation de réponse aux incidents peut durer plusieurs semaines, voire plusieurs mois.

- p) Afin de réduire la charge de la prestation et donc son coût tout en répondant aux objectifs de la prestation, le prestataire peut proposer au commanditaire de réaliser un échantillonnage en utilisant une approche par les risques.
- q) Le commanditaire doit désigner en son sein un correspondant de la prestation dont le rôle est d'établir et tenir à jour, en collaboration avec le prestataire, la note de cadrage de la prestation. Le correspondant de la prestation gère la relation avec le prestataire et veille à la bonne exécution de la prestation en s'assurant que la convention de service et la note de cadrage sont respectées.

Il est recommandé que le correspondant de la prestation au sein du commanditaire dispose des moyens lui permettant d'engager la responsabilité du commanditaire et de répondre rapidement aux demandes du prestataire.

- r) Il est recommandé que le commanditaire dispose d'un dispositif de gestion de crise d'origine cyber. Ce dispositif permet au commanditaire de disposer d'une gouvernance de gestion de crise d'origine cyber et des moyens associés (organisation, politiques, procédures, outils, etc.) afin d'être en mesure d'apporter une réponse stratégique et opérationnelle durant la crise. Il comprend également la communication de crise, une prise en compte des aspects juridiques et potentiellement assurantiels.

Il est recommandé que le commanditaire fasse appel à une prestation qualifiée de conseil et d'accompagnement en préparation à la gestion de crise d'origine cyber réalisée par un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) qualifié pour concevoir un dispositif de gestion de crise d'origine cyber, ou faire évoluer ou revoir un dispositif existant.

Si le commanditaire ne dispose pas d'un dispositif de gestion de crise d'origine cyber préexistant, alors il est recommandé que le correspondant de la prestation au sein du commanditaire mette en place une structure projet disposant du niveau de décision adéquat et permettant d'assurer une chaîne de décision courte, rapide et simplifiée de l'ensemble des processus nécessaires à la bonne exécution de la prestation : achat, communication, etc. Il est indispensable que la direction du commanditaire soit représentée dans cette structure.

Il est recommandé que le commanditaire s'appuie sur le guide (23) pour gérer une crise d'origine cyber et le guide (24) pour gérer la communication de crise.

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

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	45/49

- t) Il est recommandé que le commanditaire informe le prestataire de toutes les actions (administration, maintenance, etc.) prévues ou en cours sur le système d'information afin de ne pas perturber la prestation de réponse aux incidents.
- u) Il est recommandé que le commanditaire mette en place des procédures d'urgence, parfois appelées procédures « bouton-rouge », afin d'isoler rapidement le système d'information cible en cas de besoin.

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 4 afin de lui permettre d'acquérir rapidement une compréhension initiale du système d'information cible et de l'incident de sécurité.
- b) Il est recommandé que le commanditaire mette à disposition du prestataire une zone sécurisée et dédiée pour le stockage (coffre-fort, salle surveillée, etc.) des informations et supports sensibles relatifs à la prestation. Cette zone doit respecter les contraintes réglementaires associées au niveau de sensibilité ou de classification des informations et supports stockés.
- c) Il est recommandé que le commanditaire mette à disposition du prestataire les moyens techniques (matériels, équipements, connexions, etc.) dont il a besoin pour sa prestation, et que ces moyens constituent un environnement d'analyse sécurisé et déconnecté du système d'information cible.
- d) Il est recommandé que le commanditaire mette en œuvre des moyens de communication sécurisés et dédiés pour tous les échanges relatifs à incident de sécurité, en interne et en externe, notamment avec le prestataire. Il est recommandé que ces moyens soient déconnectés du système d'information cible afin de ne pas permettre à l'attaquant d'obtenir des informations relatives à la prestation en cours.
- e) Dans le cadre d'une prestation qualifiée au niveau substantiel réalisée par un prestataire qualifié au niveau élevé, il est recommandé que le commanditaire, dans la note de cadrage, exige que le prestataire traite l'ensemble des informations et supports relatifs à la prestation sur son système d'information homologué Diffusion Restreinte et ce quel que soit le marquage de ces informations et supports.
- f) Il est recommandé que le commanditaire trace et informe le prestataire de toutes les opérations qu'il réalise sur le système d'information cible durant la prestation (opérations d'administration, sauvegarde, restauration, etc.) afin de permettre au prestataire d'identifier les actions illégitimes réalisées par l'attaquant.
- g) Il est recommandé que le commanditaire, dès lors que la prestation nécessite l'installation d'un outil ou l'exécution d'une commande sur le système cible, réalise lui-même ces actions ou, à défaut, autorise le prestataire à réaliser ces actions avec des comptes dédiés bénéficiant du principe du moindre privilège et sous la supervision constante du commanditaire.
- h) Il est recommandé que le commanditaire crée des comptes permettant au prestataire de réaliser les opérations de collecte. Ces comptes doivent être dédiés, bénéficier du principe du moindre privilège et, dans la mesure du possible, démarqués et respecter la politique de nommage du commanditaire afin de ne pas éveiller l'attention de l'attaquant.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	46/49

III. Après la prestation

- a) Il est recommandé que le commanditaire, en se fondant sur le rapport d'analyse élaboré par le prestataire de réponse aux incidents de sécurité, élabore un plan d'actions pour la remédiation de l'incident de sécurité en s'appuyant le guide (25).
- b) Il est recommandé que le commanditaire fasse appel à une prestation qualifiée de conseil et d'accompagnement en préparation à la gestion de crise d'origine cyber réalisée par un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) qualifié pour concevoir un dispositif de gestion de crise d'origine cyber, ou faire évoluer ou revoir un dispositif existant.
- a) Il est recommandé que le commanditaire fasse appel à une prestation de conseil et d'accompagnement qualifiée réalisée par un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) qualifié pour accompagner le commanditaire afin de rétablir son système d'information, améliorer le niveau de sécurité et ainsi limiter l'occurrence d'un nouvel incident de sécurité.
- b) Il est recommandé que le commanditaire fasse appel à une prestation d'audit qualifiée réalisée par un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié pour contrôler le niveau de sécurité du système d'information cible après la mise en œuvre d'un plan de remédiation.
- c) Il est recommandé que le commanditaire fasse appel à une prestation qualifiée réalisée par un prestataire de détection des incidents de sécurité (PDIS) qualifié afin de détecter au plus tôt l'occurrence d'un nouvel incident de sécurité.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	47/49

Annexe 4 Prérequis à fournir par les commanditaires

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

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

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	48/49

- les éventuels rapports d'incidents précédents ;
- les éventuelles procédures d'urgence déjà existantes.

Prestataires de réponse aux incidents de sécurité – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
3.0	28/07/2024	PUBLIC	49/49