Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de détection des incidents de sécurité

Référentiel d'exigences

Version 2.0 du 21 décembre 2017

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
20/03/2014	0.1	*Version préliminaire présentée en GT1*	ANSSI
16/04/2014	0.2	*Version préliminaire présentée en GT2*	ANSSI
03/06/2014	0.3	*Version de travail en prévision du GT3*	ANSSI
25/06/2014	0.4	*Version de travail en prévision du GT4*	ANSSI
22/07/2014	0.5	*Version de travail en prévision du GT5*	ANSSI
05/09/2014	0.6	*Version de travail en prévision du GT6*	ANSSI
10/10/2014	0.7.4	*Version préliminaire de travail en prévision de la relecture interne ANSSI*	ANSSI
25/11/2014	0.8	*Version préliminaire de travail en prévision de la relecture interne ANSSI*	ANSSI
17/12/2014	0.9.1	*Version publiée pour appel public à commentaires*	ANSSI
6/10/2015	1.0	*Version révisée suite à l'appel à commentaires*	ANSSI
10/02/2017	1.01	*Version de travail en prévision du GT3 de revue du référentiel*	ANSSI
10/05/2017	1.02	*Version de travail en prévision du GT4 de revue du référentiel*	ANSSI
08/06/2017	1.03	*Version préliminaire de travail en prévision de la relecture interne ANSSI*	ANSSI
21/12/2017	2.0	*Première version applicable.* Modifications principales : • Précisions apportées aux modalités de qualification • Précisions apportées aux exigences de protection de l'information • Précisions apportées au périmètre des contrôles • Ajout de nouvelles possibilités de communication • Revue complète des indicateurs qualité	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

qualification@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

L'interconnexion croissante des réseaux et les besoins de dématérialisation exposent les systèmes d'information à des cyberattaques. Ainsi les points d'interconnexion avec l'extérieur et en particulier avec internet sont autant d'accès qu'un attaquant peut tenter d'exploiter pour s'introduire et se maintenir au sein d'un système d'information pour dérober, dénaturer ou détruire son patrimoine informationnel.

L'exploitation de systèmes de détection d'incidents de sécurité concourt à la protection d'un système d'information face aux menaces de cyberattaques. Les moyens humains, techniques et organisationnels peuvent se concentrer au sein d'un centre opérationnel de cybersécurité[1] dédié à la détection des incidents de sécurité. En fonction des enjeux, des besoins et des ressources du commanditaire, ce centre peut être interne[2] ou externe[2]. Dans ce dernier cas, la mutualisation peut avoir des effets vertueux comme le partage de la connaissance de la menace et de règles de détection.

Lorsqu'un centre opérationnel de cybersécurité se conforme à l'état de l'art, notamment en termes de compétence métier et d'outillage, et est adapté finement aux besoins du commanditaire il permet de prévenir des incidents de sécurité graves ou lorsqu'ils surviennent d'en limiter les conséquences, en permettant des actions de remédiation rapides pouvant être menées par un prestataire de réponse aux incidents de sécurité (PRIS) qualifié.

La concentration et l'éventuelle mutualisation des moyens de détection font d'un centre opérationnel de cybersécurité une cible de choix pour des attaquants. Par conséquent la protection de son infrastructure doit faire l'objet d'une attention toute particulière.

I.1.2. Objet du document

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

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

Il couvre les deux typologies de services de détection des incidents de sécurité : interne et externe.

Il permet au commanditaire de la prestation de disposer de garanties sur les compétences du prestataire et de son personnel, sur la qualité des prestations de détection des incidents de sécurité réalisées et sur la confiance que le commanditaire peut accorder au prestataire, notamment en matière de confidentialité.

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

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

[1] Ci-après nommé « service de détection des incidents de sécurité ».

[2] Voir chapitre III.1 Modalités de la qualification.

I.1.3. Structure du présent document

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

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

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

Le chapitre IV présente les exigences que les prestataires qualifiés doivent respecter.

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

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

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

L'Annexe 4 présente les schémas illustratifs d'architectures conformes au référentiel.

L'Annexe 5 présente les règles relatives à l'utilisation d'un agrégateur de flux.

I.2. Identification du document

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

I.3. Définitions et acronymes

I.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont :

ANSSI	Agence nationale de la sécurité des systèmes d'information
CERT-FR	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques[3]
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PDIS	Prestataire de détection des incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité

I.3.2. Définitions

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

Administrateur – membre du service de détection disposant de droits privilégiés lui permettant d'assurer le bon fonctionnement des dispositifs du service de détection.

Commanditaire – entité faisant appel au service de détection des incidents de sécurité.

Contexte d'un incident de sécurité – pour un incident de sécurité, les évènements associés ainsi que l'ensemble des informations analysées et produites lors de sa qualification (exemple : rapport(s) d'analyse(s) de qualification).

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

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

Collecteur – dispositif permettant la centralisation des évènements de sécurité en provenance des sources de collecte (exemple : serveur *syslog*, collecteur d'une solution SIEM …). Dans le cadre de ce service, les collecteurs locaux correspondent aux collecteurs déployés sur le système d'information du commanditaire, et les collecteurs centraux correspondent aux collecteurs de centralisation des évènements déployés sur le système d'information du prestataire.

Efficacité – niveau de réalisation des activités planifiées et d'obtention des résultats escomptés.

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

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

Gravité d'un incident de sécurité – niveau d'impact de l'incident de sécurité sur le système d'information du commanditaire.

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

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

Notification – action d'informer le commanditaire de l'occurrence d'un incident de sécurité portant atteinte à son système d'information.

Opérateur – membre du service de détection en charge de l'exploitation du service, c'est-à-dire de la réalisation des tâches liées à la détection constitutives de la prestation pour le compte du commanditaire.

Périmètre supervisé – tout ou partie du système d'information du commanditaire, objet de la prestation de détection des incidents de sécurité.

Prestataire – entité proposant une offre de service de détection des incidents de sécurité conforme au référentiel.

Prestation qualifiée – service de détection des incidents de sécurité conforme au référentiel, fourni à un commanditaire.

Qualification d'un incident de sécurité – détermination de la nature et de la gravité d'un incident de sécurité.

Règle de détection – liste d'éléments techniques permettant d'identifier un incident à partir d'un ou de plusieurs évènements. Une règle de détection peut être un ou des marqueurs, une ou des signatures ou une règle comportementale basée sur un comportement défini comme anormal. Une règle de détection peut provenir de l'éditeur des outils techniques d'analyse utilisés pour le service de détection, du prestataire (veille sur de nouveaux incidents, règle utilisée pour un autre commanditaire avec son accord, etc.), d'un partenaire, d'un fournisseur spécialisé, ou encore avoir été créée spécifiquement pour répondre à un besoin du commanditaire.

Risque lié à la sécurité de l'information – Scénario décrivant l'effet de l'incertitude sur l'activité et exprimé en une combinaison des conséquences d'un événement lié à la sécurité de l'information et de sa probabilité d'occurrence.

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

Sonde ou **Système de détection** – dispositif technique destiné à repérer des activités anormales, suspectes ou malveillantes sur le périmètre supervisé. Une sonde a pour but de générer des évènements de sécurité et est considérée comme une source de collecte dans le cadre du service de détection des incidents de sécurité.

Source de collecte – équipement au sein du système d'information générant des évènements liés à la sécurité de l'information.

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

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

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

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

II. Description générale du service de détection

II.1. Activités du service de détection des incidents de sécurité

Le service de détection des incidents de sécurité est composé de trois activités distinctes :

- la gestion des incidents, correspondant à l'ensemble des moyens techniques et organisationnels permettant d'identifier et de qualifier un incident de sécurité sur la base d'évènements collectés. Le stockage et la capitalisation des incidents de sécurité dans un but d'amélioration du service font aussi partie de cette activité ;
- la gestion des évènements, correspondant à l'ensemble des moyens techniques et organisationnels assurant le recueil et le stockage des évènements de sécurité ;
- la gestion des notifications, correspondant à l'ensemble des moyens techniques et organisationnels permettant d'informer le commanditaire sur les incidents de sécurité détectés et de stocker ces notifications.

Les activités de réaction et de remédiation sont hors périmètre du service. Elles sont traitées par les prestataires de réponse aux incidents de sécurité (PRIS).

II.2. Architecture du système d'information du service de détection

Le présent document n'impose aucune architecture pour le système d'information du service de détection. Plusieurs implémentations sont envisageables. En particulier, selon la typologie du service de détection (interne ou externe), les différentes zones présentées dans ce chapitre peuvent être hébergées au sein d'entités voire d'organismes différents, tant que les exigences du référentiel sont respectées.

Le schéma ci-dessous est une représentation simplifiée d'une architecture type du service de détection des incidents de sécurité, donnée uniquement à titre d'illustration. L'Annexe 4 présente d'autres représentations plus détaillés.

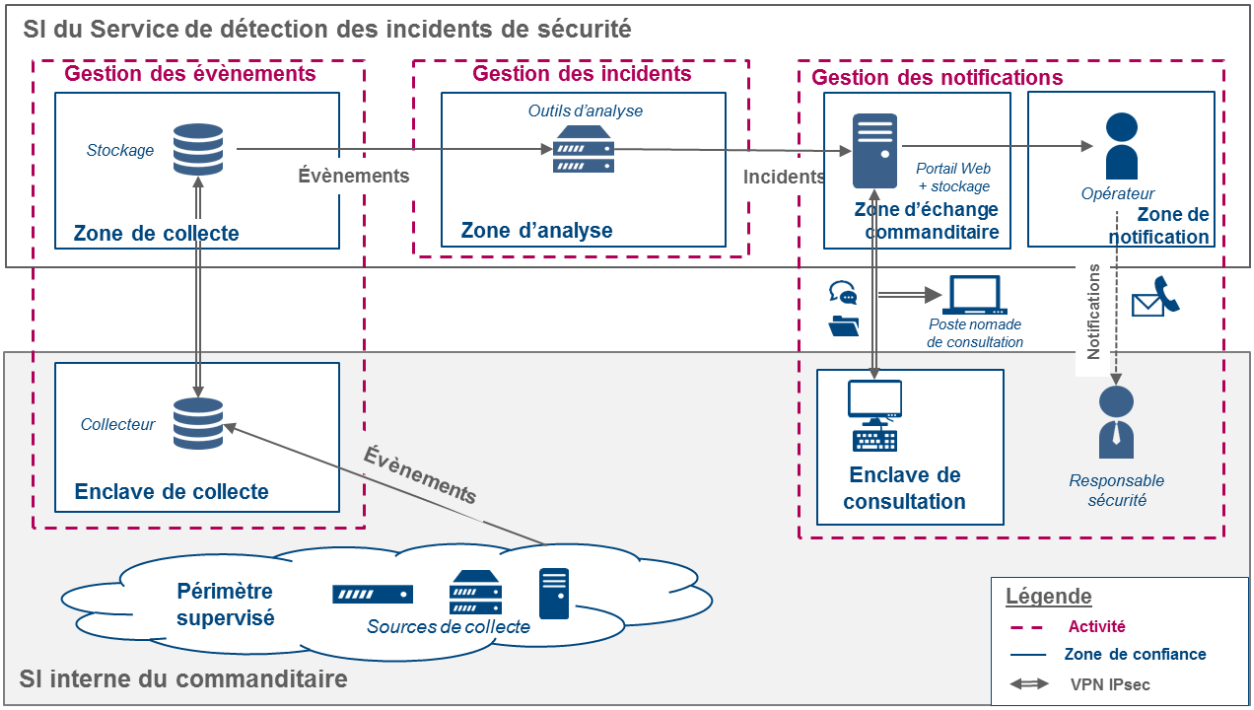


Figure 1 : Représentation simplifiée d'une architecture type du service de détection des incidents de sécurité

Le système d'information du service de détection est organisé en zones de confiance, cloisonnées entre elles par des mécanismes de filtrage, d'authentification et de contrôle d'accès. Les zones de confiance du système d'information du service de détection sont les suivantes :

- zone(s) de collecte (une ou plusieurs), regroupant l'ensemble des dispositifs impliqués dans le processus de collecte, notamment les collecteurs centraux et les systèmes de stockage des évènements et, le cas échéant, des informations contextuelles ;
- zone(s) d'analyse, regroupant l'ensemble des dispositifs impliqués dans le processus d'analyse, notamment les outils techniques d'analyse des incidents de sécurité ;
- zone(s) de notification, regroupant les systèmes de notification à destination du commanditaire, notamment les systèmes de messagerie ;
- zone(s) d'échange commanditaire, regroupant l'ensemble des dispositifs permettant au commanditaire de consulter le détail des informations concernant les incidents notifiés, notamment le portail web, et d'apporter le cas échéant des informations nécessaires à la qualification de l'incident ;
- zone(s) d'administration regroupant l'ensemble des outils d'administration et les postes d'administration ;
- zone(s) de mise à jour, regroupant les dispositifs impliqués dans le processus de téléchargement des mises à jour des dispositifs du service de détection ;
- zone(s) d'exploitation, regroupant les postes de travail des opérateurs ;
- zones d'échange, distinctes entre les administrateurs et les opérateurs, regroupant les dispositifs permettant le transfert de fichiers avec l'extérieur du système d'information du service de détection des incidents de sécurité ;

Par ailleurs plusieurs zones particulières, externes au système d'information du service de détection, doivent être mises en place (car en interaction avec celui-ci) :

- zone(s) internet, regroupant les postes mis à disposition des opérateurs et administrateurs du service de détection pour accéder à Internet ou à d'autres systèmes d'information que celui du service ;
- des zones particulières mises en place au sein du système d'information interne du commanditaire, ci-après dénommées « enclaves ». Au minimum, deux enclaves devront être mises en place :
    - une enclave de collecte pour l'hébergement des dispositifs de collecte du service de détection déployés chez le commanditaire. En particulier, l'enclave de collecte contient un ou plusieurs collecteurs locaux dont le rôle est de centraliser les évènements de sécurité issus du périmètre supervisé ;
    - une enclave de consultation pour l'hébergement des dispositifs accédant à la zone d'échange commanditaire.

Un schéma plus complet, représentant toutes ces zones, et respectant les exigences de cloisonnement attendues, est proposé en Annexe 4.

II.3. Périmètre d'application des exigences du référentiel

Le chapitre IV.1 liste des exigences générales relatives aux obligations juridiques du prestataire, notamment ses devoirs vis-à-vis du commanditaire, ses garanties, etc.

Le chapitre IV.2 liste les exigences relatives aux activités du service de détection des incidents de sécurité :

- les exigences relatives à l'activité de gestion des incidents portent notamment sur les compétences des opérateurs, les fonctionnalités des outils utilisés, l'implémentation de règles de détection, etc.
- les exigences relatives à l'activité de gestion des évènements portent notamment sur les sources de collecte, la centralisation des évènements sur un collecteur, etc.
- les exigences relatives l'activité de gestion des notifications portent notamment sur les moyens de notification, la consultation des tickets d'incident, etc.

Le chapitre IV.3 liste les exigences relatives à la protection de l'information, notamment le chiffrement, le filtrage entre les zones de confiance, la séparation des rôles entre administrateurs et opérateurs, etc.

Le chapitre IV.4 liste les exigences relatives à l'organisation du prestataire et la gouvernance du service, notamment la mise en place d'une charte éthique et de recrutement, le contenu des comités opérationnels et stratégiques, etc.

Le chapitre IV.5 liste les exigences relatives à la qualité et niveau de service, notamment la nature des indicateurs à suivre, le contenu de la convention de service établie entre le prestataire et le commanditaire, etc.

III. Qualification des prestataires de détection des incidents de sécurité

III.1. Modalités de la qualification

Le référentiel contient des exigences et des recommandations à destination des prestataires de détection des incidents de sécurité.

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

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

Un service de détection des incidents de sécurité est dit « interne »dans les deux cas suivants[4] :

- s'il est offert exclusivement à des commanditaires ayant un lien juridique au sens des articles L. 233-l et suivants du Code de commerce avec une même personne morale et opéré par un prestataire ayant lui aussi un lien juridique de même nature avec la même personne morale,
- s'il est offert à des commanditaires appartenant à la même autorité administrative, au sens de l'article I-1 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et opéré par un prestataire appartenant à la même autorité administrative.

Sinon le service de détection des incidents de sécurité est dit « externe ».

Pour un service de détection des incidents de sécurité interne, la qualification est octroyée :

- dans le 1er cas, à la personne morale qui offre le service de détection à laquelle tous les commanditaires du service de détection sont liés juridiquement au sens des articles L. 233-l et suivants du Code de commerce, ou à un commanditaire du service de détection en particulier ;
- dans le 2nd cas, à l'autorité administrative, au sens de l'article I-1 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives à laquelle appartiennent tous les commanditaires du service de détection ainsi que le prestataire lui-même.

Pour un service de détection des incidents externe :

- si le prestataire et ses éventuels sous-traitants mettent en œuvre tous les moyens humains, techniques ou organisationnels nécessaires au respect des exigences du référentiel et que le commanditaire ne met en œuvre que les mesures de sécurité de sa responsabilité liées aux enclaves (chapitre IV.3.14 et IV.3.15), la qualification est octroyée au prestataire ;
- si tout ou partie des moyens humains, techniques et organisationnels nécessaires au respect des exigences de ce référentiel sont mis en œuvre par un commanditaire[5], alors la qualification est octroyée au commanditaire.

[4] Exemples types : un service de détection créé par un commanditaire pour son usage propre, ou bien un service de détection offert par une filiale d'un groupe au profit d'autres filiales du même groupe.

Que le service de détection des incidents de sécurité soit interne ou externe, les sous-traitants mettant en œuvre tout ou partie des moyens humains, techniques et organisationnels nécessaires au respect des exigences de ce référentiel sont évalués pour vérifier qu'ils respectent les exigences qui leur incombent.

III.2. Portée de la qualification

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

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

Est considérée comme une prestation qualifiée au sens du référentiel, une prestation respectant toutes les exigences du présent référentiel.

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

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

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

III.3. Avertissement

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

[5] À l'exception des exigences portant sur les enclaves au sein du système d'information du commanditaire, pour lesquelles les responsabilités sont spécifiquement décrites dans les chapitres IV.3.14 et IV.3.15.

IV. Exigences à respecter par le prestataire

IV.1. Exigences générales

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

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

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

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

e) Le prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte du commanditaire dans le cadre de sa prestation et en particulier les éventuels dommages causés au commanditaire. À ce titre, le prestataire doit préciser les types de dommages concernés et les modalités de partage des responsabilités dans la convention de service, en tenant compte de toutes les éventuelles activités sous-traitées.

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

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

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

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

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

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

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

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

n) Le prestataire doit établir une convention de service avec le commanditaire. La convention de service doit être conforme aux exigences du chapitre IV.5.3 et approuvée formellement, par écrit, par le commanditaire avant l'exécution de la prestation.

IV.2. Activités du service de détection des incidents de sécurité

IV.2.1. Gestion des incidents

a) Le prestataire doit établir avec le commanditaire une liste des incidents redoutés et des impacts et conséquences associés basés sur les résultats d'une appréciation des risques élaborée par le commanditaire. Le prestataire doit recommander au commanditaire de mettre à jour son appréciation des risques dans le cas d'un changement de son infrastructure.

b) Le prestataire doit être capable de prendre en compte au minimum les catégories d'incidents de sécurité redoutés suivants :

- exploitation d'une vulnérabilité ;
- élévation de privilèges ;
- exfiltration de données ;
- propagation virale ;
- utilisation d'un mécanisme de persistance ;
- déni de service ;
- accès non autorisé à une ressource ;
- usurpation d'identité ;
- actions non conformes à la politique de sécurité du commanditaire.

c) Il est recommandé que le prestataire prenne en compte la liste des incidents de sécurité et de leurs causes de l'annexe B de [ISO27035], ainsi que celle de [ETSI_ISG_ISI].

d) Le prestataire doit élaborer avec le commanditaire et mettre en œuvre une stratégie d'analyse permettant de détecter l'ensemble des incidents de la liste des incidents redoutés (voir exigence IV.2.1.a). La stratégie d'analyse doit être revue avec le commanditaire lors des comités opérationnels définis au chapitre IV.4.3.

e) Le prestataire doit définir avec le commanditaire les règles de classification des incidents de sécurité au sens de [IGI_1300] et [II_901] et formaliser ces règles dans la stratégie d'analyse. Ces règles de classification doivent être revues avec la stratégie d'analyse lors des comités opérationnels définis au chapitre IV.4.3.

f) La stratégie d'analyse doit décrire précisément la mise en œuvre de règles de détection permettant de détecter les incidents de sécurité sur la base des évènements collectés.

g) Le prestataire doit créer des règles de détection en s'appuyant sur :

- la liste des incidents de sécurité redoutés du commanditaire ;
- des bases de connaissances acquises auprès d'éditeurs et de sociétés spécialisées en sécurité des systèmes d'information ;
- des bases de connaissances internes issues de l'expertise du prestataire :
  - veille et qualification de vulnérabilités, en priorité celles relatives à l'exécution de code arbitraire, localement ou à distance ;
  - veille et qualification de protocoles de contrôle commande ;
  - veille sur les modes opératoires d'attaque et les codes malveillants.
- les éléments de contexte spécifiques du commanditaire ;
- les règles provenant directement du commanditaire, évaluées au préalable par le prestataire (bon fonctionnement par rapport au comportement à détecter, impact sur les performances, correction des alertes, exploitabilité des alertes produites, etc.) ;
- les incidents de sécurité détectés auprès des éventuels autres commanditaires.

h) Le prestataire doit élaborer et mettre en œuvre une politique de marquage des règles de détection. Cette politique doit définir pour chaque règle de détection :

- un identifiant unique de la règle de détection, permettant de faire le lien entre les différents outils et bases de connaissances associées ;

- un numéro de version de la règle de détection ;
- le propriétaire de la règle de détection, c'est-à-dire celui qui dispose des droits sur la règle de détection ;
- l'auteur de la règle de détection, c'est-à-dire celui qui a créé la règle de détection ;
- la source de la règle de détection, c'est-à-dire celui qui est à l'origine des informations permettant de créer la règle de détection et qui n'est pas nécessairement le propriétaire ou l'auteur de la règle de détection (par exemple, un partenaire, un fournisseur, le commanditaire, etc.) ;
- la date de création de la règle de détection ;
- la date de dernière modification de la règle de détection ;
- le niveau de sensibilité ou de classification, au sens de [IGI_1300] et [II_901], de la règle de détection ;
- les modalités de diffusion de la règle de détection, par exemple « diffusable sans restriction », « diffusable au sein d'une communauté mais non publique », « diffusable en interne en respectant le besoin d'en connaître », « diffusion nominative sans rediffusion » ou sous la forme de *TRAFFIC LIGHT PROTOCOL* (TLP) ou autre, en accord avec les conventions définies avec les sources de la règle de détection ;
- la possibilité ou non d'effectuer des recherches en source ouverte en fonction du niveau de sensibilité et des modalités de diffusion ;
- les éléments descriptifs du comportement que la règle vise à détecter :
    - la description de la menace ;
    - le cas échéant, les descriptions et les identifiants (CVE par exemple) des vulnérabilités dont les tentatives d'exploitation ou les exploitations sont détectées par la règle ;
    - les phases d'attaque détectées par la règle, par exemple : reconnaissance, infiltration initiale, interaction avec le contrôle commande, élévation de privilèges, déplacements latéraux, exfiltration, etc. ;
    - toute autre information nécessaire à la description du comportement visé par la règle ;
- les éléments descriptifs de l'implémentation de la règle dans les outils techniques d'analyse :
    - la méthode d'analyse des évènements et de déclenchement de la règle de détection ;
    - les limitations éventuelles du fonctionnement liées à des critères techniques ;
- les consignes d'analyse et qualification à appliquer par l'opérateur en cas de déclenchement de la règle de détection.

i) Le prestataire doit élaborer et tenir à jour pour chaque commanditaire la liste de l'ensemble des règles de détection mises en œuvre ou ayant été mises en œuvre dans le cadre de la prestation. Cette liste doit préciser pour chaque règle identifiée par son identifiant et son numéro de version :

- la ou les date(s) auxquelles la règle de détection a été introduite dans les outils techniques d'analyse ;
- si le prestataire a procédé à une analyse *a posteriori* avec cette règle de détection (voir exigence IV.2.1.dd) et la date de cette analyse le cas échéant ;
- la ou les dates auxquelles la règle de détection a été retirée des outils techniques d'analyse.

Cette liste doit permettre d'établir un historique des règles de détection, permettant d'identifier les règles qui étaient actives à un instant ou sur une période donnés. Une règle de détection retirée des outils techniques d'analyse doit être marquée comme retirée et ne doit par conséquent pas être supprimée de cette liste.

Remarque : le cas où des modifications sont apportées à une règle de détection uniquement pour des sous-périmètres du périmètre supervisé est à détailler dans la liste.

j) Le prestataire doit transmettre au minimum une fois par mois au commanditaire un bulletin d'état des règles de détection présentant :

- le nombre de règles de détection créées, modifiées ou retirées des outils d'analyse ;
- l'identifiant, le numéro de version et la description de chaque règle créée, modifiée ou retirée des outils d'analyse ;
- le motif de la création, de la modification ou du retrait de la règle de sécurité (ex. : création, modification ou retrait à la demande du commanditaire, etc.).

k) Le prestataire doit protéger le bulletin d'état des règles de détection, en particulier en matière de confidentialité, en tenant compte du niveau de sensibilité ou de classification des règles de détection.

l) Il est recommandé que le prestataire transmette au commanditaire le bulletin d'état des règles de détection une fois par semaine.

m) Le prestataire doit implémenter dans les outils techniques d'analyse l'ensemble des règles de détection identifiées dans la liste mentionnée à l'exigence IV.2.1.i), sauf les règles marquées comme retirées.

n) Le prestataire doit de manière autonome ajouter dans les outils techniques d'analyse de nouvelles règles de détection.

Suite à un ajout de ce type, le prestataire doit mettre à jour le corpus documentaire et renseigner le détail des ajouts effectués de façon à assurer le suivi et la traçabilité de ces ajouts.

o) Le prestataire doit, en cas de difficulté ou d'impossibilité d'implémentation d'une règle de détection, avertir le commanditaire dans les meilleurs délais, et détailler les raisons de l'échec d'implémentation. Le délai maximum entre la décision d'implémentation de la règle de détection et la notification au commanditaire de l'échec d'implémentation doit être défini dans la convention de service.

p) Le prestataire doit élaborer et tenir à jour pour chaque commanditaire la liste des ajouts de règles dans les outils techniques d'analyse faisant figurer le résultat de l'implémentation (implémenté / échec) et les raisons de l'échec d'implémentation le cas échéant.

q) Le prestataire doit qualifier les incidents de sécurité détectés en vue d'apprécier leur véracité (vrai/faux positif, incident avéré ou non) et leur niveau de gravité (impacts fonctionnels, informationnels, etc.).

r) Le prestataire doit établir avec le commanditaire une échelle de gravité associée aux incidents redoutés, en prenant en compte l'appréciation des risques et notamment les menaces, les actifs, les impacts potentiels et leur niveau de gravité.

s) Il est recommandé que le prestataire utilise l'échelle de gravité des incidents de sécurité de l'annexe C de [ISO27035].

t) Dans le cadre de la qualification d'un incident de sécurité, le prestataire peut être amené à réaliser des recherches en sources ouvertes, sur internet notamment, à partir d'informations collectées ou issues des analyses (empreintes cryptographiques, noms de fichiers ou de codes malveillants, chaînes de caractères contenues dans des codes malveillants, noms de domaines et adresses IP, etc.).

Les recherches en sources ouvertes à partir d'informations collectées ou issues des analyses peuvent éveiller l'attention d'un attaquant. Il est donc important que le prestataire observe la plus grande prudence en les effectuant. Ainsi, il doit tenir compte du marquage des règles de détection indiquant la possibilité au non de réaliser une telle recherche (voir IV.2.1 h)).

Le prestataire doit définir une méthodologie pour la recherche en sources ouvertes à partir d'informations collectées ou issues des analyses. Elle doit préciser les types d'informations pouvant être recherchés et les modalités associées.

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

v) Le prestataire doit être en mesure d'intégrer les résultats des tests de vulnérabilités et d'intrusion réalisés par le commanditaire sur son système d'information. Cela peut notamment se traduire par :

- la création de règles de détection associées aux vulnérabilités identifiées ;
- la constitution de bases de connaissances sur les vulnérabilités existantes pour améliorer le diagnostic, que ce soit par les outils techniques d'analyse (corrélation) ou les opérateurs (capitalisation et utilisation des connaissances contextuelles du SI supervisé).

w) Le prestataire doit créer un ticket pour chaque incident de sécurité détecté et le mettre à disposition du commanditaire. Ce ticket d'incident de sécurité doit au minimum comprendre les éléments suivants :

- la date de création du ticket et des différentes opérations réalisées sur celui-ci (traçabilité des actions) ;
- la date et l'heure de la détection de l'incident de sécurité ;
- la date effective de l'évènement ou des évènements ayant donné lieu à l'incident de sécurité ;
- la description de l'incident de sécurité ;
- le niveau de classification de l'incident [IGI_1300] [II_901] ;
- la gravité de l'incident de sécurité ;
- la description de l'impact de l'incident de sécurité pour le commanditaire ;
- les identifiants et numéros de version des règles de détection déclenchées ;
- les équipements ayant généré et collecté les évènements de l'incidents ;
- les identifiants des évènements ayant permis la détection de l'incident ;
- le risque induit par l'incident.

x) Le prestataire doit définir avec le commanditaire le format des tickets d'incident de sécurité.

y) Il est recommandé que le prestataire utilise le format des tickets d'incident de sécurité détaillé dans [ETSI_ISG_ISI].

z) Le prestataire doit disposer d'un outil de gestion de tickets d'incident de sécurité.

aa) Le prestataire doit associer à chaque ticket d'incident de sécurité son contexte (évènements associés et rapport(s) d'analyse(s) de qualification) et stocker ces éléments de manière centralisée, que les incidents de sécurité soient en cours de qualification, avérés ou clôturés.

bb) Le prestataire doit mettre en place et tenir à jour un registre centralisé et chronologique par commanditaire identifiant l'ensemble des incidents de sécurité détectés.

cc) Le prestataire doit mettre en place un processus de gestion de la capacité de stockage des tickets d'incidents de sécurité et de leur contexte permettant de suivre son évolution et d'être en mesure de l'adapter pour assurer leur conservation sur toute la durée de la prestation, dans la limite du respect de la législation et la réglementation en vigueur sur le territoire national (voir exigence IV.1.b).

dd) La stratégie d'analyse doit prévoir qu'à chaque règle de détection créée ou modifiée, le prestataire procède à une analyse *a posteriori*, c'est-à-dire à une analyse sur l'ensemble des évènements stockés depuis une période définie avec le commanditaire dans la stratégie d'analyse.

Cette exigence ne s'applique pas aux règles de détection nécessitant des types d'évènements non encore présents dans les systèmes de stockage des évènements.

Le prestataire doit être en mesure de rechercher *a minima* les indicateurs de compromission des types suivants :

- fichiers : empreinte (MD5, SHA1, SHA256), empreinte du nom, chemin d'accès, taille, extension, nombre magique (*magic number*) ;
- adresses IP publiques ;
- domaines pour les protocoles suivants : HTTP, SMTP et DNS ;
- URL ;
- agent utilisateur (*user-agent*) ;
- champs d'emails : domaine source, domaine destination, empreinte du sujet, *horodate* ;
- champs de certificats *X509* : empreinte, émetteur, date de validité, sujet, extensions, nom d'hôte, *horodate*.

Il est recommandé que le prestataire soit en mesure de rechercher des combinaisons de ces indicateurs de compromission.

ee) Le prestataire doit être capable sur demande du commanditaire de procéder à une analyse sur l'ensemble des évènements stockés depuis six mois.

IV.2.2. Gestion des évènements

a) Le prestataire doit élaborer avec le commanditaire et mettre en œuvre une stratégie de collecte basée sur la liste des incidents de sécurité redoutés (voir exigence IV.2.1.a). La stratégie de collecte doit être revue avec le commanditaire lors des comités opérationnels définis au chapitre IV.4.3.

b) La stratégie de collecte doit identifier la liste des sources de collecte, des collecteurs, des évènements à collecter, décrire les méthodes de collecte (protocoles, applications, propriétés de sécurité, etc.) et identifier les fréquences de collecte.

c) Le prestataire doit être au minimum capable de collecter les évènements en provenance des sources de collecte suivantes :

- équipements de sécurité : pare-feux réseau, pare-feux applicatifs, chiffreurs, sondes dont celles qualifiées par l'ANSSI au niveau adéquat, antivirus, concentrateurs VPN, passerelles SSL, mandataires (*proxies*), mandataires inverses (*proxies* inverses) ;
- équipements réseau : routeurs, commutateurs, équipements générant des données *netflow*, serveurs DNS, répartiteurs de charge, serveurs de temps ;
- serveurs d'infrastructure : authentification, annuaires, télédistribution, télégestion, supervision, virtualisation, serveurs de fichiers, sauvegardes, messagerie, impression ;
- serveurs métier : serveurs web, bases de données, serveurs applicatifs, collecteurs ;
- postes de travail : principaux systèmes d'exploitation, applications de sécurité ;
- terminaux mobiles via les serveurs de gestion de flotte mobile.

d) Il est recommandé que le prestataire soit capable de collecter les événements en provenance des équipements constituant les systèmes d'information industriels : automates programmables industriels, pare-feux industriels, commutateurs industriels et routeurs industriels.

e) Le prestataire doit être au minimum capable de journaliser pour chacune des sources de collecte identifiées à l'exigence IV.2.2.c) les évènements identifiés dans l'annexe A de la note technique de l'ANSSI consacrée à la mise en œuvre d'un système de journalisation [NT_JOURNAL].

f) Le prestataire doit de manière autonome faire évoluer sa capacité de collecte (sources de collecte et évènements collectés), en lien avec la liste des incidents redoutés.

g) Le prestataire doit, en cas de difficulté ou d'incapacité à mettre en œuvre la collecte d'un ou plusieurs évènement(s) sur une source de collecte, avertir le commanditaire dans les meilleurs délais, et détailler les raisons de l'échec. Le délai maximum entre la décision de mise en œuvre de la collecte et la notification au commanditaire de l'échec d'implémentation doit être défini dans la convention de service.

h) Le prestataire doit exercer un devoir de conseil envers le commanditaire dans l'élaboration, l'application et la revue de la stratégie de collecte. À ce titre, il doit conseiller le commanditaire dans l'élaboration et la revue de la politique de journalisation (sources de collecte, types d'évènements à journaliser, durées de conservation, normalisation des informations, synchronisation des sources de temps, etc.) et dans le déploiement de dispositifs de journalisation sur le périmètre supervisé au sein du système d'information du commanditaire.

i) Le prestataire doit recommander au commanditaire d'intégrer dans la stratégie de collecte la mise en œuvre de sondes à chacune des interconnexions du périmètre supervisé et en particulier celles avec :

   - internet ;
   - les systèmes d'information tiers (partenaires, sous-traitants, etc.) ;
   - les autres systèmes d'information du commanditaire de niveau de sensibilité ou de classification moindre ou plus exposés.

j) Le prestataire doit recommander au commanditaire le choix de sondes qualifiées par l'ANSSI au niveau adéquat qui seront utilisées conformément aux conditions de leur qualification. Ces sondes doivent être alimentées en trafic via des équipements de type *Tap* totalement passifs et non administrables à distance.

k) Il est recommandé que les équipements de type *Tap* alimentant les sondes soient qualifiés par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur qualification.

l) Le prestataire doit être capable d'opérer des sondes alimentées en trafic via des équipements de type *Tap* totalement passifs et non administrables à distance.

   Remarque : s'il souhaite utiliser un agrégateur de flux intermédiaire entre les *Tap* et la (les) sonde(s), le prestataire doit dédier l'équipement à la fonction d'agrégation et respecter les règles relatives à l'utilisation d'un agrégateur de flux précisées dans l'Annexe 5.

m) Il est recommandé que le prestataire soit capable d'opérer des sondes dédiées aux systèmes d'information industriels.

n) Les évènements en provenance de sources de collecte doivent être centralisés sur un ou plusieurs collecteurs[6] situés dans l'enclave de collecte décrite dans l'exigence IV.3.15.

o) Le collecteur de l'enclave de collecte doit permettre de réaliser un premier filtrage des évènements afin de ne transmettre à la zone de collecte et aux outils d'analyse que les évènements utiles au service de détection et identifiés dans la stratégie de collecte.

p) Le prestataire doit élaborer et tenir à jour pour chaque commanditaire la liste de l'ensemble des règles de filtrage mises en œuvre ou ayant été mises en œuvre dans le cadre de la prestation. Cette liste doit préciser pour chaque règle identifiée par son identifiant et son numéro de version :

   - la ou les date(s) auxquelles la règle de filtrage a été introduite dans les collecteurs ;

[6] À des fins de simplification, il est fait l'hypothèse dans la suite du document qu'il n'y a qu'un seul collecteur.

- la ou les date(s) auxquelles la règle de filtrage a été retirée des collecteurs.

Cette liste doit permettre d'établir un historique des règles de filtrage, permettant d'identifier les règles qui étaient activées à un instant ou sur une période donnés. Une règle de filtrage retirée des collecteurs doit être marquée comme retirée et ne doit par conséquent pas être supprimée de cette liste.

Remarque : le cas où des modifications sont apportées à une règle de détection uniquement pour des sous-périmètres du périmètre supervisé est à détailler dans la liste.

q) Le prestataire doit transmettre au minimum une fois par mois au commanditaire un bulletin d'état des règles de filtrage présentant :

- le nombre de règles de filtrage créées, modifiées ou retirées des collecteurs ;
- l'identifiant et la description de chaque règle créée, modifiée ou retirée des collecteurs ;
- le motif de la création, de la modification ou du retrait de la règle de filtrage (ex. : création, modification ou retrait à la demande du commanditaire, etc.).

Il est recommandé que le prestataire transmette au commanditaire le bulletin d'état des règles de filtrage une fois par semaine.

r) Le collecteur doit être capable de détecter les cas de saturation ou de perte de communication l'empêchant de transmettre les évènements de sécurité au service de détection et de différer la transmission des évènements aux outils d'analyse le cas échéant. Le prestataire doit s'engager sur la capacité de conservation du collecteur dans la convention de service. L'évolution de la capacité de conservation du collecteur doit être suivie et présentée au commanditaire lors des comités opérationnels définis au chapitre IV.4.3.

s) Le prestataire doit disposer d'une vision centralisée de l'ensemble des évènements collectés, notamment en associant à chaque évènement le collecteur dont il est issu.

t) Les horloges des collecteurs doivent être synchronisées avec une source de temps unique (voir exigence IV.3.9.l).

u) Le prestataire doit indexer l'ensemble des évènements collectés et être capable de réaliser des recherches parmi les évènements collectés.

v) Le prestataire doit être capable de localiser et de fournir n'importe quel évènement collecté sur demande du commanditaire.

w) Le prestataire doit mettre en place un processus de gestion de la capacité de traitement et de stockage des évènements permettant de suivre son évolution et d'être capable de l'adapter en fonction des besoins et pour assurer leur conservation sur au minimum six mois (voir exigence IV.2.1.ee), dans la limite du respect de la législation et la réglementation en vigueur sur le territoire national (voir exigence IV.1.b).

IV.2.3. Gestion des notifications

a) Le prestataire doit disposer de deux canaux d'information à destination du commanditaire :

- un canal pour la notification (voir exigence IV.2.3.b) ;
- un canal sécurisé, notamment pour l'échange d'informations détaillées (voir exigence IV.2.3. l).

b) Le prestataire doit disposer au minimum de deux moyens de notification : un moyen nominal et un moyen secondaire. Le moyen de communication secondaire doit être testé au minimum tous les six mois et à chaque modification du système d'information du service de détection des incidents de sécurité. Les moyens de notification peuvent être par exemple :

- courriel ;
- message court (SMS) ;

- téléphone.

c) Le prestataire doit élaborer avec le commanditaire et mettre en œuvre une stratégie de notification des incidents de sécurité permettant de prévenir le commanditaire lors de la détection d'un incident de sécurité. La stratégie de notification doit être revue avec le commanditaire lors des comités opérationnels définis au chapitre IV.4.3.

d) La stratégie de notification doit identifier au minimum la liste des incidents de sécurité à notifier, le format, le contenu, le délai, le niveau de sensibilité ou de classification des notifications ainsi que les personnes à notifier notamment en fonction de l'incident de sécurité et de son niveau de gravité.

e) Le prestataire doit exercer un devoir de conseil envers le commanditaire dans l'élaboration, l'application et la revue de la stratégie de notification. À ce titre, il doit conseiller le commanditaire sur les personnes à avertir et les méthodes de notification.

f) Le prestataire doit recommander au commanditaire d'intégrer dans la stratégie de notification des notifications spécifiques en cas de détection d'incidents de sécurité majeurs au sein de son système d'information.

g) Les notifications doivent contenir exclusivement les informations suivantes : le numéro du ticket d'incident.

Les notifications ne doivent en aucun cas contenir des informations détaillées sur l'incident de sécurité et notamment sur les évènements collectés ou les règles de détection ayant permis de détecter l'incident de sécurité, la partie du système d'information du commanditaire concernée par l'incident de sécurité ou les impacts de l'incident de sécurité.

h) Le prestataire doit centraliser toutes les notifications dans un système de stockage des notifications. Les informations suivantes doivent être stockées : date et heure de la notification, mode de notification, destinataire(s) de la notification, contenu de la notification incluant notamment le numéro du ticket d'incident.

Remarque : les informations ci-dessus concernant les notifications peuvent être incluses dans les tickets d'incidents.

i) Le prestataire doit être capable de fournir le ticket d'incident de sécurité et le contexte associé (évènements associés et rapport(s) d'analyse(s) de qualification) à l'origine d'une notification.

j) Le prestataire doit mettre en place et tenir à jour un registre centralisé et chronologique par commanditaire référençant toutes les notifications effectuées pour le commanditaire. Le registre doit notamment faire figurer : date et heure de la notification, mode de notification, destinataire(s) de la notification, contenu de la notification incluant notamment le numéro du ticket d'incident.

k) Le prestataire doit mettre en place un processus de gestion de la capacité de stockage des notifications permettant de suivre son évolution et d'être en mesure de l'adapter pour assurer leur conservation sur toute la durée de la prestation, dans la limite du respect de la législation et la réglementation en vigueur sur le territoire national (voir exigence IV.1.b).

l) Le prestataire doit mettre à disposition du commanditaire :

- un portail web lui permettant de visualiser et mettre à jour l'état des incidents de sécurité et des actions engagées ;
- un dispositif de stockage permettant au commanditaire de :
  - récupérer le contexte des incidents de sécurité (évènements associés et rapport(s) d'analyse(s) de qualification) le concernant ;
  - déposer le cas échéant des informations contextuelles nécessaires aux opérateurs pour la qualification d'un incident.

IV.3. Protection de l'information

IV.3.1. Politique de sécurité des systèmes d'information

a) Le prestataire doit élaborer une appréciation des risques et le plan de traitement des risques associé sur l'intégralité du périmètre du service de détection des incidents de sécurité. L'appréciation et le plan de traitement doivent être validés formellement et par écrit auprès de la direction du prestataire.

b) L'appréciation des risques doit prévoir une liste d'incidents redoutés sur le périmètre du service de détection des incidents de sécurité. Cette liste doit intégrer *a minima* :

- les tentatives d'intrusion sur le système d'information du service de détection depuis une de ses interconnexions (voir chapitre IV.3.10) ;
- les tentatives de rebond entre les systèmes d'information des commanditaires via le système d'information du service de détection ;
- les tentatives d'élévation de privilèges par les opérateurs ou les administrateurs du service de détection des incidents de sécurité ;
- la perte de communication avec un ou plusieurs équipements du service de détection ;
- les infections virales originaires de codes malveillants rencontrés dans le cadre de la prestation.

c) Le prestataire doit réviser l'appréciation des risques et le plan de traitement des risques associé au minimum annuellement, et en cas de modifications structurantes du service de détection, notamment celles concernant son hébergement, son infrastructure ou son architecture.

d) Le prestataire doit mettre le plan de traitement des risques à disposition du commanditaire si ce dernier en fait la demande. Le prestataire devra indiquer au commanditaire les conditions de sécurité liées à la transmission et au stockage de ce plan de traitement des risques.

e) Le prestataire doit définir et mettre en œuvre une politique de sécurité des systèmes d'information basée sur l'appréciation des risques. Cette politique doit préciser les niveaux de qualification ou d'agrément des différents équipements mis en œuvre (niveaux dits « adéquat » dans le présent référentiel).

f) Il est recommandé que le prestataire soit certifié [ISO27001] sur l'intégralité du périmètre du service de détection des incidents de sécurité.

IV.3.2. Niveaux de sensibilité ou de classification

a) Le prestataire doit au minimum respecter les règles établies par l'ANSSI et relatives aux mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau *Diffusion Restreinte* [IGI_1300] [II_901], en particulier pour les informations identifiées comme sensibles dans l'appréciation des risques (voir exigence IV.3.1.a).

b) Le prestataire doit appliquer au minimum le *Niveau Standard* du guide d'hygiène informatique de l'ANSSI [HYGIENE] au système d'information du service de détection des incidents de sécurité.

c) Le système d'information du service de détection doit être homologué au minimum au niveau *Diffusion Restreinte* pour superviser les systèmes d'information non classifiés de défense du commanditaire.

d) Le système d'information du service de détection doit être homologué au minimum au même niveau de classification que les systèmes d'information classifiés de défense du commanditaire [IGI_1300].

e) Il est recommandé que le prestataire utilise la démarche décrite dans le guide [HOMOLOGATION] pour homologuer le système d'information du service de détection des incidents de sécurité.

f) Il est recommandé que le prestataire fasse appel à une prestation qualifiée d'audit de la sécurité des systèmes d'information par un PASSI pour la réalisation de l'audit dans le cadre de l'homologation.

IV.3.3. Territorialité du service

a) Le prestataire doit héberger et traiter les données relatives au service de détection des incidents de sécurité exclusivement au sein de l'Union Européenne. Dans le cas où certaines sources de collecte seraient situées en dehors de l'Union Européenne, les évènements issus de ces sources devront être transmis à un collecteur situé au sein de l'Union Européenne.

b) Le prestataire doit exploiter et administrer le service de détection des incidents de sécurité exclusivement depuis l'Union Européenne.

IV.3.4. Contrôles

a) Le prestataire doit documenter et mettre en œuvre un plan de contrôle définissant le périmètre et la fréquence des contrôles en accord avec la gestion du changement, les politiques, et les résultats de l'appréciation des risques.

b) Ce plan de contrôle doit permettre de vérifier la bonne mise en œuvre des mécanismes de sécurité et de protection de l'information dont le prestataire porte la responsabilité. Ce plan de contrôle doit intégrer au minimum :

- le contrôle des accès logiques et physiques aux dispositifs du service de détection ;
- la revue des privilèges et des droits d'accès aux dispositifs du service de détection des incidents de sécurité. Cette revue doit prévoir la revue des comptes des administrateurs et des opérateurs au minimum mensuellement.

c) Le prestataire doit réviser le plan de contrôle au minimum annuellement et en cas de modifications structurantes du service de détection, notamment celles concernant son hébergement, son infrastructure et son architecture.

d) Le prestataire doit inclure la liste des incidents de sécurité redoutés (voir exigence IV.3.1.b) dans le plan de contrôle afin d'éprouver ces scénarios.

e) Le plan de contrôle doit inclure un programme d'audit sur trois ans couvrant notamment :

- des audits de configuration des serveurs et équipements réseau inclus dans le périmètre du service de détection. Ces audits sont réalisés par échantillonnage et doivent inclure tous types d'équipements et de serveurs présents dans le système d'information du service ;
- des tests d'intrusion sur le service (une attention particulière sera portée aux interconnexions) ;
- si le service bénéficie de développements internes, des audits de code source portant sur les fonctionnalités de sécurité implémentées ainsi que les fonctionnalités à risque (ex. : entrées/sorties).

f) Le programme d'audit doit inclure au minimum un audit qualifié par an, réalisé par un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié. Les prestataires PASSI mandatés doivent être juridiquement indépendants du prestataire.

g) Le prestataire doit protéger les résultats des contrôles au minimum au même niveau de sensibilité ou de classification que le système d'information contrôlé.

h) Le prestataire doit mettre à jour le plan de traitement des risques (voir exigence IV.3.1.a) pour intégrer les résultats des contrôles.

i) Le prestataire doit communiquer les résultats des contrôles à sa direction. Les résultats des contrôles doivent être validés formellement et par écrit auprès de la direction du prestataire.

IV.3.5. Sécurité physique

a) Le prestataire doit élaborer et tenir à jour la liste des personnes autorisées à accéder aux locaux hébergeant le service de détection des incidents de sécurité.

b) Le prestataire doit mettre en œuvre les mécanismes permettant de garantir que seules les personnes autorisées peuvent accéder aux locaux hébergeant le service de détection des incidents de sécurité.

c) Le prestataire doit mettre en œuvre les mécanismes permettant de journaliser les accès aux locaux hébergeant le service de détection des incidents de sécurité.

d) Le prestataire doit définir et mettre en œuvre les mesures permettant d'assurer la confidentialité et l'intégrité des journaux d'accès aux locaux hébergeant le service de détection à l'aide de solutions agréées par l'ANSSI [CRYPTO_B1], [CRYPTO_B3] au niveau adéquat et utilisées conformément aux conditions de leur agrément.

IV.3.6. Sauvegardes

a) Le prestataire doit élaborer et mettre en œuvre un plan de sauvegarde et de restauration des dispositifs du service de détection des incidents de sécurité. Le plan de sauvegarde doit comporter plusieurs volets distincts, au minimum les volets suivants :

- sauvegarde des systèmes ;
- sauvegarde des configurations ;
- sauvegarde des données.

b) Le prestataire doit tester le plan de sauvegarde et de restauration au minimum une fois par an.

c) Le prestataire doit définir et mettre en œuvre les mesures permettant d'assurer la confidentialité et l'intégrité des sauvegardes effectuées, au même niveau que celui pour lequel le système de détection a été homologué. Le dispositif de sauvegarde doit être dédié et hébergé dans une zone d'administration en prévoyant un cloisonnement des activités de sauvegarde, conforme au plan de sauvegarde.

d) Il est recommandé que le prestataire respecte l'ensemble des mesures et préconisations sur la sécurisation des sauvegardes de [ISO27002].

IV.3.7. Service de détection du service

a) Le prestataire doit mettre en œuvre, pour son propre compte, un service de détection des incidents de sécurité, ci-après dénommé « service de détection du service », portant sur le système d'information du service de détection des incidents de sécurité.

b) Le prestataire doit respecter les exigences du chapitre IV.3 pour le service de détection du service, à l'exception des exigences IV.3.7.a) et des exigences des chapitres IV.3.13, IV.3.14 et IV.3.15.

c) Le prestataire doit, sur la base de l'appréciation des risques (voir exigence IV.3.1.a) et de la liste des incidents de sécurité redoutés associée (voir exigence IV.3.1.b), élaborer une stratégie de collecte, une stratégie d'analyse et une stratégie de notification dans le cadre du service de détection du service.

d) Il est recommandé, selon le résultat de l'appréciation des risques et la liste des incidents de sécurité redoutés associée, que le prestataire cloisonne le service de détection du service (séparation des moyens humains, techniques et organisationnels).

e) Le prestataire doit déployer une ou plusieurs sondes sur le système d'information du service de détection des incidents de sécurité. Ces sondes doivent notamment permettre la supervision de chacune des interconnexions du système d'information du service de détection des incidents de sécurité. Ces sondes doivent être des sources de collecte pour le service de détection du service.

f) Les sondes déployées par le prestataire dans le cadre du service de détection du service doivent être qualifiées par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur qualification. Ces sondes doivent être alimentées en trafic via des équipements de type *Tap* totalement passifs et non administrables à distance.

Remarque : s'il souhaite utiliser un agrégateur de flux intermédiaire entre les *Tap* et la (les) sonde(s), le prestataire doit dédier l'équipement à la fonction d'agrégation et respecter les règles relatives à l'utilisation d'un agrégateur de flux précisées dans l'Annexe 5.

g) Il est recommandé que le prestataire mette en place un transfert des journaux des dispositifs de son système de détection des incidents de sécurité vers une zone de confiance dédiée conformément aux exigences de [NT_JOURNAL]. Dans ce cas, il est recommandé que la zone de confiance dédiée mette en œuvre un contrôle d'accès interdisant l'accès aux administrateurs et opérateurs du service de détection des incidents de sécurité respectivement depuis les zones d'administration et d'exploitation.

h) Le prestataire doit élaborer un processus de gestion des incidents de sécurité du service. Ce processus doit prévoir une notification aux commanditaires lors de l'occurrence d'un incident de sécurité sur le service de détection des incidents de sécurité. La notification doit spécifier la nature de l'incident de sécurité et les mesures mises en œuvre par le prestataire pour y répondre.

i) Il est recommandé que le prestataire mette en place un processus de gestion de crise en cas de détection d'un incident de sécurité majeur au sein de son service de détection.

j) Il est recommandé que le prestataire utilise des outils permettant de réaliser une analyse statique ou dynamique de fichiers suspects.

k) Dans le cas où le prestataire utilise des outils d'analyse statiques ou dynamiques de fichiers suspects faisant appel à des ressources hébergées sur Internet, le prestataire doit réaliser ces opérations hors du système d'information du service de détection des incidents de sécurité

l) Il est recommandé que le prestataire fasse appel à un prestataire de réponse aux incidents qualifié (PRIS)[7] afin de réaliser l'étude des fichiers suspects par une prestation d'investigation numérique sur périmètre restreint d'analyse de codes malveillants. Dans ce cas, le prestataire de détection des incidents de sécurité s'assurera que la portée de qualification du prestataire de réponse aux incidents inclut ce type de prestation.

IV.3.8. Cloisonnement du système d'information du service

a) Le prestataire doit dédier le système d'information du service de détection des incidents de sécurité aux prestations qualifiées ou l'employer dans des conditions où la mutualisation des prestations ne dégrade pas le niveau de sécurité du système d'information du service. Toute autre prestation doit être réalisée sur un système d'information cloisonné physiquement du système d'information du service.

b) Le prestataire doit cloisonner le système d'information du service de détection des incidents de sécurité en plusieurs zones de confiance dans lesquelles sont répartis tous les dispositifs impliqués dans le service de détection :

- zone(s) de collecte (une ou plusieurs), regroupant l'ensemble des dispositifs impliqués dans le processus de collecte, notamment les collecteurs centraux et les systèmes de stockage des évènements et, le cas échéant, des informations contextuelles ;
- zone(s) d'analyse, regroupant l'ensemble des dispositifs impliqués dans le processus d'analyse, notamment les outils techniques d'analyse des incidents de sécurité ;

[7] Le catalogue des prestataires de réponse aux incidents de sécurité de l'information (PRIS) qualifiés est publié sur le site de l'ANSSI.

- zone(s) de notification, regroupant les systèmes de notification du commanditaire, notamment les systèmes de messagerie ;
- zone(s) d'échange commanditaire, regroupant l'ensemble des dispositifs permettant l'échange sécurisé d'informations avec le commanditaire, notamment le portail web ;
- zone(s) d'administration, regroupant l'ensemble des outils d'administration et les postes d'administration ;
- zone(s) de mise à jour, regroupant l'ensemble des dispositifs impliqués dans le processus de téléchargement des mises à jour des dispositifs du service de détection ;
- zone(s) d'exploitation, regroupant les postes de travail des opérateurs ;
- zones d'échange, distinctes entre les administrateurs et les opérateurs, regroupant les dispositifs permettant le transfert de fichiers avec l'extérieur du système d'information du service de détection des incidents de sécurité.

c) Le prestataire doit mettre en œuvre les mesures garantissant le cloisonnement entre les différentes zones de confiance, notamment par des mécanismes de filtrage, d'authentification et de contrôle d'accès.

d) Le prestataire doit élaborer et tenir à jour la matrice des flux de référence du système de détection des incidents de sécurité, ainsi que la politique de filtrage associée, n'autorisant que les flux strictement nécessaires au fonctionnement du service de détection des incidents de sécurité.

e) Le prestataire doit mettre en œuvre des solutions de chiffrement et d'authentification IP entre ces zones de confiance dès lors que les informations échangées entre ces zones transitent par des réseaux de transport non dédiés au service de détection. Ces solutions de chiffrement et d'authentification IP doivent être agréées par l'ANSSI au niveau adéquat et être utilisées conformément aux conditions de leur agrément.

f) Le prestataire doit élaborer et maintenir à jour une description détaillée de l'architecture du système d'information du service de détection des incidents de sécurité. Cette description doit identifier tous les dispositifs du système d'information et les zones de confiance du service de détection.

g) Le prestataire doit cloisonner entre les commanditaires :

- les systèmes de stockage et de traitement des évènements et des informations contextuelles associées ;
- les systèmes de stockage et de traitement des incidents de sécurité, les outils techniques d'analyse et les outils de gestion de tickets d'incident de sécurité ;
- les notifications, le portail web et le système de messagerie.

Ce cloisonnement doit être réalisé via des mécanismes de contrôle d'accès au minimum logique, mis en œuvre en fonction du juste besoin opérationnel (droits, privilèges, authentification, etc.).

IV.3.9. Administration et exploitation du service

a) Les administrateurs doivent administrer les dispositifs du service de détection des incidents de sécurité avec des postes d'administration dédiés, hébergés dans la zone d'administration[8] et distincts des postes de travail des opérateurs.

[8] Il est recommandé de respecter la note technique de l'ANSSI pour l'administration sécurisée des systèmes d'informations [NT_ADMIN].

b) L'administration des dispositifs du service de détection des incidents de sécurité ne doit être réalisable que depuis la zone d'administration via les interfaces réseau des dispositifs dédiées à l'administration.

c) Le prestataire doit journaliser tous les accès aux dispositifs du service de détection des incidents de sécurité ainsi que les actions réalisées[9].

d) Le prestataire doit mettre en place un annuaire centralisé et dédié à l'authentification des administrateurs et des opérateurs du service, permettant en particulier l'authentification sur leurs postes de travail ainsi que sur l'ensemble des dispositifs du service de détection.

   La solution mise en place doit assurer un cloisonnement logique strict des populations administrateurs et opérateurs au sein de l'annuaire centralisé, pour l'authentification, l'autorisation et la gestion des identités.

e) Le prestataire doit mettre en œuvre les mesures garantissant que les administrateurs administrent les dispositifs du service de détection des incidents de sécurité depuis des comptes d'administration dédiés à ces tâches et accessibles uniquement par les administrateurs ;

f) Les administrateurs ne doivent pas disposer des droits d'administration sur leur poste d'administration.

g) Le prestataire doit mettre en œuvre les mesures garantissant que les administrateurs et les opérateurs n'accèdent qu'aux ressources utiles dans le cadre de leurs missions (voir Annexe 2).

h) Le prestataire doit appliquer des mesures privant les opérateurs de droits d'administration sur les dispositifs du service de détection, y compris sur leur poste de travail.

i) Les postes de travail des administrateurs et des opérateurs doivent être raccordés exclusivement au système d'information de détection des incidents de sécurité.

   En cas de besoin d'accès à internet ou à d'autres systèmes d'information (système d'information interne du prestataire par exemple), les administrateurs et les opérateurs doivent disposer d'un poste distinct de leur poste de travail, déployé au sein d'une zone externe au système d'information du service de détection, appelée zone internet (voir exigence IV.3.16.a).

j) Le prestataire doit mettre en place une zone d'échange permettant le transfert de fichiers avec l'extérieur du système d'information du service de détection dans le cadre de l'administration ou de l'exploitation du service de détection. Cette zone d'échange doit être distincte entre les administrateurs et les opérateurs. Le prestataire doit respecter les exigences relatives à la zone d'échange décrites au chapitre « Système d'échange » de la note technique [NT_ADMIN].

   Remarque : les outils d'analyse de contenu malveillant peuvent être mutualisés entre la zone d'échange utilisée par les administrateurs et celle utilisée par les exploitants.

   Le prestataire doit prévoir, pour les outils d'analyse de contenu malveillant, un traitement spécifique pour les fichiers chiffrés ou ne pouvant être analysés.

   Le prestataire doit mettre en place la journalisation de l'horodate, du nom et de l'empreinte cryptographique de tous les fichiers transitant par les outils d'analyse de contenu malveillant.

k) Tous les échanges liés au service de détection depuis les postes d'administration ou les postes d'exploitation doivent être réalisés à l'aide de protocoles de chiffrement et d'authentification conformes aux exigences de l'ANSSI [CRYPTO_B1], [CRYPTO_B3].

l) Le prestataire doit héberger dans la zone d'administration un serveur de temps de référence pour assurer la synchronisation des horloges de l'ensemble des dispositifs du service de détection.

[9] Il est recommandé de respecter la note technique de l'ANSSI pour la mise en œuvre d'un système de journalisation [NT_JOURNAL].

m) Le prestataire doit assurer la synchronisation de son serveur de temps de référence en utilisant un canal nominal et un canal de secours, via les canaux suivants :

- via internet : le prestataire doit pour cela mettre en place un relais dans la zone de mise à jour ;
- via antenne : le prestataire doit pour cela mettre en place un dispositif dédié de type antenne (radio, *GPS*)

n) Il est recommandé que les sources de temps utilisées par le prestataire pour un commanditaire donné soient les mêmes que celles du commanditaire.

o) L'utilisation de sources de temps différentes entre le commanditaire et le prestataire peuvent conduire à des problèmes d'ordonnancement des journaux, notamment entre les journaux remontés du système d'information via les collecteurs et les journaux remontés par les sondes. Le prestataire doit avoir connaissance du *delta* potentiel entre les deux sources.

IV.3.10. Interconnexions du système d'information du service

a) Les seules interconnexions du système d'information du service de détection des incidents de sécurité autorisées sont celles avec :

- le système d'information du commanditaire :
  - pour la collecte des évènements et informations contextuelles via l'enclave de collecte ;
  - pour l'administration des dispositifs de collecte et, le cas échéant, de consultation[10] ;
  - pour l'exploitation des dispositifs de collecte ;
  - pour l'envoi d'information non sensible via canal non sécurisé, notamment la notification des incidents de sécurité ;
  - pour l'échange d'information sensible avec l'enclave de consultation via canal sécurisé, notamment l'échange d'informations nécessaires à la qualification et l'interaction avec le portail web de suivi des incidents de sécurité ;
- les postes d'administration et d'exploitation nomades (voir IV.3.17) via des passerelles spécifiques ;
- les postes de consultation nomades via une passerelle spécifique (voir IV.3.17) ;
- les serveurs de mise à jour pour télécharger les mises à jour des dispositifs du service de détection des incidents de sécurité via une zone de mise à jour (voir IV.3.11) ;
- la zone internet permettant l'échange de fichiers avec l'extérieur par l'intermédiaire des zones d'échange (voir IV.3.16).

b) Le prestataire doit filtrer tous les flux aux interconnexions du système d'information du service de détection des incidents de sécurité, à l'aide de solutions de filtrage qualifiées par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur qualification.

Remarque : les interconnexions du système d'information du service de détection doivent de plus être conformes aux exigences de cloisonnement des réseaux de l'Annexe 2 de l'instruction interministérielle relative à la protection des systèmes d'information sensibles [II_901] (voir exigence IV.3.2.c).

[10] Uniquement si le commanditaire autorise le prestataire à administrer un ou plusieurs dispositifs hébergés dans cette zone (voir exigence IV.3.14.b).

c) Les flux aux interconnexions avec le service de détection des incidents de sécurité doivent être chiffrés à l'aide de solutions de chiffrement et d'authentification *IPsec* agréées par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur agrément.

Seules font exception à cette exigence, dans la mesure où les exigences des parties IV.3.11 et IV.3.12 sont respectées, les interconnexions avec :

- les serveurs de mise à jour pour télécharger les mises à jour des dispositifs du service de détection des incidents de sécurité via la zone de mise à jour (voir IV.3.11) ;
- le système d'information du commanditaire pour l'envoi d'information non sensible, notamment la notification des incidents de sécurité (voir IV.3.12).

d) Les équipements utilisés pour le chiffrement et l'authentification des interconnexions doivent être dédiés aux prestations de détection des incidents de sécurité qualifiées ou employés dans des conditions où la mutualisation des prestations ne dégrade pas le niveau de sécurité du système d'information du service de détection.

e) Le prestataire doit protéger en confidentialité, en intégrité et en authenticité toutes les informations échangées entre le système d'information du service de détection des incidents de sécurité et le système d'information du commanditaire à l'aide de solutions agréées par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur agrément.

IV.3.11. Zone de mise à jour

a) Le prestataire peut mettre en place une zone de mise à jour contenant un ou plusieurs dépôt(s) relais connecté(s) à une passerelle internet dédiée pour permettre le téléchargement de mises à jour des dispositifs du service de détection des incidents de sécurité.

Remarque : le terme « mise à jour » couvre également la mise à jour à partir de sources officielles des référentiels utilisés par les dispositifs du service de détection (exemple : outils de veille et d'analyse de la menace).

b) Le prestataire doit procéder à une mise à jour manuelle et déconnectée des dispositifs du service de détection des incidents de sécurité qui ne permettraient pas de mise à jour via un dépôt relais.

Les exigences suivantes s'appliquent uniquement dans le cas de la mise en place d'une zone de mise à jour.

c) Le prestataire doit mettre en œuvre un filtrage par liste blanche afin de n'autoriser le(s) dépôt(s) relais qu'à télécharger les mises à jour officielles des dispositifs du service de détection des incidents de sécurité auprès des sources de mise à jour officielles des éditeurs.

d) Le prestataire doit s'assurer de l'authenticité et l'intégrité des mises à jour téléchargées auprès des sources de mise à jour autorisées, et mettre en œuvre des certificats en s'appuyant sur les règles et recommandations de l'ANSSI concernant la gestion des clés utilisées dans les mécanismes cryptographiques [CRYPTO_B2].

e) Le prestataire doit configurer les solutions de filtrage (voir exigence IV.3.10.b) pour n'autoriser que les flux initiés depuis le(s) dépôt(s) relais vers la passerelle internet.

IV.3.12. Zone de notification

a) Lorsque des systèmes de messagerie électronique sont utilisés dans le cadre de la gestion des notifications, ceux-ci doivent être dédiés aux activités de notification dans le cadre de prestations qualifiées ou ne dégradant pas le niveau de sécurité du système d'information du service, et hébergés dans la zone de notification.

b) Le dispositif de filtrage (voir exigence IV.3.10.b) à l'interconnexion du système d'information du service de détection, entre l'extérieur du système d'information du service et la zone

de notification, ne doit autoriser que les flux émis depuis la zone de notification pour l'envoi d'information non sensible (exemples : notification d'incident de sécurité).

IV.3.13. Zone d'échange commanditaire

a) Le prestataire doit mettre en place une zone d'échange commanditaire contenant au minimum :

- un portail Web permettant la visualisation et la mise à jour de l'état des incidents de sécurité et des actions engagées ;
- un dispositif de stockage permettant la mise à disposition du commanditaire des contextes des incidents de sécurité détectés sur son périmètre supervisé (évènements associés et rapport(s) d'analyse(s) de qualification), et permettant au commanditaire de déposer s'il le souhaite des informations nécessaires à la qualification d'un incident.

Le prestataire doit respecter les exigences relatives à la zone d'échange décrites au chapitre « Système d'échange » de la note technique [NT_ADMIN].

Remarque : les outils d'analyse de contenu malveillant peuvent être mutualisés entre la zone d'échange commanditaire et la zone de collecte.

Le prestataire doit prévoir, pour les outils d'analyse de contenu malveillant, un traitement spécifique pour les fichiers chiffrés ou ne pouvant être analysés.

Le prestataire doit mettre en place la journalisation de l'*horodate*, du nom et de l'empreinte cryptographique de tous les fichiers transitant par les outils d'analyse de contenu malveillant.

b) Le prestataire doit dédier une machine physique ou virtuelle par commanditaire afin d'y héberger une instance du portail web et du dispositif de stockage des incidents de sécurité et des notifications.

c) Le prestataire doit mettre en place un annuaire dédié à l'authentification du commanditaire sur les dispositifs hébergés dans la zone d'échange commanditaire. Le prestataire doit authentifier le commanditaire avec :

- des comptes nominatifs et au minimum deux facteurs pour l'authentification d'une personne vis-à-vis d'une machine ;
- une authentification mutuelle pour l'authentification de machine à machine.

Le prestataire doit tenir à jour une liste des comptes autorisés à accéder à cette zone avec leurs privilèges associés.

d) Il est recommandé que le prestataire mette en œuvre une authentification aux dispositifs de la zone d'échange commanditaire basée sur des certificats électroniques délivrés par des prestataires de services de certification électroniques qualifiés par l'ANSSI RGS *** et impliquant par conséquent l'utilisation de supports cryptographiques qualifiés par l'ANSSI au niveau renforcé.

e) Le prestataire doit mettre en œuvre les mesures garantissant que le commanditaire n'accède qu'aux ressources utiles dans le cadre de sa prestation.

f) Le prestataire doit appliquer des mesures privant le commanditaire de droits d'administration ou d'exploitation sur les dispositifs du service de détection.

g) Le prestataire doit mettre en œuvre un pare-feu applicatif afin de filtrer les requêtes à destination du portail web.

h) Le dispositif de filtrage (voir exigence IV.3.10.b) entre la zone d'échange commanditaire et le système d'information interne du commanditaire doit interdire tous les flux exceptés :

- ceux entre cette zone d'échange commanditaire et l'enclave de consultation au sein du système d'information interne du commanditaire, permettant uniquement la consultation et la mise à jour de l'état des incidents et actions engagées via le portail web et l'échange sécurisé d'information entre ces deux zones ;

- ceux entre cette zone d'échange commanditaire et les postes nomades de consultation (voir exigence IV.3.17.l) permettant uniquement la consultation et la mise à jour de l'état des incidents et actions engagées via le portail web et l'échange sécurisé d'information avec ces postes ;
- ceux permettant au prestataire d'administrer depuis la zone d'administration (voir exigence IV.3.8.b) les dispositifs hébergés dans l'enclave de consultation[11] ;
- ceux permettant la mise à jour des dispositifs hébergés dans l'enclave de consultation à partir de la zone de mise à jour[11] (voir exigence IV.3.8.b).

IV.3.14. Enclave de consultation au sein du système d'information du commanditaire

a) L'intégralité des dispositifs pouvant accéder à la zone d'échange commanditaire depuis le système d'information interne du commanditaire doit être positionnée au sein d'une ou plusieurs[12] enclaves de consultation au sein de ce système d'information.

b) Le prestataire doit définir avec le commanditaire dans la convention de service les responsabilités concernant :
   - la propriété des dispositifs hébergés dans l'enclave de consultation ;
   - l'administration et la mise à jour de ces dispositifs ;
   - le respect des mesures de sécurité définies dans les exigences IV.3.14.c) à IV.3.14.g).

c) L'enclave de consultation doit être homologuée au minimum au niveau *Diffusion Restreinte* [IGI_1300] [II_901].

   Remarque : l'entité (prestataire ou commanditaire) en charge de l'homologation doit demander à l'autre entité les éléments de preuve de la mise en œuvre des mesures dont cette dernière a la responsabilité et les porter au dossier d'homologation.

d) Il est recommandé que le prestataire fasse appel à une prestation qualifiée d'audit de la sécurité des systèmes d'information par un PASSI pour la réalisation de l'audit dans le cadre de l'homologation.

e) Les postes de travail utilisés par le commanditaire pour accéder à la zone d'échange commanditaire doivent être dédiés à cette fin et hébergés dans l'enclave de consultation (en cas d'accès nomade à la zone d'échange commanditaire, les exigences du chapitre IV.3.17 doivent être respectées).

f) Les utilisateurs des postes de travail de l'enclave de consultation ne doivent pas disposer des droits d'administration sur leur poste.

g) Le cloisonnement de l'enclave de consultation doit être réalisé par :
   - un dispositif de filtrage entre cette enclave et le système d'information du service de détection des incidents de sécurité du prestataire ;
   - des dispositifs de filtrage et de rupture de flux entre cette enclave et le système d'information interne du commanditaire, conformément aux exigences de cloisonnement des réseaux de l'Annexe 2 de l'instruction interministérielle relative à la protection des systèmes d'information sensibles [II_901].

h) Le dispositif de filtrage entre cette enclave de consultation et le système d'information interne du commanditaire doit interdire tous les flux, excepté ceux initiés depuis l'enclave de consultation vers le système d'information interne du commanditaire.

[11] Uniquement si le commanditaire autorise le prestataire à administrer un ou plusieurs dispositifs hébergés dans cette enclave (voir exigence IV.3.14.b).

[12] À des fins de simplification, il est fait l'hypothèse dans la suite du document qu'il n'y a qu'une enclave de consultation.

i) Il est recommandé de mettre en place à l'interconnexion entre l'enclave de consultation et le système d'information interne du commanditaire une diode agréée par l'ANSSI, utilisée conformément aux conditions de son agrément, pour garantir le caractère unidirectionnel des flux depuis l'enclave de consultation vers le système d'information interne du commanditaire.

IV.3.15. Enclave de collecte au sein du système d'information du commanditaire

a) L'intégralité des dispositifs du service de détection des incidents de sécurité interconnectés au périmètre supervisé (en particulier les collecteurs) doit être positionnée au sein d'une ou plusieurs[13] enclaves de collecte au sein du système d'information interne du commanditaire.

b) Le prestataire doit définir avec le commanditaire dans la convention de service les responsabilités concernant :

- la propriété des dispositifs hébergés dans l'enclave de collecte ;
- le respect des mesures de sécurité définies dans les exigences IV.3.15.d) et IV.3.15.s).

c) Le prestataire doit formaliser dans la convention de service les responsabilités suivantes en matière d'administration et d'exploitation des dispositifs hébergés dans l'enclave de collecte :

- le commanditaire doit avoir la responsabilité de l'administration du dispositif de filtrage entre cette enclave de collecte et le système d'information interne du commanditaire (voir IV.3.15.l) ;
- le prestataire doit avoir la responsabilité de l'administration et de l'exploitation de l'ensemble des autres dispositifs hébergés dans l'enclave de collecte, dont le dispositif de filtrage entre cette enclave de collecte et l'équipement utilisé pour le chiffrement et l'authentification *IPsec* des flux échangés avec le système d'information du prestataire.

d) L'enclave de collecte ne doit héberger que les dispositifs permettant d'assurer le service de détection des incidents de sécurité, à savoir :

- les dispositifs impliqués dans la supervision (sondes, *Tap*, agrégateurs) ;
- les dispositifs de collecte des évènements (collecteurs locaux) ;
- le dépôt relais permettant le transfert d'informations contextuelles du commanditaire ;
- les dispositifs de filtrage assurant le cloisonnement de cette enclave (voir exigence IV.3.15.l) ;
- les dispositifs permettant de protéger la confidentialité et l'authenticité des informations échangées entre cette enclave et le système d'information du service de détection des incidents de sécurité.

e) L'enclave de collecte doit être homologuée au minimum au *Niveau Standard* du guide d'hygiène informatique de l'ANSSI [HYGIENE]. La démarche d'homologation de cette enclave doit inclure une prestation qualifiée d'audit de la sécurité des systèmes d'information par un PASSI.

f)

Remarque : l'entité (prestataire ou commanditaire) en charge de l'homologation doit demander à l'autre entité les éléments de preuve de la mise en œuvre des mesures dont cette dernière à la responsabilité, et les porter au dossier d'homologation.

g) Il est recommandé d'appliquer les exigences du chapitre IV.3.2 concernant la protection de l'information au sein du service de détection des incidents de sécurité du prestataire à cette enclave.

[13] À des fins de simplification, il est fait l'hypothèse dans la suite du document qu'il n'y a qu'une enclave de collecte.

h) Les dispositifs impliqués dans la chaîne de supervision (sondes, *Tap* et agrégateurs) doivent être reliés par un lien réseau physiquement dédié.

i) Le prestataire doit administrer et opérer les dispositifs hébergés dans l'enclave de collecte à partir respectivement des zones d'administration et d'exploitation de son système d'information du service de détection des incidents de sécurité (voir exigence IV.3.8.b).

j) Le prestataire ne doit en aucun cas disposer de droits sur le dispositif de filtrage entre l'enclave de collecte et le système d'information interne du commanditaire (voir exigence IV.3.15.l).

k) Le prestataire doit appliquer les recommandations définies dans la note technique de l'ANSSI consacrée à la mise en œuvre d'un système de journalisation [NT_JOURNAL].

l) Le cloisonnement de l'enclave de collecte doit être réalisé par :

- un dispositif de filtrage entre cette enclave et le système d'information interne du commanditaire ;
- un dispositif de filtrage entre cette enclave et le système d'information du service de détection des incidents de sécurité du prestataire.

m) Le dispositif de filtrage entre cette enclave de collecte et le système d'information interne du commanditaire doit interdire tous les flux exceptés ceux initiés depuis le périmètre supervisé vers cette zone et permettant :

- aux sources de collecte hébergées sur le périmètre supervisé de transmettre les évènements à cette zone à destination d'un collecteur, excluant des actions de commande vers des éléments logiciels du système d'information supervisé ;
- le cas échéant, aux référentiels centralisés du commanditaire (exemple : base de données de gestion de configuration) de déposer automatiquement des fichiers d'informations contextuelles propres à son système d'information sur le dépôt relais.

n) Il est recommandé de mettre en place à l'interconnexion entre l'enclave de collecte et le système d'information interne du commanditaire une diode agréée par l'ANSSI, utilisée conformément aux conditions de son agrément, pour garantir le caractère unidirectionnel des flux depuis le système d'information interne du commanditaire vers l'enclave de collecte.

o) Les collecteurs doivent être configurés uniquement en écoute des sources de collecte. Aucun flux ne doit être initié par les collecteurs vers les sources de collecte.

p) Il est recommandé de mettre en œuvre un collecteur intermédiaire sous la responsabilité du commanditaire lorsque les sources de collecte ne peuvent pas transmettre directement les évènements aux collecteurs dans la zone de collecte.

q) Le dispositif de filtrage entre l'enclave de collecte et le système d'information du service de détection des incidents de sécurité du prestataire doit interdire tous les flux exceptés :

- ceux initiés depuis cette enclave de collecte vers le système d'information du service de détection des incidents de sécurité du prestataire et permettant uniquement de transmettre les évènements et fichiers d'informations contextuelles transmis par le commanditaire, de cette enclave vers la zone de collecte. Le prestataire doit limiter au maximum le nombre de flux permettant la remontée des évènements et fichiers de cette enclave vers le système d'information du service de détection ;
- ceux permettant au prestataire d'administrer depuis la zone d'administration (voir exigence IV.3.8.b) les dispositifs hébergés dans cette enclave de collecte ;
- ceux permettant au prestataire d'opérer depuis la zone d'exploitation (voir exigence IV.3.8.b) les dispositifs hébergés dans cette enclave de collecte ;
- ceux permettant la mise à jour des dispositifs de l'enclave de collecte à partir de la zone de mise à jour (voir exigence IV.3.8.b).

r) Un dépôt relais peut être mis en place dans l'enclave de collecte pour permettre la transmission automatique d'informations contextuelles depuis le système d'information interne du commanditaire.

Le cas échéant, le dépôt relais doit être configuré uniquement en écoute des référentiels centralisés du commanditaire. Aucun flux ne doit être initié par le dépôt relais vers le système d'information interne du commanditaire.

L'exigence suivante s'applique uniquement dans le cas de la mise en place d'un tel dépôt relais.

s) Le prestataire doit mettre en place un système d'échange au sein de sa zone de collecte, permettant le transfert de fichiers depuis le dépôt relais de l'enclave de collecte vers le système d'information du service de détection. Le prestataire doit respecter les exigences relatives à la zone d'échange décrites au chapitre « Système d'échange » de la note technique [NT_ADMIN].

Remarque : les outils d'analyse de contenu malveillant peuvent être mutualisés entre la zone de collecte et la zone d'échange commanditaire.

Le prestataire doit prévoir, pour les outils d'analyse de contenu malveillant, un traitement spécifique pour les fichiers chiffrés ou ne pouvant être analysés.

Le prestataire doit mettre en place la journalisation du nom et empreinte cryptographique de tous les fichiers transitant par les outils d'analyse de contenu malveillant.

IV.3.16. Zone internet au sein du système d'information du prestataire

a) Le prestataire doit mettre en place en dehors du système d'information du service de détection une zone internet contenant des postes de travail dédiés utilisés par les opérateurs et administrateurs pour accéder à internet ou à d'autres systèmes d'information (système d'information interne du prestataire par exemple). La zone internet doit être déconnectée des systèmes d'information du commanditaire.

b) Les postes de travail hébergés dans la zone internet doivent être physiquement dédiés à la zone internet (dédiés à l'accès à d'autres systèmes d'information que le système d'information du service de détection).

c) L'ensemble des flux sortant de la zone internet vers internet doit transiter par un serveur mandataire puis par une sortie vers internet distincte de celle utilisée par le système d'information du commanditaire.

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

e) La zone internet doit être homologuée au minimum au *Niveau Standard* du guide d'hygiène informatique de l'ANSSI [HYGIENE].

f) Le prestataire doit horodater et journaliser les recherches en sources ouvertes réalisées.

g) Il est recommandé que le prestataire journalise tous les accès aux dispositifs hébergés dans la zone internet ainsi que les actions réalisées, et applique les recommandations définies dans la note technique de l'ANSSI consacrée à la mise en œuvre d'un système de journalisation [NT_JOURNAL].

h) Il est recommandé que les journaux de la zone internet alimentent les outils d'analyse du service de détection des incidents de sécurité interne.

i) Si les journaux de la zone internet sont collectés, la collecte doit être réalisée via une zone d'échange exploitation du service de détection des incidents de sécurité ou par la mise en place d'une enclave de collecte comme pour un commanditaire classique.

j) Le dispositif de filtrage entre la zone internet et le système d'information du service de détection (voir exigence IV.3.10.b) doit interdire tous les flux exceptés :

- ceux initiés depuis la zone internet vers les zones d'échange et permettant aux postes de travail hébergés dans la zone internet de déposer ou collecter des fichiers dans les zones d'échange ;
- si la collecte des journaux de la zone internet est effectuée, ceux permettant aux dispositifs hébergés dans la zone internet de transmettre les journaux d'évènements à la zone d'échange exploitation du service de détection des incidents de sécurité interne.

IV.3.17. Accès nomades

a) En cas d'accès distant au système d'information du service de détection des incidents de sécurité, le prestataire doit mettre en place :
   - au minimum une passerelle dédiée à l'administration et l'exploitation[14] des dispositifs du service de détection ;
   - le cas échéant, une passerelle dédiée à l'accès distant du commanditaire à la zone d'échange commanditaire, distincte de(s) passerelle(s) d'administration et d'exploitation.

b) Dans le cas où l'accès à la zone d'échange commanditaire par des postes nomades de consultation est autorisé, le prestataire doit définir avec le commanditaire dans la convention de service les responsabilités concernant :
   - la propriété des postes nomades de consultation ;
   - l'administration et la mise à jour de ces dispositifs ;
   - le respect des mesures de sécurité définies dans les exigences IV.3.17.e) à IV.3.17.l).

c) Il est recommandé de mettre en place des passerelles d'administration et d'exploitation distinctes.

d) Les postes nomades utilisés par les administrateurs et les opérateurs doivent être dédiés aux prestations qualifiées et à toute prestation respectant les exigences de la partie IV.3 - Protection de l'information.

e) Les postes nomades utilisés par le commanditaire doivent être dédiés à l'accès à la zone d'échange commanditaire.

f) En cas d'utilisation d'une passerelle unique pour les accès distants des administrateurs et des opérateurs, le prestataire doit mettre en œuvre une solution permettant d'assurer une séparation stricte des flux :
   - d'administration depuis les postes nomades d'administration jusqu'à la zone d'administration ;
   - d'exploitation depuis les postes nomades d'exploitation jusqu'à la zone d'exploitation.

g) Les flux entre les postes nomades et les passerelles sont chiffrés à l'aide de solutions de chiffrement et d'authentification *IPsec* agréées par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur agrément.

h) Les administrateurs, opérateurs et utilisateurs des postes nomades de consultation doivent s'authentifier avec au minimum deux facteurs.

i) Il est recommandé que le prestataire mette en œuvre pour les accès distants une authentification basée sur des certificats électroniques délivrés par des prestataires de services de certification électronique qualifiés par l'ANSSI RGS *** et impliquant par conséquent l'utilisation de supports cryptographiques qualifiés par l'ANSSI au niveau renforcé.

j) Les postes nomades doivent être durcis, configurés pour ne pouvoir communiquer qu'avec la passerelle d'accès distant dédiée via une connexion *IPsec* chiffrée et authentifiée, ne permettre

[14] Conformément à la note technique [NT_ADMIN].

que l'usage de supports amovibles autorisés par la politique de sécurité des systèmes d'information, et avoir l'intégralité de leurs disques chiffrée à l'aide d'une solution de chiffrement agréée par l'ANSSI au minimum au niveau *Diffusion Restreinte* et utilisée conformément aux conditions de son agrément.

k) Le prestataire doit prévoir les mécanismes de mise à jour et d'administration des postes nomades dans le cas où il les fournit au commanditaire et les administre.

l) Le prestataire doit configurer les solutions de filtrage (voir exigence IV.3.10.b) pour n'autoriser que les flux :

- initiés depuis les postes nomades d'administration vers la zone d'administration (voir exigence IV.3.8.b) ;
- initiés depuis les postes nomades d'exploitation vers la zone d'exploitation (voir exigence IV.3.8.b) ;
- initiés depuis les postes nomades de consultation vers la zone d'échange commanditaire (voir exigence IV.3.8.b) ;
- initiés depuis la zone d'administration (voir exigence IV.3.8.b) vers les postes nomades pour l'administration des postes qu'il fournit et administre ;
- initiés depuis les postes nomades vers la zone de mise à jour (voir exigence IV.3.8.b) pour la mise à jour des postes qu'il fournit et administre.

IV.4. Organisation du prestataire et gouvernance

IV.4.1. Charte d'éthique et recrutement

a) Le prestataire doit procéder à une vérification des formations, qualifications, références professionnelles des candidats pour le service de détection et de la véracité de leur *curriculum vitae* préalablement à leur embauche.

b) Le prestataire doit demander aux candidats de lui fournir une preuve qu'ils ne font pas l'objet d'une inscription au bulletin n° 3 du casier judiciaire.

c) Les opérateurs, les administrateurs et les experts du service de détection doivent être liés contractuellement avec le prestataire ou avec un de ses sous-traitants dans le cas de la sous-traitance d'une partie de son activité.

d) Le prestataire doit disposer d'une charte d'éthique intégrée au règlement intérieur, prévoyant notamment que :

- les prestations sont réalisées avec loyauté, discrétion et impartialité ;
- les personnels ne recourent qu'aux méthodes, outils et techniques validés par le prestataire ;
- les personnels s'engagent à ne pas divulguer d'informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de la prestation sauf autorisation formelle et écrite du commanditaire ;
- les personnels s'engagent à signaler au prestataire tout contenu manifestement illicite découvert pendant la prestation ;
- les personnels s'engagent à respecter la législation et la réglementation nationale en vigueur et les bonnes pratiques liées à leurs activités.

e) Le prestataire doit faire signer à l'ensemble de son personnel la charte d'éthique prévue à l'exigence précédente et préalablement à la réalisation de la prestation.

f) Le prestataire doit veiller au respect de la charte d'éthique et prévoir des sanctions disciplinaires à l'intention des opérateurs, des administrateurs et des experts du service de détection ayant enfreint les règles de sécurité ou la charte d'éthique.

g) Le prestataire doit élaborer et mettre en œuvre un plan de sensibilisation de son personnel à la sécurité des systèmes d'information et des mesures de sécurité associées ainsi qu'à la législation et la réglementation nationale en vigueur en rapport avec le service de détection des incidents de sécurité.

IV.4.2. Organisation et gestion des compétences

a) Le prestataire doit disposer d'une équipe :

- assurant au minimum les missions décrites dans l'Annexe 2 ;
- disposant des compétences associées à ces missions.

b) Le prestataire doit définir et formaliser la liste exhaustive :

- des rôles d'administrateur de son service de détection des incidents de sécurité et des missions associées ;
- des rôles d'opérateur de son service de détection des incidents de sécurité et des missions associées.

Cette liste doit au minimum inclure les rôles d'opérateur analyste et administrateur d'infrastructure (cf. Annexe 2).

Le prestataire doit justifier de la compatibilité des rôles d'opérateurs entre eux et des rôles d'administrateurs entre eux, notamment vis-à-vis des ressources accédées, selon les principes du moindre privilège et du besoin d'en connaître.

c) Le prestataire doit employer un nombre suffisant de personnels et éventuellement recourir à la sous-traitance (voir chapitre IV.5.3.7 intitulé « Sous-traitance ») pour assurer totalement et dans tous ses aspects la prestation qualifiée.

d) Le prestataire doit élaborer et mettre en œuvre un plan de formation à destination de l'équipe du service de détection et adapté à ses missions.

e) Le prestataire doit élaborer et mettre à disposition des personnels les guides d'exploitation ou d'administration des dispositifs du service de détection des incidents de sécurité.

f) Il est recommandé que le prestataire mette en place des astreintes lui permettant la mobilisation d'une partie de son équipe en dehors des heures ouvrées.

g) Le prestataire doit disposer en interne d'un centre de veille, d'alerte aux attaques d'informatiques ou souscrire à un tel service.

h) Il est recommandé que le centre de veille, d'alerte aux attaques d'informatiques soit référencé par le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR).

i) Le prestataire doit mettre à disposition du commanditaire un service d'assistance à distance permettant notamment :

- au commanditaire de déclarer au prestataire un incident de sécurité suspecté ou avéré ;
- au prestataire d'aider le commanditaire à la résolution de problèmes de production liés aux dispositifs gérés par le prestataire ;
- au prestataire d'assister et de conseiller le commanditaire.

j) Le prestataire doit rendre le service d'assistance accessible via un numéro téléphonique ou une adresse *mail*.

k) Le prestataire doit mettre en œuvre les mécanismes permettant d'échanger avec le commanditaire des informations au minimum de niveau *Diffusion Restreinte* via le service d'assistance.

l) Le prestataire doit désigner un référent opérationnel pour le commanditaire. Il est l'interlocuteur privilégié concernant le fonctionnement opérationnel du service de détection des incidents de sécurité et le suivi des incidents de sécurité détectés. Le prestataire doit informer le commanditaire de tout changement de l'interlocuteur opérationnel pour le service de détection des incidents de sécurité.

m) Il est recommandé au commanditaire de désigner un référent opérationnel pour le service de détection des incidents de sécurité.

n) Les référents opérationnels doivent participer aux comités opérationnels et stratégiques définis dans le chapitre IV.4.3.

IV.4.3. Comités opérationnels et stratégiques

IV.4.3.1. Comité opérationnel

a) Le prestataire doit mettre en place et animer en présence du commanditaire un comité opérationnel, au minimum une fois par trimestre.

b) Il est recommandé que le prestataire organise un comité opérationnel une fois par mois.

c) Le comité opérationnel doit traiter au minimum des sujets suivants :

- bilan du service de détection des incidents de sécurité :
  - revue des indicateurs opérationnels (voir chapitre IV.5.1) selon un cycle de revue de chaque indicateur convenu avec le commanditaire ;
  - revue des incidents de sécurité détectés ;
  - revue des stratégies de collecte, d'analyse et de notification ;
  - revue de la liste des règles de détection (voir exigence IV.2.1.i) ;
  - revue des bulletins d'état des règles de détection (voir exigence IV.2.1.j).
- périmètre du service de détection des incidents de sécurité :
  - revue du contexte du commanditaire ;
  - revue des changements concernant le système d'information du commanditaire ;
  - présentation des projets d'évolutions impactant le périmètre du service ;
  - revue de la liste des incidents de sécurité redoutés.
- amélioration du service de détection des incidents de sécurité :
  - revue des indicateurs de qualité (voir chapitre IV.5.1) selon un cycle de revue de chaque indicateur convenu avec le commanditaire ;
  - analyse des évolutions opérationnelles du service de détection des incidents de sécurité (évolution de l'outillage, modification d'un processus opérationnel, etc.) ;
  - présentation des règles de détection créées, modifiées ou retirées ;

d) Le prestataire doit rédiger un compte rendu à la suite de chaque comité opérationnel et le transmettre au commanditaire pour validation. Ce compte rendu doit contenir au minimum la liste des participants, les décisions prises en comités et le plan d'action associé.

e) Le prestataire doit protéger le compte rendu du comité opérationnel, en particulier en matière de confidentialité, en tenant compte du niveau de sensibilité ou de classification de son contenu.

f) Le prestataire doit stocker et archiver les supports des comités opérationnels et comptes rendus associés dans un espace spécifique au sein de l'infrastructure du service de détection, avec un cloisonnement des données au minimum logique entre les commanditaires.

IV.4.3.2. Comité stratégique

a) Le prestataire doit mettre en place et animer en présence de représentants de la direction du commanditaire un comité stratégique, au minimum une fois par an.

b) Il est recommandé que le prestataire organise un comité stratégique une fois par semestre.

c) Le comité stratégique doit traiter au minimum des sujets suivants :

- revue des indicateurs stratégiques (voir chapitre IV.5.1) ;
- revue de la convention de service ;
- revue du plan de réversibilité ;
- présentation consolidée de l'efficacité du service de détection ;
- revue et anticipation de la menace.

d) Le prestataire doit rédiger un compte rendu à la suite de chaque comité stratégique et le transmettre au commanditaire pour validation. Ce compte rendu doit contenir au minimum les participants et les décisions prises en comité.

e) Le prestataire doit protéger le compte rendu du comité stratégique, en particulier en matière de confidentialité, en tenant compte du niveau de sensibilité ou de classification de son contenu.

f) Le prestataire doit stocker et archiver les supports des comités stratégiques et comptes rendus associés dans un espace spécifique au sein de l'infrastructure du service de détection, avec un cloisonnement des données au minimum logique entre les commanditaires.

IV.5. Qualité et niveau de service

IV.5.1. Qualité du service

a) Il est recommandé que le prestataire soit certifié [ISO9001] sur le périmètre du service de détection des incidents de sécurité.

b) Le prestataire doit élaborer et mettre en œuvre un processus de capitalisation sur les incidents de sécurité détectés afin d'améliorer continuellement l'efficacité de son service de détection.

c) Le prestataire doit définir avec le commanditaire les indicateurs opérationnels et stratégiques du service de détection des incidents de sécurité.

d) Il est recommandé que le prestataire utilise les indicateurs proposés dans [ETSI_ISG_ISI].

e) Le prestataire doit au minimum mettre en place les indicateurs opérationnels d'activité suivants :

- gestion de l'infrastructure support du service de détection
    - le taux de remplissage des systèmes de stockage des incidents,
    - la capacité restante des systèmes de stockage des incidents,
    - le taux de disponibilité des dispositifs techniques du service de détection :
        - portail web de la zone d'échange commanditaire ;
        - dépôt relais de l'enclave de collecte ;
        - collecteur de l'enclave de collecte ;
        - système d'envoi des notifications d'incidents ;

    - outils techniques d'analyse ;
    - etc.

- gestion de la sécurité des interconnexions du SI du service de détection
    - le nombre d'échecs d'authentification et authentifications réussies ainsi que la liste détaillée associée concernant :
        - l'accès à la zone d'échanges commanditaire ;
        - l'accès depuis des postes nomades d'exploitation ;
        - l'accès depuis des postes nomades d'administration.
- gestion des capacités de détection
    - le nombre d'alertes de sécurité détectées par mois ;
    - le nombre d'incidents avérés suite à une qualification par mois ;
    - le nombre de règles de détection implémentées dans les outils techniques d'analyse ;
    - le nombre de règles de détection créées, modifiées ou retirées par mois en fonction de l'origine de la demande (activité de veille, demande du commanditaire, etc.) ;
    - le classement des 20 règles de détection les plus déclenchées.
- gestion des incidents
    - le nombre de nouveaux tickets d'incidents ouverts par mois ;
    - le nombre de tickets d'incidents de sécurité clos par mois ;
    - le nombre de tickets ouverts cumulé par mois ;
    - la durée minimale, moyenne, maximale entre la création d'un ticket et sa clôture ;
    - le nombre d'incidents créés selon le niveau de gravité de l'incident.
- gestion des évènements
    - le nombre d'évènements non reconnus et donc non pris en compte par les outils techniques d'analyse ;
    - le taux d'évènements non reconnus et donc non pris en compte par les outils techniques d'analyse ;
    - le nombre de sources de collecte par type d'équipement source ;
    - le nombre de collecteurs ;
    - le nombre d'évènements collectés par jour et par mois ;
    - le nombre d'évènements collectés par collecteur par jour et par mois ;
    - le nombre d'évènements transmis au système de stockage par jour et par mois ;
    - le taux de remplissage de chaque système de stockage des évènements, y compris les collecteurs dans l'enclave ;
    - la capacité restante de chaque système de stockage des évènements, y compris les collecteurs dans l'enclave ;
    - la capacité de rétention des collecteurs si la communication est impossible (lien réseau coupé par exemple) avec le collecteur supérieur (en volumétrie et en temps).
- gestion des notifications

- le nombre de comptes autorisés à accéder au portail web et pouvant accéder aux informations du commanditaire,
- le nombre de comptes d'accès au portail web créés par mois,
- le nombre de comptes d'accès au portail web supprimés par mois.

f) Le prestataire doit au minimum mettre en place les indicateurs opérationnels d'efficacité suivants :

- gestion des capacités de détection
  - le délai moyen de mise à jour des règles de détection suite à une demande du commanditaire ;
  - le temps de recherche moyen d'un indicateur de compromission, lors d'une recherche *a posteriori*, dans le système de stockage, par type d'indicateur de compromission.
- gestion des incidents
  - la durée moyenne des qualifications d'incident, par typologie d'incident et selon son niveau de gravité.
- gestion des évènements
  - la durée minimale, moyenne, maximale entre la génération d'un évènement par la source de collecte et son stockage dans les systèmes de stockage des évènements.
- gestion des notifications
  - la durée minimale, moyenne, maximale entre la détection d'un évènement de sécurité et la notification d'un incident associé, selon le niveau de gravité de l'incident.

g) Le prestataire doit au minimum mettre en place les indicateurs stratégiques suivants :

- gestion de la sécurité des interconnexions du SI du service de détection
  - l'évolution du nombre d'anomalies et incidents relevés concernant les différents accès externes au SI du service de détection ;
- gestion de l'infrastructure support du service de détection
  - l'évolution par mois du taux de disponibilité des dispositifs techniques du service de détection :
    - portail web de la zone d'échanges commanditaire ;
    - dépôt relais de l'enclave de collecte ;
    - collecteur de l'enclave de collecte ;
    - système d'envoi des notifications d'incidents ;
    - outils techniques d'analyse ;
    - etc.
- gestion des capacités de détection
  - les écarts identifiés par rapport aux différents SLA définis.
- gestion des incidents
  - l'évolution du temps moyen de traitement des tickets d'incidents, par criticité, par mois ;
  - l'évolution du nombre de tickets d'incidents ouverts cumulé, par criticité, par mois ;
  - le nombre d'incidents avérés par mois pour le périmètre du service de détection du commanditaire.

- gestion des évènements
    - l'évolution du taux de couverture de collecte des journaux des équipements du parc identifiés dans la stratégie de collecte.

h) Le prestataire doit élaborer et tenir à jour un processus de mesure des indicateurs décrivant, pour chacun des indicateurs opérationnels et stratégiques définis, les méthodes et moyens mis en œuvre par le prestataire pour mesurer l'indicateur.

IV.5.2. Réversibilité

a) Le prestataire doit élaborer avec le commanditaire un plan de réversibilité du service de détection des incidents de sécurité permettant une reprise du service par le commanditaire ou un autre prestataire de service.

b) Le plan de réversibilité doit au minimum contenir les éléments suivants :

- l'inventaire exhaustif des informations et matériels à restituer ;
- la durée de réversibilité ;
- les intervenants et les actions requises par chacun d'eux ;
- les formats des informations à restituer ;
- les moyens de restitution.

Le prestataire doit être capable, si le commanditaire en fait la demande, de restituer les évènements de sécurité stockés ainsi que les règles de détection spécifiques au commanditaire du service.

c) La durée de réversibilité doit être au minimum de trois mois.

d) Il est recommandé que la durée de réversibilité soit de six mois.

e) Le prestataire doit assurer le maintien en conditions opérationnelles du service de détection des incidents de sécurité durant la mise en œuvre du plan de réversibilité.

f) Le prestataire doit détruire l'ensemble des informations relatives au commanditaire à l'issue de l'exécution du plan de réversibilité à l'exception de celles pour lesquelles il a reçu une autorisation de conservation de la part du commanditaire (voir exigence IV.5.3.4.a).

IV.5.3. Convention de service

IV.5.3.1. Modalités de la prestation

a) La convention de service doit :

- décrire le périmètre et les objectifs de la prestation, le service de détection des incidents de sécurité et notamment les activités de gestion des évènements, des incidents et des notifications ;
- décrire les moyens techniques et organisationnels mis en œuvre par le prestataire dans le cadre de sa prestation ;
- décrire la localisation du stockage et du traitement des données, ainsi que celle de l'exploitation et de l'administration du service de détection ;
- définir les livrables attendus dans le cadre de la prestation, les publics destinataires, leur niveau de sensibilité ou de classification ainsi que les modalités associées ;
- décrire les méthodes de communication qui seront employés lors de la prestation entre le prestataire et le commanditaire ;

- définir les règles de titularité des éléments protégés par la propriété intellectuelle tels que les livrables, les outils et les règles de détection développés spécifiquement par le prestataire dans le cadre de la prestation ;
- décrire le processus d'enregistrement et de traitement des plaintes portant sur la prestation déposées par le commanditaire ou par des tiers, ainsi que la marche à suivre pour le dépôt de plainte.

IV.5.3.2. Organisation du service

a) La convention de service doit :

- stipuler que le prestataire désigne un interlocuteur auprès du commanditaire en charge d'assurer le suivi opérationnel de la prestation ;
- stipuler que le prestataire et le commanditaire identifient les noms, rôles, responsabilités ainsi que les droits et besoins d'en connaître des personnes intervenant dans le cadre de la prestation. Cette clause est d'autant plus importante si l'existence d'un incident de sécurité ne doit pas être rendue publique ;
- stipuler que le prestataire collabore avec des tiers mandatés par le commanditaire et spécifiquement désignés par ce dernier. Cette clause doit notamment permettre au prestataire de collaborer avec un prestataire de réponse aux incidents de sécurité mandaté par le commanditaire en cas d'incident de sécurité suspecté ou avéré ;
- stipuler que le prestataire ne fait pas intervenir de personnels n'ayant pas de relation contractuelle avec lui, n'ayant pas signé sa charte d'éthique ou ayant fait l'objet d'une inscription au bulletin n°3 du casier judiciaire ;
- stipuler si le prestataire autorise l'accès distant des administrateurs et des opérateurs au système d'information du service de détection des incidents de sécurité.

IV.5.3.3. Responsabilités

a) La convention de service doit :

- stipuler que le prestataire ne débute la prestation qu'après approbation formelle et écrite par le commanditaire de la convention de service ;
- stipuler que le prestataire informe le commanditaire en cas de manquement à la convention de service ;
- stipuler que le prestataire informe le commanditaire en cas d'incident de sécurité détecté sur le système d'information du service de détection des incidents de sécurité, et le délai maximal autorisé pour transmettre l'information suite à un incident ;
- stipuler que le prestataire ne réalise que des actions strictement en adéquation avec les objectifs de la prestation ;
- stipuler que le commanditaire dispose de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.) ou qu'il a recueilli l'accord des éventuels tiers, et notamment de ses prestataires ou partenaires, dont les systèmes d'information entrent dans le périmètre de la prestation ;
- stipuler que le commanditaire remplit toutes les obligations légales nécessaires à la prestation et notamment celles relatives à la collecte et à l'analyse d'informations ;
- définir les responsabilités et les précautions à respecter par l'ensemble des parties concernant les risques potentiels liés à la prestation, notamment en matière de confidentialité des informations collectées et analysées ainsi qu'en matière de disponibilité et d'intégrité du système d'information du commanditaire ;

- stipuler que le prestataire dispose d'une assurance professionnelle couvrant les éventuels dommages causés au commanditaire et notamment à son système d'information dans le cadre de sa prestation, préciser la couverture de l'assurance et inclure l'attestation d'assurance ;
- définir les responsabilités entre le prestataire et le commanditaire concernant les enclaves de collecte et de consultation au sein du système d'information du commanditaire, conformément aux exigences IV.3.14.b), IV.3.15.b) et IV.3.15.c) ;
- stipuler que le prestataire a mis en place une procédure de gestion des changements concernant son propre système d'information ;
- stipuler que le prestataire a mis en place une procédure d'amélioration permanente de l'efficacité de son service de détection s'appuyant notamment sur les indicateurs opérationnels mentionnés dans la partie IV.5.1.

IV.5.3.4. Confidentialité et protection de l'information

a) La convention de service doit :

- identifier le niveau de sensibilité ou de classification du service de détection des incidents de sécurité mis en œuvre par le prestataire ;
- identifier le niveau de sensibilité ou de classification du périmètre supervisé ;
- stipuler que le prestataire ne collecte et n'analyse que les informations strictement nécessaires au bon déroulement de la prestation ;
- stipuler que le prestataire ne divulgue aucune information relative à la prestation à des tiers, sauf autorisation formelle et écrite du commanditaire ;
- préciser les clauses relatives à l'éthique du prestataire et inclure la charte d'éthique du prestataire ;
- préciser les modalités d'accès, de stockage, de transport, de reproduction, de destruction et de restitution des informations collectées et analysées par le prestataire. Si besoin, le prestataire doit définir, en collaboration avec le commanditaire, les modalités selon les types d'informations ;
    - stipuler que le prestataire peut, sauf refus formel et écrit du commanditaire, conserver certains types d'informations liées à la prestation et préciser ces types d'information (ex. : règles de détection, codes malveillants, scénarios d'attaque, indicateurs de compromission, etc.) ;
    - stipuler que le prestataire anonymise et décontextualise (suppression de toute information permettant d'identifier le commanditaire, de toute information à caractère personnel, etc.) l'ensemble des informations que le commanditaire l'autorise à conserver ou à transmettre à un tiers ;
    - stipuler que le prestataire, sauf refus formel et écrit du commanditaire, transmet au centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) ces informations anonymisées et décontextualisées, ainsi que leur niveau de sensibilité et leurs conditions d'utilisation ;
    - stipuler que le prestataire doit protéger les données transmises à des tiers, en confidentialité, conformément à leur niveau de sensibilité ou de classification ;
    - stipuler que le prestataire détruit l'ensemble des informations relatives au commanditaire à l'issue de la prestation ou à la date d'échéance de la durée de conservation, au premier terme échu, à l'exception de celles pour lesquelles il a reçu une autorisation de conservation de la part du commanditaire ;
- définir la fréquence à laquelle le prestataire teste le plan de sauvegarde et de restauration du service de détection des incidents de sécurité.

IV.5.3.5. Réversibilité

a) La convention de service doit préciser les modalités de mise en œuvre d'un plan de réversibilité de la prestation : durée, mise en œuvre, surcoût éventuel, etc. (voir chapitre IV.5.2).

IV.5.3.6. Lois et réglementations

a) La convention de service doit :

- être rédigée en français. Le prestataire doit fournir une traduction de courtoisie de la convention de service si le commanditaire en fait la demande ;
- stipuler que seule la version française fait foi, notamment dans le cadre d'un litige ;
- préciser la législation applicable à la convention de service;
- préciser les moyens techniques et organisationnels mis en œuvre par le prestataire pour le respect de la législation applicable notamment ceux concernant :
  - les données à caractère personnel ;
  - l'abus de confiance ;
  - le secret des correspondances privées ;
  - le secret médical ;
  - l'atteinte à la vie privée ;
  - l'accès ou le maintien frauduleux à un système d'information ;
  - le secret professionnel ;
- préciser les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire et notamment celles liées à son secteur d'activité ;
- prévoir les mesures à mettre en place par le prestataire dans le cadre d'une affaire judiciaire, civile ou arbitrale. Dans ce cas, il est recommandé de faire appel à un expert judiciaire [LOI_EJ] ;
- définir la durée de conservation des informations liées à la prestation et notamment les évènements collectés et les incidents de sécurité détectés. Si besoin, une distinction de la durée de conservation peut être faite en fonction des types d'information. La durée minimale de conservation, en accord avec la législation et la réglementation française en vigueur, est de :
  - six mois pour les évènements collectés ;
  - toute la durée de la prestation pour les incidents de sécurité ainsi que le contexte (évènements associés et rapport(s) d'analyse(s) de qualification) et les notifications associés.

b) Il est recommandé que la législation applicable à la convention de service soit la législation française.

c) Si la législation applicable à la convention de service est la législation française, le prestataire doit préciser dans la convention de service les moyens techniques et organisationnels qu'il met en œuvre pour le respect des textes suivants :

- les données à caractère personnel [LOI_IL] ;
- l'abus de confiance [CP_ART_314-1] ;
- le secret des correspondances privées [CP_ART_226-15] ;
- le secret médical [CSP_ART_L1110-4] ;
- l'atteinte à la vie privée [CP_ART_226-1] ;

- l'accès ou le maintien frauduleux à un système d'information [CP_ART_323-1] ;
- le secret professionnel [CP_ART_226-13], le cas échéant sans préjudice de l'application de l'article 40 alinéa 2 du Code de procédure pénale relatif au signalement à une autorité judiciaire.

IV.5.3.7. Sous-traitance

a) La convention de service doit préciser que le prestataire peut si nécessaire sous-traiter tout ou partie de la prestation à un autre prestataire sous réserve que :
   - il existe une convention de service entre le prestataire et le sous-traitant ;
   - le recours à la sous-traitance est connu et formellement accepté par écrit par le commanditaire ;
   - le sous-traitant respecte les exigences du présent référentiel.

IV.5.3.8. Livrables

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

IV.5.3.9. Qualification du service

a) La convention de service doit indiquer que :
   - la prestation réalisée est une prestation qualifiée et doit inclure l'attestation de qualification du prestataire ;
   - conformément au processus de qualification des prestataires de service de confiance [QUAL_SERV_PROCESS] le commanditaire peut déposer une réclamation contre le prestataire auprès de l'ANSSI ;
   - le commanditaire autorise, conformément au processus de qualification des prestataires de service de confiance [QUAL_SERV_PROCESS], l'ANSSI et le centre d'évaluation à auditer le système d'information du service de détection des incidents de sécurité du prestataire ;
   - le commanditaire autorise, conformément au présent référentiel (voir exigence IV.3.4.f), un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié mandaté par le prestataire à auditer le système d'information du service de détection des incidents de sécurité du prestataire dans le cadre du plan de contrôle.

b) Lorsque le prestataire réalise une prestation non qualifiée (cf. III.2), il doit l'indiquer explicitement dans la convention de service et sensibiliser le commanditaire aux risques de ne pas exiger une prestation qualifiée.

IV.5.3.10. Niveau de service

a) La convention de service doit :
   - définir les indicateurs opérationnels et stratégiques permettant de mesurer le niveau de service de la prestation ;
   - définir les plages horaires opérationnelles du service de détection des incidents de sécurité ;
   - stipuler que le prestataire organise en présence du commanditaire des comités opérationnels et stratégiques ;
   - détailler les objectifs de ces comités et leur fréquence ;
   - identifier, pour le prestataire et le commanditaire, la charge des ressources humaines consacrée à la gestion des règles de détection et notamment à leur création ou leur modification ;

- définir la fréquence à laquelle le prestataire transmet au commanditaire le bulletin d'état des règles de détection ;
- stipuler que le prestataire met à disposition du commanditaire un service d'assistance et les plages horaires opérationnelles de ce service d'assistance ;
- préciser le type du service d'assistance (téléphone, *mail*, etc.), sa disponibilité et le niveau de sensibilité ou de classification des informations qu'il permet d'échanger ;
- stipuler le niveau de compétence du personnel réalisant les astreintes, en fonction des besoins du commanditaire et dans le cas où des astreintes sont mises en place.

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

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

II. Normes et documents techniques

Renvoi	Document
[PDIS_LPM]	Exigences supplémentaires applicables aux prestataires de détection des incidents de sécurité dans le cadre de la loi n°2013-1168 du 18 décembre 2013. Document de niveau *Diffusion Restreinte*, ce document peut être obtenu auprès de l'ANSSI.
[CRYPTO_B1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version 2.03. Disponible sur http://www.ssi.gouv.fr
[CRYPTO_B2]	Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. Disponible sur http://www.ssi.gouv.fr

Renvoi	Document
[CRYPTO_B3]	Règles et recommandations concernant les mécanismes d'authentification, ANSSI. Disponible sur http://www.ssi.gouv.fr
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HYGIENE]	Guide d'Hygiène Informatique, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[NT_JOURNAL]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, note technique n° DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013, ANSSI. Disponible sur http://www.ssi.gouv.fr
[NT_ADMIN]	Recommandations relatives à l'administration sécurisée des systèmes d'information, note technique n° DAT-NT-22/ANSSI/SDE/NP du 20 février 2015, ANSSI Disponible sur http://www.ssi.gouv.fr
[ETSI_ISG_ISI]	Standards ETSI ISI Indicators (ISI 001-1 and Guides 001-2), ISI Event Model (ISI-002), ISI Maturity (ISI-003), ISI Event Detection (ISI-004) – 5 standards sur la détection des incidents de sécurité. Disponible sur http://www.etsi.org
[ISO9001]	Norme internationale ISO 9001:2008 : Systèmes de management de la qualité – Exigences. Disponible sur http://www.iso.org
[ISO27000]	Norme internationale ISO/IEC 27000:2014 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – vue d'ensemble et vocabulaire. Disponible sur http://www.iso.org
[ISO27001]	Norme internationale ISO/IEC 27001:2013 : Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences. Disponible sur http://www.iso.org
[ISO27002]	Norme internationale ISO/IEC 27002:2013 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information. Disponible sur http://www.iso.org
[ISO27005]	Norme internationale ISO/IEC27005:2011 – Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information. Disponible sur http://www.iso.org
[ISO27035]	Norme internationale ISO/IEC 27035:2011 : Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information. Disponible sur http://www.iso.org

III. Autres références documentaires

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

Annexe 2 Missions et compétences du personnel du prestataire

I. Opérateur analyste

I.1. Missions

- identifier, analyser et qualifier des incidents de sécurité ;
- accompagner le traitement des incidents par des équipes d'investigation.

I.2. Compétences

- connaissance des protocoles et architectures réseau ;
- pratique de l'analyse de journaux (systèmes ou applicatifs) ;
- connaissances en sécurité des systèmes d'information ;
- pratique de l'analyse de flux réseaux ;
- maîtrise des fonctionnalités métier des dispositifs du service de détection notamment la recherche d'évènements dans les systèmes de stockage des évènements.

II. Administrateur d'infrastructure

II.1.Missions

- administrer les dispositifs de l'infrastructure technique du service de détection des incidents de sécurité ;
- maintenir en conditions opérationnelles les dispositifs de l'infrastructure technique du service de détection de sécurité ;
- mettre à jour et maintenir en conditions de sécurité les dispositifs de l'infrastructure technique du service de détection des incidents de sécurité.

II.2.Compétences

- maîtrise des dispositifs du service de détection des incidents de sécurité et notamment ceux dans les activités de gestion des évènements, des incidents et des notifications.

III. Expert architecture

III.1. Missions

- concevoir et maintenir une architecture du service de détection ;
- intégrer voire développer et maintenir les composants du service de détection ;
- intégrer voire développer et maintenir de nouveaux moteurs de corrélation.

III.2. Compétences

- connaissances du fonctionnement des sondes et d'outils de corrélation de journaux d'évènements ;
- maîtrise des protocoles courants pour le fonctionnement des services ;
- bonnes connaissances des applications les plus classiques et de leur sécurisation (serveurs web, de messagerie, de base de données, DNS, mandataires, pare-feux, etc.) ;

- bonnes connaissances de l'architecture globale d'un réseau et de la sécurisation de ses composants (routeurs, commutateurs, etc.).

IV. Expert collecte et analyse de journaux

IV.1. Missions

- contribuer à la définition et à la révision de la stratégie de collecte ;
- contribuer à la définition de la politique de journalisation du commanditaire par type d'équipement (systèmes d'exploitation, services d'infrastructure, équipements réseau, équipements de sécurité, etc.) ;
- apporter un soutien aux administrateurs d'infrastructure dans le cadre du déploiement des systèmes de détection (tests, maintien en conditions opérationnelles, support aux analystes utilisant ces systèmes, etc.) ;
- participer au développement et au maintien de mécanismes et de règles de corrélation d'évènements.

IV.2. Compétences

- connaissances approfondies en analyse de journaux d'évènements systèmes, réseaux et applicatifs ;
- connaissances d'outils et de méthodes de corrélation de journaux d'évènements ;
- connaissances des solutions d'analyse de journaux ou de supervision de la sécurité (*SIEM*).

V. Expert métier détection

V.1. Missions

- alimenter des bases de connaissances internes de capitalisation des menaces, vulnérabilités, codes malveillants ;
- gérer les règles de détection au travers de leur cycle de vie (conception, implémentation, documentation, modification, désactivation, etc.) ;
- assurer l'amélioration continue des processus du service.

V.2. Compétences

- connaissance des vulnérabilités ;
- connaissance des protocoles de contrôle commande ;
- connaissance des modes opératoires d'attaque et des codes malveillants ;
- maîtrise des outils de développement des règles de détection.

VI. Responsable des droits d'accès

VI.1. Missions

- gérer la création et la désactivation de comptes sur les outils d'exploitation du service ;
- gérer l'attribution, la modification et la suppression de droits d'accès aux outils d'exploitation du service ;

VI.2. Compétences

- maîtrise de l'administration des outils d'exploitation du service ;
- connaissance des rôles du service de détection et des droits associés.

Annexe 3 Recommandations aux commanditaires

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

I. Qualification

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 faisant l'objet d'un appel d'offres ou d'un contrat.

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

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

- choisir le prestataire dans le catalogue des prestataires qualifiés publié sur le site de l'ANSSI ;
- exiger du prestataire de stipuler dans la convention de service que la prestation réalisée est une prestation qualifiée.

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

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

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

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

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

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

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

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

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

Il est possible pour un commanditaire de recourir à un prestataire qualifié après s'être assuré que ce dernier dispose au minimum des décisions d'accès aux ACSSI (DACSSI) adéquates pour

les ACSSI classifiés ou des attestations de formation à la manipulation des ACSSI pour les ACSSI non classifiés.

II. Avant la prestation

a) Il est recommandé que le commanditaire désigne en son sein un référent opérationnel chargé d'être l'interlocuteur privilégié avec le prestataire concernant le fonctionnement opérationnel du service de détection des incidents de sécurité et le suivi des incidents de sécurité détectés.

b) Il est recommandé que le commanditaire fasse appel à un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié[15] pour élaborer l'appréciation des risques permettant d'établir la liste des incidents de sécurité redoutés et des impacts associés (voir exigence IV.2.1.a) à partir desquelles les stratégies de collecte, d'analyse et de notification sont élaborées.

c) Il est recommandé que le commanditaire mette à jour son appréciation des risques pour chaque modification dans son infrastructure ou ses services, et communique ces changements et leurs conséquences au prestataire.

d) Il est recommandé que le commanditaire identifie dans la convention de service les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité.

e) Il est recommandé que le commanditaire exige du prestataire que la fréquence des comités opérationnels (voir chapitre IV.4.3.1) devant être définie dans la convention de service soit mensuelle.

f) Il est recommandé que le commanditaire exige du prestataire que la fréquence des comités stratégiques (voir chapitre IV.4.3.2) devant être définie dans la convention de service soit semestrielle.

g) Il est recommandé que le commanditaire exige du prestataire que la fréquence des bulletins d'état des règles de détection (voir exigence IV.2.1.j) devant être définie dans la convention de service soit hebdomadaire.

h) Il est recommandé que le commanditaire choisisse parmi les indicateurs proposés par [ETSI_ISG_ISI] les indicateurs opérationnels et stratégiques devant être définis dans la convention de service et permettant de mesurer le niveau de service de la prestation.

i) Il est recommandé que le commanditaire utilise [ETSI_ISG_ISI] pour définir le format et le contenu des tickets d'incident de sécurité.

j) Il est recommandé que le commanditaire exige du prestataire d'intégrer dans la stratégie de collecte (voir exigence IV.2.2.a) la mise en œuvre de sondes à chacune des interconnexions de son système d'information et en particulier celles avec :

   - internet ;
   - les systèmes d'information tiers (partenaires, sous-traitants, etc.) ;
   - les autres systèmes d'information du commanditaire de niveau de sensibilité ou de classification moindre ou plus exposés.

k) Il est recommandé que les sondes déployées aux interconnexions du système d'information du commanditaire soient qualifiées par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur qualification.

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

l) Il est recommandé que le commanditaire :

- synchronise les sources de collecte hébergées sur son système d'information avec une source de temps unique ;
- élabore et mette en œuvre une politique de journalisation des évènements.

Pour ce faire, le commanditaire peut utiliser la note technique de l'ANSSI consacrée à la mise en œuvre d'un système de journalisation [NT_JOURNAL] et recourir au prestataire de détection des incidents de sécurité (PDIS) ou à un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié.

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

n) Il est recommandé que le commanditaire exige du prestataire d'intégrer dans la stratégie de notification (voir exigence IV.2.3.c) des notifications spécifiques en cas de détection d'incidents de sécurité majeurs au sein de son système d'information.

III. Pendant la prestation

a) Il est recommandé que le commanditaire transmette au prestataire régulièrement et durant toute la prestation toutes les informations lui permettant de créer de nouvelles règles de détection spécifiques aux besoins du commanditaire.

À ce titre, le commanditaire peut notamment transmettre les résultats des tests de vulnérabilités et d'intrusion réalisés sur son système d'information.

b) Il est recommandé que le commanditaire informe le prestataire de tout projet d'évolution de son système d'information pouvant impacter l'efficacité du service de détection des incidents de sécurité.

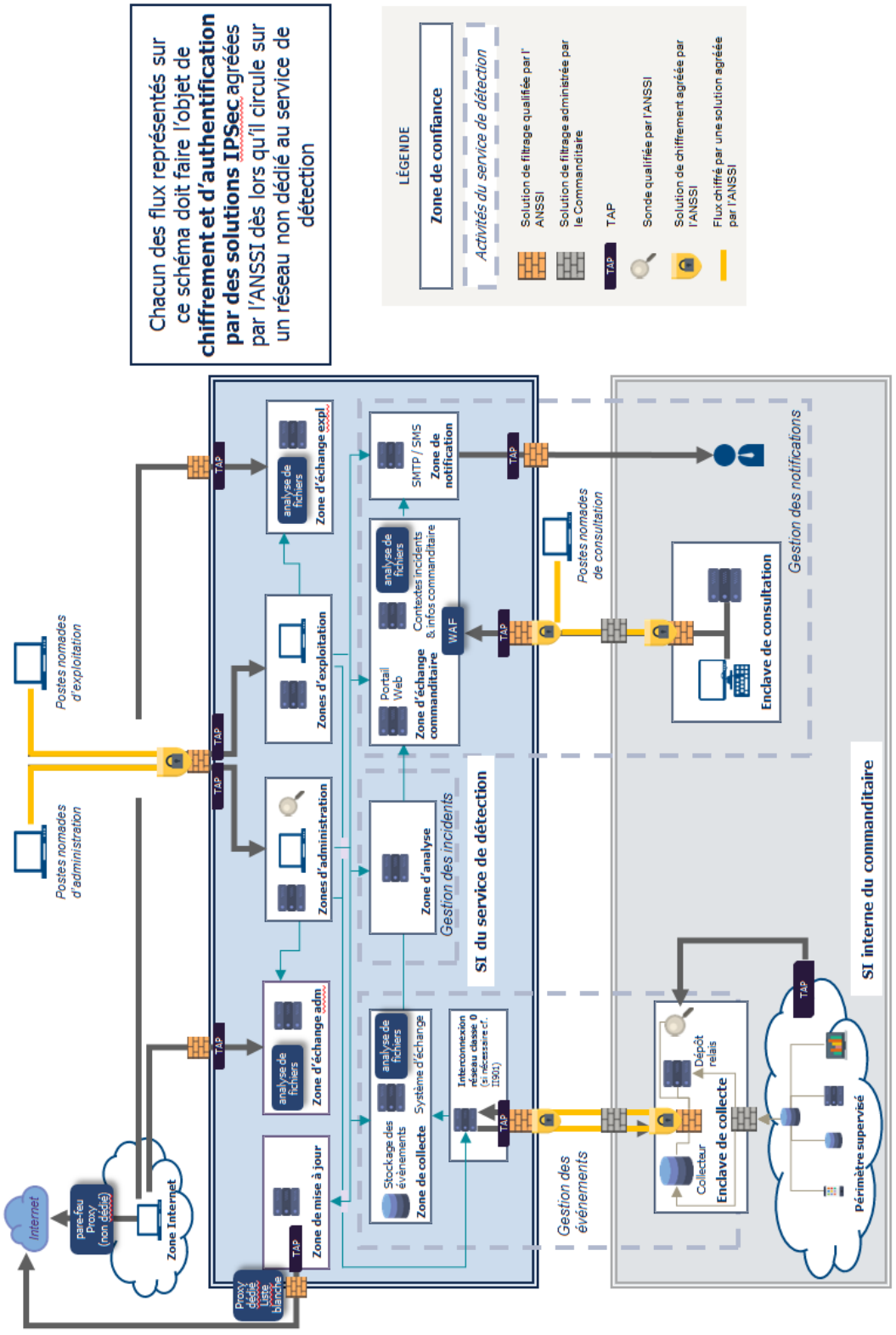
c) Il est recommandé que le commanditaire mette en place un processus de gestion des changements lui permettant d'informer en continu le prestataire de toutes modifications sur son système d'information supervisé (configuration, paramètres, versions logicielles, etc.).

d) Il est recommandé que le commanditaire recoure à une prestation qualifiée réalisée par un prestataire de réponse aux incidents de sécurité (PRIS)[16] en cas d'incident de sécurité suspecté ou avéré.

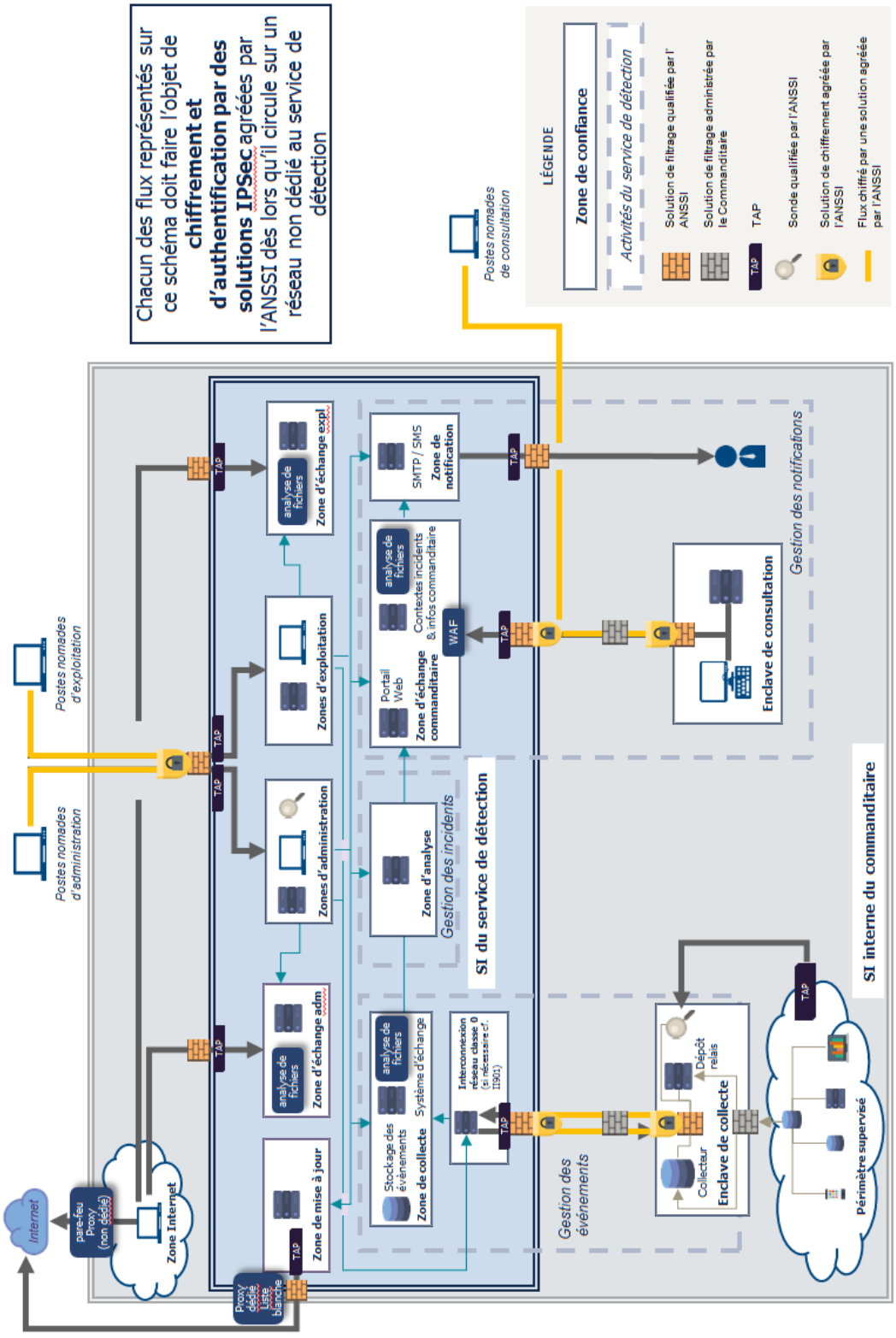
[16] Le catalogue des prestataires de réponse aux incidents de sécurité (PRIS) qualifiés par l'ANSSI est publié sur le site de l'ANSSI.

Annexe 4 Schémas illustratifs d'une architecture conforme PDIS

Le schéma ci-dessous est une représentation d'une architecture conforme possible pour le système d'information du service de détection. Ce schéma est donné uniquement à titre d'illustration et n'exclut pas la mise en place d'autres architectures.



Le schéma suivant, toujours à titre illustratif, met en avant le fait que les mêmes exigences doivent être respectées par un service de détection interne.



Annexe 5 Règles relatives à l'usage d'un agrégateur de flux

Il est autorisé d'utiliser un agrégateur entre des *Tap* et une sonde, dans les conditions suivantes :

- L'agrégateur doit être utilisé exclusivement pour assurer la fonction d'agrégation :
    - toutes les autres fonctions de l'agrégateur doivent être désactivées ;
    - il n'est pas autorisé d'utiliser un équipement réalisant les fonctions de *Tap* et d'agrégateur (un équipement dédié est nécessaire pour assurer chaque fonction) ;
- L'agrégateur doit être administré de la même manière et dans les mêmes conditions de sécurité que pour les sondes qualifiées par l'ANSSI ;
- Les responsabilités d'administration de l'agrégateur doivent être détaillées dans la convention de service ;
- L'agrégateur doit être administré depuis le service de détection d'incidents de sécurité ;
- L'agrégateur doit être supervisé afin d'identifier des éventuelles pertes de paquets ;
- Les mises à jour de l'agrégateur doivent être réalisées dans les mêmes conditions que les sondes.

Il est recommandé que l'agrégateur soit dimensionné pour supporter la capacité réseau théorique de chaque réseau agrégé.

À défaut d'utiliser un agrégateur, il est autorisé d'utiliser une sonde disposant de plusieurs interfaces réseau et assurant la fonction d'agrégation.