RÉFÉRENTIEL D'EXIGENCES POUR LA QUALIFICATION D'UN PRESTATAIRE DE DÉTECTION D'INCIDENTS DE SÉCURITÉ, EXTERNE, EXPLOITANT DES SYSTÈMES DE DÉTECTION QUALIFIÉS

Annexe à l'Arrêté Ministériel n° 2021-150
du 18 février 2021

ANNEXE AU « JOURNAL DE MONACO » N° 8.527

DU 26 FÉVRIER 2021

Table des matières

I. Introduction

I.1. Présentation générale

Un système de détection qualifié concourt à la protection d'un système d'information face aux menaces de cyberattaques. La détection consiste à repérer toute anomalie, appelée évènement de sécurité, dans les flux d'information du système d'information supervisé.

La présente annexe constitue le référentiel d'exigences applicables à un prestataire, externe, exploitant des systèmes de détection qualifiés pour le compte d'un commanditaire .

Il permet au commanditaire de la prestation de disposer de garanties sur les compétences du prestataire et de son personnel, sur la qualité de la prestation de détection des évènements de sécurité réalisée à l'aide de systèmes de détection qualifiés et sur la confiance que le commanditaire peut accorder au prestataire, notamment en matière de confidentialité.

I.2. Définitions et abréviations

I.2.1. Abréviations

Les abréviations utilisées dans le présent référentiel sont :

AMSN	Agence Monégasque de Sécurité Numérique
ANSSI	Agence nationale de la sécurité des systèmes d'information ;
CERT-MC	centre d'expertise, de réponse et de traitement en matière d'attaques numériques ;
PASSI	Prestataire d'audit de la sécurité des systèmes d'information ;
PDIS	Prestataire de service de détection des incidents de sécurité ;
PRIS	Prestataire de réponse aux incidents de sécurité ;
OIV	Opérateur d'Importance Vitale ;
[R]	Recommandation ;
SOC	Centre Opérationnel de cyber Sécurité ;
TAP	Test Access Point

I.2.2. Définitions

Les définitions ci-après reproduites s'appuient sur les normes de la suite [ISO27000] et notamment la norme [IS27035] relative à la gestion des incidents de sécurité.

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 qui décide de mettre en place un système de détection d'incident de sécurité qualifié, cela comprends de fait les OIV mais reste applicable aux entités non OIV qui le souhaitent.

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.

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

Incident de sécurité – un incident de sécurité découle d'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.

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.

Opérateur d'Importance Vitale - s'entendent d'opérateurs publics ou privés : a) qui exercent dans des secteurs essentiels pour le fonctionnement des institutions et des services publics, pour l'activité économique ou plus généralement pour la vie en Principauté ; b) qui exploitent des établissements ou utilisent des installations ou des ouvrages dont l'indisponibilité risquerait d'affecter de façon importante les intérêts mentionnés à la lettre a).

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

Prestation qualifiée – service de détection des évènements 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, 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 (organisationnels, humains, …) 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.

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 de détection – dispositif technique destiné à repérer des activités anormales, suspectes ou malveillantes sur le périmètre supervisé. Un système de détection 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 évènements de sécurité.

Système de détection qualifié – est un système de détection qui a fait l'objet d'une qualification par l'AMSN. La qualification est la recommandation par l'État de produits de cyber sécurité éprouvés et approuvés par l'AMSN ; elle atteste de leur conformité aux exigences règlementaires, techniques et de sécurité promues par l'AMSN en apportant une garantie de robustesse du produit et d'engagement du fournisseur de solutions à respecter des critères de confiance.

Système d'information – Est qualifié de système d'information, tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

Tiers – personne ou organisme reconnu comme indépendant.

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 externe de détection

II.1. Activités du service de détection

Le service de détection est composé de deux activités distinctes :

- la gestion des évènements, correspondant à l'ensemble des moyens techniques et organisationnels :
  - permettant d'identifier un évènement de sécurité sur la base d'évènements collectés ;
  - assurant le recueil, le stockage des évènements de sécurité ;
  - la capitalisation des évènements de sécurité dans un but d'amélioration du service ;
- la gestion des notifications, correspondant à l'ensemble des moyens techniques et organisationnels permettant d'informer le commanditaire sur les évènements de sécurité détectés et de stocker ces notifications.

Les activités de corrélation et d'analyse permettant la qualification d'évènements en incidents sont hors périmètre du document.

Les activités de réaction et de remédiation ne sont pas concernées par la présente annexe. Elles sont traitées par une équipe compétente en la matière ou un prestataire 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, les différentes zones présentées dans ce chapitre peuvent être hébergées au sein d'entités voire d'organismes différents, tant que les exigences de ce document sont respectées.

Le schéma ci-dessous est une représentation générale d'une architecture type du service de détection externe. L'Annexe 4 présente des représentations plus détaillés.

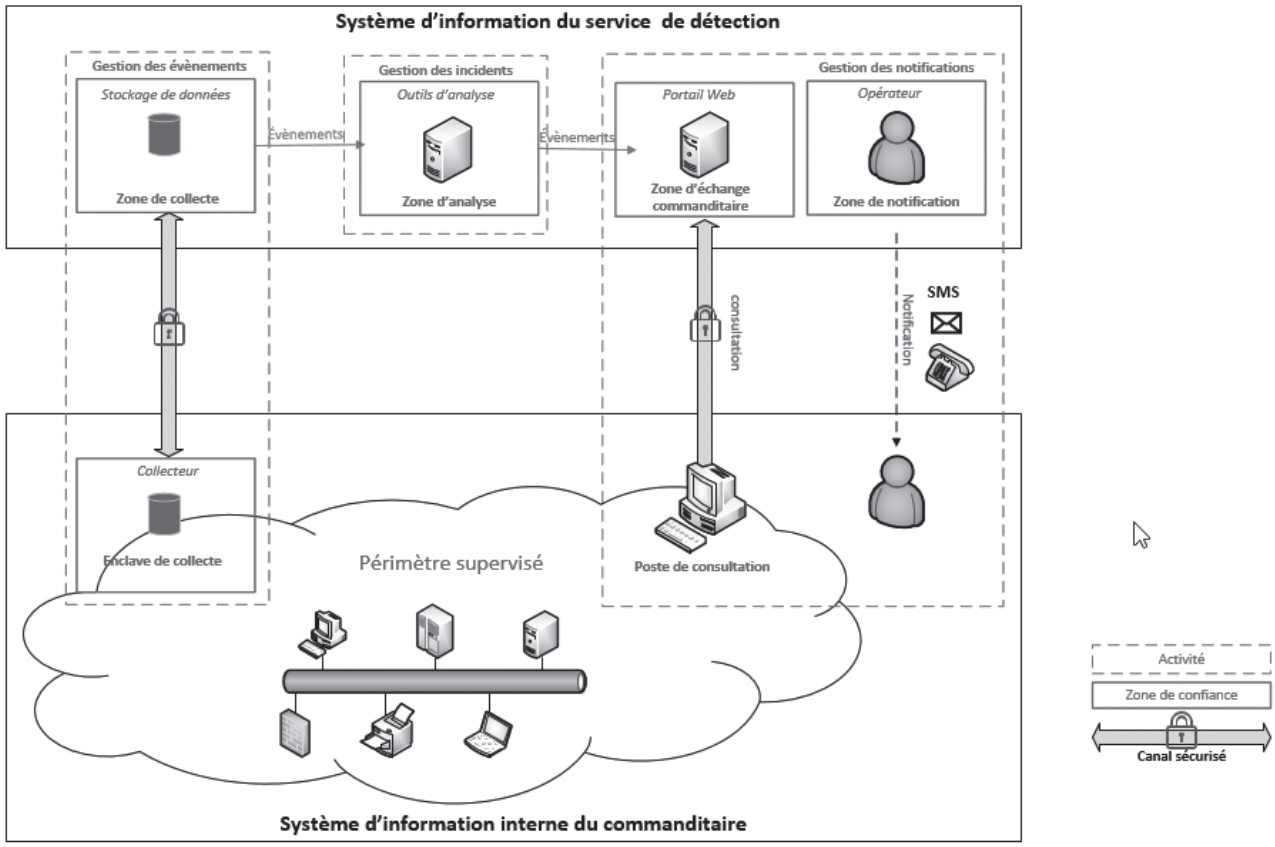


Figure 1 : Représentation générale d'une architecture type du service de détection externe

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 évènements de sécurité ;
- zone(s) de notification, regroupant les systèmes de notification à destination du commanditaire ;
- zone(s) d'échange commanditaire, regroupant l'ensemble des dispositifs éventuels permettant au commanditaire de consulter le détail des informations concernant les évènements notifiés ;

- 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.

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 de détection ;

- des zones particulières mises en place au sein du système d'information interne du commanditaire, ci-après dénommées « enclaves ». Au moins une enclave de collecte, devra être mise en place, 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.

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

III. Prestataires de détection externes

III.1. Modalités de la qualification

Le présent référentiel contient les exigences et les recommandations à destination des prestataires de détection pour l'exploitation d'un système de détection qualifié.

Les exigences doivent être respectées par les prestataires de détection dans le but d'obtenir la qualification de prestataire de détection exploitant des systèmes de détection qualifiés.

Les recommandations sont données à titre de bonnes pratiques et ne font pas l'objet d'une quelconque vérification en vue de la qualification.

La qualification des prestataires est prononcée par le Directeur de l'Agence Monégasque de Sécurité Numérique conformément au e) de l'article 6 de de l'Ordonnance Souveraine n° 8.504 du 18 février 2021 portant application de l'article 24 de la loi n°1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, et selon le processus suivant qui permet d'attester de la conformité du prestataire aux exigences du référentiel.

a) Le respect des exigences du référentiel par les prestataires de détection est vérifié par un organisme de certification accrédité par le comité français d'accréditation (COFRAC) et habilité par l'Agence Monégasque de Sécurité Numérique. La liste des organismes de certification est disponible sur le site de l'Agence Monégasque de Sécurité Numérique https://amsn.gouv.mc/.

b) Aux fins de vérification du respect des exigences prescrites, l'organisme de certification :

- audite l'établissement[1] du prestataire de détection en Principauté ;

- évalue les compétences des personnels.

c) La qualification est attribuée, pour une durée maximale de trois ans, aux prestataires de détection par le Directeur de lAgence Monégasque de Sécurité Numérique :

- sur la base du rapport de l'organisme de certification ;

- après examen de vérification de connaissance des textes législatifs et règlementaires du personnel du prestataire candidat.

d) Un audit de surveillance est réalisé par un organisme de certification dix-huit mois après la décision de qualification. Les prestataires de détection peuvent se procurer le règlement de qualification auprès de l'organisme de qualification. Pour les PDIS qualifiés en France par l'ANSSI, l'Agence Monégasque de Sécurité Numérique peut prononcer leur qualification en Principauté dans la mesure où les exigences du présent référentiel sont remplies par le prestataire.

III.2. Portée de la qualification

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

[1] L'établissement correspond au lieu de travail habituel des en Principauté. Il peut s'agir du siège social ou d'établissements secondaires.

Les prestataire 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 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 qualifié peut notamment être qualifié pour d'autres familles de prestataires de service de confiance (PASSI, PRIS).

III.3. Avertissement

Une prestation de détection non qualifiée, c'est-à-dire ne respectant pas intégralement les exigences la concernant du présent document, 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.

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 en Principauté.

c) Le prestataire doit décrire l'organisation de son activité de détection 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. À ce titre, le prestataire doit préciser 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 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.

h) 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.

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

j) 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.

k) 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.

l) Le prestataire doit établir une convention de service, avec le commanditaire, approuvée formellement, par écrit, avant l'exécution de la prestation.

IV.2. Détection des évènements de sécurité

IV.2.1. Gestion des évènements

a) Le commanditaire doit établir, éventuellement avec l'aide d'un PASSI, 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'évènements de sécurité suivants, pouvant mener aux incidents redoutés :

- exploitation d'une vulnérabilité ;
- élévation de privilèges ;
- exfiltration de données ;
- propagation virale ;
- utilisation d'un mécanisme de persistance.

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

f) 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, notamment :
  - 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 par d'éventuels autres commanditaires.

g) 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, dans la mesure du possible :

- un identifiant unique de la règle de détection, permettant de faire le lien entre les différents outils et bases de connaissances associées ;
- 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 l'auteur de la règle de détection (par exemple, un partenaire, un fournisseur, le commanditaire, etc.) ;
- 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 ;
  - 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.

h) 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 :

- la date à laquelle la règle de détection a été introduite dans les outils techniques d'analyse ;

- la date à laquelle la règle de détection a été désactivée 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 désactivée des outils techniques d'analyse doit être marquée comme désactivée et ne doit pas être supprimée de cette liste.

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

- le nombre de règles de détection créées, modifiées ou désactivées des outils d'analyse ;

- l'identifiant, et la description de chaque règle créée ou désactivée des outils d'analyse ;

- le motif de la création ou du retrait de la règle de sécurité (exemple : création, ou retrait à la demande du commanditaire, etc.).

j) 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.

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

l) 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.h).

m) Le prestataire doit être capable, de manière autonome, d'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. 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.

n) Le prestataire doit élaborer et tenir à jour pour chaque commanditaire la liste des ajouts de règles dans les outils techniques d'analyse.

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

p) Dans le cadre du support au commanditaire pour 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.g)).

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.

q) 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.

r) Le prestataire doit créer un ticket pour chaque évènement de sécurité détecté et le tenir à disposition du commanditaire. Ce ticket 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'évènement de sécurité ;

- la description de l'évènement de sécurité ;

- les identifiants des règles de détection déclenchées ;

- les équipements ayant généré et collecté l'évènement.

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

t) Le prestataire doit disposer d'un outil de gestion de tickets.

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

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

w) Le prestataire doit mettre en place un processus de gestion de la capacité de stockage des tickets 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 en Principauté.

x) 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, taille, extension, nombre magique (*magic number*) ;
- adresses IP publiques ;
- domaines pour les protocoles suivants : HTTP et SMTP ;
- URL ;
- agent utilisateur (*user-agent*) ;
- champs d'emails : domaine source, domaine destination, *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.

y) Le prestataire doit être capable sur demande du commanditaire de procéder à une analyse sur l'ensemble des évènements stockés sur une durée conforme à la legislation en vigueur.

IV.2.2. Stratégie de collecte

a) Le commanditaire doit élaborer, avec éventuellement un PASSI, 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 prestataire 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.).

c) Le prestataire doit être capable de journaliser les évènements pour chacun des systèmes de détection qualifiés.

d) Le prestataire doit de manière autonome faire évoluer sa capacité de collecte, en lien avec la liste des incidents redoutés.

e) 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.

f) Le prestataire doit exercer un devoir de conseil envers le commanditaire dans l'élaboration, l'application et la revue de la stratégie de collecte.

g) Le prestataire doit recommander au commanditaire d'intégrer dans la stratégie de collecte la mise en œuvre de systèmes de détection qualifiés 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.

h) Il est **recommandé** que les équipements de type Tap alimentant les systèmes de détection qualifiés soient qualifiés par l'ANSSI et utilisées conformément aux conditions de leur qualification.

i) Le prestataire doit être capable d'opérer des systèmes de détection qualifiés alimentés 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 le (les) système(s) de détection, 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'Appendice 5.

j) Il est **recommandé** que le prestataire soit capable d'opérer des systèmes de détection qualifiés dédiés aux systèmes d'information industriels.

k) 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.

l) 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 :

- la ou les date(s) auxquelles la règle de filtrage a été introduite dans les collecteurs ;
- la ou les date(s) auxquelles la règle de filtrage a été désactivée 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 désactivée des collecteurs doit être marquée comme désactivée et ne doit par conséquent pas être supprimée de cette liste.

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

- le nombre de règles de filtrage créées, modifiées ou désactivées des collecteurs ;
- l'identifiant et la description de chaque règle créée, modifiée ou désactivée 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.).

n) 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.

o) 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.

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

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

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

s) 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 (voir exigence IV.2.1.ee), dans la limite du respect de la législation et la réglementation en vigueur en Principauté (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 qui peuvent être par exemple :
  - courriel ;
  - message court (SMS) ;
  - téléphone ;
- un canal sécurisé, notamment pour l'échange d'informations détaillées (voir exigence IV.2.3. l).

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.

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

c) La stratégie de notification doit identifier au minimum la liste des évènements de sécurité à notifier, le format, le contenu, le délai des notifications ainsi que les personnes à notifier.

d) 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, une fois les notifications reçues, et les canaux à utiliser en fonction du niveau de sensibilité.

e) Les notifications doivent contenir exclusivement les informations suivantes : un numéro de référence unique.

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

f) 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 de l'évènement.

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

g) Le prestataire doit être capable de fournir la référence de l'évènement de sécurité à l'origine d'une notification.

h) Le prestataire doit mettre en place et tenir à jour un registre centralisé et chronologique par commanditaire référençant toutes les notifications effectuées pour ceux-ci. 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'évènement.

i) 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 en Principauté (voir exigence IV.1.b).

j) Le prestataire doit mettre à disposition du commanditaire un portail web lui permettant de visualiser les évènements de sécurité.

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 évènements 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 évènements 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 tous les trois ans, et en cas de modifications structurantes du service de détection, notamment celles concernant son hébergement, son infrastructure ou son architecture.

d) Le prestataire doit tenir 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 consulatation 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 [AM_791] relatives aux mesures de protection des systèmes d'information traitant d'informations sensibles (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 sécurité nationale du commanditaire.

d) 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.

e) 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 évènements de sécurité exclusivement en Principauté sauf dérogation délivrée par le Directeur de l'Agence Monégasque de Sécurité Numérique. En cas de dérogation, le prestataire doit héberger et traiter les données au sein de l'Union Européenne. Dans le cas où certaines sources de collecte seraient situées en dehors de la Principauté, les évènements issus de ces sources devront être transmis à un collecteur situé en Principauté.

b) Le prestataire doit exploiter et administrer le service de détection des évènements de sécurité exclusivement depuis la Principauté sauf dérogation délivrée par le Directeur de l'Agence Monégasque de Sécurité Nunmérique. En cas de dérogation le prestataire doit exploiter et administrer le service au sein de 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 trimestriellement.

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

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

h) Les résultats des contrôles doivent être validés formellement et par écrit par 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 évènements 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 évènements 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, si elles existent, 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. 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 la norme [ISO27002].

IV.3.7. Service de détection du service

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

b) Ce service doit être conforme aux exigences du titre IV.3 à l'exception des titres IV.3.13, IV.3.14, IV.3.15.

c) Il est **recommandé** que le prestataire mette en place un transfert des journaux des dispositifs de son système de détection des évènements de sécurité vers une zone de confiance dédiée conformément aux exigences du document de l'ANSSI [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 évènements de sécurité respectivement depuis les zones d'administration et d'exploitation.

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

e) 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 du service.

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

g) 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 du service.

h) Il est **recommandé** que le prestataire fasse appel à un prestataire de réponse aux incidents qualifié (PRIS)[2] 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 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 de détection

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

b) Le prestataire doit cloisonner le système d'information du service de détection 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 ;

---

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

- zone(s) d'analyse, regroupant l'ensemble des dispositifs impliqués dans le processus d'analyse ;

- zone(s) de notification, regroupant les systèmes de notification du commanditaire ;

- 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 ;

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 de référence des flux du système de détection, ainsi que la politique de filtrage associée, n'autorisant que les flux strictement nécessaires au fonctionnement du service de détection.

e) Le prestataire doit mettre en œuvre des solutions de chiffrement et d'authentification 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.

f) Le prestataire doit élaborer et maintenir à jour une description détaillée de l'architecture du système d'information du service de détection. 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 notifications et le portail web.

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 avec des postes d'administration dédiés, hébergés dans la zone d'administration[3] et distincts des postes de travail des opérateurs.

b) L'administration des dispositifs du service de détection 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 ainsi que les actions réalisées[4].

d) Il est **recommandé** au prestataire de 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 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 de 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.

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.

---

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

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

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) 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 [AM_635], [AM_636] et [AM_637].

k) 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.

l) Le prestataire doit assurer la synchronisation de son serveur de temps de référence en utilisant un canal nominal et un canal de secours, via antenne. Le prestataire doit pour cela mettre en place un dispositif dédié de type antenne (radio, GPS).

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

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

- le système d'information du commanditaire :
  - pour la collecte des évènements ;
  - pour l'administration des dispositifs de collecte ;
  - pour l'exploitation des dispositifs de collecte ;
  - pour l'envoi d'information non sensible via canal non sécurisé, notamment la notification des évènements de sécurité ;
  - pour l'échange d'information sensible via canal sécurisé, et l'interaction avec le portail web de suivi des évènements de sécurité ;
- les serveurs de mise à jour pour télécharger les mises à jour des dispositifs du service de détection 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, à l'aide de solutions de filtrage qualifiées et utilisées conformément aux conditions de leur qualification.

c) Les flux aux interconnexions avec le service de détection doivent être chiffrés à l'aide de solutions de chiffrement et d'authentification conformes aux exigences de [AM_635], [AM_636] et [AM_637].

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 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 événements 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 évènements 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 et le système d'information du commanditaire à l'aide de solutions qualifiées lorsqu'elles existent, à défaut avec des solutions conformes aux exigences de [AM_635], [AM_636] et [AM_637].

IV.3.11. Zone de mise à jour

a) Le prestataire doit 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.

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 qui ne permettraient pas de mise à jour via un dépôt relais.

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

- 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 auprès des sources de mise à jour officielles des éditeurs ;
- 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 conformémant aux exigences de [AM_635], [AM_636] et [AM_637] ;
- 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.

IV.3.13. Zone d'échange commanditaire

a) Le prestataire doit mettre en place une zone d'échange commanditaire contenant un portail Web permettant la visualisation et la mise à jour de l'état des évènements de sécurité.

b) Il est **recommandé** au prestataire de mettre en place un annuaire dédié à l'authentification du commanditaire sur les dispositifs hébergés dans la zone d'échange commanditaire.

c) Le prestataire doit authentifier le commanditaire avec :

- des comptes individuels et au minimum deux facteurs pour l'authentification d'une personne vis-à-vis d'une machine ;
- la politique de mot de passe doit prendre en compte une longueur minimale, des chiffres, lettres majuscules, lettres minuscules, caractères spéciaux, un délai de modification, un nombre de tentatives de connexion avant verrouillage du compte, l'historique, etc.

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

e) 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 confiance qualifiés par l'AMSN.

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

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

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

i) 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 les postes de travail de consultation du commanditaire situé dans le système d'information du commanditaire (voir exigence IV.3.17.l) permettant la consultation de l'état des évènements via le portail web.

j) Les postes de travail utilisés par le commanditaire pour accéder au portail web doivent être intégrés au systèmes d'information du commanditaire.

k) Les recommandations des guides de bonnes pratiques de l'ANSSI (Recommandations de configuration matérielle de postes clients et serveurs x86, Recommandations pour les pour les déploiement sécurisé du navigateur, exigences de sécurité matérielles) doivent être appliquées aux postes de travail utilisés par le commanditaire. Les postes de travail doivent avoir fait l'objet d'une homologation.

l) La convention de service doit prévoir que le dispositif de filtrage du système d'information du commanditaire doit interdire les flux initiés depuis la zone d'échange commanditaire.

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

a) L'intégralité des dispositifs du service de détection interconnectés au périmètre supervisé (en particulier les collecteurs) doit être positionnée au sein d'une ou plusieurs[5] 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).

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 ;
- 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.

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

- les dispositifs impliqués dans la supervision des systèmes de détection qualifiés, agrégateurs ;
- 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.

e) Les dispositifs impliqués dans la chaîne de supervision des systèmes de détection qualifiés doivent être reliés par un lien réseau physiquement dédié.

f) 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 (voir exigence IV.3.8.b).

g) 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.

h) 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 évènements de sécurité du prestataire.

i) 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 par les systèmes de détection qualifiés.

j) Les systèmes de détection qualifiés doivent être configurés uniquement en écoute. Aucun flux ne doit être initié par les systèmes de détection qualifiés vers le système d'information du commanditaire.

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

- ceux initiés depuis cette enclave de collecte vers le système d'information du service de détection du prestataire et permettant uniquement de transmettre les évènements issus des systèmes de détection qualifiés de cette enclave vers la zone de collecte. Le prestataire doit limiter au maximum le nombre de flux permettant la remontée des évènements 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).

---

[5] 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

IV.3.15. 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) Il est **recommandé** que 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) Il est **recommandé** que le prestataire horodate et journalise les recherches en sources ouvertes réalisées.

f) 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].

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

h) 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.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.

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 respecter la législation et la réglementation monégasque 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 monégasque 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'Appendice 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. Appendice 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 pour assurer totalement et dans tous ses aspects la prestation.

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 évènements 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 d'expertise, de réponse et de traitement en matière d'attaques numériques (CERT-MC).

i) 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.

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

k) Le commanditaire doit désigner un référent opérationnel pour le service de détection des incidents de sécurité.

l) 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 deux fois par an.

b) 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 évènements 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 évènements 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) ;
- 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 désactivées ;

c) 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.

d) 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.

e) Le prestataire doit stocker et archiver les supports des comités opérationnels et comptes rendus associés dans un espace spécifique en tenant compte du niveau de sensibilité ou de classification de son contenu.

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 ;
- 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 en tenant compte du niveau de sensibilité ou de classification de son contenu.

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 évènements 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 évènements de sécurité.

d) Il est **recommandé** que le prestataire utilise les indicateurs proposés dans la norme [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 disponibilité des dispositifs techniques du service de détection :
    - o portail web de la zone d'échange commanditaire ;
    - o collecteur de l'enclave de collecte ;
    - o système d'envoi des notifications d'évènements ;
    - o outils techniques d'analyse ;

- gestion de la sécurité des interconnexions du SI du service de détection :

    o le nombre d'échecs d'authentification et authentifications réussies ainsi que la liste détaillée associée concernant l'accès à la zone d'échange commanditaire ;

- gestion des capacités de détection des évènements :

    • le nombre d'évènements collectés par le système de détection qualifié par mois ;

    • le nombre d'évènements de sécurité détectées par mois ;

    • le nombre de tickets ouverts par mois ;

    • le nombre de tickets clos par mois ;

    • la durée minimale, moyenne, maximale entre la création d'un ticket et sa clôture ;

    • le nombre de règles de détection implémentées dans les outils techniques d'analyse ;

    • le nombre de règles de détection créées ou désactivées 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 notifications :

    • le nombre de comptes autorisés à accéder au portail web pour le 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 ;

- gestion des évènements :

    • l'évolution du temps moyen de traitement des tickets, par mois ;

    • l'évolution du nombre de tickets ouverts cumulé par mois.

f) 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 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 évènements 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

La convention de service doit :

- décrire le périmètre et les objectifs de la prestation, le service de détection des évènements de sécurité et notamment les activités de gestion des évènements 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 employées lors de la prestation entre le prestataire et le commanditaire ;

- décrire le processus d'enregistrement et de traitement des plaintes portant sur la prestation déposées par le commanditaire, ainsi que la marche à suivre pour le dépôt de plainte.

IV.5.3.2. Organisation du service

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 ;

- stipuler que le prestataire collabore avec des tiers mandatés par le commanditaire et spécifiquement désignés par ce dernier ;

- 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.

IV.5.3.3. Responsabilités

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 évènements de sécurité ;

- 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 ;

- 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) ;

- stipuler que le prestataire a mis en place une procédure de gestion des changements concernant son propre système d'information ;

IV.5.3.4. Confidentialité et protection de l'information

La convention de service doit :

- identifier le niveau de sensibilité du service de détection des évènements de sécurité mis en œuvre par le prestataire ;

- identifier le niveau de sensibilité 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, ou obligation légale ;

- 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 transmises à un tiers ;

  • stipuler que le prestataire transmet au centre d'expertise, de réponse et de traitement en matière d'attaques numériques (CERT-MC) 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 ;

  • 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. Lois et réglementations

La convention de service doit :

- être rédigée en français ;

- préciser que seule la législation monégasque est applicable à la convention de service ;

- la durée de conservation des informations liées à la prestation et notamment les évènements collectés et les incidents de sécurité détectés doit être en accord avec la législation monégasque en vigueur.

IV.5.3.6. Livrables

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.5.3.7. Qualification du service

La convention de service doit indiquer que la prestation réalisée est une prestation conforme au présent document. Si la prestation est qualifiée, la convention doit inclure l'attestation de qualification du prestataire.

IV.5.3.8. Niveau de service

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 ;

- 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.

APPENDICES

APPENDICE 1 - RÉFÉRENCES DOCUMENTAIRES

1. Codes, textes législatifs et réglementaires

[LOI_IN]	Loi 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée Disponible sur https://www.ccin.mc/
[CP_308]	Article 308 du Code pénal relatif au secret professionnel. Disponible sur https://www.legimonaco.mc/
[CP_308-2]	Article 308-2 du Code pénal relatif à l'atteinte à la vie privée. Disponible sur https://www.legimonaco.mc/
[CP_341]	Article 341 du Code pénal relatif au secret des correspondances privées. Disponible sur https://www.legimonaco.mc/
[CP_389-1]	Article 389-1 du Code pénal relatif aux délits relatifs aux systèmes d'information. Disponible sur https://www.legimonaco.mc/
	Loi 1.435 du 08 novembre 2016 relative à la lutte contre la criminalité techno-logique. Disponible sur https://amsn.gouv.mc/
[AM_723]	Arrêté ministériel n°2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié. Disponible sur https://amsn.gouv.mc/
[AM_791]	Arrêté Ministériel 2019-791 du 17 décembre 2019 portant application de l'article 2, a) de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Mo-négasque de Sécurité Numérique, modifiée, définissant les règles destinées à garan-tir la sécurité des systèmes d'information sensibles. Disponible sur https://amsn.gouv.mc/
[AM_635]	Arrêté Ministériel n° 2018-635 du 2 juillet 2018 portant application de l'arrête ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée, définissant les règles et recommandations concernant le choix et le dimensionnement de l'ensemble des mécanismes cryptographiques. Disponible sur https://amsn.gouv.mc/
[AM_636]	Arrêté Ministériel n° 2018-636 du 2 juillet 2018 portant application de l'arrête ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée, definissant les règles et recommandations concernant les mécanismes d'au-thentification. Disponible sur https://amsn.gouv.mc/
[AM_637]	Arrêté Ministériel n° 2018-637 du 2 juillet 2018 portant application de l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée, définissant les règles et recommandations concernant la gestion des clés cryptographiques utilisées dans l'ensemble des mécanismes cryptographiques Disponible sur https://amsn.gouv.mc/

2. Normes et documents techniques

Renvoi	Document
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, AMSN, sur https://amsn.gouv.mc
[HYGIENE]	Guide d'Hygiène Informatique, ANSSI, version en vigueur. Dis-ponible sur http://www.ssi.gouv.fr
[NT_JOURNAL]	Recommandations de sécurité pour la mise en œuvre d'un sys-tème 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 sys-tèmes 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
[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 manage-ment 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

APPENDICE 2 - MISSIONS ET COMPÉTENCES DU PERSONNEL DU PRESTATAIRE

1. Opérateur analyste

a) Missions :

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

b) 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.

2. Administrateur d'infrastructure

a) 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.

b) 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.

3. Expert architecture

a) Missions :

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

b) Compétences :

- connaissances du fonctionnement des systèmes de détection ;
- 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.).

4. Expert métier détection

a) 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.

b) 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.

5. Responsable des droits d'accès

a) 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.

b) Compétences :

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

APPENDICE 3 - RECOMMANDATIONS AUX COMMANDITAIRES

Cette appendice liste les recommandations de l'AMSN aux commanditaires de prestations de détection des incidents de sécurité.

1. Qualification

a) Le commanditaire peut, lorsqu'il est une autorité administrative ou un opérateur d'importance vitale, demander à un PASSI 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'AMSN, 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 conforme au présent document, le commanditaire doit :

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

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 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.

f) Le commanditaire peut, conformément au processus de qualification de l'ANSSI des prestataires de service de confiance [QUAL_SERV_PROCESS], déposer auprès de l'AMSN une réclamation concernant un prestataire qualifié qui n'aurait pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée.

2. 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[6] 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 choisisse parmi les indicateurs proposés par la norme [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.

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

g) Il est **recommandé** que le commanditaire intégre dans la stratégie de collecte (voir exigence IV.2.2.a) la mise en œuvre de système de détection qualifié 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.

h) 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.

---

[6] [15] Le catalogue des prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés est publié sur le site de l'AMSN

i) 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.

3. 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.

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)[7] en cas d'incident de sécurité suspecté ou avéré.

e) Le commanditaire doit établir, éventuellement avec l'aide d'un PASSI, 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.

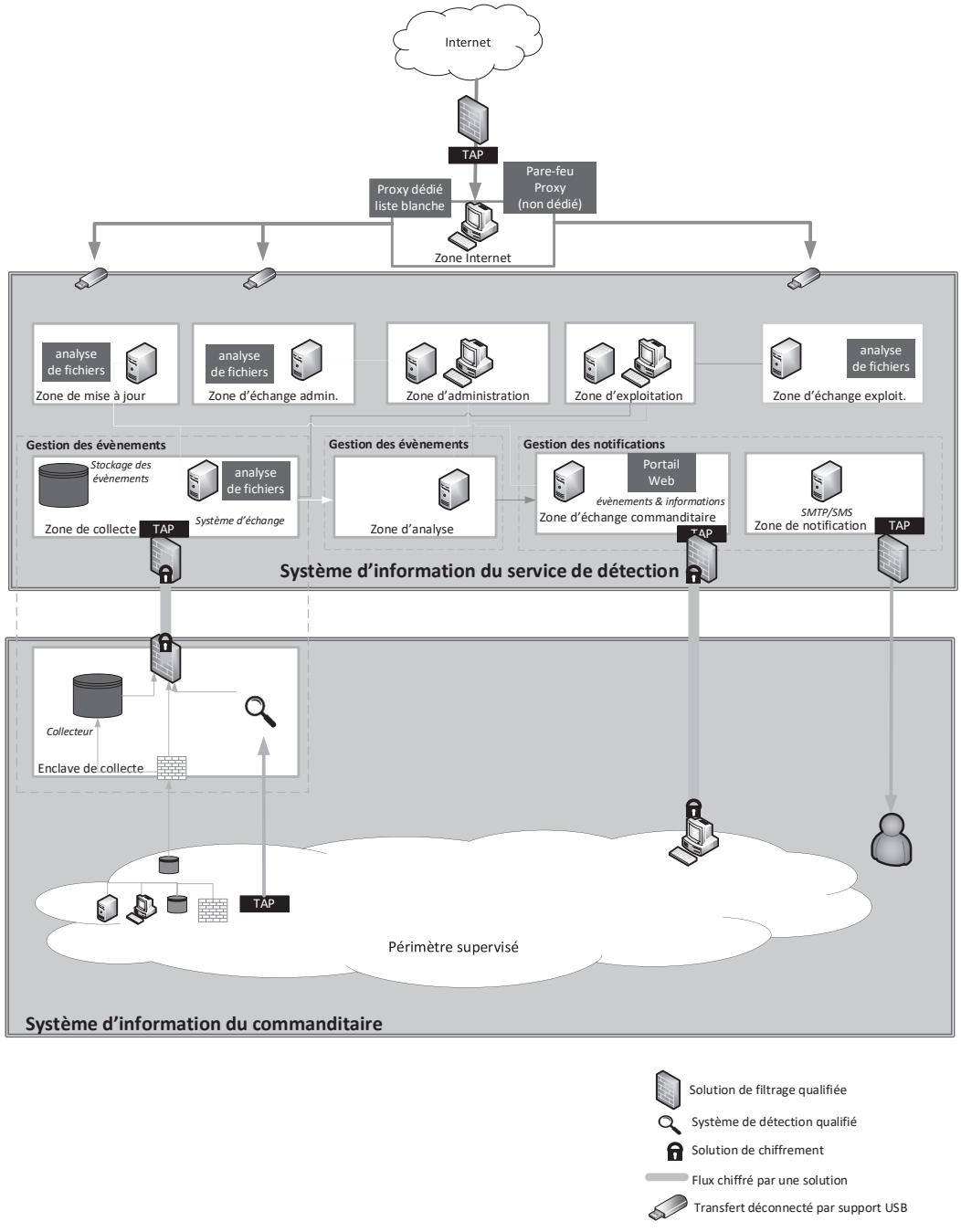
f) Il est **recommandé** que le prestataire et le commanditaire utilise l'échelle de gravité des incidents de sécurité de l'annexe C de la norme [ISO27035].

---

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

APPENDICE 4 - SCHÉMA ILLUSTRATIF D'UNE ARCHITECTURE CONFORME AU RÉFÉRENTIEL

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.



APPENDICE 5 - RÈGLES RELATIVES À L'USAGE D'UN AGRÉGATEUR DE FLUX

Il est autorisé d'utiliser un agrégateur entre des Tap et un système de détection, dans les conditions suivantes :

- L'agrégateur doit être utilisé exclusivement pour assurer la fonction d'agrégation ;
- L'agrégateur doit être administré de la même manière et dans les mêmes conditions de sécurité que pour les systèmes de détection qualifiés ;
- 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' évènements 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 système de détection qualifié.

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 un système de détection qualifié disposant de plusieurs interfaces réseau et assurant la fonction d'agrégation.

imprimé sur papier recyclé

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO