LE PREMIER MINISTRE

REPUBLIQUE TOGOLAISE
Travail-Liberté-Patrie

ARRETE N° 2025-006 /PMRT
portant adoption du référentiel d'exigences des prestataires de détection des incidents de sécurité

LE PREMIER MINISTRE,

Vu la constitution du 06 mai 2024 ;

Vu la loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité modifiée par la loi n° 2022-009 du 24 juin 2022 ;

Vu le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité ;

Vu l'arrêté n° 2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise ;

Vu le décret n° 2022-09/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;

Vu le décret n° 2024-040/PR du 1er août 2024 portant nomination du Premier ministre ;

Vu le décret n° 2024-041/PR du 20 août 2024 portant composition du gouvernement ;

Vu le procès-verbal de la réunion du Comité stratégique de l'Agence nationale de la cybersécurité (ANCy), en sa séance du 02 décembre 2024 ;

ARRETE :

Article 1er : Objet

Le présent arrêté porte adoption du référentiel d'exigences des prestataires de détection des incidents de sécurité en République togolaise.

Article 2 : Application

Les ministres, chacun en ce qui le concerne, veillent à l'application des dispositions du présent arrêté par les administrations et les opérateurs de services essentiels (OSE) relevant de leur ressort.

Article 3 : Exécution

Le Directeur général de l'Agence nationale de la cybersécurité (ANCy), est chargé de l'exécution du présent arrêté qui sera publié au Journal officiel de la République togolaise.

Fait à Lomé, le 31 JAN 2025

Le Premier ministre

SIGNE

Victoire S. TOMEGAH-DOGBE

Pour ampliation,
Le Ministre,
Secrétaire général du Gouvernement

Christian Eninam TRIMUA

ANCy
Agence Nationale de la Cybersécurité

RÉPUBLIQUE TOGOLAISE

REFERENTIEL D'EXIGENCES

Prestataires de Détection des Incidents de Sécurité (PDIS)

Version 1.0 du 31 JAN 2025

Premier Ministre	
Comité Stratégique	Agence Nationale de la Cybersécurité (ANCy)

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
31/01/2025	1.0	Première version applicable	ANCy

Les commentaires sur le présent document sont à adresser à :

Agence Nationale de la Cybersécurité

63, Boulevard du 13 janvier, Nyékonakpoè

07 BP 7878 Lomé – TOGO

Téléphone : + 228 70 60 60 58 / 97 52 58 58

secretariat.ancy@ancy.gouv.tg

Table des matières

FICHE SYNTHETIQUE

1. Introduction

Un **Prestataire de Détection des Incidents de Sécurité (PDIS)** est une organisation spécialisée dans la surveillance proactive des systèmes d'information pour identifier les anomalies, les intrusions ou les cyberattaques. Sa mission principale est de :

- **Surveiller en temps réel** les infrastructures pour détecter les menaces ;
- **Analyser les événements suspects** afin de confirmer ou d'infirmer une attaque ;
- **Alerter leurs clients** et les accompagner dans les premières étapes de la gestion des incidents.

2. Objectifs du référentiel

Le référentiel des PDIS poursuit trois objectifs principaux :

- **Renforcer la sécurité des systèmes d'information** : en exigeant des mécanismes avancés de surveillance et d'analyse ;
- **Garantir la crédibilité des services proposés** : en imposant des normes strictes et des exigences spécifiques ;
- **Établir la confiance entre les PDIS et leurs clients** : grâce à des règles claires concernant la confidentialité, la protection des données et l'efficacité opérationnelle.

3. Principes clés du référentiel

- **Proactivité dans la surveillance** : les PDIS doivent mettre en œuvre des mécanismes permettant de détecter les incidents en temps réel ou dans les délais les plus courts possibles, afin de limiter les impacts des cyberattaques ;
- **Protection des données** : les informations collectées et traitées dans le cadre des activités de détection doivent être strictement protégées contre tout accès non autorisé ou usage abusif ;
- **Professionnalisme et compétence** : les PDIS doivent démontrer une expertise avérée en matière de détection des menaces, d'analyse des événements et de gestion des incidents.

Étapes essentielles du processus de détection

- **Surveillance et collecte d'informations** : le prestataire doit utiliser des outils performants pour surveiller en continu les infrastructures des clients. Ces outils collectent des données telles que les journaux de connexion, les alertes systèmes ou les flux réseau afin d'identifier des anomalies ;
- **Analyse et détection** : les données collectées sont ensuite analysées pour détecter des événements suspects ou des indicateurs de compromission. Cette étape repose sur des algorithmes, des règles de corrélation ou des modèles comportementaux avancés ;

- **Signalement des incidents** : lorsqu'un incident est détecté, le prestataire doit en informer immédiatement le client et fournir des informations détaillées sur la nature, la gravité et les impacts potentiels de l'incident ;
- **Assistance à la réponse** : les PDIS ne se limitent pas à la détection. Ils doivent également accompagner leurs clients dans les premières étapes de réponse, comme l'isolation des systèmes affectés ou la collecte de preuves pour l'investigation.

4. Exigences applicables aux PDIS

- **Infrastructure technique** : les PDIS doivent disposer d'une infrastructure robuste et résiliente, capable de supporter des volumes importants de données. Tous les équipements doivent être hébergés localement au Togo, sauf dérogation accordée par l'Agence Nationale de la Cybersécurité ;
- **Compétences et ressources humaines** : le personnel technique doit être qualifié, avec des certifications en cybersécurité et en détection des incidents. Par ailleurs, 100 % du personnel technique doit être de nationalité togolaise, sauf exception justifiée et approuvée ;
- **Confidentialité et éthique** : le prestataire est tenu de respecter des normes strictes de confidentialité et d'éthique, en veillant à ne pas exploiter les informations collectées à d'autres fins que celles convenues avec le client ;
- **Conformité réglementaire** : les PDIS doivent se conformer aux réglementations nationales et internationales en matière de sécurité et de protection des données.

5. Types d'incidents couverts

- **Menaces internes** : les PDIS doivent être capables de détecter des comportements suspects ou des malveillances provenant de l'intérieur de l'organisation ;
- **Cyberattaques externes** : cela inclut les attaques telles que les tentatives d'intrusion, les attaques par déni de service (DDoS) ou les campagnes de phishing ;
- **Anomalies systémiques** : les PDIS doivent également identifier des anomalies pouvant indiquer des vulnérabilités ou des failles exploitables au sein des systèmes surveillés.

6. Importance du référentiel pour la sécurité nationale

- **Encadrer la profession** : Éviter la prestation de services de détection de faible qualité ou non conformes.
- **Assurer une sécurité renforcée** : Prévenir efficacement les cyberattaques et limiter leurs impacts.
- **Créer une dynamique locale** : Favoriser l'emploi de professionnels togolais qualifiés et renforcer les capacités nationales en cybersécurité.

7. Conclusion

Le référentiel des PDIS est une pierre angulaire du système de cybersécurité au Togo. En définissant des exigences précises pour les infrastructures, les compétences et les processus de détection, il garantit un niveau de protection élevé pour les organisations tout en contribuant au renforcement des capacités nationales. Il s'inscrit dans une vision globale d'un espace numérique sûr, résilient et digne de confiance.

1.PRESENTATION GENERALE

1.1. AVANT-PROPOS

Le service de détection des incidents de sécurité s'adresse à des organisations qui désirent maîtriser leurs risques et augmenter le niveau de sécurité de leurs systèmes d'information. La finalité du service de détection des incidents de sécurité se base sur une approche proactive, en vue de gérer des menaces à l'aide d'une veille, de la mise en place de mesures de sécurité, de l'installation d'outils de détection des intrusions, de détection des vulnérabilités, de filtrage et de découverte des actifs, ainsi que la détection des incidents et leurs analyses.

L'exploitation de systèmes de détection d'incidents de sécurité concourt ainsi à la protection d'un système d'information face aux menaces de cyberattaques.

1.2. OBJECTIF DU REFERENTIEL ET DOMAINE D'APPLICATION

Ce document constitue le Référentiel d'exigences applicables aux Prestataires de détection des incidents de sécurité qualifiés par l'ANCy.

Il vise à établir un cadre permettant la qualification et le maintien de la qualification des Prestataires de services de détection des incidents de sécurité par l'ANCy.

Le présent Référentiel permet d'une part d'accompagner les Prestataires dans la fourniture des services de détection des incidents, et d'autre part au Client final de disposer de garanties sur les compétences du Prestataire et de son personnel, sur la qualité des prestations de détection des incidents et sur la confiance qu'il peut leur accorder, en particulier en ce qui concerne la confidentialité.

Il a vocation à permettre la qualification de cette famille de Prestataires de services de confiance en cybersécurité, conformément à la règlementation en vigueur et selon les modalités décrites dans le Modèle de qualification des Prestataires de service de confiance en cybersécurité au Togo.

1.3. DOCUMENTS DE REFERENCE

Le présent Référentiel s'inscrit dans un cadre légal et règlementaire plus global en vigueur au Togo, et applicable aux Prestataires de services de confiance en cybersécurité.

L'ensemble des textes découlant de ce cadre légal et règlementaire et susceptibles de s'appliquer aux Prestataires de détection des incidents de sécurité ainsi qu'à leurs prestations sont listés ci-dessous de manière non-exhaustive. Ils sont identifiés dans le Référentiel en tant que « Documents de référence ».

Le présent Référentiel s'applique en complément des Documents de référence dont il n'exclut pas l'application. Il n'exclut pas non plus l'application des règles générales imposées aux Prestataires en leur qualité de professionnels, et notamment leur devoir de conseil vis-à-vis des Clients finaux.

Le référentiel peut être utilisé à titre de bonnes pratiques en dehors de tout contexte règlementaire.

1.3.1. Normes Internationales

- La norme ISO 9001 :2015 relatives aux exigences pour la mise en place d'un système de management de la qualité ;
- La norme ISO 22301 :2019, Sécurité et résilience, Systèmes de management de la continuité d'activité ;
- La norme ISO 27001 :2022, Sécurité de l'information, cybersécurité et protection de la vie privée ;
- La norme ISO 27002 : 2022, Sécurité de l'information, cybersécurité et protection de la vie privée- Mesures de sécurité de l'information, ;
- La norme NIST SP 800-53 : Cadre de contrôles de sécurité et de confidentialité des systèmes d'information ;
- La norme ISO 27005 :2022, Sécurité de l'information, cybersécurité et protection de la vie privée- Préconisations pour la gestion des risques liés à la sécurité de l'information ;
- La norme ISO 27035, Gestion des incidents de sécurité de l'information.

1.3.2. Textes législatifs et règlementaires

- La loi n° 2017-007 du 22 juin 2017 relative aux transactions électroniques en République togolaise ;
- La loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité, modifiée par la loi n° 2022-009 du 24 juin 2022 ;
- La loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;

- La loi n°2020-009 du 10 septembre 2020 relative à l'identification biométrique des personnes physiques au Togo ;
- Le décret n°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo ;
- Le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'ANCy ;
- Le décret n° 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;
- Le décret n°2019-098/PR du 11 juillet 2019 portant création, attributions et organisation de la société CYBER DEFENSE AFRICA (CDA) ;
- Le décret n° 2022-09/PR du 25 août 2022 relatif à la qualification des Prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;
- L'arrêté n°016/MPEN/CAB du 17 décembre 2018 fixant les conditions de reconnaissance au Togo des certificats et signatures électroniques délivrés par des Prestataires de services de confiance établis hors du territoire national ;
- L'arrêté n° 2022-040/PRMT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise.

Ces documents sont disponibles sur les sites de l'ANCy.

1.3.3. Documents de l'ANCy

- Décision ANCy portant liste des pays tiers de confiance ;
- Modèle de qualification des Prestataires de services de confiance en cybersécurité ;
- Déclaration de la politique de qualification.

1.3.4. Autres

- Cadre : Enissa, CSIRT Maturity Framework
  Cadre SOC-CMM, SIM3

1.4. IDENTIFICATION DU DOCUMENT ET DATE D'APPLICATION

Le présent document est dénommé « Référentiel d'exigences des Prestataires de détection des incidents de sécurité ».

Il peut être identifié par son nom, sa référence, son numéro de version et sa date de mise à jour.

Ce document est applicable à compter de sa publication.

Il est élaboré, mis à jour et publié par l'ANCy, qui précisera les modalités de transition et la date d'effet pour chaque mise à jour.

1.5. ACTIVITES DE DETECTION D'INCIDENT VISEES PAR LE REFERENTIEL

La prestation de détection d'incident permet aux entreprises de bénéficier d'un service de supervision pérenne de leurs systèmes d'information afin de détecter et de traiter proactivement tout type d'anomalies ou de suspicions.

Pour assurer ce service, le Prestataire est amené à déployer des technologies de détection de menaces telles que les solutions SIEM, XDR, EDR, IDS/IPS ou autres, et ce en fonction du périmètre à couvrir et des spécificités du système d'information à superviser.

La détection d'incident, nécessite la mise en œuvre d'un ensemble de services complémentaires pour maximiser la visibilité et l'efficacité des opérations de supervision.

À cet égard, le Prestataire doit fournir au minimum les prestations ci-après :

- Le *monitoring* : Supervision des systèmes en 24/24h et 7/7j ;
- Le traitement des alertes : les alertes doivent être analysées et devront passer par une procédure de triage et d'escalade ;
- La réponse à l'incident du premier niveau : pour les alertes avérées, le Prestataire doit engager un processus de réponse de premier niveau ;
- L'escalade : Pour les alertes avérées, le Prestataire doit informer le Client final en se basant sur une procédure préétablie, et s'il s'agit d'un incident grave il peut escalader vers un prestataire de réponse aux incidents de sécurité qualifié pour assurer le service de réponse aux incidents ou les traiter s'il est qualifié pour la prestation de réponse aux incidents.

Le service de détection des incidents de sécurité regroupe les prestations ci-après :

- ***Détection des incidents***
  - ***Détection des alertes***

C'est l'ensemble des moyens techniques et organisationnels visant à détecter et évaluer un incident de sécurité à partir d'événements recueillis ainsi que le stockage et l'archivage des incidents dans le but d'améliorer le processus de détection.

  - ***Réponse du premier niveau***

C'est l'ensemble des moyens techniques et organisationnels permettant de traiter les alertes et d'escalader les incidents avérés.

- ***Gestion des événements***

C'est l'ensemble des moyens techniques et organisationnels assurant la collecte et l'enregistrement des événements liés à la sécurité.

- ***Gestion des notifications***

C'est l'ensemble des moyens techniques et organisationnels permettant de communiquer au Client final l'état des incidents de sécurité détectés ainsi que le stockage de ces incidents.

Par ailleurs, le Prestataire peut assurer d'autres activités qui ne sont pas sujettes à qualification, à l'instar de :

- L'activité de veille, également appelée *Threat Intelligence,* qui regroupe l'ensemble des activités de renseignement permettant de prémunir toute entité d'une menace potentielle. Elle englobe la veille sur les attaques, la veille sur les adresses IP publiques associées à des activités malveillantes, la veille sur les fuites de données, le *Brand Abuse* (veille sur les messages publiés), la veille sur l'état du nom de domaine incluant le *mail/web server* (blacklist, erreur, etc.) ;
- L'activité d'anti-phishing, qui consiste à explorer en temps-réel les URLs des pages de phishing et en analyser le contenu, pour vérifier si les informations associées au domaine du Client final y figurent, ce qui peut indiquer la probabilité qu'une attaque par phishing aura lieu. Le Prestataire procédera à signaler ces domaines au CERT avec lequel il est souscrit. ;
- L'activité d'analyse du *Dark Web* qui consiste à scruter le *Dark Web* et d'autres sources Internet pour vérifier si les informations associées aux Clients finaux ont été compromises ou sont en cours ;

Ces activités constituent des sources d'informations essentielles pour les services de réponse aux incidents.

1.6. DEFINITIONS ET ACRONYMES

1.6.1. Client final

C'est la partie qui sollicite ou commande la réalisation d'une prestation de détection des incidents de sécurité.

1.6.2. Collecteur

Un collecteur est un dispositif technique servant à centraliser les événements de sécurité générés par les sources de collecte comme un équipement réseau, serveur syslog, collecteur d'une solution d'analyse d'évènements de sécurité (SIEM).

Il existe deux types de collecteurs dans le cadre du service de détection :

- Les collecteurs locaux : déployés sur le système d'information du Client final, qui centralisent les événements au niveau local.
- Les collecteurs centraux : déployés sur le système d'information du Prestataire, qui centralisent de manière sécurisée l'ensemble des événements remontés par les collecteurs locaux.

1.6.3. Contrat de prestation

C'est l'accord formel entre le Prestataire de service de détection des incidents de sécurité et le Client final. Il doit obligatoirement contenir certaines informations, dont le contenu est précisé dans le Référentiel.

1.6.4. État de l'art

Ensemble de bonnes pratiques et de connaissances relatives à la détection des incidents de sécurité, publiquement accessibles et reconnues à un moment donné, ainsi que des informations qui en découlent de façon évidente.

1.6.5. Prestataire de service de détection des incidents de sécurité qualifié

Un Prestataire de service de détection des incidents de sécurité qualifié est un Prestataire qui dispose d'une qualification pour la réalisation des prestations de détection des incidents de sécurité.

1.6.6. Prestataire

Fait référence au Prestataire de service de détection des incidents de sécurité dans le cadre du présent Référentiel.

1.6.7. Référentiel

Le présent document.

1.6.8. Segmentation du système

C'est la séparation ou l'isolation des différentes composantes, unités ou fonctions, au sein d'une organisation du service de détection ou du système du Client final. Cette segmentation assure notamment le stockage sécurisé de l'historique des actions déployées.

1.6.9. Service SOC interne

C'est le service de détection des incidents ayant pour périmètre le système d'information du Prestataire.

2. EXIGENCES RELATIVES AUX PRESTATAIRES DE SERVICES DE DETECTION DES INCIDENTS DE SECURITE

2.1. EXIGENCES GENERALES

a. Le Prestataire de détection des incidents doit être une entité ou une partie d'une entité, dotée de la personnalité morale, dûment enregistrée au RCCM (Registre du Commerce et du Crédit Mobilier) pour les besoins de l'activité de détection des incidents de sécurité, de façon à pouvoir en être tenu juridiquement responsable.

b. Le Prestataire de détection des incidents doit respecter la règlementation en vigueur au Togo y compris le Modèle de qualification des Prestataires de Services de Confiance en Cybersécurité et le présent Référentiel, ainsi que l'état de l'art.

c. Le Prestataire doit mettre en œuvre, pour son propre compte, un service SOC interne, portant sur le système d'information du service de détection des incidents de sécurité.

d. Le Prestataire de détection des incidents doit décrire l'organisation de son activité de détection des incidents à chaque Client final et garantir que les informations qu'il fournit à cet égard sont exactes.

e. Le Prestataire de détection des incidents a l'obligation de formaliser les prestations qu'il réalise pour le compte du Client final dans le cadre d'un contrat de prestation de services écrit et signé avec celui-ci. Ce contrat doit être conforme aux exigences du Référentiel et aux lois en vigueur au Togo.

f. En sa qualité de professionnel, le Prestataire est redevable d'un devoir de conseil à l'égard du Client final.

g. Le Prestataire de détection des incidents doit solliciter le Client final afin d'obtenir communication des éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité, s'y conformer, et le cas échéant accompagner le Client final dans la démarche de mise en œuvre de ces obligations si ce dernier lui en fait la demande et dans la mesure où la mobilisation du Prestataire est nécessaire à ces fins.

h. Le Prestataire de détection des incidents peut, après approbation du Client final, sous-traiter une partie des activités requises par le Client final à un autre Prestataire de détection des incidents qualifié, sous réserve que ce dernier soit conforme aux exigences du Référentiel d'exigences qui lui est applicable.

i. Le Prestataire de détection des incidents doit réaliser la prestation de manière loyale et impartiale. Il doit par ailleurs faire preuve de respect personnel et de professionnalisme à l'égard du Client final, de son personnel et de ses infrastructures. A cet égard, le prestataire doit apporter une preuve suffisante que son organisation, ses moyens mis en œuvre pour délivrer la prestation, et les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du Client final ou de provoquer des conflits d'intérêts.

j. Le Prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte du Client final dans le cadre de la prestation, et en particulier les éventuels dommages qu'il pourrait lui causer. À ce titre, le prestataire doit préciser les types de dommages concernés et les modalités de partage des responsabilités dans le contrat de prestation de services, en tenant compte de toutes les éventuelles activités sous-traitées.

k. En vue de garantir sa responsabilité vis-à-vis du Client final, le Prestataire a l'obligation de souscrire à une assurance professionnelle couvrant les éventuels dommages causés au Client final et notamment à son système d'information dans le cadre de la prestation.

l. Le prestataire de détection des incidents de sécurité doit informer le Client final lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementale (par exemple à l'ANCy dans le cadre de l'article 17 du décret n°2019-095/PR relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes) et doit l'accompagner dans cette démarche si ce dernier en fait la demande.

m. Le Prestataire de détection des incidents de sécurité doit fournir au Client final un service d'assistance à distance qui lui permet de signaler un incident de sécurité suspecté ou confirmé. Ce service devrait faciliter au Prestataire la résolution des problèmes de production liés aux

dispositifs qu'il gère et lui permettre d'assister et conseiller le Client final. Ce service doit être accessible via un numéro téléphonique et une adresse email.

n. Le Prestataire doit garantir la confidentialité, l'intégrité et la non-répudiation de toutes les informations échangées entre le système d'information du service de détection des incidents de sécurité et le système d'information du Client final dans le cadre de la prestation, à l'aide de solutions qualifiées par l'ANCy.

o. Le Prestataire doit désigner au sein de son service un point de contact pour le Client final, chargé d'assurer le suivi avec celui-ci. Cet interlocuteur devra participer aux réunions du comité de pilotage entre le Client final et le Prestataire.

2.2. ORGANISATION DU PRESTATAIRE ET GOUVERNANCE

2.2.1. Gestion des ressources et des compétences

a. Le Prestataire doit en permanence, disposer au minimum de quatre (04) Analystes de niveau 1, et d'un (01) analyste de gestion d'incident de sécurité. Le non-respect de cette condition sur une période au moins égale à six (06) mois constitue pour l'ANCy un motif de suspension de la qualification du prestataire de détection des incidents de sécurité.

b. Le Prestataire doit disposer d'un Responsable Opérationnel et d'un administrateur réseau et système, et pouvoir avoir recours à la sous-traitance pour avoir un nombre suffisant d'analystes afin d'assurer totalement et dans tous ses aspects, la prestation qualifiée.

c. Le Prestataire doit établir de manière claire et documentée la liste complète des dispositifs hébergés ainsi que les différents rôles d'administrateur et d'utilisateur au sein de son service de détection des incidents de sécurité.

d. Le Prestataire doit posséder en interne, un centre de surveillance et d'alerte dédié aux cyberattaques.

e. Le Prestataire doit instaurer un système de roulement (*Shift*) pour assurer la couverture du service 24/24H. À cet égard, il doit garantir la disponibilité de son équipe en tout temps, et notamment en dehors des heures habituelles de travail.

f. Le Prestataire doit s'assurer de la compétence de ses ressources et du maintien de cette compétence, à travers un processus de formation continue et une veille technologique. La formation continue du Prestataire et de son personnel peut prendre plusieurs formes notamment des modules d'auto-formation, des séminaires internes, ou des séminaires assurés par le CERT.tg ou par l'ANCy. La nature et la liste des formations validantes au titre de la formation continue du prestataire de détection et de son personnel font l'objet d'une

publication sur le site de l'ANCy. Le Prestataire doit à tout moment, être en mesure de documenter son plan de formation continue à l'ANCy sur simple demande de celle-ci.

g. Le Prestataire doit s'assurer de créer et de fournir au personnel technique, des manuels d'exploitation ou d'administration relatifs aux dispositifs du service de détection des incidents de sécurité.

h. Le Prestataire justifie, au travers de ses ressources (dont l'évaluation a été faite au moment de la qualification en tant que Prestataire de détection des incidents de sécurité), qu'il dispose des compétences techniques, théoriques et pratiques nécessaires pour mener des activités de détection des incidents de sécurité couvertes par la portée de la qualification obtenue.

Plus spécifiquement, le service du Prestataire nécessite les compétences suivantes :

Compétences techniques
Administration des systèmes d'exploitation et des équipements réseaux
Administration des systèmes de détection
Connaissance approfondie des protocoles réseau et expertise dans l'analyse de flux réseau
Compétences en sécurité
Connaissance des principales techniques d'attaques
Connaissances des produits de sécurité
Expérience en interprétation de résultats et des alertes
Capacité de veille technique sur les alertes de vulnérabilité et l'évolution des cyber menaces
Connaissances spécifiques du système d'information du Client final
Topologie du SI et points d'accès externes
Topologie applicative et connaissances des flux considérés comme normaux
Populations à risque et Périodes de charge
Lacunes opérationnelles et de sécurité du système d'information

2.2.2. Organes de pilotage

La gouvernance du service de détection des incidents de sécurité doit s'appuyer sur des comités de suivi et pilotage. Indépendamment de la structure du service, l'objectif de ces comités est de coordonner l'ensemble des parties impliquées dans la fourniture de la prestation.

a. Comité de pilotage

Le Prestataire met en place, en collaboration avec le Client final, des réunions de pilotage planifiées à une fréquence au moins mensuelle, dans le but d'assurer le bon pilotage du service de détection des incidents de sécurité. Elles sont animées par le responsable opérationnel du service, qui doit à minima traiter les points suivants :

- Le récapitulatif de la période précédente du point de vue du service de supervision inclut : la liste des incidents critiques, les principales requêtes, les résultats des changements effectués, ainsi que l'état des actions en cours,
- Le tableau de bord projet synthétisant les indicateurs clés de performance contractuels (nombre d'incidents, nombre de tickets clos, les services impactés par les incidents),
- L'évolution du périmètre du service et la stratégie de prise en compte des changements ou actions demandés le mois précédent.

b. Comité stratégique

Le Prestataire met en place, en présence des représentants de l'organe de direction du Client final, un comité stratégique consistant en des réunions planifiées à une fréquence annuelle ou semestrielle, et clôturées par des procès-verbaux.

Le comité stratégique doit à minima, traiter les thèmes suivants :

- Le bilan de la période écoulée : synthèse des moments forts, tableau de bord projet et du service.
- Les risques et changements ayant un impact potentiel sur le bon déroulement du service, ou la stratégie de prise en compte des évolutions sur la période à venir.
- Le planning prévisionnel correspondant.

2.2.3. Recrutement et code d'éthique

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.

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.

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

Le Prestataire doit disposer d'un code d'éthique, signé et/ou ratifié par chaque membre du personnel, et dont une copie doit être adressée à l'ANCy.

Le Code d'éthique inclut au minimum les exigences ci-après :

- Les prestations sont réalisées avec loyauté, discrétion et impartialité ;
- Les membres du personnel ne recourent qu'aux méthodes, outils et techniques validés par le Prestataire ;
- Les membres du personnel 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 écrite et préalable du Client final ;
- Les membres du personnel s'engagent à signaler au Prestataire tout contenu manifestement illicite découvert pendant la prestation ;
- Les membres du personnel s'engagent à respecter la législation et la réglementation nationale en vigueur et les bonnes pratiques liées à leurs activités.
- Le Prestataire est tenu de rappeler à tous les membres de son personnel les principes du Code d'éthique qu'ils ont préalablement signé avant d'effectuer la prestation.

Le Prestataire doit veiller au respect du Code d'éthique par son personnel et prévoir des sanctions disciplinaires visant à minima les opérateurs, administrateurs et experts du service de détection ayant enfreint les règles de sécurité ou le Code d'éthique.

A cet égard, le Prestataire doit élaborer et mettre en œuvre un plan de sensibilisation de son personnel à la sécurité des systèmes d'information et des mesures de sécurité associées ainsi qu'à la législation

et la réglementation nationale en vigueur en rapport avec le service de détection des incidents de sécurité.

2.2.4. Politique de sécurité

Le Prestataire doit établir un document comportant une appréciation des risques et un plan de traitement des risques associé sur l'ensemble du périmètre du service de détection des incidents de sécurité.

L'appréciation des risques et le plan de traitement doivent être formellement validés et consignés auprès de l'organe de direction du Prestataire.

L'appréciation des risques doit faire l'objet d'une revue au moins une fois par an.

Cette appréciation doit prévoir une liste d'incidents redoutés qui pourraient affecter le système d'information du service de détection des incidents, à savoir :

- Les tentatives d'intrusion sur le système d'information du service de détection depuis une de ses interconnexions ;
- Les tentatives de rebond entre les systèmes d'information des Clients finaux à travers le système d'information du service de détection ;
- Les tentatives d'élévation de privilèges par les utilisateurs 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.

En cas de modifications significatives du service de détection, notamment celles liées à son hébergement, son infrastructure ou son architecture, le Prestataire doit procéder à une révision de l'appréciation des risques ainsi que du plan de traitement des risques associés. Le Prestataire doit par ailleurs disposer d'une politique de sécurité des systèmes d'information basée sur l'appréciation des risques.

Le Prestataire doit réaliser un audit sur son propre système d'information, s'il est qualifié comme prestataire d'audit ou faire appel, le cas échéant à un Prestataire de services d'audit qualifié par l'ANCy.

Il doit au surplus disposer d'un programme d'audit sur trois (03) ans couvrant toutes les activités de détection des incidents de sécurité.

Le Prestataire doit respecter l'ensemble des mesures et préconisations relatives à la sécurisation des sauvegardes telles que définies dans la norme ISO 27002.

Le Prestataire peut par ailleurs se conformer à la norme ISO27001.

Enfin, il est fortement recommandé que les prestations fournies par le Prestataire soient certifiées ISO27001.

3. EXIGENCES RELATIVES À LA FOURNITURE DU SERVICE DE DETECTION DES INCIDENTS DE SECURITE

3.1. EXIGENCES MINIMALES DE LA FOURNITURE DU SERVICE DE DETECTION DES INCIDENTS DE SECURITE

a. Le Prestataire doit disposer d'une localisation physique, des équipes, et de son propre système d'information sécurisé d'accès, du secours, et d'un ensemble de matériels dédiés au service de détection, ainsi que de son segment du système dédié. Les locaux du Prestataire doivent être protégés par un système de contrôle d'accès physique, un système de vidéosurveillance et un système anti-incendie.
b. Le Prestataire doit déployer des équipements et système qualifiés ou reconnus par l'ANCy dans son service de détection des incidents de sécurité. La salle abritant ces systèmes doit disposer d'une bonne protection physique et environnementale.
c. Le Prestataire doit mettre en place des collecteurs pour recueillir des données provenant des environnements du Client final.
d. Le Prestataire peut exploiter une solution existante chez le client final sans avoir besoin de collecter des données.
e. Le Prestataire doit mettre en place un système de stockage centralisé sécurisé pour conserver les données sensibles du Client final, conformément aux réglementations de sécurité et de confidentialité, et aux Documents de référence.
f. Le Prestataire doit établir un canal de communication sécurisé entre les composants du service de détection des incidents de sécurité et d'autres systèmes.
g. Le Prestataire doit lorsqu'il gère concomitamment des opérations de sécurité pour plusieurs Client finaux, agir de manière isolée et procéder à une ségrégation claire et stricte des données et activités desdits clients.

h. Le Prestataire doit assurer le service de veille et de *monitoring,* et générer des rapports détaillés sur les activités de sécurité pour chaque Client final.

i. Le Prestataire doit disposer d'interfaces internes et externes sécurisées contre les accès non autorisés, les atteintes à la confidentialité, et les autres menaces potentielles.

j. Le Prestataire doit disposer d'une architecture permettant la ségrégation claire des rôles au sein du service pour garantir la confidentialité et la protection des informations sensibles.

k. Le Prestataire doit disposer d'une architecture robuste avec des mécanismes de redondance capables de s'adapter à la croissance du nombre de Client finaux et à l'augmentation du volume de données à traiter, tout en assurant la continuité du service.

l. Le Prestataire doit utiliser des outils d'analyse centralisés en vue d'assurer des prestations pour l'ensemble des Client finaux.

m. Le Prestataire doit intégrer dans ses processus, des mécanismes d'automatisation en vue d'améliorer son efficacité opérationnelle et accélérer le temps de réponse.

n. Le Prestataire doit avoir documenté toutes les procédures de détection et qualification d'incidents, de supervision, de contrôle d'administration du service de détection des incidents, ainsi que de veille.

o. Le Prestataire doit définir avec le Client final des indicateurs opérationnels et stratégiques du service de détection des incidents de sécurité. Il doit au minimum définir les indicateurs suivants :

    - Indicateurs opérationnels : gestion de l'infrastructure, support du service de détection, gestion de la sécurité des interconnexions du SI du service de détection, gestion des capacités de détection, gestion des incidents, gestion des événements, et gestion des notifications.
    - Indicateurs stratégiques : gestion de la sécurité des interconnexions du SI du service de détection, gestion des événements et gestion des notifications.

3.2. RESSOURCES HUMAINES NECESSAIRES POUR LA FOURNITURE DU SERVICE

L'organisation minimale liée à la fourniture d'un service de détection et de qualification des évènements de sécurité que doit respecter un Prestataire de détection des incidents de sécurité est la suivante :

3.2.1. Analyste de niveau 1

Éducation
Minimum Niveau Bac +3 et plus en technologie des systèmes d'information et des communications ou équivalent.
Formation
Formation en opérations de cybersécurité dans un domaine connexe (par exemple opérations de sécurité, sécurité des réseaux, détection et atténuation des menaces).
Principales missions
La détection précoce des menaces de sécurité et la gestion initiale des alertes.
Les connaissances, compétences et aptitudes
• Maîtrise parfaite des systèmes Windows, Linux, Unix ; • Maîtrise de la sécurité des systèmes d'information (SIEM, Firewall, VPN, antivirus, proxy, EDR, XDR, ...) ; • Maîtrise de la gestion de logs ; • Maîtrise de l'analyse des protocoles réseaux ; • Connaissance de la collecte d'informations ; • Connaissance des protocoles et architectures réseaux et connaissance des techniques de corruption et d'intrusion ; • Capacité de surveillance de logs et des alertes de sécurité en temps réel ; • Compétences pour identifier les activités suspectes sur les réseaux et les systèmes ; • Capacité à analyser les alertes et compétence pour établir une priorité de traitement ; • Capacité à analyser les alertes générées par les systèmes de sécurité et à déterminer leur légitimité ; • Capacité de gestion initiale des Incidents ; • Compétence de gestion initiale des incidents et d'escalade appropriée.

3.2.2. Analyste de traitement d'incident

Éducation
Minimum Niveau Bac +5 /ingénieur en technologie des systèmes d'information et des communications.
Formation et expérience
• Formation en opérations de cybersécurité dans un domaine connexe (par exemple opérations de sécurité, sécurité des réseaux, détection et atténuation des menaces, traitement des incidents). • Avoir une expérience minimale de (02) ans.
Principales missions
Résoudre les incidents qui ont été escaladés depuis le niveau 1.
Les connaissances, compétences et aptitudes
• Maîtrise parfaite des systèmes Windows, Linux, Unix ; • Maîtrise de la sécurité des systèmes d'information (SIEM, Firewall, VPN, antivirus, proxy, EDR, XDR, ...) ; • Maîtrise de la gestion de logs ; • Maîtrise de l'analyse des protocoles réseaux ; • Connaissance des protocoles et architectures réseaux et connaissance des techniques de corruption et d'intrusion ; • Connaissance des modes opératoires d'attaque et des codes malveillants ; • Connaissance des vulnérabilités ; • Connaissance en collecte d'informations ; • Compétence en diagnostic des incidents et capacité à analyser et à diagnostiquer des problèmes complexes liés aux systèmes, aux réseaux ou aux applications ; • Compétences analytiques et capacité à analyser les tendances d'incidents pour identifier les causes sous-jacentes et proposer des solutions préventives.

3.2.3. Responsable Opérationnel

Le Prestataire doit disposer d'un responsable opérationnel dont la mission est de réaliser l'analyse détaillée des alertes, communiquer avec les équipes concernées, accompagner dans le traitement des incidents de sécurité, et dans quelques cas, mettre en place des remédiations.

Éducation
Minimum Niveau Bac +5 /ingénieur en technologie des systèmes d'information et des communications.
Formation et expérience
• Formation en opérations de cybersécurité dans un domaine connexe (par exemple opérations de sécurité, sécurité des réseaux, détection et atténuation des menaces, traitement des incidents de sécurité, gestion de crise). • Avoir une expérience minimale de (02) ans.
Principales missions
Assurer le bon fonctionnement des opérations de sécurité.
Compétences techniques
• Maîtrise parfaite des systèmes Windows, Linux, Unix ; • Maîtrise de la sécurité des systèmes d'information (SIEM, Firewall, VPN, antivirus, proxy ; • Connaissance des protocoles et architectures réseau et maîtrise des techniques de corruption et d'intrusion ; • Maîtrise parfaite des attaques sur TCP/IP et l'analyse des protocoles réseaux ; • Maîtrise de la gestion de logs ; • Maîtrise de l'analyse des protocoles réseaux ; • Connaissance des protocoles et architectures réseaux et connaissance des techniques de corruption et d'intrusion ; • Connaissance des modes opératoires d'attaque et des codes malveillants ; • Connaissance des vulnérabilités ; • Connaissance en collecte d'informations ; • Connaissance en réponse aux incidents de sécurité ; • Compétence dans l'optimisation des solutions de sécurité ; • Compétence en gestion des opérations et aptitude à l'élaboration de plans opérationnels ; • Compétence dans l'analyse des menaces et capacité à anticiper leur évolution.

3.2.4. Administrateur Système

Le Prestataire doit disposer d'un administrateur système dont la mission est de maintenir les conditions opérationnelles des dispositifs de l'infrastructure du service et leur niveau de sécurité.

Expériences et formation
Minimum Niveau Bac +5 /ingénieur en technologie des systèmes d'information et des communications.
Formation et expérience
• Formation en opérations de cybersécurité dans un domaine connexe (par exemple opérations de sécurité, sécurité des réseaux, durcissement des réseaux). • Formation spécifique à un produit ou solution. • Avoir une expérience minimale de (02) ans.
Principales missions
Assurer les opérations d'administration du réseau du service de détection (intégration et mise à jour des composants).
Compétences techniques
• Maîtrise parfaite des systèmes Windows, Linux, Unix ; • Maîtrise de la sécurité des systèmes d'information (SIEM, Firewall, VPN, antivirus, proxy) ; • Maîtrise des techniques d'interconnections des réseaux et de leur administration ; • Maîtrise des protocoles et architectures réseaux et maîtrise des techniques de corruption et d'intrusion ; • Maîtrise des environnements techniques de détection et réponse ; • Maîtrise des environnements cloud ; • Connaissance en gestion des incidents de sécurité ; • Connaissances en outils d'automatisation ; • Connaissances des systèmes SCADA ; • Compétence en administration des systèmes ; • Compétence en durcissement des systèmes et déploiement des mesures de sécurité ;

3.3. SERVICE SOC INTERNE

Le Prestataire doit disposer d'un service de détection d'incidents de sécurité de son système d'information.

Le Prestataire doit, sur la base de l'appréciation des risques et de la liste des incidents de sécurité redoutés associée, élaborer une stratégie de collecte, une stratégie d'analyse et une stratégie de notification, dans le cadre du service SOC interne.

Selon le résultat de l'appréciation des risques et la liste des incidents de sécurité redoutés associée, le Prestataire peut procéder à une segmentation du système du service SOC Interne.

Le Prestataire doit déployer une ou plusieurs collecteurs (qualifiés par l'ANCy) sur le système d'information du service de SOC Interne qui permettrait notamment la supervision de chacune des interconnexions du système d'information du service de détection des incidents de sécurité.

Le Prestataire doit élaborer un processus de gestion des incidents de sécurité du service SOC interne.

Le Prestataire doit élaborer un processus de gestion de crise en cas de détection d'un incident de sécurité majeur au sein de son service de SOC interne.

3.4. Les Exigences relatives au Contrat de prestation de services

3.4.1. Exigences générales

Le Contrat de prestation entre le Prestataire et le Client final fait obligatoirement référence à un ensemble d'exigences dont le contenu est listé ci-dessous.

Le Contrat de prestation doit préciser que la prestation réalisée est une prestation qualifiée et doit inclure l'attestation de qualification du Prestataire. Lorsque le Prestataire réalise une prestation non qualifiée, il doit l'indiquer explicitement dans le Contrat de prestation, et sensibiliser le Client final aux risques de ne pas exiger une prestation qualifiée.

Le Contrat de prestation doit être rédigé en français, et indiquer que la loi applicable au contrat est la loi togolaise.

Le Contrat de prestation de services précise les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le Client final et notamment celles liées à son secteur d'activités.

Il définit la durée de conservation des informations liées à la prestation et notamment les évènements collectés et les incidents de sécurité détectés, avec indication le cas échéant, de la distinction de durée de conservation en fonction des types d'information.

3.4.2. Modalités de la prestation

Le contrat de prestation de services doit obligatoirement décrire le périmètre et les objectifs de la prestation, le service de détection des incidents de sécurité et notamment les activités de gestion des évènements, des incidents de sécurité et des notifications.

Il contient en outre les modalités de service, les termes et conditions spécifiques, l'organisation du service, le niveau de qualité de service, la localisation du stockage et du traitement des données, ainsi que celle de l'exploitation et de l'administration du service de détection.

Cet accord prévoit également les obligations, les responsabilités, les délais et coûts, liés à la prestation, et définit les livrables attendus dans le cadre de la prestation, les publics destinataires, leur niveau de sensibilité ou de classification ainsi que les modalités associées. A cet égard, il précise les règles de titularité des livrables concernés, ainsi que les règles de titularité des autres éléments protégés par la propriété intellectuelle tels que les outils et les règles de détection développés spécifiquement par le Prestataire dans le cadre de la prestation le cas échéant.

Le contrat de prestation de services décrit en sus, les méthodes de communication qui seront employées lors de la prestation entre le Prestataire et le Client final, et décrit le processus d'enregistrement et de traitement des réclamations portant sur la prestation déposée par le Client final ou par des tiers, ainsi que la démarche à suivre pour le dépôt de réclamation.

3.4.3. Organisation du service

Le Contrat de prestation de services doit prévoir que le Prestataire désigne un point de contact auprès du Client final en charge d'assurer le suivi opérationnel de la prestation.

Le contrat précise en outre que le Client final et le Prestataire identifient les noms, rôles, responsabilités, ainsi que les droits et besoins d'en connaître des personnes intervenant dans le cadre de la prestation. Il indique également si le Prestataire autorise l'accès distant des administrateurs et des opérateurs du système d'information du service de détection des incidents de sécurité.

Il stipule par ailleurs que le Prestataire pour l'exécution de la prestation, n'a pas recours à des personnels n'ayant pas de relation contractuelle avec lui, n'ayant pas signé son Code d'éthique, ou ayant fait l'objet d'une inscription au bulletin n°3 du casier judiciaire.

3.4.4. Responsabilités et sous-traitance

Le Contrat de prestation doit stipuler que le prestataire ne débute la prestation qu'après approbation formelle et écrite par le commanditaire de la convention de service.

Il doit stipuler que le prestataire informe le Client final en cas de manquement au Contrat de prestation, et indiquer que le Prestataire informe le Client final en cas d'incident de sécurité détecté sur le système d'information du service de détection des incidents de sécurité. Il précise expressément à cet égard, le délai maximal autorisé pour transmettre ladite information suite à un incident de sécurité.

Le Contrat de prestation doit prévoir que le prestataire ne réalise que des actions strictement en adéquation avec les objectifs de la prestation.

Il doit indiquer si le Client final dispose de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.) ou s'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.

Le Contrat de prestation définit les responsabilités et les précautions à respecter par l'ensemble des parties concernant les risques potentiels liés à la prestation, notamment en matière de confidentialité des informations collectées et analysées ainsi qu'en matière de disponibilité et d'intégrité du système d'information du Client final.

Le Contrat de prestation doit préciser si le Prestataire peut en cas de nécessité, sous-traiter tout ou partie de la prestation à un autre prestataire de services.

En cas de sous-traitance à un Prestataire de services de confiance en cybersécurité qualifié par l'ANCy, le Prestataire devra veiller au respect des conditions ci-dessous :

- Le Prestataire de services de confiance en cybersécurité qualifié par l'ANCy sous-traitant se conforme aux exigences du référentiel qui lui sont applicables ;
- Le Prestataire de détection des incidents de sécurité qui sous-traite la prestation notifie le projet d'accord de sous-traitance à l'ANCy dans un délai raisonnable avant la signature envisagée du contrat avec le sous-traitant.
- Le Client final a formellement donné son accord par écrit pour le recours à la sous-traitance ;
- Il existe un contrat de prestation de services entre le Prestataire et le sous-traitant ;

En cas de sous-traitance avec un prestataire ne bénéficiant pas d'une qualification délivrée par l'ANCy, le Prestataire devra veiller au respect des conditions ci-dessous :

- Le Prestataire soumet le projet d'accord de sous-traitance à l'accord préalable de l'ANCy. Le projet devra être envoyé à l'ANCy dans un délai minimum de deux (02) mois avant la signature envisagée du contrat avec le sous-traitant ;
- Le recours à la sous-traitance est validé par le Client final ;
- Il existe une convention ou un cadre contractuel documenté entre le Prestataire et le sous-traitant avant le début de l'exécution de sa mission par le sous-traitant.

3.4.5. Confidentialité et protection de l'information

Le contrat de prestation de services doit obligatoirement décrire le périmètre et les objectifs de la prestation, le service de détection des incidents de sécurité et notamment les activités.

Le Contrat de prestation doit identifier le niveau de sensibilité ou de classification du service de détection des incidents de sécurité mis en œuvre par le Prestataire et identifier le niveau de sensibilité ou de classification du périmètre supervisé.

Il stipule en outre que le Prestataire ne collecte et n'analyse que les informations strictement nécessaires au bon déroulement de la prestation. A cet égard, le Contrat de prestation précise les modalités d'accès, de stockage, de transport, de reproduction, de destruction et de restitution des informations collectées et analysées par le Prestataire. Il indique en outre que le prestataire ne divulgue aucune information relative à la prestation à des tiers, sauf autorisation formelle et écrite du Client final.

Le Contrat de prestation précise par ailleurs les clauses relatives à l'éthique du Prestataire, et inclut le Code d'éthique de ce dernier.

3.4.6. Niveau de service

Le Contrat de prestation définit les indicateurs opérationnels et stratégiques permettant de mesurer le niveau de service de la prestation.

Il définit les plages horaires opérationnelles du service de détection des incidents de sécurité, et stipule que le prestataire organise en présence du Client final, des comités opérationnels et stratégiques. A cet égard, il fournit des détails sur les objectifs de ces comités et leur fréquence.

Le Contrat de prestation identifie, pour le Prestataire et le Client final, la charge des ressources humaines consacrée à la gestion des règles de détection et notamment à leur création ou leur modification.

Il définit en outre la fréquence à laquelle le Prestataire transmet au Client final le bulletin d'état des règles de détection.

Il indique que le prestataire met à disposition du Client final un service d'assistance et les plages horaires opérationnelles de ce service d'assistance, et précise 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.

3.5. Les Exigences relatives a la protection de l'information du service

3.5.1. Étendue géographique du service

Le Prestataire doit exploiter et administrer le service de détection des incidents de sécurité exclusivement depuis le territoire togolais.

Le Prestataire doit héberger et traiter les données relatives au service de détection des incidents de sécurité exclusivement au sein du territoire togolais.

Dans le cas où certaines sources de collecte seraient situées en dehors du Togo, les évènements issus de ces sources devront être transmis au collecteur central situé au Togo. Cependant, l'Agence Nationale de la Cybersécurité (ANCy) peut accorder une dérogation à cette obligation d'hébergement, sous réserve que le prestataire concerné fournisse une justification crédible et documentée de son incapacité à satisfaire cette exigence. La demande de dérogation sera soumise à une évaluation rigoureuse avant approbation.

3.5.2. Sécurité physique

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

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

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

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 respectant les mécanismes d'authentification.

3.5.3. Contrôles

Le Prestataire doit documenter et mettre en place un plan de contrôle définissant le champ d'application et la fréquence des contrôles, en conformité avec la gestion du changement, les politiques, et les résultats de l'évaluation des risques. Ce plan vise à assurer la mise en œuvre adéquate des mécanismes de sécurité et de protection de l'information dont le Prestataire est responsable, incluant les accès logiques et physiques aux dispositifs du service de détection, ainsi que la revue des privilèges et des droits d'accès aux dispositifs.

Ce plan doit être révisé en cas de modifications structurantes du service de détection (son hébergement, son infrastructure et son architecture), ou au minimum annuellement.

Les conclusions des contrôles doivent être validées formellement et par écrit auprès de l'organe de direction du Prestataire.

3.5.4. Sauvegardes

Le Prestataire doit documenter et mettre en place un plan de sauvegarde et de restauration des dispositifs du service de détection des incidents de sécurité, et couvrir notamment les sauvegardes des systèmes, des configurations, et des données.

Ce plan doit être testé au minimum annuellement.

Le dispositif de sauvegarde et de restauration doit être hébergé dans un segment du système du service, et précisément dans le segment d'administration, en application du plan de sauvegarde préétabli.

3.5.5. Segmentation du Système d'Information du Service

Le système d'information du service de détection doit être organisé en segments séparés à l'aide de mécanismes de filtrage, d'authentification et de contrôle d'accès. Le Prestataire doit mettre en œuvre les mesures nécessaires pour cette séparation.

Le Prestataire peut se référer à la norme ISO27001 et à la Norme NIST SP 800-53 concernant les recommandations et les règles de filtrage à mettre en place.

Le Prestataire peut disposer de plusieurs segments réseaux.

Le Prestataire doit prendre également des mesures de segmentation des différents systèmes des Client finaux à savoir : les systèmes de stockage et de traitement des évènements et des informations contextuelles associées, les systèmes de stockage et de traitement des incidents de sécurité, les outils techniques d'analyse, les outils de gestion des tickets d'incident, les notifications, et le système de messagerie. Cette séparation peut être mise en place en utilisant au moins des mécanismes de type contrôle d'accès logique.

Le Prestataire doit élaborer et maintenir à jour une description approfondie de l'architecture du système d'information du service de détection des incidents de sécurité permettant d'identifier tous les dispositifs du système d'information ainsi que les segments de confiance du service de détection. Ces segments de confiance sont conçus pour protéger les informations sensibles ou critiques contre les accès non autorisés. Le Prestataire doit élaborer et mettre à jour une matrice des flux de références du système de détection des incidents de sécurité, ainsi que la politique de filtrage qui lui est associée. Cette politique doit autoriser uniquement les flux strictement nécessaires au bon fonctionnement du service.

Le Prestataire doit déployer des solutions de chiffrement et d'authentification entre les segments de confiance lorsque les informations échangées entre ces segments circulent à travers des réseaux de communication non spécifiquement dédiés au service de détection.

La segmentation du système d'information du service de détection peut être répartie par activités du service de détection des incidents de sécurité et activités liées à sa gestion.

3.5.6. Segmentation liée à la gestion des évènements

3.5.6.1. Segment de collecte

Ce segment regroupe tous les dispositifs participant au processus de collecte, notamment les dispositifs de centralisation des évènements générés par les sources de collecte (collecteurs centraux) ainsi que les systèmes de stockage des évènements.

3.5.6.2. Compartiment de collecte

Cette zone se trouve dans le système d'information du Client final et permet d'assurer la réception et le stockage sécurisé des événements de sécurité en provenance des sources de collecte déployées sur le périmètre supervisé du Client final.

Les dispositifs impliqués dans la chaîne de supervision doivent être reliés par un lien réseau physiquement dédié.

Le Client final doit avoir la responsabilité de l'administration du dispositif de filtrage entre le compartiment et son système d'information.

Le Prestataire doit avoir la responsabilité de l'administration et de l'exploitation de l'ensemble des autres dispositifs hébergés dans le compartiment de collecte.

Le Prestataire doit déployer un dispositif de filtrage entre ce compartiment et le système d'information du service de détection.

Le Prestataire doit s'assurer que le dispositif de filtrage entre ce compartiment et le système d'information interne du Client final interdit tous les flux, excepté ceux initiés depuis le périmètre supervisé vers ce segment, et permettant aux sources de collecte hébergées sur le périmètre supervisé de transmettre les évènements de cette zone à destination d'un collecteur.

3.5.7. Segmentation liée à la gestion des incidents de sécurité :

3.5.7.1. Le segment d'analyse

Ce segment regroupe tous les dispositifs participant au processus d'analyse, y compris les outils d'analyse (SIEM, antivirus, sandbox, etc.), dédiés à l'analyse des incidents de sécurité. La corrélation et l'analyse des évènements collectés sont réalisées au sein de ce segment.

3.5.8. Segmentation liée à la gestion des notifications

3.5.8.1. Segment de notification

Ce segment regroupe l'ensemble des dispositifs participant au processus de notification, qui permet d'élaborer et d'envoyer des notifications au Client final lors de la détection d'un incident de sécurité.

Le Prestataire doit dédier des systèmes de messageries aux activités de notifications, dans le cas où le processus de gestion des notifications utilise l'e-mail comme moyen de notification.

Le Prestataire doit s'assurer que le dispositif de filtrage à l'interface entre le système d'information du service de détection et l'extérieur, en direction du segment de notification n'autorise que les flux émis depuis le segment de notification.

3.5.8.2. Segment de reporting

Ce segment regroupe l'ensemble des dispositifs permettant au Client final de consulter le détail des informations remontées par les analyses effectuées sur les incidents de sécurité détectés (rapports, preuves techniques, etc.) et le cas échéant, de fournir les informations supplémentaires pour pouvoir qualifier l'incident.

Le Prestataire doit mettre à disposition du Client final dans le segment de *reporting*, un portail de *ticketing* lui permettant de consulter et mettre à jour le statut des incidents de sécurité et des recommandations, ainsi qu'un dispositif de stockage.

Le Prestataire doit fournir un annuaire destiné à l'authentification du Client final sur les dispositifs hébergés dans le segment de *reporting*.

Le Prestataire doit authentifier le Client final à l'aide de comptes nominatifs, en prévoyant que l'accès à une machine se fasse à l'aide d'une méthode d'authentification à plusieurs facteurs, et une authentification mutuelle pour l'authentification de machine à machine.

Le Prestataire doit maintenir une liste actualisée des comptes autorisés à accéder au segment de *reporting*, en y incluant leurs privilèges respectifs.

Le Prestataire doit s'assurer que le dispositif de filtrage déployé entre le segment de reporting et le système d'information du Client final ne doit autoriser que les flux émis depuis le compartiment de consultation, les flux émis depuis les postes nomades de consultation, et ceux permettant au Prestataire d'administrer depuis le segment d'administration.

3.5.8.3. Compartiment de consultation

Ce compartiment se trouve dans le système d'information du Client final et permet de fournir aux équipes du Prestataire un accès distant et sécurisé à des informations contextuelles utiles à la qualification des incidents de sécurité détectés sur le périmètre supervisé du Client final.

Le Prestataire doit déployer un dispositif de filtrage entre cette enclave et le système d'information du service de détection des incidents de sécurité et le système d'information du Client final.

Le Prestataire doit s'assurer que le dispositif de filtrage entre ce compartiment et le système d'information interne du Client final interdit tous les flux, excepté ceux initiés depuis le compartiment de consultation vers le système d'information interne du Client final.

3.5.9. Segmentation liée aux activités de gestion du Service

3.5.9.1. Segment d'administration

Ce segment regroupe l'ensemble des dispositifs et des outils d'administration, ainsi que les postes d'administration impliqués dans le processus d'administration du service.

3.5.9.2. Segment d'exploitation

Ce segment regroupe les postes de travail de l'équipe du service.

3.5.9.3. Segment de mise à jour

Ce segment regroupe l'ensemble des dispositifs impliqués dans le processus de téléchargement des mises à jour des dispositifs du service de détection.

3.5.9.4. Segments d'échanges

Ces segments regroupent l'ensemble des dispositifs permettant le transfert de fichiers avec l'extérieur du système d'information du service de détection des incidents de sécurité, que ce soit pour les administrateurs ou pour l'équipe du service.

3.5.9.5. Autres segments

a. Segment Internet

Ce segment concerne la partie externe au système d'information du service, communiquant avec l'extérieur via Internet. Il regroupe l'ensemble des postes mis à disposition des administrateurs et de l'équipe du service pour accéder à Internet ou à d'autres systèmes d'information.

b. Passerelles dédiées

Ces passerelles permettraient un accès distant de manière nomade au système d'information du service de détection des incidents de sécurité, pour certains membres de l'équipe du service dans la mesure où c'est nécessaire à la continuité du service.

Pour ces segments, le Prestataire peut :

- Les isoler physiquement ;

- Mettre en place des contrôles d'accès basés sur des règles ;
- Appliquer les règles de filtrage adéquat ;
- Procéder à un chiffrement des communications ;
- Sécuriser les points d'entrée.

3.5.10. Protection du lien d'interconnexion entre le Prestataire et le Client final

Le Prestataire doit limiter l'autorisation d'interconnexion uniquement :

- Au système d'information du Client final ;
- Aux postes d'administration et d'exploitation des passerelles dédiées ;
- Aux serveurs de mise à jour pour télécharger les mises à jour des dispositifs du service de détection des incidents de sécurité via le segment de mise à jour ;
- Au segment Internet permettant l'échange de fichiers avec l'extérieur du système d'information.

Le Prestataire doit appliquer un filtrage à toutes les interconnexions du système d'information du service de détection à l'aide de solutions de filtrage qualifiées par l'ANCy.

Les flux relatifs aux interconnexions avec le service de détection des incidents de sécurité doivent être chiffrés à l'aide de solutions de chiffrement et d'authentification qualifiées par l'ANCy.

Le Prestataire doit mettre en place un lien d'interconnexion sécurisé basé sur :

- Un tunnel VPN permanent (Site à Site) entre le réseau du Prestataire et le réseau du Client final. A travers le VPN :
  - Le Prestataire ne doit être en mesure d'accéder à aucun système en dehors du système de collecte ;
  - Le Client final ne doit être en mesure d'accéder à aucun système en dehors du système de gestion des tickets d'incidents de sécurité et aux interfaces fournies par le prestataire.
- Une restriction par IP des deux côtés en l'absence d'un tunnel VPN ;
- Un système d'authentification robuste ;
- Un système de journalisation des accès.

4.EXIGENCES RELATIVES AUX ACTIVITES DU SERVICE DE DETECTION DES INCIDENTS

4.1. DETECTION DES INCIDENTS

C'est l'ensemble des moyens techniques et organisationnels visant à détecter et évaluer un incident de sécurité à partir d'événements recueillis, ainsi que le stockage et l'archivage des incidents dans le but d'améliorer le processus de détection.

4.1.1. Incidents redoutés

Le Prestataire doit dresser avec le Client final une liste des incidents de sécurité redoutés et leurs impacts, en se basant sur les résultats de l'appréciation des risques précédemment élaborée par le Client final. Cette liste doit être régulièrement mise à jour en cas de modifications.

Il est nécessaire que cette liste intègre au moins les types d'incidents de sécurité suivants :

- Exploitation d'une vulnérabilité ;
- Élévation de privilèges ;
- Exfiltration de données ;
- Propagation virale ;
- Utilisation d'un mécanisme de persistance ;
- Déni de service ;
- Accès non autorisé à une ressource ;
- Usurpation d'identité ;
- Actions non conformes à la politique de sécurité du Client final.

Il doit établir une échelle de gravité associée aux incidents de sécurité redoutés, en prenant en compte l'appréciation des risques, et notamment les menaces, les actifs, les impacts potentiels et leur niveau de gravité. Le Prestataire peut à cet égard se référer à l'annexe C de la norme [ISO27035].

4.1.2. Stratégie d'analyse

Le Prestataire doit développer et mettre en place une stratégie d'analyse permettant de détecter tous les incidents de sécurité répertoriés dans la liste des incidents redoutés. Cette stratégie d'analyse doit être revue lors des comités opérationnels et doit faire référence aux règles de classification des incidents de sécurité et à la mise en œuvre de ces règles.

La stratégie d'analyse doit prévoir, entre autres, les mises à jour des règles de détection (création ou modification).

4.1.3. Règles de détection

Le Prestataire doit créer des règles de détection en s'appuyant sur la liste des incidents redoutés, des bases de connaissances internes issues de son expertise, des bases de connaissances des éditeurs, les éléments de contexte spécifiques du Client final, les incidents de sécurité détectés auprès des éventuels autres Clients finaux, ainsi que les éléments issus des autres activités que le Prestataire peut assurer, comme l'activité de veille sur les menaces.

Ces règles doivent être soumises à une politique de marquage qui définit pour chaque règle de détection, son propriétaire, son auteur, sa source.

Le Prestataire doit dans le cadre de la prestation, élaborer et maintenir pour chaque Client final, une liste complète des règles de détection mises en place ou ayant été utilisées. Cette liste doit permettre de retracer l'historique des règles de détection, facilitant l'identification des règles actives à un moment précis ou sur une période donnée.

Le Prestataire doit, au minimum une fois par mois, fournir au Client final un bulletin d'état des règles de détection mis à jour.

Le Prestataire doit intégrer toutes les règles de détection répertoriées dans la liste des règles de détection identifiées au sein des outils techniques d'analyse, notamment ceux associés aux vulnérabilités identifiées à l'occasion d'éventuelles activités de tests d'intrusion réalisées par le Client final sur son système d'information.

Le Prestataire doit créer des bases de connaissances sur les vulnérabilités décelées lors des activités de tests d'intrusion réalisées par le Client final pour améliorer le diagnostic.

Le Prestataire doit, de manière autonome, intégrer de nouvelles règles de détection dans les outils techniques d'analyse, et mettre à jour l'ensemble des documents correspondants. En cas de difficulté d'implémentation, le Prestataire doit avertir le Client final dans les meilleurs délais, et détailler les raisons de l'échec d'implémentation.

Lorsqu'une règle est modifiée, le Prestataire procède à une analyse a posteriori, qui consiste en une analyse de l'ensemble des évènements stockés.

4.1.4. Incidents de sécurité détectés

Le Prestataire doit qualifier les incidents de sécurité détectés en vue d'apprécier leur véracité (vrai positif/faux positif), leur niveau de gravité et leurs impacts.

Lors des recherches d'informations à l'occasion de la qualification d'un incident, le Prestataire doit privilégier des bases d'informations internes issues de sources ouvertes, afin de limiter au maximum les recherches sur internet.

Si la recherche est effectuée à l'aide de l'outil internet, le Prestataire doit définir une méthodologie pour la recherche en sources ouvertes, et tenir compte de la politique de marquage des règles de détection, et notamment si celles-ci indiquent ou non la possibilité d'effectuer une telle recherche. Cette méthodologie doit spécifier les types d'informations susceptibles d'être recherchés (tels que des noms de fichiers ou de codes malveillants, des noms de domaines et des adresses IP, des CVEs) ainsi que les modalités qui y sont associées.

Le Prestataire doit générer un ticket pour chaque incident de sécurité détecté et le mettre à disposition du Client final. Le format de ce ticket doit être défini avec le Client final, et doit comprendre au minimum les éléments suivants :

- la date de création du ticket et des différentes opérations réalisées sur celui-ci (traçabilité des actions) ;
- la date et l'heure de la détection de l'incident de sécurité ;
- la date effective de l'évènement ayant donné lieu à l'incident de sécurité ;
- la description de l'incident de sécurité ;
- le niveau de classification de l'incident de sécurité par rapport à la norme de L'ISO 27035 ;
- la gravité de l'incident de sécurité ;
- la description de l'impact de l'incident de sécurité ;
- les identifiants et numéros de version des règles de détection déclenchées ;
- les équipements ayant généré et collecté les évènements de l'incident de sécurité ;
- les identifiants des évènements ayant permis la détection de l'incident de sécurité ;
- le risque induit par l'incident de sécurité.

Le Prestataire doit disposer d'un outil de gestion des tickets d'incident de sécurité.

4.1.5. Réponse de premier niveau

C'est l'ensemble des moyens techniques et organisationnels permettant de traiter les alertes et d'escalader les incidents avérés dits de premier niveau.

Le Prestataire doit être capable de traiter les alertes et d'escalader les incidents avérés dits de premier niveau permettant de vérifier la pertinence des alertes remontées par les systèmes de détection, afin de faire un triage et détecter les incidents à travers notamment la liste des incidents redoutés.

Les incidents sont classés dans la liste des incidents redoutés selon leur sévérité, et sont ensuite traités selon le niveau accordé :

- Les incidents de sécurité mineurs du premier niveau ainsi que les incidents moyens du deuxième niveau, doivent être traités par le Prestataire en coordination avec le Client final.
- Les incidents de sécurité graves de troisième niveau, devront faire l'objet d'une escalade vers une équipe de réponse aux incidents qualifiés pour assurer cette prestation.

Si le Prestataire est qualifié pour la réponse aux incidents de sécurité, il peut assurer ces activités. Dans l'hypothèse contraire, le Client final devra faire appel à un autre Prestataire qualifié pour faire la réponse aux incidents.

Le Prestataire doit être en mesure de rechercher à minima les indicateurs de compromission suivants :

- Empreinte des fichiers (SHA1, SHA256), empreinte du nom, chemin d'accès, taille, extension ;
- Adresses IP publiques ;
- Noms de domaines ;
- URL ;
- *user-agent* ;
- champs d'e-mails : domaine source, domaine destination, empreinte du sujet, horodate ;
- champs de certificats X509 : empreinte, émetteur, date de validité, sujet, extensions, nom d'hôte, horodate.

Lors de la confirmation de l'incident, le Prestataire doit disposer d'un ensemble de procédures pour le traitement des incidents :

❖ Procédure d'évaluation d'incident de sécurité

- **Classification préliminaire** : Évaluer la gravité apparente de l'incident en fonction de son impact initial sur les opérations et la sécurité.
- **Attribution d'une priorité** : Assigner une priorité à l'incident en fonction de sa criticité, de son impact potentiel et des risques associés.
- **Élaboration d'une équipe de réponse** : Constituer une équipe pour gérer et répondre à l'incident en fonction de ses caractéristiques.

❖ Procédure de classification d'incident de sécurité

- **Analyse approfondie** : Examiner en détail les caractéristiques de l'incident pour comprendre sa nature, son origine et son impact potentiel ;
- **Évaluation de l'impact** : Déterminer les conséquences réelles ou potentielles de l'incident sur l'organisation, les données, les systèmes ou les utilisateurs ;
- **Catégorisation** : Classer l'incident en fonction de son type (exemple : violation de données, attaque de *malware*, tentative d'accès non autorisé, etc.) ;
- **Attribution d'un niveau de gravité** : Assigner un niveau de gravité à l'incident en se basant sur des critères prédéfinis pour déterminer son importance et son urgence.

❖ Procédure d'escalade

- **Identification du besoin d'escalade** : Déterminer si l'incident dépasse les capacités ou les compétences de l'équipe de réponse initiale ;
- **Notification de l'escalade** : Communiquer de manière formelle et précise aux niveaux supérieurs ou aux personnes concernées, l'escalade de l'incident ;
- **Transfert des responsabilités** : Passer la responsabilité de la gestion de l'incident à une équipe ou à des individus disposant des ressources ou des compétences nécessaires pour gérer l'incident de manière efficace.

❖ Manuel de traitement

- **Documentation détaillée** : Fournir des instructions détaillées étape par étape, pour gérer spécifiquement chaque type d'incident ;
- **Scénarios de réponse** : Inclure des scénarios typiques avec des recommandations sur les actions à entreprendre, les outils à utiliser et les contacts à impliquer ;
- **Validation et mise à jour** : Tester régulièrement les manuels pour s'assurer de leur efficacité et les mettre à jour en fonction des nouvelles menaces ou des changements dans l'environnement technologique.

4.2. GESTION DES EVENEMENTS

C'est l'ensemble des moyens techniques et organisationnels assurant la collecte et l'enregistrement des événements liés à la sécurité.

4.2.1. Stratégie de collecte

Le Prestataire doit développer et mettre en place avec la collaboration du Client final, une stratégie de collecte basée sur la liste des incidents de sécurité redoutés. Cette stratégie doit être revue lors des comités opérationnels.

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

Le Prestataire est tenu de fournir des conseils au Client final tout au long du processus d'élaboration, d'application et de révision de la stratégie de collecte. Cela comprend la revue de la politique de journalisation ainsi que le déploiement de dispositifs de journalisation dans le segment supervisé.

4.2.2. Sources de collecte

Le Prestataire doit déterminer exactement les composants des systèmes d'information qui entrent dans le périmètre de surveillance et s'assurer que les événements pertinents sont bien remontés dans les logs.

Le Prestataire doit être au minimum capable de collecter les évènements en provenance des sources de collecte suivantes, sans s'y limiter :

- *Firewall* pour la vision des accès aux différents segments du SI ;
- Passerelles VPN pour la surveillance des accès distants ;
- IDS et WAF qui remontent les alertes de sécurité réseau ;
- *Sandbox* utilisée dans la protection des accès *Web* et de la messagerie pour les alertes de sécurité d'intrusion et de malwares ;
- *Proxy* pour la surveillance des accès aux sites identifiés malveillants et pour surveiller les exfiltrations ;
- Antivirus sur la détection des *malwares* connus et leur propagation ;
- Messagerie pour la surveillance des exfiltrations ;
- *Active Directory* qui est la cible de la majorité des attaques ;
- Annuaire LDAP et équipements d'authentification pour avoir une référence comportementale des utilisateurs ;
- Serveurs DNS pour identifier les attaques de type « *Tunneling* DNS ».

Le Prestataire doit utiliser le collecteur déployé dans le service SOC interne comme une source de collecte pour le service de détection du service.

Le Prestataire doit recommander au Client final le choix de collecteurs qualifiés par l'ANCy.

Les évènements en provenance de sources de collecte doivent être centralisés sur au moins un collecteur situé dans le compartiment de collecte. Ce collecteur doit permettre de réaliser un premier filtrage des évènements afin de ne transmettre au segment de collecte et aux outils d'analyse, que les évènements utiles au service de détection et identifiés dans la stratégie de collecte.

Le Prestataire doit de manière autonome faire évoluer sa capacité de collecte en lien avec la liste des incidents redoutés, et mettre à jour l'ensemble des documents correspondants. En cas de difficulté de mise en œuvre, le Prestataire doit avertir le Client final dans les meilleurs délais, et détailler les raisons de l'échec d'implémentation.

Le Prestataire doit dans le cadre de la prestation et pour chaque Client final, élaborer et maintenir une liste complète des règles de filtrage mises en œuvre ou ayant été mises en œuvre. Cette liste doit permettre de retracer l'historique des règles de filtrage, facilitant l'identification des règles actives à un moment précis ou sur une période donnée.

Le Prestataire doit au minimum une fois par mois, fournir au Client final un bulletin d'état des règles de filtrage mis à jour.

Afin de pouvoir localiser et fournir tout évènement collecté sur demande du Client final, le Prestataire doit à l'aide d'une indexation, disposer d'une vision centralisée de l'ensemble des évènements collectés, notamment en associant à chaque évènement le collecteur dont il est issu.

Le Prestataire doit instaurer un processus de gestion de la capacité de traitement et de stockage des événements, permettant de surveiller son développement et d'ajuster cette capacité en conséquence, pour garantir la conservation des données pendant une période d'au moins six mois.

4.3. GESTION DES NOTIFICATIONS

C'est l'ensemble des moyens techniques et organisationnels permettant de communiquer au Client final, l'état des incidents de sécurité détectés ainsi que le stockage de ces incidents.

4.3.1. Stratégie de notification

Le Prestataire doit développer et mettre en place avec la collaboration du Client final, une stratégie de notification permettant de notifier le Client final lors de la détection d'un incident de sécurité. Cette stratégie doit être revue lors des comités opérationnels.

La stratégie de notification doit identifier la liste d'incidents redoutés ainsi que les personnes à contacter en fonction de l'incident de sécurité et de son niveau de gravité.

Le Prestataire est tenu de fournir des conseils au Client final tout au long du processus d'élaboration, d'application et de révision de la stratégie de notification, notamment sur les personnes à avertir et les méthodes de notification.

4.3.2. Modalités liées aux notifications

Les notifications ne doivent pas inclure des informations sur l'incident. Ils sont référencés à l'aide du numéro du ticket d'incident.

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

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

Le Prestataire doit mettre en place et tenir à jour un journal de notifications référençant toutes les notifications effectuées pour le Client final mentionnant toutes les informations liées à la notification.

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.

Le Prestataire doit mettre à disposition du Client final :

- Un portail de *ticketing* lui permettant de visualiser et mettre à jour l'état des incidents de sécurité et des actions engagées ;
- un dispositif de stockage permettant au Client final de : récupérer le contexte des incidents de sécurité le concernant, et disposer le cas échéant, des informations contextuelles nécessaires à l'équipe du service pour la qualification d'un incident.

4.3.3. Les canaux et moyens de notifications

Le Prestataire doit disposer de deux canaux d'information à destination du Client final :

- Un canal pour la notification ;
- Un canal sécurisé, notamment pour l'échange d'informations détaillées ;
- Le Prestataire doit disposer au minimum de deux moyens de notification à savoir un numéro téléphonique et une adresse électronique.