République Islamique de Mauritanie

Honneur – Fraternité – Justice

Ministère de la Transformation Numérique et de la Modernisation de l'Administration (MTNMA)

Transformation Numérique pour l'Afrique / Programme Régional d'Intégration Numérique en Afrique de l'Ouest
(WARDIP – Composante Mauritanie)
Unité de Gestion du Projet WARDIP-Mauritanie

Cahier des Charges pour la mise en place de l'équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et du centre d'opérations de cybersécurité (SOC) pour le Réseau Intranet de l'Administration à haut Débit (RIAD)

(Mise en place du CSIRT national et du SOC RIAD)

Avril 2025

Table des matières

Contexte & Objectifs

Rappel du contexte

Le Gouvernement de la République Islamique de Mauritanie, avec l'appui de la Banque Mondiale, a intégré le Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP) pour promouvoir la mise en œuvre de la stratégie de transformation numérique du Pays qui vise à développer la pénétration de l'Internet haut débit, des services financiers numériques et des services en ligne (e-Gouvernement).
Le Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP) – Composante Mauritanie, (ci-après le « **Projet** ») à travers des actions impliquant les pays de la sous-région, vise spécifiquement à :

a) créer un environnement propice au bon développement d'infrastructures numériques adéquates grâce à l'adaptation du cadre juridique et institutionnel du secteur du numérique et son harmonisation en particulier pour la connectivité et les données,
b) développer les réseaux à large bande et les services d'internet et de transit à travers le déploiement de réseaux backbones en fibre optique interconnectés au niveau régional,
c) simplifier l'accès aux services ligne tel que le e-commerce ainsi que les services publics par le développement d'un environnement favorable et la mise en place de plateformes e-Gouvernement dans une approche de mutualisation et de coordination régionale,
d) développer les compétences dans le domaine du numérique.

La composante Mauritanienne du Programme Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP – Mauritanie) vise à élargir l'accès aux services haut débit et numériques grâce au développement et à l'intégration des marchés numériques du pays avec ceux de la région de l'Afrique de l'Ouest. Le projet est axé sur 3 éléments essentiels à l'intégration des technologies numériques au niveau régional : le marché de la connectivité, le marché des données et le marché en ligne. Il s'agira ainsi de (i) poursuivre les efforts entamés dans le cadre du Projet WARCIP-Mauritanie pour étendre la connectivité, diminuer le coût et améliorer la qualité de service, (ii) permettre l'échange, le stockage et le traitement sécurisés des données au-delà des frontières, et soutenir le déploiement régional et l'accès aux services et à l'innovation basés sur les données ; et (iii) développer l'accès et la fourniture des services en ligne publics et privés, et établir un commerce électronique transparent et sécurisé au niveau régional.

Pour atteindre ces objectifs, le Projet est structuré autour des composantes suivantes :

- **Composante-1 « Développement et intégration du marché de la connectivité »** qui soutiendra les réformes visant à réduire les obstacles à la fourniture de services de télécommunications transfrontaliers par le biais de marchés ouverts ainsi que le déploiement de l'infrastructure de connectivité à large bande dans le cadre d'une approche MFD (Maximisation des Financements pour l'Investissement).

- **Composante 2 « Développement et intégration du marché des données »** qui vise à permettre l'échange, le stockage et le traitement sécurisés des données à travers les frontières

pour soutenir le déploiement régional et l'accès aux services, à l'innovation et à l'infrastructure axés sur les données, la réduction des restrictions régionales sur la libre circulation des données et l'augmentation des investissements dans l'infrastructure de données. Il est donc essentiel d'améliorer l'environnement juridique et réglementaire de la cybersécurité, ainsi que la protection des données et de la vie privée. Il est donc essentiel d'améliorer l'environnement juridique et réglementaire de la cybersécurité, ainsi que la protection des données et de la vie privée. Un marché des données plus intégré en Afrique de l'Ouest pourrait stimuler l'innovation et améliorer l'analyse des données, ce qui se traduirait par des avantages économiques et sociaux importants et des gains d'efficacité dans pratiquement tous les secteurs. La création d'un marché des données plus vaste générerait également des réductions de coûts substantielles en créant des économies d'échelle qui rendraient les investissements dans les centres de données régionaux qui prennent en charge les services en ligne, y compris l'hébergement en nuage, plus viables financièrement. Conformément aux objectifs régionaux, cette composante pourrait éventuellement inclure un soutien aux objectifs nationaux qui seraient essentiels pour favoriser l'intégration.

  - **La sous-composante 2.1 : Création d'un environnement propice au développement et à l'intégration du marché des données** cible principalement à développer une règlementation des données et un cadre d'interopérabilité qui soient conformes aux dispositions régionales et internationales. La sous composante cible également à renforcer les aspects de cybersécurité et la protection des données à travers des activités d'appui pour le renforcement des compétences et des structures en charge de ces aspects.

  - **La sous-composante 2.2: Soutien du marché des données** sera consacrée au financement des infrastructures essentielles et des plateformes, pour le développement du marché des données (identifiées dans la sous-composante 2.1), et l'acquisition des équipements techniques.

- **Composante 3 « Développement et intégration du marché en ligne »** qui vise à soutenir le développement et l'intégration du marché en ligne, ce qui créera un environnement propice à la fourniture et à l'accès transfrontaliers de biens ou de services numériques. Cette composante aiderait les gouvernements, les entreprises et les citoyens des pays participants à accéder et à fournir des services privés et publics en ligne, ainsi qu'à effectuer des achats en ligne de manière transparente depuis n'importe où dans la région.

- **Composante 4 : « Gestion de projet ».** Cette composante financera diverses activités liées aux aspects environnementaux et sociaux, et fiduciaires, au renforcement des capacités et le soutien à la mise en œuvre du Projet. Elle vise à fournir une assistance technique et un renforcement des capacités pour la préparation et la mise en œuvre du programme.

- **Composante 5 : « Composante d'intervention d'urgence contingente CERC ».** Dans le contexte de la crise du COVID-19, une composante d'intervention d'urgence contingente (CERC) est ajoutée à la structure du projet pour fournir un soutien aux pays participants pour répondre aux urgences, y compris la crise du COVID-19. Elle aura une valeur initiale nulle mais pourra être financée pendant la mise en œuvre du projet pour permettre une réponse agile aux événements émergents, avec des fonds redirigés depuis d'autres composantes.

Le Projet est sous la tutelle du Ministère de la Transformation Numérique et de la Modernisation de l'Administration (MTNMA). Il est mis en œuvre par son Unité de Gestion de Projet (UGP).

Dans le cadre de la composante 2 « Développement et intégration du marché des données », le Projet cherche à recruter un Consultant (firme) qui assistera le Gouvernement de la République Islamique de Mauritanie (RIM) pour réaliser **la mise en place de l'équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et du centre d'opérations de cybersécurité (SOC) pour le Réseau Intranet de l'Administration à haut Débit (RIAD)** (en abrégé « **Mise en place du CSIRT national et du SOC RIAD** »). Il s'agira de prendre en charge l'aménagement, l'intégration ainsi que la mise en production technique et organisationnelle du CSIRT et du SOC. L'approche doit permettre une mise en service rapide des activités attendues avec l'appui du consultant (prestataire spécialisé), et une montée en compétence progressive des équipes internes pour atteindre une autonomie sous un délais de 3 ans.

Dans la suite de ce document, la terminologie ci-dessous pourraient être utilisée :

- MTNMA sera référé au « **Ministère** » ou « **maitre d'ouvrage** ». Il s'agit notamment de la Direction de l'Administration des Systèmes et de la Sécurité (DASS) du MTNMA.
- Le CSIRT et le SOC sera référé à « **CSIRT/SOC** » ou « **RIMCERT** », sauf mention explicite pour désigner individuellement le CSIRT ou le SOC.

Objectifs du projet

Le projet a pour objectif de couvrir les prestations réparties dans les 3 lots suivants :

- **Lot 1 - Mise en place de l'espace physique du CSIRT/SOC**
- **Lot 2 - Mise en œuvre de la plateforme technique CSIRT/SOC**
- **Lot 3 - Mise en œuvre de la gouvernance, des services et des formations pour le CSIRT/SOC**

En termes d'allotissement :

- Le Lot 1 est indépendant.
- Les Lots 2 et 3 sont solidaires et seront attribués au soumissionnaire ayant l'offre la plus avantageuse pour les 2 lots.

Les détails préliminaires sont donnés ci-dessous :

- <u>Le lot 2 :</u>
  - Mise en place de l'ensemble des fonctionnalités techniques du SOC en un seul jalon.

- <u>Le lot 3 :</u>
  Pour suivre la montée progressive en maturité du CSIRT/SOC, le lot 3 est réparti en 3 phases, pour une durée minimale de 3 ans (comme suit) :
  - Phase 1 : Gestion organisationnelle et développement des compétences accompagnant la mise en place du SOC de maturité niveau 1 (« Basic » selon SIM3v2)
  - Phase 2 : Gestion organisationnelle et développement des compétences accompagnant la mise en place du SOC de maturité niveau 2 (« intermédiaire » selon SIM3v2)

- Phase 3 : Gestion organisationnelle et développement des compétences accompagnant la mise en place du SOC de maturité niveau 3 (« advanced » selon SIM3v2)

NB : Le lot 3, dans son exécution, est dépendant de la mise en place des technologies du SOC dans le lot 2.

Pour chaque lot et chaque phase, la durée d'exécution est définie ci-dessous. Prière de noter que les lots 2 et 3 se déroulent en parallèle.

Durée d'exécution	**Lot 1**	**Lot 2**	**Lot 3**		
	3 mois	**6 mois**	**Phase 1**	**Phase 2**	**Phase 3**
			12 mois	**12 mois**	**12 mois**

Planning prévisionnel

Les prestations par lot sont à mettre en œuvre sur base du macro-planning proposé ci-dessous. Le soumissionnaire peut proposer des ajustements tout en justifiant le bien-fondé de ces derniers et en s'alignant aux autres contraintes spécifiques liées au contexte local.

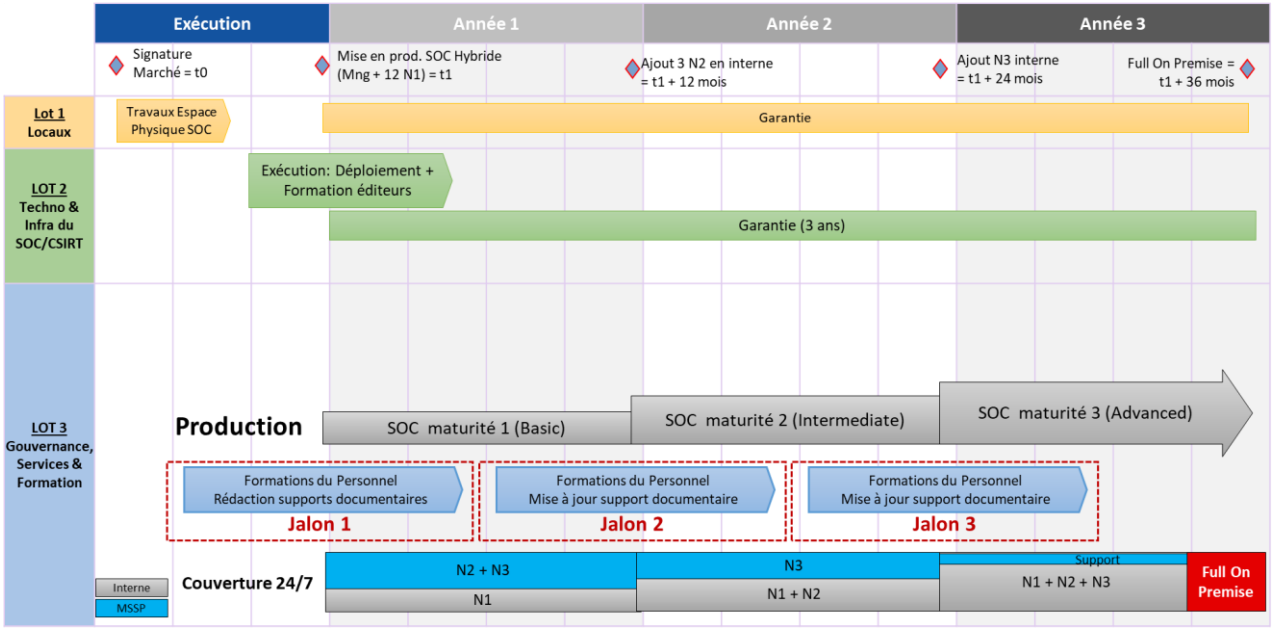
- Lot 1 - Mise en place de l'espace physique sur les **3 premiers mois** ;
- Lot 2 - Mise en œuvre de la plateforme technique du CSIRT/SOC : En une phase sur les **6 premiers mois du marché**, avec déploiement et formation éditeur, puis une phase de garantie de 3 ans, avec les modules minimums suivants :
    - SIEM (Collecte de logs, Corrélation, stockage & archivage, administration, reporting, notification, ...)
    - Détection des menaces sur les hôtes
    - Gestion des tickets
    - SOAR
    - Threat Intelligence
    - Threat Hunting
    - Forensiques
    - Capture de flux
    - Tableaux de bord
- Lot 3 - Mise en œuvre de la gouvernance, des services et des formations CSIRT/SOC, en 3 phases et sur les 3 années du marché. Les 3 phases contiennent la création de la documentation relative aux services CSIRT/SOC. En détails, le planning de cette phase est découpé de la façon suivante :
    - Jalon 1 :
        - Pour la partie formation du personnel, une première équipe interne constituée **d'un manager et de 12 analystes N1** devra être prête à opérer le SOC en 24/7 à partir de « t1 ». Les formations devront donc commencer **6 mois avant** cette date.
        - D'autre part, la partie gouvernance s'étalera sur les 12 mois de la phase pour mettre en œuvre les services CSIRT/SOC, avec au démarrage une **supervision externalisée 24/7 pour les analystes niveaux N2 et N3 (à la charge du soumissionnaire)**, la création de la documentation ainsi que la mise en place des indicateurs de performance, avec alignement au niveau **« intermediate »** de SIM3v2.
    - Jalon 2 :
        - La formation du personnel s'étalera sur 12 mois pour faire monter en compétences à la fois l'équipe existante, les nouveaux arrivants prévus (**ajout de 3 Analystes N2**) ou non prévus (remplacement d'anciens collaborateurs).
        - En parallèle, la partie gouvernance et services suivra la montée en maturité du SOC, avec réduction de la **supervision externalisée 24/7 pour le niveau N3 uniquement (à la charge du soumissionnaire)**, la mise à jour de la documentation et la mise à jour des indicateurs de performance, avec alignement au niveau **« advanced »** de SIM3v2.
    - Jalon 3 :

- La formation du personnel s'étalera sur 12 mois pour faire monter en compétences à la fois l'équipe existante, les nouveaux arrivants prévus (**ajout d'un Analystes N3**) ou non prévus (remplacement d'anciens collaborateurs).
- En parallèle, la partie gouvernance et services suivra la montée en maturité du SOC, sans **aucune supervision externalisée mais avec le support du soumissionnaire pour les escalades éventuelles**, la mise à jour de la documentation et la mise à jour des indicateurs de performance en liés, avec confirmation de la maturité au niveau **« advanced »** de SIM3v2.

Les jalons sont donc en lien avec chaque évolution du CSIRT/SOC par rapport à l'internalisation niveau d'escalade. Le développement et la mise en production d'indicateurs de performance se fera également tout au long du projet.

Les premières formations devront avoir lieu juste avant la mise en production du CSIRT/SOC. Une fois les opérations du SOC démarrées, les formations se feront au besoin au cours des 3 années, selon la montée en effectif des équipes.

Le macro-planning prévisionnel d'implémentation est illustré ci-dessous.



Garantie - Retenue de garantie & niveaux de services (SLA)

Lot 1 et Lot 2 (Garantie et SLA des matériels et technologies)

Le prestataire s'engage pendant cette période de garantir le remplacement du matériel défectueux de tous les équipements présentant des vis de fabrication ou un mauvais fonctionnement dans un délai maximum de 30 jours et à endosser la responsabilité entière en cas d'accident dû aux défectuosités de ses installations ou configurations matérielles ou logicielles et ce sans frais supplémentaires.
Durant cette période le prestataire s'engage à garantir la continuité de service en mettant à la disposition du maitre d'ouvrage et à titre de prêt, des équipements équivalents de remplacement, et ce selon les SLA défini ci-dessous.
Le prestataire est tenu, également le long de cette période, de fournir et installer les mises à jour logicielles et signatures une fois apparues ou déclarées nécessaires et obligatoires par le constructeur ou éditeur. Il est tenu par ailleurs d'informer le maitre d'ouvrage de ces mises à jour, de leurs criticités, opportunités et de leurs impacts dès leurs sorties et d'établir un planning de déploiements en commun accord avec le maitre d'ouvrage.
Rentre également dans le périmètre de la garantie la mise à jour de la documentation technique et l'accès au support des constructeurs et éditeurs de toutes les solutions proposées dans le cadre du présent projet.

Le tableau ci-dessous ainsi que le macro-planning plus haut (article 3) résument le délai de garantie pour chaque lot et phase :

Délai de garantie	**Lot 1**	**Lot 2**	**Lot 3**		
	3 ans	**3 ans**	**Phase 1**	**Phase 2**	**Phase 3**
			Non Applicable		

Pour le **lot 1**, Le délai de garantie est fixé à **trois (3) ans** à compter de la date de réception provisoire des prestations objet du lot en question.
Pour le **lot 2,** Le délai de garantie est fixé à **trois (3) ans** à compter de la date de réception provisoire de la solution.

Niveau de service (SLA – Service Level Agreement) applicable sur les lots 1 et 2 :

Cas	**Délai d'intervention**	**Remplacement de matériel (si pas de réparation possible sur place)**	**Remise en service de matériel (après réparation)**
problème bloquant causant un arrêt de service total ou partiel des services CSIRT/SOC	1h maximum	Sous un délais de 24h depuis déclaration incident	Sous un délais de 10 jours depuis déclaration incident
problème causant un dérangement non bloquant du fonctionnement normal des services CSIRT/SOC	3h maximum	Sous un délais de 72h (depuis déclaration incident)	Sous un délais de 20 jours depuis déclaration incident

Lot 3 (SLA des services)

Le prestataire est tenu de respecter les niveaux de services minimum prévus notamment pour la prestation de supervision externalisée, à savoir la mise à disposition 24/7 des niveaux d'escalade attendus pendant les 3 ans minimum, et (en option) un support au besoin sur une durée d'un an. Les propositions du prestataire sont attendu à cet effet.

Maintenance

A l'exclusion du lot 3, le prestataire doit joindre à son offre un projet de contrat de maintenance et de support du matériel et des logiciels. Le contrat de maintenance prendra effet à l'expiration de la période de garantie de chaque lot.

Ce contrat de maintenance devra porter la garantie totale pièces et main d'œuvre sur site à 3 ans. Cette garantie doit être appuyée sur une garantie du constructeur et de l'éditeur. Pour les produits du lot 2, un compte support directe avec le constructeur/éditeur doit être fourni.

Une solution d'enregistrement et de suivi des tickets doit être mise à disposition par le titulaire du marché, pour les besoins de notification des incidents. Les interventions du titulaire du marché sont également consignées dans la même solution précisant la nature de l'intervention, les intervenants, le descriptif de l'incident et les phases de déroulement de la résolution des problèmes.

Ce contrat inclus à minima les aspects ci-dessous :

Maintenance préventive

La visite d'entretien préventif devra être programmée trimestriellement. Le programme de la visite doit être planifié et coordonné avec le Maître d'ouvrage un mois avant la date de la visite.

Dans le cadre de cette visite, le prestataire est tenu de:

- Vérifier et analyser le fonctionnement des différentes composantes des solutions objet du présent appel d'offres,
- Analyser et vérifier les performances physiques des équipements,
- Analyser les fichiers logs des produits et investiguer les messages d'erreurs,
- Recommander et appliquer les modifications à apporter pour l'optimisation des performances,
- Fournir et installer les mises à jour (patch, correctif) des produits ou composante de produits,
- Fournir et installer les licences des produits et fichiers de signatures,
- Fournir et installer les upgrades mineurs/ majeurs,
- Vérifier le paramétrage des différentes solutions et faire un tuning des configurations pour un meilleur fonctionnement et optimisation des performances,
- Réaliser toutes les simulations et tests nécessaires pour s'assurer du bon fonctionnement des produits (test HA, redémarrage, sauvegarde et restauration des config …),
- Fournir des extensions matérielles nécessaires requises par les mises à jour ou upgrade,
- Echanger les pièces défectueuses par autres neuves,
- Nettoyer et dépoussiérer l'ensemble des solutions matérielles,
- Effectuer un transfert de connaissance pour l'équipe d'administration du maître d'ouvrage en cas d'un upgrade causant ainsi un changement d'interface d'administration ou ajout de nouvelles fonctionnalités.

Maintenance curative

- Dans le cas où un équipement de l'offre globale tombe en panne, le Maître d'ouvrage informe le prestataire qui intervient dans un délai de :
  - 1 heure maximum quand il s'agit d'un problème bloquant causant ainsi un arrêt de service total ou partiel des services SOC (Cas 1),

- 3 heures maximum quand il s'agit d'un problème causant un dérangement non bloquant du fonctionnement normal des services SOC (Cas 2),

- La maintenance curative consiste à dépanner ou changer les composantes / équipements défaillants (matériel ou logiciel) objet du présent contrat, sur appel du maître d'ouvrage.
- Le prestataire s'engage à mettre à la disposition du maître d'ouvrage son service de maintenance :
  - Pour le lot 1 : 8 heures par jour de 8h 30 à 16h30 courant les jours ouvrables
  - Pour le lot 2 : 24h/24 durant tous les jours de la semaine.

Ce service comprend :

<u>Cas 1 : Problème bloquant causant un arrêt de service partiel ou global des services SOC</u>

- L'intervention sur site sur appel du maitre d'ouvrage et ce conformément aux délais d'intervention précité ci-dessus,
- Le diagnostic de l'anomalie,
- Le contournement de l'anomalie dans le cas où le prestataire juge la nécessité d'avoir plus de temps pour faire les investigations nécessaires ; ou bien des circonstances qui imposent la continuité du service ; et ce sans porter atteinte aux niveaux de sécurité de départ.
- L'exécution de toutes les prestations de maintenance (l'installation des patchs correctifs, mise à jour OS etc. …), réparations, remplacements des pièces défectueuses nécessaires pour la normalisation de la situation,
- Si malgré tout, une composante ne pourrait être réparée sur place, elle devra être remplacée par une autre composante neuve équivalente ou supérieure en termes de performance et de configuration matérielle (sans facturation supplémentaire) et ce dans un délai maximum qui ne devra pas dépasser les <u>24 heures</u>, à compter de l'heure de déclaration de l'incident. La composante défectueuse devra être reprise par le prestataire pour réparation et remise en service dans un délai maximal qui ne devra pas dépasser <u>10 jours</u>.

<u>Cas 2 : Problème non bloquant, ne provoquant aucun arrêt de service partiel ou global des services SOC</u>

- L'intervention sur site sur appel du maitre d'ouvrage et ce conformément aux délais d'intervention précité ci-dessus,
- Le diagnostic de l'anomalie,
- L'exécution de toutes les prestations de maintenance (l'installation des patchs correctifs, mise à jour OS etc. …), réparation et remplacements des pièces défectueuses nécessaires pour la normalisation de la situation,
- Si malgré tout une composante ne pourra être réparée sur place, elle devra être remplacée par une autre composante neuve équivalente ou supérieure en termes de performance et de configuration matérielle (sans facturation supplémentaire) et ce dans un délai maximum qui ne devra pas dépasser les <u>72 heures</u>, à compter de l'heure de déclaration de l'incident. La composante défectueuse devra être reprise par le prestataire pour réparation et remise en service dans un délai maximal qui ne devra pas dépasser en aucun cas <u>20 jours</u>.

Le prestataire prendra toutes les mesures nécessaires pour rendre exploitable le matériel en panne. Il ne peut en aucun cas justifier un manquement à ses obligations en évoquant une indisponibilité de la main d'œuvre qualifiée ou de la pièce de rechange. Si malgré tout l'équipement ne pourrait être réparé, il devra être définitivement remplacé par un autre équipement neuf du même constructeur équivalent ou supérieur en termes de performances et de configuration matérielle.
Le support de stockage défectueux ou d'un équipement défectueux ainsi que l'équipement de remplacement restent toujours la propriété du Maître d'ouvrage.

Spécifications Techniques du Lot 1 (espace physique du CSIRT/SOC)

Dans le cadre de la mise en place de RIMCERT, le Ministère compte par le présent lot, aménager un espace physique existant, pour abriter le CSIRT/SOC. Pour se faire le prestataire devra démontrer sa capacité à créer cet espace de travail sécurisé respectant le besoin fonctionnel exprimé ci-dessous :

- Le SOC sera installé à Nouakchott dans des locaux désignés par le maitre d'ouvrage
- La permanence sera assurée sur le site, 24 heures sur 24 et 7 jours sur 7,
- L'équipe du SOC sera constituée à terme d'une vingtaine de personne (une dizaine pendant un shift) et pourra être assistée, sur site, de compétences externes si nécessaire.

Pour information, l'espace physique existant dispose déjà des mesures de sécurité physique de base pour la protection incendie, et la protection contre la perte d'énergie, dont le soumissionnaire devra s'assurer avant de faire sa proposition. Le besoin technique est défini ci-dessous.

Prestations attendues

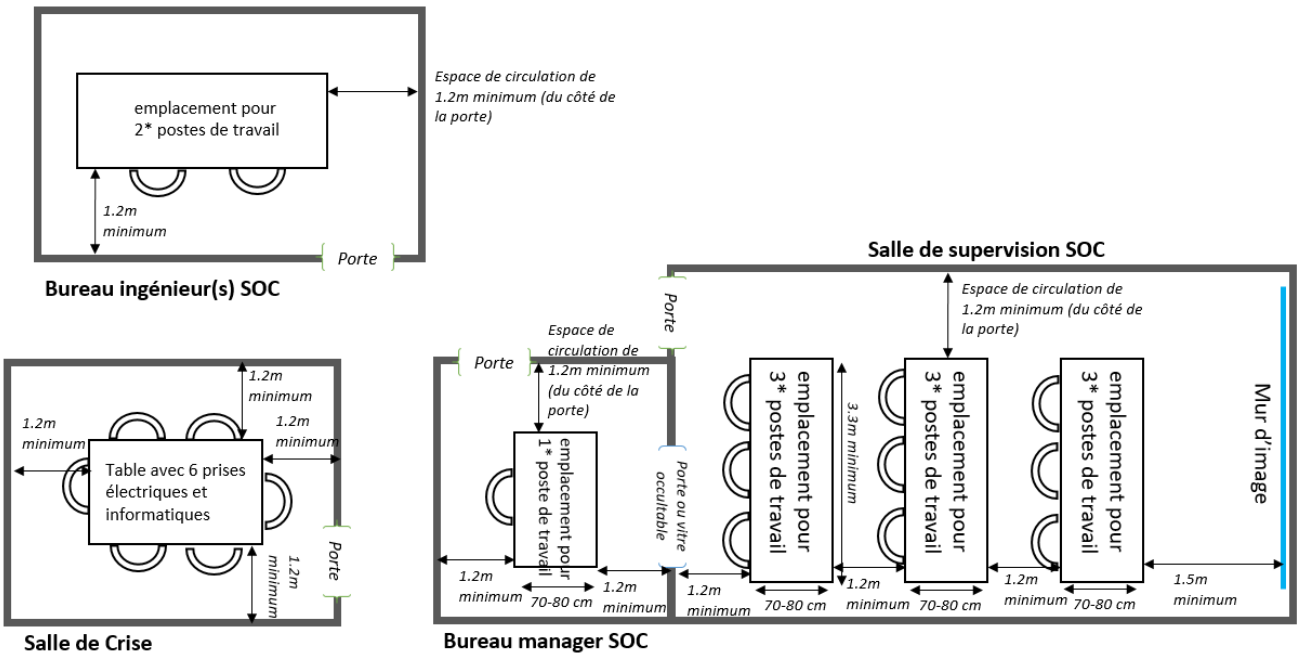
Activités

- Cadrage & conception :
    - Etudier l'existant
    - Fournir une proposition justifiée de design pour la salle de supervision du SOC précisant entre autres la disposition de :
        - Bureaux analystes (nombre de rangées, distance par rapport au mur d'image …),
        - Mur d'image,
        - Protection physique et environnementale,
- Implémentation - Aménagement de l'espace physique :
    - Fournir et installer l'ensemble du câblage nécessaire (réseau et électrique) à la mise en œuvre de l'espace physique CSIRT/SOC
    - Elaborer et fournir le schéma de câblage (plan de récolement)
    - Fournir, installer et mettre en service les composants matériels et logiciels objet du présent lot (mur d'image, contrôle d'accès, postes de travail …)
    - Fournir la documentation requise et nécessaire pour le lot en question.
    - Aménager de manière effective les différents locaux prévus
    - Assurer les tests et recette des équipements, avec transfert de compétences
- Maintenance
    - Assurer la garantie et maintenance des équipements

NB : le prestataire est tenu d'assurer tous les raccordements nécessaires en particulier les éléments nécessaires à l'affichage des consoles SOC sur le mur d'image.

Modèle de Plan 2D pour l'espace physique

Le schéma ci-dessous représente les principes d'organisation requise pour les locaux qui accueilleront le CSIRT/SOC. Il ne représente pas l'espace réellement mis à disposition du soumissionnaire, mais établi les règles à respecter pour l'implantation des tables et postes de travail.



En particulier :

- Chaque poste de travail indiqué devra disposer d'au moins une (1) prise électrique (ondulée), et au moins une (1) prise informatique Ethernet.
- Hormis le bureau du manager du SOC qui doit être contigu à la salle de supervision, les autres salles n'ont pas de requis de contiguïté. Elles sont schématisées pour définir leur implantation interne, sans dépendance par rapport aux autre salles.
- Les fenêtres ne sont pas connues ni indiquées dans le schéma. L'emplacement des portes est indicatif pour illustrer l'implantation des salles. Le soumissionnaire devra raisonnablement prendre en compte les contraintes d'emplacement des fenêtres et des portes dans le local cible identifié.

NB : Le soumissionnaire, durant la préparation de sa réponse, et lors de la visite des lieux, sera tenu de faire ces propres relevés.

L'espace minimal est décrit comme suit :

Local	Description
Salle de supervision	Espace sécurisé pour analystes niveau 1 et 2, avec au moins 10 bureaux, équipé d'un mur d'écran pour partager une vue globale de supervision. Les postes (tables et chaises) seront organisés en 2 ou 3 rangées, et contrôlant 2 écrans chacun.
Bureau ingénieur CSIRT/SOC	2 bureaux pour les opérations d'étude, intégration et maintien en opération du SI du CSIRT/SOC.
bureau manager CSIRT/SOC	1 bureau pour la gestion au quotidien de l'équipe CSIRT/SOC et définition de la stratégie.
Salle de gestion de crise	Salle totalement séparée pour gérer les crises.

Livrables

- Cadrage & conception
    - Plan d'Assurance Qualité
    - Rapport de l'état des lieux selon les exigences attendues
    - Planning et plan de charge de l'exécution
    - Design de la salle de supervision du SOC
    - Dossier d'ingénierie
- Implémentation
    - Plan de récolement
    - Dossier d'exploitation
    - Dossier de recette et test
- Maintenance
    - Contrat de maintenance
    - Planning de maintenance préventive (si applicable)
    - PV des interventions de maintenance curative & préventive

PS : Cette liste est non exhaustive, le prestataire est tenu de proposer tout autre livrable cohérent pour la réussite de la prestation.

Besoins technologiques pour l'espace physique SOC

Câblage informatique

Fourniture et pose de câble informatique (catégorie 6), goulottes, switch, prises informatiques et panneau de brassage pour l'espace physique SOC.
Le câblage à mettre en place sera un réseau isolé, segmenté du réseau du ministère (idéalement une segmentation physique).
Le raccordement réseau de l'espace SOC au réseau du Ministère (et au périmètre RIAD à superviser) devra être effectué au niveau d'un local technique dédié.

Mur d'image

Il permettra la projection permanente 24h/24 et 7j/7 de (04) principales consoles web et tableaux de bord du SOC. Il doit être de forme plate comprenant (04) écrans dont le format est compatible paysage et portrait.
Le soumissionnaire justifiera, dans son offre, le mode d'intégration et d'installation à assurer (encastré dans une cloison, fixé sur une cloison, posé sur un pied …) ainsi que le type du support à fournir (fixe, orientable, mural …).

Le mur d'image, à fournir et à installer, doit être muni de son propre système de gestion d'affichage et de contrôle. Dans le cas où ce dernier s'appuie sur un tiers, le soumissionnaire est tenu de justifier la compatibilité, par un écrit, fourni par le constructeur du mur d'image.

Le maître d'ouvrage, s'il y a lieu, doit avoir accès au support logiciel du système de gestion, du mur d'image, pour télécharger et appliquer les mises à jour et correctifs nécessaires.

Le soumissionnaire est tenu de fournir tout accessoire ou prérequis de mise en service, jugé nécessaire et utile (câblage, goulotte, protection électrique, système de refroidissement …).

- Le mur d'images devra être composé de 4 modules écrans plats de 46 pouces de diagonale disposés en matrice de 2x2 (Largeur x Hauteur).
- La séparation entre les écrans (de pixel à pixel) doit être inférieure à 5.7mm.
- Chacun de ces modules doit avoir une résolution (Full-HD).
- Type de rétro éclairage : LED.
- Economies d'énergie : Les écrans doivent posséder une horloge interne permettant la programmation du mode allumage et extinction automatique.

Postes de travail pour analystes

Pour le travail quotidien de supervision, il est demandé de fournir (08) ordinateurs dont les caractéristiques sont les suivantes :

- Ordinateur de bureau avec processeur I7 Quatre cœur 2.9 GHz ou supérieur, 4MB cache
- Compatible avec le Système d'exploitation 64 bit Windows 11 version entreprise,
- Stockage minimum : 500 Go, SSD
- Mémoire vive : 16 Go DDR2 à 800 MHz
- 1 carte graphique avec minimum 2 sorties vidéo (VGA, XVGA, HDMI) pour connecter 2 écrans LCD
- 2 Écrans LCD (ou équivalent LED) 20 '' avec traitement antireflet
- Carte réseau Ethernet 100/1000 Mbps avec connecteur RJ45
- Souris et clavier.

Besoins de sécurité physique et environnementale

Pour ces besoins, le soumissionnaire devra impérativement se basé sur les relevés de la visite des lieux pour confirmer les dispositifs existants sur lesquels s'appuyer, et faire sa proposition uniquement en complément de ce dernier. Tout dispositif répondant déjà aux exigences ci-dessous ne devra pas être intégré dans la proposition.

Détection et extinction d'incendie

Un système de détection d'incendie avec sirènes est à placer dans chaque salle ou bureau. Le système permettra d'envoyer une information déportée au local de supervision pour alerter l'opérateur de supervision.
Pour chacune des salles de l'espace physique SOC, il est également à prévoir des extincteurs manuels.

Alimentation électrique / ondulation

Fourniture et installation d'un onduleur, pour l'espace physique SOC, de capacité 30 KVA et d'une autonomie de 30 min à plein charge pour assurer la stabilisation de l'alimentation électrique et l'ondulation, des équipements de l'espace SOC, en cas de perturbations touchant les sources d'énergie électrique principales.

L'onduleur doit être doté d'une interface réseau et lié à la solution de supervision.

Le prestataire est tenu de réaliser tous les travaux de câblage électrique. Il est tenu également de fournir et installer tous les prérequis nécessaires de protection électrique et mise sous tension des équipements de l'espace physique SOC.

L'installation du système d'ondulation sera effectuée dans un local adjacent à l'espace physique SOC.

Mécanismes de détection des inondations

L'espace physique SOC devra être équipé de mécanisme de détection d'inondation. Ce dernier devra être capable de produire une alerte visuelle, sonore et via console de supervision indiquant la zone d'inondation.

Contrôle d'accès et caméras de vidéosurveillance

1- Système de contrôle d'accès des portes

La porte d'entrée au SOC et la porte de la salle de supervision doivent être équipées par un système de contrôle d'accès. Ceci doit permettre de limiter l'accès aux seules personnes autorisées.

Le système se compose de :

- Contrôleurs placés à proximité des deux portes ;
- Lecteurs d'empreinte digitale ;
- Ventouses de verrouillage de portes ;
- Interrupteurs à clé de déverrouillage des portes ;
- Contacts magnétiques d'ouverture des portes ;
- Fermes portes automatiques ;
- Gâches électriques ;
- Bris de glace.

2- Caméras de vidéosurveillance

2 cameras IP fixes de vidéosurveillance sont à installer dans l'espace physique SOC afin de surveiller la porte d'entrée au SOC et la porte de la salle de supervision.

Les caractéristiques minimales des caméras sont :

- Caméras HD ;
- Mode de compression : H264, MPEG/MPEG 4, MJPEG ;
- Fonction jour/nuit avec filtre IR ;
- Option d'archivage des alarmes ;
- Disposition d'une maintenance constructeur en termes de mise à jour d'OS.

3- Système d'enregistrement

Fournir et installer un système d'enregistrement des évènements de vidéosurveillance, à l'aide d'un enregistreur (type NVR), avec une période minimale de rétention des enregistrements d'un mois avec optimisation de stockage en termes de compression, …

Les caractéristiques minimales des enregistreurs sont :

- Analyseur vidéo intégré ;
- Journal des évènements et du système ;
- Définition d'enregistrement jusqu'à 1280x1024 ;
- Mode d'affichage 1/4/6/9/10/13/16 ;
- Méthode de compression : H264, MPEG/MPEG 4, MJPEG ;
- Compatibles avec différentes marques de produits IP.

Système de supervision

Fourniture et installation d'un système de supervision (matériel et logiciel) qui permettra de donner une visibilité centralisée sur les états des contrôles en place dans l'espace physique SOC en général et la salle de supervision en particulier : température, humidité, inondation, incendie, ondulation, contrôle d'accès, …

Spécifications techniques du Lot 2 (Plateforme technique du CSIRT/SOC)

Prestations attendues

Activités

Comme précisé dans le macro-planning, le présent lot doit permettre de réaliser ce qui suit :

- Conception de la solution
    - Conception et ingénierie de l'architecture de déploiement de la solution proposée
    - Livraison des fourniture et licences liée à la solution proposée
- Implémentation de la solution
    - Installation et mise en production des solutions
    - Fine tuning des solutions pour un paramétrage idéale
    - Tests de recette et transfert de compétences
- Maintenance de la solution
    - Assurer la garantie et maintenance des solutions déployées

La solution doit couvrir à minima ce qui suit :

- SIEM avec capacité de 1500 EPS, pouvant évoluer jusqu'à 2500 EPS sur les 3 années.
- Système de ticketing,
- Système de Threat intelligence,
- Système d'orchestration (SOAR),
- Système Forensic,
- Système de Threat Hunting,
- Système de collecte de flux.

Par ailleurs Le prestataire doit assurer :

- La fourniture, mise en service, paramétrage, intégration, fine tuning et test de recette des composants du SOC (SIEM, Threat Intelligence, Gestion de tickets, SOAR, Dashboard, Threat Hunting, Forensic, Capture de flux) :
- La validation des niveaux de logs et events ID activés sur les sources de logs avant intégration au niveau du SIEM,
- La collecte des logs (intégration des sources des logs),
- Le développement de parseurs (20 au minimum),
- La définition, implémentation, et test des uses cases adaptés au contexte,
- L'intégration entre les différents composants technologiques du SOC,
- La fourniture de la documentation requise et nécessaire,
- L'implémentation des indicateurs de performances,
- Le transfert des connaissances,
- La formation technique éditeur du personnel chargé de l'administration/exploitation des composants.

NB :

- Toute modification de configuration à apporter sur les sources de logs à superviser relève de la responsabilité du maître d'ouvrage.

- Le titulaire du marché, lors de la configuration des solutions, est tenu d'appliquer toutes les recommandations du constructeur/éditeur en matière de sécurité des configurations et des Framework.

Livrables

- Conception :
  - Plan d'Assurance Qualité
  - Planning et plan de charge de l'exécution
  - Dossier d'ingénierie
- Implémentation :
  - Dossier d'exploitation
  - Dossier des fiches de use case, tel que décrit dans l'annexe 1 « Description du contenu d'une fiche use case et les domaines d'attaque à couvrir »,
  - Dossier de recette et test.
  - Dossier de transfert de compétences
  - Dossier documentant, pour chaque source de logs (asset), le type de logs à récupérer (Syslog, log Windows (ID), …), méthode de récupération (WMI …), et le niveau de sévérité du log à récupérer.
- Maintenance :
  - Contrat de maintenance
  - Planning de maintenance préventive (healthcheck)
  - PV des interventions de maintenance curative & préventives

PS : Cette liste est non exhaustive, le prestataire est tenu de proposer tout autre livrable cohérent pour la réussite de la prestation.

Descriptif technique de chaque composant technologique

SIEM (Security Information and Event Management)

Le soumissionnaire doit proposer une solution permettant l'automatisation de la collecte, la corrélation, l'analyse, le stockage et archivage des évènements issus des différentes sources de logs du périmètre.

La solution cible doit être fournie avec toutes les licences et agents/client nécessaires, et doit répondre aux besoins fonctionnels généraux et spécifiques suivants :

- Il doit être capable de supporter jusqu'à 10.000 EPS (2500 prévus dans la première licence au bout de 3 ans) ;
- En plus de la partie « Threat Intelligence » de l'éditeur, le SIEM doit être en mesure de recevoir des IOC /IOA/Marqueur de compromission issue de la Threat Intelligence,
- Il doit pourvoir faire de l'analyse comportementale permettant de détecter des comportements déviant dans le système d'information,
- Il doit proposer une console d'administration hautement disponible et complète permettant l'analyse et l'investigation rapide d'une alerte,
- Il doit proposer des rapports par défaut avec des possibilités de faire des comparatifs par rapport à des normes ou standard du marché (ISO 27001, …),

- Il doit pouvoir s'interfacer avec un système de vulnérabilité pour majorer ou minorer les alertes en fonctions des vulnérabilités du système d'information,
- Il doit être intégrable avec l'ensemble des modules technologies du SOC,
- Il doit être capables de garder au moins les logs pendant six mois en ligne et un an en archive.
- Les communications entre tous les composants de la solution proposée doivent être chiffrées.
- Il doit pouvoir intégrer et réaliser la capture de flux réseau

Collecte des logs

- La solution proposée doit pouvoir supporter une collecte allant jusqu'à 10.000 EPS.
  A l'installation, la License devra couvrir 1500 EPS, et évoluer pour atteindre 2500 au total la 3e année.
  La possibilité d'évolution future pour collecter jusqu'à 10.000 EPS (au-delà des 3 ans), doit s'effectuer sans impact sur les performances de la plateforme proposée (moyennant les ajustement nécessaire, à préciser).
- La solution proposée doit permettre la collecte des évènements issus de tous les assets du périmètre (équipements réseau, équipements sécurité, serveurs d'infrastructure (serveur d'annuaire, serveur de messagerie, serveur Web, base de données …).
  La liste des technologies sera communiquée lors de la séance d'information prévue.
- Il doit pouvoir supporter plusieurs formats de logs pouvant être collectés de manière structurée (décomposition et normalisation) ou non structurée (texte brut),
- La solution proposée doit permettre la normalisation, l'enrichissement en temps réel et la consolidation des différents évènements collectés. Cela dans le but de réduire le temps de la détection et fournir instantanément l'information utile à l'analyste SOC.
- Si le module de management du SIEM proposé n'est pas opérationnel momentanément, les collecteurs doivent avoir la capacité de stocker les informations collectées le temps que la situation soit rétablie. (Exigence valable au cas où le soumissionnaire propose des collecteurs séparés)
- Le soumissionnaire doit fournir une estimation des pics supportés et signaler toute limitation éventuelle en cas de dépassement de licence. A noter que la solution proposée ne doit en aucun cas provoquer une perte de données.
- La solution doit disposer de connecteurs natifs et faciliter l'intégration de connecteurs à construire (**parseurs**) en fonction du besoin.
- Pour maintenir la traçabilité des échanges, la solution de gestion des journaux et l'infrastructure SIEM doivent être sécurisés et fiables (non-répudiation des données) et permettre de valider l'intégrité des données.
- Il doit être capable de réaliser des audits et des analyses forensic. En conséquence, le SIEM doit être en mesure de démontrer la confidentialité, l'intégrité et la disponibilité des données collectées selon leurs sources. La disponibilité de sources brutes est également importante pour mener des **activités forensiques**

Corrélation des logs

- La solution proposée doit permettre une corrélation à la fois en temps réel et en mode différé agissant sur les logs historiques.
- La solution proposée doit offrir des scénarios de corrélation évolués intégrant plusieurs journaux et plusieurs paramètres tels que : l'adresse IP source/destination, le temps, le démarrage/arrêt d'un service, l'utilisateur, le risque...etc.
- La solution proposée doit intégrer nativement un moteur intelligent de renseignement sur les menaces (threat intelligence) mis à jour automatiquement. La solution doit permettre une corrélation basée sur les paramètres fournis par ce moteur tel que les botnets, C&C, les malwares...etc.
- Il doit pouvoir corréler, analyser et traiter l'incident via une console unique. Cela signifie que les événements sous-jacents doivent être synchronisés dans le temps et collectés en temps réel à partir des différentes sources du périmètre (périphériques réseau, applications et systèmes) afin de pouvoir détecter les menaces internes ou externes. Violation de la politique de sécurité du Maître d'ouvrage ou des règlementations en vigueur,
- La solution doit permettre une corrélation basée sur les vulnérabilités remontées par le scanner de vulnérabilités utilisé par le maître d'ouvrage.
- La solution doit disposer de règles de corrélations prédéfinies et supporter leurs mises à jour automatique que leurs personnalisations. La solution doit intégrer plusieurs règles natives d'alerte et de corrélation.
- La solution doit permettre l'enrichissement de la couverture de détection via l'ajout de nouvelles règles de détection.
- La solution doit permettre la contextualisation des règles de détection en fonction des politiques internes en vigueur.
- La solution doit disposer d'une interface pour effectuer des requêtes et recherches dans les logs.
- La solution doit classer les alertes par rapport à la totalité des tactiques et techniques d'attaques de la matrice Mitre.
- La solution doit permettre la recherche d'IOC (Marqueurs), la détection d'anomalies et l'analyse de signaux faibles.
- La solution doit permettre notamment :
    - La détection des menaces inconnues du type APT, virus, malware, ransomware, … ainsi que les attaques inconnues.
    - La détection de comportements déviants au sein des systèmes d'information.
    - L'identification de signaux faibles précurseurs d'une catastrophe.
    - L'identification de la perte ou l'extraction de données.
    - La détection d'usurpation de droits.
    - La détection d'anomalies au sein du réseau.
    - La détection des menaces avancées.
    - La détection des intrusions.
    - La proposition des recommandations et des actions de remédiation.

Stockage et archivage

- La solution proposée doit permettre la conservation des logs bruts et des logs normalisés pour une durée de rétention de **3 mois en ligne et 1 an en offline.**

- Les logs doivent être stockés d'une manière compressée et sans atteinte à leur intégrité (cryptées).
- La solution doit permettre la récupération des logs (bruts ou normalisés) sur une période spécifique pour toute utilisation ultérieure (investigation, application de nouvelles règles de corrélation, apparition de nouvelles menaces). Cette récupération doit être rapide et transparente et à partir de la même interface d'administration.
- Le soumissionnaire doit détailler le calcul de la capacité du stockage interne et externe proposée, en prenant en considération l'évolution en termes de nombre d'EPS et d'extension de module (tel que les collecteurs du trafic réseau requis dans la troisième phase).

Interopérabilité des logs et données

- La solution proposée doit pouvoir démontrer une interopérabilité des logs collectés et données traitées et transformées avec de futures solutions ou modules de big data et intelligence artificielle qui pourraient être déployés dans l'environnement du SOC.

Administration, reporting et notification

- La solution proposée doit disposer d'une console unifiée pour administrer, gérer et configurer toutes les composants de la solution SIEM (collecte, reporting, créations de règles personnalisés, stockage...).
- La solution proposée doit enregistrer tous les logs d'audits de l'activité effectuée par des administrateurs ou opérateurs de la solution.
- La solution proposée doit disposer d'un système de remontée d'alertes en temps réel (email, Syslog, SNMP ou via l'affichage instantané d'une fenêtre au niveau de l'écran) pour chaque risque de sécurité et use case identifié.
- La solution proposée doit présenter des tableaux de bord par profil et personnalisable contenant entre autres les événements de sécurité critiques, les incidents, etc.
- La solution proposée doit supporter la génération et le stockage des rapports sous format PDF, EXCEL, HTML, CSV…etc.
- La solution proposée doit permettre la création des rapports consolidés à partir de plusieurs sources d'informations.

NB :

- ✓ **Le soumissionnaire doit dûment remplir le tableau ci-dessous, précisant les systèmes et équipements supportés, les versions supportées, et les méthodes de récupération de log pour chaque système et équipement : installation d'un agent, Syslog, WMI…**

Systèmes/équipements supportés	Versions supportées	Méthodes de collecte

- ✓ Le soumissionnaire est tenu de fournir une solution clé en main (**software ou hardware**). Le hardware éventuel doit être de type rackable, muni de tous les accessoires de mise en rack, et disposer d'alimentation redondante. Pour les besoins de ce marché, en cas de solution sous Appliance virtuelle (software), il est attendu du soumissionnaire de préciser les exigences de performance hardware pour la solution, afin que ces derniers soient mis à disposition par le maître d'ouvrage.

- ✓ Le soumissionnaire doit détailler les dimensions de chaque boitier en Unité.
- ✓ La solution SIEM doit être compatible avec les solutions de gestions de vulnérabilités communes du marché, ainsi que tous les modules technologiques proposés dans le cadre de cet appel d'offres.

Détection des menaces sur les hôtes

La solution proposée doit être intégrée avec le SIEM proposée et doit répondre aux besoins fonctionnels suivants, sur des plates-formes différentes, notamment Windows, Linux, Mac OS X, AIX, Solaris et HP-UX :

- Surveillance des hôtes pour détecter les menaces, les tentatives d'intrusion, les anomalies du système, les applications mal configurées et les actions utilisateur non autorisées.
- Effectuer un certain nombre de tâches dans le but de détecter les menaces et, si nécessaire, de déclencher des réponses automatiques.
- Collecte de données de journaux et d'événements
- Surveillance de l'intégrité des fichiers et des clés de registre
- Inventaire des processus en cours et des applications installées
- Surveillance des ports ouverts et de la configuration du réseau
- Détection de rootkits ou d'artefacts de logiciels malveillants
- Évaluation de la configuration et surveillance des politiques
- Exécution des active responses
- Analyse des logs, de traitement des événements à travers le SIEM et les règles, et l'utilisation des informations sur les menaces pour rechercher des IOC (Indicators Of Compromise) bien connus.
- Déclenchement d'une réponse lorsqu'une menace est détectée.
- Surveille les terminaux, les serveurs, les services cloud et les conteneurs.
- Analyse les systèmes surveillés à la recherche de logiciels malveillants, de rootkits et d'anomalies suspectes et détecte les fichiers cachés, les processus masqués ou les écouteurs réseau non enregistrés, ainsi que les incohérences dans les réponses aux appels système.
- Utilise une approche basée sur les signatures pour la détection des intrusions, en utilisant son moteur d'expression régulière pour analyser les données de journal collectées et rechercher des indicateurs de compromis.
- Extrait les données d'inventaire logiciel et envoient ces informations pour corrélation avec les bases de données CVE (Common Vulnerabilities and Exposure) mises à jour en continu, afin d'identifier les logiciels vulnérables bien connus.
- Tableaux de bord prêts à l'emploi pour la conformité réglementaire (par exemple PCI DSS, GDPR, …), les applications vulnérables détectées, la surveillance de l'intégrité des fichiers, l'évaluation de la configuration, les événements de sécurité, la surveillance de l'infrastructure cloud et autres.

Collecte de trafic réseau

La solution proposée peut être intégrée avec Le SIEM et doit répondre aux besoins fonctionnels suivants :

- Capturer et analyser l'ensemble du trafic réseau.

- L’administration et la surveillance du trafic réseau doivent être centralisées et depuis la même solution d’administration du SIEM proposée.
- Le soumissionnaire doit spécifier les modalités de récupération du flux réseau, et intégrer tous les prérequis nécessaires (tap, ... etc.).
- Le module doit être en mesure de traiter un débit internet de 100 Mbps.

Gestion des tickets

La solution de gestion de tickets doit répondre aux exigences suivantes :

- Elle doit permettre la gestion et la traçabilité des incidents, des problèmes et des changements,
- Elle doit s’interfacer avec les autres outils du SOC et être compatible et intégrable avec la majorité des SIEM du marché spécialement le SIEM à proposer.
- Elle doit offrir un portail web intuitif permettant de créer, modifier et suivre l’état d’avancement des tickets,
- Elle doit pouvoir envoyer des notifications par emails aux différentes étapes du cycle de vie du ticket (ouverture, modification, clôture),
- Elle doit permettre l’affectation, la planification et le suivi du traitement des demandes d’assistance en s’appuyant sur un inventaire complet (CMDB) et détaillé ainsi que sur une base de connaissances pour améliorer la qualité de services et capitaliser sur les incidents déjà survenus,
- Elle doit fournir des tableaux de bord ou rapport en lien avec chaque utilisateur en vue e pouvoir suivre l’évolution de chaque ticket ainsi que les performances de l’équipe.
- Elle doit comprendre une fonctionnalité permettant d’empêcher plusieurs agents de travailler sur un ticket en même temps
- Attribution automatique et manuelle des tickets
- Elle doit contenir le contrôle d'accès basé sur les rôles (RBAC).

Orchestration (SOAR)

La solution doit s’intégrer avec le SIEM proposé et doit répondre aux exigences suivantes :

- Elle doit permettre la gestion et la traçabilité des incidents, des problèmes et des changements,
- Elle doit s’interfacer avec les autres outils du SOC et être compatible et intégrable avec la majorité des SIEM du marché spécialement le SIEM à proposer.
- Elle doit offrir un portail web intuitif permettant de créer, modifier et suivre l’état d’avancement des tickets,
- Elle doit pouvoir envoyer des notifications par emails aux différentes étapes du cycle de vie du ticket,
- Elle doit fournir des tableaux de bord ou rapport en lien avec chaque utilisateur en vue de pouvoir suivre l’évolution de chaque ticket ainsi que les performances de l’équipe.
- Elle doit offrir la possibilité à plusieurs analystes SOC de collaborer simultanément sur des enquêtes, grâce à la diffusion des informations en temps réel des cases, des tâches, des observables et des IOC nouveaux ou existants.

- Elle doit gérer ou affecter de nouvelles tâches et de prévisualiser les nouveaux événements et alertes publiés dans les plateformes de renseignement sur les menaces à partir de plusieurs sources telles que les rapports par e-mail, les fournisseurs de cyber threat intelligence et les SIEM. Ils peuvent ensuite les importer et les analyser immédiatement.
- Elle doit permettre l'enregistrement des progrès de réponse à un incident, joindre des éléments de preuve ou des fichiers, importer des archives ZIP protégées par mot de passe contenant des logiciels malveillants ou des données suspectes sans les ouvrir.
- Elle doit permettre l'ajout des centaines ou des milliers d'observables à chaque cas crée ou importé directement à partir d'un événement publié dans la plateforme de partage d'informations sur les logiciels malveillants et doit pouvoir interroger simultanément plusieurs instances plateforme de partage d'informations sur les logiciels malveillants.
- Elle doit permettre interroger plus d'une centaine d'analyseurs pour des services populaires tels que Virus Total, Joe Sandbox, Domain Tools, Passive Total, Google Safe Browsing, Shodan et Onyphe. Identifiez les contacts abusifs, analysez les fichiers dans plusieurs formats tels que OLE et OpenXML pour détecter les macros VBA, générez des informations utiles sur les fichiers PE, PDF et bien plus encore.

Threat Intelligence

Le prestataire devra intégrer une ou plusieurs souscriptions à des flux de Threat Intelligence afin de collecter des informations liées aux menaces cyber. Ces marqueurs de compromission ou indicateurs de compromissions (IOC) seront collectés, triés et normalisés afin de pouvoir être intégrés dans la plateforme SIEM. Le but étant d'augmenter la qualité de détection par rapport à des éléments connus. Cette solution devra apporter une réelle plus-value au sein du système de détection du SOC. Cette solution devra répondre aux conditions suivantes :

- Elle doit permettre le regroupement et la contextualisation de renseignements provenant de plusieurs sources et avec différents formats,
- Elle doit permettre de catégoriser les données (type d'attaque et de menace par exemple),
- Elle doit s'interfacer avec le SIEM pour mettre en place des scénarios de détection sur base des indicateurs de compromissions récoltés.
- Elle doit prendre en considération les IOC et IOA ciblant différentes technologiques.

Threat Hunting

Le prestataire devra mettre en œuvre des outils de Threat Hunting pour rechercher de manière itérative et proactive les incidents que les scénarios de détection n'auront pas pu faire remonter. Il s'agit donc de chercher et identifier les cyber-menaces sur le réseau qui n'ont pas été détectés par les défenses de sécurité initiales.

Les outils de Threat Hunting proposés par le prestataire doivent permettre :

- De s'intégrer avec la plateforme SIEM,
- De créer un graphique visuel interactif permettant aux analystes d'explorer les entités et leurs relations,
- D'obtenir des informations et des statistiques décisives sur les attaques exploitables,
- Aux analystes d'avoir un accès rapide aux logs de flux enrichis, notamment les types de trafic et d'applications, volumes échangés, résolution d'adresses IP, géolocalisation,

historique des types de périphériques sur le réseau, … permettant ainsi une gestion en profondeur des données détaillées fournisses, au niveau de la sécurité du réseau.
- Aux analystes d'analyser à long terme des données réseau à un niveau granulaire.
- De se baser, entre autres sur des techniques de datamining et de l'analyse comportementale pour identifier le trafic malicieux que les solutions "traditionnelles" (détection d'intrusion, antivirus, Firewalls, …) ne sont pas en mesure de détecter et pouvant indiquer la présence d'une activité malveillante.
- Aux analystes de dresser un portrait global de la surface d'attaque du Maître d'ouvrage tout en identifiant les risques. D'intégrer les « risk scores » (score de risque) d'utilisateurs finaux.

Enfin la solution de Threat Hunting doit être évolutive pour pouvoir adapter le changement, notamment en prenant en charge tous les nouveaux actifs informatiques du périmètre.

Forensic

Le prestataire devra mettre en œuvre une combinaison d'outils de Forensic pour analyser en détails les incidents les plus graves remontés par le SOC. Les outils forensiques proposés par le prestataire doivent permettre :

- De collecter les traces afin de reconstituer le parcours de l'attaquant,
- De produire des preuves numériques fiables,
- D'identifier les informations exfiltrées et de comprendre les vulnérabilités exploitées.
- D'effectuer des recherches sur les logs ou flux réseaux, sur la mémoire vive des systèmes ou encore les systèmes de stockage (fichiers temporaires, secteurs effacés des disques durs…),
- De récupérer les fichiers effacés,
- D'analyser des fichiers infectés,
- D'analyser de la mémoire,
- De faire du hachage de tous les fichiers, ce qui permet d'effectuer un filtrage comparatif,
- De faire un hachage d'un disque dans sa totalité afin de confirmer que les données n'ont pas été modifiées.

Tableau de bord

En tant qu'élément de contrôle et de visualisation de l'état de santé de sécurité, un tableau de bord SOC unique doit être proposée, parfaitement détaillée dans la proposition du soumissionnaire, et comme exigences minimales devraient inclure d'une manière automatisée, personnalisée et en temps réel les informations suivantes :

- Croisement entre les actifs, les vulnérabilités et les menaces afin d'établir le niveau de risque jour après jour et rapporter l'état de santé de chacun des actifs
- Aide à la mise en conformité avec les bonnes pratiques de sécurité
- Fourniture des résultats d'aide à la décision en un simple clic
- Gestion de l'application de la PSSI
- Vision de haut niveau de la surveillance ainsi que des événements ou des incidents de sécurité ;

- Vision de bas niveau (ou détail) de la surveillance, ainsi que des événements ou des incidents de sécurité ;
- Affichages personnalisés pour chaque profil.
- Possibilité d'effectuer d'exploitation des données et génération de rapports.

Transfert de connaissances

Le prestataire assurera pendant l'exécution et à l'achèvement du projet, un transfert de connaissances pour les ressources qui seront affectées au projet.

- ✓ Volet SIEM et détection des menaces (au moins 5 jours)
- ✓ Volet gestion des tickets & SOAR (au moins 2 jour(s))
- ✓ Volet Threat Intelligence (au moins 2 jour(s))
- ✓ Volet Forensique (au moins 3 jours)
- ✓ Volet Threat Hunting (au moins 3 jours)

Il est à noter que le titulaire du marché, lors de la configuration des solutions, est tenu d'appliquer toutes les recommandations du constructeur/éditeur en matière de sécurité des configurations et des Framework.

Spécifications techniques du Lot 3 (Gouvernance, services et formations CSIRT/SOC)

Prestations attendues

Gouvernance et mise en service du CSIRT/SOC (avec supervision en mode hybride)

Le prestataire spécialisé est tenu d'assurer la gouvernance et les prestations nécessaires pour la mise en service du SOC. Il doit notamment assurer :

- Conception du service :
  - La conception et la mise en place du modèle opérationnel du CSIRT/SOC, basé sur les recommandations de l'étude de faisabilité réalisée dans ce sens;
  - La mise en place du catalogue de services CSIRT/SOC, conforme aux exigences SIM3v2 et FIRST, ainsi qu'au contexte national (la liste minimale des services à prévoir est celle prévue dans lesdits référentiels, en vue d'une adhésion au réseau FIRST);
- Implémentation du service :
  - L'élaboration et la fourniture des nouveaux processus/procédures complémentaires nécessaires au fonctionnement du CSIRT/SOC mis en place ;
  - La rédaction et la mise à jour de la documentation en adéquation avec l'architecture technique ;
  - La définition et revue des indicateurs de performance des services du CSIRT/SOC ;
  - L'élaboration de canevas de reporting, à destination de la hiérarchie et du manager du SOC, afin de suivre les indicateurs de performances définis, mesurant l'efficacité des fonctions SOC. L'objectif est de se prononcer sur le besoin des actions correctives à entreprendre pour une amélioration continue du fonctionnement du SOC, et la montée vers les niveaux de maturité attendus.
- Maintien du service :
  - La prestation de supervision externalisée pour les niveaux souhaités, en appui à l'équipe interne CSIRT/SOC.
  - L'alignement de la prestation à l'évolution de l'environnement et du contexte, des bonnes pratiques et des tendances de menaces.

Le prestataire doit assurer le démarrage du CSIRT/SOC en mode hybride, et sa montée en maturité sur 3 ans vers le mode « On premise » (100% interne) selon les configurations suivantes :

- ✓ Jalon 1 (1ère année) : Maturité 1 (au moins niveau « Intermediate » selon SIM3v2)
  - Conception et organisation du modèle opérationnel et du catalogue de services du SOC
  - Rédaction et mise en œuvre de la documentation nécessaire pour la maturité visée
  - Accompagnement à la montée en compétence sur le métier CSIRT/SOC (cf. Formations)
  - **Prestation de supervision externalisée** pour les niveaux N2 et N3 (Equivalent à 3 analystes N2, 1 analyste N3, et un coordinateur)

- ✓ Jalon 2 (2e année) : Maturité 2 (au moins niveau « Advanced » selon SIM3v2)
  - Mise à jour du modèle opérationnel et du catalogue de services du SOC
  - Rédaction et mise en œuvre de la documentation nécessaire pour la maturité visée

- Accompagnement à la montée en compétence sur le métier CSIRT/SOC (cf. Formations)
- **Prestation de supervision externalisée** pour le niveau N3 (Equivalent à 1 analyste N3 et un coordinateur)

✓ Jalon 3 (3e année) : Maturité 3 (confirmation du niveau « advanced » selon SIM3v2)

- Mise à jour du modèle opérationnel et du catalogue de services du CSIRT/SOC
- Rédaction et mise en œuvre de la documentation nécessaire pour la maturité visée
- Accompagnement à la montée en compétence sur le métier CSIRT/SOC (cf. Formations)
- **Prestation de support pour la réponse à incident au besoin**

NB : Les prestations fournies doivent s'aligner aux bonnes pratiques en vigueur, notamment les référentiels SIM3v2, ITIL.

Formations CSIRT/SOC

Organisation des sessions de formations pour les différents profils de l'équipe, tout au long des 3 années, selon l'audience suivante alignée à la montée en maturité du CSIRT/SOC :

- ✓ Phase 1 : 1 manager, 12 analystes N1, 1 ingénieur/technicien SOC
- ✓ Phase 2 : 1 manager, 12 analystes N1, 3 analystes N2, 1 ingénieur/technicien SOC
- ✓ Phase 3 : 1 manager, 12 analystes N1, 3 analystes N2, 1 analyste N3, 1 ingénieur/technicien SOC

Livrables

- Plan d'Assurance Qualité
- Planning et plan de charge de l'exécution

Pour la partie gouvernance :

- Fourniture de la documentation existante mise à jour
- Fourniture de canevas de rapports reprenant les indicateurs de performance
- Fourniture de la documentation complémentaire autour de l'organisation des services du SOC, comprenant entre autres la liste des procédures / processus (non exhaustive) ci-dessous :
  - Amélioration continue du service
  - Rotation des postes
  - Cycle de vie des scénarios de détection
  - Gestion des connaissances et des documents
  - Création, test, utilisation et gestion des scénarios de détection (use case)
  - Création des rapports
  - Gestion de la configuration
  - Gestion des problèmes
  - Gestion et réponse aux incidents

- Threat Hunting,
- Gestion des actifs.

Pour la mise à disposition des services SOC externalisés :

- Modèle de contrat de prestation, incluant les reporting réguliers
- Clause de réversibilité

Pour la partie formation :

- Fourniture des manuels de formation sous format papier ou sur support électronique.

Cette liste est non exhaustive, le prestataire est tenu de proposer tout autre livrable cohérent à la réussite de la prestation.

Descriptif technique

Définition du périmètre

Dans cette étape le Prestataire doit réaliser les activités suivantes :

- Etude des besoins et des objectifs cyber sécurité.
- Etude de l'existant en matière d'architectures, de systèmes, d'applications, de bases de données et d'équipements de sécurité et des réseaux.
- Indentification des mesures de sécurité en place.
- Délimitation des périmètres logique, physique et organisationnel à couvrir par le SOC.
- Identification des systèmes manquants en qualité et en quantité pour couvrir le périmètre technique de supervision. Ces systèmes doivent être inscrits sur une feuille de route pour les futures évolutions du service.
- Etude de l'existant en matière de procédures techniques, des processus organisationnels existants, des perspectives d'évolution en matière de cyber sécurité et système d'information.
- Collecte de la documentation technique, organisationnelle ainsi que de toutes les informations nécessaires pour mener à bien la prestation objet de la présente consultation.
- Vérification des prérequis nécessaires aux services SOC.
- Etude de la politique de gestion des journaux, inventaire des sources de journaux et estimation de la volumétrie des journaux collectés avec la durée de rétention applicable.
- Etude de tout détail, information ou document nécessaires pour la conception du SOC.

Conception du SOC

- Elaboration de la méthodologie et du plan de déploiement, de mise en production et de fine tuning des services SOC ;
- Définition de l'organisation cible, des rôles et responsabilités des ressources liés au projet SOC, à sa supervision et réponse aux incident et à son exploitation ;
- Identification des types de journaux d'évènements significatifs pour l'activité de détection ;
- Définition des durées de rétention et d'archivage des journaux d'événements ;

- Analyse des risques et définition des scénarios de menaces puis les scénarios de détection. Pour cela, le Prestataire doit tenir compte au minimum des cas suivants. Tout autre cas jugé nécessaire et/ou utile par le Prestataire devra être intégré (Environ 20 règles spécifiques à développer pour couvrir des scénarios de menaces identifiés):
    - Malware
    - APT
    - Ransomware
    - Intrusion
    - Spam / phishing
    - Déni de service
    - Services / protocoles dangereux ou illicites utilisés
    - Accès illicite en interne ou à internet
    - Accès non autorisé à une ressource
    - Exfiltration de données
    - Vulnérabilités non corrigées
    - Désactivation de l'enregistrement des journaux
    - Transfert illicite de fichiers
    - Station de travail ou serveur non sécurisé
    - Usurpation d'identité
    - Mots de passe gérés illicitement
    - Connexions réseau illicites
    - Faible configuration du pare-feu / systèmes mal ou non configurés / trace de dysfonctionnement
    - Utilisation d'un mécanisme de persistance
    - Actions non conformes à la politique de sécurité en vigueur

- Etude de l'impact engendré par les services SOC sur les performances réseau et système avec les différents scénarios d'optimisation possibles ;
- Conception des tableaux de bord destinés à visualiser la dimension technique et fonctionnelle du SI (couverture des risques, qualité de la politique de sécurité, suivi des audits, des actions et des alertes, indicateurs SOC, …).
- Elaboration de l'ensemble de processus et procédures autour de l'organisation et du fonctionnement du SOC. Ci-dessous une liste non exhaustive des documents à élaborer :
    - Documents de gouvernance SOC
    - Processus de gestion des incidents
    - Processus de veille
    - Procédure de gestion des changements
    - Procédure de gestion des vulnérabilités
    - Procédure de gestion des notifications
    - Procédure de sauvegarde, archivage, et rétention des logs
    - Démarche d'amélioration continue du SOC
    - Processus régissant les interactions entre le SOC et d'autres entités support capables de soutenir les efforts du SOC (Equipes Réseau, Production, Sécurité, etc.)
    - Processus de contrôle et d'administration du SOC
    - Dispositifs de continuité/Reprise (PCA/PRA) et de gestion de crise cyber sécurité

En vue de constituer un référentiel documentaire complet pour le fonctionnement global du SOC, respectant les bonnes pratiques et recommandations internationales, le Prestataire est tenu de compléter la liste ci-dessus par d'autres processus nécessaires pour le bon fonctionnement du SOC, notamment ceux exigés par le référentiel SIM3v2 en termes de processus.

Mise à disposition des services

Le Prestataire doit :

- Mettre en œuvre le SOC selon le scénario arrêté convenu;
- Désigner les équipes chargées du SOC et affecter les rôles et les responsabilités selon l'organisation définie ;
- Mettre en œuvre une stratégie de conduite du changement induite par la prestation ;
- Mettre en place les canaux de communication avec les parties prenantes;
- Mettre en application les procédures du SOC élaborées dans la phase « Conception du SOC »

Le service SOC que le Prestataire mettra à la disposition du maître d'ouvrage doit :

- Être certifié à la norme ISO 27001, ISO 9001, FIRST, CNDP, …
- Être fournisseur SOC MSSP depuis au moins 5 ans, avec au moins deux références dans la région, et au moins 3 sur les 5 dernières années avec montant proche de celui du présent marché ;
- Être configuré, managé et supervisé afin d'anticiper d'éventuels problèmes et incidents
- Répondre aux différentes exigences applicables, à savoir :
  - les exigences spécifiées dans le tableau de conformité du présent dans ce cahier de charge
  - le model fonctionnel et les descriptifs techniques des composants SOC, exprimés dans le présent cahier de charge,
  - Garantir une rapidité du temps de réponse selon les niveaux de services définis ;
  - Garantir le load balancing et la sécurité des échanges entre les composants SOC. Les échanges d'informations au sein même de l'architecture SOC doivent être également sécurisés ;
  - Détecter les menaces selon les référentiels internationaux comme MITRE ATT&K ;
  - Détecter les menaces sur la base des normes référentes internationales notamment la totalité des menaces répertoriées au niveau du référentiel MITRE ATT&K ;
  - Être capable de se remettre d'une attaque DDOS en un temps raisonnable ;
  - Identifier plus rapidement les attaques potentielles et les avorter avant qu'elles ne causent des dommages ;
  - Être capable de se remettre des attaques en un temps raisonnable à décider en commun accord;
  - Avoir les ressources humaines nécessaires et compétentes pour sa bonne gestion ;
  - Être doté d'une bonne stratégie de surveillance.

Le Prestataire doit détailler sur son offre la méthodologie prévue pour l'activation du SOC managé selon les paramètres ci-dessous.

Type de contrat	Supervision 24/7
Nombre de licence monitorées	Supporter jusqu'à **2500 EPS** sans frais supplémentaire
Fréquence des comités Opérationnels	2 / semaine
Fréquence des rapports	1 / mois
Fréquence du comité de Pilotage	1 / mois
Niveau 1 Managé	NON
Niveau 2 Managé	OUI pour 1 an minimum (Année 1)
Niveau 3 Managé	OUI pour 2 ans minimum (Année 1 & 2)
Réponse à incident	A la demande (notamment à partir de la 3e année)
Délai de rétention (en ligne / Hors ligne)	90 jours / 1 an
Heures de service	Support Premium 24/7/365
Gestion des crises	Oui
24H / 7J	Traitement 24/7 des incidents
Dashboard / Reporting	Accessible au maître d'ouvrage
Disponibilité de la solution	Supérieur à 98 %

Organisation de la prestation de supervision externalisée

Pour maintenir le SOC en condition opérationnelle et assurer son amélioration continue, le Prestataire doit :

- Maintenir à jour et effectuer les montés de versions nécessaires pour tous les composants (matériel ou logiciel) objet de la consultation. Ces évolutions doivent être actées de commun accord.
- Surveiller et ajuster les taux et les seuils d'alertes pour éviter une saturation du SOC et une constitution d'un backlog important. Les opérations de tunning de la solution sont une activité continue durant toute la période du marché.
- Faire de la veille de sécurité et rester à niveau par rapport aux évolutions des menaces afin d'affiner les scénarios de détection mis en place.
- Produire des tableaux de bord opérationnels et managériaux selon la périodicité convenue en commun accord avec le Prestataire.
- Maintenir les use cases mis en place par la mise en place de nouveaux cas (suite à l'apparition d'une nouvelle menace de sécurité par exemple), la suppression ou la modification de cas existants doit être mené de commun accord.
- Faire monter en compétences l'équipe interne en charge du SOC avec qui elle collabore au quotidien
- Animer des réunions de suivi avec :

    - **Comité de suivi :** instance programmée principalement de façon mensuelle ou, le cas échéant, sur la base d'un planning fixé de commun accord selon les contraintes de disponibilité. Elle est animée par le responsable opérationnel du SOC et permet d'effectuer une revue des incidents de la période précédente. Les participants de ce comité (généralement les équipes opérationnelles) planifient les actions de la période à venir en fonction de la criticité des incidents en cours. Les points et difficultés majeurs sont remontés aux comités de pilotage.

- **Comité de pilotage** : instance programmée principalement de façon trimestrielle avec le management du maître d'ouvrage ou le cas échéant, à sa demande. Elle a pour but de s'assurer du bon pilotage du service SOC. Elle est animée par le responsable opérationnel du SOC en présence des responsable en charge de la sécurité SI, des structures informatiques et métiers concernés. L'accent est mis sur :
    - Le bilan de la période écoulée d'un point de vue service de supervision (quantitatifs et qualitatifs) : incidents critiques, principales requêtes, résultats des changements effectués, statut des actions.
    - Le tableau de bord projet synthétisant les KPI contractuels (ex. nombre d'incident, nombre de ticket clos, secteurs du SI les plus touchés par les incidents, etc.).
    - L'évolution du périmètre du service et la stratégie de prise en compte des changements ou actions demandés lors des réunions précédentes.

Le prestataire est tenu également d'élaborer, en se basant, entre autres, sur les indicateurs déjà définis dans « la démarche pour l'amélioration continue du SOC », deux modèles de rapports :

- Le premier ciblant une hiérarchie managériale qualifiant l'efficacité du service SOC.
- Le deuxième à destination du manager du SOC en vue de mesurer l'efficience technique et humaine des ressources SOC.

Le maître d'ouvrage s'engage à informer le Prestataire de tout changement opéré sur son Système d'Information pouvant avoir un impact sur le service SOC mis à disposition dans le cadre du présent marché. Ceci permettra d'éviter des changements non répertoriés pouvant provoquer un accroissement des évènements et incidents et/ou une saturation des équipes en charge.

Le niveau de service attendu est soumis au minimum aux SLA ci-dessous. La liste complète des SLA sera élaborée de commun accord :

Service	Niveau de service attendu (SLA)
Résolution d'une défaillance de la solution de supervision n'impliquant pas de perte de log	Résolution du problème dans les 24 heures
Résolution d'une défaillance de la solution de supervision impliquant une perte de logs	Résolution du problème dans les deux heures
Disponibilité de la solution/ du service (Taux de disponibilité calculé selon une base trimestrielle)	Supérieur à 98 %
Temps de génération des rapports à partir de la solution proposée (Un rapport sur les temps de réponse de la solution aux requêtes soumises doit être élaboré par le Prestataire selon une périodicité mensuelle)	Le temps de réponse de la solution aux requêtes adressées doit être immédiat pour les données en ligne
Détection d'alertes/incident et notification du maître d'ouvrage, avec communication d'un plan de mitigation	- Notification d'un incident « critique » et communication d'un plan de mitigation dans une heure suivant son identification. Des rappels doivent être effectués toutes les deux heures jusqu'à la clôture de l'incident. - Notification d'un incident « Haut » et communication d'un plan de mitigation dans les deux heures suivant son

	identification. Des rappels doivent être effectués toutes les quatre heures jusqu'à la clôture de l'incident. - Notification d'un incident « Moyen » et communication d'un plan de mitigation dans les huit heures suivant son identification. Des rappels doivent être effectués tous les jours jusqu'à la clôture de l'incident. - Notification d'un incident « Bas » dans les 24 heures suivant son identification. Des rappels doivent être effectués tous jours jusqu'à la clôture de l'incident.
Résolution des incidents relatifs au périmètre de supervision (demande initiée par le maître d'ouvrage)	- Résolution d'un incident « critique » dans les deux jours suivant leur détection - Résolution d'un incident « Haut » dans les cinq jours suivant leur détection - Résolution des incidents « moyens » dans les dix jours suivant leur détection - Résolution des incidents « faibles » dans les quinze jours suivant leur détection
Communication des rapports et des tableaux de bord	Production des rapports et des tableaux de bord selon le planning et la périodicité convenus
Patch management des composants du SOC	Patching et montées de version des firmwares et des logiciels du SOC définis de commun accord
Audit du SOC	Prendre en charge, dans les délais prescrits, les recommandations issues des missions d'audit du SOC
Mobilisation des ressources humaines du SOC	Mobilisation des ressources humaines nécessaires au fonctionnement du SOC conformément à l'organisation convenue
Prise en compte de nouveaux uses cases demandés	Prise en compte de nouveaux uses cases demandés dans les 24 heures et dans la limite de 20 maximum.
Ajout d'une nouvelle source de log	Ajout d'une nouvelle source de log dans les 48 heures suivant la formulation de la demande
Réalisation des investigations « forensics »	Fourniture du rapport des résultats des investigations « forensic » des actifs faisant partie du périmètre de supervision dans les trois jours ouvrés suite à la formulation de la demande

Le Prestataire est tenu, selon les SLA, d'appliquer les procédures de correction et/ou de contournement afin de réussir la résolution des incidents détectés.
Le Prestataire est tenu de suivre les tickets ouverts jusqu'à résolution de l'incident et la documentation du rapport d'incident.

Réversibilité

Le Prestataire doit élaborer un plan de réversibilité permettant une reprise du service par le maître d'ouvrage ou par un autre prestataire de service désigné par ce dernier, et ce dans les meilleures conditions.
La durée de réversibilité est fixée à 6 mois avant l'arrivée à terme du contrat. Le plan décrivant les modalités opérationnelles du processus de réversibilité est réalisé par le Prestataire durant les trois (3) premiers mois de la prise du service et actualisé, au moins tous les trois mois par ce dernier.
Après chaque actualisation, le plan de mise en œuvre de la réversibilité est soumis à l'approbation du maître d'ouvrage.
Le plan de réversibilité doit décrire les aspects suivants :

- L'inventaire exhaustif des informations à restituer ;
- Les intervenants et les actions requises par chacun d'eux ;
- Les formats des informations à restituer ;

- Les moyens de restitution ;
- L'organisation à mettre en place, les responsabilités, le planning et les dates jalons (principalement : date de fin de contrat, date de basculement), les engagements en matière d'assistance, les différentes options de réversibilité, le contrôle de la mise en œuvre de la réversibilité ;

Le Prestataire doit assurer le maintien en conditions opérationnelles de la solution durant toute la période de mise en œuvre du plan de réversibilité.
En fin de marché et à la demande du maître d'ouvrage, le Prestataire s'engage à :

- Remettre l'ensemble des codes d'accès dont il dispose ;
- Remettre l'ensemble des documents et procédures produits ou récupérés dans le cadre de l'exécution des services (au format Word ou PDF).
- Transférer l'intégralité des droits de propriété, y compris intellectuelle, nécessaires à la réalisation des services, notamment par rapport aux éventuels développements spécifiques entrepris dans le cadre du présent marché ;
- Détruire l'ensemble des informations relatives au maître d'ouvrage à l'issue de l'exécution du plan de réversibilité à l'exception de celles pour lesquelles il a reçu une autorisation de conservation formelle de la part du maître d'ouvrage.

Formations

Dans le cadre de la mise en place de RIMCERT, le maître d'ouvrage compte développer davantage les compétences et connaissances théoriques et pratiques de l'équipe, au tour des services CSIRT/SOC. Pour cela le soumissionnaire est tenu d'assurer les formations spécifiées dans le tableau ci-après.

Ces formations doivent être déroulées dans des centres de formations agréés et assurées par des formateurs expérimentés et certifiés formateurs chacun dans son domaine d'intervention.

Le prestataire est tenu d'assurer toute la logistique pour garantir le bon déroulement des formations.

Les formations demandées sont préparatoires à la certification. Le soumissionnaire doit proposer des cursus de formations certifiantes sans inclure, dans son offre financière, le prix de la certification.

Le programme, le centre de formation et le formateur doivent être approuvés par le Maître d'ouvrage 20 jours calendaires avant le démarrage de chaque formation. Le soumissionnaire fournira les CV signés, paraphés et cachetés ainsi que les certifications des formateurs. **Il doit présenter également un justificatif attestant que le ou les centre(s) de formations sont agrées**.

Le maître d'ouvrage se réserve le droit de refuser un formateur, sur la base de son CV ou après démarrage de la formation ou d'une session à l'autre, s'il juge que ses compétences ne sont pas satisfaisantes pour accomplir à bien la mission qui lui a été confiée.

Le tableau ci-après explicite les formations à suivre pour chaque profil du SOC sur les 3 phases :

NB 1 : Comme déjà décrit au niveau de l'article macro-planning, le présent lot est segmenté en 3 phases. En vue de suivre la montée en maturité technologique SOC, il est à noter que les formations relatives à chaque phase doivent être achevées :

- Pour la phase 1 : avant t1
- Pour la phase 2 : avant t1+ 15mois

- Pour la phase 3 : avant t1+ 27 mois

NB 2 :
Pour les 3 lots, le ou les prestataire(s) est (sont) tenu(s), au cas où une ressource projet quitte le prestataire, pour une raison ou une autre, de la remplacer par une autre au minimum ayant les mêmes compétences en termes de certifications et nombres d'années d'expérience.

Les formations minimales prévues par profil sont les suivantes :

- Formations transverse de l'équipe CSIRT/SOC
  - Formation ITIL
  - Soft skills : Gestion du stress ou équivalent ; Gestion du temps ; travail d'équipe.

- Analystes N1 (12)
  - Google Cybersecurity Professional Certificate (Formation en ligne de 5 mois sur Coursera)
  - Comptia Security+ (avec certification)
  - Blue Team Level 1 (BTL1) (avec certification)

- Analystes N2 (3)
  - CompTIA Cybersecurity Analyst (CySA+) (avec ateliers en ligne et certification)
  - Blue Team Level 2 (BTL2)
  - ECIH – EC Council Incident handler (avec certification)

- Analyste N3 & Manager SOC (2)
  - SANS GIAC LDR553: Cyber Incident Management Leader
  - SANS GIAC LDR512: Security Leadership Essentials for Managers

Liste des Fournitures et Calendrier de livraison

[L'Acheteur remplit ce tableau, à l'exception de la colonne « Date de livraison offerte par le Soumissionnaire » qui est remplie par le Soumissionnaire. La liste des articles doit être identique à celle qui apparaît au bordereau des prix, Section IV]

Lot 1 (Aménagement de l'espace physique CSIRT/SOC)

Article No.	**Description des Fournitures**	**Quantité (Nb. d'unités)**	**Unité**	**Site (projet) ou Destination finale comme indiqués aux DPAO**	**Date de livraison (selon les Incoterms)**	
					Date de livraison au plus tard	**Date de livraison offerte par le Soumissionnaire [*à indiquer par le Soumissionnaire*]**
Besoins Technologiques						
01	Câble informatique	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
02	Mur d'image	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
03	Postes de travail pour analystes	**8**	**U**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
Besoins en sécurité physique & environnementale						
04	**Contrôle d'accès et vidéosurveillance**					
04.1	Système de contrôle d'accès des portes	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
04.2	Caméras de vidéosurveillance	**2**	**U**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
04.3	Système d'enregistrement	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
05	Détection et extinction incendie	**1**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
06	Alimentation électrique	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
07	Mécanismes de détection des inondations	**1**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**4 mois**	
08	Système de supervision	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**4 mois**	
Prestation de services						
09	Prestation de services	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**4 mois**	

Lot 2 (Plateforme technique CSIRT/SOC)

Article No.	Description des Fournitures	Quantité (Nb. d'unités)	Unité	Site (projet) ou Destination finale comme indiqués aux DPAO	Date de livraison (selon les Incoterms)	
					Date de livraison au plus tard	Date de livraison offerte par le Soumissionnaire [*à indiquer par le Soumissionnaire*]
01	Plateforme technique CSIRT/SOC, avec à minima les modules suivants • SIEM, • Détection des menaces, • Gestion des tickets, • Orchestration (SOAR) • Threat intelligence, • Threat hunting, • Collecte de trafic réseau, • Forensic, • Tableaux de bord	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
02	Garantie et maintenance sur 3 ans	**3**	**An**	*Site du CSIRT/SOC - Nouakchott*	**36 mois**	
03	Prestations de service	**ENS**	**ENS**	*Site du CSIRT/SOC - Nouakchott*	**6 mois**	

Lot 3 (Gouvernance, Services & Formations CSIRT/SOC)

Article No.	Description des Fournitures	Quantité (Nb. d'unités)	Unité	Site (projet) ou Destination finale comme indiqués aux DPAO	Date de livraison (selon les Incoterms)	
					Date de livraison au plus tard	Date de livraison offerte par le Soumissionnaire [*à indiquer par le Soumissionnaire*]
Gouvernance et mise en service CSIRT/SOC						
01	Conception de la gouvernance du SOC	**1**	**F**	*Site du CSIRT/SOC - Nouakchott*	**3 mois**	
02	Supervision SOC 24H/24 et 7J/7 en mode hybride pour 1 an – (3 Analystes N2)	**1**	**An**	*Site du CSIRT/SOC - Nouakchott*	**4 mois**	
03	Supervision SOC 24H/24 et 7J/7 en mode hybride pour 1 an – (1 Analyste N3 & coordination)	**2**	**An**	*Site du CSIRT/SOC - Nouakchott*	**4 mois**	
04	Jours/Homme d'assistance supplémentaire au besoin	**20**	**JH**	*Site du CSIRT/SOC - Nouakchott*	**1 jour**	
Formations CSIRT/SOC						
05	Formation équipe SOC (ITIL, Gestion du stress / du temps, travail d'équipe)	**18**	**Pers.**	*Site du CSIRT/SOC - Nouakchott*	**12 mois**	
06	Formations Analystes N1 • Cybersecurity Professional • Comptia Security+ • Blue Team Level 1	**12**	**Pers.**	*Site du CSIRT/SOC - Nouakchott*	**6 mois**	
07	Formations Analystes N2 • CompTIA Cybersecurity Analyst • Blue Team Level 2 • ECIH – EC Council Incident handler	**3**	**Pers.**	*Site du CSIRT/SOC - Nouakchott*	**12 mois**	
08	Formations Manager et Analyste N3 • SANS GIAC LDR553: Cyber Incident Management Leader • SANS GIAC LDR512: Security Leadership Essentials for Managers	**2**	**Pers.**	*Site du CSIRT/SOC - Nouakchott*	**24 mois**	

Liste des Services Connexes et Calendrier de réalisation

[Ce tableau est rempli par l'Acheteur. Les dates de réalisation des services doivent être réalistes, et cohérentes avec les dates de livraison (selon les Incoterms)]

Lot 1 (Aménagement de l'espace physique CSIRT/SOC)

Article No. Service.	**Description du Service**	**Quantité**[1]	**Unité physique**	**Site ou lieu où les Services doivent être exécutés**	**Date finale de réalisation des Services**
[insérer le numéro du Service	*[insérer la description du service]*	*[insérer le nombre d'articles à fournir]*	*[unité de mesure]*	*[lieu de réalisation du service]*	*[insérer la date]*
01	**Conception de l'espace physique** • Analyse de l'existant • Conception des bureaux & salles	1	U	*Site du CSIRT/SOC - Nouakchott*	*1 mois*
02	**Aménagement de l'espace physique** • Préparation de l'espace • Installation des équipements • Disposition des bureaux et salles • Tests de bon fonctionnement • Transfert de compétences • Documentation finale	1	U	*Site du CSIRT/SOC - Nouakchott*	*4 mois*
03	**Maintenance de l'espace physique** • Garantie sur 3 ans • Maintenance préventive • Maintenance curative	1	U	*Site du CSIRT/SOC - Nouakchott*	*36 mois*

[1] Si applicable

Lot 2 (Plateforme technique CSIRT/SOC)

Article No. Service.	Description du Service	Quantité[2]	Unité physique	Site ou lieu où les Services doivent être exécutés	Date finale de réalisation des Services
[insérer le numéro du Service	*[insérer la description du service]*	*[insérer le nombre d'articles à fournir]*	*[unité de mesure]*	*[lieu de réalisation du service]*	*[insérer la date]*
01	**Conception de la solution** • Cadrage et planification • Ingénierie de la solution	1	U	*Site du CSIRT/SOC - Nouakchott*	*2 mois*
02	**Implémentation de la solution** • Installation et fine tuning • Tests & recette de la solution • Transfert de compétences	1	U	*Site du CSIRT/SOC - Nouakchott*	*6 mois*
03	**Maintenance de la solution** • Garantie 3 ans • Maintenance préventive • Maintenance curative	1	U	*Site du CSIRT/SOC - Nouakchott*	*36 mois*

La solution doit bénéficier d'une garantie de 3 ans, activée dès la réception provisoire de la solution :

- Garantie 3 ans
- Maintenance préventive
- Maintenance curative

[2] Si applicable

Lot 3 (Gouvernance, Services & Formations CSIRT/SOC)

Article No. Service.	Description du Service	Quantité[3]	Unité physique	Site ou lieu où les Services doivent être exécutés	Date finale de réalisation des Services
[insérer le numéro du Service	*[insérer la description du service]*	*[insérer le nombre d'articles à fournir]*	*[unité de mesure]*	*[lieu de réalisation du service]*	*[insérer la date]*
Conception & Implémentation du service CSIRT/SOC					
01	**Gouvernance et mise en service**	1	U	*Site du CSIRT/SOC - Nouakchott*	*4 mois*
Maintien du service CSIRT/SOC					
02	**Supervision externalisée (hybride) – Phase 1 (N2 & N3) (Année 1)**	1	U	*Site du CSIRT/SOC - Nouakchott*	*4 mois*
03	**Supervision externalisée (hybride) – Phase 2 (N3) (Année 2)**	1	U	*Site du CSIRT/SOC - Nouakchott*	*12 mois*
04	**Supervision externalisée (hybride) – Phase 3 (Support N3) (Année 3)**	1	U	*Site du CSIRT/SOC - Nouakchott*	*24 mois*
Formations CSIRT/SOC					
05	**Formations transverses CSIRT/SOC**	1	U	*Site du CSIRT/SOC - Nouakchott*	*12 mois*
06	**Formations Analyste N1**	1	U	*Site du CSIRT/SOC - Nouakchott*	*12 mois*
07	**Formations Analyste N2**	1	U	*Site du CSIRT/SOC - Nouakchott*	*18 mois*
08	**Formations Analyste N3 & Manager**	1	U	*Site du CSIRT/SOC - Nouakchott*	*24 mois*

[3] Si applicable