REPUBLIQUE DE GUINEE

Travail-Justice-Solidarité

.....

MINISTERE DE LA COMMUNICATION, DE L'ECONOMIE NUMERIQUE ET DE L'INNOVATION (MCENI)

.....

PROJET DE TRANSFORMATION NUMERIQUE POUR L'AFRIQUE/PROJET REGIONAL D'INTEGRATION NUMERIQUE EN AFRIQUE DE L'OUEST (WARDIP-GUINEE)

AVIS A MANIFESTATIONS D'INTERET

SERVICES DE CONSULTANT (Individu)

Client : Ministère de la Communication, de l'Economie Numérique et de l'Innovation (MCENI) représenté par le Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GUINEE).

Référence de l'accord de financement : IDA : Crédit N° 74440GN

L'APPEL A MANIFESTATION D'INTERET POUR LE RECRUTEMENT D'UN (1) EXPERT EN DETECTION ET SUPERVISION DE SECURITE DANS LE CADRE DU PROJET DE MISE EN PLACE ET D'OPÉRATIONNALISATION DU CERT/SOC NATIONAL EN RÉPUBLIQUE DE GUINÉE

Date début : 14 Septembre 2026 **Date limité : 05 Octobre 2026**

Contexte et justification de la mission

Le Gouvernement de la République de Guinée a obtenu un financement de 60 millions de dollars $ de l'Association Internationale pour le Développement (IDA) pour financer le coût du Projet de Transformation Numérique pour l'Afrique/ Projet Régional d'Intégration Numérique de l'Afrique de l'Ouest (DTfA/WARDIP) placé sous la tutelle du Ministère de la Communication, de l'Economie Numérique et de l'Innovation (MCENI). Le Projet a l'intention d'utiliser une partie de ce montant pour effectuer les payements au titre du **recrutement d'un Expert en Détection et Supervision de Sécurité, chargé de renforcer les capacités opérationnelles du Security Operations Center (SOC) national.**

Objectif de la mission :

Sous l'autorité du Manager du CERT/SOC National, l'Expert en Détection et Supervision de Sécurité contribuera à la mise en œuvre, à l'exploitation et à l'optimisation des capacités de supervision, de détection et d'analyse des événements de sécurité du CERT/SOC National.

Son intervention s'inscrit dans les cinq piliers stratégiques du programme d'opérationnalisation du CERT/SOC National, avec une contribution particulière au renforcement des capacités SOC.

RESPONSABILITE PRINCIPALES

L'expert aura notamment pour responsabilités :

Supervision et analyse des alertes

- Assurer la surveillance permanente des événements de sécurité ;
- Analyser et qualifier les alertes issues du SIEM et des outils associés ;
- Identifier les incidents critiques et assurer leur escalade conformément aux procédures établies ;
- Réaliser les investigations initiales nécessaires à la qualification des incidents.

Détection et amélioration continue

- Concevoir, développer et maintenir les règles de détection ;
- Développer les cas d'usage SOC alignés sur MITRE ATT&CK ;
- Effectuer le tuning régulier des règles afin de réduire les faux positifs ;
- Optimiser les tableaux de bord et indicateurs SOC.

Threat Hunting

- Réaliser des activités régulières de recherche proactive de menaces ;
- Identifier des comportements suspects non détectés automatiquement ;
- Exploiter les IOC, TTP et informations CTI disponibles.

Documentation et reporting

- Produire les rapports d'analyse d'alertes ;
- Maintenir la documentation technique SOC ;
- Produire les tableaux de bord opérationnels ;
- Contribuer aux rapports mensuels d'activité.

Transfert de compétences

L'expert devra :

- Élaborer et mettre en œuvre un plan de transfert de compétences ;
- Travailler en co-traitement avec les analystes nationaux ;
- Assurer au minimum une session pratique hebdomadaire documentée ;
- Constituer une base documentaire comprenant :
    - Procédures ;
    - Fiches techniques ;
    - Règles de détection ;
    - Playbooks ;
    - Guides opérationnels.

Le Ministère de la Communication, de l'Economie Numérique et de l'Innovation (MCENI), représenté par le Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GN) invite les Consultants individuels à présenter leur candidature en langue française en vue de fournir les services décrits ci-dessus. **Les consultants intéressés doivent fournir les documents suivants : Cv détaillé, Copies des diplômes, Copies des certifications, Attestations de missions similaires, Références professionnelles vérifiables.**

QUALIFICATION ET EXPERIENCES REQUISES

Le candidat devra satisfaire aux exigences minimales suivantes :

Formation académique

- Être titulaire d'un diplôme de niveau **Bac+5** en cybersécurité, réseaux, systèmes d'information ou domaine équivalent.

Expérience professionnelle

Le candidat devra justifier :

- D'au moins **trois (03) années d'expérience professionnelle** dans la détection, l'analyse et la qualification des alertes de cybersécurité ;
- D'une expérience opérationnelle dans un environnement SOC, CERT, CSIRT ou centre de supervision de sécurité ;
- D'une expérience démontrée dans la mise en production ou la montée en charge d'une solution SIEM :
    - Intégration de sources ;

- Création de règles de corrélation ;
- Tuning ;
- Création de tableaux de bord ;
- Développement de cas d'usage.

Compétences techniques requises

Le candidat devra maîtriser :

- **Les solutions SIEM telles que :**
  - Splunk ;
  - ELK ;
  - IBM QRadar ;
  - Microsoft Sentinel ;
  - Ou solutions équivalentes ;
- **L'analyse des sources suivantes :**
  - Logs systèmes ;
  - Logs réseaux ;
  - EDR ;
  - Pares-feux ;
  - Équipements réseaux ;
- **Les mécanismes de normalisation des journaux :**
  - CEF (Common Event Format) ;
  - LEEF (Log Event Extended Format);
- Les mécanismes de parsing et d'intégration de sources hétérogènes dans un SIEM ;
- Les techniques de Threat Hunting basées sur :
  - Les IOC ;
  - Les TTP ;
  - MITRE ATT&CK ;
  - Les anomalies comportementales.

Compétences SOAR

- Le candidat devra avoir une connaissance des plateformes SOAR incluant :
- La conception de playbooks automatisés ;
- L'intégration avec les outils de ticketing ;
- L'orchestration des actions de réponse.

Certifications souhaitées

Les certifications suivantes seront fortement appréciées :

- CySA+ ;
- GCIA ;
- GMON ;
- GCIH ;
- CEH ;
- CISSP ;
- OSCP ;
- ou certifications équivalentes

Les critères d'éligibilité, l'établissement de la liste restreinte et la procédure de sélection seront conformes aux directives de sélection de consultants individuels de la Banque mondiale « Règlements pour la Passation des Marchés pour les Emprunteurs sollicitant le FPI » de la Banque mondiale édition septembre 2025.

Les candidats intéressés peuvent obtenir des informations supplémentaires au sujet des documents de référence (TDR) à l'adresse mentionnée ci-dessous et aux heures suivantes :
Du lundi au jeudi : de 9 heures à 16 heures 30 mn Le vendredi : de 9 heures à 13 heures.

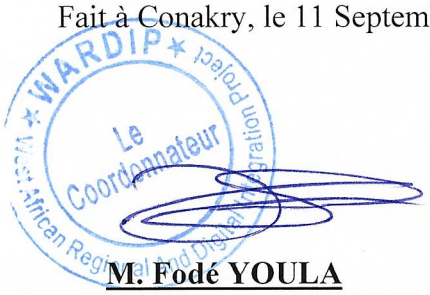
Les expressions d'intérêt doivent être déposées ou transmises par courriel à l'adresse mentionnée ci-dessous au plus tard le **05 Octobre 2026 à 16 h 00 mn GMT.** Les enveloppes doivent porter

expressément la mention « ***Manifestation d'intérêt pour le Recrutement d'un Expert en Détection et Supervision de Sécurité, chargé de renforcer les capacités opérationnelles du Security Operations Center (SOC) national*** ».

À l'attention de : Monsieur le Coordonnateur par intérim du Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GN).

L'adresse dont il est fait mention ci-dessus est : Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GN), Quartier Kaporo, Commune de Ratoma-Conakry, Immeuble BAH Kadiatou, référence la Société Easycom et à proximité du pont Kiridi, **E-mail : coordonnateur@wardip.gn cc spm@wardip.gn avec copie obligatoire à : assistant.spm@wardip.gn**

Fait à Conakry, le 11 Septembre 2026



M. Fodé YOULA
Coordonnateur du Projet WARDIP