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 CSIRT / REPONSE AUX INCIDENTS & FORENSIC 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 (1) Analyste CSIRT / Expert en Réponse aux Incidents et Investigation Forensique.**

Objectif de la mission :

Sous l'autorité du Manager du CERT/SOC National, l'Analyste CSIRT / Expert en Réponse aux Incidents et Investigation Forensique contribuera à la mise en œuvre, à l'exploitation et à l'amélioration continue des capacités nationales de gestion des incidents de cybersécurité.

Son intervention s'inscrit dans les cinq piliers stratégiques de l'opérationnalisation du CERT/SOC National.

RESPONSABILITE PRINCIPALES

L'expert aura notamment pour responsabilités :

Gestion opérationnelle des incidents

L'expert devra :

- Réceptionner et analyser les signalements d'incidents de cybersécurité ;
- Classifier les incidents selon leur criticité et leur impact ;
- Définir les priorités de traitement conformément aux procédures établies ;

- Coordonner les actions de réponse avec les équipes concernées ;
- Assurer le suivi des incidents jusqu'à leur résolution complète ;
- Produire les rapports de clôture et de retour d'expérience.

Investigation numérique et analyse forensic

L'expert devra :

- Réaliser des investigations techniques avancées sur les incidents majeurs ;
- Collecter, préserver et analyser les preuves numériques ;
- Garantir la traçabilité des éléments collectés (chaîne de conservation / chain of custody) ;
- Effectuer des analyses :
- Identifier :

Coordination de la réponse aux incidents

L'expert devra :

- Coordonner les actions ;
- Participer à la gestion des incidents à fort impact national ;
- Appuyer la prise de décision lors des cellules de crise cyber ;
- Préparer les éléments techniques nécessaires à la communication de crise.

Élaboration des procédures et playbooks

L'expert devra :

- Concevoir et maintenir les procédures CSIRT ;
- Développer des playbooks de réponse aux incidents ;
- Définir les processus ;
- Tester régulièrement les procédures à travers des exercices.

Exercices de simulation de crise cyber

L'expert devra :

- Concevoir des scénarios réalistes d'attaque ;
- Préparer les injects techniques et organisationnels ;
- Participer à l'animation des exercices tabletop ;
- Évaluer les réactions des parties prenantes ;
- Produire les rapports d'évaluation et plans d'amélioration.

Au moins **deux (02) exercices de simulation de crise cyber** devront être réalisés pendant la durée de la mission.

Transfert de compétences

L'expert devra :

- Assurer le coaching des analystes nationaux ;
- Organiser des sessions pratiques hebdomadaires ;
- Réaliser les investigations en co-traitement avec les équipes nationales ;
- Documenter les méthodes, outils et procédures ;
- Contribuer à la création d'une base de connaissances CSIRT.

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 MINIMALES

Le candidat devra satisfaire aux exigences minimales suivantes :

Formation académique

- Être titulaire d'un diplôme de niveau **Bac+5** en cybersécurité, informatique, réseaux, systèmes d'information ou domaine équivalent ;
- Justifier d'une formation spécialisée en réponse aux incidents, investigation numérique ou sécurité opérationnelle.

Expérience professionnelle

Le candidat devra justifier :

- D'au moins **trois (03) années d'expérience professionnelle** dans la gestion des incidents de cybersécurité, la réponse aux attaques informatiques ou les activités CSIRT/CERT ;
- D'une expérience pratique dans la conduite d'investigations numériques sur des incidents réels ;
- D'une expérience dans l'analyse forensic ;
- D'une expérience dans la rédaction de rapports d'incidents destinés à des décideurs techniques et non techniques ;
- D'une expérience de coordination avec plusieurs parties prenantes.

Une expérience dans un CERT national, CSIRT sectoriel, SOC d'entreprise ou centre opérationnel de sécurité sera fortement appréciée.

Compétences techniques requises

Le candidat devra maîtriser :

Réponse aux incidents

- Maîtrise du cycle de gestion des incidents :
  - Préparation ;
  - Détection et analyse ;
  - Confinement ;
  - Éradication ;
  - Récupération ;
  - Retour d'expérience
- Bonne connaissance des référentiels :
  - **NIST SP 800-61 Rev.3 Incident Response** ;
  - **ISO/IEC 27035 Gestion des incidents de sécurité de l'information** ;
  - **FIRST CSIRT Services Framework**.
- Capacité à définir et appliquer des procédures opérationnelles de réponse aux incidents.
- **Investigation numérique (Digital Forensics)**
- Le candidat devra maîtriser :

Forensic système

Analyse d'images disque ;

- Analyse mémoire (Memory Forensics) ;
- Recherche d'artefacts de compromission ;
- Analyse des journaux systèmes ;
- Reconstruction de chronologie d'événements.

Forensic Windows

Connaissance des principaux artefacts :

- Windows Event Logs ; Prefetch ; MFT ; Amcache ; Shimcache ; Registry ; LNK files ; Browser artifacts ; Powershell logs.

Forensic Linux

Maîtrise notamment :

- Logs système ; Journaux d'authentification ; Processus actifs ; Tâches planifiées ; Fichiers suspects ; Traces réseau.

Forensic réseau

Capacité à analyser :

- Captures réseau PCAP ; Flux réseau ; Traces DNS ; Communications suspectes ; Comportements anormaux.

Analyse Malware

Le candidat devra être capable de :

- Réaliser une analyse statique et dynamique de logiciels malveillants ; Identifier les mécanismes de persistance ; Analyser les comportements malveillants ; Extraire les IOC ; Identifier les TTP selon MITRE ATT&CK.

La connaissance d'outils tels que :

- Ghidra ; IDA ; Cuckoo Sandbox ; YARA ; VirusTotal Enterprise ; REMnux ;

Sera considérée comme un atout.

Outils d'investigation et de réponse

Le candidat devra avoir une expérience avec plusieurs outils parmi :

Forensic

- Autopsy / Sleuth Kit ; Volatility ; FTK ; EnCase ; Magnet AXIOM ; X-Ways Forensics

Analyse réseau

- Wireshark ; Suricata ; Zeek ; Tcpdump

Réponse aux incidents

- TheHive ; Cortex ; DFIR-IRIS ; Velociraptor ; Outils EDR/XDR

Threat Intelligence et MITRE ATT&CK

Le candidat devra :

- Identifier les techniques et tactiques utilisées par les attaquants ;
- Mapper les activités observées au framework MITRE ATT&CK ;
- Contribuer à l'enrichissement des bases CTI ;
- Transformer les enseignements issus des incidents en capacités de prévention et détection.

Certifications souhaitées

Les certifications suivantes constituent des atouts importants :

- GCIH (GIAC Certified Incident Handler) ;
- GCFA (GIAC Certified Forensic Analyst) ;
- GNFA (GIAC Network Forensic Analyst) ;
- GCFE (GIAC Certified Forensic Examiner) ;
- CHFI (Computer Hacking Forensic Investigator) ;
- CISM ;
- CISSP ;
- OSCP ;
- CREST CCT / CRT ;
- Ou toute certification équivalente.

Compétences complémentaires appréciées

Le candidat devra disposer des qualités suivantes :

- Excellente capacité d'analyse et de synthèse ;
- Capacité à travailler sous pression lors d'incidents majeurs ;
- Capacité de rédaction de rapports techniques et exécutifs ;
- Aptitude à coordonner plusieurs intervenants lors d'une crise cyber ;
- Capacité à expliquer des sujets techniques à des décideurs non techniques ;
- Sens élevé de la confidentialité et de la protection des informations sensibles.
- Une expérience dans la gestion de crise cyber nationale ou sectorielle, impliquant plusieurs institutions publiques ou opérateurs critiques, constituera un avantage significatif.

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 (1) Analyste CSIRT / Expert en Réponse aux Incidents et Investigation Forensique ».***

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