REPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie

Ministère des Postes
et Télécommunications

Projet d'accélération de la transformation numérique au Cameroun

Unité de gestion du projet

COOPERATION
Cameroon-World Bank
Cameroun-Banque mondiale

PATNUC

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

Ministry of Posts and
Telecommunications

Project for the Acceleration of Digital Transformation of Cameroon

Project Implementation Unit

AVIS DE SOLLICITATION A MANIFESTATION D'INTERET
N° 015/ASMI/MINPOSTEL/PATNUC/UGP/RC2/SPM/2025 POUR LA SELECTION D'UN CONSULTANT POUR LE RENFORCEMENT DES CAPACITES DES ENTITES DEDIEES A LA SECURITE DES RESEAUX, FORMATION A LA CERTIFICATION GIAC (GLOBAL INFORMATION ASSURANCE CERTIFICATION) DE L'ORGANISME SANS.

DATE : 01 OCT 2025

FINANCEMENT : IDA 69870-CM

1. CONTEXTE ET JUSTIFICATION

1.1. Contexte

Le Projet d'Accélération de la Transformation Numérique au Cameroun (PATNUC) qui résulte d'un accord entre le Gouvernement du Cameroun et la Banque mondiale a pour objectif d'accroître l'inclusion numérique et l'utilisation de solutions agricoles numériques par des petits exploitants agricoles acteurs des chaînes de valeur agricoles cibles. Ainsi, le PATNUC incarne l'approche de la transformation numérique, ciblant un secteur hautement stratégique pour le Cameroun tout en proposant de réformer le cadre règlementaire du secteur des Technologies de l'Information et de la Communication (TIC). Ce projet, avec son investissement dans la connectivité et les compétences numériques, soutient des interventions qui tirent parti des innovations numériques pour stimuler la croissance économique.

Le PATNUC est structuré autour de 4 composantes : (i) Stratégie, politique publique et réglementation numériques pour l'inclusion et la transformation numérique ; (ii) connectivité et inclusion numériques ; (iii) facilitation de l'implémentation des solutions numériques basées sur les données dans le secteur agricole ; et (iv) gestion du projet et l'engagement citoyen. Ainsi, le gouvernement à travers la SND30, ambitionne d'enclencher véritablement la transformation structurelle de l'économie camerounaise qui s'appuiera sur une modernisation du secteur agricole (agriculture, élevage, pêche et aquaculture) à travers l'amélioration de la productivité et la compétitivité des exploitations familiales agricoles et la promotion d'une dynamique d'industrialisation véritable.

La transformation digitale passera forcément par un renforcement de capacité des principaux acteurs du numérique dans l'écosystème camerounais. Le PATNUC à travers sa *Sous-composante 1.2 : Environnement propice pour des services numériques sûrs et résilients envisage financer des sessions de formation et programmes de renforcement des capacités, en particulier pour les entités de sécurité réseau dédiées telles que l'équipe d'intervention d'urgence informatique (CIRT) de l'Agence Nationale des Technologies de l'Information et le Communication (ANTIC) et les départements de sécurité informatique d'autres agences gouvernementales telles que la direction de la sécurité des réseaux et des systèmes d'information du MINPOSTEL.*

1.2. Justificatif de la mission

Le Décret n° 2012/512 du 12 novembre 2012 portant organisation du Ministère des Postes et télécommunications, confère à la direction de la sécurité des réseaux et systèmes d'informations du MINPOSTEL, la sécurisation des infrastructures critiques de l'Etat et des applications des Administrations

Publiques et des Collectivités Territoriales Décentralisées, en liaison avec les administrations et organismes concernés.

Par ailleurs, à la faveur **de la loi N°2010/012 du 21 décembre 2010**, L'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) s'est vue attribuée la responsabilité d'assurer la sécurité du cyberespace camerounais à travers des activités telles que la veille cybernétique assurée par son CIRT, les audits de sécurité, les investigations numériques, la cryptographie et la certification électronique.

Pour assurer ces missions au combien importantes et délicates, ces agences (DSR MINPOSTEL ET CIRT ANTIC) ont effectué ces dernières années, plusieurs vagues de recrutement d'ingénieurs IT relativement jeunes dont il est indispensable de renforcer les capacités opérationnelles, avec des indicateurs permettant d'apprécier leur évolution, afin d'assurer de manière plus efficace leurs missions au sein de ces structures.

Le PATNUC de concert avec lesdites structures ont conçu un programme de renforcement des capacités qui s'articule autour de quatre (04) cursus répartis chacun en trois (03) niveaux (débutant, professionnel et expert). Il s'agit du ***Forensic Investigation, Audit and Pentesting, Governance and Incident Management, Offensive security*** et ***Cyberintelligence and OSINT*** qui mettront l'accent sur les risques, les menaces et les stratégies d'atténuation de la violence en ligne à l'égard des femmes. Cela devrait contribuer de manière significative au renforcement de notre souveraineté numérique. Pour chacun de ces domaines et à différents niveaux, des formations pratiques certifiantes ont été identifiées par les parties prenantes il s'agit de :

1. Security Audit & Penetration Testing

Skill Level	Organization	Course Title	Description	Observation
Beginner	SANS	GIAC Security Essentials Certification (GSEC)	Validate foundational knowledge in information security, covering essential concepts and best practices	Base de formation
Intermediate	SANS	GIAC Certified Penetration Tester (GPEN)	Attest to the skills to perform penetration tests methodically, focusing on offensive techniques	Specialization
Intermediate	SANS	GIAC Web Application Penetration Tester (GWAPT)	Prove the ability to identify and exploit vulnerabilities specific to web applications	Specialization
Advanced	SANS	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	Validate in-depth expertise in exploit research and development, as well as advanced penetration testing	Expertise

2. Offensive Security (Threat Intelligence)

Skill Level	Organization	Course Title	Description	Observation
Beginner	SANS	GIAC Security Essentials Certification (GSEC)	Validate foundational knowledge in information security, covering essential concepts and best practices	Base de formation
Intermediate	SANS	GIAC Open-Source Intelligence (GOSI)	Validate the skills to effectively gather and analyze information from publicly available sources for intelligence purposes.	Specialization

Intermediate	SANS	GIAC Cyber Threat Intelligence	Certify the ability to produce and utilize cyber threat intelligence to understand threat actors and their campaigns.	Specialization

3. Governance and Incident Management

Skill Level	Organization	Course Title	Description	Observation
Beginner	SANS	GIAC Security Essentials Certification (GSEC)	Validate foundational knowledge in information security, covering essential concepts and best practices	Base de formation

Skill Level	Organization	Course Title	Description	Observation
Intermediate	SANS	GIAC Certified Incident Handler (GCIH)	Validate the in-depth knowledge and skills required to detect, respond to, and recover from security incidents.	Specialization
Intermediate	SANS	GIAC Strategic Management (GSM)	Certify the understanding of strategic security management principles and practices for organizational leadership.	Specialization

4. Forensic Investigations

Skill Level	Organization	Course Title	Description	Observation
Beginner	SANS	GIAC Security Essentials Certification (GSEC)	Validate foundational knowledge in information security, covering essential concepts and best practices	Base de formation

Tableau 1 : Besoins en formation GIAC des entités dédiées à la sécurité des réseaux.

2. OBJECTIFS DE LA MISSION

Le présent projet vise à permettre au personnel des entités dédiées à la sécurité des réseaux et CERT d'acquérir les compétences avancées pratiques nécessaires pour gérer, maintenir et sécuriser le cyberespace Camerounais. De manière spécifique, il s'agira de :

- Valider un contenu pédagogique et les objectifs y afférents en français et en anglais pointu et adapté aux menaces cyber actuelles et futures, permettant à la DSR MINPOSTEL et du CIRT ANTIC de remplir efficacement sa mission de protection du cyberspace national ;
- Définir un site de formation fixe pour la durée de la formation ;
- Définir et proposer un calendrier de formation pour toutes les ressources, tenant compte des différentes vagues de personnel devant participer à la formation ;
- Faire une évaluation optimale des coûts des différentes formations ;
- Assurer la mise à disposition de tout le matériel nécessaire pour la formation et des supports de formation

- Définir les modules de formation et une durée de formation optimale pour chaque module, garantissant une acquisition approfondie des compétences nécessaires à la lutte contre la cybercriminalité et à la sécurisation des infrastructures nationales et accompagner de sessions pratiques les différents modules abordés ;
- Doter les Ingénieurs de la DSR MINPOSTEL et du CIRT ANTIC d'aptitudes et de compétences leur permettant d'assurer de manière efficace les missions de veille cybernétique et de sécurisation des infrastructures critiques et assurer des travaux pratiques et étude de cas ;
- Doter les Ingénieurs du CIRT ANTIC et les entités dédiées à la sécurité informatique (la DSR du MINPOSTEL) d'aptitudes et de compétences leur permettant de réaliser de manière efficace les activités d'audit de sécurité et de tests d'intrusion et assurer des travaux pratiques et études de cas ;
- Doter les Ingénieurs de la DSR MINPOSTEL ET CIRT ANTIC d'aptitudes et de compétences leur permettant de réaliser de manière efficace les activités Cyberintelligence et de s'imprégner des techniques et tactiques de Open Source Intelligence (OSINT) et assurer des travaux pratiques et études de cas ;
- Assurer des évaluations formatives régulières pour s'assurer de la bonne acquisition des connaissances,
- Former et certifier cinq personnels en GIAC Reverse Engineering Malware (GREM) et Smartphone Forensic analysis in depth GASF certification et Advanced Open-Source Intelligence (OSINT) Gathering and Analysis à SANS INSTITUTE ;
- Veiller que la présence par participants et par modules soit supérieure ou égale à 90% (preuves : feuilles d'émargement et journaux de connexion aux labs) ;
- Veiller au suivi efficace afin d'atteindre le taux de réussite minimale acceptable de 70% dans les 120 jours suivant chaque session (preuves : certificats / e-mails des organismes) ;
- Payer la totalité des frais des deux formations et de certifications de niveau expert pour cinq cadres.
- Capaciter les cadres à l'analyse et à la compréhension des fonctionnalités d'un logiciel malveillant par des techniques de rétro-ingénierie
- Assurer la délivrance des attestations et certificats de compétences à tous les participants.

3. PORTEE DE LA MISSION

Il sera question de capaciter cinq (05) personnels en ligne sur deux formations à savoir :
- Smartphone Forensic analysis in depth GASF certification;
- Advanced Open-Source Intelligence (OSINT) Gathering and Analysis.

NB : Il n'est prévu aucun déplacement à l'étranger dans le cadre de cette prestation.

4. METHODOLOGIE

Dans une démarche pragmatique orientée vers les résultats, le centre de formation en liaison avec l'UGP et les parties prenantes devront sur la base des besoins de formations qui ont été exprimé arrêter un calendrier de formation qui permettra aux personnels de mieux cerner leur cursus et de pouvoir valider les examens de certifications GIAC.

Afin de faciliter une meilleure appropriation des connaissances dispensées, il serait indiqué que les apprenants bénéficient d'un environnement propice (matériel didactique, infrastructure réseau). A cet effet,

le Centre de formation devra apprêter des dispositifs logistiques permettant d'héberger les participants dans un environnement approprié, de les transporter et de les nourrir durant la durée de la formation.
Les consultants proposeront une méthodologie de mise en œuvre de cette activité. Toutefois, des séances de travail avec les responsables désignés pour le suivi de cette activité seront faites pour l'appropriation et la validation de la méthodologie proposée. Dans l'exécution de chacune des tâches prévues, il devra travailler de manière étroite avec ces responsables du suivi.

L'exécution de cette prestation se fera par un centre de formation agrée **SANS INSTITUTE.**

Il devra dans son offre de services :

- Disposer du personnel qualifié en fonction des modules de formation, ainsi que les ressources matérielles, logicielles et logistiques nécessaires ;
- Proposer les différents modules et méthodologie de la formation ;
- Justifier de son expérience et son expertise dans chacune des formations à dispenser.

Au cours de la réunion de cadrage, le consultant devra proposer la démarche à suivre selon une méthodologie bien détaillée dont les contenus seront envoyés et validés préalablement par le groupe de travail commis pour le suivi de cette activité, et qui devra comprendre :

- La mise à disposition de chaque participant du matériel approprié ordinateur performant pour suivre le cursus, simuler des ateliers pratiques sur les logiciels et les équipements réseaux et sécurité mettre en exergue dans des équipements réels en production préparer à cet effet (en cas d'impossibilité d'avoir accès au matériel adéquat pour des ateliers, le consultant devra soumettre des alternatives pertinentes).
- La fourniture de toute la documentation nécessaire à la formation :
- Les différentes formes clairement détaillées, sous lesquelles la formation se déroulera :
  - Cours théoriques (Exposés théoriques sur les technologies de transmission) ;
  - Ateliers pratiques (installation, configuration et maintenance des équipements) ;
  - Mise en situation et études de cas concrets (démonstrations et études de cas sur des scénarii réels de gestion et d'optimisation des réseaux) ;
  - Evaluations des acquis (exercices pratiques, mini test).

5. RESULTATS ATTENDUS

Aux termes de ces formations, les résultats attendus sont les suivants :

- Un contenu pédagogique en français et en anglais pointu et adapté aux menaces cyber actuelles et futures, permettant à la DSR MINPOSTEL et du CIRT ANTIC de remplir efficacement sa mission de protection du cyberspace national Validé ;
- Un site de formation fixe pour la durée de la formation est défini ;
- Une durée de formation optimale pour chaque module, garantissant une acquisition approfondie des compétences nécessaires à la lutte contre la cybercriminalité et à la sécurisation des infrastructures nationales ;
- Une évaluation optimale des coûts des différentes formations est effective ;
- Les Ingénieurs de la DSR MINPOSTEL et du CIRT ANTIC sont Dotés d'aptitude et de compétence leur permettant d'assurer de manière efficace les missions de veille cybernétique et de sécurisation des infrastructures critiques ;
- Le matériel nécessaire pour la formation et des supports de formation est mis à disposition ;

- Les modules de formation et une durée de formation optimale pour chaque module, garantissant une acquisition approfondie des compétences nécessaires à la lutte contre la cybercriminalité et à la sécurisation des infrastructures nationales et accompagner de sessions pratiques les différents modules abordés sont déterminés ;
- Les Ingénieurs des CIRT et DSR MINPOSTEL sont dotés d'aptitudes leur permettant de réaliser de manière efficace les activités D'investigations forensique ;
- Les frais des formations et de certifications de niveau expert pour cinq cadres sont payés ;
- Cinq personnels sont Formés et certifiés Smartphone Forensic analysis in depth GASF certification et Advanced Open-Source Intelligence (OSINT) Gathering and Analysis ;
- La totalité des frais de formation et de certification de niveau expert pour cinq cadres est payée ;
- L'analyse et la compréhension de la fonctionnalité d'un logiciel malveillant par des techniques de rétro-ingénierie sont maitrisés ;
- Le taux présence par participants et par modules d'au moins 90% est atteint ;
- Un taux de réussite d'au moins de 70% dans les 120 jours suivant chaque session (preuves : certificats / e-mails des organismes) est acquis.

6. DUREE DE LA MISSION

La formation en ligne est prévue pour une durée de 05 jours par formation :

- Smartphone Forensic analysis in depth GASF certification;
- Advanced Open-Source Intelligence (OSINT) Gathering and Analysis.

7. CONTENU DE LA FORMATION

Le consultant proposera les contenues jugée pertinente pour les deux (02) formations ci-dessus.

Afin de garantir le succès total des participants aux examens certifiants, les critères d'acception pour la validation de cette prestation sont les suivants :

- Présence ≥ 90 % (preuves : émargement, logs labs) ;
- Réussite examens ≥ 70 % (preuves : certificats) ;
- Complétion des labs ≥ 85 % (preuves : rapports plateforme) ;
- Satisfaction ≥ 4/5 (preuves : questionnaires agrégés) ;
- Inclusion : part des femmes ≥ 30 % (si possible) — liste agrégée.

8. DUREE DE LA MISSION

La durée de réalisation de la prestation est de 40 jours :

- 07 jours pour la tenue de la réunion de cadrage ;
- 05 pour la formation smartphone forensic analysis in depth ;
- 05 jours pour la formation Advanced open-source intelligence Gathering and analysis;
- 20 jours pour l'élaboration du rapport de suivi.

9. PROFIL DU CONSULTANT

9.1. Qualifications du centre de formation

Le cabinet ou groupement de cabinets sélectionné sera un centre de formation et de certification en cybersécurité ou une école de formation polytechnique spécialisée dans l'ingénierie informatique/télécom).

9.2. Profil du personnel

FL

Le cabinet devra respecter les exigences ci-après :

- Le personnel formateur du centre doit disposer **d'au moins cinq (05) ans d'expérience** dans le domaine de la cybersécurité et certifié **SANS** ou équivalent ;
- Le cabinet doit disposer du matériel nécessaire pour la réalisation des travaux pratiques afférents à la formation ;
- Les formateurs doivent avoir une maitrise de la langue anglaise ou française ;

Pour chacune des formations, le cabinet doit présenter un ou des experts certifiés dans la ***Smartphone Forensic analysis in depth GASF certification*** et ***Advanced Open-Source Intelligence (OSINT) Gathering and Analysis.***

10. METHODE DE SELECTION

Il est porté à l'attention des Consultants que les Cabinets ou Groupement de Cabinets/Bureau d'études seront sélectionnés selon la Méthode « **Sélection Fondée sur la Qualification des Consultants » (SQC) telle que décrite dans le Règlement de Passation des Marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI) de la Banque Mondiale édition de Novembre 2020.** La langue de travail est le français et l'anglais. Il est également porté à l'attention des Consultants que les dispositions relatives aux règles de la Banque Mondiale en matière de conflit d'intérêts sont applicables.

11. CONTENU DES MANIFESTATIONS À ADRESSER AU PATNUC

Le Coordonnateur National du Projet d'Accélération de la Transformation Numérique au Cameroun (PATNUC) invite, en vue d'élaborer la liste restreinte, les consultants admissibles à manifester leur intérêt à fournir les services décrits ci-dessus. Les cabinets/groupement de cabinets intéressés doivent fournir les informations (dépliants, brochures, etc.) indiquant qu'ils sont qualifiés pour exécuter les services. Cette manifestation rédigée en français ou en anglais devra contenir :

- Une lettre de manifestation d'intérêt datée et signée ;
- La justification du statut juridique du consultant
- La méthodologie de travail accompagnée d'un calendrier de mobilisation des experts impliqués ;
- Les pièces justificatives (copies des marchés similaires ou contrat, attestation de services fait, référence des experts) permettant la vérification des critères de sélection tel que présenté ci-dessus.

12. CONTACT ET INFORMATIONS SUPPLÉMENTAIRES

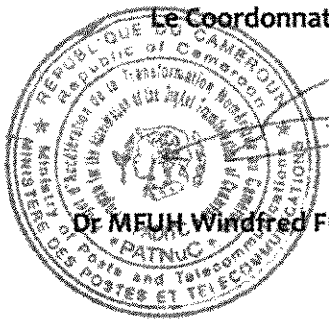
Les dossiers doivent parvenir au plus tard le 17 OCT 2025 à **16 heures** :

- Soit par courriel à : procurement@patnuc.cm avec copie à patnuc.composante1@patnuc.cm ; patnuccomposante1@gmail.com
- Soit déposés sous pli fermé en cinq (05) exemplaires (un original et quatre copies) à l'Unité de gestion du Projet, à la nouvelle route Bastos, derrière Tradex, bâtiment Ancien SNV. Tél. : +237 222 232 628. (Coordonnées géographiques : 3.88433, 11.51239) portant la mention :

« AVIS DE SOLLICITATION A MANIFESTATION D'INTERET N° 045/ASMI/MINPOSTEL/PATNUC/UGP/RC2/SPM/2025 POUR LA SELECTION D'UN CONSULTANT POUR LE RENFORCEMENT DES CAPACITES DES ENTITES DEDIEES A LA SECURITE DES RESEAUX, FORMATION A LA CERTIFICATION GIAC (GLOBAL INFORMATION ASSURANCE CERTIFICATION) DE L'ORGANISME SANS. »

Yaoundé le, 0 1 OCT 2025

Le Coordonnateur National du PATNUC



Dr MFUH Windfred FUAYE KENJI

Ampliations:
- PATNUC;
-ARMP;
- SOPECAM;
- ARCHIVES;
- AFFICHAGE.

NOTICE OF REQUEST FOR EXPRESSION OF INTEREST N° 015/ASMI/MINPOSTEL/PATNUC/UGP/RC2/SPM/2025 FOR THE SELECTION OF A CONSULTANT FOR CAPACITY BUILDING OF ENTITIES DEDICATED TO NETWORK SECURITY, TRAINING FOR GIAC (GLOBAL INFORMATION ASSURANCE CERTIFICATION) CERTIFICATION OF THE SANS ORGANIZATION.

DATE: 0 1 OCT 2025

FUNDING : IDA 69870-CM

1. CONTEXT AND JUSTIFICATION

1.1. Context

The Cameroon Digital Transformation Acceleration Project (PATNUC), which is the result of an agreement between the Government of Cameroon and the World Bank, aims to increase digital inclusion and the use of digital agricultural solutions by smallholder farmers involved in targeted agricultural value chains. PATNUC embodies the digital transformation approach, targeting a highly strategic sector for Cameroon while proposing to reform the regulatory framework for the Information and Communication Technology (ICT) sector. With its investment in connectivity and digital skills, this project supports interventions that leverage digital innovations to stimulate economic growth.

The PATNUC is structured around 4 components: (i) Digital strategy, public policy and regulation for inclusion and digital transformation; (ii) digital connectivity and inclusion; (iii) facilitation of the implementation of data-driven digital solutions in the agricultural sector; and (iv) project management and citizen engagement. Thus, the government, through the SND30, aims to truly initiate the structural transformation of the Cameroonian economy, which will be based on a modernization of the agricultural sector (agriculture, livestock, fisheries and aquaculture) through the improvement of the productivity and competitiveness of family farms and the promotion of a dynamic and genuine industrialization.

Digital transformation will necessarily involve capacity building for the main digital stakeholders in the Cameroonian ecosystem. PATNUC, through its Sub-component 1.2: Enabling Environment for Secure and Resilient Digital Services, plans to finance training sessions and capacity building programs, particularly for dedicated network security entities such as the Computer Emergency Response Team (CIRT) of the National Agency for Information and Communication Technologies (ANTIC) and the IT security departments of other government agencies such as the Directorate of Network and Information Systems Security of MINPOSTEL.

1.2. Justification of the mission

Decree No. 2012/512 of November 12, 2012, on the organization of the Ministry of Posts and Telecommunications, assigns the Network and Information Systems Security Directorate of MINPOSTEL the responsibility for securing critical state infrastructure and applications of Public Administrations and Decentralized Local Authorities, in liaison with the relevant administrations and organizations.

Furthermore, through Law No. 2010/012 of December 21, 2010, the National Agency for Information and Communication Technologies (ANTIC) was given responsibility for ensuring the security of Cameroon's

cyberspace through activities such as cyber monitoring conducted by its CIRT, security audits, digital investigations, cryptography, and electronic certification.

To ensure these very important and delicate missions, these agencies (DSR MINPOSTEL AND CIRT ANTIC) have carried out several waves of recruitment of relatively young IT engineers in recent years, whose operational capacities must be strengthened, with indicators allowing their development to be assessed, in order to more effectively ensure their missions within these structures.

PATNUC, together with the said structures, has designed a capacity building program that is structured around four (04) courses, each divided into three (03) levels (beginner, professional and expert). These are ***Forensic Investigation, Audit and Pentesting, Governance and Incident Management, Offensive security and Cyberintelligence and OSINT***, which will focus on the risks, threats and mitigation strategies of online violence against women. This should contribute significantly to strengthening our digital sovereignty. For each of these areas and at different levels, practical certification training courses have been identified by the stakeholders:

Security Audit & Penetration Testing

Skill Level	Organization	Course Title	Description	Observation
Beginner	SANS	GIAC Security Essentials Certification (GSEC)	Validate foundational knowledge in information security, covering essential concepts and best practices	Base de formation
Intermediate	SANS	GIAC Certified Penetration Tester (GPEN)	Attest to the skills to perform penetration tests methodically, focusing on offensive techniques	Specialization
Intermediate	SANS	GIAC Web Application Penetration Tester (GWAPT)	Prove the ability to identify and exploit vulnerabilities specific to web applications	Specialization
Advanced	SANS	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	Validate in-depth expertise in exploit research and development, as well as advanced penetration testing	Expertise

1. **Offensive Security (Threat Intelligence)**

Skill Level	Organization	Course Title	Description	Observation
Beginner	SANS	GIAC Security Essentials Certification (GSEC)	Validate foundational knowledge in information security, covering essential concepts and best practices	Base de formation
Intermediate	SANS	GIAC Open-Source Intelligence (GOSI)	Validate the skills to effectively gather and analyze information from publicly available sources for intelligence purposes.	Specialization
Intermediate	SANS	GIAC Cyber Threat Intelligence	Certify the ability to produce and utilize cyber threat intelligence to understand threat actors and their campaigns.	Specialization

2. **Governance and Incident Management**

56

Skill Level	Organization	Course Title	Description	Observation
Beginner	SANS	GIAC Security Essentials Certification (GSEC)	Validate foundational knowledge in information security, covering essential concepts and best practices	Base de formation

Skill Level	Organization	Course Title	Description	Observation
Intermediate	SANS	GIAC Certified Incident Handler (GCIH)	Validate the in-depth knowledge and skills required to detect, respond to, and recover from security incidents.	Specialization
Intermediate	SANS	GIAC Strategic Management (GSM)	Certify the understanding of strategic security management principles and practices for organizational leadership.	Specialization

3. Forensic Investigations

Skill Level	Organization	Course Title	Description	Observation
Beginner	SANS	GIAC Security Essentials Certification (GSEC)	Validate foundational knowledge in information security, covering essential concepts and best practices	Base de formation

Table 1: GIAC training needs of entities dedicated to network security.

2. OBJECTIVES OF THE MISSION

This project aims to enable staff of network security entities and CERTs to acquire the advanced practical skills needed to manage, maintain, and secure Cameroon's cyberspace.

Specifically, this will involve:

- Validating training content and related objectives in French and English that are specific and adapted to current and future cyber threats, enabling the MINPOSTEL DSR and the ANTIC CIRT to effectively fulfill their mission of protecting the national cyberspace;
- Defining a fixed training site for the duration of the training;
- Defining and proposing a training schedule for all resources, taking into account the different waves of personnel expected to participate in the training;
- Conducting an optimal cost assessment of the various training courses;
- Ensure the provision of all necessary training materials and hand-outs;
- Define training modules and an optimal training duration for each module, ensuring in-depth acquisition of the skills necessary to combat cybercrime and secure national infrastructure, and support the various modules covered with practical sessions;
- Equip engineers from the MINPOSTEL DSR and the ANTIC CIRT with the skills and competencies to effectively carry out cyber monitoring and critical infrastructure security missions, and provide practical work and case studies;

- Equip engineers from the ANTIC CIRT and the IT security entities (MINPOSTEL DSR) with the skills and competencies to effectively carry out security audits and intrusion tests, and provide practical work and case studies;
- Equip engineers from the MINPOSTEL DSR and ANTIC CIRT with the skills and competencies to effectively carry out cyberintelligence activities and to familiarize themselves with Open Source Intelligence (OSINT) techniques and tactics, and provide practical work and case studies;
- Conduct regular formative assessments to ensure proper knowledge acquisition,
- Train and certify five staff members in GIAC Reverse Engineering Malware (GREM) and Smartphone Forensic analysis in depth GASF certification and Advanced Open-Source Intelligence (OSINT) Gathering and Analysis at SANS INSTITUTE;
- Ensure that attendance per participant and per module is greater than or equal to 90% (evidence: attendance sheets and lab login logs);
- Ensure effective follow-up to achieve the minimum acceptable success rate of 70% within 120 days following each session (evidence: certificates/emails from organizations);
- Pay the full fees for the two expert-level training courses and certifications for five managers.
- rain managers in analyzing and understanding malware functionalities using reverse engineering techniques.
- Ensure the issuance of certificates and competency certificates to all participants.

3. SCOPE OF THE MISSION

The aim will be to train five (05) online staff members in two training courses:
- Smartphone Forensic Analysis in Depth GASF Certification;
- Advanced Open-Source Intelligence (OSINT) Gathering and Analysis.

Note: No travel abroad is planned within the framework of this service.

4. METHODOLOGY

In a pragmatic, results-oriented approach, the training center, in conjunction with the PMU and stakeholders, will establish a training schedule based on the training needs expressed. This will allow staff to better understand their curriculum and validate the GIAC certification exams.

To facilitate better appropriation of the knowledge provided, it would be advisable for learners to benefit from a suitable environment (teaching materials, network infrastructure). To this end, the training center will need to prepare logistic arrangements to accommodate participants in an appropriate environment, transport them, and provide them with food throughout the training.

The consultants will propose a methodology for implementing this activity. However, working sessions with the designated supervisors will be held to ensure the implementation and validation of the proposed methodology. In carrying out each of the planned tasks, the consultant will need to work closely with these supervisors. This service will be carried out by an approved training center **WITHOUT AN INSTITUTE.**

The consultant's Bid must include:
- Qualified personnel for the training modules, as well as the necessary hardware, software, and logistical resources;
- Propose the various training modules and methodology;

FB

- Demonstrate their experience and expertise in each of the training courses to be delivered.

During the scoping meeting, the consultant must propose the approach to be followed based on a detailed methodology, the content of which will be sent to and previously validated by the working group assigned to monitor this activity.

The methodology must include:

- Providing each participant with appropriate high-performance computer equipment to follow the curriculum, simulate practical workshops on network and security software and equipment, and highlight the use of actual production equipment. Prepare for this purpose (if adequate equipment is not available for workshops, the consultant must provide relevant alternatives).
- Providing all necessary training documentation:
- The various clearly detailed formats in which the training will be conducted:
  o Theoretical courses (theoretical presentations on transmission technologies);
  o Practical workshops (equipment installation, configuration, and maintenance);
  o Real-life scenarios and case studies (demonstrations and case studies on real-life network management and optimization scenarios);
  o Assessments of acquired knowledge (practical exercises, mini-tests).

5. EXPECTED RESULTS

The expected outcomes of these training courses are as follows:

- In-depth educational content in French and English, tailored to current and future cyber threats, enabling the MINPOSTEL Regional Directorate for Strategic Research (DSR) and the ANTIC Research and Training Centre (CIRT) to effectively fulfill their mission of protecting the national cyberspace. Validated;
- A fixed training site is defined for the duration of the training;
- An optimal training duration for each module, ensuring in-depth acquisition of the skills necessary to combat cybercrime and secure national infrastructure;
- An optimal cost assessment for the various training courses is effective;
- MINPOSTEL Regional Directorate for Strategic Research (DSR) and the ANTIC Research and Training Centre (CIRT) are equipped with the skills and competencies to effectively carry out cyber monitoring and critical infrastructure security missions;
- The necessary training equipment and training materials are provided;
- Training modules and an optimal training duration for each module are determined, ensuring in-depth acquisition of the skills necessary to combat cybercrime and secure national infrastructure, and supporting the various modules covered with practical sessions;
- MINPOSTEL CIRT and DSR engineers are equipped with the skills to effectively carry out forensic investigation activities;
- Expert-level training and certification fees for five managers are paid;
- Five staff members are trained and certified in Smartphone Forensic Analysis in depth (GASF certification) and Advanced Open-Source Intelligence (OSINT) Gathering and Analysis;

- All expert-level training and certification fees for five executives are paid;
- The analysis and understanding of malware functionality using reverse engineering techniques are mastered;
- An attendance rate of at least 90% per participant and per module is achieved;
- A success rate of at least 70% within 120 days following each session (evidence: certificates/emails from organizations) is achieved.

6. DURATION OF THE MISSION

The online training is scheduled to last five days per course:

- Smartphone Forensic Analysis in Depth (GASF Certification);
- Advanced Open-Source Intelligence (OSINT) Gathering and Analysis.

7. CONTENT OF THE TRAINING

The consultant will propose content deemed relevant for the two (02) training courses listed above.

To ensure the complete success of participants in the certification exams, the acceptance criteria for validation of this service are as follows:

- o Attendance ≥ 90% (evidence: attendance, lab logs);
- o Exam success ≥ 70% (evidence: certificates);
- o Lab completion ≥ 85% (evidence: platform reports);
- o Satisfaction ≥ 4/5 (evidence: aggregated questionnaires);
- o Inclusion: proportion of women ≥ 30% (if possible) — aggregated list.

8. DURATION OF THE MISSION

The service delivery period is 40 days:

- 7 days for the scoping meeting;
- 5 days for the in-depth smartphone forensic analysis training;
- 5 days for the Advanced Open-Source Intelligence Gathering and Analysis training;
- 20 days for the follow-up report.

9. CONSULTANT'S PROFILE

9.1. Training Center Qualifications

The selected firm or group of firms will be a cybersecurity training and certification center or a polytechnic training school specializing in IT/telecom engineering).

9.2. Personnel profile

The firm must meet the following requirements:

- The center's training staff must have at least **five (5) years of experience in the field of cybersecurity and be SANS certified or equivalent;**
- The firm must have the necessary equipment to carry out the practical work related to the training;
- Trainers must be fluent in English or French;

FL

For each training course, the firm must present one or more experts certified in **Smartphone Forensic analysis in depth GASF certification and Advanced Open-Source Intelligence (OSINT) Gathering and Analysis.**

10. METHOD OF SELECTION

Consultants are informed that the Firms or Groups of Firms/Consulting Firms will be selected using the **"Quality and Cost Based Selection" (QCBS) Method as described in the World Bank's Procurement Regulations for Borrowers Requesting Investment Project Financing (IPF), November 2020 edition.** The working language is French and English. Consultants are also informed that the provisions relating to the World Bank's rules on conflict of interest are applicable.

11. CONTENT OF BIDS ADDRESSED TO PATNUC

The National Coordinator of the Project for the Acceleration of Digital Transformation in Cameroon (PATNUC) invites eligible consultants to express their interest in providing the services described above to develop the shortlist. Interested firms/groups of firms must provide information (leaflets, brochures, etc.) indicating their qualifications to perform the services. This expression, written in French or English, must include:

- A dated and signed expression of interest letter;
- Proof of the consultant's legal status
- The work methodology accompanied by a schedule for mobilizing the experts involved;
- Supporting documents (copies of similar contracts or procurements, certificates of services provided, references from experts) to verify the selection criteria as presented above.

12. CONTACT AND ADDITIONAL INFORMATION

Applications must be submitted latest by 4 p.m. on the 17 OCT 2025 :

- Either by e-mail to: procurement@patnuc.cm with a copy to patnuccomposante1@gmail.com ; patnuc.composante1@patnuc.cm .
- Or submitted in a sealed envelope in five (05) copies (one original and four copies) to the Project Implementation Unit, at the nouvelle route Bastos, behind Tradex, former SNV building. Tel.: +237 222 232 628. (Geographical coordinates: 3.88433, 11.51239) marked:

« NOTICE OF REQUEST FOR EXPRESSION OF INTEREST N° 016/ASMI/MINPOSTEL/PATNUC/UGP/RC2/SPM/2025 FOR THE SELECTION OF A CONSULTANT FOR CAPACITY BUILDING OF ENTITIES DEDICATED TO NETWORK SECURITY, TRAINING FOR GIAC (GLOBAL INFORMATION ASSURANCE CERTIFICATION) CERTIFICATION OF THE SANS ORGANIZATION. »

Yaoundé the, 07 OCT 2025

The National Coordinator of PATNUC

Dr. MFUH Winifred FUAYE KENJI

Ampliations:
- PATNUC;
- ARMP;
- SOPECAM;
- ARCHIVES;
- NOTICE BOARD.