AVIS DE SOLLICITATION A MANIFESTATION D'INTERET
N° 014/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 EC-COUNCIL, PECB, VMWARE & ORACLE.

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, aussi compte tenue du projet de la mise en place des CIRT sectoriels (industrie, éducation, santé...) dont la phase d'étude finaliser en 2024 révèle la nécessité de capaciter le personnel de la DSR_MINPOSTEL dans la prévention, détection et réponse au incidents informatique .

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 attribuer 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 effectuées ces dernières années, plusieurs vagues de recrutement d'ingénieurs IT relativement jeunes.

Toutefois ces personnels pour assurer pleinement leurs missions dans un domaine aussi pointu et en constante évolution que la cybersécurité et dans lequel plusieurs spécialisations existent, il apparait indispensable de leur faire suivre un programme de formation pratique destiné à renforcer leurs capacités opérationnelles avec des indicateurs permettant d'apprécier leur évolution.

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*** et ***Offensive Security*** 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 tel qu'indiqué dans le tableau en annexe.

Pour chacun de ces domaines et à différents niveaux, des formations pratiques certifiantes ont été identifiées au cours des séances de travail avec ces entités :

- ✓ **Pour le profil Security Audit & Penetration Testing**

Skill Level	Organization	Course Title	Description	Observation
Beginner	EC-Council	Certified Ethical Hacker (CEH)	Understand hacking techniques to better defend, focusing on common attack tools and methodologies.	Base de formation
Beginner	PECB	ISO 270001 & ISO 270002 (Lead Auditor)	Acquire the skills to audit and implement an Information Security Management System (ISMS) compliant with ISO standards	Base de formation
Intermediate	EC-Council	EC-Council Certified Security Analyst (ECSA)	Develop the skills to analyze system and network security, going beyond simple vulnerability identification	Specialization
Advanced	EC-Council	EC-Council Certified Penetration Testing Professional (CPENT) / Licensed Penetration Tester (LPT)	Master advanced penetration testing techniques, including defense evasion and complex exploitation	Expertise

9 6

Advanced	Offensive Security (OffSec)	Offensive Security Experienced Penetration Tester	Demonstrate the ability to perform advanced penetration tests in an Active Directory environment, focusing on evasion and persistence.	Expertise

✓ **Offensive Security (Threat Intelligence)**

Skill Level	Organization	Course Title	Description	Observation
Beginner	EC-Council	Certified Ethical Hacker (CEH)	Understand hacking techniques to better defend, focusing on common attack tools and methodologies.	Base de formation
Beginner	PECB	ISO 270001 & ISO 270002 (Lead Auditor)	Acquire the skills to audit and implement an Information Security Management System (ISMS) compliant with ISO standards	Base de formation
Intermediate	EC-Council	Cyber Threat Intelligence Analyst (CTIA)	Develop the expertise to analyze threat data and produce actionable intelligence to inform security decisions.	Specialization
Advanced	Offensive Security (OffSec)	OSCP (Offensive Security Certified Professional)	Prove hands-on penetration testing skills by successfully compromising systems in a challenging lab environment.	Expertise

✓ **Governance and Incident Management**

Skill Level	Organization	Course Title	Description	Observation
Beginner	EC-Council	Certified Ethical Hacker (CEH)	Understand hacking techniques to better defend, focusing on common attack tools and methodologies.	Base de formation
Beginner	PECB	ISO 270001 & ISO 270002 (Lead Auditor)	Acquire the skills to audit and implement an Information Security Management System (ISMS) compliant with ISO standards	Base de formation

Skill Level	Organization	Course Title	Description	Observation
Intermédiaire	VMware	VMware Certified Professional Data Center Virtualization (VCP-DCV)	Aborde les aspects de virtualisation et de gestion d'un datacenter à l'aide des outils VMware	Intermediate
Intermédiaire	VMware	VMware Certified Professional Security (VCP-SEC)	Aborde les aspects de sécurité mis en œuvre à l'aide des outils VMware	Intermediate

4 1

Intermediate	EC-Council	Certified Incident Handler (ECIH)	Acquire the fundamental skills and knowledge to effectively handle and respond to security incidents.	Intermediate
Advanced	Oracle	Oracle Database 12c Administrator Certified Master	Aborde les notions avancées en administration des bases de données Oracle 12c	Expertise
Advanced	EC-Council	Certified Chief Information Security Officer (CCISO)	Recognize individuals with the knowledge and experience necessary to lead and manage an organization's information security program.	Expertise
Advanced	ISC2	Certified Information Systems Security Professional (CISSP)	Attest to a broad range of knowledge and expertise in information security, covering various domains.	Expertise

✓ **Forensic investigations**

Skill Level	Organization	Course Title	Description	Observation
Beginner	EC-Council	Certified Ethical Hacker (CEH)	Understand hacking techniques to better defend, focusing on common attack tools and methodologies.	Base de formation
Beginner	PECB	ISO 270001 & ISO 270002 (Lead Auditor)	Acquire the skills to audit and implement an Information Security Management System (ISMS) compliant with ISO standards	Base de formation

Skill Level	Organization	Course Title	Description	Observation
Intermediate	EC-Council	Computer Hacking Forensic Investigator (CHFI)	Develop the skills to investigate computer-based crimes, analyze digital evidence, and present findings in a legal context.	Specialization
Intermediate	Cloud Security Alliance	Certificate of Cloud Security Knowledge (CCSK)	Demonstrate a foundational understanding of cloud security principles and best practices.	Specialization

2. OBJECTIFS DE LA MISSION

2.1) Objectif global

Le présent projet vise à permettre au personnel des agences gouvernementales d'acquérir les compétences avancées pratiques nécessaires pour gérer, maintenir et sécuriser le cyberespace Camerounais.

2.2) Objectif spécifiques

De manière spécifique, il s'agira de :

- Prévoir des sessions de formation en français et en anglais en ligne un mois avant le début de chaque formation en présentiel ;
- Préparer les apprenants à assimiler les bases avant la formation intensive en présentiel ;

- Accompagner les apprenants via un encadrement interactif et individualisé ;
- Formés et certifier dix personnels au profil Security Audit & Penetration Testing ;
- Capacités et certifier dix personnels au profil Offensive Security (Threat Intelligence) ;
- Certifier dix personnels au profil Governance and Incident Management ;
- Renforcer les capacités et certifier cinq (05) personnels au profil Forensic Investigations ;
- Assurer un accompagnement post-formation personnalisé selon les besoins, Retours sur les chapitres critiques vus en formation, Accompagnement personnalisé selon les besoins ;
- Former à la sécurisation physique des infrastructures en réel sur des équipements physiques au centre de formation en présentiel, un aspect crucial de la protection globale du cyberspace national ;
- Doter les Ingénieurs de la DSR MINPOSTEL ET CIRT ANTIC d'aptitudes et de compétences leur permettant de réaliser de manière efficace les activités Cyber Intelligence et de s'imprégner des techniques et tactiques de Open Source Intelligence (OSINT) ;
- Mettre en place un calendrier de formation qui minimise l'impact sur les opérations courantes de la DSR-MINPOSTEL et du CIRT-ANTIC, tout en assurant une formation complète et opportune de l'ensemble du personnel concerné.
- Assurer une organisation logistique à sans faille pour permettre aux équipes de la DSR-MINPOSTEL et du CIRT-ANTIC de se concentrer pleinement sur leur apprentissage et leur développement de compétences ;
- Mettre en œuvre une évaluation rigoureuse des compétences acquises, permettant de mesurer l'impact de la formation sur la capacité de la DSR MINPOSTEL et CIRT ANTIC à détecter, analyser et répondre aux incidents de cybersécurité ;
- Proposer des recommandations pour des formations complémentaires, assurant une mise à niveau continue des compétences du personnel de la DSR-MINPOSTEL et du CIRT-ANTIC face à l'évolution constante des menaces ;
- Créer un environnement pratique réaliste pour permettre au personnel de la DSR-MINPOSTEL et du CIRT-ANTIC de développer des réflexes et des compétences opérationnelles directement applicables à la protection des infrastructures nationales ;
- Fournir à chaque participant de la DSR-MINPOSTEL et du CIRT-ANTIC les outils et ressources nécessaires pour participer activement à la formation et appliquer les connaissances acquises ;
- Former le personnel à assurer la disponibilité et la sécurité des réseaux de communication critiques pour l'État, une mission fondamentale de la DSR-MINPOSTEL et du CIRT-ANTIC ;
- Veiller que la présence par participants et par modules soit supérieure ou égale a 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, Complétion des laboratoires ≥ 85 % preuves : rapports plateforme, Satisfaction ≥ 4/5 preuves : questionnaires agrégés) ;
- Animer 04 ateliers pour la formation en présentiel des personnels et 01 atelier de restitution des travaux et de validation du rapport final (runbooks, preuves : PV signés + documents).

3. PORTEE DE LA MISSION

Il sera question de capaciter trente-cinq (35) personnes en ligne sur une période de seize (16) mois au Cameroun.

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 en formations qui ont été exprimés proposer un calendrier de formation qui permettra aux personnels de mieux cerner leur cursus et de pouvoir valider les examens de certifications.

Le centre de formation et l'UGP PATNUC devront si nécessaire, mieux structurer le déroulement des formations permettant d'obtenir les compétences précédemment identifiées ; chaque niveau correspondant à un ensemble de formations certifiantes à passer, les cursus seront constitués de trois (03) formations qui resteront ouvertes et accessible en ligne pour une durée de seize (16) mois.

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

Les consultants proposeront au besoin 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 au moins sur une des trois organismes **EC-Council, PECB,** ayant une expertise dans la Cybersécurité et la cybercriminalité.

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 méthodologies de la formation ;
- Justifier de son expérience.

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.

Dans sa démarche le consultant devra prendre en compte :

- La fourniture des kits techniques (ordinateurs, équipements réseau, logiciels avec licence) :

Il devra mettre à la disposition de chaque participant le matériel approprié performant pour suivre le cursus, simuler des ateliers pratiques sur les logiciels et les équipements réseaux et sécurité, mettre en application dans des équipements réels en production préparés 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 la documentation nécessaire à la formation :

Il devra mettre gratuitement à disposition des apprenants 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 présentiel sera organisée par le centre de formation avec l'accompagnement des experts qui viendront sur site pour dispenser les modules clés qui permettront les certifications complexes qui nécessitent des cas pratiques et un accompagnement quotidien sera organisée comme suite :

- Trente (30) jours sur les formations de Base en présentiel au Cameroun dans un site qui sera choisi et le reste en ligne ;
- Trente (30) sur les formations de spécialisation en présentiel au Cameroun dans un site qui sera choisi et le reste en ligne ;
- Trente (30) jours sur les formations de niveau expert en présentiel au Cameroun dans un site qui sera choisi et le reste en ligne.

Une fois les 30 jours de formation en présentiel terminés l'apprenant retournera pour reprendre service et des formations en lignes avec un suivi des experts seront ouvertes pour une durée de 16 mois couvrant la période de la convention.

7. CONTENU DE LA FORMATION

Outre les contenus jugés pertinents à l'issu de ses analyses et proposés par le consultant, les modules de formation devront inclure les aspects suivants :

7.1 Security Audit & Penetration Testing :

- Formation de base
  - Établir et régir des normes minimales pour l'accréditation des spécialistes professionnels de la sécurité de l'information dans les mesures de piratage éthique ;
  - Posséder les connaissances et les compétences pour auditer la conformité d'un SMSI suivant la norme ISO/IEC ;
  - Gestion et réponse des incidents, prévention de la perte de données, sécurité des appareils mobiles, analyse de vulnérabilité et test de pénétration.
- Formation de spécialisation
  - Fondamentaux de l'analyse du trafic et des protocoles d'application ;
  - Sécuriser les organisations grâce à des tests de pénétration et à une compréhension approfondie des problèmes de sécurité des applications Web ;
  - Analyser les résultats des outils d'hacking pour identifier et exploiter les vulnérabilités.
- Formation d'expert
  - Attaques Windows avancées, exploitation de vulnérabilités IoT/OT, pivotage double, contournement de réseaux filtrés ;
  - Écriture d'exploits (exploitation binaire), automatisation d'attaques via scripts, escalade de privilèges ;
  - Maitriser la création d'exploits pour des vulnérabilités complexes (débordements de pile, corruption mémoire) sur Windows et Linux35 ;
  - Apprendre à contourner les mécanismes de sécurité modernes (ASLR, DEP, canaris) sur les systèmes protégés ;
  - Évaluer et compromettre des systèmes configurés avec des mécanismes de sécurité renforcés (pare-feux, IDS/IPS, segmentation réseau) ;
  - Bypasser les protections modernes (chiffrement, sandboxing) pour identifier les vulnérabilités critiques ;
  - Exécuter des attaques organisées en minimisant les traces pour simuler des cyberattaques réalistes.

7.2. Offensive Security (Threat Intelligence) :

- Formation de base
  - Former des professionnels capables de détecter les failles de sécurité dans les systèmes et réseaux avant qu'elles ne soient exploitées par des hackers malveillants ;
  - Apprendre à imiter les techniques des hackers pour tester la sécurité des infrastructures tout en respectant un cadre légal et éthique ;
  - Utiliser les mêmes outils que les hackers malveillants pour effectuer des tests d'intrusion, analyser les risques, et protéger les systèmes ;
  - Aider les organisations à sélectionner et à mettre en œuvre les contrôles appropriés pour leur SMSI ;

g 6

- Aider les organisations à gérer les risques liés à la sécurité de l'information de manière efficace ;
- Acquérir des connaissances sur les architectures réseau, cryptographie, protocoles TCP/IP, et politiques de sécurité.

➢ Formation de spécialisation

- Collecter, analyser et rapporter des informations spécifiques à une organisation en utilisant des données publiques et des données de failles pour identifier et atténuer les risques ;
- Identifier les risques de confidentialité et d'intégrité lors des enquêtes OSINT et mettre en œuvre des meilleures pratiques de sécurité opérationnelle pour minimiser l'exposition et la vulnérabilité ;
- Utiliser des moteurs de recherche et une automatisation simple pour collecter, traiter et analyser des données et métadonnées de tailles et de formats variés ;
- Utiliser des cadres comme le **MITRE ATT&CK Framework** et le **Diamond Model** pour analyser les attaques ;
- Apprendre à planifier, collecter et analyser des données de renseignement provenant de sources diverses (OSINT, HUMINT, CCI) ;
- Maîtriser les techniques de collecte de données à partir de sources diverses (renseignement open source, flux de menaces, certificats TLS) ;
- Maîtriser les techniques d'analyse des données pour identifier les indicateurs de compromission (IoCs) ;
- Comprendre comment utiliser le pivoting pour élargir les collections d'intelligence et analyser les liens entre les données.

➢ Formation d'expert

- Identifier, exploiter et documenter les vulnérabilités dans des environnements réels ;
- Utiliser des outils et techniques offensifs pour évaluer la sécurité des systèmes et réseaux ;
- Travailler avec Kali Linux, exploiter des failles réseau, et effectuer des escalades de privilèges ;
- Maîtriser les concepts de TCP/IP, scripting (Python, Bash) et exploitation des vulnérabilités ;
- Adopter une approche structurée pour effectuer des tests d'intrusion en suivant les bonnes pratiques ;
- Comprendre les principes fondamentaux de la sécurité offensive pour anticiper les attaques.

7.3. Gouvernance and Incident Management :

➢ Formation de base

- Apprendre à rédiger des rapports détaillés sur les incidents pour améliorer la sécurité et la conformité ;
- Identifier et analyser les risques potentiels pour anticiper et atténuer les incidents ;
- Développer et mettre en œuvre des politiques de sécurité efficaces pour protéger les actifs informationnels ;
- Intégrer la gestion des risques dans la gouvernance de la sécurité pour minimiser les vulnérabilités ;
- Garantir la conformité avec les exigences légales et réglementaires en matière de sécurité de l'information ;
- Développer et mettre en œuvre des politiques et procédures de sécurité alignées avec les normes internationales ;
- Assurer la continuité des activités en mettant en place des plans de gestion des incidents et de reprise après sinistre ;

F C

- Planifier et mener des audits internes et externes pour évaluer la conformité du SMSI aux normes ISO 27001 ;
- Développer des compétences pour détecter, analyser et répondre efficacement aux cyberattaques et incidents de sécurité.

➢ Formation de spécialisation

- Apprendre à planifier, déclarer, contenir, éradiquer et récupérer après un incident ;
- Identifier et analyser les indicateurs de compromission pour détecter les incidents ;
- Assurer la conformité avec les lois et réglementations locales et internationales lors de la gestion des incidents ;
- Développer des plans pour assurer la continuité des activités en cas d'incident.

➢ Formation d'expert

- Comprendre et appliquer les cadres de gouvernance pour aligner la sécurité avec les objectifs organisationnels ;
- Identifier et analyser les risques liés à la sécurité pour atténuer les vulnérabilités ;
- Superviser les opérations de sécurité pour gérer efficacement les incidents et minimiser leur impact ;
- Tester les systèmes pour garantir leur résilience face aux cyberattaques ;
- Mettre en place des politiques et procédures pour détecter, contenir, éradiquer et récupérer après un incident.

7.4. Forensic Investigations :

➢ Formation de base

- Apprendre à détecter les empreintes laissées par les hackers après une intrusion afin d'analyser les mécanismes utilisés pour compromettre un système ;
- Maîtriser les techniques de collecte de preuves numériques tout en garantissant leur intégrité pour une utilisation dans des procédures légales ou judiciaires ;
- Identifier les techniques utilisées par les attaquants pour masquer leurs traces (anti-forensics) et développer des contre-mesures efficaces ;
- Analyser les fichiers malveillants pour comprendre leur fonctionnement, leur origine, et leur impact sur le système.

➢ Formation de spécialisation

- Utiliser des outils tels que les audit trails pour examiner les systèmes affectés et identifier les failles exploitées ;
- Identifier les techniques utilisées par les attaquants pour masquer leurs traces (anti-forensics) et développer des contre-mesures efficaces ;
- Comprendre les principes fondamentaux de la forensique numérique et son application dans les enquêtes ;
- Apprendre à suivre une approche méthodologique pour les enquêtes numériques, incluant la recherche, la saisie, la chaîne de possession, l'acquisition, la préservation, l'analyse et le rapport des preuves numériques ;
- Identifier et analyser les traces laissées par les attaquants pour reconstruire les incidents ;
- Utiliser des outils pour extraire et analyser les logs de divers appareils (proxy, pare-feu, IDS, etc ;
- Comprendre comment enquêter sur les incidents liés au Dark Web, à l'IoT et aux infrastructures cloud ;

- Apprendre à rédiger des rapports détaillés et juridiquement valables pour soutenir des actions judiciaires ;
- Maîtriser la forensique sur Windows, Linux et Mac pour analyser les systèmes compromis.

➢ Formation d'expert

- Comprendre les fondements de la forensique mobile et les techniques d'analyse des systèmes de fichiers des appareils mobiles ;
- Analyser le comportement des applications mobiles et identifier les artefacts liés aux événements ;
- Comprendre les méthodologies utilisées par Android et iOS pour la sauvegarde des appareils et le stockage en nuage, et comment analyser ces données ;
- Comprendre comment les malwares interagissent avec les appareils mobiles et utiliser des outils pour détecter et analyser les activités malveillantes ;
- Apprendre à analyser les systèmes de fichiers d'Android et iOS pour collecter et préserver les preuves numériques ;
- Identifier les emplacements courants des artefacts et les activités des utilisateurs sur ces appareils ;
- Examiner les mécanismes internes des malwares ciblant des plateformes courantes comme Microsoft Windows, les navigateurs web, et les fichiers exécutables protégés ;
- Identifier les caractéristiques communes des malwares, telles que les appels API, l'injection de code, et les techniques d'obfuscation ou de défense active.

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 ;
- Transfert : 4 ateliers + 2 runbooks livrés (PV + documents).

8. DUREE DE LA MISSION

La durée de réalisation de la prestation est de 480 jours :

- 30 jours de préformation en ligne ;
- 90 jours de formation en présentiel ;
- 360 jours des vouchers en ligne et de suivi post formation.

9. PROFIL DU CONSULTANT

Le cabinet ou groupement de cabinets sélectionné sera centre de formation et de certification en cybersécurité ou une école de formation polytechnique spécialisé dans l'ingénierie informatique/télécom **PECB Authorized Training Partners (ATP)** ou **autorisé par l'EC-Council (International Council of E-Commerce Consultants). Le cabinet doit justifier d'au moins une formation sur la cybersécurité en Afrique au cours des cinq (05) dernières années.** Le cabinet doit également justifier d'une expérience dans la formation d'une structure opérationnelle de cybersécurité (CIRT, SOC, etc.).

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 Qualité et le Coût** » **(SFQC) telle que décrite dans le Règlement de Passation des Marchés pour les Emprunteurs sollicitant le Financement de Projets**

FL

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°011/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° 044/ASMI/MINPOSTEL/PATNUC/UGP/RC2/SPM/2025 FOR THE SELECTION OF A CONSULTANT FOR CAPACITY BUILDING OF ENTITIES DEDICATED TO NETWORK SECURITY, TRAINING FOR EC-COUNCIL, PECB, VMWARE & ORACLE CERTIFICATION.

DATE : 01 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 require capacity building for key digital stakeholders in the Cameroonian ecosystem. PATNUC, through its Sub-component 1.2: Enabling Environment for Secure and Resilient Digital Services, plans to fund 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 to the Directorate of Network and Information Systems Security of MINPOSTEL the responsibility for securing the State's critical infrastructure and the applications of Public Administrations and Decentralized Territorial Authorities, in liaison with the relevant administrations and organizations, also taking into account the project to establish sectoral CIRTs (industry, education, health, etc.), the study phase of which, to be finalized in 2024, reveals the need to equip DSR_MINPOSTEL staff in the prevention, detection, and response to IT incidents.

Furthermore, under Law No. 2010/012 of December 21, 2010, the National Agency for Information and Communication Technologies (ANTIC) was given the responsibility of ensuring the security of Cameroonian cyberspace through activities such as cyber monitoring carried out by its CIRT, security audits, digital investigations, cryptography and electronic certification.

To carry out these critically important and sensitive missions, these agencies (DSR MINPOSTEL and CIRT ANTIC) have carried out several recruitments rounds of relatively young IT engineers in recent years.

However, to fully carry out these personnel's missions in a field as specialized and constantly evolving as cybersecurity, in which several specializations exist, it appears essential to provide them with a practical training program designed to strengthen their operational capabilities, with indicators to assess their progress.

PATNUC, in collaboration with these organizations, has designed a capacity-building program based on four (04) curricula, each divided into three (03) levels (beginner, professional, and expert). These are Forensic **Investigation, Audit and Pentesting, Governance and Incident Management**, and Offensive Security, which will focus on the risks, threats, and mitigation strategies of online violence against women. This should significantly contribute to strengthening our digital sovereignty. For each of these areas and at different levels, practical certified training courses have been identified as indicated in the table in the appendix.

For each of these areas and at different levels, practical certified training courses were identified during working sessions with these entities:

- ✓ **For the Security Audit & Penetration Testing profile**

Skill Level	Organization	Course Title	Description	Observation
Beginner	EC-Council	Certified Ethical Hacker (CEH)	Understand hacking techniques to better defend, focusing on common attack tools and methodologies.	Base de formation
Beginner	PECB	ISO 270001 & ISO 270002 (Lead Auditor)	Acquire the skills to audit and implement an Information Security Management System (ISMS) compliant with ISO standards	Base de formation
Intermediate	EC-Council	EC-Council Certified Security Analyst (ECSA)	Develop the skills to analyze system and network security, going beyond simple vulnerability identification	Specialization
Advanced	EC-Council	EC-Council Certified Penetration Testing Professional (CPENT) / Licensed Penetration Tester (LPT)	Master advanced penetration testing techniques, including defense evasion and complex exploitation	Expertise
Advanced	Offensive Security (OffSec)	Offensive Security Experienced Penetration Tester	Demonstrate the ability to perform advanced penetration tests in an Active Directory environment, focusing on evasion and persistence.	Expertise

✓ **Offensive Security (Threat Intelligence)**

Skill Level	Organization	Course Title	Description	Observation
Beginner	EC-Council	Certified Ethical Hacker (CEH)	Understand hacking techniques to better defend, focusing on common attack tools and methodologies.	Base de formation
Beginner	PECB	ISO 270001 & ISO 270002 (Lead Auditor)	Acquire the skills to audit and implement an Information Security Management System (ISMS) compliant with ISO standards	Base de formation
Intermediate	EC-Council	Cyber Threat Intelligence Analyst (CTIA)	Develop the expertise to analyze threat data and produce actionable intelligence to inform security decisions.	Specialization
Advanced	Offensive Security (OffSec)	OSCP (Offensive Security Certified Professional)	Prove hands-on penetration testing skills by successfully compromising systems in a challenging lab environment.	Expertise

✓ **Governance and Incident Management**

Skill Level	Organization	Course Title	Description	Observation
Beginner	EC-Council	Certified Ethical Hacker (CEH)	Understand hacking techniques to better defend, focusing on common attack tools and methodologies.	Base de formation
Beginner	PECB	ISO 270001 & ISO 270002 (Lead Auditor)	Acquire the skills to audit and implement an Information Security Management System (ISMS) compliant with ISO standards	Base de formation

Skill Level	Organization	Course Title	Description	Observation
Intermédiaire	VMware	VMware Certified Professional Data Center Virtualization (VCP-DCV)	Aborde les aspects de virtualisation et de gestion d'un datacenter à l'aide des outils VMware	Intermediate
Intermédiaire	VMware	VMware Certified Professional Security (VCP-SEC)	Aborde les aspects de sécurité mis en œuvre à l'aide des outils VMware	Intermediate
Intermediate	EC-Council	Certified Incident Handler (ECIH)	Acquire the fundamental skills and knowledge to effectively handle and respond to security incidents.	Intermediate
Advanced	Oracle	Oracle Database 12c Administrator Certified Master	Aborde les notions avancées en administration des bases de données Oracle 12c	Expertise

5 6

Advanced	EC-Council	Certified Chief Information Security Officer (CCISO)	Recognize individuals with the knowledge and experience necessary to lead and manage an organization's information security program.	Expertise
Advanced	ISC2	Certified Information Systems Security Professional (CISSP)	Attest to a broad range of knowledge and expertise in information security, covering various domains.	Expertise

✓ **Forensic Investigations**

Skill Level	Organization	Course Title	Description	Observation
Beginner	EC-Council	Certified Ethical Hacker (CEH)	Understand hacking techniques to better defend, focusing on common attack tools and methodologies.	Base de formation
Beginner	PECB	ISO 270001 & ISO 270002 (Lead Auditor)	Acquire the skills to audit and implement an Information Security Management System (ISMS) compliant with ISO standards	Base de formation

Skill Level	Organization	Course Title	Description	Observation
Intermediate	EC-Council	Computer Hacking Forensic Investigator (CHFI)	Develop the skills to investigate computer-based crimes, analyze digital evidence, and present findings in a legal context.	Specialization
Intermediate	Cloud Security Alliance	Certificate of Cloud Security Knowledge (CCSK)	Demonstrate a foundational understanding of cloud security principles and best practices.	Specialization

2. OBJECTIVES OF THE MISSION

2.1) Global objective

This project aims to enable government agency personnel to acquire the advanced practical skills needed to manage, maintain and secure Cameroonian cyberspace.

2.2) Specific objective

- Specifically, this will involve:
- Scheduling online training sessions in French and English one month before the start of each in-person training ;
- Preparing learners to master the basics before the intensive in-person training ;
- Supporting learners through interactive and personalized coaching;
- Training and certifying ten employees in the Security Audit & Penetration Testing profile;
- Capabilities and certifying ten employees in the Offensive Security (Threat Intelligence) profile;
- Certifying ten employees in the Governance and Incident Management profile;
- Building capacity and certifying five (05) employees in the Forensic Investigations profile;

§ 6

- Providing personalized post-training support as needed, including feedback on critical chapters covered in training and personalized support as needed;
- Provide training in real-life physical infrastructure security using physical equipment at the in-person training center, a crucial aspect of the overall protection of the national cyberspace;
- Equip MINPOSTEL and CIRT ANTIC DSR engineers with the skills and competencies to effectively carry out cyber intelligence activities and to become familiar with Open Source Intelligence (OSINT) techniques and tactics;
- Implement a training schedule that minimizes the impact on DSR-MINPOSTEL and CIRT-ANTIC's day-to-day operations, while ensuring comprehensive and timely training for all relevant personnel.
- Ensure seamless logistical organization to allow DSR-MINPOSTEL and CIRT-ANTIC teams to fully focus on their learning and skills development;
- Implement a rigorous assessment of acquired skills, allowing for the measurement of the impact of training on DSR-MINPOSTEL and CIRT-ANTIC's ability to detect, analyze, and respond to cybersecurity incidents;
- Propose recommendations for additional training, ensuring the continuous upgrading of DSR-MINPOSTEL and CIRT-ANTIC staff's skills in the face of constantly evolving threats;
- Create a realistic, practical environment to enable DSR-MINPOSTEL and CIRT-ANTIC staff to develop operational reflexes and skills directly applicable to the protection of national infrastructure;
- Provide each DSR-MINPOSTEL and CIRT-ANTIC participant with the tools and resources necessary to actively participate in the training and apply the knowledge acquired;
- Train staff to ensure the availability and security of critical communications networks for the State, a fundamental mission of DSR-MINPOSTEL and CIRT-ANTIC;
- Ensure that attendance by participants and by modules is greater than or equal to 90% (evidence: attendance sheets and lab connection 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, Laboratory completion ≥ 85% evidence: platform reports, Satisfaction ≥ 4/5 evidence: aggregated questionnaires);
- Lead 04 workshops for face-to-face training of staff and 01 workshop for the restitution of work and validation of the final report (runbooks, evidence: signed minutes + documents).

3. SCOPE OF THE MISSION

The goal will be to train thirty-five (35) people online over a period of sixteen (16) months in Cameroon.

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 PIU and stakeholders, will have to propose a training schedule based on the training needs that have been expressed, which will enable staff to better understand their course and to be able to validate the certification exams.

The training center and the PATNUC PMU will, if necessary, better structure the training program to achieve the previously identified skills. Each level corresponds to a set of certified training courses to be completed. The curricula will consist of three (03) training courses that will remain open and accessible online for a period of sixteen (16) months.

To facilitate better appropriation of the knowledge provided, it would be advisable for learners to benefit from a suitable environment (teaching materials, network infrastructure).

F6

The consultants will, if necessary, propose a methodology for implementing this activity. However, working sessions with the managers designated to monitor this activity will be held to ensure the appropriation and validation of the proposed methodology. In the execution of each of the planned tasks, the consultant will work closely with these monitoring managers.

The execution of this service will be carried out by a training center approved by at least one of the three organizations **EC-Council, PECB,** having expertise in Cybersecurity and cybercrime.

The consultant's service offering must include:

- ✓ Qualified personnel for the training modules, as well as the necessary hardware, software, and logistical resources;
- ✓ Propose the various training modules and methodologies;
- ✓ Demonstrate their experience.

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 oversee this activity.

In their approach, the consultant must take into account:

- ✓ Provision of technical kits (computers, network equipment, licensed software):

They must provide each participant with the appropriate, high-performance equipment to follow the curriculum, simulate practical workshops on network and security software and equipment, and implement them on real, specially prepared production equipment (if the appropriate equipment is not available for workshops, the consultant must submit relevant alternatives).

- ✓ Provision of the necessary training documentation:

They must provide learners with all the necessary training documentation free of charge.

- ✓ 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 test).

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;

FB

- 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;
- The training modules and an optimal training duration for each module, guaranteeing in-depth acquisition of the skills necessary for the fight against cybercrime and securing national infrastructures and supporting the different modules covered with practical sessions are determined;

- ✓ 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 covered;
- ✓ 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 managers are covered;
- ✓ Mastery of reverse engineering techniques in analyzing and understanding malware functionality;
- ✓ 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 in-person training will be organized by the training center with the support of experts who will come on-site to deliver the key modules that will enable complex certifications requiring practical cases. Daily support will be organized as follows:

- ✓ Thirty (30) days of basic training will be delivered in-person in Cameroon at a selected location, with the remainder delivered online;
- ✓ Thirty (30) days of specialized training will be delivered in-person in Cameroon at a selected location, with the remainder delivered online;
- ✓ Thirty (30) days of expert-level training will be delivered in-person in Cameroon at a selected location, with the remainder delivered online.

Once the 30 days of in-person training are completed, the learner will return to work, and online training with expert support will be available for a period of 16 months, covering the period of the agreement.

7. CONTENT OF THE TRAINING

In addition to the content deemed relevant following its analyses and proposed by the consultant, the training modules must include the following aspects:

7.1 Security Audit & Penetration Testing:

- ✓ Basic Training

o Establish and govern minimum standards for the accreditation of professional information security specialists in ethical hacking measures;

o Possess the knowledge and skills to audit the compliance of an ISMS according to ISO/IEC standards;

o Incident management and response, data loss prevention, mobile device security, vulnerability scanning, and penetration testing.

86

✓ Specialization Training

o Fundamentals of traffic analysis and application protocols;

o Securing organizations through penetration testing and a thorough understanding of web application security issues;

o Analyze the results of hacking tools to identify and exploit vulnerabilities.

✓ Expert Training

o Advanced Windows attacks, IoT/OT vulnerability exploitation, double-pivoting, bypassing filtered networks;

o Writing exploits (binary exploitation), automating attacks via scripts, and escalating privileges;

o Mastering the creation of exploits for complex vulnerabilities (stack overflows, memory corruption) on Windows and Linux35;

o Learning to bypass modern security mechanisms (ASLR, DEP, canaries) on protected systems;

o Evaluating and compromising systems configured with enhanced security mechanisms (firewalls, IDS/IPS, network segmentation);

o Bypassing modern protections (encryption, sandboxing) to identify critical vulnerabilities;

o Executing organized attacks while minimizing traces to simulate realistic cyberattacks.

7.2. Offensive Security (Threat Intelligence) :

➢ Basic Training

o Train professionals capable of detecting security vulnerabilities in systems and networks before they are exploited by malicious hackers;

o Learn to mimic hacker techniques to test infrastructure security while respecting a legal and ethical framework;

o Use the same tools as malicious hackers to perform penetration tests, analyze risks, and protect systems;

o Help organizations select and implement appropriate controls for their ISMS;

o Help organizations effectively manage information security risks;

o Acquire knowledge of network architectures, cryptography, TCP/IP protocols, and security policies.

➢ Specialisation Training

o Collect, analyze, and report organization-specific information using public and vulnerability data to identify and mitigate risks;

o Identify confidentiality and integrity risks during OSINT investigations and implement operational security best practices to minimize exposure and vulnerability;

o Use search engines and simple automation to collect, process, and analyze data and metadata of various sizes and formats;

o Use frameworks such as **the MITRE ATT&CK** Framework and the Diamond Model to analyze attacks;

o Learn how to plan, collect, and analyze intelligence data from various sources (OSINT, HUMINT, CCI);

o Master data collection techniques from various sources (open source intelligence, threat feeds, TLS certificates);

o Master data analysis techniques to identify indicators of compromise (IoCs);

o Understand how to use pivoting to expand intelligence collections and analyze relationships between data.

f 6

✓ Expert Training

o Identify, exploit, and document vulnerabilities in real-world environments;
o Use offensive tools and techniques to assess the security of systems and networks;
o Work with Kali Linux, exploit network vulnerabilities, and perform privilege escalations;
o Master the concepts of TCP/IP, scripting (Python, Bash), and vulnerability exploitation;
o Adopt a structured approach to performing penetration tests by following best practices;
o Understand the fundamental principles of offensive security to anticipate attacks.

7.3. Governance and Incident Management :

✓ Basic Training

o Learn how to write detailed incident reports to improve security and compliance;
o Identify and analyze potential risks to anticipate and mitigate incidents;
o Develop and implement effective security policies to protect information assets;
o Integrate risk management into security governance to minimize vulnerabilities;
o Ensure compliance with legal and regulatory information security requirements;
o Develop and implement security policies and procedures aligned with international standards;
o Ensure business continuity by implementing incident management and disaster recovery plans;
o Plan and conduct internal and external audits to assess ISMS compliance with ISO 27001 standards;
o Develop skills to effectively detect, analyze, and respond to cyberattacks and security incidents.

- Specialization Training

o Learn how to plan, report, contain, eradicate, and recover from an incident;
o Identify and analyze indicators of compromise to detect incidents;
o Ensure compliance with local and international laws and regulations during incident management;
o Develop plans to ensure business continuity in the event of an incident.

✓ Expert Training

o Understand and apply governance frameworks to align security with organizational objectives;
o Identify and analyze security risks to mitigate vulnerabilities;
o Oversee security operations to effectively manage incidents and minimize their impact;
o Test systems to ensure their resilience to cyberattacks;
o Implement policies and procedures to detect, contain, eradicate, and recover from an incident.

7.4. Forensic investigations:

- Basic Training
- o Learn how to detect the fingerprints left by hackers after an intrusion in order to analyze the mechanisms used to compromise a system;
- o Master digital evidence collection techniques while ensuring their integrity for use in legal or judicial proceedings;
- o Identify the techniques used by attackers to hide their tracks (anti-forensics) and develop effective countermeasures;
- Analyze malicious files to understand their operation, origin, and impact on the system

✓ Specialized Training

o Use tools such as audit trails to examine affected systems and identify exploited vulnerabilities;

o Identify the techniques used by attackers to hide their tracks (anti-forensics) and develop effective countermeasures;

o Understand the fundamental principles of digital forensics and its application in investigations;

o Learn to follow a methodological approach for digital investigations, including the search, seizure, chain of custody, acquisition, preservation, analysis, and reporting of digital evidence;

o Identify and analyze traces left by attackers to reconstruct incidents;

o Use tools to extract and analyze logs from various devices (proxies, firewalls, IDS, etc.);

o Understand how to investigate incidents related to the Dark Web, IoT, and cloud infrastructures;

o Learn to write detailed and legally valid reports to support legal actions;

o Master forensics on Windows, Linux, and Mac to analyze compromised systems.

✓ Expert Training

o Understand the fundamentals of mobile forensics and techniques for analyzing mobile device file systems;

o Analyze mobile application behavior and identify event-related artifacts;

o Understand the methodologies used by Android and iOS for device backup and cloud storage, and how to analyze this data;

o Understand how malware interacts with mobile devices and use tools to detect and analyze malicious activity;

o Learn how to analyze Android and iOS file systems to collect and preserve digital evidence;

o Identify common artifact locations and user activities on these devices;

o Examine the internal mechanisms of malware targeting common platforms such as Microsoft Windows, web browsers, and protected executable files;

o Identify common malware characteristics, such as API calls, code injection, and obfuscation or active defense techniques.

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

o Attendance ≥ 90% (evidence: sign-in, 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;
o Transfer: 4 workshops + 2 runbooks delivered (reports + documents).

8. DURATION OF THE MISSION

The service delivery period is 480 days:
- 30 days of online pre-training;
- 90 days of in-person training;
- 360 days of online vouchers and post-training follow-up.

F C

9. CONSULTANT'S PROFILE

The selected firm or group of firms will be a cybersecurity training and certification center or a polytechnic training school specializing in computer/telecom engineering **PECB Authorized Training Partners (ATP) or authorized by the EC-Council (International Council of E-Commerce Consultants). The firm must have at least one cybersecurity training course in Africa in the last five (05) years**. The firm must also have experience in training an operational cybersecurity structure (CIRT, SOC, etc.)

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.

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 patnuc.composante1@patnuc.cm ; patnuccomposante1@gmail.com.
- 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° 041/ASMI/MINPOSTEL/PATNUC/UGP/RC2/SPM/2025 FOR THE SELECTION OF A CONSULTANT FOR CAPACITY BUILDING OF ENTITIES DEDICATED TO NETWORK SECURITY, TRAINING FOR EC-COUNCIL, PECB, VMWARE & ORACLE CERTIFICATION. »

Yaoundé the, 01 OCT 2025

The National Coordinator of PATNUC

Dr. MFUH Windfred FUAYE KENJI

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