PRÉSIDENCE DE LA RÉPUBLIQUE

SECRETARIAT GENERAL

Projet de Gouvernance Digitale et de Gestion de l'Identité Malagasy
(PRODIGY)

Unité de Gouvernance Digitale (UGD)

Termes de référence pour le recrutement d'un(e) « Assistant(e) Technique Analyste en Sécurité des Systèmes »

1. Contexte et justification

Madagascar a reçu un financement de 133 millions de dollars américains, au travers du PROjet de Gouvernance DIgitale et de Gestion de l'Identité Malagasy (PRODIGY). Ce financement doit permettre la modernisation ainsi que la transformation de l'administration publique à travers le pays.

Cette transformation passe par la rationalisation et la numérisation des services publics qui constituent les bases de la composante 2 du projet. Il s'agit d'augmenter l'offre, la couverture et la qualité des services publics, en renforçant les infrastructures et la capacité de l'administration à fournir des services publics plus rapides, moins chers et de meilleure qualité.

Ainsi les objectifs principaux sont de renforcer la capacité du gouvernement à rationaliser et à fournir des services publics par le biais de canaux multiples (par exemple, en ligne, par la voix, hors ligne), et de fournir une infrastructure institutionnelle et technologique (back-end et front-end) soutenant la fourniture de services.

Madagascar a adopté une loi sur la protection des données en 2014 (loi n° 2014-038) et une législation plus récente relative à la cybersécurité et la cybercriminalité a été adoptée en 2016 (loi n° 2016-031 amendant la loi n° 2014-006).

Le gouvernement a l'obligation de garantir la sécurisation des données et de respect de la vie privée afin d'asseoir la confiance dans la fourniture des services digitaux publics et privés pour tous les utilisateurs et tous les citoyens.

Dans ce contexte, un(e) assistant(e) technique (AT) Analyste en Sécurité des Systèmes sera recruté(e) afin de renforcer et d'appuyer l'UGD pour la mise en place des actions nécessaires à la correction ou à l'anticipation des menaces informatiques et pour garantir la sécurité des solutions développées, avec l'appui du PROjet de gouvernance DIgitale et de Gestion de l'identité MalagasY (PRODIGY).

2. Objectif(s) de la mission

Sous la supervision du responsable chargé de la sécurité, l'AT Analyste en sécurité est en charge de surveiller des alertes, d'analyser les menaces et contribuer à la réponse efficace aux incidents de sécurité en collaborant avec les équipes techniques et de gestion. L'analyse de Sécurité contribue à la protection et à la défense de l'entreprise contre les menaces cybernétiques.

3. Étendue de la mission, tâches

Le/la consultant(e) fournira une assistance technique relativement aux activités suivantes :

Tâches principales :

- Mettre en place, configurer et maintenir les outils modernes de surveillance liés à sécurité des systèmes d'information
- Surveiller en temps réel les alertes générées par des outils de détection des intrusions et les systèmes de sécurité ;
- Analyser les alertes pour déterminer leur validité, leur criticité et leur impact potentiel ;
- Effectuer des investigations approfondies pour identifier les activités suspectes ou malveillantes ;
- Collaborer avec les autres équipes du SOC pour coordonner la réponse aux incidents de sécurité ;
- Produire (ou contribuer) des rapports d'analyse d'incident et des recommandations pour améliorer le niveau de sécurité ;
- Contribuer à l'amélioration continue des processus de détection et de réponse aux incidents ;
- Faire de la veille sur les tendances en matière de menaces et les développements de la cybersécurité ;
- Participer aux exercices de simulation d'incidents pour tester la préparation du SOC ;
- Assister les autres membres de l'équipe du SOC dans la formation et le coaching

Tâches secondaires

- Assister les analystes en réponse aux incidents de sécurité dans toutes leurs tâches
- Toutes autres tâches liées à la sécurité que la hiérarchie lui confie

4. Livrables attendus

- Dashboard mise à jour automatiquement des alertes et menaces ;
- Rapport sur les investigations menées, les préventions aux attaques et les actions liées à sécurité des systèmes

5. Critères de qualification du consultant

Le/la consultant(e) sera évalué(e) sur la base des critères suivants :

- Diplôme de licence en informatique, cybersécurité ou domaine connexes ;
- Trois (03) ans d'expériences cumulées dans le domaine de la sécurité des systèmes d'information
- Une expérience réussie en tant qu'analyste de sécurité ou dans un rôle similaire ;
- Une expérience réussie dans l'utilisation d'outils de sécurité tels que les systèmes de gestion des informations et des événements de sécurité (SIEM) ;
- Une expérience réussie en test de pénétration ;
- Excellentes compétences en résolution de problèmes et en prises de décision ;
- Capacité à travailler en équipe et à collaborer avec d'autres directions ;
- Aptitude à communiquer clairement les résultats de l'analyse et des recommandations ;
- Sens de l'initiative pour rester à jour sur les dernières tendances en matière de cybersécurité.

6. Rapports à fournir et Calendrier

Le consultant sera tenu de fournir un rapport d'activité mensuel en version électronique des activités réalisées conformément aux termes de référence.

7. Durée de la mission

La durée de la mission est estimée jusqu'au 30 juin 2026 sous réserve d'une évaluation satisfaisante des performances du/de la consultant(e) après six (06) mois puis de façon annuelle.

Le poste est basé à Antananarivo.