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 Réponse aux incidents de sécurité »

1. Contexte

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 Réponse aux incidents de sécurité sera recruté afin de renforcer et d'appuyer l'UGD pour gérer les incidents de sécurité, d'isoler les menaces et de coordonner les actions correctrices en collaboration avec les équipes techniques, 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 Réponse aux incidents de sécurité est chargé de gérer les différents incidents de sécurité, d'isoler les menaces, les attaques , les intrusions et de coordonner les actions correctrices en collaboration avec les équipes techniques.

3. Étendue de la mission, tâches

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

Tâches principales

- Collecter, évaluer et prioriser les incidents de sécurité signalés ou détectés ;
- Mener des enquêtes approfondies pour comprendre l'ampleur des incidents et leurs vecteurs d'attaques ;
- Mettre en œuvre avec l'équipe technique des mesures d'urgence pour contenir les impacts et empêcher leur propagation ;
- Coordonner la communication et la collaboration avec d'autres équipes internes ou externes ;
- Documenter les incidents, les actions prises et les leçons apprises pour l'amélioration continue ;
- Participer à la rédaction de rapports sur les incidents à destination des dirigeants de l'UGD ;
- Contribuer à la mise en place de processus et modes opératoires de réponse aux incidents ;
- Fournir une assistance technique et du coaching aux autres membres de l'équipe du SOC.

Tâches secondaires

- Assister les analystes en sécurité des systèmes 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 incidents de sécurité et leur status
- Rapport sur l'évolution et la correction des incidents de sécurité
- Document sur les éléments de langage pour l'équipe communication
- Document sur les modes opératoires pour le traitement des incidents de sécurité
- Document de procédure spécifique pour déclencher les mesures d'urgence

5. Critères de qualification du consultant

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

- un diplôme de licence en informatique, cybersécurité ou domaine connexe ;
- Trois (03) ans d'expérience cumulée dans le domaine de la sécurité des systèmes d'information
- Une expérience réussie dans la réponse aux incidents de sécurité ou rôles similaires ;
- Une expérience réussie sur des méthodologies de réponse aux incidents et des techniques de détection ;
- Une expérience réussie sur l'analyse de logiciels malveillants et en forensique numérique ;
- Une expérience réussie dans les domaines des réseaux et des protocoles de communication ;
- Aptitude à prendre des décisions rapides et éclairées pendant des situations critiques ;
- Capacité à travailler sous pression et à gérer plusieurs incidents simultanément.

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.