SYSTEME D'INFORMATION ET TRANSFORMATION DIGITALE

INTITULE DU POSTE :
Techniciens SI – Cyber-sécurité

INTITULE DU POSTE DU SUPERIEUR HIERARCHIQUE :
Chef de la Division Cyber-Sécurité

1. Finalité(s)

Contribuer à la protection du Système d'Information de l'Agence en participant à la mise en œuvre des dispositifs de cyber-sécurité, au maintien en conditions de sécurité des infrastructures, à la détection des incidents, ainsi qu'au respect des exigences du Système de Management de la Sécurité de l'Information (SMSI).

2. Missions

I. **Participer à l'exploitation des solutions de cyber-sécurité et au maintien en conditions de sécurité du Système d'Information ;**
II. **Contribuer à la surveillance, à la détection et au traitement des incidents de sécurité;**
III. **Participer à la mise en œuvre des exigences du SMSI, aux actions de conformité, et au veille technologique.**

3. Activités principales

I. **Participer à l'exploitation des solutions de cyber-sécurité et au maintien en conditions de sécurité du Système d'Information:**
- Assurer l'administration de premier niveau des équipements et solutions de sécurité (Firewall, EDR, Antivirus, VPN, NAC, SIEM, etc.) ;
- Participer au déploiement des solutions de sécurité informatique ;
- Réaliser les contrôles de sécurité périodiques des infrastructures ;
- Appliquer les procédures de durcissement (Hardening) des systèmes ;
- Participer à la gestion des correctifs de sécurité (Patch Management) ;

II. **Contribuer à la surveillance, à la détection et au traitement des incidents de sécurité :**
- Assurer la supervision quotidienne des événements de sécurité ;
- Analyser les alertes remontées par les outils de sécurité ;
- Participer aux investigations lors des incidents de sécurité ;
- Escalader les incidents nécessitant une expertise avancée ;
- Participer à la remédiation des vulnérabilités détectées ;

III. **Participer à la mise en œuvre des exigences du SMSI, aux actions de conformité, et au veille technologique.**
- Participer aux audits de sécurité et aux campagnes d'évaluation des vulnérabilités ;
- Contribuer au suivi des plans d'actions de sécurité ;
- Assurer une veille sur les nouvelles menaces et vulnérabilités ;

Direction Générale DCH ANP

4. Relations internes et externes

Relations internes

- Division Infrastructures;
- Division Transformation Digitale;
- Directions métiers ;
- Directions des Ports et Régions.

Relations externes

- Prestataires et intégrateurs ;
- Editeurs de solutions de sécurité ;
- Auditeurs ;
- Autres.

5. Profil requis

Formation de Référence Titulaire d'un diplôme de technicien spécialisé ou technicien supérieur délivré par un établissement public ou privé reconnu par l'Etat (Bac+2).
Spécialité : Cyber-sécurité, Réseaux Informatiques ; Systèmes et Réseaux.
Expérience : Deux (02) ans minimum dans le domaine des systèmes d'information.

6. Compétences

Savoir :

- Bonne connaissance des systèmes Windows et Linux ;
- Connaissance des réseaux TCP/IP et des protocoles de communication ;
- Connaissance des principes de sécurité des systèmes d'information ;
- Connaissance des solutions Firewall, VPN, Antivirus, EDR, NAC et SIEM ;
- Connaissance des outils d'analyse de vulnérabilités ;
- Connaissance des procédures de gestion des incidents de sécurité

Savoir-faire :

- Administrer les solutions de sécurité de premier niveau ;
- Analyser les journaux et les alertes de sécurité ;
- Diagnostiquer les incidents de sécurité ;
- Appliquer les procédures de remédiation.

Savoir- être :

- Sens de l'organisation, de rigueur et réactivité ;
- Capacité d'écoute et de communication.
- Esprit d'analyse ;
- Esprit d'équipe ;
- Capacité d'apprentissage et de veille technologique.