CADRE SENIOR

Dans le cadre de l'accompagnement de son développement, l'Office National des Chemins de Fer recrute un Cadre Sénior expérimenté pour le poste suivant :

Manager SOC

Rattaché à l'entité Cyber sécurité de la Direction des Systèmes d'Information et Digital, le titulaire du poste sera chargé des missions principales suivantes :

Principales missions du poste :

- Définir et faire évoluer la stratégie du SOC, assurer la cohérence technique et prendre en compte les exigences réglementaires ;
- Définir, mettre en œuvre, réviser et optimiser les processus et procédures du SOC ;
- Planifier et organiser les opérations quotidiennes du SOC ;
- Évaluer et valider l'efficacité des outils déployés dans le SOC et conduire les plans d'action correctifs ;
- Assurer un appui opérationnel à la gestion de crise de sécurité en cas d'incidents de sécurité majeurs ;
- Définir et mettre en œuvre les outils du SOC pour la collecte des évènements, l'accès aux plateformes de sécurité, la recherche d'événements suspects, la gestion des alertes, les workflows de suivi d'incidents de sécurité ;
- Alimenter la stratégie de détection à partir d'une vision globale de la nature et du niveau de vulnérabilité du SI ;
- Analyser les menaces spécifiques aux ICS et défendre les systèmes de contrôle industriels tout en donnant la priorité à la sécurité et à la fiabilité des opérations ;
- Définir et développer les playbooks pour une meilleure détection et réponse à un besoin spécifique.
- Prendre en compte les alertes de sécurité critiques (qualification, traitement, remédiation, forensic) ;
- Produire des indicateurs (KPI) / rapports en fonction des besoins SI et métiers spécifiques.

Profil recherché :

- Formation BAC +5 avec une spécialisation « Sécurité des Systèmes d'Information » ;
- Expérience au moins de 5 ans dans la sécurité SI, avec 2 ans minimum dans le SOC.

Compétences techniques exigées :

- Connaissance de la réglementation nationale, des bonnes pratiques et Standards de la Sécurité des systèmes d'information des deux environnements IT et OT : ISO 27001, NIST, IEC 62443...
- Bonne compréhension des risques Cyber en lien avec les processus métier de l'ONCF ;
- Bonnes connaissances des concepts de sécurité des systèmes d'information ;
- Maitrise des outils SOC type (SIEM, EDR, NDR, XDR ...) et techniques d'intrusion Endpoints/ Réseau ;
- Connaissances des solutions de sécurité de type Firewall, Sondes (IDS/IPS/…), VPN, AV, scanner des vulnérabilités, Gateway mail et web…
- Connaissances des système et applications (middleware, web, WAF) ;
- Connaissances en administration et architecture des environnements Windows & Linux ;
- Expérience probante dans les Technologies : Cisco, Fortinet, F5, Kaspersky …,
- Avoir des certifications reconnues en sécurité SI, est très souhaitable : GIAC, GSOC, CISSP, GCFA ou similaires ;
- La maîtrise de l'anglais technique est recommandée.

Compétences comportementales :

- Bonnes qualités relationnelles et managériales ;
- Disponibilité ;
- Esprit d'équipe, professionnalisme ;
- Sens de l'analyse et de curiosité ;
- Esprit de synthèse ;
- Résistance au stress et à la pression.

Les candidats intéressés par cette offre doivent renseigner leur candidature au plus tard le **25 Avril 2023** à **23H00** sur le lien suivant :

https://concours-recrutement.ma/offre-emploi-152.html-of=0

- **Seuls les diplômes délivrés par les établissements publics et ceux disposant d'attestation d'équivalence délivrée par les autorités compétentes seront éligibles.**
- **Le dossier de candidature doit comprendre les documents suivants :**
  - **Une copie conforme du diplôme**
  - **Une copie conforme de la carte d'identité nationale**
  - **Le CV actualisé**
  - **Attestation(s) de travail**
- **Tout dossier incomplet ou ne correspondant pas au profil recherché sera automatiquement écarté**
- **Renseigner la demande de candidature à travers le lien communiqué en haut**
- **Seules les candidatures reçues via internet seront traitées**