RECRUTEMENT D'UN INGENIEUR SECURITE DES SYSTEMES D'INFORMATION

Créée en juin 1989, la Société Nationale des Autoroutes du Maroc (ADM) est une société anonyme de droit privé, dont l'actionnariat est majoritairement public. Sa mission principale est de construire, exploiter et entretenir le réseau autoroutier qui lui est concédé par l'Etat. Aujourd'hui, ADM est concessionnaire d'un réseau d'autoroutes en exploitation de 1800 kilomètres.

Mission :
Contribuer à la protection du Système d'Information d'ADM en assurant le suivi opérationnel du dispositif de supervision et de détection de sécurité, et en constituant l'interface technique et opérationnelle entre ADM et le SOC (Security Operations Center) externalisé. Assurer le suivi de l'activité du SOC, l'exploitation et l'amélioration du SIEM, le suivi des alertes et incidents de sécurité, ainsi que la coordination avec les équipes techniques internes et les différents intervenants concernés. Contribuer également à l'amélioration continue de la qualité, de la couverture et de l'efficacité du dispositif de détection et de réponse aux incidents de sécurité.

Activités & Responsabilités :

1. Interface et suivi du SOC :
- Assurer le rôle de référent technique et opérationnel entre ADM et le SOC externalisé.
- Suivre l'activité du SOC et veiller au respect des niveaux de service définis.
- Assurer le suivi des alertes, événements et incidents remontés par le SOC.
- Coordonner les échanges entre le SOC et les équipes techniques internes concernées.
- Organiser et assurer le suivi des actions et demandes adressées au SOC.
- Participer aux points de suivi avec le SOC et assurer le suivi des actions décidées.
- Identifier les dysfonctionnements ou insuffisances dans le fonctionnement du dispositif et proposer les actions d'amélioration.
- Veiller à la bonne application des procédures d'escalade et de communication entre le SOC et ADM.

2. SIEM et supervision de sécurité :
- Assurer le suivi du bon fonctionnement et de la disponibilité du SIEM.
- Veiller à la bonne collecte et à la qualité des journaux de sécurité issus des différentes sources du SI.
- Suivre l'intégration des nouvelles sources de logs nécessaires à la couverture de supervision.
- Contribuer, en coordination avec le SOC, à l'évolution des règles de corrélation et des cas d'usage de sécurité.
- Identifier les besoins d'amélioration de la couverture de détection et contribuer à leur mise en œuvre.

3. Gestion et suivi des incidents de sécurité :
- Assurer le suivi des incidents de sécurité détectés et remontés par le SOC.
- Coordonner, lorsque nécessaire, les actions entre le SOC et les équipes techniques internes.
- Veiller au respect des procédures d'escalade et de traitement des incidents.
- Assurer le suivi des actions de remédiation jusqu'à la clôture des incidents.
- Participer aux analyses post-incident et aux retours d'expérience.
- Contribuer à l'amélioration des procédures et scénarios de réponse aux incidents.

4. Reporting et suivi de la performance du SOC
- Produire et maintenir les tableaux de bord relatifs à l'activité du SOC et à la supervision de sécurité.
- Suivre les principaux indicateurs du SOC : volume d'alertes, incidents, délais de prise en charge, délais de traitement, escalades, faux positifs, etc.
- Suivre les niveaux de service et les engagements contractuels du SOC.
- Identifier les tendances, anomalies ou points d'attention dans l'activité du SOC.
- Préparer les éléments de reporting nécessaires aux points de suivi avec le SOC et aux instances internes de sécurité.
- Assurer la traçabilité et le suivi des actions d'amélioration convenues avec le SOC.

Profil :
- Être titulaire d'un diplôme (Bac+5) d'ingénieur d'État en Cybersécurité, Sécurité des Systèmes d'Information, Informatique, Réseaux et Télécommunications, ou diplôme équivalent.
- Fraîchement diplômé (Promotion 2025 ou 2026), avec ou sans première expérience dans le domaine de la sécurité SI.

Compétences requises :
- Connaissances fondamentales en cybersécurité et en sécurité des systèmes d'information.
- Bonne compréhension du fonctionnement d'un SOC, des processus de supervision, de détection et de traitement des événements de sécurité.
- Connaissances des principaux mécanismes et technologies de sécurité : EDR/XDR, pare-feu, IDS/IPS, VPN, Proxy, antivirus, etc.
- Bonnes connaissances en réseaux et protocoles TCP/IP.
- Bonnes connaissances des environnements Windows et Linux.
- Connaissance des principaux référentiels et normes de sécurité SI, notamment ISO 27001, ISO 27002 et NIST
- Rigueur, curiosité technique, réactivité et capacité à monter rapidement en compétence.

Consistance du dossier de candidature :
Le dossier de candidature doit comprendre les documents suivants :
- Un CV actualisé ;
- Une lettre de motivation ;
- Une copie du ou des diplôme(s) ;
- Une copie des attestations de travail ;
- Une copie de la carte nationale d'identité.

L'avis d'appel à candidatures est publié sur les sites web www.adm.co.ma et emploi-public.ma. Les candidats doivent déposer leurs dossiers de candidature sur le site web https://adm.etalent.ma, **et ce au plus tard le 11 septembre 2026 à 23h59.**