INGENIEUR CYBERSECURITE & IT (H/F)

Qui sommes-nous ?

AMA est un éditeur d'applications de productivité sécurisées, conçues pour les travailleurs de terrain connectés. Expert de l'Intelligence Artificielle (IA) depuis 2017, nous la combinons avec des technologies de pointe telle que la réalité assistée (aR) pour permettre l'assistance à distance et la digitalisation des inspections et instructions de travail. Notre suite d'applications sécurisées XpertEye permet aux clients d'améliorer leur productivité, d'accélérer le temps de résolution, de conserver leurs connaissances et de réduire leur empreinte carbone.

Certifiés B Corp, nous sommes présents dans le monde entier, avec des bureaux en Europe, dans la région APAC et aux États-Unis.

Poste basé à Rennes (35).

Votre Rôle :

Vous jouerez un rôle clé dans la gestion, la maintenance et la sécurisation de nos infrastructures informatiques. Vous serez responsable de l'optimisation et de la protection des systèmes, des réseaux et des données contre les menaces internes et externes, tout en garantissant la disponibilité, la performance et la scalabilité des solutions IT. Vous viendrez également en appui de l'Administrateur Système et Réseau, pour l'administration quotidienne des systèmes et des réseaux.

Vos Missions :

<u>Responsabilités Cybersécurité</u>

- **Conception et mise en œuvre de solutions de sécurité** : pare-feu, systèmes de détection d'intrusions (IDS/IPS), anti-virus, VPN, etc.
- **Surveillance et analyse des systèmes** : détection des menaces et des anomalies, gestion des alertes de sécurité.
- **Audits de sécurité réguliers** : identification des vulnérabilités dans les infrastructures IT.
- **Réponse aux demandes et questionnaires clients** sur tous les sujets liés à la sécurité des infrastructures et des informations du produit XpertEye, y compris sur la partie IA.
- **Gestion des incidents de sécurité** : analyse des attaques potentielles, intervention rapide pour limiter les dommages, documentation des actions correctives et interagir avec le SOC.
- **Conformité aux normes** : veiller au respect des réglementations (RGPD, ISO 27001, etc.) et mise en place des politiques de sécurité internes.
- **Formation et sensibilisation** : participation à la formation des équipes sur les bonnes pratiques de sécurité informatique.
- **Veille technologique** : rester informé des dernières menaces et tendances en matière de cybersécurité.

Responsabilités IT

- **Gestion et administration des infrastructures IT** : maintenance des serveurs, des postes de travail et des systèmes de stockage.
- **Supervision et optimisation des réseaux** : assurer la disponibilité et la performance des réseaux LAN, WAN, VPN, etc.
- **Gestion des bases de données** : assurer leur sécurité, disponibilité, sauvegarde et restauration.
- **Support technique** : assistance de niveau 2 ou 3 aux utilisateurs et résolution des problèmes techniques.
- **Gestion des environnements cloud** : déploiement, administration et optimisation des services dans des environnements Cloud (AWS, Azure).
- **Virtualisation** : gestion des infrastructures virtualisées (VMware, Kubernetes, etc.).
- **Mise en place et gestion des politiques de backup et de restauration**.
- **Gestion des projets IT** : participation à la planification et à l'exécution de projets d'amélioration ou de mise à jour de l'infrastructure informatique.

Profil recherché :

- **Formation :** Diplôme d'ingénieur ou Master en informatique, cybersécurité, ou domaine connexe. Certifications en cybersécurité et IT appréciées (CISSP, CEH, CISM, ITIL, etc.).
- **Expérience** : Expérience professionnelle d'au moins 3-5 ans dans un poste similaire couvrant à la fois des responsabilités cybersécurité et IT
- **Qualités personnelles :** Esprit analytique et rigoureux, capacité à résoudre les problèmes rapidement, excellente communication, capacité à vulgariser des sujets techniques, capacité à travailler sous pression et à gérer plusieurs projets simultanément, autonomie, organisation et esprit d'équipe.

Compétences requises :

- **Maîtrise des environnements systèmes** : Windows, Linux, Unix.
- **Expertise en réseaux** : protocoles (TCP/IP, DNS, DHCP), routage, switching, sécurité des réseaux.
- **Connaissances en cybersécurité** : firewalls, SIEM, systèmes IDS/IPS, DLP, cryptographie, etc.
- **Expérience en virtualisation et en cloud computing** (AWS, Azure).
- **Maîtrise des outils de gestion des bases de données** (SQL, NoSQL).
- **Compétences en scripting et automation** (PowerShell, Python, Bash).
- **Connaissances des normes de sécurité** (ISO 27001, NIST).
- **Anglais professionnel**