I-TRACING
CYBERSECURITY EXPERT

Ingénieur MCO CyberSOC CDI (H/F)

Au sein de nos locaux, ta mission principale consiste à assurer le maintien en condition opérationnelles et en condition de sécurité des architectures de nos services managés de cyberdéfense : CyberSOC, CERT et Centre de Gestion des Vulnérabilités.

A ce titre, tu assures le lien entre l'administration, l'exploitation des infrastructures et les utilisateurs des services et applications supportées (analystes CyberSOC, CERT et vulnérabilités, SOC managers, data scientists, etc.).

Tes activités incluent :

- La mise en œuvre et l'exploitation des mécanismes de supervision permettant de garantir le bon fonctionnement des architectures : applications, interconnexions réseau, systèmes et middlewares,
- Le capacity planning, la maintenance évolutive et corrective d'architectures incluant notamment les briques de collecte et d'analyse des logs (SIEM), les référentiels de threat-intelligence, les outils d'analyse de malware, outils analytics/big data, des environnements Cloud, etc.
- Le maintien en condition de sécurité et conformité : gestion des mises à jour, contrôle d'accès, cloisonnement réseau, sauvegardes et continuité d'activité, etc.
- La rédaction et mise à jour de la documentation
- La gestion du plan d'amélioration continu partagé entre les utilisateurs de la Direction Cyberdéfense et les équipes en charge de l'Infrastructure Interne.

Au-delà des compétences techniques, ton principal challenge est de concilier les besoins dynamiques des analystes (liés aux évolutions des menaces et des contre-mesures, aux engagements de service pris auprès de nos clients et les contraintes d'exploitation internes).

Comment savoir si je peux vous rejoindre ?
Si tu as des capacités en :

- Sécurité des systèmes Windows, Linux/Unix,…, virtualisation (VMware), PKI, …
- Réseaux, sécurité TCP/IP et services IP : DNS, Proxy, NAC, DHCP, LDAP, etc.), solutions de rebond,
- Sécurité : firewall, load balancer, WAF, IDS/IPS, Deep Packet Inspection, chiffrement, SIEM, authentification, sécurité bases de données, pen testing, vulnérabilités, DLP, protection DDoS,…
- Une appétence pour les petits développements
- La connaissance du Log Management est un plus (Splunk, ELK, QRadar, etc.)

Et que tu es :

- De niveau bac +4/5 et justifiant d'une expérience dans le domaine de la sécurité, des systèmes et des réseaux IP.
- Dynamique, curieux(se) et en veille technologique permanente,

Alors n'hésites plus et rejoins Sébastien, Daniel et leur équipe pour continuer de grandir avec nous !

Poste situé à Puteaux, en plein centre-ville dans des locaux avec vue sur la Défense
Rémunération : attractive et selon ton niveau d'expertise
Participation et primes exceptionnelles selon votre investissement