

FICHE DE POSTE :

Intitulé du poste	Chef de Service «Infrastructure, Sécurité et Assistance»
Rattachement hiérarchique	Chef de Division Systèmes d'Information et de la Digitalisation
Missions et responsabilités	<p><b>Mission principale</b></p> <ul style="list-style-type: none"> <li>- Assurer la disponibilité, la performance, la sécurité et la continuité des infrastructures matérielles et logicielles de l'organisation.</li> <li>- Garantir la conception, l'évolution et la maintenance des systèmes et réseaux, dans le respect des niveaux de service et des exigences métiers.</li> <li>- Gérer les incidents, demandes de service, changements et assurer le lien opérationnel avec les utilisateurs métiers, dans une logique d'amélioration continue.</li> </ul> <p><b>Responsabilités principales :</b></p> <ol style="list-style-type: none"> <li><b>1. Architecture et gestion des infrastructures</b> <ul style="list-style-type: none"> <li>- Concevoir, maintenir et optimiser les architectures réseau, serveurs, stockage, virtualisation, bases de données, etc.</li> <li>- Définir les normes et standards techniques, documenter l'architecture des composants.</li> <li>- Assurer la gestion des actifs (serveurs, postes, licences, équipements réseau).</li> </ul> </li> <li><b>2. Supervision et exploitation</b> <ul style="list-style-type: none"> <li>- Assurer la supervision proactive des équipements et services (applicatifs, serveurs, réseaux).</li> <li>- Gérer les incidents techniques de niveau 1/2.</li> <li>- Maintenir un niveau de performance optimal des systèmes et infrastructures.</li> <li>- Suivre les tâches récurrentes d'exploitation (sauvegardes, batchs, ...).</li> <li>- Surveiller les seuils d'alerte, générer les rapports d'état des services.</li> </ul> </li> <li><b>3. Disponibilité, capacité et continuité</b> <ul style="list-style-type: none"> <li>- Analyser les niveaux de disponibilité et la capacité (CPU, RAM, bande passante, etc.).</li> <li>- Élaborer et tester les plans de reprise d'activité (PRA) et plans de continuité (PCA).</li> <li>- Collaborer avec la sécurité IT sur les dispositifs de résilience.</li> </ul> </li> <li><b>4. Gestion des incidents et problèmes</b> <ul style="list-style-type: none"> <li>- Résoudre les incidents dans les délais convenus (SLA).</li> <li>- Analyser les causes racines des problèmes récurrents.</li> <li>- Documenter les solutions et procédures (base de connaissance).</li> </ul> </li> <li><b>5. Automatisation et industrialisation</b> <ul style="list-style-type: none"> <li>- Déployer des outils d'automatisation de l'infrastructure.</li> <li>- Participer à l'intégration continue et à la mise en place d'environnements reproductibles.</li> </ul> </li> <li><b>6. Support aux projets et évolutions techniques</b> <ul style="list-style-type: none"> <li>- Fournir les environnements nécessaires aux projets de développement.</li> <li>- Participer aux comités d'architecture technique.</li> </ul> </li> </ol>



	<ul style="list-style-type: none"> <li>- Accompagner les évolutions Cloud/hybrides.</li> </ul> <p><b>7. Sécurité opérationnelle</b></p> <ul style="list-style-type: none"> <li>- Sécurité : EDR/XDR (SentinelOne, Defender ATP), SIEM, MFA, DLP, PKI, chiffrement, durcissement</li> <li>- Réseaux sécurisés : VLAN, VPN IPsec, filtrage, reverse proxy, firewall (Fortinet, Palo Alto)</li> <li>- Audit &amp; conformité : ISO 27001/27002, gestion des vulnérabilités, RGPD</li> <li>Surveillance &amp; détection : journaux</li> </ul>
<p><b>Compétences et qualifications requises</b></p>	<p><b>Formation :</b></p> <ul style="list-style-type: none"> <li>- Formation : Bac+5 en systèmes, réseaux, ou sécurité informatique</li> <li>- Minimum 5 ans minimum dans un poste similaire</li> </ul> <p><b>Certifications souhaitées</b></p> <ul style="list-style-type: none"> <li>- Windows Server Hybrid Administrator Associate</li> <li>- EC Council Disaster Recovery Professional V2 EDRP</li> <li>- VMware VCP ou equivalent</li> <li>- Cisco Certified Network Associate (CCNA) ou CCNP Enterprise</li> <li>- ISO/CEI 27001 ET ISO/CEI 27002 Foundations</li> </ul> <p><b>Compétences techniques :</b></p> <ul style="list-style-type: none"> <li>- Systèmes : Windows Server, Active Directory, GPO, PKI</li> <li>- Réseaux : TCP/IP, VLAN, VPN, DNS, DHCP, firewalling, SD-WAN</li> <li>- Supervision : Zabbix, Centreon, ...</li> <li>- Sauvegarde &amp; Stockage : Veeam,, SAN/NAS</li> <li>- Virtualisation : VMware vSphere.</li> <li>- Automatisation : Ansible, PowerShell.</li> <li>- Sécurité : Antivirus/EDR/XDR (CrowdStrike, SentinelOne, Defender ATP), MFA, journaux, SIEM</li> <li>- La connaissance des logiciels de réglementation des laboratoires serait un atout</li> </ul> <p><b>Comportementales :</b></p> <ul style="list-style-type: none"> <li>- Réactivité et rigueur</li> <li>- Capacité d'analyse et de diagnostic</li> <li>- Communication claire avec les équipes métiers et projets</li> <li>- Sens du service client</li> </ul> <p><b>Langues :</b></p> <ul style="list-style-type: none"> <li>- Maîtrise de l'arabe et du français.</li> <li>- La maîtrise de l'anglais sera un atout.</li> </ul>
<p><b>Conditions de travail</b></p>	<ul style="list-style-type: none"> <li>- Lieu : Rabat (avec des déplacements à prévoir)</li> <li>- Emploi contractuel.</li> </ul>

