Responsable Infrastructure & Sécurité (H/F)

Fondation Bordeaux Université – IHU LIRYC

Contexte	L'IHU Liryc (Institut des Maladies du Rythme cardiaque) recrute un(e) Responsable Infrastructure & Sécurité. Liryc est un Institut Hospitalo-Universitaire (IHU) avec une quadruple mission de recherche, de soin, d'innovation et d'enseignement, au service du patient. Il a pour vocation de mieux comprendre et traiter les dysfonctions électriques du cœur qui sont à l'origine de nombreuses maladies cardiovasculaires représentant près d'un tiers des décès dans le monde. L'IHU Liryc est structuré en fondation de coopération scientifique abritée par la Fondation Bordeaux Université (FBU). Dans le cadre du déploiement de sa stratégie data, l'IHU se dote d'une Direction Data et structure son socle technique autour de trois piliers : un environnement HDS (Hébergeur de Données de Santé) initialement cloud-based, un Entrepôt de Données de Santé (EDS) thématique national en électrophysiologie cardiaque, et une plateforme de gestion des données de recherche on-premise (Keycloak, eLabFTW, Girder, Affine, Orthanc, REDCap). Le/la Responsable Infrastructure & Sécurité est la pierre angulaire opérationnelle de ce dispositif.
Intitulé de poste	**Responsable Infrastructure & Sécurité** Sous la responsabilité du/de la Directeur(rice) Data.
Rattachement hiérarchique	Directeur(rice) Data de l'IHU Liryc.
Encadrement	Équipe initiale : 2 techniciens en charge du parc informatique, du support utilisateur et de l'événementiel. Équipe cible (24-36 mois) : ajout d'un Ingénieur Système / SRE et d'un Ingénieur Cybersécurité opérationnelle.
Nature de l'emploi	CDI Dès que possible
Niveau de qualification	Bac+5 en informatique, ingénierie ou domaine équivalent (école d'ingénieur, M.Eng., Master 2). Minimum 7 ans d'expérience professionnelle, dont une expérience significative dans un environnement régulé (HDS, ISO 27001, hôpital/CHU, recherche clinique) et dans des architectures hybrides on-premise / cloud. Certifications appréciées : certifications cloud (Azure, AWS ou cloud souverain), ISO 27001 Lead Implementer, ITIL, CISSP/CISM.
Rémunération et avantages sociaux	Entre 40 et 50 K€ selon profil et expérience. Prévoyance, mutuelle, 35 jours de congés payés +15 RTT sur la base d'un temps plein.

Situation du poste	IHU Liryc Site de l'Hôpital Xavier Arnozan Avenue du Haut Lévêque – 33600 PESSAC
Mission principale	Le/la Responsable Infrastructure & Sécurité définit, déploie, opère et sécurise l'ensemble des infrastructures informatiques de l'IHU Liryc : socles on-premise (recherche, calcul scientifique, parc) et environnements cloud destinés à l'hébergement HDS et à l'EDS. Il/elle est le garant opérationnel de la disponibilité, de la performance, de la sécurité et de la conformité des plateformes, en lien étroit avec le/la Directeur(rice) Data et le DPO. À ce titre, il/elle pilote en particulier : • Le maintien en conditions opérationnelles et de sécurité du socle on-premise (serveurs, stockage, sauvegardes, réseau, postes de travail, infrastructures de calcul scientifique et GPU). • La conception, le déploiement et l'exploitation des environnements cloud supportant l'environnement HDS et l'EDS. • La cybersécurité opérationnelle (durcissement, journalisation, supervision, gestion des vulnérabilités, gestion des identités et des accès, sauvegardes immuables, anti-ransomware). • La contribution active à l'obtention et au maintien des certifications HDS et ISO 27001, en lien avec le/la Directeur(rice) Data. • Le pilotage des prestataires (hébergeur HDS, intégrateurs cloud, MSSP éventuel, mainteneurs équipements scientifiques) et la maîtrise des coûts cloud (FinOps). • L'encadrement et la montée en compétences de l'équipe infrastructure.
Activités principales	**Infrastructure on-premise et recherche** • Administrer et faire évoluer les serveurs (Linux / Windows), le stockage, la virtualisation, le réseau (LAN/WAN, switches, firewalls, VPN, Wifi) et les services associés (DNS, DHCP, AD/Entra ID, messagerie). • Opérer et fiabiliser la plateforme de gestion des données de recherche (Keycloak, eLabFTW, Girder, Affine, Orthanc, REDCap), déployée via Docker Compose puis migrable vers Kubernetes. • Dimensionner, déployer et maintenir les ressources de calcul scientifique et GPU (HPC) au service des équipes de recherche, en lien avec les besoins en imagerie 4D, électrophysiologie et modélisation. • Anticiper les besoins futurs (calcul, IA, stockage haute performance) et proposer des trajectoires d'investissement. **Infrastructure cloud et environnement HDS** • Concevoir et déployer l'architecture cloud cible (cloud souverain, cloud public) supportant l'environnement HDS, l'EDS et les applications moins sensibles : réseau privé, segmentation, bastion, VPN, DNS privé, IAM, journalisation centralisée. • Mettre en œuvre une approche Infrastructure-as-Code (Terraform), de l'orchestration de conteneurs (Kubernetes), de l'automatisation (Ansible) et de pipelines CI/CD pour standardiser les environnements (dev / staging / prod).

- Opérer l'observabilité (Prometheus, Grafana, Loki ou équivalent), les alertes, l'auto-scaling et la gestion fine des coûts (FinOps : budgets, tagging, optimisation).
- Piloter, en lien avec le/la Directeur(rice) Data, les arbitrages cloud public / cloud souverain / on-premise selon les cas d'usage cliniques, recherche et industriels, en tenant compte des exigences de souveraineté.

Cybersécurité opérationnelle

- Mettre en œuvre la politique de sécurité définie avec le/la Directeur(rice) Data : durcissement des systèmes, MFA généralisé, gestion des secrets, gestion des privilèges (PAM).
- Opérer la chaîne de détection et de réponse : journalisation centralisée, SIEM, EDR, supervision sécurité 24/7 (via MSSP si nécessaire), gestion des vulnérabilités (scan, patching), tests d'intrusion réguliers.
- Concevoir et tester les dispositifs de continuité : sauvegardes immuables et hors-ligne (anti-ransomware), PRA et PCA documentés et éprouvés au minimum annuellement, définition des RTO/RPO par service.
- Segmenter le SI (DMZ, réseaux recherche, réseaux administratifs, environnements HDS/EDS) selon une approche Zero Trust.

Conformité, qualité et documentation

- Contribuer activement au dossier HDS et à la certification ISO 27001 (analyse de risques, mesures de sécurité, preuves, audits).
- Documenter les architectures, les procédures d'exploitation, les runbooks d'incident et les plans de continuité.
- Participer à la démarche qualité (rédaction, validation et mise à jour des procédures, validation des SI) en lien avec le/la responsable qualité.
- Assurer la veille technologique et réglementaire sur le périmètre infrastructure et cybersécurité.

Pilotage, prestataires et événementiel

- Piloter le budget infrastructure et les achats associés ; suivre les contrats prestataires (hébergeur HDS, intégrateurs, MSSP, mainteneurs).
- Gérer le parc informatique (entrées / sorties / besoins spécifiques aux projets scientifiques) en s'appuyant sur l'équipe de techniciens.

Assurer l'infrastructure informatique des événements de l'IHU (réseau, postes, captation IT) — conférences, summer school, comités scientifiques. L'audiovisuel n'est pas du périmètre de l'IT.

La liste des tâches ci-dessus énumérées n'est pas exhaustive.

Champ relationnel du poste

Interne	Externe
• Directeur(rice) Data, DPO, responsable qualité. • Équipes Data : data engineers, data managers, développeurs. • Chercheurs, médecins et ingénieurs scientifiques de l'IHU.	• Hébergeur HDS, fournisseurs cloud, intégrateurs, MSSP, éditeurs. • Partenaires fondateurs : CHU, Université de Bordeaux.

	• Équipe administrative de l'IHU et de la FBU. • Écosystème hospitalo-universitaire (CHU de Bordeaux, Université de Bordeaux, Inserm, CNRS, Inria selon partenariats). • Partenaires académiques et industriels nationaux et internationaux. • Instances et réseaux nationaux et européens : Health Data Hub, F-CRIN, EHDS, ANSSI. • Prestataires.
Compétences	**Savoirs** • Expertise approfondie des infrastructures systèmes et réseaux : serveurs Linux (Ubuntu, Rocky/RHEL) et Windows, virtualisation Hyper-V en cluster, stockage (SAN, NAS, objet S3), segmentation et micro-segmentation. L'écosystème matériel et réseau actuellement déployé à l'IHU est le suivant : serveurs Dell et HP, SAN Dell et Seagate, switches Dell et Cisco, Wifi Aruba, firewall et VPN Fortinet (FortiGate, FortiAnalyzer/FortiManager, FortiClient). Une expérience de tout ou partie de cet écosystème est appréciée ; des arbitrages futurs sur l'une ou l'autre brique sont possibles, la transition serait alors à conduire par le titulaire du poste. • Maîtrise des architectures cloud modernes en environnement régulé. Connaissance opérationnelle d'au moins un cloud souverain certifié HDS et SecNumCloud (Scaleway, OVHcloud, Outscale, Numspot, S3NS, Bleu…) ; une expérience complémentaire sur un hyperscaler (Azure, AWS) est un atout. Capacité à arbitrer les choix cloud en fonction des contraintes de souveraineté, de coût et des cas d'usage. • Maîtrise de la conteneurisation (Docker, Kubernetes), de l'Infrastructure-as-Code (Terraform), de l'automatisation (Ansible) et des pipelines CI/CD (GitLab CI, GitHub Actions, Azure DevOps). • Solides connaissances en cybersécurité : ISO 27001/27002, référentiels ANSSI (PSSI, HDS, SecNumCloud, doctrine cloud au centre), guides CIS, gestion des identités (Active Directory, Entra ID, Keycloak), SIEM/EDR, durcissement, gestion des secrets. • Connaissance des environnements de calcul scientifique : HPC (Slurm ou Kubernetes batch), GPU, stockage haute performance (Lustre, BeeGFS), bonnes pratiques de partage de données scientifiques. • Connaissance du cadre réglementaire applicable aux données de santé : RGPD, HDS, doctrine Health Data Hub, méthodologies de référence CNIL. • Bonnes pratiques d'ingénierie et de gestion de production : ITIL, observabilité, SRE, gestion d'incident. Anglais professionnel (oral et écrit) indispensable. **Savoir-faire opérationnels** • Concevoir, déployer et faire évoluer des architectures hybrides on-premise / cloud, sécurisées et scalables. • Conduire et soutenir des projets de certification (HDS, ISO 27001) et des audits. • Piloter des prestataires et tenir un budget cloud / infrastructure (FinOps).

	• Diagnostiquer, traiter et capitaliser sur les incidents (post-mortem, plans d'action). • Planifier, installer, automatiser, superviser et améliorer les processus de production. • Sécuriser la production : sauvegardes immuables, segmentation, PRA/PCA testés. • Rédiger et maintenir une documentation fonctionnelle et technique de qualité. • Dialoguer avec des interlocuteurs scientifiques, cliniques, juridiques et réglementaires. **Savoir-être** • Rigueur, sens de la méthode et goût pour la qualité. • Capacité de décision, force de proposition et autonomie. • Leadership et capacité à faire grandir une équipe technique. • Sens du service, pédagogie et écoute des utilisateurs (chercheurs, cliniciens, partenaires). • Discrétion, intégrité et respect strict de la confidentialité. • Curiosité technologique et veille active. • Esprit d'équipe et capacité à travailler en transverse.
Contact	Lettre de motivation + CV À adresser jusqu'au 30/06/2026 inclus à : recrutement@ihu-liryc.fr