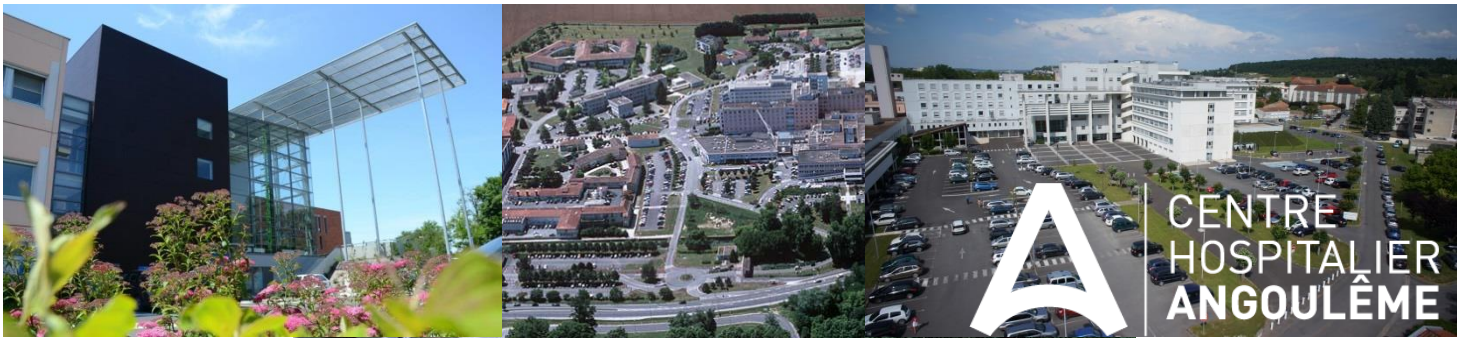

LE CENTRE HOSPITALIER D'ANGOULEME RECRUTE …

Un(e) Technicien système et réseau

L'ÉTABLISSEMENT ET SON ENVIRONNEMENT

Le Centre Hospitalier d'Angoulême est l'établissement de référence de la Charente. C'est aussi l'établissement support du Groupement Hospitalier Territorial de Charente.

Il est en direction commune avec trois établissements : le CH de La Rochefoucauld, le CH de Confolens, le CH de Ruffec et l'Ehpad Habrioux d'Aigre.

Sa capacité d'accueil est de 1 157 lits et places répartis en MCO, SSR, USLD et EHPAD.

Doté de 9 pôles d'activités cliniques et médico-techniques, l'établissement compte environ 2 500 professionnels qualifiés, ce qui fait de lui le plus gros employeur du département.

De plus, le CH d'Angoulême est desservi par la LGV (35 mn de Bordeaux et 2h15 de Paris) et à 1h30 en voiture de la côte Atlantique.

LE POSTE

100% / Poste à pourvoir dès que possible – basé au CH Angoulême

Contractuel ou Titulaire de la FP

Candidature à adresser à Monsieur le Directeur des Ressources Humaines et des Relations Sociales avec votre lettre de motivation et votre CV exclusivement par mail à l'adresse suivante :

recrutement@ch-angouleme.fr

Pour tout complément d'information jugé utile, vous pouvez contacter M. ROBINET, Directeur du Système d'Information (05.45.23.72.32)

CENTRE HOSPITALIER ANGOULÊME	Direction des Ressources Humaines et des Relations Sociales	
	Technicien Système et Réseau	Page : 1
	Thématique : Management du système d'information	

Famille : Système d'information

Sous-famille : Support et exploitation

Métier : Technicien Système et Réseau

Pôle : Administratif et logistique

Service ou unité fonctionnelle : Service informatique, GHT 16

Définition / Mission (*cf fiche métier*) :

Sous la responsabilité du responsable infrastructure du GHT et en lien fonctionnel avec le chef de projet Cyber, le technicien assure l'exploitation et le maintien en condition opérationnelle du socle réseau et des solutions de sécurité du système d'information convergent du GHT. Il applique la politique de sécurité (PSSI) définie par le RSSI, surveille les systèmes, traite les alertes et incidents de premier et second niveau, et contribue à la résilience du SI au service de la continuité des soins et de la sécurité des patients.

Recrutement par le Centre hospitalier d'Angoulême pour exercer ses missions au sein du Groupement Hospitalier de Territoire

Responsable hiérarchique direct : Responsable Service informatique du GHT

Responsable fonctionnel : Directeur du Système d'information du GHT

ACTIVITES

Exploitation et maintien en condition opérationnelle

- Exploite et maintient les équipements réseau (cœur de réseau, switches, bornes et contrôleurs Wi-Fi) et les solutions de sécurité (pare-feu, proxy et reverse proxy, antispam, antivirus / EDR).
- Applique les règles de filtrage et les paramétrages définis par le RSSI ; réalise les revues régulières de règles.
- Pilote la maintenance corrective, évolutive et préventive avec les fournisseurs de son périmètre.

Détection et réponse (niveaux 1 et 2)

- Surveille les systèmes et réseaux (sondes, supervision, journaux / SIEM) afin de détecter les événements de sécurité.
- Qualifie et traite les alertes, applique les procédures de réponse à incident et escalade au RSSI ou au niveau 3 si nécessaire.
- Contribue aux exercices de crise cyber et au signalement des incidents (CERT Santé).

Gestion des vulnérabilités et durcissement

- Réalise les scans de vulnérabilités, suit l'application des correctifs (patch management) et met en œuvre les mesures de durcissement.
- Assure une veille technique et sur les menaces (CVE, bulletins ANSSI et CERT Santé).

Sauvegarde et résilience

- Exploite les sauvegardes (y compris copies immuables ou déconnectées), réalise et documente les tests de restauration.
- Contribue à la mise en œuvre du PCA / PRA et au fonctionnement en mode dégradé.

Accès, segmentation et documentation

- Administre au quotidien les accès, dont les accès à privilèges via le bastion, selon les règles définies.
- Participe à la segmentation réseau, notamment la sécurisation des réseaux et dispositifs biomédicaux (NAC / 802.1X).

SAVOIR-FAIRE / Compétences	Niveau requis
Gestion des infrastructures réseaux (réseaux niveau 2 et 3) filaire et sans fils	**Maîtrise**
Gestion des composants de sécurité élémentaires (proxy WEB, Antispams, antivirus centralisé….)	**Maîtrise**
Gestion et maintenance des environnements physiques et virtuels	**Maîtrise**
Gestion et maintenance des environnements système Microsoft, unix, linux	**Maîtrise**

*Niveau : Non requis/ A développer / Pratique courante / Maîtrisé / Expert

CONNAISSANCES	Degré**
Connaissances principales : - Protocoles et services réseau (TCP/IP, DHCP, DNS, SNMP) ; commutation et routage (VLAN, STP/RSTP, LACP, VRRP) ; interconnexion de sites (VPN). - Exploitation des solutions de sécurité du parc : pare-feu, EDR / antivirus, antispam, proxy et reverse proxy. - Supervision et analyse de journaux ; diagnostic réseau (Wireshark, tcpdump) ; scripting de base (Bash, PowerShell). - Exploitation des sauvegardes et tests de restauration.	**Approfondies**
Connaissances spécifiques : - SIEM et corrélation de journaux ; NAC / 802.1X ; bastion / gestion des accès à privilèges ; sécurité de l'Active Directory ; segmentation des réseaux biomédicaux. - Notions ITIL (gestion des incidents et des changements)	**Très bonne**

** Degré : Connaissances Générales / Connaissances détaillées / Connaissances approfondies / Connaissances d'Expert

SAVOIR-ETRE
Savoir gérer la relation avec les différentes équipes techniques du service et les autres services logistiques (et administratifs) • Rigueur, sens de l'analyse, autonomie et capacité d'initiative. • Qualités relationnelles, pédagogie et sens du compte rendu. • Gestion du stress en situation de crise et capacité à travailler en mode dégradé.

INFORMATIONS COMPLEMENTAIRES				
Conditions particulières d'exercice	Horaires : 37 h /semaine 8h-16h30 / 9h-17h30 / 9h30- 18h			
	Travail isolé :	❒ Oui		x Non
	Déplacement :	x Oui		❒ Non
	Temps partiel possible :	❒ Oui		x Non
	Horaires :	X Fixe	❒ variable	❒ nuit
	Repos hebdomadaire :	x Fixe		❒ Variable
	Contact malade/public :	x Oui		❒ Non
	Compléter si besoin : Des astreintes informatiques (déplacement possible) sont organisées (WE/JF- 24h/24 , 18h – 8h30 en semaine).			
Risques professionnels	En lien avec le Document Unique			
Prérequis nécessaires à l'exercice du poste	Diplôme exigé : **Bac+2 en informatique (BTS SIO option SISR, BUT Réseaux & Télécommunications) ; licence professionnelle cybersécurité appréciée** Expérience conseillée **2 à 4 ans sur une fonction réseau / sécurité** De préférence connaissance du contexte d'établissement de santé (public ou privé)			