GIP E-SANTE CENTRE-VAL DE LOIRE

Fiche de poste :

REFERENT(E) REGIONAL(E) CYBERSECURITE

Rédacteur : Elisée PFENDER DELUBAC Fonction : Responsable de la Sécurité des Systèmes d'Information (RSSI)	Validation : février 2023

LOCALISATION ET RATTACHEMENT

LIEU D'EXERCICE ET ENVIRONNEMENT

Groupement Régional d'Appui au Développement de la e-Santé (GRADeS) en Centre-Val de Loire, le Groupement d'Intérêt Public (GIP) e-Santé Centre-Val de Loire est chargé de mettre en œuvre la stratégie régionale d'e-santé.
Son action s'inscrit dans une politique d'intérêt général au service de la modernisation du système de santé, grâce à la transformation numérique dans les champs du sanitaire, du médico-social et du social.
Le GIP Centre-Val de Loire e-santé est Maître d'Ouvrage Opérationnel pour les Systèmes d'Information de Santé de la région Centre-Val de Loire. Dans ce cadre, il :

- contribue à l'élaboration de la stratégie régionale e-santé
- conduit les projets de la stratégie régionale et les projets que ses membres lui confient
- conduit d'autres projets en lien avec les acteurs nationaux ou régionaux
- veille à la sécurité, interopérabilité, urbanisation à l'échelle régionale
- anime, fédère et coordonne les acteurs de la région autour de la stratégie régionale
- promeut l'usage des services numériques en santé dans les territoires
- apporte son expertise aux acteurs régionaux.

POURQUOI NOUS REJOINDRE ?

Rejoindre le GIP e-Santé Centre-Val de Loire, c'est participer à un projet enrichissant humainement, qui a du sens, avec une finalité d'intérêt public ! La bonne humeur et l'esprit d'équipe sont de mise, avec l'enjeu de se surpasser collectivement pour accompagner les professionnels de santé du territoire au quotidien, et relever les défis de la santé numérique !

RELATIONS HIERARCHIQUES

Le(la) Référent(e) régional(e) cybersécurité est placé(e) sous l'autorité hiérarchique de la RSSI du groupement.

RELATIONS FONCTIONNELLES

- **Relations internes principales :** Directeur, équipe SSI/RGPD, directeurs/chefs de projets, ensemble de l'équipe
- **Relations externes principales :**
  - Acteurs de santé de la région, RSSI, DPO, Directions des SI des établissements, prestataires
  - ARS (Agence Régionale de Santé), ANS (Agence du numérique en santé, ANSSI (Agence nationale de la sécurité des systèmes d'information)

DESCRIPTION DU POSTE

CONTEXTE

A l'heure de l'accélération des décloisonnements entre organisations et acteurs de santé, le changement d'échelle des solutions numériques et leur interopérabilité nécessitent un haut niveau de sécurisation.

Le(la) Référent(e) régional(e) cybersécurité a pour missions de participer aux actions définies dans la feuille de route régionale d'accompagnement cybersécurité et dans le cadre du volet numérique du Ségur en santé.
Dans le cadre de ce programme, il(elle) est rattaché(e) au Responsable Sécurité des Systèmes d'Information (RSSI) et intégré(e) dans une équipe de 2 personnes dédiées à la sécurité des systèmes d'informations.

Il est en contact avec les établissements de santé (hôpitaux, établissements médico-sociaux…) qu'il(elle) accompagne dans la mise en œuvre des référentiels nationaux. Cet accompagnement sera réalisé en étroite collaboration avec l'Agence Régionale de Santé (ARS).

De ce fait, au sein de l'équipe SSI/RGPD, il(elle) apporte son expertise à la fois pour :

- Sécuriser et participer à la conformité des services numériques portés par le groupement
- Accompagner les acteurs régionaux sur ces mêmes thèmes
- Remplir les missions nationales et régionales confiées par l'ANS et l'ARS

Les responsabilités seront réparties au sein de l'équipe sur les missions : Sécurité du SI du groupement et sur la mise en œuvre du plan régional cybersécurité à destination des acteurs de santé.

MISSIONS

- Mettre en œuvre le dispositif régional de renforcement de la cybersécurité sur les thèmes de la prévention, le suivi et la remédiation.
- Suivre les indicateurs de maturité des acteurs de la région.
- Participer à l'administration de la plateforme régionale de sensibilisation, et à la mise en œuvre de la stratégie de sensibilisation et de phishing régionale.
- Participer à l'animation le réseau régional des référents sur la sécurité des systèmes d'information et la conformité RGPD.
- Organiser des évènements d'information et de sensibilisation.
- Conseiller et accompagner les acteurs régionaux dans la mise en œuvre de leur plan d'action SSI.
- Promouvoir les usages des services numériques et référentiels socles (MSS, DMP, INS, PSC…).
- En complément, proposer, avec l'aide de prestataires externes, des services adaptés aux besoins des acteurs régionaux dans leur diversité et leur capacité humaine et financière.

Les activités décrites ne sont pas exhaustives et peuvent évoluer en fonction du contexte des projets et l'évolution de la structure.

EXIGENCES DU POSTE

CONNAISSANCES

Savoir-Faire

- Bonnes connaissances des concepts réglementaires de la sécurité des systèmes d'information
- Capacité à gérer des situations de crise
- Connaissance de l'architecture d'un système d'information
- Connaissances en conduite de projets
- Accompagnement du changement
- Proposition d'axes pour améliorer les actions existantes
- Notions sur la réglementation et procédures des marchés publics

Savoir-Être

- Capacité à travailler en équipe
- Capacité d'écoute, d'adaptation, de pédagogie
- Capacité d'alerte, de transparence et partage d'information
- Rigueur, autonomie et responsabilité professionnelle, impartialité
- Respect de la hiérarchie
- Dynamisme, force de proposition
- Capacité rédactionnelle
- Organisation de travail structurée
- Aisance à l'oral, capacité à organiser et animer des réunions/webinaires et autres évènements

Savoir-associés

- Connaissance du droit des données informatiques
- Expérience(s) des secteurs sanitaires, ambulatoires et/ou médico-sociaux serait un plus

PROFIL

- **Niveau d'études, diplômes recherchés** : Bac +3/+ 5 dans le domaine de la SSI et la protection des données
- **Expérience(s) :**
  - Vous disposez idéalement d'une première expérience dans la cybersécurité et/ou les systèmes d'informations de santé
  - Poste ouvert à l'alternance pour un diplôme en cybersécurité

CONDITIONS D'EXERCICE

SPECIFICITES DU POSTE

- Poste à temps plein ou alternance
- Poste basé au siège, 45160 OLIVET
- Déplacements dans la région Centre-Val de Loire (ponctuellement hors région)
- Des réunions peuvent avoir lieu en soirée
- Nécessité d'avoir un véhicule assuré professionnellement + permis B
- Travaillant avec des établissements ou avec des professionnels de santé prenant en charge des personnes soignées, vous serez soumis au secret professionnel.

MOYENS MIS A DISPOSITION

- Bureau équipé et moyens mobiles de communication, PC portable
- Véhicule de service du GIP e-Santé Centre-Val de Loire pour les déplacements professionnels (hors déplacements domicile-travail)

CONTRAT

- Contrat à durée déterminée (CDD) de 1 an, transformable en contrat à durée indéterminée, ou poste à pourvoir par voie de mise à disposition ou de détachement ;
- Frais de déplacement (hors domicile-travail) : indemnité kilométrique + frais de repas selon barème fonction publique d'Etat
- Comité d'entreprise : adhésion au CGOS (Comité de Gestion des Œuvres Sociales)
- Restaurant inter-entreprise (+ à venir en 2023 : tickets restaurant)
- Participation : mutuelle, abonnement transport, forfait mobilité durable
- Télétravail possible 2 à 3 jours par semaine
- Salaire à négocier, à partir de 35K€ brut annuel

Début de la mission : dès que possible

CANDIDATURE

Adressez votre candidature à

- Aurélie BILLAC, Secrétaire générale : abillac@esante-centre.fr
- Elisée PFENDER-DELUBAC : edelubac@esante-centre.fr

Joindre à votre candidature : Curriculum Vitae+ Lettre de motivation+ Prétentions salariales