> OFFRE D'EMPLOI

- Technicien infrastructure et cybersécurité (F/H) -

INFORMATIONS CLÉS

Réponse avant le :
17/03/2025

Référence :
18755

Direction :
Systèmes d'information et du numérique

Cadre d'emploi :
Techniciens territoriaux

Lieu de Travail :
Centre Simone Signoret
38090 Villefontaine

Horaires :
Temps complet ouvrant droit à des jours de RTT

Spécificités du poste :
Permis B obligatoire
Astreintes possibles

Où adresser votre candidature :
Rappeler la référence **18755** sur votre candidature
Par courrier : 17 avenue du Bourg, 38081 L'Isle d'Abeau cedex **Par mail :** recrutement@capi38.fr
Joindre obligatoirement : lettre de motivation et curriculum vitae

CONTEXTE

La Communauté d'Agglomération Porte de l'Isère est une intercommunalité constituée de 22 communes, comptant 112 905 habitants. Elle occupe une situation géographique privilégiée (idéalement située à 20 minutes à l'est de Lyon) et dotée d'un excellent niveau d'accessibilité : aéroport, TGV et autoroutes.
C'est un territoire singulier, à taille humaine, où patrimoine urbain, industriel et naturel vivent en parfaite harmonie. Engagée dans le développement durable, la transition énergétique et le respect de l'environnement, la CAPI est un territoire agréable à vivre, avec un tissu économique dynamique et innovant.
Elle assure une large palette de compétences au quotidien : des missions de planification, aménagement et développement (habitat, économie, urbanisme, mobilités, éclairage public, voiries, transition énergétique), mais aussi une offre de services aux habitants : petite enfance, gestion d'équipements sportifs et culturels, lecture publique, eau et assainissement…

Au sein de la CAPI, **la Direction des Systèmes d'Information mutualisée** est constituée sous la forme d'un service commun. Ce dernier regroupe aujourd'hui, outre la CAPI, les communes de Bourgoin-Jallieu et de La Verpillière.
Le nécessaire développement de l'e-administration et des e-services aux usagers appelle le déploiement d'un Système d'information propre à répondre aux nouveaux enjeux et besoins des administrés et des services. Les collectivités membres du service commun DSI attendent de disposer d'un SI contributeur à l'efficience des services par son apport en termes de qualité de service et de solutions techniques (démarche ITIL, sécurité, dématérialisation, relations utilisateurs, open data).

Ainsi, sous la responsabilité du responsable de service Infrastructures Informatiques et Cybersécurité et rattaché(e) fonctionnellement à 50% au RSSI, **vous serez garant du bon fonctionnement et de la disponibilité des infrastructures systèmes, réseaux et télécommunications. Vous assurerez la prévention des dysfonctionnements et contribuerez au bon fonctionnement du système d'information. Vous serez en charge de l'optimisation et de l'évolution des infrastructures afin d'en accroitre les performances et la stabilité et interviendrez sur l'ensemble des éléments d'infrastructures liés à la sécurité du SI.**

Plus d'information sur **www.capi-agglo.fr/la-capi/rh**

Dans ce cadre, vos activités seront :

Le technicien IICS est responsable d'activités de support, de gestion ou d'administration de la sécurité d'un point de vue technique ou administratif : conception, production, conditionnement et gestion des réseaux de chiffrement et des éléments secrets.

Il a pour mission de :

- Opérer le déploiement et l'administration d'une infrastructure sécurisée d'un système d'information en fonction des évolutions de l'organisme :

  Participer au déploiement des architectures de sécurité des systèmes d'information, des réseaux, de tous objets communicants, assurer la conformité des paramétrages des équipements de sécurité, durcir les systèmes d'exploitation en vue de maintenir l'intégrité des fonctionnalités et la fiabilité de l'ensemble du système, intégrer des équipements de sécurité (pare-feu, sonde, IDS…) afin répondre aux exigences de la politique de sécurité, gérer la sécurisation des flux, assurer le maintien en condition de sécurité (MCS) des applications, s'assurer de la bonne réalisation des sauvegardes de l'infrastructure, participer, sur un plan sécurité, à la conformité des actifs du SI.

- Superviser les réseaux et les systèmes d'information de l'infrastructure et assurer une veille technologique et réglementaire en matière de sécurité :

  Participer à l'analyse de la vulnérabilité du système et des risques liés à la sécurité, analyser les différentes remontées d'alertes, gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité, rechercher (via des outils d'analyse de log) les événements de cybersécurité et les menaces, améliorer la supervision de la sécurité, assurer une veille technologique.

- Gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité :

  Opérer au sein de cellules opérationnelles de gestion de crise, mettre en œuvre des solutions palliatives ou correctives, assurer le suivi des incidents, prélever les traces d'une attaque informatique passée ou en cours.

- Contrôler le droit d'accès au système et aux données de l'organisme, sensibiliser et former le personnel et conseiller l'officier de la sécurité des systèmes d'information de l'entreprise :

  Veiller à ce que l'attribution des habilitations aux collaborateurs soit réduite au strict nécessaires et mener des revues d'habilitations régulières, accompagner l'équipe d'accompagnement aux usages à sensibiliser les utilisateurs, collaborer au travail de sensibilisation et de formation de l'ensemble du personnel, contribuer à la mise en œuvre de bonnes pratiques, en proposant de nouvelles procédures, mesurer l'évolution du niveau de sensibilisation du personnel.

- Assurer l'exploitation informatique dans le respect des plannings et de la qualité attendue par la direction et les utilisateurs
- Gérer les incidents d'exploitation de niveau 2/3
- Collaborer avec les autres pôles dans le cadre des projets et de l'assistance aux utilisateurs
- Assurer la gestion du parc informatique en respectant les délais et les procédures en cohérence avec la politique du service commun de la CAPI
- Assurer le fonctionnement optimal et sécurisé des équipements informatiques, dans le cadre des normes, méthodes d'exploitation et de priorité défini par le chef du pôle en collaboration avec les ingénieurs systèmes et réseaux

Savoir et savoir-faire :

- Système : Services Active Directory, Windows server, Linux, Citrix, Exchange, VMWare
- Réseau/télécom : LAN/WAN/VLAN/FW, etc…
- Souhaitable : Apache, IIS, notion de Scripting DOS/VB/VBA/PowerShell, Certificats, Antivirus
- Connaitre les réseaux TCP/IP
- Connaitre la méthodologie ITIL et sa déclinaison opérationnelle dans un logiciel
- Connaître les environnements Windows server et linux, ainsi que les rôles et fonctionnalités principales de ces systèmes
- Maitriser les outils bureautiques (Ms Office, etc…)
- Savoir utiliser les environnements bureautiques et la suite bureautique MICROSOFT,
- Maîtriser des problématiques de sécurité du parc informatique
- Gérer les incidents de cybersécurité en assurant les premières réactions et investiguer sur les événements de cybersécurité
- Capacité de compréhension des menaces cybersécurité
- Travailler en situations de crise
- Être en mesure d'identifier les vulnérabilités/failles des composants du SI
- Collaborer avec les autres pôles de la DSI mutualisée
- Travailler en autonomie sur des projets de service et rendre compte à sa hiérarchie de son activité

Savoir être :

- Disponibilité et sens du service public
- Autonomie, convivialité et esprit d'équipe
- Sens affirmé du service à l'utilisateur

Votre rémunération :

- Rémunération statutaire + RIFSEEP + Prime de fin d'année.
- **Autres avantages :** Chèques déjeuners + Épargne chèques vacances + Comité des œuvres sociales + participation employeur mutuelle et prévoyance sous condition.

Plus d'information sur **www.capi-agglo.fr/la-capi/rh**