Groupement d'Intérêt Public « France Enfance Protégée »

Intitulé du poste : Chargé de mission – Sécurité SI & Exploitation

Classification : catégorie A (fonction publique)

Description de l'employeur :

Le GIP France Enfance Protégée, créé le 1er janvier 2023, est un opérateur national de la politique publique de prévention et de protection de l'enfance. Il assure des missions de service public sur l'enfance en danger, l'adoption nationale et internationale et l'accès aux origines personnelles. Il est également un organisme ressources, produisant et diffusant des données, des connaissances et des outils en matière de protection de l'enfance. Enfin, il assure des missions de secrétariat général des conseils nationaux de protection de l'enfance, d'adoption et d'accès aux origines.

Le GIP comprend environ 120 agents en France et un réseau de correspondants dans les Départements, ainsi que des agents dans plusieurs pays pour son activité à l'international.

Le **Chargé de mission – Sécurité SI & Exploitation** a pour mission principale de garantir la sécurité et la conformité du Système d'Information, dans un environnement où la protection des données sensibles est un enjeu majeur.

Sous l'autorité du Responsable des Systèmes d'Information et en lien régulier avec le RSSI externalisé, il est chargé de : **piloter la sécurisation du SI, assurer la conformité réglementaire piloter des projets SI** de son domaine et coordination des prestataires.

En appui au Responsable Infrastructure & Exploitation, il/elle intervient **en collaboration** sur le support technique. Il contribue également à la documentation des processus et à la sensibilisation des utilisateurs aux bonnes pratiques de sécurité.

Il travaille en collaboration avec l'ensemble des utilisateurs internes et les prestataires externes, dans un cadre exigeant où **rigueur, autonomie et sens du relationnel** sont indispensables.

Activités du poste :

- **Sécurité du Système d'Information :**
    - Piloter la sécurisation du SI : Mettre en œuvre et maintenir les mesures et règles de sécurité (accès, chiffrement, sauvegardes, conformité RGPD/NIS2).
    - Assurer la surveillance et la réponse aux incidents : Être référent pour la gestion des incidents de sécurité, en coordination avec le RSSI externalisé.
    - Garantir le Maintien en Condition Opérationnelle (MCO) : Superviser les mises à jour de sécurité, les correctifs et la disponibilité des infrastructures.
    - Conduire les audits et tests de sécurité : Organiser et suivre les audits (tests d'intrusion, analyses de vulnérabilités), puis piloter les plans de remédiation.
    - Veille technologique : Assurer une veille active sur les menaces et les solutions de sécurité émergentes.

- **Gestion de projet et conformité :**
    - Piloter des projets de sécurité : Exemples : déploiement d'un SIEM, mise en place d'un WAF, centralisation des logs, déploiement d'une solution EDR/XDR.
        - Rédiger les cahiers des charges, organiser les appels d'offres et assurer le suivi des prestataires.
        - Coordonner les acteurs internes et externes pour garantir le respect des délais et des budgets.
    - Contribuer à la conformité réglementaire : Veiller à l'alignement du SI avec les normes en vigueur (NIS-2, RGPD, etc.).
- **Sensibilisation et documentation :**
    - Animer des actions de sensibilisation : Former les équipes aux bonnes pratiques de sécurité (phishing, gestion des mots de passe, etc.).
    - Gérer la documentation de d'activité (PSSI, compte rendu d'audit de sécurité, rapports annuel cybersécurité …)
- **Exploitation et Support Technique :**
    - Assurer le support utilisateur : En collaboration avec le responsable infrastructure, résoudre les incidents techniques (N2/N3) et accompagner les utilisateurs.
    - Documenter et optimiser les processus : Participer à la documentation des astreintes et des protocoles d'urgence. Participer à la mise à jour des procédures techniques, des schémas réseau et des guides utilisateurs.

Compétences requises :

Techniques :

- Réseaux : protocoles, wifi, Ethernet, modèle OSI, redondance
- Sécurité : gestion antivirus, administration firewall, gestion des flux
- Connaissance des solutions de sécurisation (sans expertise) : SIEM, WAF, EDR, XDR, SOC …
- Système : administration des systèmes Windows (poste de travail et serveur) et Linux
- Applicative : administration via annuaire active directory, prise en main à distance, Office 365, Cloud, Outil de suivi des demandes et incidents, administration d'un système de téléphonie, …
- Documentation : conception, lecture et compréhension de schéma réseau & cartographie des flux, création & mise en application de process à destination du service et des utilisateurs

Relationnelles :

- Réactif
- Autonome
- Rigoureux et organisé
- Pédagogue, capacité à vulgariser les enjeux de sécurité pour des utilisateurs non techniques
- Doté d'un bon sens du relationnel

Niveau d'études / diplôme ou formation souhaité :

Profil junior : diplôme de niveau 7, spécialisé en cybersécurité

Profil sénior : diplôme de niveau 5 minimum, spécialisé en cybersécurité + 5 ans d'expérience à un poste équivalent. Expérience dans le secteur public appréciée

Formations complémentaires régulières pour une remise à niveau sur les évolutions technologiques

Spécificités (astreinte, horaires atypiques, déplacements France entière …) :

Participation à l'astreinte technique du 119 en équité avec les autres membres du service.

Informations complémentaires :

Statut : fonctionnaire en détachement, mis à disposition ou contractuel en CDD de 3 ans

Salaire annuel à temps complet selon expérience + Primes + Chèques repas + Participation mutuelle + CNAS (Organisme national d'action sociale) + Télétravail possible (maximum 2 jours par semaine)

Envoi des candidatures CV et lettre de motivation à transmettre par mail à : recrutement@france-enfance-protegee.fr