FICHE DE POSTE : INGENIEUR CYBERSÉCURITÉ

1. Identité du poste :

- **Intitulé :** Ingénieur Cybersécurité
- **Catégorie :** A (ou B confirmé selon expérience)
- **Rattachement hiérarchique :** RSSI-DPO
- **Direction de rattachement :** Direction Ingénierie Informatique, Télécom et Usages Numériques
- **Localisation :** Service Sécurité de l'Information et Protection des Données, Communauté Urbaine d'Arras

2. Contexte et finalité :

Garantir la sécurité opérationnelle des systèmes d'information de la collectivité par la mise en œuvre de mesures techniques et organisationnelles alignées sur les référentiels de sécurité (ISO 27001, ANSSI). Contribuer activement à la gestion proactive des risques informatiques afin d'assurer la robustesse, la disponibilité et l'intégrité du SI.

3. Missions principales :

- Déployer les mesures techniques définies par la politique de sécurité des systèmes d'information (PSSI)
- Assurer la détection, le traitement et la résolution des incidents de sécurité
- Conduire et suivre les audits techniques de sécurité selon les référentiels de sécurité
- Assurer une veille technologique constante et proposer des améliorations en continu
- Participer à la sensibilisation et la formation en cybersécurité des utilisateurs
- Superviser les prestations externes et contrôler leur conformité aux exigences techniques de sécurité

4. Activités techniques, spécifiques au métier :

- Surveiller les systèmes d'information à l'aide d'outils de sécurité
- Analyser, qualifier et traiter les alertes et incidents de sécurité en appliquant des méthodes rigoureuses d'investigation technique
- Gérer activement les vulnérabilités : scans réguliers, analyse des résultats, suivi et traitement des correctifs
- Piloter les audits techniques internes et externes et suivre les plans d'action associés
- Assurer une veille continue sur les référentiels et bonnes pratiques de sécurité (ANSSI, RGS, ISO 27001..)
- Mettre en place, administrer et optimiser les outils techniques de sécurité du SI
- Créer et animer des sensibilisation et des formations en lien avec la sécurité du réseau.

5. Activités secondaires :

- Élaborer et maintenir à jour les procédures et documentations techniques associées
- Contribuer à la rédaction des cahiers des charges techniques pour les projets de sécurité
- Assister ponctuellement les équipes informatiques dans la résolution de problématiques techniques complexes
- Participer à la définition, la rédaction, la mise à jour et l'animation des dispositifs de continuité et de reprise d'activité (PCA/PRA) en lien avec les directions métiers et les services techniques.

6. Compétences requises :

- Expertise avérée en sécurité technique des systèmes d'information
- Bonne maîtrise des outils techniques spécifiques de cybersécurité (SIEM, pare-feux, EDR, solutions d'authentification forte)
- Excellente connaissance des référentiels de sécurité ISO 27001 et ANSSI
- Capacité à mener des analyses de risques techniques détaillées (méthodologie EBIOS Risk Manager)

- Fortes compétences analytiques, rédactionnelles et pédagogiques
- Réactivité, adaptabilité et autonomie opérationnelle

7. Compétences ou connaissances souhaitées :

- Compétence en analyse forensique et gestion d'incidents complexes
- Connaissance des environnements Cloud (Azure) et Microsoft et en sécurité réseau
- Aptitude en gestion de projet technique informatique

8. Profil recherché :

- Formation supérieure en informatique (Bac +3 à Bac +5) spécialisée en cybersécurité
- Expérience professionnelle confirmée (minimum 3 à 5 ans) dans un poste similaire
- Rigoureux, méthodique, doté d'un esprit analytique et pragmatique
- Discrétion, intégrité, respect strict de la confidentialité
- Bon communicant, capable de travailler en équipe et en transversalité