

**L'Institut du Cerveau (ICM), recrute**  
**Un(e) Ingénieur(e) Sécurité Systèmes Informatique (H/F)**  
**Poste à pourvoir dès à présent**  
**CDI**  
**A Paris 13<sup>ème</sup>**

*L'Institut du Cerveau est une Fondation privée reconnue d'utilité publique dont l'objet est la recherche fondamentale et clinique sur le système nerveux. Sur un même lieu, 850 chercheurs, ingénieurs et médecins couvrent l'ensemble des disciplines de la neurologie, dans le but d'accélérer les découvertes sur le fonctionnement du cerveau, et les développements de traitements sur les maladies comme : Alzheimer, Parkinson, Sclérose en plaques, épilepsie, dépression, paraplégies, tétraplégies, etc.*

## **POSTE**

Sous la responsabilité opérationnelle du Directeur des Systèmes d'Information de l'ICM, Systèmes d'Information traitant les besoins informatiques de 26 équipes de chercheurs, 11 plateformes scientifiques et 15 services supports (achats, dsi, finances...). Pour précision, l'institut représente 897 personnes dont 137 chercheurs, 141 doctorants, 353 ITA.

Les ressources mises à disposition de cette communauté, représentent un parc de 1 500 postes de travail, plus de 250 applications métiers utiles à son fonctionnement, un stockage de données scientifiques de 6 pétaoctets, un cluster de calcul 800 CPUs.

L'Ingénieur Sécurité Informatique Orienté Opérationnel sera responsable de la mise en œuvre et de la gestion des solutions de sécurité informatique pour assurer la protection des systèmes, des données et des réseaux de l'entreprise. Ce rôle implique une compréhension approfondie des menaces potentielles, des vulnérabilités des systèmes, ainsi que la capacité à élaborer et à exécuter des stratégies de sécurité efficaces. Devra être capable de formaliser des recommandations en vue de mettre en application ces dernières

### **MISSIONS PRINCIPALES**

- Surveillance et Gestion des Menaces :
  - Surveiller activement les activités susceptibles de représenter une menace pour la sécurité des systèmes d'information.
  - Analyser les vulnérabilités et les incidents de sécurité et prendre des mesures correctives appropriées.
  - Mettre en place des mécanismes de détection et de réponse aux incidents pour minimiser les risques de sécurité.
- Gestion des Outils de Sécurité :
  - Gérer et maintenir les outils de sécurité informatique tels que les systèmes de détection d'intrusion, les antivirus, etc.
  - Évaluer régulièrement l'efficacité des outils de sécurité et recommander des améliorations si nécessaire.
  - Assurer la configuration optimale des outils de sécurité pour répondre aux besoins spécifiques de l'institut.
- Implémentation des Politiques de Sécurité :
  - Développer, mettre en œuvre et maintenir les politiques de sécurité des systèmes d'information.
  - Former le personnel sur les meilleures pratiques en matière de sécurité informatique et assurer leur conformité aux politiques de sécurité établies.

- Gestion des Accès et des Identités :
  - Gérer les droits d'accès aux systèmes et aux données sensibles en accord avec les principes de moindre privilège.
  - Mettre en place des processus d'authentification solides pour protéger les identités des utilisateurs et prévenir les accès non autorisés.
- Évaluation de la Conformité et des Risques :
  - Effectuer des évaluations régulières de la conformité aux normes de sécurité et réglementations en vigueur.
  - Identifier les risques pour la sécurité et recommander des mesures d'atténuation appropriées.
  - Capacité à rester à jour sur les dernières tendances et technologies en matière de sécurité informatique.

## PROFIL

### SAVOIR-FAIRE

- Capacité à comprendre les impacts de l'architecture du système d'information sur la SSI.
- Compréhension de l'environnement et des activités de recherche scientifique, des besoins et des contraintes des utilisateurs
- Connaissance approfondie des principes de sécurité informatique, des protocoles de sécurité et des meilleures pratiques.
- Compétences techniques solides en matière de configuration et de gestion des outils de sécurité tels que les systèmes de détection d'intrusion, etc.
- Capacité à analyser et à résoudre les incidents de sécurité de manière efficace.
- Excellentes compétences en communication et capacité à travailler en équipe.

### SAVOIR

- Diplôme universitaire en informatique, en sécurité informatique ou dans un domaine connexe.
- Certification en sécurité informatique (ex. CISSP, CISM, CEH, EBIOS, ITIL) serait un plus.
- Expérience professionnelle préalable dans le domaine de la sécurité informatique, de préférence en environnement opérationnel.
- Anglais lu, écrit, parlé.

### SAVOIR-ETRE

- Capacité à travailler en équipe
- Bonnes qualités relationnelles et de communication afin d'assurer une collaboration efficace
- Sens des responsabilités et de la confidentialité.
- Capacité à travailler sous pression et à gérer les situations d'urgence.
- Capacité à prendre des décisions rapidement et de manière autonome.
- Forte éthique professionnelle et intégrité

*L'Institut du cerveau s'engage pour lutter contre toute forme de discrimination. Nous garantissons un environnement de travail inclusif et respectueux de toutes les diversités. Tous nos postes sont ouverts aux personnes en situation de handicap.*

**CV à envoyer à : [recrutement@icm-institute.org](mailto:recrutement@icm-institute.org) en indiquant « Poste Ingénieur(e) Sécurité Systèmes Informatique (h/f) »**