L'HNFC recrute

TECHNICIEN SECURITE SI H/F

QUI SOMMES-NOUS ?

Né de la fusion de deux établissements et ouvert en 2017, l'Hôpital Nord Franche-Comté est un établissement moderne et récent. L'ensemble des sites est doté d'équipements à la pointe de la technologie qui vous permettront d'exceller dans votre spécialité.

Situé en Franche-Comté, il est proche de la frontière Suisse et de l'Allemagne et est desservi par l'aéroport de Bâle et une gare TGV.
Notre établissement propose un environnement de travail ressourçant et verdoyant au sein d'un patrimoine culturel et gastronomique riche.

NOS AVANTAGES

- Crèche dédiée à l'établissement
- CGOS + Amicale du personnel
- Self d'entreprise
- Association sportive
- Évènements festifs
- Ateliers bien-être

VOTRE POSTE

- Quotité de travail : 100 %
- Lieu d'exercice : Site de Trévenans et tous les autres sites de l'établissement
- Grade / fonction : Technicien supérieur
- Horaires : 37h30 / semaine
- Contraintes organisationnelles et relationnelles : Astreintes de semaine (2 à 3 / an) et de weekend (2 à 3 / an)

VOTRE SERVICE

Direction du Système d'Information / Equipe « Production »

ENVIRONNEMENT

- Environnements : 150 applications en production
- 500 serveurs virtuels / 100 serveurs physiques / 2 datacenters / 3000 postes de travail
- Socle technique : Linux, AIX, Microsoft Windows, Exchange, Active Directory, SCCM, SUS - Citrix - VmWare
- Antivirus TrendMicro - Sauvegarde Netbackup
- Outil de gestion des incidents/des changements : EasyVista
- SGBD : Oracle (RAC et DataGuard) - SQL Server - MySql

VOS MISSIONS

- **Mettre en place des mesures de sécurité pour protéger les systèmes informatiques**
  - Installer et configurer des pare-feu, des systèmes de détection d'intrusion, WAF,.. pour protéger les réseaux et les systèmes contre les attaques
  - Appliquer les politiques de sécurité et des procédures pour garantir la confidentialité et l'intégrité des données
  - Suivre les procédures des instances (ANSSI, …) pour améliorer les sécurités des systèmes
  - Tester les procédures de gestion des incidents de sécurité pour éprouver leur efficacité
- **Surveiller les réseaux pour détecter d'éventuelles vulnérabilités ou intrusions**
  - Mettre en place des systèmes de surveillance et d'alerte pour détecter les tentatives d'intrusion en lien avec le SOC
  - Effectuer des audits de sécurité réguliers pour identifier les vulnérabilités et mettre en place des mesures correctives
  - Analyser les logs et les journaux d'événements pour détecter les activités suspectes et les anomalies de sécurité
- **Répondre aux incidents de sécurité et mettre en place des mesures correctives**
  - Collaborer avec le SOC pour réagir face aux différentes alertes de sécurité
  - Mettre en œuvre les procédures de gestion des incidents de sécurité et coordonner les actions avec les équipes informatiques et de sécurité
  - Mettre en place des outils pour collecter et analyser les preuves et les informations relatives au incidents de sécurité

- Mettre en place des mesures correctives pour prévenir la répétition des incidents de sécurité et améliorer la sécurité globale des systèmes

- **Effectuer des tests de pénétration pour évaluer la sécurité des systèmes**
  - Planifier et organiser des tests de pénétration pour évaluer la sécurité des systèmes informatiques en interne et externe
  - Utiliser des outils et des techniques de test de pénétration pour simuler des attaques et identifier les vulnérabilités des systèmes
  - Analyser les résultats des tests de pénétration et rédiger des rapports détaillés sur les vulnérabilités identifiées et les mesures correctives recommandées
  - Collaborer avec les équipes informatiques et de sécurité pour mettre en place des mesures correctives et améliorer la sécurité des systèmes

- **Collaborer avec les équipes informatiques pour mettre en place des solutions de sécurité adaptées**
  - Travailler en étroite collaboration avec les équipes informatiques pour identifier les besoins en matière de sécurité et définir les solutions adaptées
  - Participer à la conception et à la mise en œuvre de projets informatiques en veillant à intégrer les considérations de sécurité dès la phase de conception
  - Assurer la maintenance et la mise à jour régulières des solutions de sécurité mises en place pour garantir leur efficacité et leur adéquation aux besoins

- **Assurer une veille technologique pour se tenir informé des dernières menaces et tendances en matière de cybersécurité**
  - Suivre régulièrement les actualités et les publications spécialisées dans le domaine de la cybersécurité pour se tenir informé des dernières menaces et tendances
  - Participer à des conférences, des ateliers et des formations pour approfondir ses connaissances et compétences en matière de cybersécurité
  - Échanger avec d'autres professionnels de la cybersécurité pour partager des informations et des bonnes pratiques
  - Tester et évaluer régulièrement de nouveaux outils et technologies de sécurité pour déterminer leur pertinence et leur efficacité
  - Analyser les rapports de sécurité et les alertes émis par les éditeurs de logiciels et les organismes de sécurité pour identifier les vulnérabilités et les menaces potentielles et mettre en place des mesures de protection adaptées.

VOS DIPLÔMES OU FORMATIONS

- Diplôme : Bac+2 ou Bac+3 en informatique avec une spécialité sécurité des systèmes d'information
- Expérience 3 ans minimum dans un poste équivalent
- Maitrise de l'anglais technique
- Permis B obligatoire

APTITUDES

Compétences / Connaissances

- Connaissances solides en cybersécurité (mise en place d'outils de sécurité et test d'intrusion) et dans les technologies de sécurité :
    - Connaissance des techniques d'attaque / APT
    - Expérience dans l'analyse et corrélation : analyse des journaux systèmes et applicatifs
    - Bonne connaissance technique des technologies telles que VPN, Firewall, WAF, IPS/IDS, Proxy/Reverse Proxy, EDR, SIEM
    - Capacité d'analyse de traces réseau
- Très bonnes compétences techniques générales sur les systèmes IT
    - Connaissances en administration Linux et Windows
    - Connaissance en réseau (adressage, routage, filtrage) et en virtualisation
- Capacité à rédiger des documentations de qualité (claires, concises, précises)
- Maîtrise des outils informatiques Word, Excel, Powerpoint, Outlook
- Capacité à rédiger des documentations de qualité (claires, concises, précises)
- Maîtrise de l'anglais technique

Qualités

- Qualités relationnelles / Esprit d'équipe / Discrétion / Sens très élevé du respect de la confidentialité des données
- Rigoureux, méthodique et organisé
- Capacité de travail : charge, multiplicité des sujets à traiter, sens de l'engagement
- Esprit curieux / autonome dans son travail