

POSTE

Branche d'activité professionnelle (B.A.P): **E : Informatique, Statistiques et Calcul scientifique**
 Famille d'activité professionnelle (F.A.P) : **Ingénierie technique et de production**
 Emploi-type : **E2B43 - Administrateur-trice systèmes et réseaux**
 Corps : **Ingénieur d'études**
 Nature du recrutement : **concours externe**
 Nombre de postes offerts : **1**

AFFECTATION

Etablissement : **Université de Pau et des Pays de l'Adour (UPPA)**
 Composante : **Direction du Numérique**
 Ville : **Pau**

MISSION

Affecté à la direction du Numérique, l'administrateur Systèmes et Réseaux aura pour mission générale, la mise en oeuvre et l'exploitation des dispositifs de sécurité Numérique. Ses missions principales :

- Contribuer à la sécurisation des dispositifs techniques ;
- Apporter une expertise technique en matière de Sécurité Numérique, avec pour objectif la préconisation et la mise en oeuvre de solutions et de méthodes ;
- Analyser les attaques observées sur les systèmes d'information de l'établissement, définir l'état de compromission, proposer des mesures adaptées et guider les victimes dans leur prise en compte.

Il est l'interlocuteur technique de l'équipe de Direction, du RSSI et des CSSI de l'UPPA ainsi que des partenaires externes à l'UPPA en charge de sécurité numérique (ANSSI, Cert Renater, ...).

METIER

Ingénieur Cybersécurité
 Administrateur de réseaux
 Administrateur de systèmes

ACTIVITES PRINCIPALES

- Contribuer à la définition des règles de sécurité à appliquer (dispositifs réseau, système, proximité, audiovisuel, applications) et des équipements de sécurité (parefeu, proxy, antivirus, authentification, ...) ;
- Préconiser et implémenter des solutions de sécurité, configurer et superviser les équipements de sécurité, de journalisation et de surveillance ;
- Analyser et interpréter les différentes remontées d'alertes issues de centres de détection, prendre les mesures correctives nécessaires ;
- Travailler et échanger avec les différents acteurs nationaux
- Contribuer aux contrôles et audits de sécurité (audit de configuration, d'architecture ou tests d'intrusion) et assurer le suivi de la correction des écarts identifiés ;
- Prendre en charge la documentation d'architecture technique des infrastructures ;
- Mener une veille technique sur le domaine de la sécurité numérique.
- Référencer et documenter les composants liés à l'infrastructure, aux logiciels et leurs liens avec la couche applicative
- Sécuriser la production (sauvegarder, sécuriser les flux, prévoir et mettre en pratique des solutions de repli ou de contournement (PRA, PCA)
- Gérer l'interconnexion de l'entité avec les réseaux extérieurs et gérer la mobilité des usagers
- Animer une équipe, piloter des projets
- Négocier avec les fournisseurs et les prestataires de services
- Assurer la veille technologique sur les différents aspects de l'infrastructure système et de communication (matériels, logiciels, architecture, protocole, mode de transferts)

CONDITIONS PARTICULIERES D'EXERCICE

Possibilité d'astreintes ou d'horaires décalés adaptés aux nécessités de service

COMPETENCES PRINCIPALES

CONNAISSANCES

- Détection et Réponse (SIEM, EDR/NDR/XDR, SOAR)
- Techniques d'attaques et contre-mesures (Test d'intrusion)
- Gestion des vulnérabilités (Scanners et analyse des rapports)
- Analyse Forensique
- Méthodes d'authentification sécurisée
- Cryptographie
- Sauvegardes
- Normes de sécurité numérique
- Sécurité des systèmes d'information et de communication (connaissance approfondie)
- Architecture et l'environnement technique du système d'information
- Méthodes de mise en production
- Normes d'exploitation
- Performance et métrologie
- Diagnostic et résolution de problèmes
- Techniques de virtualisation (connaissance approfondie)
- Méthodes, outils, normes et procédures de la qualité (connaissance générale)
- Langage de programmation (connaissance approfondie)
- Anglais technique (connaissance approfondie)

COMPETENCES OPERATIONNELLES

- Anticiper les évolutions fonctionnelles et techniques
- Gérer la sécurité de l'information
- Modéliser et concevoir les architectures techniques du système d'information
- Pratiquer une veille technologique
- Rédiger et mettre à jour la documentation fonctionnelle et technique
- Travailler en équipe
- Évaluer une solution informatique ou de télécommunication

COMPETENCES COMPORTEMENTALES

- Rigueur et sens du détail
- Esprit d'analyse et résolution de problèmes
- Curiosité et veille permanente
- Communication claire et adaptée
- Résistance au stress et gestion des urgences
- Travail d'équipe et collaboration
- Éthique et intégrité
- Réactivité, Adaptabilité et flexibilité

DIPLOME REGLEMENTAIRE EXIGÉ FORMATION PROFESSIONNELLE SI SOUHAITABLE

Être titulaire à la date de la première épreuve d'une licence ou d'un diplôme classé au moins au niveau 6 (anciennement niveau II).

TENDANCES D'EVOLUTION

FACTEURS D'EVOLUTION A MOYEN TERME

Sécurité sur les domaines systèmes et réseaux

IMPACTS SUR L'EMPLOI-TYPE (QUALITATIF)

Devenir expert sur l'ensemble des activités liées à la sécurité du numérique