Administrateur.trice de solutions logicielles de cybersécurité

Poste n°xxxx - Pôle Ressources Humaines et Modernisation – Direction de l'Innovation Numérique et des Systèmes d'Information – Pôle Stratégie des Systèmes d'Information (PSSI)	
Classification du poste	Type de domaine : Informatique Emploi-type : Chef de projet Fonction d'encadrement : NON Groupe IFSE : A4-1 Quotité de travail : 100%
Définition de l'emploi	Filière technique Poste de catégorie A relevant du cadre d'emplois des ingénieurs
Environnement du poste de travail	Direction : Direction de l'innovation numérique et des systèmes d'information Pôle : Stratégie des systèmes d'information Composition de l'équipe : 5 A Lieu d'affectation : Saint Denis
Position du poste dans l'organisation	Supérieur hiérarchique direct : Directeur de la DINSI

Raison d'être du poste : L'administrateur-trice participe à la conception et au maintien des systèmes d'information sécurisés. Il assure l'installation, la mise en production, l'administration et l'exploitation des solutions de sécurité du SI (on-premise ou SaaS.), en garantissant leur maintien en conditions opérationnelles et de sécurité. Il agit en interface technique entre les équipes projets, intégrateurs applicatifs, postes de travail, support et les équipes d'infrastructures.

Missions principales :

1/ Administration de sécurité

- Installer et configurer les outils de sécurité,
- Administrer les solutions de sécurité y compris celle de M365 (mises à jour, supervision, alertes),
- Définir et superviser la réalisation des prototypes et de preuves de concept (POC) et des tests fonctionnels de la solution ou de l'infrastructure de sécurité choisie,
- Effectuer la recette des solutions de sécurité et apprécier leur conformité au cahier des charges,
- Contribuer à la conception et à l'intégration des solutions de sécurité adoptées (incluant notamment les aspects d'architecture, la prise en compte des identités et des accès, le paramétrage des authentifications SSO M365 et de contribution à la stratégie de surveillance et de détection) et assurer leur suivi.

2/ Activités opérationnelles de cybersécurité

- Détecter, analyser et qualifier les incidents, les menaces et les attaques cyber,
- Identifier leurs sources, leurs mécanismes et bloquer leur accès aux solutions existantes,
- Orienter les équipes applicatives et techniques quant aux correctifs ou remédiation à mettre en œuvre pour sécuriser le réseau et les systèmes informatiques,
- Rédiger et documenter les procédures et assurer le suivi des actions,
- Veiller à leur application et à leur exploitabilité par tous les utilisateurs concernés.

	3 / Activités de gouvernance • Assurer le pilotage de la gouvernance de la supervision des vulnérabilités, • Participer aux orientations techniques du pôle cybersécurité, • Former et sensibiliser les utilisateurs aux enjeux de la sécurité, à la cybersécurité et aux outils de sécurité proposés par le Département.

Compétences

- **Relationnelles**
  - Savoir travailler en équipe et en transverse au sein de l'organisation,
  - Savoir alerter ses interlocuteurs ou sa ligne hiérarchique de façon constructive
  - Savoir organiser et animer des groupes projet,
  - Savoir s'exprimer auprès des partenaires internes et externes au nom de son service,
  - Capacité à gérer des situations de crise,
- **Organisationnelles**
  - Gestion de projets et de portefeuille de projets
  - Capacité à prendre en compte les nouvelles méthodes de gestion de projet
  - Savoir planifier la mise en œuvre de projets et des opérations et en définir les modalités de pilotage
  - Savoir organiser et animer des réunions et groupes de travail
  - Savoir organiser le travail en fonction des objectifs et de la charge de travail
  - Savoir établir des rapports de suivi et renseigner des indicateurs et tableaux de bord
  - Faire preuve de rigueur
- **Techniques**
  - Connaissance du système d'information et des principes d'architecture
  - Maîtrise des fondamentaux dans les principaux domaines de la SSI
  - Connaissances des solutions de sécurité du marché
  - Connaitre les principes de sécurisation des environnements exposés sur Internet
  - Connaitre les méthodes d'homologations de sécurité
  - Définir les règles opérationnelles d'un système de gestion de la sécurité de l'information
  - Savoir formuler des avis et rédiger des rapports d'aide à la décision

Moyens mis à disposition

Niveau d'études : BAC + 5
Diplômes requis : Ingénieur ou Master Cybersécurité

Expérience (s) professionnelle(s) sur un poste similaire

Requise(s)
- Formations et diplômes nécessaires à l'accès au cadre d'emplois des ingénieurs,
- Expérience en cybersécurité, en supervision de vulnérabilités
- Expérience en pilotage de projet informatique
- Maitrise des fondamentaux des principaux domaines de la sécurité des SI et de l'IA
- Connaissance des menaces numériques
- Maîtrise des outils de sécurité (EDR / XDR, vulnérabilités, simulation phishing, contrôle de logs, ...)

Souhaitée(s)
- AD, Entra ID / Azure, administration tenant M365, Microsoft Defender, EDR/XDR, SOC, SIEM, IA,
- Connaissance des systèmes Microsoft, Linux, de la sécurité des réseaux et protocoles

Caractéristiques principales liées au poste

☒ Interventions possibles hors temps ouvrable notamment le week-end
☐ Permis de conduire obligatoire
☐ Déplacements province et étranger
☐ Astreintes
☐ Logement de fonction
☐ Vaccins obligatoires
☐ Port d'une tenue de travail obligatoire