

POSTE VACANT D'UN ANALYSTE EN SECURITE ET CONFIDENTIALITE SOUS LE STATUT DE L'EMPLOYE PUBLIC (M/F) DANS LE GROUPE D'INDEMNITE A1

Infos clés

Carrière : Employé public dans le groupe d'indemnité A1

Type de recrutement : Externe

Type de contrat : Contrat à durée déterminée de deux ans

Tâche : Tâche complète ou à temps partiel

Date limite de candidature : 11 mai 2025

Date de publication : 18 avril 2025

ORGANISME RECRUTEUR

Commission nationale pour la protection des données (CNPD)

ORGANISME D'AFFECTATION

Commission nationale pour la protection des données (CNPD)

MISSIONS

La CNPD recherche un Analyste en Sécurité et Confidentialité spécialisé en reverse engineering pour rejoindre notre équipe. Votre mission principale sera d'évaluer les produits et services numériques afin de vérifier leur conformité avec la réglementation applicable (en ce inclus le Règlement Général sur la Protection des Données (RGPD), le Règlement sur l'Intelligence Artificielle et le Règlement sur la Cyber Résilience) et les politiques de confidentialité déclarées.

Vous utiliserez des techniques avancées de reverse engineering pour détecter et analyser les vulnérabilités des produits, services, systèmes et applications et de leur environnement pouvant impliquer des modèles d'intelligence artificielle et recommander les mesures de mitigation à mettre en oeuvre.

Vos responsabilités consisteront en :

- Analyser des systèmes et produits numériques pour vérifier leur conformité avec le RGPD, le Règlement IA et d'autres réglementations applicables ;
- Utiliser des techniques de reverse engineering pour examiner le code source (ou le cas échéant le code compilé) et les comportements des applications de système d'IA ;

- Identifier les failles de sécurité et les pratiques de collecte de données non conformes aux réglementations applicables ou au plan de test déclaré ;
- Rédiger des rapports détaillés sur les résultats des analyses, incluant des recommandations pour améliorer la conformité et la sécurité ;
- Collaborer avec les équipes techniques pour corriger les vulnérabilités identifiées ;
- Participer à des audits de sécurité et de conformité ;
- Rester à jour avec les évolutions réglementaires et les meilleures pratiques en matière de sécurité et organiser des présentations techniques de l'état de l'art aux équipes internes ;
- Participer à des réunions au niveau national ou international dans les groupes de travail dédiés.

PROFIL

Les candidats doivent être titulaires d'un grade ou diplôme délivré par un établissement d'enseignement supérieur reconnu par l'Etat du siège de l'établissement et sanctionnant l'accomplissement avec succès d'un master en informatique, cybersécurité, ou un domaine connexe. Les grades ou diplômes visés doivent être inscrits au registre des titres de formation prévu par la loi modifiée du 28 octobre 2016 relative à la reconnaissance des qualifications professionnelles.

Compétences techniques :

- Expérience confirmée en reverse engineering et analyse de logiciels ;
- Solide compréhension du RGPD et des politiques de confidentialité ;
- Maîtrise des outils de reverse engineering (IDA Pro, Ghidra, etc.) et des langages de programmation (C, C++, Java, Python etc.) ;
- Excellentes compétences en rédaction de rapports techniques ;
- Capacité à travailler de manière autonome et en équipe ;
- Bonne communication écrite et orale en français et en anglais.

Compétences comportementales :

- Capacité d'apprentissage et d'adaptation ;
- Sens de la collégialité et responsabilité individuelle ;
- Faire preuve d'objectivité ainsi que d'une confidentialité et d'une discrétion absolue ;
- Capacité à travailler individuellement ou en équipe ;
- Être autonome et responsable ;

- Ouverture au changement et à l'innovation, vous vous ouvrez à la diversité et vous vous intéressez à d'autres disciplines.

Langues :

Les candidats doivent répondre aux exigences de la connaissance des trois langues administratives pour le groupe de traitement A1. Une bonne maîtrise de la langue anglaise est requise.

DOCUMENTS A FOURNIR

La candidature doit obligatoirement être accompagnée :

- d'une lettre de motivation ;
- du curriculum vitae, certifié sincère et mentionnant de façon détaillée notamment la formation scolaire et l'expérience professionnelle acquises antérieurement par le candidat ;
- d'une copie du/des diplômes et/ou certificats requis pour la formation demandée.

Les candidats présentant des diplômes étrangers sont priés de joindre :

- l'inscription au registre des titres des diplômes universitaires, délivré par le Ministère de l'Enseignement supérieur et de la Recherche.

ADRESSE D'ENVOI

Les demandes sont à adresser jusqu'au **11 mai 2025** au plus tard à la

Commission nationale pour la protection des données
Service Ressources Humaines

15, boulevard du Jazz
L-4370 Belvaux

par voie électronique à l'adresse rh@cnpd.lu

RENSEIGNEMENTS

Madame Maryse WINANDY, Tél: 26 10 60 – 1, E-mail: rh@cnpd.lu

COMMENTAIRES EVENTUELS

* Ce poste est ouvert aux ressortissants des Etats membres de l'Union européenne.