

Offre d'emploi H/F

Ingénieur(e) de recherche en Data Science pour la cybersécurité

Niveau requis : BAC+5 ou doctorant(e) en informatique ou équivalent

Structure d'accueil : Laboratoire Informatique et Société Numérique (LIST3N) - Université de Technologie de Troyes. Quelques déplacements à prévoir.

Projet : MobileGuard®

Mots clés : Cybersécurité, détection d'anomalies, smartphones, MDM (Mobile Device Management), statistique, intelligence artificielle.

Type et durée du contrat : CDD de 12 mois (renouvelable)

Prise de poste : 1er novembre 2026

Contexte

Le projet MobileGuard®, soutenu par le **Programme de Transfert au Campus Cyber (PTCC)**, vise à développer un module MTD (Mobile Threat Defense) innovant pour l'anticipation et la détection des menaces sur les terminaux mobiles en entreprise. Porté par l'Université de Technologie de Troyes (UTT) et l'entreprise Mobile Process, ce projet s'inscrit dans une démarche de renforcement de la **cybersécurité souveraine en France**. L'objectif est d'intégrer des algorithmes prédictifs et explicatifs dans une solution MDM (Mobile Device Management) existante, afin de détecter proactivement les risques de compromission des données ou des applications et d'automatiser des réponses adaptées.

Missions

Dans le cadre de ce projet, l'ingénieur(e) recruté(e) sera amené(e) à :

- Concevoir et développer un outil de collecte des données des terminaux nomades (identification des données complémentaires collectables, développement de l'outil logiciel, validation),
- Analyser les risques et identifier les cas critiques (définition des événements redoutés, analyse des risques, proposition de mesures de réduction),
- Mettre en place des algorithmes de détection d'anomalies (détection comportementale, intelligence artificielle, tests et validation),
- Assurer l'intégration du module MTD à la solution MDM de Mobile Process, les expérimentations et la validation du module,
- Collaborer avec les équipes de Mobile Process et de l'UTT pour garantir une solution robuste, explicable et adaptée aux contraintes opérationnelles (souveraineté, frugalité, respect de la vie privée).

Profil recherché

- Formation : Diplôme de niveau BAC+5 (école d'ingénieur, master) ou doctorat en informatique, data science, cybersécurité, ou domaine connexe.
- Expérience : Expériences significatives en traitement de données, en apprentissage automatique et en développement d'algorithmes.

Compétences recherchées

Nous recherchons un(e) ingénieur(e) ou post-doctorant(e) en Data Science, avec une expertise avérée dans les domaines suivants :

Compétences techniques

- Connaissances en cybersécurité (audit, risques et conformité), en analyse comportementale des terminaux mobiles et en détection d'anomalies,
- Maîtrise des langages de programmation : C++ (atout), Java, Python, Javascript, React,
- Maîtrise des bases de données : MySQL, PostgreSQL,
- Expérience en gestion de données (gouvernance, sécurité, habilitation, rôles et droits),
- Connaissances en statistiques avancées, en modélisation mathématique et IA,
- Connaissances en Mobile Device Management (MDM) et en sécurité des systèmes mobiles (Android),
- Connaissances en conception d'indicateurs (KPI) et de tableaux de bord.

Compétences transversales

- Capacité à travailler en équipe pluridisciplinaire (recherche académique et développement industriel),
- Bonne capacité de rédaction (publications scientifiques, rapports techniques),
- Maîtrise de l'anglais technique (lu, écrit, parlé).

Qualités attendues

- Rigueur et méthodologie dans la conduite des travaux de recherche et développement,
- Esprit d'équipe et capacité d'adaptation dans un environnement dynamique,
- Curiosité scientifique et envie d'apprendre dans un domaine en constante évolution,
- Sens de l'autonomie et de l'organisation pour respecter les échéances et les livrables du projet,
- Éthique professionnelle et respect des règles de confidentialité (RGPD, propriété intellectuelle).

Candidature

- Le dossier devra comprendre un CV, une lettre de motivation et des exemples de réalisations (portfolio-GitHub ou autre).
- Les candidatures devront être adressées avec pour objet « Candidature Projet MobileGuard® » **avant le 30 septembre 2026** à contact@mobileguard.fr
- En raison des délais de recrutement, cette offre s'adresse aux personnes disposant déjà des autorisations nécessaires pour un CDD en France à la date de prise de poste. Aucune nouvelle procédure d'autorisation et de visa ne pourra être engagée.