Civils de la Défense

Plateforme de recrutement de personnel civil
contractuel du ministère des Armées

Expert sécurité de l’IA F/H

Bruz, 35, Ille-et-Vilaine, Bretagne

Type de contrat	Niveau d'études
CDD 3 ans renouvelable	Bac + 5 (MASTER - DEA - DESS - ING) ou équivalent
Prise de fonction souhaitée	**Date limite de candidature**
01/07/2025	01/05/2025
Domaine professionnel	**Niveau d'expérience**
Systèmes d'information	Confirmé (5 à 10 ans)
Rémunération	**Avantages liés au poste**
Selon grille DINUM mensuel net Selon grille DINUM annuel brut (selon expérience)	Restauration collective Parking RTT
Contraintes particulières d'exercice	**Télétravail**
Déplacements fréquents en France Habilitation particulière (voir descriptif de l'offre)	Non

Descriptif de l'organisation

Dans le contexte géopolitique actuel, vous cherchez à participer à des initiatives d'envergure nationale et donner du sens à votre activité ? Pour vous il est important que la France soit un acteur majeur de l’Intelligence Artificielle de Défense et maintienne son avance technologique dans les années à venir ? La nouvelle Agence Ministérielle pour l’IA de Défense (AMIAD) recrute des ingénieurs civils talentueux et motivés. Rejoignez notre équipe pour façonner l’avenir de l’IA.
L'AMIAD est chargée de piloter les projets d'envergure en matière d’IA. Avec toutes les entités du Ministère, elle intervient, à travers des développements internes ou en lien avec des acteurs industriels et académiques, sur des projets couvrant un large domaine d'activité : systèmes d’armes, opérations, renseignement, commandement, soutien, administration. Vous disposerez de moyens techniques conséquents et bénéficierez d’une grande autonomie pour réaliser des choix techniques pertinents.

Descriptif des missions

Au sein de l’AMIAD votre rôle est de piloter les travaux autour de la sécurité de l’IA, et plus particulièrement de la prise en compte des vulnérabilités inhérentes aux algorithmes d’IA. Cela passera par la conception, le développement et la mise en œuvre de solutions d’audit et de

sécurisation/robustification des briques d’IA face à des attaques malveillantes en vue de leur intégration dans des systèmes opérationnels. A ce titre, vous êtes donc amené(e) à réaliser des prestations techniques au profit des projets intégrant de l’IA :• Effectuer une veille permanente sur les avancées technologiques en rapport avec l’analyse des vulnérabilités particulières à l’utilisation d’IA (empoisonnement des données, porte dérobée, évasion, extraction d’informations sensibles, injection de prompts, etc.),
• Participer à la prise en compte de la sécurité de l’IA dans les processus de mise en place des systèmes opérationnels,
• Développer et expérimenter les approches à l’état de l’art afin de sécuriser les briques d’IA,
• Suivre les processus émergents dans le domaine de l’IA de confiance sur la sécurité de l’IA, notamment au niveau national et européen,
• Contribuer à la spécification technique de contrats, à l’évaluation et au suivi de projets industriels et académiques,
• Porter l’expertise technique sur l’analyse des risques secAI et les stratégies de mitigation lors des commissions d’export de systèmes opérationnels intégrant de l’IA.

#Intelligence Artificielle #Apprentissage Machine #Réseaux de neurones #Vulnérabilités #Risques et Sécurité #IA de confiance #MLSecOps #SecAI #adversarial #backdoor #privacy #jailbreak #prompt-injection

REF 2024-AMIAD-13 #AMIAD

Profil recherché

Titulaire d’un diplôme de niveau bac+5 et d’au moins trois années d’expérience, vous possédez des compétences solides sur plusieurs sujets parmi les suivants :· Le machine learning et l’apprentissage profond (Deep Learning),· La sécurité de l’IA et l’analyse des vulnérabilités particulières à l’IA,· La sécurité des systèmes d’information et l’analyse de risques malveillants.

Le poste s’inscrivant dans la montée en puissance de l’activité au profit du ministère des armées, vous savez faire preuve d’autonomie, aimez le travail d’équipe, êtes organisé et méthodique, avez de bonnes qualités relationnelles.

Process de recrutement

Le poste nécessitant d'accéder à des informations relevant du secret de la défense nationale, vous ferez l'objet d'une procédure d’habilitation, conformément aux dispositions des articles R.2311-1 et suivants du Code de la défense et de l’IGI n°1300 du 09 août 2021.
Les entretiens de recrutement (techniques, RH et management) auront lieu à DGA MI Bruz.Le salaire et les responsabilités seront déterminés en fonction de vos compétences et de votre expérience professionnelle