Civils de la Défense
Plateforme de recrutement de personnel civil
contractuel du ministère des Armées

Ingénieur Cybersécurité F/H

Bruz, 35, Ille-et-Vilaine, Bretagne

Type de contrat	Niveau d'études
CDI	Bac + 5 (MASTER - DEA - DESS - ING) ou équivalent
Prise de fonction souhaitée	**Date limite de candidature**
20/01/2027	-
Domaine professionnel	**Niveau d'expérience**
Cybersécurité	Confirmé (5 à 10 ans)
Rémunération	**Avantages liés au poste**
Selon grille DINUM mensuel net Selon grille DINUM annuel brut (selon expérience)	Restauration collective RTT Proximité transports en commun
Contraintes particulières d'exercice	**Télétravail**
Permis B obligatoire	Oui

Descriptif de l'organisation

Vous souhaitez donner du sens à votre activité et prendre part à des projets d'envergure nationale comportant de forts enjeux, et contribuer à l'avance technologique et à la souveraineté de la France dans le domaine de l'IA en soutenant les forces armées ? Vous souhaitez rejoindre une équipe projet dynamique et agile, animée par un esprit start-up et tournée vers l'excellence opérationnelle ?

Alors, postulez et rejoignez l'AMIAD.

L'Agence Ministérielle pour l'IA de Défense. Rattachée au ministre des armées, l'AMIAD est une entité en pleine expansion qui mène des projets IA d'envergure, en collaboration avec toutes les entités du ministère et sur de nombreux domaines d'activité (systèmes d'armes, opérations, renseignement, commandement, soutien, administration).

Descriptif des missions

Au sein de l'équipe « Systèmes d'Informations et Données Relationnelles », composée d'ingénieurs en IA et en Cybersécurité, en qualité d'Ingénieur Cybersécurité, vos missions principales sont les

suivantes :

• Concevoir et implémenter des solutions IA innovantes pour optimiser et sécuriser les systèmes d'information, incluant par exemple le développement d'outils d'aide à la rétro-ingénierie de code assistée par IA.
• Préparer, structurer et analyser des jeux de données pour développer et évaluer nos solutions IA.
• Concevoir et implémenter des agents intelligents utilisant des techniques d'IA agentique afin de renforcer la supervision des systèmes d'information.
• Évaluer les performances des méthodes et modèles développés pour garantir leur efficacité.
• Collaborer avec les équipes métier pour co-construire des solutions IA adaptées aux besoins opérationnels.
• Assurer une veille technologique proactive dans le domaine de l'IA et de la Cybersécurité afin d'identifier les innovations les plus pertinentes.
• Participer à la rédaction de documentations techniques et de rapports d'analyses afin de faciliter la prise de décision et le partage des connaissances.

Pour les profils les plus expérimentés, vous serez également responsable de conduire des projets stratégiques, en pilotant des équipes pluridisciplinaires et en prenant des décisions éclairées pour répondre aux défis complexes de Cybersécurité.

Profil recherché

Titulaire d'un diplôme de niveau bac + 5 en Cybersécurité, vous avez au moins 5 ans d'expérience dont une expérience en audit de sécurité, analyse forensic, pentest ou gestion d'incidents.

Ainsi, vous maitrisez : • Les systèmes d'exploitation (Windows et Linux), les protocoles réseaux (TCP/IP, DNS, VPN) et les outils de supervision (événements Windows, Sysmon, Syslog, EDR)
• Les principaux SIEM, et éventuellement certaines technologies de traitement des données
• Les mécanismes d'attaques, les techniques et outils d'intrusion cyber.
• Les frameworks et outils de cybersécurité (Metasploit, Burp Suite, etc)
• Les langages Python et C.

Vous avez des notions en apprentissage automatique et suivez les évolutions récentes de l'écosystème de l'IA, notamment les LLM (Large Language Models), et les approches d'IA générative et agentique.

Doté d'un fort esprit d'équipe, autonome, proactif et bon communicant, vous savez expliquer des concepts techniques complexes à des interlocuteurs variés.

Process de recrutement

1. Échange téléphonique pour vérifier l'adéquation du profil et des aspirations par rapport au poste.
2. Entretiens sur site : entretien avec les collaborateurs techniques et le management, entretien RH (prévoir ½ journée)

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.

NB : Le poste est à pourvoir en CDD ou CDI selon profil et expérience