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

Ingénieur en système de cyberdéfense F/H

Type de contrat	Niveau d'études
CDI (ASC)	Bac + 5 (MASTER - DEA - DESS - ING) ou équivalent
Prise de fonction souhaitée	**Date limite de candidature**
03/05/2027	-
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**
Habilitation particulière (voir descriptif de l'offre)	Non

Descriptif de l'organisation

Le ministère des armées assure la protection du territoire, de la population et des intérêts français. Il est également DGA Maîtrise de l'Information est l'expert technique du Ministère des Armées pour les systèmes d'information et de communication, la cybersécurité, la guerre électronique, les fonctions de navigation des systèmes d'armes et les systèmes de missiles.
Au sein du principal centre d'expertise de la direction technique de la DGA, vous contribuez à la réalisation de l'outil de défense et à la préparation des programmes futurs.

Descriptif des missions

Le titulaire du poste sera intégré au sein d'une équipe chargée de conseiller et soutenir les projets d'équipement des différents SOC (Security Operation Center) du ministère des armées.
Les missions sont variées et couvrent les activités suivantes : • Caractériser des produits qui équipent les SOC : gestion de la connaissance de la menace (CTI : Cyber Threat Intelligence), détection d'intrusion (sondes réseau, EDR, SIEM, …), investigations numériques (prélèvement, analyse de malwares, …)…
• Proposer et valider des architectures systèmes qui intègrent ces différents types de produits
• Capitaliser des moyens d'expertise et d'évaluation tels que des infrastructures représentatives d'un SOC ou d'un système à surveiller, des jeux de données réels ou synthétiques, des bancs de test

automatisés, …

Cela implique de maitriser à la fois des techniques de surveillance et détection mais également de savoir mettre en œuvre des techniques offensives qui vont permettre tester les capacités de détection. Du temps est réservé à une activité de veille sur les menaces et l'évolution des techniques de détection. Tirer parti de l'évolution rapide des capacités d'intelligence artificielle est un des enjeux majeurs pour répondre à une menace dont l'évolution est constante et garantir la pertinence des résultats.

Mots clés : #détection intrusion, #edr, #nids, #siem, #sandbox, #honeypot, #cyberrange, #python, #C, #IA, #Machine learning, #LLM #cyberexpert

Profil recherché

Connaissances métier :• Mise en œuvre d'une ou plusieurs solutions de supervision de la sécurité et de détection d'intrusion (SIEM, sondes de détection d'intrusion, honeypot, sandbox, …)
• Connaissance du comportement des malwares et de techniques d'exploitation
• Rédaction de stratégie d'évaluation, de dossier de synthèse et de référentiel technique
• Développement pour la réalisation de preuve de concept

Connaissances générales :• Sécurité informatique
• Réseau/Télécommunication (VoIP, Active Directory, SDN, Cloud, …)
• Intelligence artificielle, Machine Learning, LLM, développement d'agents
• Techniques de virtualisation
• Windows, Linux
• Développement informatique : C, C++, Go, Rust. Scripting (bash, python, …)

Qualités personnelles :• Rigueur, Autonomie, Créativité, Curiosité

Process de recrutement

Les entretiens de recrutement auront lieu à DGA MI Bruz. Le salaire sera déterminé en fonction de l'expérience et de l'emploi de raccordement au référentiel des métiers du numérique de l'Etat (DINUM) version 2021.
Le poste pouvant nécessiter d'accéder à des informations relevant du secret de la défense nationale, le titulaire fera 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.