ANSSI - Agence nationale de la sécurité des systèmes d'information

Mise en œuvre d’un système d’Intelligence Artificielle de type RAG F/H

Paris 15e Arrondissement, 75, Paris, Île-de-France

Type de contrat	Niveau d'études
Stagiaire école	Master 1 ou titre équivalent de niveau Bac +4
Prise de fonction souhaitée	**Date limite de candidature**
03/02/2025	-
Domaine professionnel	**Niveau d'expérience**
Spécialiste sécurité d'un domaine technique	Etudiant
Rémunération	**Avantages liés au poste**
Gratification ou rémunération légale mensuel net Gratification ou rémunération légale annuel brut (selon expérience)	-
Contraintes particulières d'exercice	**Télétravail**
-	Non

Descriptif de l'organisation

Rejoindre l’Agence nationale de la sécurité des systèmes d’information (ANSSI), c’est mettre ses compétences au service de l’intérêt général en participant à une mission capitale, d’actualité et porteuse de grandes responsabilités dans un monde où la cybersécurité est devenue l’affaire de tous !
Vous êtes passionné(e) par la technique, la sécurité informatique et les LLM ? Rejoignez le Bureau Sécurisation des Systèmes (BSS) au sein de la Division Assistance Technique (DAT) qui aide les administrations et les entreprises à augmenter le niveau de sécurité de leurs systèmes d’information d’importance vitale pour la France.

Descriptif des missions

Objectif du stage :
Ce stage est une occasion de participer à un projet concret tout en renforçant votre expertise sur l'IA et la sécurité grâce à l'accompagnement des experts cyber de la division.
L'objectif principal du stage est le déploiement d'un outil d'aide aux agents qui répondent à une boite aux lettres d'assistance technique en s'appuyant sur une base de connaissances.
La démarche à mettre en œuvre est exploratoire de type R&D avec pour finalité la mise en place d'une maquette d'un modèle RAG LLM pour l'extraction d'information et la génération d'une ébauche de réponse qui pourra être reprise par les agents.

La mission consistera à conduire une partie des taches suivantes en fonction de la durée du stage :• Etudier le choix d'outil pour instancier un RAG (Retrieval Augmented Generation) et les différentes méthodes de récupération de données dans un bibliothèque de connaissances
• Etudier les choix d'un LLM (Large Language Model) open source déployable sur une infra interne
• Déployer une maquette et utiliser les guides ANSSI pour création de la base de connaissances
• Etudier les outils de tests automatisés de sécurité d'un LLM (ex : Garak) et leur intégration pour valider le projet et mesurer l'impact des différentes évolutions
• Etudier la mise en œuvre d'optimisation du RAG :
• Evaluation d'autres méthode d'indexation et récupération de données (graphes de connaissances, ontologies, …) pour la création de la base de connaissances.
• Evaluer les méthodes de filtrage afin de réduire les hallucinations.
• Revoir le prompt système.
• Etudier la sécurisation de l'infra du RAG
• Etude sur réduction des injections de prompt

Chaque étude donnera lieu à la rédaction d'une documentation et à une évolution de la maquette (si résultat pertinent). Ces évolutions sont axées sur le déploiement ou la configuration d'outils et pas sur du codage.
Vous ferez, de manière régulière, des restitutions des travaux en revue de pairs et des démonstrations.

Profil recherché

Vous êtes étudiant(e) en Master ou fin de cursus d'écoles d'ingénieurs avec une spécialité orienté informatique et en recherche d'un stage d'une durée de 4 à 6mois.
Compétences requises :• Une connaissance des concepts de LLM et de RAG ;
• Être assez autonome sur le déploiement d'une petite infrastructure de serveurs virtualisés et/ou conteneurisés ;
• Connaissance de système d'exploitation open source

Qualités attendues : • Curiosité d'esprit et rigueur ;
• Curiosité et appétence pour les sujets techniques ;
• Autonomie ;
• Capacité de rédaction et de synthèse.

Process de recrutement

• Si votre candidature est présélectionnée, vous serez contacté(e) pour apprécier vos attentes et vos motivations au cours d'un entretien téléphonique ou physique.
• Des tests techniques pourront vous être proposés.
• Vous ferez l'objet d'une procédure d'habilitation.