Alternant IA au service de la cybersécurité (H/F)

POSTE BLC N°087/2026

DEFINITION ET CARACTERISTIQUES DU POSTE

CONTEXTE :

Dans un contexte où les volumes d'évènements de sécurité augmentent constamment, l'Intelligence Artificielle constitue un levier majeur pour améliorer la détection des menaces, accélérer les investigations et assister les architectes de cybersécurité.

MISSION :

Au sein de l'équipe Cybersécurité du service SDP/SIE, vous participerez à un projet stratégique visant à intégrer des modèles d'IA à nos moyens de détection afin de renforcer nos capacités d'analyse et de réponse aux incidents.

Cette alternance vous permettra de conduire un projet de bout en bout, depuis l'étude de l'existant jusqu'au déploiement d'une solution opérationnelle.

1. Réaliser un benchmark des solutions d'IA appliquées à la cybersécurité

Vous étudierez les solutions du marché (open source et commerciales) permettant d'exploiter l'IA dans un contexte SOC et SIEM.

À ce titre, vous serez amené(e) à :

- Assurer une veille technologique sur les innovations en IA appliquées à la cybersécurité ;
- Comparer différentes solutions (LLM, IA générative, moteurs RAG, IA locale, assistants SOC, etc.) ;
- Evaluer leurs performances, leur coût, leur facilité d'intégration, leur niveau de sécurité et leur conformité aux exigences de confidentialité ;
- Identifier les cas d'usage les plus pertinents pour notre environnement ;
- Formuler des recommandations argumentées.

2. Concevoir et développer une preuve de concept (POC)

Vous participerez à la conception et à la réalisation d'un prototype permettant de démontrer l'apport de l'IA dans l'analyse des événements de sécurité.

Vous serez notamment chargé(e) de :

- Réaliser un cahier des charges selon les résultats du benchmark ;
- Formaliser une méthodologie de projet ;
- Définir l'architecture technique du POC ;

- Installer et configurer les composants nécessaires ;
- Interfacer la solution avec nos moyens ;
- Développer les scripts, API ou connecteurs nécessaires ;
- Mettre en oeuvre plusieurs cas d'usage, tels que :
    - Assistance à l'investigation ;
        - Synthèse automatique des incidents ;
        - Enrichissement contextuel des alertes ;
        - Détection d'anomalies ;
        - Génération de recommandations de remédiation.

3. Évaluer les performances de la solution

Vous définirez les critères d'évaluation du POC et mesurerez sa valeur ajoutée.

Vous serez amené(e) à :

- Définir des indicateurs de performance (Key Performance Indicator) ;
- Mesurer les gains obtenus (temps d'analyse, qualité des réponses, pertinence des résultats) ;
- Identifier les limites techniques et fonctionnelles ;
- Rédiger un rapport d'évaluation présentant les bénéfices, les risques et les axes d'amélioration.

4. Participer à l'industrialisation

Selon les résultats obtenus, vous contribuerez au déploiement de la solution dans un environnement opérationnel.

- Vos missions pourront inclure :
- L'automatisation du déploiement ;
- La documentation technique et fonctionnelle ;
- La rédaction des procédures d'exploitation ;
- L'accompagnement des équipes dans la prise en main de la solution ;
- La proposition de nouveaux cas d'usage.

PROFIL :

Diplôme et/ou expérience requise (en années) :

- Vous préparez un Master 2 (ou dernière année d'école d'ingénieur) spécialisé en cybersécurité, sécurité des systèmes d'information ou intelligence artificielle.

Compétences techniques (Savoir-faire) :

- De bonnes connaissances des systèmes Linux et des réseaux ;
- Des notions sur les architectures SIEM et le fonctionnement d'un SOC ;
- Une bonne maîtrise du scripting ;
- Un intérêt marqué pour les technologies d'IA générative et les modèles de langage (LLM) ;
- Des capacités d'analyse et de résolution de problèmes..

Qualités professionnelles (Savoir-être) :

- Curiosité technique et goût pour l'innovation ;
- Esprit d'analyse et sens critique ;
- Autonomie et capacité à prendre des initiatives ;
- Rigueur et méthode dans la conduite des expérimentations ;
- Capacité à vulgariser et à synthétiser des sujets techniques ;
- Bonnes qualités rédactionnelles ;
- Sens du travail en équipe et aptitude à collaborer avec différents interlocuteurs ;
- Force de proposition et volonté d'amélioration continue.

Les candidatures seront examinées au regard des besoins de l'entreprise, des prérequis du poste et des compétences individuelles en accord avec notre politique de promotion de l'égalité professionnelle dans

l’entreprise.

En notre qualité d’EPIC (Etablissement Public à Caractère Industriel et Commercial), un principe de neutralité (notamment religieuse) s’applique à tous les collaborateurs du CNES.

DATE D’ENTREE EN FONCTION*: Au plus tôt*

Postulez directement sur le site internet du CNES : CLIQUEZ ICI !!