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

Stage - génération automatique de règles YARA F/H

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

Type de contrat	**Niveau d'études**
Stagiaire école	Diplôme d'ingénieur, Master 2 ou titre équivalent de niveau Bac + 5
Prise de fonction souhaitée	**Date limite de candidature**
03/02/2025	18/12/2024
Domaine professionnel	**Niveau d'expérience**
Analyste de la menace cybersécurité	Junior (1 à 5 ans d'expérience)
Rémunération	**Avantages liés au poste**
A définir selon expérience mensuel net A définir selon expérience 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 !

Au sein de la Sous-Direction Expertise (SDE), La Division Scientifique et Technique (DST), le Laboratoire Exploration et Recherche en Détection (LED) est en charge du domaine de la détection et de l'analyse des attaques informatiques contre les systèmes d'information, incluant notamment la détection d'intrusion, l'analyse de systèmes compromis ou de logiciels malveillants. Il réalise le développement et l'adaptation de démonstrateurs visant l'amélioration de la capacité de détection d'attaque et d'analyse de systèmes, et il collabore avec les équipes opérationnelles sur ces

thématiques.

Descriptif des missions

Les règles YARA sont omniprésentes dans le domaine de la détection et de la CTI (Cyber Threat Intelligence) pour le suivi et la classification de codes malveillants. Ce stage s'intéresse à la génération automatique de règles YARA.

Les missions sont les suivantes:

• Dresser l'état de l'art ;
• Mettre en œuvre un banc d'évaluation des outils et techniques identiques pour étudier la qualité de règles YARA générées au regard d'un contexte opérationnel ;
• Identifier les résultats obtenus qui permettront de faire des propositions d'amélioration sur les approches évaluées et éventuellement de les implémenter et de les tester ;
• Les méthodes étudiées pourront être a base d'apprentissage machine (IA) ou basées sur de la connaissance métier Il sera important de tester et proposer des méthodes interprétables et facilement modifiables par les operateurs ;
• Ces méthodes feront également l'objet d'une étude (statistique) de leurs performances.

Profil recherché

Etudiant en dernière année d'école d'ingénieur ou cursus universitaire voire équivalent dans le domaine des nouvelles technologies (informatique/mathématiques). Avoir de l'appétence pour l'études orienté recherche et pour le domaine de la cybersécurité dont plus particulièrement pour les problématiques où pour l'outillage associés à la CTI (Cyber Threat Intelligence).

Compétences requises• Maitriser la programmation en Python, les principaux formats de fichier exécutables (PE et ELF) et avoir des connaissances en mathématiques appliquées (statistiques) ;
• Connaissances des systèmes d'exploitation ;
• Connaissances du désassemblage et assembleur (x86) ;
• Connaissance en apprentissage machine (IA, machine learning, deep-learning).

Savoir être • Curiosité d'esprit et rigueur ;
• 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.