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

Stage - similarités entre binaires en contexte opérationnel 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

La capacité à déterminer des similarités entre binaires a de nombreuses applications, allant de la détection de clones à la classification en passant par la détection de vulnérabilités ou la comparaison de binaires. C'est un outil puissant pour la rétro-ingénierie logicielle.

Au cours de ce stage vous êtes amené à faire un état des lieux des méthodes :• Existantes pour construire des similarités entre binaires ;
• Inclura dans un premier temps une recherche bibliographique associée à l'implémentation d'un banc de tests commun permettant d'évaluer les techniques et outils retenus en relation avec un contexte opérationnel d'analyse et de chasse des codes malveillants ;
• Être amené à faire une synthèse de ces résultats qui devront préciser le contexte d'exploitation de chaque solution (par exemple l'algorithme traite t-il de similarités entre fichiers ou fonctions ? Doit-on de désassembler le fichier ou peut-on travailler directement sur code binaire ? etc.) ainsi que ses points forts et ses limites.
• Proposer des axes d'amélioration ou de nouvelles méthodes de calcul dissimilarités ;
• Comparer des méthodes basées sur de la connaissance métier ou sur de l'apprentissage machine (IA).

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 pour les problématiques et l'outillage associé à l'analyse de codes malveillants.

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) ;
• Capacité de rédaction et de synthèse.
• Connaissance en apprentissage machine (IA, machine learning, deep-learning).

Savoir être :• Curiosité d'esprit et rigueur ;
• Appétence pour les sujets techniques ;
• Autonomie.

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.