Ingénieur logiciel/pédagogique en cybersécurité offensive (F/H)

Campus de Rennes de CentraleSupelec

Environnement du poste

Créé le 1er janvier 2015, CentraleSupélec est un Établissement Public à caractère Scientifique, Culturel et Professionnel, regroupant l'Ecole des Arts et Manufacture (Centrale Paris) et l'Ecole supérieure d'électricité (Supélec).
CentraleSupélec se compose de 3 campus situés à Gif-sur-Yvette (Essonne), à Metz (Moselle) et à Rennes (Ille-et-Vilaine). Elle est à la tête d'un réseau international avec 3 campus en Chine, en Inde et au Maroc.
CentraleSupélec est une référence dans les domaines de la formation des ingénieurs généralistes de haut niveau, de la recherche en Sciences de l'Ingénieur, en Sciences et Technologies de l'Information et de la Communication et en Sciences de l'Entreprise.
CentraleSupélec rassemble 4700 étudiants dont 3500 élèves ingénieurs et 30% d'étudiants internationaux, 600 doctorants, 70 post-doctorants, 65 chercheurs, 300 enseignants-chercheurs, 70 enseignants et 482 personnels non enseignants.
Ambitionnant de rester moteur au sein de l'université Paris-Saclay, 16eme rang au classement de Shanghai, et reconnue pour l'excellence de ses formations d'ingénieurs, CentraleSupélec poursuit ses démarches de synergie et d'innovation avec les acteurs de la recherche et de l'enseignement supérieur.

Contexte

Dans le cadre du plan de relance France 2030, nous sommes impliqués dans le **projet Train-Cyber-Expert** (TCE) financé par l'appel à projets CMA (Compétences et Métiers d'Avenir). TCE est un projet collaboratif entre plusieurs partenaires académiques qui a pour but de construire des ressources pédagogiques, sous forme de contenus numériques et de plates-formes technologiques, organisés par blocs de compétences, dans une optique de modularité, de réutilisabilité et de pédagogie centrée sur les compétences conduisant à des certifications.

Dans le cadre du projet TCE, nous aimerions pouvoir partager ces ressources, cependant cela nécessiterait d'une part de porter une partie des ressources de cours de l'assembleur x86 32 bits vers 64 bits. Ce travail a déjà été entamé par la réalisation d'un programme permettant de générer automatiquement des slides LateX à partir de la trace d'exécution d'un binaire (car le cours contient de nombreux exemples d'exécution de programmes vulnérable ainsi que de l'exploitation de ces vulnérabilités). Il conviendrait aussi de mettre au propre les sujets de travaux pratiques en rédigeant une correction, ainsi que la réalisation de capsules vidéo à partir des slides de cours.

Par ailleurs, l'équipe de recherche INRIA/CentraleSupélec PIRAT\') a développé URSID, un générateur de scénarios cyber-range multi-instances. Cet outil a déjà été utilisé pour déployer un exercice de Capture The Flag (CTF) de type test d'intrusions lors de l'école de printemps recherche de l'EUR Cyberschool en 2023 et pour le BreizhCTF en 2024. Dans le cadre du projet TCE, nous souhaiterions améliorer l'outil URSID afin de créer de nouveaux scénarios de tests d'intrusion pour le projet TCE.

Mission

Dans ce contexte, nous recherchons un(e) ingénieur(e) ayant une **solide formation technique en programmation, système et réseaux.** Idéalement, nous souhaitons que la personne recrutée ait l'expérience de la **cybersécurité** et un très fort attrait pour la **pédagogie**. Sa mission principale sera de **construire des ressources en sécurité offensive** en particulier dans deux directions : tests d'intrusion et attaques par débordement en mémoire.

Nous recrutons un(e) ingénieur(e) logiciel/pédagogique pour la cybersécurité offensive pour une durée de 24 mois dans l'équipe d'enseignement cybersécurité, en collaboration avec les équipes de recherche PIRAT\') ; et SUSHI sur le campus de Rennes de l'école. Sa mission sera de réaliser des supports techniques pour l'enseignement et la pratique de la sécurité offensive.

Activités principales

1. **Support pédagogique en cybersécurité :**

- Développement de ressources en sécurité offensive
- Création de scénarios de tests d'intrusion et d'attaques par débordement en mémoire
- Amélioration de l'outil URSID pour déployer des scénarios cyber-range

2. **Formation en cybersécurité :**

- Participation aux cursus généralistes et spécialisés en cybersécurité (Infosec, Mastère spécialisé)
- Construction de ressources pédagogiques (cours, travaux pratiques, vidéos)
- Adaptation des ressources existantes pour le projet Train-Cyber-Expert (TCE)

Compétences opérationnelles

- Langages : C, Python des connaissances en Rust et Assembleur x86 seraient très appréciées
- Utilisation de machines virtuelles (VirtualBox, Qemu) et conteneurs (Docker)
- Outils de déploiement automatisé : Ansible, Vagrant
- Connaissance de l'enseignement supérieur et de la recherche publique

Compétences comportementales

- Autonomie
- Proactivité
- Organisation
- Rigueur
- Qualités relationnelles

Profil

- Formation : Solide background en programmation, systèmes et réseaux
- Expérience : Cybersécurité et pédagogie
- Intérêt : Sécurité offensive, tests d'intrusion, vulnérabilités par débordement en mémoire

Informations complémentaires :

- Lieu de travail : **Campus de Rennes** de CentraleSupelec
- Date de début : Dès que possible
- CDD 24 mois
- Statut : Contractuel de droit public – Catégorie A
- Salaire selon diplôme et expérience
- Pour candidater, merci d'adresser une LM et un CV à : recrutement@centralesupelec.fr

Nous sommes à votre disposition pour répondre à vos questions. N'hésitez pas à contacter :
jean-francois.lalande@centralesupelec.fr ; frederic.tronel@centralesupelec.fr ;
valerie.viettriemtong@centralesupelec.fr