Offer #2025-08864

Ingénieur Cybersécurité - Développement d'un outil de type CyberRange communautaire

The offer description below is in French

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : Temporary scientific engineer

About the research centre or Inria department

Le centre Inria de l'Université de Rennes est un des neuf centres d'Inria et compte plus d'une trentaine d'équipes de recherche. Le centre Inria est un acteur majeur et reconnu dans le domaine des sciences numériques. Il est au cœur d'un riche écosystème de R&D et d'innovation : PME fortement innovantes, grands groupes industriels, pôles de compétitivité, acteurs de la recherche et de l'enseignement supérieur, laboratoires d'excellence, institut de recherche technologique.

Context

Dans le cadre du projet **CR:ACKED** financé par CreachLabs, l'Inria de Rennes propose un poste d'ingénieur au sein du **Laboratoire de Haute Sécurité** de Rennes (LHS) et de l'équipe **PIRAT\');** sur le site de Rennes.

Le LHS est une plateforme regroupant des services et des outils de cybersécurité difficiles ou impossibles à mettre en œuvre via les moyens classiques offerts par les DSI. Le LHS a vocation à permettre ou faciliter le prototypage de tout genre de projet expérimental nécessitant une infrastructure isolée (analyses de malware, honey pots, etc.).

Le LHS cherche à se doter d’un service de type CyberRange permettant de déployer des environnements vulnérables de façon automatisée et flexible afin d’étudier le comportement d’attaquants. Un CyberRange est un environnement virtuel hébergeant des machines ou des réseaux vulnérables sur lesquels les équipes de sécurité peuvent s’entrainer et tester leurs outils. Un CyberRange est un environnement dont l’objectif est d’être attaqué, il doit donc être soigneusement isolé du réseau Inria tout en étant accessible à ses utilisateurs qui peuvent être externes à l’organisation.

L'outil **URSID**, issu des travaux de l'équipe PIRAT\'); permet de créer des environnements vulnérables à des scénarios d’attaques à partir de descriptions de haut niveau et en s’appuyant sur un catalogue d’implémentations de procédures MITRE ATT&CK enrichi régulièrement par nos soins. Ces environnements doivent ensuite être hébergés sur des plateformes isolées du type de HopLab (HoneyPot Laboratory) du LHS où ils seront attaqués, par des joueurs, des botnets, des agents d’attaques.

URSID a été aussi bien utilisé ces deux dernières années pour de l'enseignement, que la création de honey pots et des CTF de type Pentest pour les 600 joueurs du BreizhCTF 2024 et BreizhCTF 2025.

L'objectif de ce poste est de faire un refactoring complet d'URSID afin d'en faire une référence pour la communauté cyber, de le doter de nouvelles fonctionnalités et d'enrichir son catalogue de vulnérabilités.

Assignment

Missions :
Avec l'aide des membres du LHS de Rennes et de l'équipe PIRAT\'); la personne recrutée sera amenée à proposer une architecture logicielle permettant à URSID de gagner en souplesse, robustesse et maintenabilité, puis de réaliser les développements.

L'objectif principal est d'être en mesure d'ajouter du contenu (procédures d'attaque ou scénario complets) de façon simple et rapide afin de permettre aux utilisateurs de se concentrer sur l'exploitation d'environnements vulnérables plutôt que sur leur déploiement.

La pérénisation de ce contenu est un enjeu majeur et nécéssitera une réflexion de fond sur la documentation, les tests, l'accompagnement des contributions, et idéalement l'animation d'une communauté d'utilisateurs.

Main activities

Tache 1 : Génération des CyberRange

• consolider l’outil URSID de génération d’environnements vulnérables destiné à peupler un CyberRange

• augmenter le nombre de procédures supportées par URSID

• ajouter le support de machines virtuelles Windows à URSID

Tache 2 : Déploiement des CyberRange

• améliorer le déploiement automatique de CyberRange complexes (réseaux isolés, firewalls, etc.) construit à l’aide de URSID dans l’environnement isolé HopLab

• étudier la possibilité d’avoir différents backend pour permettre de déployer sur des infrastructures cloud classiques (OVH, AWS, google cloud…) ou spécifiques (PROXMOX, CyberRange Airbus...)

• intégrer des modules de fausses activités (réseau, système, mail, fichiers, etc.) si possible parmi les solutions existantes

Tache 3 : Supervision des CyberRange

• développer des briques de supervision (pour suivre la progression des joueurs et attaquants)

• développer des solutions permettant l’archivage des logs de supervision

Taches de fond :

• promouvoir et documenter l’outil développé

• animer une communauté d’utilisateurs / contributeurs

• participer activement à l’animation et à l’amélioration des services du LHS

Skills

Nous recherchons un candidat ayant de bonnes connaissances en développement informatique et DevOps et une forte appétence pour la cybersécurité.

- De bonnes bases en systèmes et réseaux seront nécessaires
- Bonnes compétences en communication et en travail d'équipe
- Maîtrise de l'anglais technique (écrit et oral)

Les compétences indispensables sont :

- Python

- Ansible
- Linux
- Git

Connaissances appréciées :

- PROXMOX
- Packer
- Terraform
- Gitlab-CI

Technologies qui pourront être acquises pendant la mission :

- Molecule (pour Ansible)
- Poetry
- Système Windows et Active Directory

Benefits package

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail (après 6 mois d'ancienneté) et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle
- Sécurité sociale

Remuneration

Selon expériences

General Information

- **Town/city :** Rennes
- **Inria Center :** Centre Inria de l'Université de Rennes
- **Starting date :** 2025-10-01
- **Duration of contract :** 2 years

- **Deadline to apply :** 2025-06-29

Contacts

- **Inria Team :** SED-RBA (DGD-I)
- **Recruiter :**
  Sanchez Alexandre / alexandre.sanchez@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

The keys to success

Pour réussir dans ce poste, vous devez avoir de bonnes compétences en développement **Python** qui s'appuient sur un socle de connaissances techniques parmi celles citées, autorisant une adaptabilité aux différents travaux proposés. Vous êtes ingénieur·e ou docteur·e en informatique.

Vous évoluerez au sein d'une petite équipe dynamique de développeurs sur un projet innovant dans le cadre d'un laboratoire de recherche publique en lien étroit avec les entreprises et de nombreux partenaires.

Vous appréciez le **travail en équipe** mais vous êtes capable **d'autonomie** et d' **esprit d'initiative**.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Merci de déposer en ligne CV, lettre de motivation et éventuelles recommandations

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.