Institut Mines-Télécom

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

cyber-cni.fr/

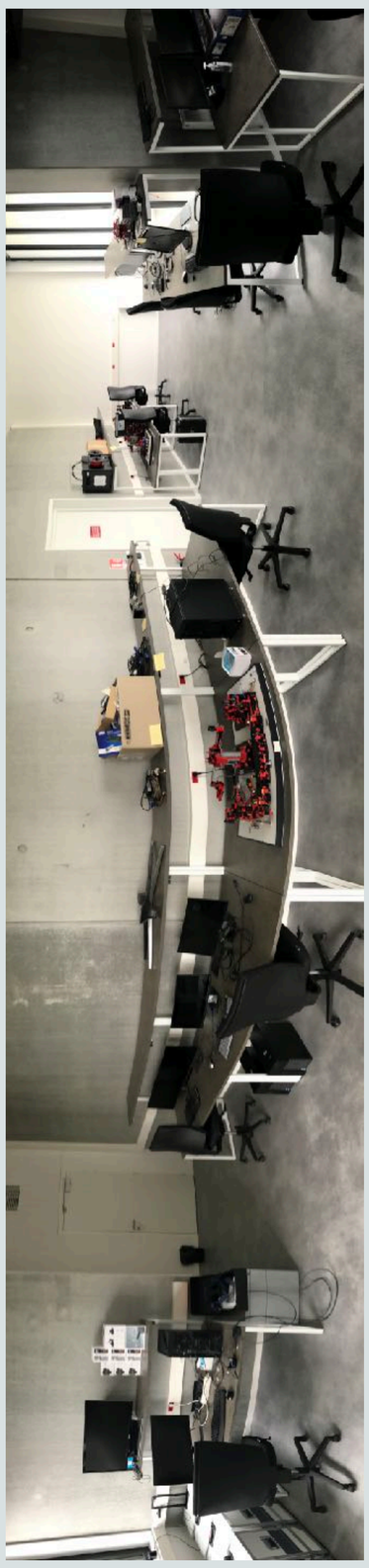
Nous recrutons !

Jeune Docteur (<2ans après doctorat)

(24 mois/ temps plein 35h/w)

Honeynet - un pot de miel réaliste

Nous sommes à la recherche d'un candidat exceptionnel pour renforcer notre équipe de recherche. Nous offrons une recherche stimulante dans un environnement riche avec d'excellentes perspectives de recherche. Ce poste est à pourvoir à partir du 15 octobre 2021.



Description

L'objectif de ces travaux de R&D est de mettre en œuvre un système de honeynet (pot de miel réaliste) pour pouvoir observer le mode opératoire de groupes d'attaquants. Grace à cet environnement, l'ambition est de pouvoir identifier des failles de sécurité utilisées par ces groupes d'attaquants pour compromettre le système d'information exposé par le pot de miel. D'un point de vue technique, l'objectif est de pouvoir identifier des codes d'exploitation zero-day et one-day utilisés au sein des modes opératoires de groupes d'attaquants.

La connaissance des codes d'exploitation zero-day et one-day est aujourd'hui un sujet d'importance afin de pouvoir produire des signatures de détection permettant de protéger des systèmes d'information à jour.

Les problématiques à résoudre pour arriver à ces objectifs concernent d'une part la qualité du leurrage obtenu. Il est en effet important que l'attaquant ait l'impression d'être sur un environnement réel afin de dérouler ses scénarios d'attaque complets. Par ailleurs, le système d'information simulé doit constamment exposer des services et applicatifs à jour ou récemment mis à jour, afin de pouvoir identifier des zero-day et one-day. D'autre part, il doit être possible de détecter l'exploitation de ces types de vulnérabilités.

Ces travaux s'appuieront sur la plateforme Cyber Range d'AMOSSYS et l'environnement BEEZH Platform, qui mettent à disposition des briques technologiques permettent de construire un honeynet (ou système d'information simulé). Les plateformes Cyber Range et BEEZH seront mis à disposition, avec un soutien de l'équipe R&D d'AMOSSYS qui développe ces outils.

Sur ces plateformes, les travaux de R&D consisteront à :

• concevoir l'architecture du SI simulé (services exposés, ressources et leurres déployés, …) pour le rendre réaliste et attrayant afin d'attirer de potentiels groupes d'attaquants ;
• mettre au point des capacités de collecte, d'analyse et de visualisation des traces laissées par les attaquants pour comprendre leur mode opératoire ;
• réaliser des expérimentations et potentiellement identifier l'exploitation de zero-day et de one-day.

Exigences - ce que vous devez apporter

PhD récent (<2 ans) dans un domaine connexe, compétences extraordinaires en matière de recherche. Curiosité et motivation pour travailler dans un environnement de recherche dynamique.

Langues : Français, anglais (capacité à lire et à rédiger des articles de recherche en anglais).

Procédure de candidature

Date limite de dépôt des candidatures : 30.9.2021, 15h00 CEST

Veuillez envoyer un email avec un (1) PDF comprenant :
une lettre de motivation (couvrant les points "exigences")
votre CV
vos certificats
une proposition de recherche (contenant vos méthodologies de recherche et les directions de recherche possibles que vous seriez intéressé à développer, y compris les références)
les adresses de contact (mail et téléphone) de 1 à 3 personnes que nous pouvons contacter pour obtenir des informations sur vous.

to **recruit-amossys-2021-1@cybercni.fr**.

Your future hosting environment: Excellence in Cybersecurity research and education in France

cyber-cni.fr/

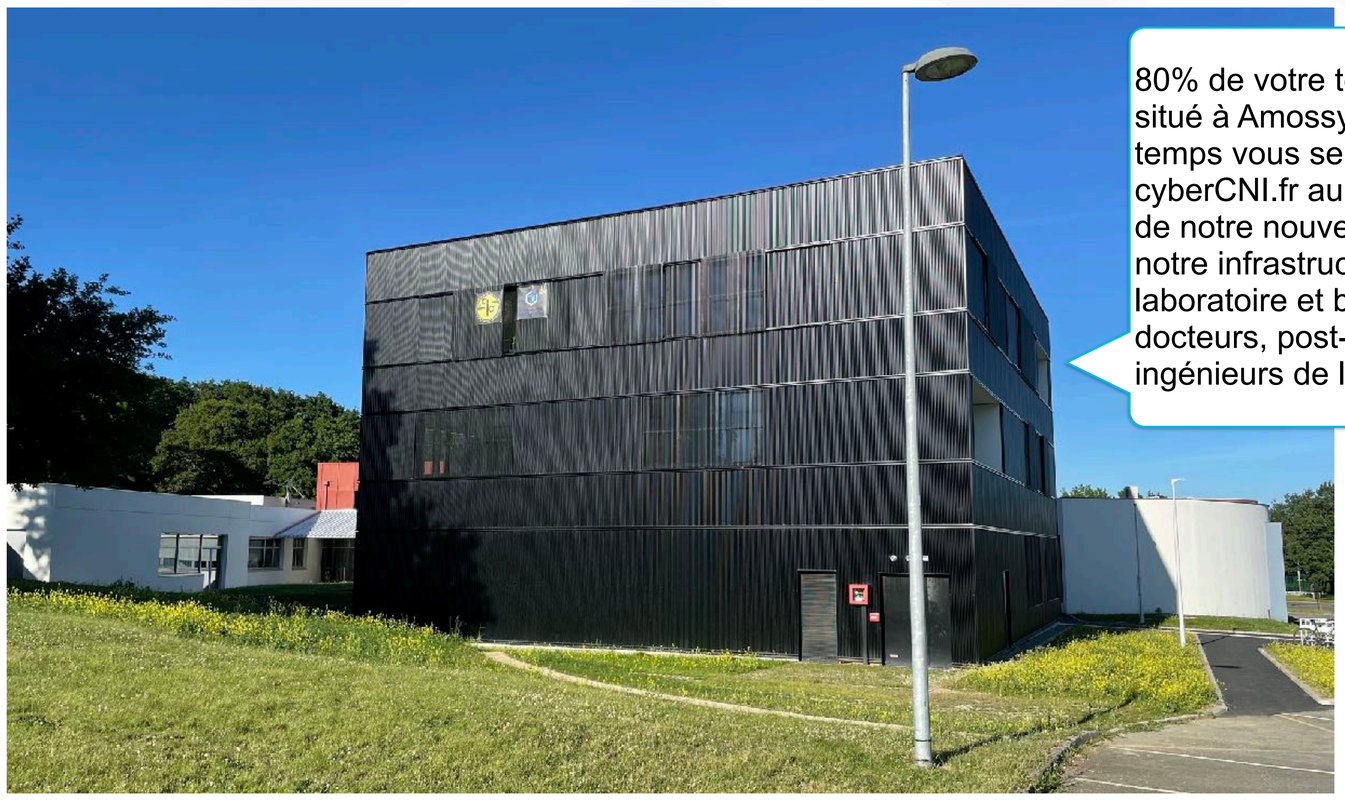
L'environnement d'hébergement

Le poste proposé se situe dans l'une des meilleures adresses de recherche en France, au sein d'une chaire reconnue pour son excellence en matière de cybersécurité. Cette offre est conjointe avec Amossys (https://www.amossys.fr/), une société de conseil et d'expertise en Sécurité des Technologies de l'information, où vous passerez 80% de votre temps. 20% de votre temps vous serez à la chaire.

Un déménagement à Rennes est requis.

IMT: L'Institut Mines Télécom (IMT) est la plus grande école d'ingénieurs de France. Elle est comparable à une université d'élite en Allemagne par exemple. IMT est un établissement public dédié à l'enseignement supérieur et à la recherche pour l'innovation.
Il est un acteur clé de la fusion des sciences, de l'ingénierie et du numérique, et porte les compétences de ses écoles dans les grands domaines de transformation du numérique, de l'industrie, de l'énergie et de l'environnement ainsi que leur impact sur l'industrie du futur, la ville, la santé et l'autonomie. Pour plus d'informations : https://www.imt.fr/en/imt/presentation-of-imt/

IMT Atlantique: Internationalement reconnue, la recherche d'IMT Atlantique la positionne dans le Top 400 des universités technologiques mondiales. Cette recherche, menée dans les domaines des sciences du numérique, des sciences de l'ingénieur, de la physique et du management, favorise les conditions d'une recherche interdisciplinaire, source d'innovation pour répondre aux grands enjeux des entreprises et de la société. Pour plus d'informations : https://www.imt-atlantique.fr/en/research-innovation



Chair Cyber CNI: La chaire Cyber CNI est une chaire de recherche industrielle. La chaire Cyber CNI d'IMT Atlantique est consacrée à la recherche, l'innovation et l'enseignement dans le domaine de la cybersécurité des infrastructures critiques, notamment les processus industriels, les systèmes financiers, l'automatisation des bâtiments, les réseaux d'énergie, les usines de traitement des eaux, les transports.

La chaire couvre l'ensemble de la pile de capteurs et d'actionneurs et leurs signaux sur les systèmes de contrôle industriels, les services distribués à la périphérie ou dans le nuage, les interfaces utilisateur avec la réalité mixte collaborative et les politiques de sécurité.

La chaire accueille actuellement 6+3 doctorants, 1+3 post-docs, 11 professeurs, 1+1 ingénieurs et 1 étudiant en stage. La chaire gère un vaste banc d'essai qui permet de mener des recherches appliquées en collaboration avec les partenaires industriels. Les partenaires industriels du deuxième tour de financement sont Airbus, Amossys, BNP Paribas, EDF, Nokia Bell Labs, et SNCF.

La Bretagne est la région de cybersécurité numéro 1 en France. La chaire Cyber CNI est fortement ancrée dans l'écosystème de la cybersécurité grâce à ses partenariats avec le Pôle d'Excellence Cyber (PEC) et la Région Bretagne. La chaire offre un environnement unique pour la recherche en cybersécurité avec de nombreuses possibilités de développement. Pour plus d'informations : https://cybercni.fr

This poster was made at the chaire Cybersecurity for Critical Networked Infrastructures (Cyber CNI) | https://cyber-cni.fr/ | Our monthly cybersecurity speaker series https://talk.cybercni.fr/ | Our science blog https://future-iot.org/