Fiche de poste

UNIVERSITE DE BRETAGNE SUD - ENSIBS	Poste n° A créer

Corps :	PR	**Article de référence :**	
Sections :	27		
Profil :			
Localisation :	Vannes		
Etat du poste : (vacant ou SV)	V		
Adresse d'envoi du dossier :	Le dossier est entièrement dématérialisé et à déposer sur l'application GALAXIE		
Contact administratif :	Mélanie LE QUINTREC		
N° de téléphone :	02 97 87 66 30		
N° de Fax :		**e-mail :**	drh.gestion.ens@listes.univ-ubs.fr

❍ **Profil enseignement :**

Composante / UFR :	ENSIBS École Nationale Supérieure d'Ingénieurs de Bretagne Sud	**Référence UFR :**	

❍ **Profil recherche :**

Nom laboratoire 1 :	IRISA	**N° unité du laboratoire 1 :**	UMR CNRS 6074
Nom laboratoire 2 :	Lab-STICC	**N° unité du laboratoire 2 :**	UMR CNRS 6285

Mots-clés enseignement et/ou recherche :	Cybersécurité	Utiliser la liste des mots-clés fournie en pj
Mots-clés enseignement et/ou recherche	Analyse	5 mots clés maximum
Mots-clés enseignement et/ou recherche	Modélisation	Les mots clés sont proposés en fonction des section CNU du profil. Pas de création possible
Mots-clés enseignement et/ou recherche :	Sécurité	
Mots-clés enseignement et/ou recherche :		

Fiche de poste : Informations complémentaires

Job profile : *brève synthèse en anglais comprenant les coordonnées de la composante qui publie le poste, le profil du poste saisie obligatoire dans l'encadré (300 caractères max.)*

ENSIBS prepares students to become graduate engineers in 5 specialties. The job profile is part of cyber-defense. The candidate will have to integrate IRISA or LabSTICC, which are both research laboratories whose activity include cybersecurity.

Research Fields : *Utiliser la liste de mots-clés en anglais (à partir de la liste des termes euraxess) saisie obligatoire*

Cybersecurity ; Analysis ; Modeling ; Security ;

Enseignement :

Département d'enseignement : ENSIBS
Lieu(x) d'exercice : Vannes
Equipe pédagogique : Cyberdéfense
Nom directeur département : Pr Éric MARTIN
Tel et email directeur Département : eric.martin@univ-ubs.fr
URL Département : https://www.ensibs.fr

Type d'enseignement et filière : École d'ingénieur – filière Cyberdefense

L'école d'ingénieur ENSIBS, au sein de l'Université de Bretagne-Sud, est une école associée Polytech. Elle forme près de 800 étudiants dont la moitié dans les domaines de la cybersécurité et de la cyberdéfense. Première école en France pour ce domaine de formation, l'ENSIBS est associée au Pôle d'Excellence Cyber Bretagne, partenaire de grands acteurs de la cyberdéfense (Orange, Airbus, Thales, Amossys, Sopra-Steria, MinArm) et reçois le label SecNumEdu de l'ANSSI.

L'ENSIBS propose sur son site de Vannes une formation sur la sécurité des systèmes d'information (RNCP 35799), nommée ingénieur en cyberdéfense. Cette formation est structurée en 8 blocs de compétences que doivent atteindre les ingénieurs diplômés.

Les formations dispensées par le professeur recruté entreront dans le cadre du développement de ces compétences et plus particulier dans les blocs « Détecter et corréler les incidents » (Analyser et modéliser les risques informatiques et les incidents de sécurité informatique par des approches formelles ou de l'IA) et « Réagir aux incidents » (Analyser et modéliser la résilience des IT).

Les enseignements effectués permettront de développer les connaissances et les compétences des apprenants en cybersécurité, et en particulier dans les domaines de la prévention et de la détection de cyberattaques, et des moyens de réaction et de remédiation face à elles.

Le·La candidat·e devra avoir la capacité à enseigner dans des disciplines fondamentales etappliquées de la sécurité et de l'informatique. Parmi les compétences théoriques et pratiques recherchées, on peut citer la cybersécurité des systèmes ; la prévention et la détection d'intrusions et de menaces ; l'évaluation de la résistance des systèmes ; l'IA appliquée à la cybersécurité, , etc.

Le·La candidat·e aura en charge des enseignements théoriques et pratiques ainsi que l'encadrement de projets d'étudiants. Nous attendons un·e candidat·e ayant une forte expérience et reconnaissance internationale, à même de s'impliquer fortement dans la coordination des enseignements d'informatique de la formation Ingénieur en cyberdéfense. Le·La candidat·e possèderapar conséquent idéalement une solide expérience d'animation d'une filière pédagogique au sein d'un établissement ou d'une composante délivrant des masters ou diplômes d'ingénieur.

La personne recrutée devra réaliser une partie de ses enseignements en langue anglaise et sera également appelée à intervenir en formation continue (DU Cyberdéfense des TEP/PME).

Responsabilités pédagogiques/administratives (dans le département, la composante, l'établissement) :

Selon le référentiel de la CTI, « *la formation des ingénieurs comporte une activité de recherche fondamentale ou appliquée* ». De même « *l'ouverture du futur ingénieur sur l'innovation et la création d'activité ou d'entreprise s'appuie sur le développement d'un état d'esprit, la réalisation d'activités etun processus de formation* ».
Le·La professeur·e aura à définir et à coordonner une équipe de 8 enseignant·e·s-chercheur·e·s, qui par différents types d'activités pédagogiques permettront aux élèves ingénieur·e·s de développer leurs compétences du référentiel de la CTI « *la capacité à effectuer des activités de recherche, fondamentale ou appliquée, à mettre en place des dispositifs expérimentaux* » ; « *la capacité à trouverl'information pertinente, à l'évaluer et à l'exploiter : compétence informationnelle* ».
Afin de renforcer le lien entre formation – innovation et entreprise, le·la professeur·e s'emploiera à développer une chaire dans le domaine de la cyberdéfense.

Missions transversales (TICE, aide à l'insertion professionnelle, formation continue, apprentissage, …) :

☒ Innovation pédagogique et outils numériques :

Le·La professeur·e développera ses enseignements par compétence ; selon le référentiel de la CTIcommission du titre d'ingénieur, « *Une compétence se traduit par un savoir agir nécessitant de mobiliser et de combiner un ensemble de savoirs, savoir-faire et savoir-être en vue de réaliser une tâche ou une activité a priori complexe. Elle a toujours une finalité professionnelle* ».

☒ Formation par apprentissage :

Le·La professeur·e a vocation à prendre des responsabilités dans le développement de la formation en alternance, et en formation continue, et participera activement au dialogue avec les partenaires industriels de la filière cyberdéfense.

☒ Formation en langue étrangère :

La maîtrise de l'anglais est une nécessité pour participer au rayonnement à l'international de la formation. Le·La professeur·e sera amené·e à participer à des projets de formations internationales enlien avec le développement de l'ENSIBS.

Recherche :

Deux laboratoires d'accueil sont possibles pur ce poste : IRISA OU Lab-STICC

IRISA

Lieu(x) d'exercice (si unité présente sur plusieurs sites, préciser l'ensemble des sitesde l'UBS) : Vannes

Nom directeur laboratoire : Guillaume Gravier

Tel et email directeur laboratoire : 02 99 84 72 39 guillaume.gravier@irisa.fr

URL laboratoire : https://www.irisa.fr/

Descriptif laboratoire : L'IRISA est l'un des plus grands laboratoires de recherche français (850+ personnes) dans le domaine de l'informatique et des nouvelles technologies de l'information, bénéficiant d'une excellente visibilité internationale et d'un écosystème d'innovation riche. Structuré en sept départements scientifiques, le laboratoire, implanté à Rennes, Lannion et Vannes, couvre un large spectre thématique dans le domaine de la science informatique et des sciences de l'information. Ses domaines d'excellence sont : cybersécurité ; systèmes distribués, cloud et environnements intelligents (IoT) ; conception, vérification et certification logicielle ; robotique, environnements virtuels et interaction haptique ; interprétation des signaux, des images et du langage ; données, IA et bioinformatique.

Description détaillée du profil de recherche : Le projet de recherche du candidat ou de la candidate devra présenter une intégration au sein de l'une des équipes de l'IRISA et s'inscrire dans l'axe transverse Cybersécurité. À moyen terme, on attend de la personne recrutée de s'investir dans la structuration des recherches en cybersécurité sur le site de Vannes.

Nous attendons un candidat ou une candidate ayant une forte expérience de la recherche en cybersécurité, fondamentale et/ou appliquée, et une reconnaissance académique internationale (collaborations scientifiques, projets européens, comités d'organisation de manifestations internationales, comités de programmes de conférences réputées...), ainsi qu'une implication dans la vie du laboratoire, notamment via la participation aux responsabilités collectives scientifiques ou autres.

Lab-STICC

Lieu(x) d'exercice (si unité présente sur plusieurs sites, préciser l'ensemble des sitesde l'UBS) : Vannes

Nom directeur laboratoire : Christian Person

Tel et email directeur laboratoire : 02 29 00 13 19 / christian.person@imt-atlantique.fr

URL laboratoire : http://www.lab-sticc.fr/

Descriptif laboratoire : Le Lab-STICC (Laboratoire des sciences et techniques de l'information, de la communication et de la connaissance, UMR CNRS 6285), fort de son double rattachement aux instituts INS2I et INSIS du CNRS, est une unité de recherche historiquement reconnue en Bretagne Océane et en France dans le domaine des STIC. Elle affiche une capacité avérée de couvrir un large spectre scientifique autour des sciences du numérique, et avec en particulier cette faculté d'adresser des champs disciplinaires variés (Théorie de l'Information, Ondes & Matériaux, Electronique et Informatique embarquées, Sciences des données, Communication et détection de signaux, Interfaces Homme-Machines,..) suivant des thématiques/secteurs applicatifs multiples : l'environnement maritime, les objets communicants, la défense, le spatial, la santé, la sécurité, la robotique...

Le laboratoire, qui regroupe plus de 600 personnes, est structuré en neuf pôles scientifiques, 25 équipes de recherche et 6 axes transverses. La cybersécurité est à ce titre l'un des 6 projets transverses du laboratoire. Toutefois, cette thématique est également implicitement portée par d'autres programmes transverses à vocation applicative, en l'occurrence celui de l'« Industrie dufutur » ou encore au sein du programme transverse « systèmes embarqués autonomes ».

Description détaillée du profil de recherche : Le·La candidat·e devra avoir une solide expérience recherche dans tous les aspects de la cybersécurité/ cyberdéfense : prévention, protection, détection, réponse aux incidents et gestion… Les domaines de recherche d'intérêts sont, entre autres, la détection des menaces avancées persistantes,la détection basée sur le « machine learning », la détection des dispositifs IoT compromis, le Social MediaIntelligence (SOCMINT), les cyber-ranges et la prévention du phishing.

Il sera porté une attention particulière au projet d'intégration, de préférence dans l'une des équipes du Lab-STICC, parmi IRIS, Maths&Net ou P4S. Ces équipes abordent des thématiques variées (dont l'apprentissage automatique pour la surveillance et la protection des systèmes, la gestion et ledéploiement des politiques de sécurité, les contrôles d'accès,

le tatouage de l'information, la détection d'intrusion, la réaction aux cyber-attaques, la cyber-résilience des systèmes, les processus d'ingénierie de la sécurité, la certification et la vérification formelle de propriété de sécurité, le maintien en condition de sécurité) dans lesquelles le·la candidat·e pourra développer son projet d'intégration en lien avec son expertise.

Nous attendons un·e candidat·e ayant une forte expérience de la recherche et une reconnaissance académique internationale (collaborations scientifiques, projets européens, comités d'organisation de manifestations internationales, comités de programmes de conférences réputées...), ainsi qu'une implication dans la vie du laboratoire, notamment via la participation aux responsabilités collectives scientifiques ou autres. Le·La candidat·e devra être apte à structurer une nouvelle thématique de recherche autour de la cybersécurité/cyberdéfense appliquée aux grands domaines industriels et répondant aux enjeux scientifiques nationaux et internationaux de protection des données et des systèmes complexes.

Le·La candidat·e sera soutenu·e dans son activité par un classement prioritaire à hauteur d'une demande de financement de thèse et d'une demande de post-doctorant.

Le·La candidat·e retenu·e pourra s'impliquer en lien avec les partenaires académiques et industriels (ycompris les chaires) à la valorisation et diffusion des résultats de recherche dans les domaines d'application des équipes du Lab-STICC.

Activités de transfert de technologie ou de culture scientifique :

☒ Activités de transfert de technologie :

Le·La professeur·e s'impliquera dans un projet de chaire d'entreprise dans le domaine de la cyberdéfense avec les missions d'innovation et de formation initiale et continue.

Autres informations :

Compétences particulières requises :

Zone d'accès à Régime Restrictif (ZRR) :

Poste concerné par la ZRR : oui * ☒ non ☐

*Si oui, Nom de l'entité concernée :

le décret 2017-854 du 9 mai 2017 modifiant le décret 84-431 du 6 juin 1984 intègre dans les statuts des enseignants-chercheurs la précision selon laquelle la nomination à un emploi impliquant l'accès à une zone à régime restrictif est subordonnée à la délivrance d'une autorisation d'accès à cette zone. La décision finale doit être approuvée par le Haut Fonctionnaire de Défense et de Sécurité (HFDS) du Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation

Audition – Mise en situation professionnelle (MESP) : oui ☐ non ☒

Leçon ☒
Audition publique : oui ☐ non ☒
Durée : 5 minutes ☐ 15 minutes ☒ Autre (précisez) :…….…. ☐
Langue utilisée pour la MESP : Français *(obligatoire pour les non francophones)* ☒
Anglais ☐ Autre (précisez) :……. ☐
Sujet libre ☐ Sujet commun *(à préciser sur la convocation)* ☒

Séminaire de présentation des recherches ☐
Audition publique : oui ☐ non ☐

Durée : 5 minutes ☐ 15 minutes ☐ Autre (précisez) :…….. ☐ Langue utilisée pour la MESP : Français *(obligatoire pour les non francophones)* ☐ Anglais ☐ Autre (précisez) :…….…… ☐

Date & Visa de la direction de composante : Martin Signature numérique de Martin Date : 2022.01.20 13:39:15 +01'00'	Date & Visa de la direction de laboratoire : Philippe COUSSY Signature numérique de Philippe COUSSY Date : 2022.01.20 13:44:09 +01'00' Date & Visa de la direction du site UBS :	Date & Visa de la direction de laboratoire : Date & Visa de la direction du site UBS : Frédéric GUIDEC Signature numérique de Frédéric GUIDEC Date : 2022.01.20 13:50:02 +01'00'
Date & Visa de la Présidente :		