INFORMATIQUE

INGENIEUR ENSIBS - Sécurité des Systèmes d'Information

Dernière mise à jour le 29 octobre 2020

Métier

Cette formation a été construite avec des entreprises publiques et privées référentes du domaine de la cyberdéfense. Elles ont un besoin important de professionnels capables de :

- Comprendre la menace et les modes opératoires des attaquants dans une approche système,
- Construire la sécurité des infrastructures dans une approche globale pour mieux se protéger (architecte cyberdéfense),
- Gérer des crises cybernétiques, quelle que soit leur ampleur,

Les besoins en recrutement d'ingénieurs sont estimés actuellement par ces entreprises à plus de 1000 ingénieurs par an (800 pour le privé et 200 pour le public).

Durée et organisation

Formation en contrat d'apprentissage

- **Durée :** 3 ans
- **Alternance :**
  - 1ère et 2ème année : 1 mois en entreprise | 1 mois en centre de formation
  - 3ème année : 6 mois en entreprise | 6 mois en centre de formation
- **International :** 8 semaines obligatoires minimum à l'étranger.

Lieu | Date

ENSIBS - LORIENT | de septembre 2021 à septembre 2024

Objectif de la formation

A l'issue de la formation, les stagiaires devront être capables de :

Analyser le risque cybernétique

- Analyser la menace et diagnostiquer le mode opératoire

Admission

Public

- Etre âgé de 15 à moins de 30 ans*.
- Etre de nationalité française, ressortissant de l'UE ou étranger en situation régulière de séjour et de travail.

*Pour les plus de 30 ans, possibilité de se former en contrat de professionnalisation (nous consulter).

Pré-requis d'entrée en formation

- Titulaire d'un DUT INFORMATIQUE, R&T ou GEII
- Titulaire d'un BTS SIO ou SN
- Prépa intégrée ENSIBS, prépa ATS ou CPGE
- Être admis suite au processus de recrutement : dossier et entretien de motivation

Modalités et délais d'accès

Modalités

Dossier de pré-inscription en ligne, entretien collectif et/ou individuel, signature d'un contrat d'apprentissage

Délais d'accès

Fonction de la date de signature du contrat d'apprentissage

Parcours adaptés

Adaptation possible du parcours selon les pré-requis

Handicap

Formation ouverte aux personnes en situation de handicap (moyens de compensation à étudier avec le référent handicap du centre)

Coût

des attaquants
- Etudier les vulnérabilités matérielles et logicielles ainsi que les attaques sur les infrastructures
- Comprendre l'interconnexion et l'évolutivité à grande échelle des systèmes dans le cyberspace
- Définir une politique de sécurité

Construire la sécurité dynamique des infrastructures dans une approche système

- Résoudre des problèmes complexes de niveau système (de nature technologique) par un panel de solutions à la fois méthodologiques, technologiques, organisationnelles, humaines, juridiques et déontologiques
- Concevoir, réaliser et mettre en oeuvre un ensemble de solutions de sécurité
- Concevoir, réaliser et mettre en oeuvre la protection des systèmes des opérateurs d'infrastructures vitales (OIV)
- Conduire une approche systémique de la sécurité pour sécuriser des systèmes industriels, des systèmes d'information, des sytèmes financiers, des systèmes d'armes

Gérer des crises cybernétiques

- Concevoir, développer et exploiter un centre opérationnel de cybersécurité
- Savoir détecter dynamiquement les attaques
- Savoir réagir en situation de gestion de crise en confrormité avec le cadre juridique, les doctrines d'emploi et les règles d'engagement de la cyberdéfense
- Expertiser, auditer et évaluer les résistances des configurations techniques de sytèmes
- Savoir adopter un comportement éthique et déontologique en situation de gestion de crise
- Savoir communiquer pendant une crise

Manager des projets complexes de sécurité des systèmes

SECTEURS CONCERNÉS

- État, Défense
- Banques et Finances
- Opérateurs internet et télécom
- Énergie (EDF, nucléaire, pétrole)
- Espace
- Santé
- Transport (routier, portuaire, aérien)
- Automobile
- Aéronautique
- Electronique

Formation gratuite et rémunérée

Modalités et moyens pédagogiques

Méthodes pédagogiques

Formation en présentiel avec alternance d'apports théoriques et de mises en situations pratiques pour ancrer les apprentissages et/ou en distanciel pour certains modules.

Moyens pédagogiques

Salles de formation équipées et plateaux techniques adaptés et aménagés d'équipements spécifiques.

Équipe pédagogique

Formateurs experts titulaires au minimum d'un BAC+2/+4 et/ou d'une expérience professionnelle d'au moins 5 ans dans le domaine, professionnels du métier, responsable de formation, direction de centre, conseillers alternance, référent handicap, équipe administrative

Modalités d'évaluation et d'examen

Les candidats▪es sont présentés▪ées aux épreuves générales et techniques **la spécialité sécurité des systèmes informatiques « cyberdéfense»**, diplôme délivré par l'école et habilité par la Commission des Titres d'Ingénieurs pour la spécialité génie industriel, en partenariat avec l'Institut des Techniques d'Ingénieur de l'Industrie de Bretagne.

Validation

Ingénieur Sécurité des Systèmes d'information

Poursuites d'études et débouchés

Exemples de métiers :

- *Ingénieur expert en cybersécurité - cyberdéfense*
- *Ingénieur « cyber architecte »*
- *Manager d'un centre opérationnel de cybersécurité*
- *Chef de projet en management de la sécurité*

Contacts

ENSIBS - Spécialité cyberdéfense

Rue Yves Mainguy | BP 573 | 56017 VANNES CEDEX

- 02 97 01 72 70
- ensibs.cyberdefense@univ-ubs.fr

Programme

- Sciences pour l'Ingénieur
- Ingéniérie des technologies des solutions de sécurite
- Management et ingéniérie de sécurité des systèmes
- Séminaires de gestion de crise
- Anglais