INFORMATIQUE

INGENIEUR ENSIBS - Sécurité des Systèmes d'Information et Cybersécurité

Date de dernière mise à jour 22 février 2024

Formation éligible au CPF

Métier

Les entreprises ont un besoin croissant de professionnels capables de comprendre la menace et les modes opératoires des attaquants dans une approche système, de construire la sécurité des infrastructures, dans une approche globale, afin de mieux se protéger et gérer les crises cybernétiques.

La formation ingénieur en Cyberdéfense, conconstruite avec les entreprises, constitue une réponse à ce besoin important et urgent.

Les ingénieurs cyberdéfense sont capables de **cyberdéfendre les Opérateurs d'Importance Vitale français** :

- 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

Durée et organisation

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.

*Pas de limite d'âge pour toute personne reconnue travailleur handicapé. Pour les plus de 30 ans, possibilité de se former en contrat de professionnalisation (nous consulter).

Pré-requis d'entrée en formation

La formation est accessible après un BAC+2 scientifique ou technologique.

- Entrée en 1ère année, aux étudiants issus de :
  - Classes préparatoires : CPGE, PEI ENSIBS
  - BUT 2 et BUT 3 : INFO, STID, R&T
  - Licence : Mathématiques, Informatique
  - Autres : prendre contact pour précisions
- Entrée en 2ème année, aux étudiants issus de

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 :** période de 9 à 12 semaines à l'étranger, possibilité Erasmus en dernière année
- **Anglais :** TOEIC

Pour les + de 30 ans, possibilité de se former en contrat de professionnalisation.

Durée et alternance indicatives et ajustables en fonction des besoins de l'entreprise et des pré-requis de l'apprenant.

Salariés

Possibilité de se former dans le cadre de la formation continue | éligible CPF

Lieu | Date

ENSIBS - LORIENT | de septembre 2024 à septembre 2027

Objectif de la formation

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

- Analyser le risque cybernétique
  - Analyser la menace et diagnostiquer le mode opératoire 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

:

- M1 : Mathématique, Informatique
- M2 autres : prendre contact pour précisions

- Être admis▪e suite au processus de recrutement : dossier d'admission en ligne et entretien

Calendrier 2024

- **Inscriptions** du 1er février au 27 mars 2024 **ICI**
- Oraux : du 17 au 19 avril 2024
- Retour aux candidats : jusqu'au 3 mai

Les dossiers des postulants sont étudiés par l'équipe pédagogique qui apprécie le niveau académique. Les candidats sélectionnés sont ensuite auditionnés par un jury composé d'enseignants de l'école et de professionnels appartenant aux entreprises ou administrations susceptibles de recruter des apprentis.

Modalités et délais d'accès

Modalités

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

- *Tout savoir sur les modalités du contrat d'apprentissage **ICI** ou de professionnalisation **ICI**.*

Délais d'accès

Fonction de la date de signature du contrat d'apprentissage ou de professionnalisation

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). En savoir +, contacter notre référent handicap : **ICI**

Coût

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

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...*

Programme

Matières

- **1ère année**
  - Entreprise et société
  - Culture internationale
  - Cryptographie
  - Ingénierie des systèmes
  - Système d'information
  - Cybersécurité et cyberdéfense
  - Architecture des ordinateurs
  - Implication professionnelle
  - Projet système
  - Activité d'ouverture
- **2ème année**
  - Entreprise et société
  - Culture internationale
  - Systèmes d'exploitation sécurisés
  - Réseaux sécurisés
  - Projet pluridisciplinaire en solution de sécurité
  - Cybersécurité et cyberdéfense
  - Analyse des vulnérabilités numériques
  - Développements sécurisés
  - Systèmes industriels
  - Sécurisation des systèmes d'information
  - Architecture sécurisée
  - Agilité et société

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 formations, référent handicap, équipe administrative

Modalités d'évaluation et d'examen

La formation permet l'obtention d'un diplôme d'Etat inscrit au RNCP sous réserve de satisfaire aux modalités d'évaluation des connaissances et compétences. Chaque unité d'enseignement (UE) est évaluée indépendamment. L'évaluation de l'entreprise comptera pour 1/3 dans le résultat final de chaque UE co-évaluée.

Le▪la candidat▪e obtient le **Titre ingénieur - Ingénieur diplôme de l'ENSIBS de l'Université de Bretagne-Sud, spécialité Sécurité des systèmes d'information**, sous condition de validation :

- des 8 blocs de compétences du titre d'ingénieur de la spécialité,
- de missions réalisées au sein d'une entreprise dans le cadre de l'alternance,
- du niveau B2 en anglais, attestée par un organisme tiers,
- du niveau « orthographe professionnelle » de français, attesté par un organisme tiers,
- d'un dossier de preuves démontrant une période d'immersion à l'étranger.

Il est également possible d'acquérir par VAE l'ensemble ou une partie des blocs de compétences constitutifs du diplôme d'ingénieur.

Validation

Titre ingénieur | Ingénieur diplôme de l'ENSIBS de l'Université de Bretagne-Sud, spécialité Sécurité des systèmes d'information

- Diplôme de niveau 7 (BAC+5) reconnu par la CTI (Commission des Titres Ingénieurs)
- Code RNCP* : 35799
- Certificateur : Univeristé de Bretagne Sud UBS - ENSIBS
- Date de début des parcours certifiants : 01-09-2021
- Date d'échéance de l'enregistrement : 31-08-2026

La certification est composée de plusieurs blocs de compétences dénommés certificats de compétences professionnelles (CCP).

- Ouverture et professionnalisation

- **3ème année**
  - Entreprise et société
  - Culture internationale
  - Stratégie et renseignement cyber
  - Stratégie de réaction face aux attaques
  - Cyberdéfense des systèmes techniques
  - Projet
  - Exercice de gestion de crise
  - Professionnel agile et responsable
  - UE du parcours IT
  - UE du parcours indus
  - UE du parcours stratégie et gouvernance
  - Projet de fin d'études

Compétences validées en entreprise

- Mise en oeuvre des acquis techniques
- Conduite de projet et communication
- Management et conduite du changement

Compétences

- Mettre en oeuvre le management opérationnel pour la sécurité des systèmes d'information, en contexte pluridisciplinaire et multiculturel
- Conduire des projets complexes en matière de cybersécurité, de manière agile
- Réaliser des audits de sécurité des systèmes d'informations
- Opérationnaliser la sécurité des systèmes d'informations
- Assurer la résilience des services numériques vitaux des entreprises
- Manager le risque lié à des menaces numériques
- Détecter et corréler les incidents de sécurité numérique
- Réagir aux incidents de sécurité numérique

Indicateurs de performance

- **Réussite à l'examen :**

- **Insertion globale :**

96 %

- Taux de poursuite d'étude : 10 %

- BLOC 1 | Mettre en œuvre le management opérationnel pour la sécurité des systèmes d'information, en contexte pluridisciplinaire et multiculturel
- BLOC 2 | Conduire des projets complexes en matière de cybersécurité, de manière agile
- BLOC 3 | Réaliser des audits de sécurité des systèmes d'informations
- BLOC 4 | Opérationnaliser la sécurité des systèmes d'informations
- BLOC 5 | Assurer la résilience des services numériques vitaux des entreprises
- BLOC 6 | Managerier le risque lié à des menaces numériques
- BLOC 7 | Détecter et corréler les incidents de sécurité numérique
- BLOC 8 | Réagir aux incidents de sécurité numérique

La formation peut être validée totalement ou partiellement par acquisition d'un ou plusieurs blocs de compétences.

**Répertoire National de la Certification Professionnelle*

Passerelles, poursuites d'études et débouchés

Cette formation a pour premier objectif l'insertion professionnelle.

- **Exemples de métiers**
  - *Analyste menace cyber, Responsable de la Sécurité des Systèmes d'Informations (RSSI), Spécialiste en gestion de crise cyber, Chef de projet sécurité, Architecte sécurité, Intégrateur de sécurité, Expert réponse à incident, Consultant sécurité, Evaluateur sécurité, Analyste SOC...*

Contacts

ENSIBS Vannes

Campus Tohannic | Rue Yves Mainguy | BP 573 | 56017 VANNES CEDEX | www.ensibs.fr

- Contact : Benoît GAUDICHEAU | 02 97 01 72 70 - 07 64 78 37 08
- Candidature & retrait du dossier

A noter

L'alternance permet de mettre en pratique en entreprise les connaissances théoriques et les outils acquis au cours de la formation.

- Taux insertion professionnelle : 95%
- Taux d'interruption : 4%

Pour obtenir des données précises, merci de contacter notre serviceQualité.

Indicateurs mis à jour le 15/12/2021 (Données promo 2021 sauf taux d'insertion à 6 mois promo 2020)

Une immersion internationale de 9 semaines à l'international est obligatoire et 12 conseillées (exigence de la Commission des Titres d'Ingénieur). Cette immersion est du ressort de l'étudiant et se fera en coordination avec l'entreprise hôte et l'école, en priorité sur le temps entreprise.

Documents

ENSIBS Plaquette 2024 | Cyberdéfense