Ingénieur diplômé de l'école nationale supérieure d'ingénieurs de Bretagne-Sud de l'université de Bretagne-Sud spécialité sécurité des systèmes d'information en partenariat avec l'ITII Bretagne

INGENIEUR ENSIBS - Sécurité des Systèmes d'Information et Cybersécurité

Certifiante | **Contrat appr.** | **Contrat pro.**

Réf. : 1910241F — Mise à jour : 21 octobre 2024

Organisme responsable : **POLE FORMATION UIMM BRETAGNE - site de Plérin**

Contenu

Objectifs

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).

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

Analyser le risque cybernétique : Analyser la menace et diagnostiquer le mode opératoire des attaquants - Étudier 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 œuvre un ensemble de solutions de sécurité - Concevoir, réaliser et mettre en œuvre 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 conformité 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 systèmes - 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 - Électronique

Programme

- **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
  - 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

Certifications préparées et métiers visés

Niveau d'entrée	Niveau de sortie
Aucun prérequis	**Niveau Master, ingénieur - Bac +5 et plus**

Liste des certifications

Ingénieur diplômé de l'école nationale supérieure d'ingénieurs de Bretagne-Sud de l'université de Bretagne-Sud spécialité sécurité des systèmes d'information et cybersécurité

Métiers associés

M1805 — Études et développement informatique
M1801 — Administration de systèmes d'information
M1802 — Expertise et support en systèmes d'information
M1806 — Conseil et maîtrise d'ouvrage en systèmes d'information
M1810 — Production et exploitation de systèmes d'information

Dates et lieux de formation

N° session	Modalité	Lieu	Du	Au
1311273	Présentiel	Vannes	31/08/2023	30/08/2026
1835612	Présentiel	Vannes	31/08/2025	30/08/2028

Source : GREF Bretagne #1910241F