UIMM
PÔLE FORMATION
Bretagne
LA FABRIQUE DE L'AVENIR

INFORMATIQUE

INGENIEUR CyberDéfense

Date de dernière mise à jour 26 février 2021

Métier

L'évolution du numérique a mené à la création d'un cyberespace dont la surveillance est aujourd'hui un véritable défi. Pour se spécialiser dans le domaine, une formation adaptée est essentielle.

L'ingénieur cyberdéfense occupe une grande variété d'emplois liés à la **défense des OIV**. Il▪elle exerce dans toute structure, entreprise ou organisation sujettes aux menaces d'éventuels incidents de sécurité informatique ou de cyber-attaques, comme expert en test d'intrusion ou de compromission du SI, comme responsable de la sécurité informatique, ou encore comme consultant en organisation de la Sécurité des Systèmes d'Information (SSI).

Durée et organisation

Formation en contrat d'apprentissage

- **Durée :** 12 mois | 600 heures de formations
- **Alternance :** 60% du temps en entreprise | 40% du temps en CFA

Lieu | Date

BRUZ / RENNES | de septembre 2021 à septembre 2022

Objectif de la formation

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

- Analyser un cahier des charges d'un système d'information
- Élaborer la maquette du dossier d'architecture technique
- Élaborer l'architecture d'un système d'information sécurisé
- Définir un plan de reprise d'activités informatique
- Auditer la sécurité du système d'information
- Gérer un système d'information après compromission
- Superviser le système d'information

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

- Être titulaire d'un titre de Niv. II Cyberdéfense (Titre RNCP Concepteur en Architecture Informatique) ou un BAC+4 ou 5 en informatique ou Systèmes Informatiques et réseaux.

Qualités requises : esprit d'analyse et de synthèse, rigueur, vision d'ensemble, réactivité, polyvalence, curiosité, communication

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

- Sensibiliser les utilisateurs du système d'information à l'hygiène informatique et aux risques liés à la cybersécurité

SECTEURS CONCERNÉS

- Opérateurs d'importances vitales (OIV)
- Entreprises de service du numérique (ESN)
- Industriels
- PME

Programme

MATIÈRES

- Cyberdéfense
- Test d'intrusion
- Forensic
- Sécurité des réseaux
- Sécurité des bases de données
- Sécurité des systèmes d'exploitation
- Cryptologie
- Droit et réglementation
- Développement de logiciel sécurisé
- Système spécifiques, informatique industrielle
- Exercice de gestion de crise
- Hacking social

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 formations, référent handicap, équipe administrative

Modalités d'évaluation et d'examen

Les candidats▪es sont présentés▪ées aux épreuves générales et techniques du diplôme **INGENIEUR CyberDéfense**.

Validation

INGENIEUR CyberDéfense

Poursuites d'études et débouchés

- *La vocation de ce diplôme est l'insertion professionnelle directe.*

Exemples de métiers : Spécialiste en gestion de crise cyber, Chef de projet sécurité, Expert▪e en cybersécurité, Expert▪e en sécurité des systèmes d'information, Expert▪e en tests d'intrusion - sécurité des systèmes d'information, Expert▪e en sécurité informatique.

Contacts

ESNA Bretagne

Responsable Cyberdéfense : Guillaume CHOUQUET
06 98 88 14 88 | guillaume.chouquet@formation-industrie.bzh