UIMM
PÔLE FORMATION
Bretagne
LA FABRIQUE DE L'AVENIR

INFORMATIQUE

INGENIEUR CYBER - Parcours Cyberdéfense - Systèmes, réseaux et cybersécurité - ESNA

ESNA
École Supérieure du Numérique Appliqué

Date de dernière mise à jour 19 février 2024

CPF
Formation éligible au CPF

Métier

DEVENEZ INGÉNIEUR CYBERDÉFENSE

La numérisation de notre société a profondément bouleversé tous les secteurs de l'activité humaine. Aujourd'hui, la défense de ce cyberespace constitue un enjeu majeur. L'ESNA vous propose des formations qui vous permettront d'être un acteur avisé et compétent capable de relever ces défis.

L'ingénieur cyberdéfense occupe une grande variété d'emplois liés à la **sécurité des systèmes d'information**. Il exerce dans diverses structures, publiques comme privées, sujettes à d'éventuels incidents de sécurité informatique ou de cyberattaques. Face à ces menaces, il doit intervenir, en lien avec la direction et les métiers de l'entité, pour en protéger et défendre le patrimoine informationnel.

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

- Pour une entrée en LICENCE Informatique / Cybersécurité : être titulaire d'un BAC+2 Informatique (BTS, BUT 2...)
- Pour une entrée en INGÉNIEUR Cyberdéfense : être titulaire de la licence Informatique parcours Cybersécurité
- Satisfaire au process de recrutement

L'INGÉNIEUR CYBERDÉFENSE se fait en 3 ans avec 2 contrats successifs.

Possibilité d'intégrer directement le parcours INGÉNIEUR sous réserve d'avoir validé la licence Informatique parcours Cybersécurité.

Formation en contrat d'apprentissage

- **Durée :** 3 ans | 600 heures de formation par an
- **Contrat :** 2 contrats successifs
  - **LICENCE Informatique / Cybersécurité** | 1 an
  - **INGÉNIEUR Cyberdéfense** | 2 ans
- **Alternance :** 55% du temps en entreprise | 25% du temps en CFA | 20% à distance

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

BRUZ / RENNES | de septembre 2024 à septembre 2027

Objectif de la formation

A l'issue de la formation, les apprenants 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 informatiques
- Auditer la sécurité du système d'information
- Gérer un système d'information après compromission
- Superviser le système d'information
- 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*



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

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

Programme

PÉDAGOGIE

La pédagogie est organisée autour de plusieurs projets où les apprentis, par petits groupes, sont confrontés à des défis et problèmes actuels motivants en lien avec leur future profession.

La pédagogie par projet, centrée sur l'apprenti, permet de susciter l'intérêt, la soif d'apprendre et l'autonomie indispensables dans l'exercice de leur activité professionnelle.

MATIÈRES

- Cyberdéfense
- Test d'intrusion
- Forensique
- Exercices de gestion de crise
- CTF Jeopardy et OSINT
- Sécurité des réseaux
- Sécurité des bases de données
- Sécurité des systèmes d'exploitation
- Cryptologie
- Droit et réglementation
- Développement de logiciels sécurisés
- Systèmes spécifiques, informatique industrielle
- Hacking social
- Projets cyber sur 2 ans
- Géopolitique

Indicateurs de performance

- **Satisfaction stagiaire :**

100 %

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

Indicateurs mis à jour le 26/09/2022

Modalités d'évaluation et d'examen

Modalités d'évaluation

Plusieurs évaluations sont réalisées tout au long de la formation afin que l'apprenant puisse évaluer sa progression. Les situations d'évaluation peuvent être de plusieurs types.

- QCM | Étude de cas | Dossier | Présentation orale | Travaux pratiques | Mise en situation reconstituée | Jeux de rôles

Elles peuvent être individuelles ou collectives.

Modalités d'examen

A l'issue de la 1ère année, les candidats▪es sont présentés▪ées aux épreuves générales et techniques de la **LICENCE - Informatique.**

A l'issue de la 3ème année, les candidats▪es sont présentés▪ées aux épreuves générales et techniques d u **INGÉNIEUR EN CYBERSÉCURITÉ - Systèmes, réseaux et cyberscurité.**

- Évaluation des Unités d'Enseignement
  - Évaluations pratiques, écrites et/ou orales, dont les modalités seront précisées par les équipes pédagogiques selon les unités.
- Certification TOEIC en anglais (listening and reading)
  - Évaluation des compétences de compréhension écrite et orale dans un contexte professionnel
- Évaluation des activités et projet réalisés en entreprise
  - Mémoire (présentation entreprise, activités menées, projet réalisé)
  - Soutenance orale (avec pour support le mémoire)

Validation

LICENCE INFORMATIQUE

- Diplôme de niveau 6 (BAC+3/4)
- Code RNCP* : 24514
- Certificateur : CNAM
- Date d'échéance de l'enregistrement : 01-01-2025

INGÉNIEUR EN CYBERSÉCURITÉ - Systèmes, réseaux et cyberscurité

- Diplôme de niveau 7 (BAC+5) reconnu par la CTI (Commission des Titres Ingénieurs)
- Code RNCP* : 38105
- Certificateur : AFORP Formation

- Date de début des parcours certifiants : 18-10-2023
- Date d'échéance de l'enregistrement : 18-10-2026

INGÉNIEUR EN CYBERDÉFENSE - Titre ingénieur - Ingénieur diplômé du Conservatoire national des arts et métiers, spécialité Informatique

Double certification, réalisée hors temps de travail

- *Diplôme de niveau 7 (BAC+5) reconnu par la CTI (Commission des Titres Ingénieurs)*
- *Code RNCP* : 37357*
- Certificateur : CNAM
- *Date de début des parcours certifiants : 01-09-2022*
- *Date d'échéance de l'enregistrement : 31-08-2024*

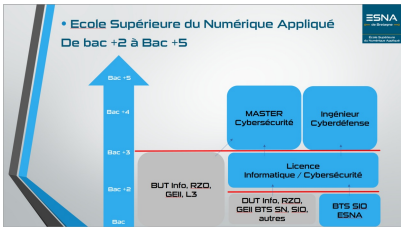
Les certifications sont composées de plusieurs blocs de compétences dénommés certificats de compétences professionnelles (CCP).

Les formations peuvent être validées 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**
  - *Spécialiste en gestion de crise cyber, Chef de projet sécurité, Expert en cybersécurité, Pentester (testeur d'intrusion), Consultant, Expert en sécurité des systèmes d'information, Expert Forensique (investigateur numérique), RSSI...*

Contacts

Pôle Formation UIMM Bretagne | Site deBruz



Ecole interne ESNA Bretagne

Campus de Ker Lann | Rue Henri Moissan | 35174 BRUZ

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