

Exemples de métiers

- Spécialiste en gestion de crise cyber
- Chef de projet sécurité
- Expert ou experte en cybersécurité
- Expert ou experte en sécurité des systèmes d'information
- Expert ou experte en tests d'intrusion - sécurité des systèmes d'information
- Expert ou experte en sécurité informatique

Lieu de formation

Rennes

À noter

L'admission définitive sera soumise à la signature d'un contrat d'apprentissage (ou de professionnalisation) avec une entreprise.

En partenariat avec

le **cnam**

En savoir +

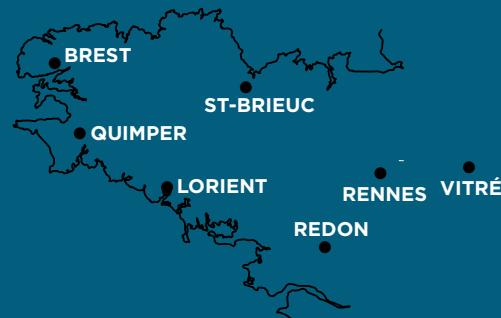
- **Nous rencontrer**
 - > Sur forums, lors de nos portes ouvertes (consulter notre site).
 - > Tous les jours, avec ou sans rendez-vous.

CONTACTS

● RENNES

Campus de Ker Lann • Rue Henri Moissan
BP 67429 • 35174 BRUZ CEDEX

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



Parcours Ingénieur Cyberdéfense

Edito 02 96 33 04 05. Ne pas jeter sur la voie publique. Photos non contractuelles.



FORMATION PAR ALTERNANCE
École Supérieure du Numérique Appliqué



CFA DE
L'INDUSTRIE



www.formation-industrie.bzh

L'évolution du numérique a mené à la création d'un cyberspace 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 sécurité des systèmes d'information. Il 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).

Profil

Construisez votre parcours d'ingénieur par étapes

- 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.
- Être âgé(e) de 15 à 29 ans révolus*.
- Être de nationalité française, ressortissant de l'union

*Pour les + de 30 ans, possibilité de se former en contrat de professionnalisation : nous consulter.

Programme au CFA

- 75% du temps en entreprise, 25% du temps en CFA
- 600 heures de formation sur 15 mois

Les 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

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.

Compétences et missions

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



Qualités requises

Esprit d'analyse
et de synthèse - Rigueur
Vision d'ensemble
Réactivité - Polyvalence
Curiosité
Communication

Secteurs concernés

Il exerce son activité au sein d'opérateurs d'importances vitales (OIV), d'une entreprise de service du numérique (ESN), d'un industriel, d'une PME.

