

L'ESNA

AU SERVICE DE LA FORMATION
DES SPÉCIALISTES DES SYSTÈMES
NUMÉRIQUES, DE LA CYBERSÉCURITÉ
ET DE LA ROBOTIQUE



L'ESNA a été créée par le Pôle Formation UIMM Bretagne qui unit les acteurs du réseau emploi-formation de l'industrie, autour d'un objectif commun : proposer aux entreprises les compétences dont elles ont besoin et donc, proposer aux futurs apprenants une palette de formations aux métiers qui recrutent ou aux métiers d'avenir.

NOS MOYENS, VOTRE OUTIL POUR LA RÉUSSITE

- Des formateurs experts, issus de la formation professionnelle.
- Une politique d'assurance Qualité.
- Un encadrement alliant bienveillance et exigence
- Une mise à disposition de ressources pour le développement des projets des apprenants
- Des formateurs experts issus notamment de l'écosystème cyber de la région rennaise.
- Des plateaux techniques et des équipements pédagogiques performants :
 - un parc machines régulièrement renouvelé pour répondre aux exigences et aux évolutions technologiques.
 - des équipements pédagogiques adaptés.
- Des ressources de formations numériques.



NOUVEAU BÂTIMENT
notre site dédié de 3000 m²
(située sur le campus à Bruz/Rennes)

Les formations cyber se déroulent sur le campus de Ker-Lann à Bruz/Rennes

L'ESNA dispose de 6 sites proposant des formations diplômantes (bac +2 à bac +5) en alternance, véritable tremplin vers l'insertion professionnelle.



www.esna.bzh



www.esna.bzh



www.formation-industrie.bzh



CONTACTEZ-NOUS

DIRECTEUR DE L'ESNA

Guillaume CHOUQUET **06 98 88 14 88**

guillaume.chouquet@formation-industrie.bzh

DÉCOUVREZ NOTRE ÉCOLE



ÉCOLE PARTENAIRE

le **cnam**
Bretagne



BAC +3 ET BAC +5 PAR ALTERNANCE

PARCOURS INGÉNIEUR CYBERDÉFENSE



ESNA
Bretagne

École Supérieure
du Numérique Appliqué

POP-COM COMMUNICATION



▶ DEVENEZ INGÉNIEUR CYBERDÉFENSE

La numérisation de notre société a profondément bouleversé tous les secteurs de l'activité humaine. Aujourd'hui, la défense de ce cyberspace 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. Voici quelques métiers pour illustrer cette activité : Pentester (Testeur d'intrusion), Expert Forensique (Investigateur numérique), Consultant en organisation de la Sécurité des Systèmes d'Information, Responsable de la sécurité des systèmes d'information (RSSI).



DIPLÔMES

Licence informatique option cybersécurité
Titre niveau 6 RNCP 24514

**Double diplomation :
Ingénieur en cybersécurité**
Titre niveau 7 RNCP 38105

Ingénieur en Cyberdéfense
Titre niveau 7 RNCP 37357
Reconnu par la CTI (Commission des Titres d'Ingénieurs)
Réalisé hors temps de travail



DURÉE

Bac +3 en 12 mois en alternance
600 heures de formation

Bac +5 en 24 mois en alternance
1 200 heures de formation

LA FORMATION



LE PROGRAMME

LES 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

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.



LES OBJECTIFS

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

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



LES MODALITÉS



ADMISSION

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

• PRÉ-REQUIS D'ENTRÉE EN FORMATION Bac+3

Être titulaire d'un Bac+2 Informatique (BTS, BUT...)

• PRÉ-REQUIS D'ENTRÉE EN FORMATION Bac+5

Être titulaire du diplôme Licence informatique parcours cybersécurité

• PUBLIC

- Être âgé(e) de 15 à 29 ans révolus en apprentissage et +29 ans en contrat de professionnalisation (formation accessible aux salariés et aux demandeurs d'emploi)
- Être de nationalité française, ressortissant de l'UE ou étranger en situation régulière de séjour et de travail



PLUS D'INFOS



DATE ET LIEU

- Campus de Ker Lann à Bruz (Rennes)
- Rentrée : septembre



EXEMPLES DE MÉTIERS

- Spécialiste en gestion de crise cyber
- Chef de projet sécurité
- Expert en cybersécurité
- Pentester
- Consultant
- Expert en sécurité des systèmes d'information
- Investigateur numérique
- RSSI