

LA FILIÈRE CYBERSÉCURITÉ EN CÔTES D'ARMOR

Département des Côtes d'Armor

Hôtel du Département
9 place du Général de Gaulle
CS 42371
22023 Saint-Brieuc Cedex

Contact

Mission Enseignement supérieur,
recherche et innovation
MESRI@cotesdarmor.fr

cotesdarmor.fr



#assisesinnovation22

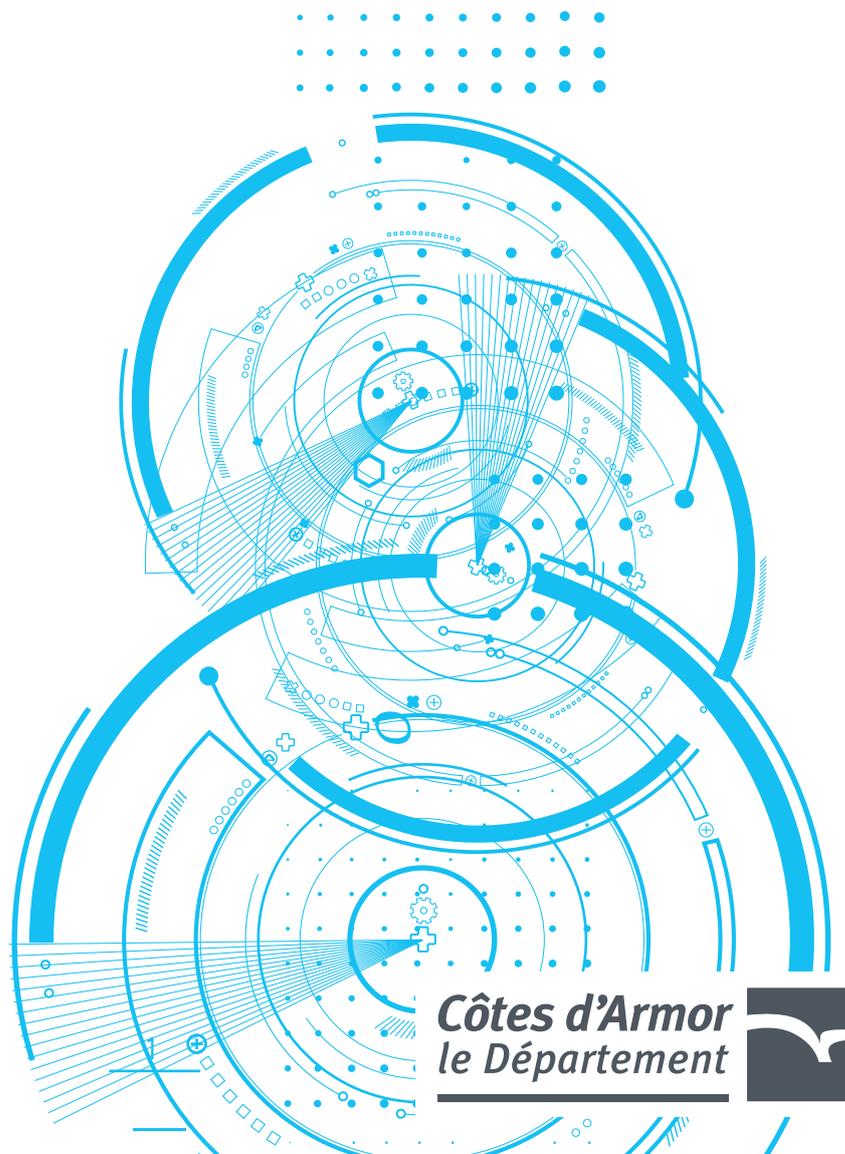
supcotesdarmor.fr

appli : sup22

la cité
des Métiers

des
Côtes
d'Armor

Côtes d'Armor
le Département





La cybersécurité est un terme nouveau dans le paysage industriel français : il concerne l'état pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Compte tenu de la place grandissante qu'occupe le numérique dans notre société, la cybersécurité est aujourd'hui incontournable, que ce soit en entreprise ou dans les institutions publiques. La cybersécurité, c'est la protection des données : des cyberattaques surviennent en effet chaque jour et dans tous les domaines (e-commerce, Défense, banques...), si bien que le marché de la cybersécurité a atteint les 13 milliards d'euros en 2016.

La Bretagne à la pointe de la filière cybersécurité

Le marché de la cybersécurité explose. Les besoins en main-d'œuvre qualifiée aussi. La Bretagne entend répondre à ces nouveaux besoins par une offre de formation pléthorique, regroupée en ce catalogue unifié et exhaustif (élaboré avec la Cité des Métiers).

Les besoins en cyberprotection ne font qu'augmenter. Les données des citoyens doivent être protégées, le savoir-faire et les outils industriels des entreprises aussi. Pour les États, il s'agit de se protéger face au cyberterrorisme. Développer l'offre de formation pour disposer d'une main-d'œuvre experte est donc une priorité.

La région Bretagne est historiquement en pointe dans le domaine des télécommunications. C'est donc en toute logique qu'elle a contribué, aux côtés du ministère de la Défense, à la création du Pôle d'Excellence Cyber (PEC). Regroupement de tous les acteurs de la formation, de la recherche et de l'économie, le PEC porte le savoir-faire hexagonal au-delà de nos frontières.

La filière défense et sécurité en Bretagne (en chiffres) :

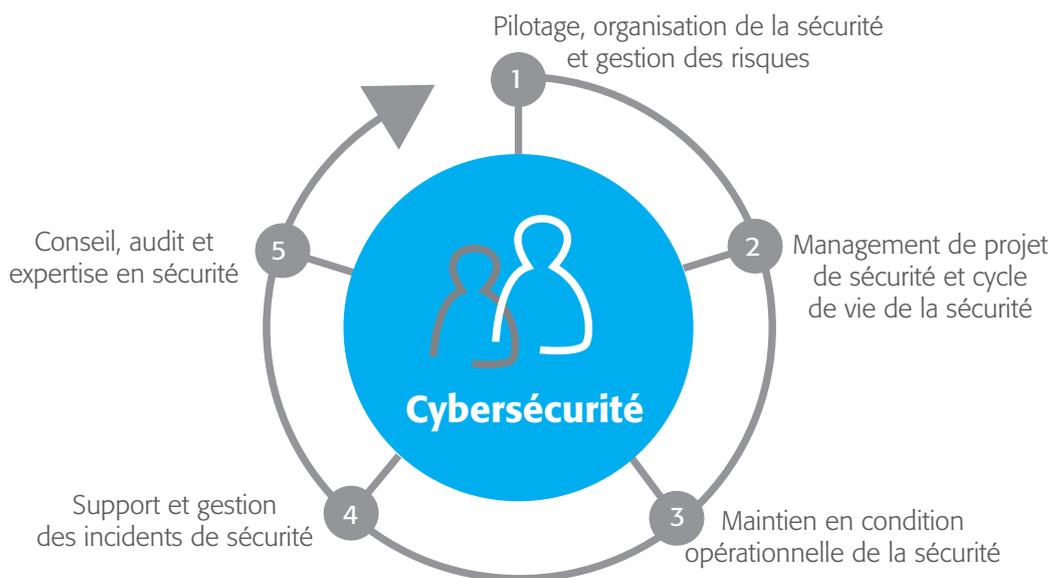


LES MÉTIERS DE LA CYBERSÉCURITÉ

Si aujourd'hui la filière emploie déjà 24 000 salariés, dans les entreprises du numérique, de l'ingénierie, des études, du conseil et de l'événement, ce chiffre devrait bondir dans les prochaines années. À l'horizon de 3 ans, ces entreprises anticipent une croissance des effectifs en cybersécurité de 6 %, soit 1 400 créations nettes d'emplois. Une croissance qui atteint les 8 % de création nette d'emplois d'ici 5 ans.

5 familles de métiers

Encore méconnus, les métiers liés à la cybersécurité sont très divers et couvrent un large champ d'activités et de compétences. Ils sont aujourd'hui structurés en 5 grandes familles :



La 1^{re} famille « pilotage, organisation de la sécurité et gestion des risques » :

regroupe l'ensemble des métiers à fortes responsabilités en termes de management de la sécurité du système d'information et de la gestion des risques :

- Responsable de la Sécurité des Systèmes d'Information (RSSI)/Responsable de la Sécurité Opérationnelle (RSO) Correspondant Sécurité
- Responsable du Plan de Continuité d'Activité

La 2^e famille « Management de projets de sécurité et cycle de vie de la sécurité » :

regroupe l'ensemble des métiers liés aux projets d'évolution de la sécurité du système d'information. Ils sont soit superviseurs de ces projets soit des acteurs majeurs :

- Directeur de programme sécurité
- Chef de projet sécurité
- Développeur sécurité
- Architecte sécurité
- Formateur en sécurité

La 3^e famille dite de « maintien en condition opérationnelle de la sécurité » :

couvre l'ensemble des métiers opérationnels ayant en charge la configuration et le déploiement de correctifs de sécurité et l'application de mesures de sécurité sur l'infrastructure technique :

- Administrateur sécurité
- Technicien sécurité

La 4^e famille « Support et gestion des incidents de sécurité » :

concerne les métiers intervenant directement sur les incidents de cybersécurité comme les virus, les ransomwares ou rançonniers, les fuites d'information... Ils participent également à l'amélioration continue des méthodes de détection et de prévention de ces incidents de sécurité :

- Analyste SOC (Security Operations Center)
- Chargé de la réponse aux incidents

La 5^e famille « Conseil, audit et expertise en sécurité » :

rassemble les métiers d'expertise en cybersécurité. Ces professionnels sont généralement missionnés par les entreprises pour répondre à un besoin ponctuel ou parce qu'ils disposent de compétences spécifiques :

- Consultant et auditeur gouvernance risques et conformité
- Consultant et auditeur sécurité technique
- Évaluateur sécurité des systèmes et des produits
- Cryptologue
- Expert juridique en cybersécurité
- Délégué à la Protection des Données (DPD)
- Formateur en sécurité

CONSULTANT CYBERSÉCURITÉ ET ANALYSTE SOC : LES PROFILS LES PLUS RECHERCHÉS

Quant à savoir quels sont les profils les plus recherchés par les entreprises françaises aujourd'hui, les plus forts besoins en recrutement se concentrent sur une poignée de métiers :



« Top 5 » des métiers que les entreprises de la branche recrutent actuellement

L'étude a été réalisée par le Syntec Numérique (syndicat professionnel des entreprises de services du numérique (ESN), des éditeurs de logiciels et des sociétés de conseil), de l'Opiiec (Observatoire Dynamique des métiers de la branche du Numérique, de l'Ingénierie, des Études et Conseil et de l'Événement) et du cabinet d'audit et de conseil comptable Ernst and Young (EY). Elle a été menée entre décembre 2016 et janvier 2017, auprès de 227 entreprises dont 202 entreprises du numérique, de l'ingénierie, des études, du conseil et de l'évènement.

LE DÉPARTEMENT TERRITOIRE DE FORMATION À LA CYBER

La cybersécurité est l'une des rares spécialités du numérique dont l'offre est cinq fois supérieure à la demande. Les candidats sont effectivement encore peu nombreux alors que les postes créés ne cessent de se multiplier. **Ce domaine vous intéresse ? Alors lancez-vous et formez-vous en Côtes d'Armor !**

NIVEAU BAC : BAC PRO des systèmes numériques (BAC PRO SN)

Établissements

- Lycée Félix Le Dantec à Lannion (modules cyber intégrés à la formation)
- Lycée Sacré-Cœur à Saint-Brieuc

Descriptif

Cette formation concrète et qualifiante déroule sur 3 ans. Elle vous permettra de devenir un professionnel lié à la préparation, l'installation, la mise en service, la maintenance préventive et/ou corrective des systèmes électroniques ou numériques.

Cette formation fait référence à des options qui sont déclinées à partir de grands secteurs d'activités de la filière électronique tels que :

- Sûreté et sécurité des infrastructures, de l'habitat et du tertiaire (SSIHT)
- Audiovisuels, Réseaux et Équipements Domestiques (ARED)
- Réseaux Informatiques et systèmes communicants (RISC)

Conditions d'accès

- Après une 3^e, 3^e PEP
- 2nde générale et technologique

NIVEAU BAC : BAC STI2D spécialité systèmes d'information et numérique (STI2D SIN)

Établissements

- Lycée La Fontaine des Eaux à Dinan (modules cyber intégrés à la formation)
- Lycée Félix Le Dantec à Lannion (modules cyber intégrés à la formation)
- Lycée Freyssinet à Saint-Brieuc
- Lycée Fulgence Bienvenue à Loudéac
- Lycée Sacré-Cœur à Saint-Brieuc

Descriptif

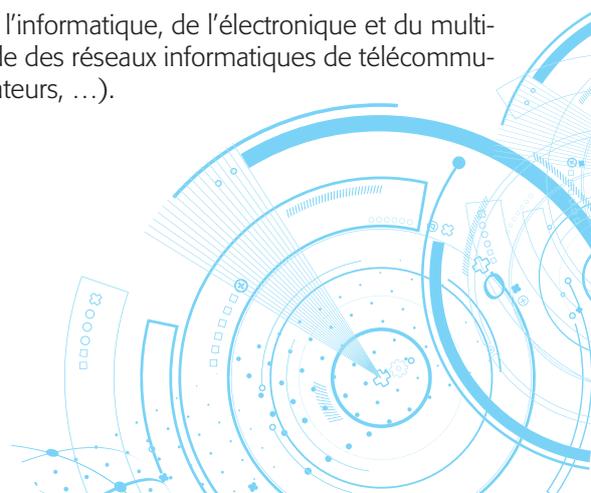
Le Bac STI2D permet d'acquérir des compétences technologiques transversales, orientées développement durable, et basées sur l'étude des matériaux, de l'énergie et de l'information.

Cette formation scientifique et technologique propose des enseignements généraux indispensables à une poursuite d'étude ouverte : mathématiques, physique-chimie, français, langues vivantes 1 et 2, philosophie, histoire-géographie, EPS, et des enseignements technologiques avec 4 spécialités au choix dont SIN.

La spécialité SIN (Système d'information et Numérique) explore les domaines de l'informatique, de l'électronique et du multi-média au travers d'activités de programmation (langage C, HTML, Android), d'étude des réseaux informatiques de télécommunications (voix, données, images) et d'électronique (étude des capteurs, amplificateurs, ...).

Conditions d'accès

- 2nde générale et technologique



NIVEAU BTS : BTS Systèmes informatiques aux organisations (SIO)

Établissements

- Lycée Rabelais à Saint-Brieuc
- Lycée Félix Le Dantec à Lannion

Descriptif

À l'ère de l'économie numérique, l'informatique est plus que jamais au service de l'entreprise. Elle répond à son besoin de performance, tant par l'équipement que par les applications car l'information se doit d'être disponible, rapide, fiable et sécurisée. Par conséquent, l'informatique est un secteur porteur et surtout plein de promesses en termes d'emploi.

Le BTS SIO est un diplôme se préparant en **2 ans après le bac**.

Il offre 2 spécialités :

- Solutions Logicielles et Applications Métiers (SLAM) qui permet de réaliser, adapter et maintenir des applications mobiles ou non.
- Solutions d'Infrastructure Systèmes et Réseaux (SISR) qui permet de mettre en place, adapter et maintenir des systèmes et des services réseau en assurant le fonctionnement optimal des équipements.

Conditions d'accès

- Titulaires d'un baccalauréat technologique STMG et STI2D, d'un baccalauréat général (S, ES) ou d'un baccalauréat professionnel (SN)
- Le futur informaticien doit être curieux et rigoureux

NIVEAU BTS : BTS Systèmes numériques option informatique et réseaux (SN-IR)

Établissement

- Lycée Félix Le Dantec à Lannion (modules cyber intégrés à la formation)

Descriptif

Le technicien supérieur en systèmes numériques intervient sur les systèmes informatiques utilisés dans tous types d'entreprises des secteurs de l'industrie ou au sein d'une SSI.

Les étudiants de BTS SN-IR se forment aux nombreux domaines et technologies de l'informatique :

- Programmation de logiciels dans le langage C++
- Développement d'applications Web (HTML5, JavaScript et PHP)
- Conception de bases de données relationnelles (SQL, Merise)
- Administration des systèmes d'exploitation Linux
- Cyber sécurité, chiffrement, signature numérique, cyber défense
- L'internet des objets (IOT), technologie énocéan (domotique), M2M, e-domotique, e-santé, e-loisir, e-robot
- Étude de l'architecture des ordinateurs et utilisation de cartes d'entrées/sorties
- Déploiement et programmation de réseaux industriels
- Installation et configuration de réseaux informatiques (VLAN, routage, pare-feu...)
- Mise en œuvre des services et étude des protocoles internet (IP, TCP, web, e-mail, FTP, DNS, DHCP...)

Les mathématiques, la physique, le français, l'anglais, l'économie et la gestion complètent la formation.

Conditions d'accès

- Titulaires des BAC : technologique STI2D, scientifiques S-SVT et S-SI, professionnel SN
- Étudiants issus d'IUT, de l'université ou d'autres BTS qui souhaitent compléter leur formation ou changer d'orientation.

NIVEAU DUT : Diplôme universitaire de technologie réseaux et télécoms DUT R&T

Établissement

- IUT Lannion

Descriptif

Le DUT R&T permet de comprendre, installer, gérer et commercialiser les réseaux informatiques et de télécommunications multimédias fixes ou mobiles (téléphone, TV, vidéo, données, jeux en ligne, web ...).

Les étudiants acquièrent des bases de cyber sécurité liées à ces différentes technologies.

Conditions d'accès

- Titulaires des BAC : scientifiques S, technologiques STI2D, ES

Poursuite d'études possibles

- ENSSAT, INSA, ESIR, ENSIBS

NIVEAU DUT : DUT R&T en année spéciale

Établissement

- IUT Lannion

Descriptif

L'année spéciale permet de préparer le DUT R&T en un an. Ce dispositif, qui tient compte du parcours antérieur, peut constituer une seconde chance ou l'occasion d'acquérir une double compétence.

Le DUT R&T permet de comprendre, installer, gérer et commercialiser les réseaux informatiques et de télécommunications multimédias fixes ou mobiles (téléphone, TV, vidéo, données, jeux en ligne, web ...).

Conditions d'accès

- Niveau Bac+2 de préférence scientifique : DUT, BTS, L2
- La formation s'adresse à des étudiants (formation initiale) et à des salariés/demandeurs d'emploi en reconversion (formation continue) ayant des connaissances dans le domaine scientifique et/ou technologique souhaitant découvrir ou approfondir des compétences en technologie des réseaux et télécommunications

Poursuite d'études possibles

- Écoles d'ingénieur : ENSSAT, IMT-Atlantique (FIP Telecom Bretagne), INSA (SRC Rennes), ESIR, ENSIBS (Cyberdéfense), IMT-Lille-Douai (FIP Télécom Lille)...
- L3 : Télécoms et Réseaux (Brest), Informatique (Brest)...
- LP : aGSRI



NIVEAU LICENCE LP :**Licence professionnelle aGSRI: administration et Gestion des Systèmes Réseaux informatiques**

Établissement

- IUT Lannion

Descriptif

La licence professionnelle aGSRI forme des administrateurs réseaux et systèmes informatiques polyvalents qui exerceront principalement dans des petites et moyennes entreprises de tous secteurs d'activité. La licence est structurée, pour les enseignements techniques, autour de trois domaines: les systèmes d'exploitation, les réseaux informatiques et les systèmes de gestion de données. Bien qu'une unité d'enseignement soit dédiée à la sécurisation des réseaux informatiques, la cyber-sécurité est une notion diffusée tout au long des apprentissages dans ces trois domaines. En disposant de connaissances précises sur la gestion des droits d'accès dans les systèmes d'exploitation et de gestion des données, des systèmes de supervision des activités d'un système ou d'un réseau, des protocoles de sécurisation des communications dans les réseaux, etc., nos étudiants diplômés sont capables de mettre en place des politiques de sécurisation d'un parc informatique.

Conditions d'accès

- Titulaires de DUT R&T, Info
- Titulaire de BTS SIO

NIVEAU LICENCE L3 :**Licence professionnelle d'analyste en sécurité des systèmes télécommunications, réseaux et informatiques (asstri)**

Établissement

- CNAM Sécurité Défense – Ploufragan

Descriptif

Construite en lien étroit avec les Ministères de la Défense et de l'Intérieur, cette licence professionnelle est officiellement reconnue par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). À l'issue de la formation, l'Analyste en Sécurité des Systèmes Télécoms Réseaux et Informatique (ASSTRI) doit être en mesure d'intervenir efficacement pour maintenir l'ensemble des équipements en état de fonctionnement. Il doit disposer de connaissances fondamentales suffisantes en lien avec certaines problématiques de sécurité. Il doit ainsi pouvoir auditer rapidement et efficacement un système afin d'en renforcer la sécurité. Sa vision des enjeux et ses aptitudes à traiter des données de sources diverses doivent lui permettre d'entreprendre des actions concrètes et pertinentes dans le cadre de ses futures responsabilités de technicien supérieur polyvalent et à haut potentiel.

Conditions d'accès

- Être titulaire d'un Bac+2 scientifique ou technique :
 - BTS : Systèmes informatiques aux organisations (SIO), Systèmes Électroniques (SE), Informatique et Réseaux (IR)
 - DUT : Réseaux et Télécommunications, Génie Électrique et Informatique Industrielle (GEII)
 - Brevet Supérieur de Technicien de l'Armée de Terre : détection et analyse des signaux électromagnétiques (DASEM)
- Ou être issu des classes préparatoires

NIVEAU LICENCE L3 : Licence informatique parcours analyste en cybersécurité

Établissement

- CNAM – Ploufragan, Lannion

Descriptif

Former des techniciens technophiles polyvalents aptes à gérer tout ou partie d'un système d'information (matériel, applications, serveurs, réseaux, données) et responsables de son fonctionnement, de son respect de la réglementation, de sa sécurité, de sa fiabilité et de son évolution

Conditions d'accès en L1

- être titulaire d'un baccalauréat scientifique, DAEU ou d'un diplôme étranger ou français admis en dispense d'acquis d'études ou de l'expérience.

Conditions d'accès en L3

- être titulaire d'un diplôme de niveau III en informatique (DUT informatique, DPCT informatique, BTS informatique de gestion, diplôme analyste programmeur du Cnam, DUT GEII, certains titres Afpa homologués au niveau III) ou d'un diplôme qui dispense des niveaux L1 et L2.
- être titulaire d'un diplôme de niveau III scientifique et des UE NFP135 et NFP136.

NIVEAU LICENCE L3 : Licence informatique parcours cybersécurité

Établissement

- CNAM Bretagne – Ploufragan

Descriptif

Former des techniciens technophiles polyvalents aptes à gérer tout ou partie d'un système d'information (matériel, applications, serveurs, réseaux, données) et responsables de son fonctionnement, de son respect de la réglementation, de sa sécurité, de sa fiabilité et de son évolution

Conditions d'accès en L1

- être titulaire d'un baccalauréat scientifique, DAEU ou d'un diplôme étranger ou français admis en dispense d'acquis d'études ou de l'expérience.

Conditions d'accès en L3

- être titulaire d'un diplôme de niveau III en informatique (DUT informatique, DPCT informatique, BTS informatique de gestion, diplôme analyste programmeur du Cnam, DUT GEII, certains titres Afpa homologués au niveau III) ou d'un diplôme qui dispense des niveaux L1 et L2.
- être titulaire d'un diplôme de niveau III scientifique et des UE NFP135 et NFP136.



CERTIFICAT DE COMPÉTENCE d'analyste en cybersécurité**Établissement**

- CNAM – Ploufragan, Lannion

Descriptif

Construite avec les entreprises membres du Pôle d'excellence cyber, cette formation vise au moins deux types de publics :

- de nouveaux profils souhaitant ouvrir et diversifier leurs compétences au travers d'une formation opérationnelle centrée sur des solutions immédiatement applicables en entreprise,
- des techniciens de la sécurité qui souhaitent élargir leur expertise et atteindre un premier niveau de certification dans le champ la cybersécurité ;

La formation est découpée en 2 modules d'enseignement :

- Cybersécurité : référentiels, objectifs et déploiement

Ce cours vise à permettre de concevoir, d'argumenter et de déployer une politique de sécurité informatique au sein d'une entreprise ou d'une collectivité en lien avec une analyse détaillée des nouveaux risques encourus.

- Menaces informatiques et codes malveillants : analyse et lutte

Cet enseignement permet d'acquérir des outils et des méthodes pour analyser les vulnérabilités des systèmes, comprendre et détecter les modes d'action des codes malveillants et entreprendre des actions de protection et de remédiation

En cumulant ces unités d'enseignement avec d'autres unités d'enseignement, les auditeurs pourront valider, à leur rythme, le certificat de compétence « Analyste en cybersécurité » lui-même intégré au sein de la licence en informatique. Il est possible aussi de continuer vers un diplôme d'ingénieur.

Conditions d'accès

- Bac+ 2 scientifique, technique ou informatique et/ou expérience professionnelle significative dans les métiers de l'informatique



NIVEAU INGÉNIEUR : Formation continue (jusqu'à 200 h)

Établissement

- Enssat (université de Rennes 1) – Lannion

Descriptif

Former des professionnels du numérique capables d'appréhender les enjeux, risques et principes de la cyber-sécurité, d'analyser la situation d'une entreprise puis de déployer une politique de cyber-sécurité. Les deux unités d'enseignement concernées abordent : les techniques d'authentification et de chiffrement (cryptographie, mises en œuvres et usages, protocoles d'authentification, vérification d'identité, protection des données, anonymisation), la sécurité des systèmes et des réseaux (systèmes d'exploitation, virtualisation, protocoles réseaux, équipements/architecture réseaux) avec en point focal la détection d'attaques, la sécurité du cycle de développement (conception, langages, tests).

Conditions d'accès

Cette formation, commune à celle d'élèves-ingénieurs de dernière année Informatique, s'adresse à tout professionnel de niveau bac+5 exerçant dans le secteur du numérique.

Contact : responsable.relations-industrielles@enssat.fr

Pour aller plus loin...

L'offre de formation bretonne en cybersécurité est regroupée en un document unique, dont le catalogue est disponible en téléchargement sur le site jeunes.bretagne.bzh.

NB : Une formation en cybersécurité de type licence professionnelle ne permet pas de se prétendre expert en cybersécurité mais elle permet néanmoins de donner une réelle plus-value à un Bac+2 en informatique.

Bac + 5 ou 6, c'est le niveau requis pour se prétendre expert en cybersécurité.



RECHERCHE

INNOVATION



Document rédigé en collaboration
avec la Cité des Métiers

Sources pour réaliser ce document :
www.onisep.fr ; www.regionsjob.com ; www.bretagne.bzh

cotesdarmor.fr    

#assisesinnovation22

supcotesdarmor.fr
appli : **sup22**

la cité
des Métiers

des
Côtes
d'Armor

Côtes d'Armor
le Département

