

Le site de formation

Université de Bretagne-Sud
Campus de Tohannic



ENSIBS - Vannes

Site de Vannes rue Yves Mainguy BP 573 – 56017 VANNES CEDEX

L'ENSIBS - Vannes se situe sur le Campus de Tohannic
Université Bretagne Sud (UBS).

Les étudiants bénéficient à cet effet de tous les services de l'UBS :
BU, Maison des Etudiants, services du CROUS
(restauration et logements, activités sportives...)

ensibs:
École
d'ingénieurs
Université Bretagne Sud

Contacts : 06 99 97 07 23
ensibs.cyberdefense@univ-ubs.fr
www.ensibs.fr

La formation Cyberdéfense en vidéos :



Ingenieur ENSIBS
l'aptitude au monde

Devenez ingénieur en cyberdéfense

Par l'alternance
et l'apprentissage

HABILITÉE PAR LA COMMISSION DES TITRES D'INGÉNIEUR

SOMMAIRE

Contexte et enjeux de la Cyberdéfense :

- Le contexte de la Cyberdéfense
- Une filière d'ingénieur en Cyberdéfense
- Les métiers de la Cyberdéfense : secteurs d'activité et profils de postes

page 3 à 9

Candidater à la formation Ingénieur Cyberdéfense :

- Votre profil
- Votre voie d'accès
- Le calendrier
- Comment candidater

page 10 à 16

La formation Ingénieur Cyberdéfense :

- La répartition des enseignements :
 - l'équipe pédagogique : enseignants et professionnels
 - les modules d'enseignements
- Une alternance École-Entreprise équilibrée
 - La formation Cyberdéfense : une co-responsabilité École-Entreprise
 - Les contrats d'alternance : apprentissage et professionnalisation

page 17 à 21

Notre éco-système

page 22

Le contexte de la cyberdéfense

Assurer en permanence la sécurité des systèmes des OIV
et des entreprises est l'enjeu fondamental de la Cyberdéfense



- Autorité gouvernementale
- Opérations militaires
- Opérateurs financiers
- Opérateurs Internet
- Industrie de l'électricité
- Industrie du nucléaire
- Industrie du pétrole
- Industrie de l'aéronautique
- Transport
- Chaîne alimentaire
- Gestion de l'eau
- Industrie spatiale

Le patrimoine français à Cyber défendre

- 218 Opérateurs d'Infrastructures Vitales (OIV)
 - 33 services de l'État : 15%
 - 185 opérateurs privés : 85%
- Et environ 600 entreprises de services

Enjeu de souveraineté nationale pour le numérique

- Perte de maîtrise technologique de la France face aux USA et la Chine
- Dépendance numérique de notre économie dans le cyberspace
- Vulnérabilité de nos infrastructures vitales interconnectées à grande échelle

Enjeu de maîtrise de la Cybercriminalité

- Prolifération et complexification des attaques sur des cibles de plus en plus variées.
- Incidents de sécurité en très forte croissance.

Soutien du gouvernement pour la formation

- La France a indiqué dans le Livre Blanc de la défense de la sécurité nationale de 2013 son intention de renforcer la formation
- L'Agence Nationale de la Sécurité des systèmes d'information (ANSSI), autorité nationale en matière de sécurité et de défense des systèmes d'information bénéficie d'un renforcement de ses compétences.

Les besoins des professionnels

Les entreprises publiques et privées ont été consultées et ont un besoin important de professionnels capables de :

- comprendre la menace et les modes opératoires des attaquants dans une approche système
- construire la sécurité des infrastructures dans une approche globale pour mieux se protéger (architecture cybersécurité)
- gérer des crises cybernétiques quelle que soit leur ampleur

Les besoins en recrutement d'ingénieurs sont estimés actuellement par ces entreprises à plus de 1000 ingénieurs par an (800 pour le privé et 200 pour le public).

Les entreprises ont peu de personnels formés spécifiquement aux métiers de la cybersécurité, domaine pluridisciplinaire pour appréhender la complexité des systèmes :

- techniques de l'informatique, de l'électronique embarquée et des réseaux de télécommunication
- cadre juridique de la cybersécurité : arsenal juridique, doctrines d'emploi, règles d'engagement
- formation humaine, économique et éthique
- approche système de la sécurité (systèmes industriels, systèmes d'information, systèmes financiers, systèmes d'armes...)

Manque de formations d'ingénieurs dédiés aux métiers de la cybersécurité en France

Une filière d'ingénieur en Cyberdéfense

Pour répondre à l'urgence des besoins de formation des entreprises françaises publiques et privées et pour constituer un réel vivier d'emploi, l'ENSIBS a créé la première école française d'ingénieurs universitaire en cybersécurité en partenariat avec :

- les organismes étatiques référents en cybersécurité :
 - l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), service du Premier ministre.
 - Ministère de la Défense, Ministère de l'Intérieur
- des industriels majeurs en cybersécurité comme, Orange, Thales, Cap Gemini, Sopra Steria, Nokia, Airbus, CGI, Atos, La Poste, ...
- le Conseil régional de Bretagne
- le Conseil départemental du Morbihan
- l'Union des Industries des Métiers de la Métallurgie de Bretagne (UIMM)
- le Centre de Formation des Apprentis de l'Industrie (CFAI de Bretagne)
- l'Institut des Techniques d'Ingénieur de l'Industrie de Bretagne (ITI)

Le soutien de ces différents partenaires :

- contribue à la notoriété de la formation
- permet d'impliquer les experts étatiques et industriels dans les enseignements
- favorise la contractualisation avec les apprentis
- facilite le recrutement des apprentis à l'issue de la formation

Cette formation d'ingénieurs est :

- Habilitée par la Commission du Titre d'Ingénieur
- Labellisée par l'Agence Nationale de la Sécurité des Systèmes d'information



Les partenaires fondateurs de la formation :



Agence Nationale de la Sécurité des Systèmes d'Information

Le Livre blanc sur la défense et la sécurité nationale considère le risque d'une attaque informatique contre les infrastructures nationales comme l'une des menaces majeures dans les quinze prochaines années et recommande à l'Etat de faire de la prévention et de la réaction aux attaques informatiques une des priorités majeures de son dispositif de sécurité nationale. Ces orientations ont été réaffirmées par le Conseil des ministres du 25 mai 2011 qui a notamment mis l'accent sur l'importance de développer la formation en matière de défense et de sécurité des systèmes d'information. Je ne peux que vous encourager à poursuivre la démarche engagée par l'ENSIBS à laquelle l'ANSSI participe. Je confirme que les besoins en recrutement de spécialistes en sécurité et défense des systèmes d'information sont très élevés.

Patrick Pailloux,
Directeur général de l'ANSSI



Alcatel-Lucent

Notre groupe est un acteur majeur de la conception et de la mise en oeuvre des réseaux de télécommunication, aussi bien fixes que mobiles. Ces réseaux sont la clé de voute de nombreux usages - toujours plus numériques - dans des domaines aussi variés et stratégiques que le commerce international, les réseaux interministériels, le transport, l'énergie, sans oublier la Défense, et de nombreux autres secteurs d'activités. Dans ce cadre, Alcatel-Lucent a été sollicité pour porter son concours à ce projet de création d'une filière d'enseignement dans le domaine de la cybersécurité et contribuera à donner certains enseignements de même qu'à accueillir des étudiants dans le cadre de cette formation en alternance. Nous sommes prêts à apporter notre savoir-faire et notre contribution au développement de cette nouvelle filière d'enseignement. Les porteurs du projet proposent qu'Alcatel-Lucent soit le parrain d'honneur du projet. Nous sommes très honorés de cette proposition que nous acceptons avec enthousiasme.

Pascal Homisy,
Président Directeur Général
Alcatel-Lucent France



La cybersécurité, une activité primordiale pour un opérateur mondial

La cybersécurité est devenue en quelques années un enjeu majeur pour nos sociétés «hyperconnectées» grâce à internet.

C'est donc pour le Groupe international Orange, à la fois opérateur domestique dans plus de 30 pays (activités internet, ADSL, téléphonie fixe et mobile) et fournisseur de services de communication aux entreprises partout dans le monde, le cœur d'une posture de sécurité dynamique face à la menace pour protéger ses propres infrastructures et garantir la continuité des services fournis à ses clients.

Le Groupe Orange s'organise en conséquence en renforçant sa gouvernance, ses structures et les compétences de ses équipes dans les différents métiers de la sécurité.

Nous avons rejoint le comité métier de l'école de cybersécurité de l'ENSIBS car cette formation globale et dédiée est unique en France, et nous souhaitons nous appuyer sur son programme pour répondre à nos besoins importants de compétences, de technicité, et de passions. Orange apportera son savoir-faire et ses nombreux retours d'expérience d'opérateur mondial dans le développement de cette nouvelle filière d'enseignement.

Au sein d'une entreprise innovante et leader dans le domaine des technologies de l'information et de la communication, seront ainsi offertes aux étudiants des perspectives de métiers passionnants dans les différentes spécialités de la sécurité (architecture, infrastructures, plateformes de services, systèmes d'information, portails, offres marketing, conseil, audit,...) et un parcours riche en expériences.

Jean-Luc MOLINER
Directeur de la sécurité
du groupe Orange



Thales communications & sécurité est depuis plusieurs mois impliqué dans le projet de l'offre de formation en cybersécurité proposée par l'ENSIBS. La cybersécurité apparaît aujourd'hui comme un enjeu stratégique pour les Etats.

Afin de répondre rapidement aux besoins de nos clients étatiques et privés, nous recherchons activement des ingénieurs formés aux techniques de cybersécurité. Il n'existe malheureusement pas de formation d'ingénieurs équivalente à ce jour en France. A ce titre, nous avons rejoint le comité métier de l'ENSIBS afin de pouvoir participer à la définition et à la mise en place de cette formation d'ingénieurs qui devrait couvrir nos besoins en recrutement.

Pierre Jeanne,
VP du domaine sécurité des
systèmes d'information de Thales

Les prérequis

Une **réelle passion** personnelle pour le nouveau domaine d'activité en plein essor qu'est la cybersécurité.

Le **désir de participer à l'aventure pionnière** qui relèvera les défis stratégiques de la protection des infrastructures vitales du pays face à la menace de cyberattaques.

Le souhait de vous **former à un métier d'ingénieur par une formation en alternance** équilibrée entre école et entreprise.

La volonté d'avoir une **formation opérationnelle** :

- **grâce à une expérience professionnelle significative** qui favorisera votre première embauche
- **en cohérence avec les besoins des entreprises** du domaine

Les compétences à acquérir

Analyser le risque cybernétique

- Analyser la menace et diagnostiquer le mode opératoire des attaquants
- Etudier les vulnérabilités matérielles et logicielles ainsi que les attaques sur les infrastructures
- Comprendre l'interconnexion et l'évolutivité à grande échelle des systèmes dans le cyberspace
- Définir une politique de sécurité

Construire la sécurité dynamique des infrastructures dans une approche système

- Résoudre des problèmes complexes de niveau système (de nature technologique) par un panel de solutions à la fois méthodologiques, technologiques, organisationnelles, humaines, juridiques et déontologiques
- Concevoir, réaliser et mettre en oeuvre un ensemble de solutions de sécurité
- Concevoir, réaliser et mettre en oeuvre la protection des systèmes des Opérateurs d'Infrastructures Vitales (OIV)
- Conduire une approche systémique de la sécurité pour sécuriser des systèmes industriels, des systèmes d'information, des systèmes financiers, des systèmes d'armes...

Gérer des crises cybernétiques

- Concevoir, développer et exploiter un centre opérationnel de cybersécurité
- Savoir détecter dynamiquement les attaques
- Savoir réagir en situation de gestion de crise en conformité avec le cadre juridique, les doctrines d'emploi et les règles d'engagement de la cybersécurité
- Expertiser, auditer et évaluer les résistances des configurations techniques des systèmes
- Savoir adopter un comportement éthique et déontologique en situation de gestion de crise
- Savoir communiquer pendant une crise

Manager des projets complexes de sécurité des systèmes

8

Les secteurs d'activité

Les secteurs d'activité visés par cette formation sont principalement ceux des Opérateurs d'Infrastructures Vitales français :

- Etat, Défense, Banques et Finances, Opérateurs Internet et télécom, Energie (EDF, nucléaire, pétrole), Espace, Santé, Transport (routier, portuaire, aérien), Automobile, Aéronautique, Electronique.....

Les secteurs d'activités suivants sont aussi concernés par cette formation :

- Entreprises industrielles et sociétés de services qui réalisent, maintiennent et supervisent les infrastructures des Opérateurs d'Infrastructures Vitales, comme : Nokia, Orange, Thales, Airbus, Sopra Steria, Cap Gemini, CGI, Atos, La Poste, Siemens, Schneider, Areva ...
- Toutes entreprises industrielles ou de services et les PME dont le système d'information est connecté à l'Internet.

Les métiers

Les principaux métiers accessibles aux ingénieurs diplômés sont :

- Ingénieur expert en cybersécurité – cybersécurité
- Ingénieur « cyber architecte »
- Manager d'un centre opérationnel de cybersécurité
- Chef de projet en management de la sécurité

Mais également :

Chef de projet sécurité, Auditeur technique ou organisationnel, Ingénieur R&D en sécurité, Ingénieur sécurité des systèmes, Développeur et intégrateur de sécurité de produits COTS, Evaluator sécurité, Ingénieur qualification sécurité, Superviseur sécurité, Consultant gouvernance, risque et conformité en sécurité, Conseil en cybersécurité, Architecte cybersécurité, Chef de produit sécurité, Manager sécurité, Responsable d'un centre opérationnel de cybersécurité, Responsable SOC, Enseignement et recherche, Ingénieur technico commercial...

9

Votre voie d'accès

Diplôme d'ingénieur

en cyberdéfense

BAC + 5

Année : Management et Ingénierie de sécurité des systèmes (défense dynamique)

600 h

BAC + 4

Année 2 : Ingénierie des technologies et solutions de sécurité

600 h

BAC + 3

Année 1 : Tronc Commun en sciences pour l'ingénieur

600 h

Voie N°1
voie principale

Contrat d'apprentissage
(limité à 50 places)

Formation en 3 ans

Recrutement :
IUT
L3
BTS (ATS)
PEI ENSIBS
CPGE

Voie N°2
en poursuite
d'études

Contrat d'apprentissage
ou de professionnalisation

Formation en 2 ans

Recrutement
à Bac + 4
ou titre équivalent

Voie N°3
en formation
continue

VAE
VAP

Procédure
sur dossier

Voie d'accès N°1

Voie d'accès principale

Formation initiale d'ingénieurs en 3 ans par alternance et par apprentissage

Pour intégrer la première année de l'école d'ingénieurs en formation initiale par alternance et par apprentissage, plusieurs solutions sont possibles :

- Être titulaire d'un DUT principalement : Informatique, Réseaux et Télécommunications (RT), Génie Electrique et Informatique Industrielle (GEII)
- Être titulaire d'une Licence
- Être titulaire d'un BTS Informatique ou Réseaux (une prépa Adaptation Technicien Supérieur (ATS) est conseillée)
- PEI ENSIBS
- CPGE

Autres conditions requises :

- Être âgé de 30 ans maximum à la date de début du contrat (Expérimentation en région Bretagne jusqu'à 2019)
- Signer un contrat d'apprentissage pour 3 ans
- Être intéressé par la complémentarité école et entreprise et motivé pour travailler dans une entreprise (comme salarié avec le statut d'apprenti) pendant 3 ans

Vous percevrez un salaire pendant la formation en fonction de votre âge et de votre année de formation. Vous cotiserez pour votre future retraite.

Il n'y a que 50 places pour cette voie d'accès

Avec le statut d'apprenti, les droits universitaires sont exemptés

Voie d'accès N°2

En poursuite d'étude

Formation d'ingénieurs en 2 ans par alternance en contrat d'apprentissage ou contrat de professionnalisation.

Pour intégrer la deuxième année de l'école d'ingénieurs par alternance, vous devez être titulaire d'un diplôme Bac + 4 dans le domaine informatique et réseaux (comme un Master 1) ou d'une 1ère année validée en école d'ingénieurs ou titre équivalent.

Deux cas de contrats :

- 1 - Formation d'ingénieurs en 2 ans par alternance en contrat d'apprentissage pour la poursuite d'études d'un étudiant
- 2 - Formation d'ingénieurs en 2 ans par alternance en contrat de professionnalisation pour une reprise d'études

Autres conditions requises :

- Signer un contrat de 2 ans auprès d'une entreprise partenaire (contrat d'apprentissage si âgé de plus de 30 ans maximum à la date de signature du contrat et contrat de professionnalisation au delà de 30 ans)
- Être intéressé par la complémentarité école et entreprise et motivé pour travailler dans une entreprise, comme salarié, pendant 2 ans

Vous percevrez un salaire pendant la formation en fonction de votre âge et de votre année de formation. Vous cotiserez pour votre future retraite.

Voie d'accès N°3

En formation continue

Pour obtenir le diplôme d'ingénieur par la voie de la formation continue, le candidat doit se rapprocher du service de formation continue de l'Université de Bretagne Sud : formation.continue@univ-ubs.fr

Il sera accompagné pour étudier son projet de validation de ce diplôme compte tenu :

- de son expérience et de son diplôme,
- des modalités de validation : VAP, VAE, formation,
- des conditions financières : plan de formation, CIF...

VAP :

Validation des Acquis Professionnels. La VAP permet d'accéder à des formations de l'enseignement supérieur, ou de faire acte de candidature à un concours, sans être titulaire des diplômes requis. Conditions exigées pour accéder au dispositif : avoir interrompu les études depuis au moins deux ans et être âgé de vingt ans minimum.

VAE :

Validation des Acquis par l'Expérience : Toute personne, quel que soit son âge, sa nationalité, son statut et son niveau de formation, qui justifie d'au moins trois ans d'expérience en rapport direct avec la certification visée, peut prétendre à la VAE.

LE CALENDRIER D'ADMISSION

Les dates clés sont actualisées chaque année sur le site de l'ENSIBS – Ingénieur Cyberdéfense – Recrutement

Décembre à Mars

- Inscription et téléchargement du dossier de candidature en ligne sur le site ENSIBS : www.ensibs.fr
- rubrique Formation Cyberdéfense Candidater

Avril

- Envoi du dossier complet (*avis de poursuite d'études en école d'ingénieurs de l'établissement d'origine obligatoire*) au plus tard à la date indiquée sur le dossier (*cachet de la poste faisant foi*) à l'ENSIBS : rue Yves Mainguy BP 573 - 56017 Vannes cedex.
- Commission pédagogique : sélection des candidats admissibles à l'oral.

Mai :

- 17 et 18 mai : entretiens de motivation par la Commission d'admission composée des entreprises partenaires.
- Les étudiants à l'étranger seront auditionnés à distance (*ils devront le mentionner dès le dossier de candidature dans leur CV*).
- Publication de la liste des candidats admis
- 25 mai Journée Alternance : informations et conseils pour décrocher son contrat

Mai-Juin-Juillet :

- Promesse d'embauche et signature du contrat

Septembre :

- 3 septembre : rentrée et inscription définitive. Seront inscrits définitivement, les admis, ayant obtenu le diplôme requis et ayant signé un contrat avec une entreprise en France, dans la limite des places disponibles.

Année 1:

Tronc Commun en sciences pour l'Ingénieur 600 h

- Sciences économiques et de gestion : 60h
- Anglais : 60h
- Mathématiques : 100h
- Base en sécurité - Base de l'électronique : 50h
- Programmation : 100h
- Ingénierie des systèmes : 55h
- Architecture et systèmes de base : 55h
- Projet système : 20h
- Séminaires de gestion de crise (Facteur Humain- Base cyber) - DTF - Ethique : 100h

Les bases

Année 2:

Ingénierie des technologies et des solutions de sécurité 600 h

- Anglais : 30h
- Sécurité des systèmes de base : 70h
- Droit et Réglementation en cybersécurité : 50h
- Sécurité des réseaux : 100h
- Projet pluridisciplinaire en solution de sécurité : 100h
- Analyse des vulnérabilités numériques : 60h
- Protection des développements et des plateformes : 70h
- Ingénierie de solutions de sécurité : 60h
- Innovations Cyber : Big data - Objets connectés - Infrastructure industrielle : 60h

Protéger

Année 3:

Management et Ingénierie de sécurité des systèmes (défense dynamique) 600 h

- Management stratégique : 90h
- Anticipation et systémique de la menace : 40h
- Détection et analyse des attaques : 30h
- Stratégie de réaction face aux attaques : 30h
- Ingénierie et exploitation d'un centre opérationnel de cyber sécurité : 25h
- Évaluation de la résistance des systèmes : 50h
- Connaissance du contexte professionnel et ouverture internationale : 25h
- Sciences économiques et de gestion et langues : 50h
- Maîtrises en cybersécurité : 60h
- Séminaires de gestion de crise (cyberdéfense d'un opérateur vital): 200h

Défendre

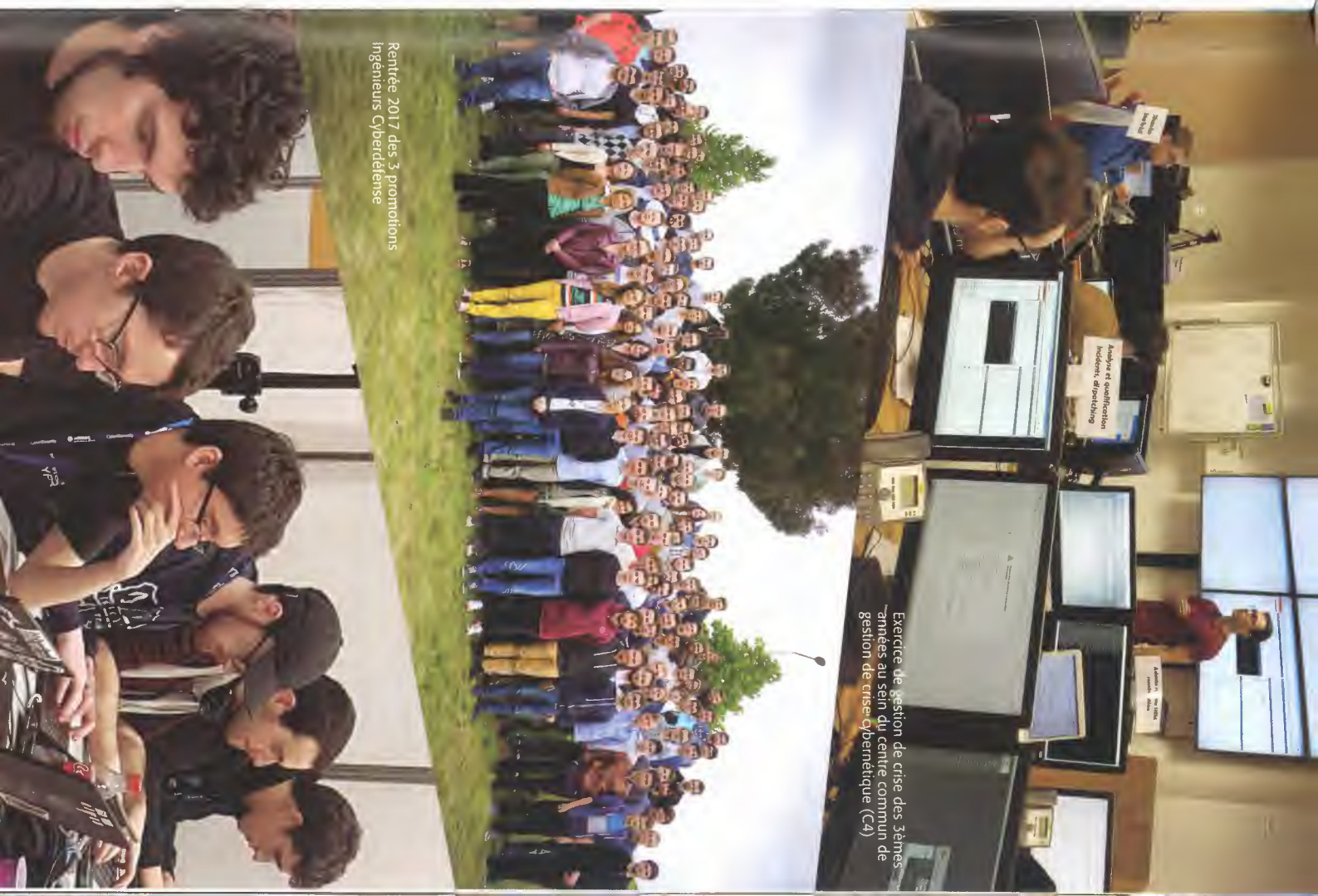


Une
équipe

[illegible]

3 Période de formation à l'école

- Les alternants passent 22 semaines en formation à l'école et 30 semaines en formation en entreprise
- Au cours des périodes de formation en entreprise, l'alternant peut poser ses congés payés



Exercice de gestion de crise des 3èmes années au sein du centre commun de gestion de crise cybernétique (C4)

Rentrée 2017 des 3 promotions
Ingénieurs Cyberdéfense

Ingénieur Cyberdéfense : une co-responsabilité École-Entreprise

Co-construction initiale de la formation

Le contenu de la formation est le fruit d'une co-construction entre les entreprises, l'École et le CFAI de Bretagne.

Co-recrutement des apprentis

Les entreprises sont fortement impliquées dans le processus de sélection des candidats, c'est donc un co-recrutement des apprentis-ingénieurs qui est effectué.

Co-formation des apprentis

La formation se fait à la fois à l'École et en entreprise. L'alternance permet :

- l'intrication de l'acquisition des compétences académiques et professionnelles
- d'être formé par une équipe permanente d'enseignants spécialisés en cybersécurité et cyberdéfense
- de bénéficier de l'expertise métiers d'intervenants issus à la fois des services de l'État et du monde de l'entreprise
- d'apprendre grâce à une pédagogie basée sur l'apprentissage et l'expérience en entreprise

Co-évaluation des apprentis

Dans la continuité de la co-formation, l'École et les entreprises co-évaluent les apprentis-ingénieurs sur les 3 années.

Co-évaluation annuelle de la formation

Grâce au conseil de perfectionnement l'École fait évoluer le contenu de la formation en lien avec les entreprises et leurs réalités professionnelles.

L'ENSIBS met en relation candidats et entreprises :

- Elle recueille les besoins des entreprises
- Elle accompagne les candidats dans les recherches de contrat

Les contrats d'alternance

Contrats d'apprentissage et contrats de professionnalisation

La recherche d'un contrat

- L'ENSIBS accompagne les candidats admis dans leurs recherches de contrats en les mettant en relation avec des entreprises partenaires
- Le recrutement d'un alternant (contrat d'apprentissage ou contrat de professionnalisation) nécessite la signature d'un contrat de travail entre l'alternant et l'entreprise employeur. L'alternant devient alors salarié à part entière de cette entreprise.
- Ce contrat engage l'alternant à travailler pour l'entreprise employeur lors des périodes prévues en entreprise et à suivre la formation à l'école et à passer les examens lors des périodes prévues à l'école.
- Une journée de formation à l'alternance est proposée aux apprentis admis en première année de cycle ingénieur afin de les aider dans leurs recherches et leur transmettre des conseils pour décrocher un contrat d'apprentissage

Le suivi du contrat

- Dans le cadre du contrat d'apprentissage, un maître d'apprentissage, ingénieur confirmé de l'entreprise d'accueil, participe à la formation de l'apprenti lors des périodes en entreprise en lui confiant des missions en relation avec la formation. Un tuteur pédagogique, enseignant au sein de l'école, suit l'évolution de l'apprenti pendant toute sa formation en lien avec le maître d'apprentissage.
 - Dans le cadre du contrat de professionnalisation, un tuteur peut être également désigné.
- Les candidats de nationalité étrangère**, non ressortissants de l'Union Européenne, devront fournir une Autorisation Provisoire de Travail (APT) portant la mention étudiant en apprentissage.

La rémunération

Contrat d'apprentissage

	18-20 ans	21-25 ans
1 ^{ère} année	41%	53%
2 nd année	49%	61%
3 ^{ème} année	65%	78%

Rémunération

d'un alternant

(en % du SMIC ou SMC)

Contrat de professionnalisation

	< 21 ans	21-25ans	> 26 ans
1 an	65%	80%	SMIC ou 85% du SMIC