École d'ingénieurs

ensibs :

Université Bretagne Sud

Devenez ingénieur en cyberdéfense

par l'alternance

Portes ouvertes

2 fev. 2019

FORMATION ACCRÉDITÉE PAR LA COMMISSION DES TITRES D'INGÉNIEUR

UIMM Pôle formation Bretagne – La fabrique de l'avenir

itii Bretagne

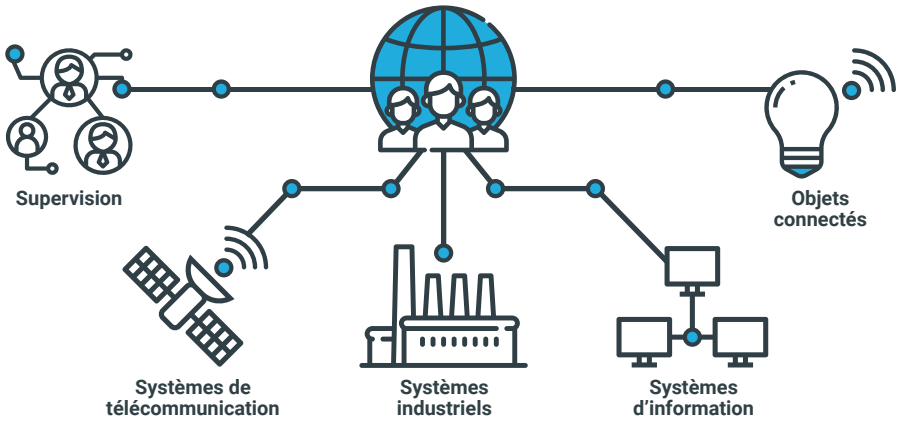
Cti Commission des titres d'ingénieur

SecNumedu ANSSI

www.ensibs.fr

Les contexte de la cyberdéfense

Assurer en permanence la sécurite des systèmes des Opérateurs d'Importance Vitale (OIV) et des entreprises est l'enjeu fondamental de la Cyberdéfense.



/ Le patrimoine français à Cyber défendre

• **218 Opérateurs d'Importance Vitale (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 cyberespace
• Vulnérabilité de nos infrastructures vitales interconnectées à grande échelle

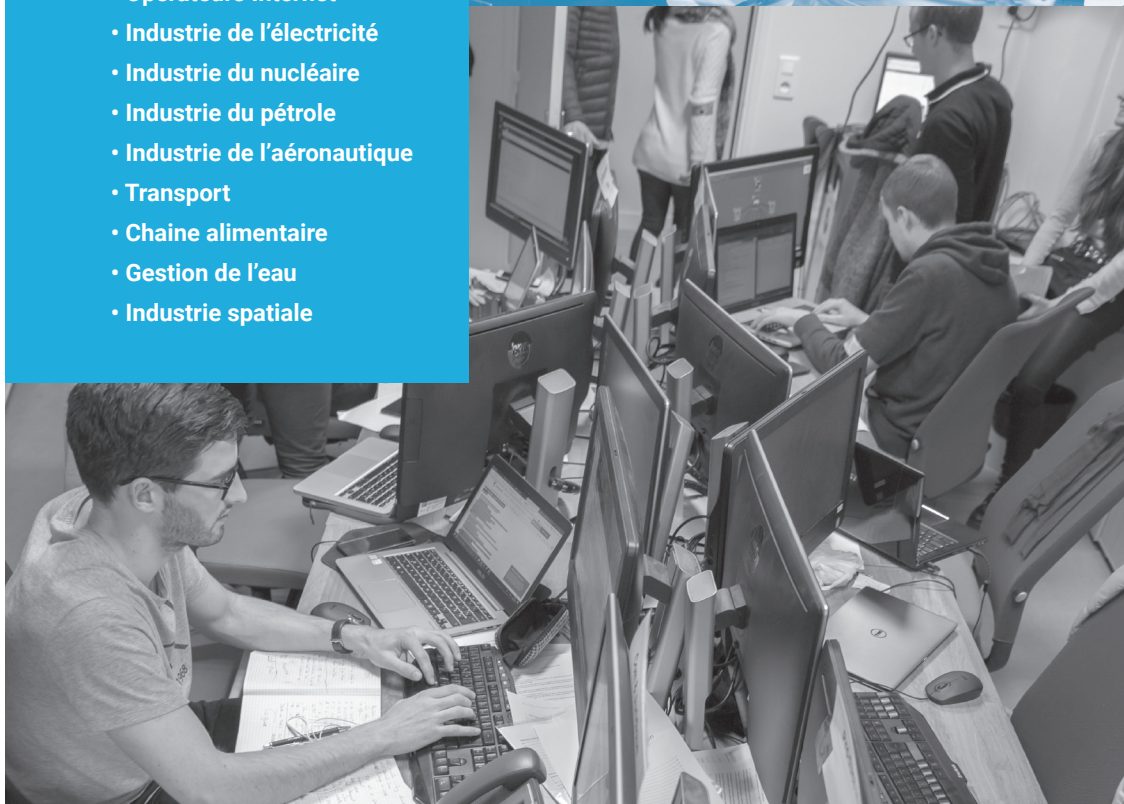
/ Enjeu de maîtrise de la Cybercriminalité

• 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.

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



Les besoins des professionnels

Une formation d'ingénieurs :

/ Accréditée par la Commission des Titres d'Ingénieur qui atteste la qualité de la formation
/ Labellisée par l'Agence Nationale de la Sécurité des Systèmes d'Information

Pour répondre à l'urgence des besoins de formation des entreprises françaises publiques et privées et pour constituer un réel vivier d'emplois, l'ENSIBS a créé la première formation française d'ingénieurs universitaire en cyberdéfense.

/ Besoins des entreprises

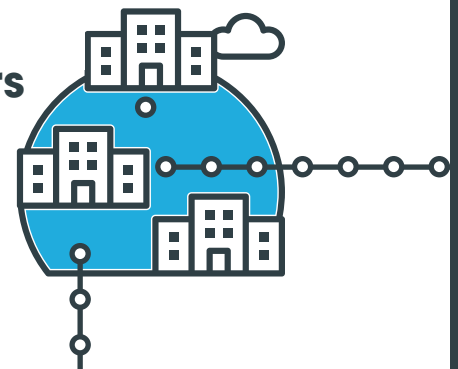
Les entreprises publiques et privées ont été consultées et ont un besoin important de professionnels capables de :
• comprendre la menace et les modes opératoires des attaquants dans une approche système,
• construire la sécurité des infrastructures dans une approche globale pour mieux se protéger (architecte cyberdéfense),
• gérer des crises cybernétiques quelle que soit leur ampleur.

/ Secteur d'avenir

Les entreprises ont peu de personnels formés spécifiquement aux métiers de la cyberdéfense, 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 cyberdéfense : 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...).

1000 ingénieurs par an*

** 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).*



Témoignages
La parole aux professionnels

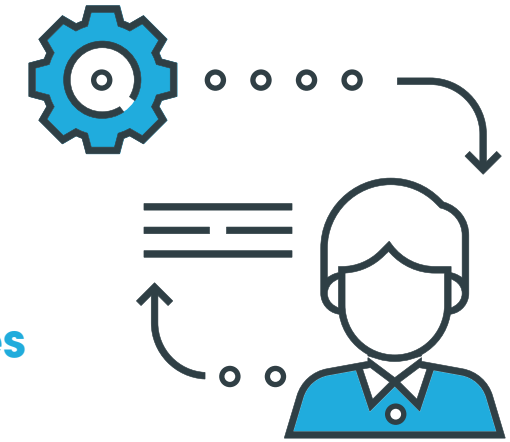
Le développement du numérique représente un changement complet de société. La cybersécurité se retrouve, de facto, au centre des nouvelles préoccupations des acteurs économiques (Etats, entreprises, citoyens). Pour répondre à ces nouveaux défis, les besoins en recrutement d'AMOSSYS sont importants : que ce soit des experts techniques mais aussi des consultants capables d'accompagner nos clients dans la sécurisation de leur espace numérique ou des personnes capables de manager et d'avoir une vision plus large de la filière cybersécurité.
Christophe Dupas,
Amossys
Président

Les entreprises membres du Pôle d'excellence cyber, les OIV et les PME/PMI innovantes n'arrivent pas à combler leurs besoins RH en profils très techniques, formés aux dernières innovations technologiques et techniques : architecte de sécurité, analyste SOC, spécialiste de gestion de crise cyber, responsable de la continuité d'activité, analyste forensic, ... L'ENSIBS a créé un diplôme pour répondre aux besoins critiques de ces organisations.
Patrick Erard,
Pôle d'excellence cyber
Délégué général adjoint

Orange a des besoins importants dans diverses entités du Groupe, en particulier sur les bassins Bretagne et Ile de France. Les métiers sont variés et la liste n'est pas exhaustive : Ingénieur Cybersécurité, Architecte en sécurité, Analyste Soc, Expert sécurité (cloud, SI, réseau, infra mobile, etc), Concepteur Solutions de Sécurité, Auditeur Sécurité, Consultant Sécurité, Ingénieur sécurité IOT, RSSI, ...
Pascal Duffy & Coralie Lefevbre,
Orange
Ressources humaines

Les entreprises recherchent des ingénieurs dans des métiers très divers : de l'amont des projets (architectes sécurité, consultants en sécurité) à l'aval des projets (audits, tests de sécurité, opérateurs de SOC, administrateurs de sécurité) en passant par le développement de produits de sécurité. L'étendue des techniques en jeu n'a pas de limite : objets connectés, systèmes de commande industriels, smartphones, etc. sont aussi des cibles. Pas de souci à se faire quant à l'avenir de ces métiers, puisque le rythme des attaques ne fait - malheureusement - qu'augmenter année après année.
Jean-Luc Gibernon,
Sopra Steria
Directeur
BU Défense & Sécurité

Naval Group est systémier, concepteur intégrateur de la capacité de cybersécurité. Pour répondre toujours plus efficacement aux attentes de nos clients, nos besoins de recrutement en experts en cyberdéfense sont très importants.
Laurent Comte,
Naval Group
Directeur Domaine Technique



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 cyberespace

• Définir une politique de sécurité

/ Construire la sécurité

• 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 œuvre un ensemble de solutions de sécurité.
• Concevoir, réaliser et mettre en oeuvre la protection des systèmes des Opérateurs d'Importance Vitale (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 cyberdéfense.
• 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

Témoignages **La parole aux entreprises partenaires**

La cyberdéfense, en plus de compétences techniques avérées, fait appel à des compétences humaines : sens de l'engagement, respect de la confidentialité, honnêteté. Techniquement, des compétences en développement, en reverse ou tests d'intrusion peuvent être utiles, mais tout dépend du type de poste occupé. Chez AMOSSYS par exemple, la maîtrise de vulnérabilités web est incontournable pour faire de l'audit, tout comme la connaissance de référentiels (ISO 27001, LPM, etc.) peut l'être pour être consultant.
Christophe Dupas,
Amossys
Président

Travailler dans la cyberdéfense requiert certes des qualités d'ingénieur, telle la capacité à modéliser des systèmes complexes, à mettre régulièrement ses connaissances et compétences à jour, ... mais aussi des compétences humaines essentielles, telles : l'humilité, la gestion du stress, la capacité à travailler en équipe et à prendre du recul face à un environnement compliqué, à partager les informations pertinentes tout en restant discret, à faire preuve de réserve, avoir l'envie du travail bien fait et du service rendu.
Patrick Erard,
Pôle d'excellence cyber
Délégué général adjoint

Au-delà de la technique, le savoir être et globalement les compétences transverses inhérentes au métier d'Ingénieur dans un Groupe international sont recherchées : engagement, résilience, résistance, qualités relationnelles, sens de l'éthique, curiosité et ouverture au monde...
Sur le plan technique, les compétences en matière de déploiement d'outils de sécurité de Cyberdéfense dans les domaines DETECTION de la menace et REACTION aux incidents sont nécessaires pour opérer dans les métiers de lutte informatique défensive des entreprises.
Eric Dupuy,
Orange CyberDefense
Directeur régional grand ouest

Je conseille toujours aux jeunes diplômés de ne pas s'enfermer dans un unique métier donné. Adoptez des parcours riches et variés, le monde de la cybersécurité vous permettra de varier les plaisirs, alors ne vous en privez pas ! La curiosité (qui est tout le contraire d'un vilain défaut, en vérité) et l'ouverture d'esprit sont des « must have ».
Jean-Luc Gibernon,
Sopra Steria
Directeur BU Défense & Sécurité

La répartition des enseignements

1ère année — Bases

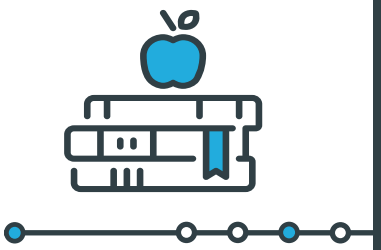
Tronc commun en sciences pour l'Ingénieur	600 h
Sciences économiques et de gestion	60h
Anglais	60h
Mathématiques	100h
Base en sécurité Base de l'électronique	50h
Programmation	100h
Ingénierie des systèmes	55h
Architecture et systèmes de base	55h
Projet ingénierie système	20h
Séminaires de gestion de crise - DTF - Ethique	100h

2ème année — Sécuriser

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

3ème année — Défendre

Management et Ingénierie de sécurité des systèmes	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
Evaluation de la résistance des systèmes	50h
Connaissance du contexte professionnel et ouverture internationale	25h
Sciences économiques et de gestion et langues	50h
Majeures en cybersécurité	60h
Exercice de gestion de crise (cyberdéfense d'un opérateur vital)	200h



Témoignages
La parole aux intervenants - experts

Depuis sa création, AMOSSYS s'investit dans la formation en cyberdéfense de l'ENSIBS. Participer aux enseignements délivrés par l'ENSIBS permet bien évidemment à AMOSSYS de se faire connaître auprès de futures recrues, de pouvoir repérer les talents, de former de futurs ingénieurs aux postes que nous proposons mais également de confronter nos consultants au public exigeant des étudiants.

Christophe Dupas,
Amossys
Président

En tant que professionnel de la sécurité, dispenser des enseignements sur la sécurité des réseaux permet de donner une vision opérationnelle, terrain et pratique aux étudiants en complément des bases théoriques.
C'est mutuellement enrichissant de pouvoir enseigner à des étudiants des techniques de sécurité et aussi d'être questionné par ces étudiants qui ont leurs 1ères expériences dans de multiples entreprises. Cela s'inscrit pleinement dans l'esprit de curiosité, de challenge et de remise en question perpétuels si spécifique à la sécurité.
Dans un environnement où les compétences sont rares et recherchées, cela permet également d'avoir une visibilité sur des talents d'avenir.

A Martin,
Orange
Intervenant en « sécurité des réseaux »

Les ingénieurs que nous formons à l'ENSIBS devront faire face à des menaces en constante évolution dans un monde hyper-connecté. Le spectre des compétences nécessaires pour en appréhender les rouages est large, allant de la micro-électronique aux sciences humaines.
Dans ce contexte, et en tant que chercheur, il me tient à cœur de développer la curiosité de nos apprentis-ingénieurs pour les thématiques scientifiques et les technologies émergentes, afin de leur permettre de construire une vue à moyen et long terme de la sécurité.
De plus, cette formation en apprentissage facilite, par construction, la création de nouvelles relations entre le monde de la recherche académique et celui de l'entreprise. Cette spécificité, en favorisant les échanges, participe pleinement à l'identification des verrous scientifiques de demain dans le domaine de la sécurité.

Vianney Lapôtre,
ENSIBS
Maître de conférences

Acquisition de compétences techniques pointues et variées dans le domaine de la SSI (sécurité des systèmes d'information) de la gestion de crise, du management des risques, du droit… Tout ceci pour pouvoir mettre en œuvre une défense efficace pour une entreprise ou une administration.

Arnaud,
ENSIBS
Apprenti ingénieur

Votre voie d'accès

Vous venez de	Mode de candidature	Niveau d'entrée à l'ENSIBS	Places
BAC + 2 : DUT Info, DUT R&T, DUT GEII, BTS Informatique ou Réseaux, PEI ENSIBS, CPGE.	**www.ensibs.fr >** Rubrique Admissions Dossier + entretien	✔ Vous intégrez le cycle ingénieur de 3 ans	55
BAC + 3 : L3 Informatique	**www.ensibs.fr >** Rubrique Admissions Dossier + entretien	✔ Vous intégrez le cycle ingénieur de 3 ans	
BAC + 4, Master 1	**www.ensibs.fr >** Rubrique Admissions Dossier + entretien	✔ Vous entrez en 2ème année du cycle ingénieur	1
VAE, VAP	Procédure sur dossier	✔ Contacter le service de formation continue : formation.continue@univ-ubs.fr Tél. 02 97 87 11 30	

Autres conditions requises :
• Etre âgé de 30 ans maximum à la date de début du contrat
• 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

Les prérequis

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

Témoignages
La parole aux apprentis étudiants

Comment avez-vous connu la formation ?

Nanding : Intervention de l'ENSIBS au sein de mon IUT.
Louis : Suite à des recherches sur Internet et un salon étudiant.
Arnaud : Site Internet de l'Ecole, vidéos sur youtube et JPO.
Dylan : Information au sein de mon IUT par des anciens ayant intégrés la formation Ingénieur Cyberdéfense.

Quelle formation et quel niveau aviez-vous avant d'intégrer la formation Ingénieur Cyberdéfense ?

Maude : Suite à un BAC STI2D, j'ai fait un BTS SN IR (ex IRIS) et ai terminé dans le top 3 de ma promo avec une moyenne générale de 16.
Arnaud : Après un BAC S moyen, j'ai fini major de promo de mon DUT R&T.
Nabila : BAC S au Maroc, puis DUT Informatique en France, j'ai fini dans les 10 premiers de la promo.
Louis : BAC STI2D, puis BTS SN IR (IRIS) et prépa ATS dans laquelle j'ai fini dans le 1er tiers de la promo.

Comment avez-vous préparé votre dossier de candidature ?

Louis : un conseil pour les futurs candidats : obtenir les meilleurs résultats dans toutes les disciplines !
François-Régis : j'ai valorisé dans mon CV un projet en bac STI2D qui m'a permis de décrocher mon contrat chez Siemens.
Nanding : quelques conseils pour les candidats :
- consulter la plaquette de la formation, s'informer sur le contenu des modules de la formation et poser des questions précises si nécessaire...,
- rechercher des informations sur la cybersécurité, les débouchés et les opportunités dans le domaine (site ANSSI...),
- faire preuve de curiosité et avoir la capacité d'apprendre et se remettre en question,
- comprendre les enjeux et défis de la cybersécurité pour l'Etat, les entreprises...

Dylan : s'investir dans la sécurité informatique, ceci peut être effectué via un stage de fin d'étude, mais aussi par la participation à des évènements liés au domaine : conférences, challenges... se documenter sur l'ANSSI, sur les dernières actualités dans le domaine.
Maude : aller à la JPO, s'informer en participant à des salons et conférences : HACK2G2 notamment ou via des sources spécialisées type MISC...
Arnaud : j'ai collecté des informations sur l'Ecole et la formation, le secteur d'activité et les entreprises y travaillant.

Calendrier d'admission

/ Novembre à février
Information sur la formation : salons étudiants, forums IUT, site de l'Ecole, veille dans le domaine, journée Portes Ouvertes à Vannes…

/ A partir de janvier
Dossier de candidature à demander en ligne sur le site de l'Ecole puis à télécharger.

/ 2 Février
Journée Portes Ouvertes de 9h à 17h bâtiment ENSIBS à Vannes.

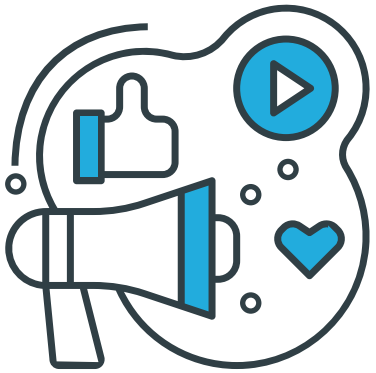
/ 28 Mars
Forum alternance de 14h à 17h :
Rencontre entre candidats et entreprises en cybersécurité (*inscription à partir de janvier sur le site de l'Ecole page Cyberdéfense*).

/ Avril
À compter du 15 avril, clôture des demandes de dossiers de candidature en ligne. Et envoi au plus tard au 20 avril *(le cachet de la Poste faisant foi)* **du dossier complet** (*et en particulier avec avis de poursuite d'études de l'établissement d'origine*) à :
ENSIBS Recrutement spécialité Cyberdéfense – rue Yves Mainguy BP 573 – 56017 Vannes Cedex
Fin Avril : commission pédagogique : sélection des candidats admissibles à l'oral.

/ 16 et 17 mai
Entretiens de motivation par les membres de l'équipe pédagogique et les entreprises partenaires. Les étudiants à l'étranger seront auditionnés à distance (*ils devront le mentionner dès le dossier de candidature dans leur CV*). Fin mai publication de la liste des admis.

/ Mai - Juin - Juillet
Accord et signature d'un contrat d'apprentissage de 3 ans avec une entreprise, dont le siège est en France, dans la limite des 55 places disponibles.

/ 2 Septembre
Début de la formation.



Témoignages **Processus de recrutement**

Orange est le partenaire majeur de l'école. Une trentaine d'offres sont proposées tous les ans avec des missions dans toute la France. Les collaborateurs d'Orange sont présents dans les jurys et s'appuient sur des questionnaires de personnalité pris en charge par Orange dans le cadre du partenariat. Nos équipes sont aussi mobilisées pour le forum alternance.
Pascal Duffy & Coralie Lefevbre,
Orange
Ressources humaines

La proximité entre l'ENSIBS et Sopra Steria nous amène à réaliser en commun les entretiens avec les candidats à l'entrée de la formation. Le croisement des avis des enseignants avec ceux des entreprises permet de sélectionner les meilleurs candidats et de tirer la formation Cyberdéfense de l'ENSIBS vers l'excellence.
Jean-Luc Gibernon,
Sopra Steria
Directeur BU Défense & Sécurité

Naval Group participe activement dans le processus de recrutement depuis plusieurs années. Cette démarche nous a permis de sélectionner chaque année des alternants de grande qualité.
Pierre-Yves Miton,
Naval Group
Recrutement domaine cybersécurité

Afin de faciliter la mise en relation entre les candidats et les entreprises, l'ENSIBS organise un FORUM ALTERNANCE en mars :
- les candidats y découvrent les postes et secteurs d'activité,
- les entreprises y rencontrent les différents profils et personnalités des candidats.

Jessica Morin-Chauvet,
ENSIBS
En charge du processus de recrutement

Comment avez-vous mis en avant votre motivation ?

Nanding : en valorisant les expériences professionnelles, humaines et transverses acquises tout au long de mon parcours (académique et personnel) et mettre en avant mon potentiel humain, relationnel, éthique.
Dylan : je me suis présenté avec les tâches effectuées pendant mon apprentissage, j'ai donc pu mettre à profit mon expérience et montrer que je maitrisais ce que j'avais fait.
Louis : j'ai réalisé plusieurs entretiens blancs avec des proches, avec de nouvelles questions à chaque fois.

Comment avez-vous trouvé votre entreprise ?

Maude : j'ai postulé en candidat libre sur différents sites d'entreprise. Ayant reçu plusieurs réponses positives, j'ai choisi mon entreprise en fonction de mes affinités.
Arnaud : en apprentissage en 2ème année de DUT, j'ai consulté l'annuaire interne de mon entreprise et suis entré en contact avec les managers des services concernés.
François-Régis : grâce à la mise en relation de l'école avec les entreprises partenaires, j'ai été contacté par l'une d'entre elles qui a été intéressée par l'un de mes projets.

La répartition de la formation

22 semaines école + 30 semaines entreprise / an

1ère année

Septembre				Octobre				Novembre				Décembre				Janvier					Février			
36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	01	02	03	04	05	06	07	08	09
Mars				Avril				Mai				Juin				Juillet					Août				
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

2ème année

Septembre				Octobre				Novembre				Décembre				Janvier					Février			
36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	01	02	03	04	05	06	07	08	09
Mars				Avril				Mai				Juin				Juillet					Août				
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

3ème année

Septembre				Octobre				Novembre				Décembre				Janvier					Février			
36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	01	02	03	04	05	06	07	08	09
Mars				Avril				Mai				Juin				Juillet					Août				
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

Période de formation à l'école Période de formation en entreprise

> Période de 8 semaines obligatoires à l'international

Témoignages **L'alternance en entreprise**

L'apprentissage représente aujourd'hui pour l'étudiant LA solution dans son cursus de formation initiale. L'association entre parcours universitaire et formation professionnelle connaît aujourd'hui, et à juste titre, un succès croissant auprès des entreprises et des jeunes. Accueillir un étudiant en alternance permet à AMOSSYS de former et d'évaluer le potentiel de futurs collaborateurs sur le long terme. Notre politique de recrutement vise en effet l'embauche des étudiants à l'issue de leur alternance chez AMOSSYS.

Christophe Dupas,
Amossys
Président

Les apprentis ont cette chance de manipuler les SI des entreprises et des administrations dans lesquelles ils sont en alternance, ainsi que des logiciels qu'elles utilisent. L'apprenti est ainsi directement formé à son futur métier, il fait partie intégrante de la chaine de valeur de l'organisation.

Patrick Erard,
Pôle d'excellence cyber
Délégué général adjoint

L'apprentissage est la meilleure des voies pour se former à la cybersécurité, tout comme aux autres métiers de l'IT plus globalement. Nous intégrons pleinement nos alternants dans les équipes projet. En fin de formation, ils ressortent de l'ENSIBS avec, en plus de leur diplôme, une expérience technique et humaine riche de 3 années passées en entreprise.

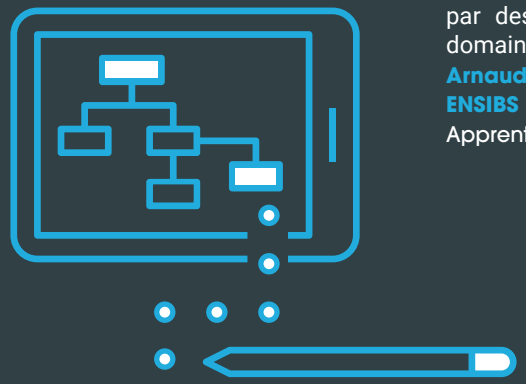
Jean-Luc Gibernon,
Sopra Steria
Directeur BU Défense & Sécurité

Pourquoi avoir fait le choix de celle formation en alternance ?

Louis : Seule école d'ingénieurs en alternance avec un parcours de 3 ans en Cyberdéfense.
Maude : Formation originale dans son contenu avec une approche globale de la Cyberdéfense via l'alternance : technique, gestion crise, droit, management, éthique…
Nabila : L'originalité des modalités d'apprentissage et d'alternance : séminaires de facteurs humains, conférences, projets, exercice de gestion de crise…
Nanding : L'apprentissage : une formule win-win pour les 3 parties : apprenti, entreprise, école et une formation en adéquation avec l'entreprise.
Arnaud : À mes yeux l'alternance représentait une double formation, adaptée au besoin de l'entreprise, ainsi qu'une autonomie financière, nécessaire à la poursuite de mes études.

Partenariat entre l'ENSIBS et l'IEP de Rennes

L'IEP de Rennes et l'ENSIBS se sont associés pour pouvoir permettre à certains diplômés de la spécialité Cyberdéfense de poursuivre leurs études au sein du Master 2 en Sécurité, Défense et Intelligence Stratégique.
Il s'agit d'un master unique dans la région du Grand Ouest sur une approche pluridisciplinaire à dominante juridique de l'intelligence stratégique en sécurité et en défense intégrant les dimensions nationale et internationale du sujet.



« Une des grandes opportunités, fournie par l'ENSIBS, a été la réalisation d'un Master 2 en Sécurité, Défense et Intelligence Stratégique avec Sciences Po et l'École Normale Supérieure de Rennes.
Avec ce Master j'ai saisi une dimension supérieure de la Cyberdéfense.
Les enseignements dispensés étant variés et uniques en France ils m'ont permis de connaître spécifiquement le secteur de la Défense. J'ai ainsi acquis de solides bases en Droit (de l'Union Européenne, des Conflits armés, de la Défense), Histoire des Relations Internationales, Géopolitique, Gestion des Crises, Programmes d'Armements, etc. Tous ces cours sont dispensés par des intervenants experts de leur domaine et sont donc passionnants. »

Arnaud,
ENSIBS
Apprenti étudiant

L'ENSIBS, co-fondatrice du « Parcours ITII Entreprendre »

Première formation en France adaptée aux problématiques de formation en apprentissage et à la volonté d'entreprendre.

« De l'initiation lors de la 1ère année à la création réelle en fin de formation, c'est tout un dispositif de sensibilisation, de formation et d'accompagnement à l'entrepreneuriat qui est proposé à toutes les écoles d'ingénieurs adhérentes à ITII Bretagne.
En première année, les apprentis assistent au colloque « Passion d'entreprendre » où un « grand témoin » et les diplômés-créateurs viennent témoigner de leur parcours. Mais pas seulement… Ils participent également à un défi de créativité « objet du futur ».
La deuxième année est le cœur de la formation, elle permet à chaque apprenti de tester ses capacités entrepreneuriales et de faire le point sur lui-même autant que sur son projet.
Et après ?
Armé d'un business plan, il est possible à l'apprenti de participer aux nombreux concours régionaux et nationaux sur l'entrepreneuriat et ainsi d'obtenir ses premiers financements.
Le statut national étudiant entrepreneur lui est accessible avec un accompagnement par des coaches professionnels pour finaliser la maturation du projet. »

Agnès Jumbou
ENSIBS
Enseignante et référente entreprenariat

« Étant bien classé au sein de ma promotion, j'ai pu voir de nouvelles opportunités s'offrir à moi. Durant 6 mois j'ai travaillé avec un groupe de projet composé d'étudiants de l'ENSIBS, ainsi qu'avec des étudiants de la fac de droit de Lorient à la création d'une plateforme de sport collaboratif et de l'entreprise associée. Cette expérience, en dehors du cadre conventionnel de la Cyberdéfense, m'a permis de maîtriser l'ensemble du processus de création d'entreprise, de l'idée à la création des statuts, en passant par l'étude du marché, la rédaction du business plan et le pitch de son projet devant des investisseurs.»

Arnaud,
ENSIBS
Apprenti ingénieur

« Je tiens à remercier l'ENSIBS et plus particulièrement Agnès Jumbou pour son accompagnement dans le cadre de mes projets entrepreneuriaux.
Ce cursus accompagné d'un suivi adapté, permet d'acquérir les bases dans la création d'entreprise mais également de fournir une première sensibilisation quant à l'esprit d'entreprendre. »

Max,
ENSIBS
Apprenti ingénieur

Campus ENSIBS

Vannes - Paris
Train : 2 h 40 min
Avion (Lorient) : 1 h 25 min

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...). Découvrez aussi les associations de l'ENSIBS :

/ Le Bureau des élèves
Toute l'année le BDE organise de nombreux événements qui rythment la vie étudiante à l'ENSIBS. Il favorise les échanges entre ses membres, les étudiants et les partenaires.
En savoir plus + : bde.ensibs@gmail.com

/ ViewUp
L'association professionalisante étudiante de type Junior-Entreprise de l'ENSIBS, permet aux étudiants de mettre en pratique leur formation en répondant aux besoins de clients au travers d'études d'ingénierie rémunérées.
En savoir plus + : www.viewup.fr

/ Hack2G2
Association commune à l'ENSIBS et à l'IUT de Vannes, elle rassemble chaque semaine des étudiants, qui partagent leurs connaissances lors de présentations et ateliers.
Bien que majoritairement tournés vers la sécurité informatique, tous les sujets peuvent être abordés et les étudiants en quête de partage sont plus que bienvenus !
En savoir plus + : www.hack2g2.fr

Notre écosystème

Le Cyber Security Center centre de formation, d'entrainement et de recherche en gestion de crise cybernétique.

/ Le Cyber Security Center en bref

• Dès 2012, l'UBS a investi avec détermination le champ de la cybersécurité : précurseur et leader, elle est l'une des rares universités à proposer une offre aussi complète dans ce domaine crucial pour l'avenir.
• Cette énergie fondatrice lui permet de garder un temps d'avance dans le domaine de la formation, de la recherche (fédération de plusieurs laboratoires) et dans le développement d'une plateforme technique de simulation et de gestion de crises cyber.
• Avec nos partenaires industriels et étatiques, les étudiants sont capables de mettre en place et contribuer à la cyberdéfense des entreprises, de sécuriser les applications et les architectures logicielles et de sécuriser les systèmes embarqués.
• Au profit de la recherche et de la formation, la plateforme technique peut générer des *use case* et bénéficie d'outils de détection, d'analyse et de remédiation.

/ Le Cyber Security Center regroupe 4 compétences

Formation
Former des ingénieurs en cyberdéfense et en informatique de confiance (ENSIBS), des techniciens en cyberdéfense et développement sécurisé (IUT de Vannes), des experts en cybersécurité des systèmes embarqués (UFR SSI).

Entraînement
Former et entraîner à la gestion de crises cybernétiques au sein du Cyber Security Center.

Sensibilisation
Sensibiliser les PME-PMI aux cyber menaces.

Recherche
Mener une R&D opérationnelle avec des programmes de recherche pluridisciplinaire.

L'enjeu est important : dans les années qui viennent, l'UBS poursuivra le développement de ses compétences et de son offre en cyber, notamment en formation continue. L'UBS travaillera avec les différents acteurs pour lutter contre la cybermenace.
cybersecuritycenter.univ-ubs.fr

/ Les partenaires de notre ecosystème Cybersécurité

Focus

L'originalité de la spécialité Cyberdéfense de l'ENSIBS

/ Séminaires « Facteurs Humains »

« Le but de ces séminaires est de développer les compétences humaines de nos apprentis : connaissance de soi, relation aux autres, gestion de son stress et de sa fatigue, prise de décision en situation inhabituelle,...
Ces compétences sont essentielles à la formation d'un ingénieur en Cyberdéfense ! »

Laurent Marot
ENSIBS
Enseignant

/ Exercice de gestion de crise

« Cet exercice de 15 jours est le cœur de la formation. Il se déroule en fin de 3ème année et consiste en la défense d'un OIV contre des attaques sur son système d'information.
Le scénario est construit en collaboration avec une entreprise partenaire afin de pouvoir simuler des situations réelles.
Les compétences mises en jeu sont pluri-disciplinaires : compétences techniques, organisationnelles, législatives, ... et bien sûr la gestion du stress !
C'est pour ça qu'il arrive en fin de cursus car c'est un condensé des 3 ans de formation ! »

Laurent Marot
ENSIBS
Enseignant

Que sont-ils devenus ?

/ Nabila
Entreprise d'apprentissage : Orange (Rennes)
Entreprise actuelle : **Orange Cyberdéfense (Rennes)**
Intitulé du poste : **Analyste CyberSOC**
Ses missions : réponse aux incidents de sécurité et amélioration continue de l'environnement CYBERSOC

/ Louis
Entreprise d'apprentissage : Securiview (Paris)
Entreprise actuelle : **Securiview**
Intitulé du poste : **Ingénieur sécurité**
Ses missions : créer et développer une offre technique et commerciale pour sécuriser le cloud et mener des investigations numériques pour corriger les vulnérabilités

/ François-Régis
Entreprise d'apprentissage : Siemens (Lyon)
Entreprise actuelle : **Siemens**
Intitulé du poste : **Ingénieur Cybersécurité**
Ses missions : conseil d'architecture sécurisée, installation d'équipements de cybersécurité, développement de nouveaux services de cybersécurité.

/ Maude
Entreprise d'apprentissage : Naval Group (Brest)
Entreprise actuelle : **Naval Group**
Intitulé du poste : **Ingénieur Cybersécurité**
Ses missions : très variées dont le maintien en Condition de cybersécurité des produits vendus par le groupe.

/ Arnaud
Entreprise d'apprentissage : Orange
Entreprise actuelle : **Ministère (Paris)**
Intitulé du poste : **Ingénieur en Cyber Threat Intelligence**
Ses missions : identifier les attaques visant l'Etat, analyser les modes opératoires et les cibles visés pour les mettre en lien avec la politique française (en France et à l'étranger), ainsi qu'avec la géopolitique mondiale.

/ Nanding
Entreprise d'apprentissage : EDF (Paris)
Entreprise actuelle : **EDF**
Intitulé du poste : **Ingénieur R&D**
Ses missions : conception technique de solutions de sécurité, appui et pilotage de projets R&D en cybersécurité, réalisation d'études de risques et de surveillance, étude de normalisation…

/ Dylan
Entreprise d'apprentissage : Amossys (Rennes)
Entreprise actuelle : **Amossys**
Intitulé du poste : **Auditeur en cybersécurité**
Ses missions : tests d'intrusions web ou interne à des systèmes d'information, audit de code ou de configuration, chez divers clients : du monde de la défense en passant par l'industrie ou encore la santé.

/ Contacts

La formation en vidéos

ENSIBS spécialité Cyberdéfense
Site de Vannes
rue Yves Mainguy BP 573
56017 VANNES CEDEX

02 97 01 72 70
ensibs.cyberdefense@univ-ubs.fr
www.ensibs.fr

Nous remercions l'ensemble de nos partenaires : experts, entreprises et institutionnels... pour leur implication dans la formation « Ingénieur en Cyberdéfense » et leurs témoignages dans cette plaquette.
Nous remercions également chaleureusement :
/ **Nanding «Promo Nokia»** 2013-2016,
/ **Arnaud « Promo Orange »** 2014-2017,
/ **Maude, Nabila, Dylan, François-Régis, Louis, « Promo Sopra Steria »** 2015-2018,
/ **Max « Promo Orange Cyberdéfense »** 2016-2019,
d'avoir fait partager leurs expériences aux futurs candidats et présenter leurs activités d'Ingénieurs en Cyberdéfense.

Création : twins communication | twins.bzh | 0671435573 - Charte graphique couverture : Jennifer Cornic - Octobre 2018

Nos partenaires