Brest MÉTROPOLE

BRETAGNE

BREST, NATURELLEMENT À LA POINTE DE LA CYBERSÉCURITÉ MARITIME

BREST LIFE

SOMMAIRE

“La cybersécurité est un sujet central en région Bretagne depuis 2013. La présence de fonctions stratégiques liées à la Défense et d'acteurs économiques et académiques a contribué à accroître l'ancrage de cette thématique sur Brest et sa métropole. Aujourd'hui, la cybersécurité est clairement identifiée pour nous tous comme un domaine d'activité à fort potentiel dans le cadre de la nouvelle stratégie métropolitaine de développement économique « Cap 2030 » adoptée par notre territoire en juin dernier. Ici, nous entendons encourager les acteurs de la cybersécurité à se constituer en cluster pour promouvoir et développer l'ensemble de la chaîne de valeur : recherche, transfert de technologies, formation, développement de solutions, offre de service aux entreprises.”

FRANÇOIS CUILLANDRE
PRÉSIDENT DE BREST MÉTROPOLE

Un monde en pleine mutation, des enjeux de cybersécurité et Brest en première ligne.

Dans un monde où la place du numérique est prépondérante, aucun secteur d'activité n'est désormais épargné par le risque de cyberattaques de plus en plus élaborées et pouvant avoir de lourdes conséquences.

Avec la présence d'une grande route maritime mondiale à proximité, Brest est aux premières loges des enjeux de la croissance du trafic maritime et des vulnérabilités liées à la numérisation sans précédent des ports, navires et infrastructures maritimes de tout genre.

Et si la métropole brestoise affirme aujourd'hui son expertise notamment en matière de cybersécurité maritime, c'est parce qu'elle rassemble toutes les composantes des enjeux du monde maritime :

- **Un port unique** concentrant des fonctions maritimes internationales de premier plan.
- **Un port militaire** majeur accueillant la base opérationnelle de la force océanique stratégique et une partie des forces navales de surface de la France.
- **Un port civil** de premier plan en matière de réparation navale et significatif sur les autres activités commerciales (vrac agroalimentaire, containers, hydrocarbures…) et au fort potentiel sur le développement des énergies marines renouvelables.
- **La Préfecture maritime de Brest** qui assure en permanence l'action de l'État en mer, notamment pour le contrôle et la sécurité du trafic en Atlantique et aux abords de la Manche.
- **Le siège national du Service Hydrographique et Océanographique de la Marine (SHOM)**, opérateur public pour l'information géographique maritime et littorale de référence des marines civiles et militaires.
- **Le Centre d'Études et d'Expertise sur les Risques, l'Environnement, la Mobilité et l'Aménagement (CEREMA)**, qui développe depuis Brest des relations étroites avec les collectivités territoriales.
- **Le siège national de l'Institut français de recherche pour l'exploitation de la mer (IFREMER)**, première place nationale en matière de recherche en sciences et technologies de la mer.

À BREST, NOUS SOMMES À LA POINTE DE LA CYBERSÉCURITÉ MARITIME

BREST, UNE EXPERTISE RECONNUE EN CYBERSÉCURITÉ MARITIME

Depuis plusieurs années, la métropole brestoise développe son expertise en cybersécurité maritime, civile et militaire, grâce à un écosystème dynamique composé d'acteurs académiques, industriels et militaires.

Aux côtés des « pure players » de la cybersécurité, les thématiques adressées concernent les drones, le spatial, la détection et les communications sous-marines, les capteurs, les données marines, l'interface homme-machine, le droit de la cybersécurité…

Cette capacité du territoire à mobiliser des approches pluri-thématiques et multidimensionnelles est un atout incontestable pour contribuer à répondre aux attentes de la communauté maritime et portuaire sur les questions de cybersécurité maritime, dans un contexte de numérisation accrue des infrastructures maritimes, de développement des drones et navires autonomes et d'augmentation des menaces cyber pesant sur ce secteur stratégique.

L'accueil, à Brest du siège de l'association nationale France Cyber Maritime (FCM), créée fin 2020 en application d'une mesure du Comité Interministériel de la Mer (CIMER), est un marqueur fort de reconnaissance des compétences présentes sur notre territoire.

Aujourd'hui, la cybersécurité, non exclusivement maritime, est clairement identifiée comme un domaine d'activité à fort potentiel dans le cadre de la nouvelle stratégie métropolitaine de développement économique de la métropole brestoise « Cap 2030 » adoptée en juin dernier.

LES PARTENAIRES SPÉCIALISÉS DU TERRITOIRE

Un concentré remarquable d'acteurs industriels tels que Naval Group, Thales, Brittany Ferries, Port de Brest, DIATEAM, Asten, CLS, IoT.bzh, Eodyn, Ellidiss, ECA… font face au quotidien aux menaces cyber dans l'exercice de leur métier maritime ou produisent des solutions de protection contre les menaces cyber.

LE MINISTÈRE DES ARMÉES

La Préfecture maritime de l'Atlantique accueille le MICA-Center (Maritime Information Cooperation and Awareness Center), centre de surveillance du trafic maritime mondial qui assure une veille permanente de la situation sécuritaire maritime. La base navale de Brest, quant à elle, accueille le Centre support cyberdéfense de la Marine nationale (CSC), une unité de la Marine spécialisée dans les questions de cyberdéfense.

LES LABORATOIRES DE RECHERCHE PUBLICS

Il existe sur le territoire plusieurs laboratoires spécialisés dans le domaine de la cybersécurité : le Lab-STICC, l'Institut de recherche de l'École navale (IRENav), le L@bisen et le Centre Européen de Réalité Virtuelle (CERV), qui couvrent un large spectre thématique : drones et robotique, conception et maintenance de navire, « security by design », simulation, entraînement, formation, communication, signaux, antennes, traitement de l'information et de l'image. Ces laboratoires s'appuient sur des infrastructures de recherche, équipements et plateformes performants : centre de données Datarmor, moyens d'essais en mer…

Au travers de différents projets, le Contrat de plan État-Région (CPER) 21-27, permettra de développer et consolider la recherche et l'innovation dans le domaine de la cybersécurité appliquée aux systèmes maritimes (navire autonome, robotique, réseaux de capteurs) et d'accroître les capacités de test de petits satellites, drones et multi-drones multi-milieux.

LE LAB-STICC

Ce laboratoire breton des Sciences et Techniques de l'Information, de la Communication et de la Connaissance est présent sur les villes de Brest, Quimper, Lorient et Vannes. Le Lab-STICC est sous tutelle de six établissements : IMT Atlantique, ENSTA Bretagne, UBO, UBS, ENIB et CNRS.

Le laboratoire développe une très forte expertise en cybersécurité. Il possède un large spectre de compétences en lien avec les enjeux de cybersécurité dans les domaines des architectures logicielles et matérielles, des communications et des réseaux, des systèmes critiques et des risques liés au facteur humain.
Sept équipes contribuent au programme transverse cyber et développent des contributions complémentaires.

LES CHAIRES INDUSTRIELLES

Elles complètent l'effort de recherche en liaison étroite avec les acteurs économiques : la chaire industrielle de cyberdéfense des systèmes navals (domaines civil et militaire) associant l'École navale, IMT Atlantique, ENSTA Bretagne et soutenue par Thales et Naval Group, la chaire Sécurité des Objets Connectés et la chaire Transnum dédiée aux systèmes d'observation marins autonomes (Thales, ENSTA Bretagne, ISEN Yncréa Ouest).

LA CHAIRE DE CYBERDÉFENSE DES SYSTÈMES NAVALS

Depuis 2014, l'École navale, IMT Atlantique, Thales, Naval Group et l'ENSTA Bretagne ont mis en place la Chaire de cyberdéfense des systèmes navals avec le soutien de la Région Bretagne et du Pôle d'Excellence Cyber.

Cette Chaire poursuit deux objectifs principaux : développer une expertise de formation et intensifier la recherche scientifique dédiée à la cybersécurité des systèmes maritimes et portuaires.
Les thématiques scientifiques sont les suivantes :

- la protection des informations sensibles embarquées,
- l'analyse de la fiabilité et de l'intégrité des informations collectées par les capteurs,
- l'analyse des failles de sécurité et intrusions,
- le déploiement de correctifs logiciels ou réaction au rétablissement de la sécurité des systèmes,
- l'aide à la prise de décisions en situations critiques.

Les compétences et savoir-faire présents au sein de la chaire participent à la formation scientifique des élèves officiers de l'École navale dans les domaines suivants : informatique, cybersécurité, réseaux, intelligence artificielle ainsi que par des exercices de mise en pratique d'incidents et de crises cyber grâce notamment au cyber range maritime.

Quelques chiffres concernant la chaire :

- Environ 10 enseignants-chercheurs des écoles partenaires actifs dans la chaire (École navale, IMT Atlantique et ENSTA Bretagne),
- Environ 10 ingénieurs-tuteurs des partenaires industriels impliqués dans le cadre des doctorats,
- 9 docteurs diplômés,
- 5 thèses en cours,
- 1 coordinateur,
- 1 informaticien spécialiste des systèmes industriels,
- 1 responsable communication.

Un projet soutenu par la Marine nationale, la Région Bretagne et le Pôle d'Excellence Cyber.

LE PÔLE D'EXCELLENCE CYBER

Initié en 2014 par le ministère des Armées et par la Région Bretagne, le Pôle d'excellence cyber a pour mission de stimuler la recherche, la formation et l'innovation dans le domaine de la cybersécurité et de la cyberdéfense. Il s'appuie sur le tissu académique et industriel régional ainsi que sur des partenaires nationaux ou d'autres territoires.

UNE DYNAMIQUE TERRITORIALE

Des dynamiques d'animation du territoire métropolitain brestois stimulent la création d'activités innovantes dans les entreprises : le Technopôle Brest-Iroise autour du Campus mondial de la mer et de la Capitale French Tech Brest+, le Pôle Mer Bretagne Atlantique, le Village by CA Finistère, la conférence de cybersécurité Unlock Your Brain Harden Your System ou encore le cluster d'innovation ORION initié par la direction générale de l'armement et le centre d'expertise des programmes navals de la marine.

© Pierre-François Watras/Brest métropole

FOCUS SUR L'EDIH BRETAGNE

En réponse à un appel à projets européen pour la constitution d'un réseau de European Digital Innovation Hubs (EDIH), la Bretagne a été retenue sur son projet de EDIH spécialisé dans le domaine de la cybersécurité.

La Région Bretagne se positionne comme l'une des plus avancées sur les enjeux de la cybersécurité et contribue à la souveraineté nationale et européenne. L'EDIH Bretagne s'appuie sur la maturité d'un écosystème unique et riche.

Le projet doit permettre l'accélération de la numérisation et de l'innovation numérique des acteurs bretons PME/ETI de l'industrie et des collectivités.

Le consortium est composé de : 4 partenaires pour réaliser la coordination, communication, sensibilisation et les services de guichet unique et de diagnostics (I&R, BDI, 7Technopoles Bretagne et PEC), plus 5 partenaires d'expertise pour réaliser la diversité des services nécessaires pour couvrir les besoins des PME.

Le projet EDIH Bretagne s'adresse aux entreprises innovantes bretonnes des secteurs clés de S3 (société numérique, activités maritimes, santé, applications industrielles et agro-alimentaire).

Pour les entreprises localisées sur le nord du Finistère, l'interlocuteur est le Technopôle Brest-Iroise.

À BREST, NOUS RÉUNISSONS UNE COMMUNAUTÉ D'ACTEURS AUX COMPÉTENCES FORTES

DIATEAM MILITARY & CIVIL CYBERSECURITY SOLUTIONS

DIATEAM

Fondée en 2002, DIATEAM est une société française indépendante de R&D spécialisée dans la sécurité informatique et les systèmes d'information innovants.

DIATEAM OFFRE SON EXPERTISE EN EUROPE ET DANS LE MONDE

En tant que pionnier de la simulation de combat cyber à travers un Cyber Range Hybride, DIATEAM est le partenaire de choix pour les grandes entreprises, les entités gouvernementales, les universités et l'industrie, en particulier pour les Opérateurs d'importance Vitale. La gamme de solutions développée par DIATEAM répond à l'ensemble des enjeux de la cybersécurité : analyser, pratiquer et comprendre.

Reconnue pour son expertise, DIATEAM est aujourd'hui un acteur clé du marché des plateformes de formation et du prototypage des cyber-infrastructures. Grâce au partenariat avec Thales, DIATEAM adresse le marché européen et le grand export.

LA CYBERSÉCURITÉ DANS LE SECTEUR MARITIME

Ce secteur est stratégique pour la France et l'Europe, il dispose de systèmes d'information spécifiques et les experts en cybersécurité ne sont pas légions. Par conséquent, il est crucial de confronter les équipages à des scénarios de crise cyber et d'évaluer leurs réactions pour s'assurer qu'elles sont appropriées et conformes aux plans de réponse à incident.

Membre du collège « solutions » de l'association France Cyber Maritime basée à Brest, DIATEAM poursuit son développement de cyber ranges hybrides combinés à des entraînements afin de mieux sécuriser la chaîne logistique en formant et en sensibilisant les hommes et les femmes de la filière maritime.

ENJEU : COMMENT RÉPONDRE À LA PÉNURIE DE COMPÉTENCES EN CYBERSÉCURITÉ ?

Pour combler le déficit de compétences en matière de cybersécurité, l'éducation en tant qu'institution doit investir concrètement dans la formation par la pratique en cybersécurité. La différence s'opérera donc au niveau des systèmes éducatifs, scientifiques et universitaires qui parviendront à développer leur offre de formation continue, voire de reconversion professionnelle, par la pratique pour permettre la montée en compétences cyber d'un plus grand nombre de citoyens et ainsi gagner en résilience.

La France et l'Europe doivent poursuivre leurs efforts pour garantir leur souveraineté sur ces enjeux stratégiques. À ce titre, l'Europe a multiplié les programmes dits H2020 sur cette thématique. Ces programmes visent à stimuler la coopération entre les organisations européennes pour améliorer les offres d'entraînement cyber à destination des industriels et des universitaires. Cette dynamique concerne notamment le maritime dont les spécificités cybernétiques méritent une attention et une mobilisation accrues.

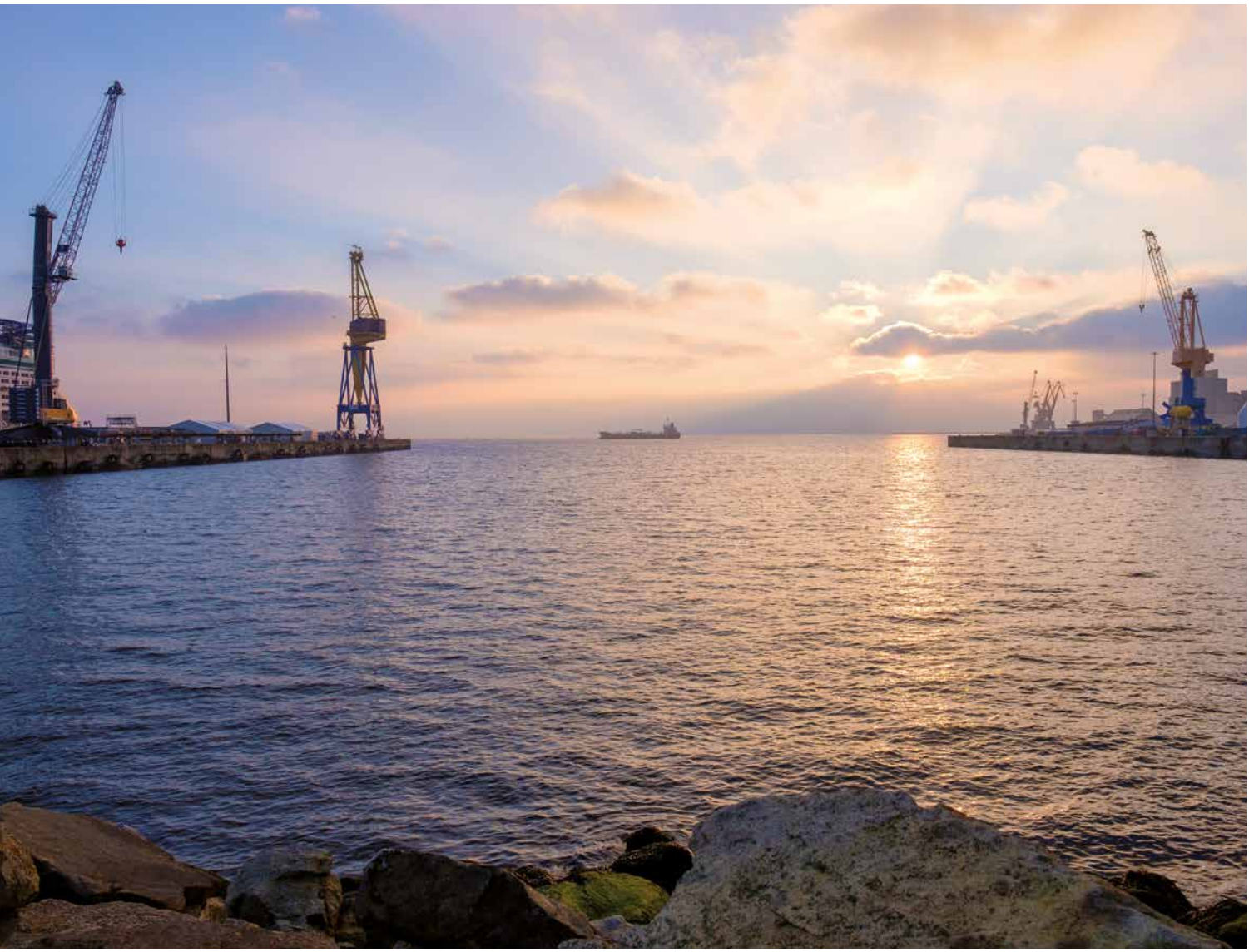
La combinaison de la solution Cyber range et des exercices menés par DIATEAM est véritablement la meilleure manière de répondre au besoin essentiel et urgent de formation en cybersécurité.

UN CYBER RANGE HYBRIDE

C'est une plateforme permettant de reproduire tout ou partie de systèmes IT classiques voire OT industriels. By design, cette plateforme se prête à une multitude d'usages comme l'entraînement Red Team / Blue Team ou encore le prototypage d'infrastructures, le test de composants technologiques voire la création de jumeaux numériques pour, par exemple, leur maintien en condition de sécurité.

● UNLOCK YOUR BRAIN, HARDEN YOUR SYSTEM : L'ÉVÉNEMENT SÉCURITÉ DU NUMÉRIQUE LE PLUS À L'OUEST !

Entre conférences, speakers de renom, rump sessions et animations, cet événement annuel brestois est ouvert à toutes et tous. Il permet de sensibiliser sur la cybersécurité des données numériques. Organisé conjointement par la Cantine numérique Brest et DIATEAM.



© Pierre-François Watras / Brest métropole

ACCOMPAGNEMENT / FORMATION(S)

- OFFENSIVE ADVERSARY OPERATIONS (Niveau EXPERT)
- RED TEAM VS BLUE TEAM TRAINING (Niveau Proficient)
- INTRODUCTION TO CYBERSECURITY (Niveau Competent)
- OFFENSIVE DEV 101 (Niveau EXPERT)
- CTI/MALWARES ANALYSIS (Niveau Proficient)
- OSINT FUNDAMENTALS (Niveau Competent)

Contact Guillaume Prigent, Chairman & co-founder - contact@diateam.net

ÉCOLE NAVALE

L'École navale forme, depuis plus de 200 ans, les marins et officiers de Marine aptes à servir la France dans un contexte géopolitique de conflictualités. Ce sont eux qui, demain, assureront la mise en œuvre de systèmes complexes, à la mer, sous la mer et dans les airs, pour préserver la paix et défendre les intérêts de la France.

Les futurs officiers de marine de carrière ont vocation à occuper des fonctions d'encadrement et de commandement au sein des unités opérationnelles de la Marine nationale (navires de combat, sous-marins, flottilles de l'aéronautique navale, commandos marine). Au cours de leur formation à l'École navale, ils développent les compétences qui feront d'eux les futurs chefs de la Marine. L'évolution permanente des moyens de la Marine et du monde implique de développer les qualités humaines, militaires et morales des élèves et à leur assurer une formation qui réponde aux enjeux stratégiques présents mais aussi futurs. Les défis actuels de la société sont également pris en considération : la préservation de l'environnement et la transition énergétique sont autant de domaines auxquels ils sont sensibilisés.

L'École navale leur délivre un diplôme d'ingénieur.
La devise de l'École navale « Pour la France, par les mers, nous combattons » incarne les valeurs d'engagement qui sont associées à l'école.

UNE ÉCOLE OUVERTE SUR L'EXTÉRIEUR

Ouverte sur le monde civil, l'école propose également des formations de niveau Master et Mastère dans les spécialités de l'ingénierie navale. Ces formations s'inscrivent dans les enjeux actuels, tel que le Mastère spécialisé (MS) Maintenance des navires. L'établissement offre également une offre spécifique en direction du public cadre dirigeant en matière de leadership et de sensibilisation aux enjeux stratégiques de sécurité maritime.

Près de 2 000 élèves et stagiaires sont ainsi formés chaque année par une équipe pluridisciplinaire réunissant enseignants-chercheurs et marins rompus aux opérations. Pour assurer cette mission de formation, l'École navale bénéficie d'atouts majeurs à partir desquels elle a développé des compétences uniques : un centre de formation maritime et terrestre de 110 hectares, des moyens pédagogiques innovants et un centre de recherche en ingénierie navale.

UN PÔLE RECHERCHE PLURIDISCIPLINAIRE AU SERVICE DE LA FORMATION, DE L'INNOVATION ET DES DÉFIS DE LA SÉCURITÉ MARITIME

La formation à l'école s'appuie sur une activité de recherche organisée autour d'un pôle scientifique, d'un pôle de sciences humaines et de deux chaires industrielles : la chaire Résilience et leadership et la chaire Cyberdéfense des systèmes navals. L'institut de Recherche de l'École navale (IRENav) oriente son expertise dans les domaines suivants : hydrodynamique, conversion d'énergie, systèmes d'information géographiques, la donnée maritime et l'intelligence artificielle.

En lien avec l'état-major de la Marine, les équipes de recherche de l'École navale concourent au développement du navire de combat du futur dans ses différentes composantes : technologiques et organisationnelles.

© Pierre-François Watras / Brest métropole

LE NAVAL CYBER RANGE

Afin de développer ses capacités en formation, recherche et innovation en cybersécurité maritime, l'École navale développe depuis plusieurs années une plateforme réaliste unique en Europe. Représentant un navire et ses systèmes d'information, elle permet aux chercheurs et élèves officiers d'évoluer dans un environnement maritime virtuel à des fins d'entraînement, mais aussi de mener des études approfondies et de haut niveau sur les menaces cyber pouvant viser le monde maritime. Financé par l'Europe et la Région Bretagne, le Naval Cyber Range, grâce à ses équipements numériques de pointe et à son réalisme, est un outil précieux pour les chercheurs, enseignants et officiers au quotidien.

Contacts

Marie Broyer, Chargée de communication - marie.broyer@ecole-navale.fr

Laure Aubagnac, VOA Adjointe chargée de communication - laure.aubagnac@ecole-navale.fr

ENSTA BRETAGNE

Héritière de 200 ans d'histoire, l'ENSTA Bretagne forme, à Brest, des ingénieurs civils et militaires et mène des activités de recherche pluridisciplinaires.
L'école est fortement liée au secteur de l'ingénierie marine qui embauche 50% de ses jeunes diplômés et représente plus de la moitié de ses programmes de recherche, en sciences mécaniques ou technologies de l'information.
L'ENSTA Bretagne représente 1 000 étudiants, et plus de 300 diplômés par an (ingénieurs, master(e)s, docteurs) dans des domaines d'excellence liés à la mer : architecture navale, énergies marines renouvelables, systèmes d'observation et de connaissance de l'environnement marin, drones maritimes autonomes…

DES DOMAINES D'EXPERTISE DE POINTE, RECONNUS

Hydrographie-océanographie, systèmes d'observation et Intelligence Artificielle, robotique mobile et autonome, systèmes embarqués, architecture navale, énergies marines renouvelables, management de projets maritimes : autant de domaines d'expertise réputés, en France comme à l'international et portés par l'ENSTA Bretagne.
Ils soutiennent le développement et l'innovation de la filière maritime et celui de la région Bretagne.
Actrice de l'économie bleue, l'ENSTA Bretagne contribue à de nombreux projets visant une meilleure connaissance de l'environnement, le développement d'énergies marines renouvelables, la durabilité de navires et plateformes navales, leur éco-conception… L'ENSTA Bretagne contribue également à l'autonomie stratégique européenne en soutenant les filières de défense de la France, à la fois dans la formation de cadres du secteur et par ses activités de recherche au service des acteurs de la défense.

UNE FORMATION HISTORIQUE DES INGÉNIEURS ET EXPERTS DU SECTEUR MARITIME

Chaque année l'école diplôme environ 300 ingénieurs et experts (masters, mastères spécialisés, docteurs) qui sont immédiatement recrutés à des postes variés, pour moitié dans le secteur maritime, et contribuent ainsi à son essor et à la préparation de l'avenir des filières maritimes.
Leurs profils ont une vocation commune : contribuer à des projets d'innovation, en conception, R&D, mesures & essais ou management de programme.
Outre les diplômes d'ingénieurs, de masters et de mastères spécialisés, l'école organise des formations dédiées aux professionnels dans le cadre de la formation continue.
La dynamique de l'école est forte. Depuis 20 ans, elle attire un nombre sans cesse croissant d'étudiants et de doctorants venus de toute la France et au-delà. Le nombre de diplômés par an a triplé en 20 ans.

UNE RECHERCHE DE POINTE SUR DES APPLICATIONS CIVILES ET MILITAIRES

Les équipes de recherche ENSTA Bretagne s'inscrivent dans des laboratoires académiques multi-tutelles (IRDL, Lab-STICC, FoAP) et des structures de recherche communes avec l'industrie. Les études visent des applications étendues, militaires et civiles, dont une large part en technologies maritimes. Le centre de recherche dispose de moyens expérimentaux inédits pour caractériser les phénomènes et valider les résultats scientifiques, en sciences mécaniques (comportement des matériaux et assemblages en environnement marin) et technologies de l'information (centre cyber, chambre anéchoïde, bassin de robotique, véhicules hydrographiques, systèmes de drones…). Les programmes de recherche régionaux, nationaux et internationaux impliquent de très nombreux partenaires. Ils sont financés par l'Etat et notamment le ministère des Armées (l'ENSTA Bretagne est sous tutelle de la Direction Générale de l'Armement), l'Europe, les collectivités territoriales (Région Bretagne, Département du Finistère, Brest métropole…) et les nombreuses entreprises partenaires.

UN INCUBATEUR « ENSTARTUPS » EN SOUTIEN ET ACCOMPAGNEMENT À L'INNOVATION

ENSTARTUPS, l'incubateur de l'ENSTA Bretagne, accueille une dizaine de porteurs de projet de création d'entreprises, souvent inspirés par le développement maritime durable et la protection de l'environnement marin (valorisation des sédiments marins, valorisation des filets de pêche usagés, éco-conception d'un navire, développement de la filière hydrogène, instrumentation de plongée).
Ils sont accompagnés et conseillés à chaque étape de leur développement. Chaque année, de nouvelles start-ups prennent leur envol.

© Pierre-François Watras / Brest métropole

UN VASTE RÉSEAU PARTENARIAL

Les nombreux partenariats tissés avec de grandes entreprises, PME et start-ups ainsi qu'avec des organismes de recherche publics, institutions, grandes écoles et universités en France et à l'international placent l'ENSTA Bretagne au centre d'un vaste réseau. Elle pilote des initiatives pour fédérer les acteurs bretons et contribue activement au développement des filières maritimes civiles et de défense sur le plan national et international.

PARLONS CYBERSÉCURITÉ

La sécurité des systèmes, qu'il s'agisse d'applications civiles ou militaires, pour les environnements marin, terrestre ou aérien, constitue un des sujets majeurs de recherche et de formation de l'ENSTA Bretagne. Avec les industriels, l'école développe des méthodes innovantes et forme des ingénieurs à la conception de systèmes complexes, communicants et sécurisés. Les travaux couvrent à la fois la sécurité des accélérateurs matériels, des systèmes embarqués, des interfaces hardware-software, des communications (analogiques et digitales), des processus (modélisation, vérification, validation), des systèmes de contrôle industriels (ICS) et des objets connectés (internet des objets).

Contact Ingrid Le Toutouze, Directrice communication - ingrid.le_toutouze@enstabretagne.fr

FRANCE CYBER MARITIME

France Cyber Maritime est une association loi 1901 créée en novembre 2020. Cette task force nationale est basée à Brest et a pour missions d'accroître la résilience du monde maritime et portuaire face aux menaces cyber et de contribuer à la création d'une filière d'excellence française en cybersécurité maritime. Pour cela, France Cyber Maritime encourage le développement de solutions de cybersécurité adaptées et opère le M-CERT (Maritime Computer Emergency Response Team), un centre à vocation nationale qui offre information et assistance à l'ensemble des opérateurs du secteur.

Forte de soixante adhérents, France Cyber Maritime accueille au sein de trois collèges des acteurs publics et des collectivités territoriales littorales de métropole et d'outre-mer, des opérateurs maritimes et portuaires ainsi que des offreurs de solutions de cybersécurité. Elle est soutenue par le Secrétariat Général de la Mer (SGMer), l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), France Relance, Brest métropole ainsi que la Région Bretagne.

SES MISSIONS

Les particularités et la complexité des secteurs maritimes et portuaires nécessitent une approche sectorielle de la cybersécurité. C'est pourquoi, avec le soutien de ses adhérents, France Cyber Maritime analyse les besoins des opérateurs du monde maritime et portuaire et les conseille afin d'identifier les solutions les plus adaptées et les plus performantes : audits et cartographie, Bug Bounty, détection d'intrusion, entraînement, sensibilisation, réponse à incident, R&D…

Par son action et au-delà de l'éventail de solutions proposées par ses adhérents du collège « solutions », France Cyber Maritime contribue également à la résilience du secteur maritime et à la réduction des risques cyber.

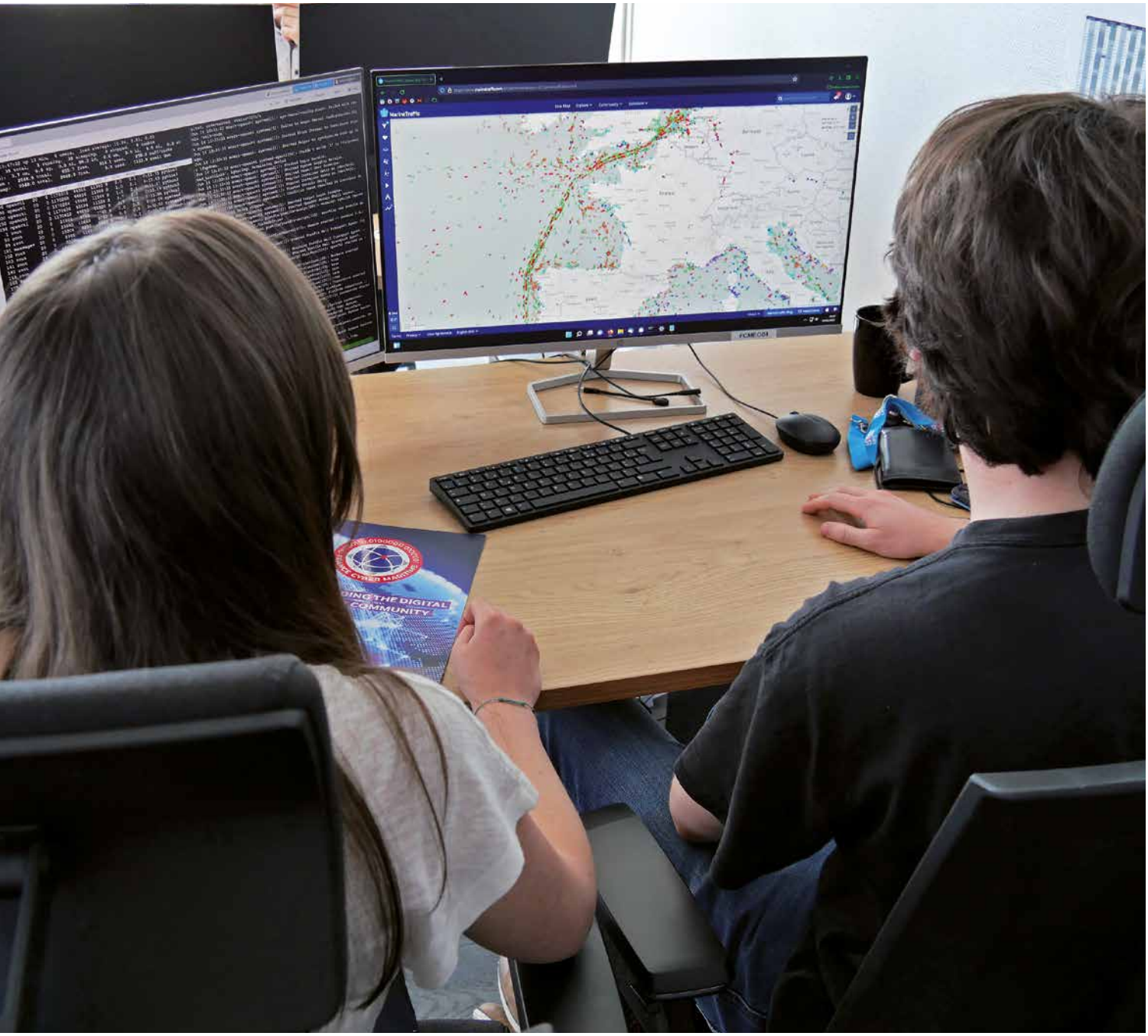
Enfin, l'association tend aussi à développer et promouvoir l'excellence française en cybersécurité maritime, en particulier par des actions de communication, d'animation et de valorisation, en France comme à l'international.

LE M-CERT : ANTICIPER, ANALYSER ET PARTAGER

Une plus grande résilience du monde maritime et portuaire passe également par une capacité à anticiper la menace et à assister les victimes de cyberattaques. C'est la mission confiée au M-CERT (Maritime Computer Emergency Response Team).

Ce centre est en premier lieu chargé de la veille et de l'analyse de la menace ainsi que de la diffusion de bulletins d'information afin de permettre aux opérateurs maritimes et portuaires d'être alertés. Il recueille les incidents et offre assistance à l'ensemble des acteurs métropolitains et ultramarins.

Le M-CERT a rejoint l'association InterCERT France en 2022, afin de s'intégrer au mieux dans le réseau des acteurs des CSIRTs et CERT français de premier plan. Il a pour objectif d'atteindre une capacité opérationnelle complète fin 2023.



Contact Clémence Petiteau, Responsable communication et relations publiques
clemence.petiteau@france-cyber-maritime.eu

IMT Atlantique est une grande école d'ingénieurs généralistes, classée 5ème dans le palmarès 2022 des écoles d'ingénieurs de l'Etudiant. Elle fait partie des 400 premières universités du monde du THE World University Ranking 2023 et 44e université mondiale de moins de 50 ans. L'école est reconnue internationalement pour sa recherche dans plusieurs disciplines des classements de Shanghaï QS et THE. Elle appartient à l'Institut Mines-Télécom et dépend du ministère en charge de de l'Économie, des Finances et de la Souveraineté industrielle et numérique.

Disposant de 3 campus, à Brest, Nantes et Rennes, d'un incubateur présent sur les 3 campus, IMT Atlantique a pour ambition de conjuguer le numérique, l'énergie et l'environnement pour transformer la société et l'industrie par la formation, la recherche et l'innovation et d'être, à l'international, l'établissement d'enseignement supérieur et de recherche français de référence dans ce domaine. IMT Atlantique propose une formation d'ingénieurs généralistes pour laquelle les étudiants sont majoritairement recrutés sur le concours Mines-Ponts. L'École délivre par ailleurs trois diplômes d'ingénieur par la voie de l'apprentissage, des diplômes de masters, mastères spécialisés et doctorats.

Les formations d'IMT Atlantique s'appuient sur une recherche de pointe, au sein de 6 unités mixtes de recherche (avec le CNRS, l'INRIA, l'INSERM, des universités ou écoles d'ingénieurs), dont elle est tutelle : GEPEA, IRISA, LATIM, LABSTICC, LS2N et SUBATECH. L'école s'appuie sur son excellence en recherche dans ses domaines phares (énergie et numérique, cybersécurité, environnement et numérique, industrie du futur, nucléaire, santé et numérique, risques et interactions) et en couplant les domaines scientifiques pour répondre aux défis de demain : transition numérique, transition environnementale, transition industrielle, transition énergétique, santé du futur et recherche fondamentale, en s'appuyant sur 2 instituts Carnot Télécom & Société Numérique et Carnot MINES.

AU CŒUR DES ENJEUX DE CYBERSÉCURITÉ

À IMT Atlantique, le spectre thématique du numérique couvre l'étude des réseaux collaboratifs, la conception des systèmes de communication distribué (infrastructures, objets communicants et centres de données frugaux), la cybersécurité, la défense et la résilience des systèmes complexes, la conception et la réalisation de dispositifs électroniques pour les communications et le traitement du signal, la fouille et la visualisation augmentée ou immersive de données, l'intelligence artificielle, la programmation par contraintes et la recherche opérationnelle pour les modèles de données et l'aide à la décision, la conception avancée de logiciels, ainsi que la robotique, la commande et les interactions homme-machine.

LA CHAIRE CYBER CNI

Lancée en janvier 2016 dans la dynamique du Pôle d'Excellence Cyber, la Chaire Cybersécurité portée par IMT Atlantique a pour objectif de contribuer au développement, au niveau international, des activités de recherche et de formation dans un domaine devenu une priorité nationale : la cybersécurité des infrastructures critiques (réseaux d'énergie, processus industriels, usines de production d'eau, systèmes financiers,...).

LA CHAIRE CYBERDÉFENSE DES SYSTÈMES NAVALS

L'École navale, Naval Group, Thales et IMT Atlantique ont depuis une vingtaine d'années une tradition de collaborations scientifiques recherche et enseignement dans les domaines des systèmes navals, des systèmes d'informations et de télécommunications. Les quatre partenaires ont ainsi créé, en octobre 2014, avec le soutien de la Région Bretagne et sous le patronage du Pôle d'Excellence Cyber, une chaire dans le domaine de la cyber défense des systèmes navals. Ils ont été rejoints en début d'année 2019 par l'ENSTA Bretagne. Cette chaire a été prolongée jusqu'en 2023 ce qui permet d'aborder l'ensemble des travaux actuels sur le long terme.

UN MASTÈRE SPECIALISÉ POUR FORMER DES EXPERTS CYBERSÉCURITÉ

L'objectif de la formation, dispensée sur 13 mois dont 5 en mission en entreprise, est l'acquisition de compétences permettant la conception, le déploiement et l'exploitation d'un système d'information en respectant les contraintes de sécurité inhérentes à un environnement dédié (ingénierie de la cryptographie, audit, supervision). Cette formation de haut-niveau apporte également les compétences spécifiques pour réagir aux incidents de sécurité (intrusions réseau et web). Le mastère spécialisé Cybersécurité permet d'acquérir les savoir-faire académiques et techniques prisés par les entreprises et ouvre aux métiers d'experts en sécurité. Le Mastère Spécialisé Cybersécurité bénéficie de la reconnaissance de l'ANSSI au travers de l'attribution du label SecNumEdu depuis la création de celui-ci. Depuis sa création en 2002 sous le nom de Mastère Spécialisé "Sécurité des systèmes d'information", plus de 280 personnes ont été formées.

Contact Priscillia Creach, responsable Pôle média et promotion - priscillia.creach@imt-atlantique.fr

NAVAL GROUP

Présent à Brest au service de la Marine nationale depuis près de quatre siècles, le savoir-faire industriel maritime de défense est aujourd'hui incarné par Naval Group, leader européen. Le site de Brest est actuellement en pleine modernisation pour relever les défis à venir.

L'activité principale du site Naval Group de Brest est le maintien en condition opérationnelle (MCO) et la modernisation des navires de surface et des quatre SNLE (Sous-marins nucléaires lanceurs d'engins) de la Marine nationale basés à l'Ile Longue, sur la partie Sud de la Rade de Brest. Dans la Base navale de Brest, au niveau des bâtiments de surface, Naval Group est en charge du MCO de multiples navires (frégates multimissions Fremm, frégate anti sousmarine de type F70, BSAM – bâtiments de soutien et d'assistance métropolitains – et chasseurs de mines). Les arrêts techniques se succèdent tout au long de l'année, en fonction du planning opérationnel des navires.

L'activité de maintien en condition opérationnelle des bâtiments de surface et sous-marins français constitue l'activité visible du site de Brest, au service du client Marine nationale. Brest intervient également sur plusieurs programmes de maintien en condition opérationnelle du groupe à l'international et dans les territoires Outre-Mer où sont basés les navires de la Marine nationale. Il s'agit de travaux réalisés en ateliers (visite de pièces et éléments de navires) et de projection de collaborateurs en mission pour des arrêts techniques réalisés sur place.

Les activités en lien avec la dissuasion représentent 60 % de l'activité du site, ce qui lui permet de bénéficier d'une charge stable, prévisible et pérenne. La maintenance et la modernisation des navires de surface pèsent environ 20 % de l'activité. Le reste de l'activité est dédiée aux activités internationales et au soutien à des programmes majeurs du groupe.

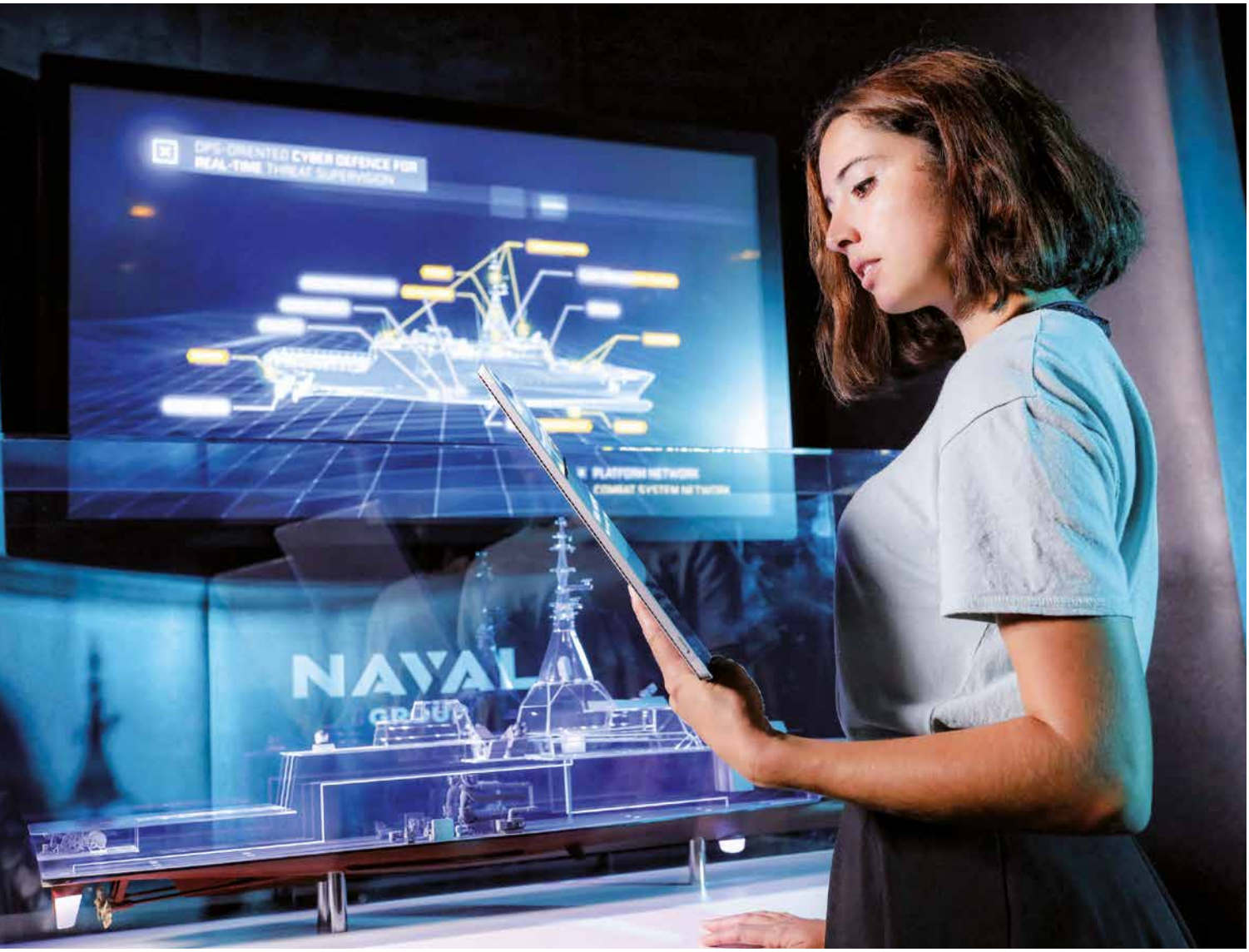
Enfin, l'activité de maintien en condition opérationnelle et de modernisation de Naval Group concerne également les systèmes et équipements de navigation, les systèmes d'armes des navires (mises à jour logicielles, détection, optique, armes, lutte sous-marine), les systèmes de communication aux standards militaires ou encore les simulateurs (de conduite des installations, de défense…).

En parallèle de ces activités, Naval Group dispose sur la zone du Froutven, à Guipavas, d'un site qui héberge environ 300 collaborateurs sur des activités support du groupe : Direction digitale des systèmes d'information (DDSI) et Centre des services partagés comptables (CSPC).

LA CYBERSÉCURITÉ : UNE PRIORITÉ STRATÉGIQUE POUR NAVAL GROUP

La cybersécurité est dorénavant un domaine de lutte de premier plan avec une augmentation constante du nombre d'opérations cybernétiques conduites sur les théâtres d'opérations et sur les différents acteurs de l'écosystème de défense. Aujourd'hui, il ne s'agit plus uniquement de gérer les risques cyber, mais de les anticiper et surtout de faire preuve d'une performance robuste et adaptée en la matière pour assurer les succès de la numérisation des systèmes et des espaces.

La supériorité opérationnelle des marines en dépend. Cette protection robuste et fiable, ajustée aux besoins cyber de chaque client et au type de mission des bateaux, propose une modularité tout au long de leur cycle de vie. L'offre de cyberdéfense de Naval Group est le fruit d'une innovation constante, conciliant le besoin impérieux de protection du navire avec les impératifs de continuité opérationnelle et de sécurité à la mer des équipages.



Afin d'assurer la résilience de ses navires et de ses infrastructures face à ces cyber-enjeux, Naval Group a fait de la cybersécurité un enjeu stratégique de son développement et de ses produits. Naval Group intègre les aspects de sécurité à toutes les étapes du cycle de vie du navire. Dès leur conception, les navires de combat de Naval Group et leurs systèmes numériques sont conçus et protégés de façon native. La cybersécurité est aussi intégrée dans les phases de développement, de production et de maintien en condition opérationnelle des navires : la performance cyber est adaptée en fonction des besoins opérationnels exprimés par le client. Cela passe aussi par l'accompagnement de la supply-chain et l'acculturation de tous les acteurs de la chaîne de valeur à la prise en compte de la menace cyber.

Naval Group entraîne dans son sillage de très nombreux fournisseurs et sous-traitants de la filière navale et maritime. Garant du dynamisme économique de cette filière et de sa croissance, le groupe est aussi soucieux de la maturité et la montée en compétence de ses acteurs en matière de cybersécurité, au bénéfice de l'ensemble de l'écosystème maritime.

Contact

Philippe Forest, Directeur communication du site Naval Group de Brest – philippe.forest@naval-group.com

THALES, UN LEADER MONDIAL DES HAUTES TECHNOLOGIES

Thales investit dans les innovations du numérique et de la « Deep Tech » – connectivité, Big Data, intelligence artificielle, cybersécurité et quantique – pour construire un avenir de confiance, essentiel au développement de nos sociétés. Le Groupe propose des solutions, services et produits qui aident ses clients – entreprises, organisations, États – dans les domaines de la défense, de l'aéronautique, de l'espace, du transport et de l'identité et sécurité numériques, à remplir leurs missions critiques en plaçant l'humain au cœur des décisions.

Thales compte 81 000 collaborateurs dans 68 pays. En 2021, le Groupe a réalisé un chiffre d'affaires de 16,2 milliards d'euros.

L'OFFRE DE SOLUTIONS CYBER DE THALES AU SERVICE D'UN CERCLE VERTUEUX DE LA SÉCURITÉ

Avec plus de 70 ans d'expérience dans ce domaine d'expertise, Thales est un leader mondial de la protection des données et de la cybersécurité. Fournisseur majeur de services et de systèmes de cybersécurité contribuant à la souveraineté de ses clients, Thales renforce ses compétences en cybersécurité à travers une stratégie cohérente d'acquisition lui permettant d'accroître l'étendue de ses solutions et son empreinte à l'international.

Ses équipes de plus de 4000 experts cybersécurité répondent aux exigences les plus poussées de ses clients, organismes gouvernementaux, opérateurs d'infrastructures critiques et entreprises de communication, industrielles, financières et de la défense, en matière de sécurisation de systèmes d'informations.

Présent sur l'ensemble de la chaîne de valeur de la cybersécurité, Thales a rassemblé au sein de son nouveau segment d'offre CyberSolutions ses trois familles de produits phare :

- Le portefeuille de solutions Cybels répondant aux besoins d'évaluation des risques, d'entraînement et de simulation, de détection et de réponse aux attaques avec ses 9 centres opérationnels de sécurité (SOC);
- Les produits dits de souveraineté comprenant le chiffrement et les sondes pour protéger les systèmes d'information critiques ;
- La plateforme CipherTrust de protection des données, de sécurité du cloud et de gestion d'accès.

THALES, UN ACTEUR INCONTOURNABLE DE LA CONFIANCE

Dans le domaine civil, Thales protège ainsi 80 % des transactions bancaires mondiales et assure la sécurité de 19 des 20 plus grandes banques mondiales via ses produits de cryptographie. Thales assure également la cybersécurité de 9 des 10 géants mondiaux de l'internet et intervient sur les systèmes d'information critiques de plus de 130 clients.

Dans la sphère étatique, Thales fournit des produits et solutions de sécurité « High Grade » (équipements de chiffrement, sécurisation de systèmes complexes dès leur conception) dans 50 pays dont 25 pays de l'OTAN.

Au-delà de ses activités de cybersécurité au service de ses clients, Thales a lancé, au sein du groupe, une démarche transversale visant à intégrer la cybersécurité de manière native, au sein de ses offres. Thales participe ainsi à la sécurisation des plus grands programmes de défense en garantissant à ses clients une sécurité « by Design » (i.e. prise en compte dès la phase de conception du système).

© Pierre-François Watras / Brest métropole

Contact Marion Bonnet, Attachée de presse - marion.bonnet@thalesgroup.com

PÔLE MER BRETAGNE ATLANTIQUE

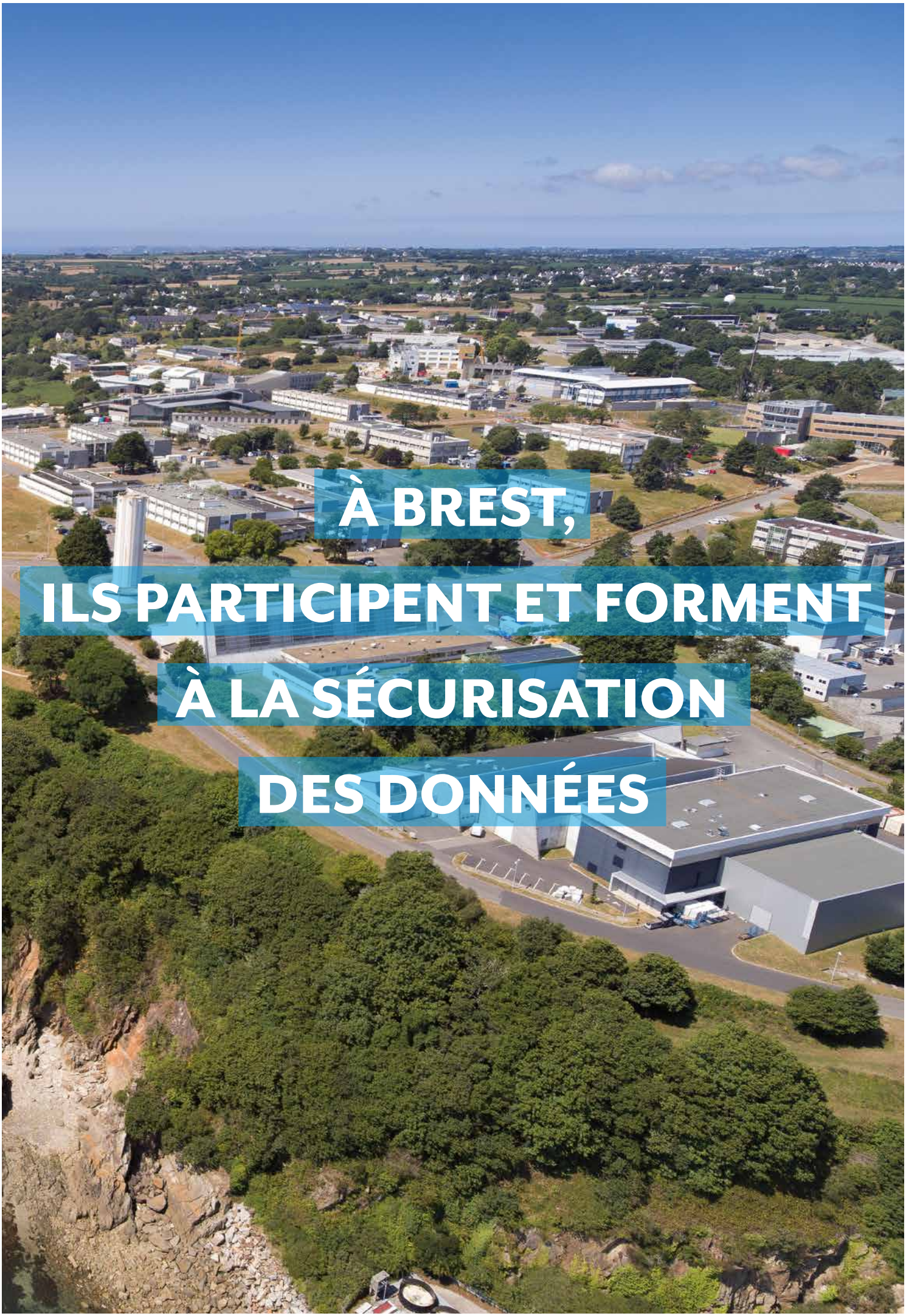
Pôle de compétitivité dédié à l'économie de la mer, le Pôle Mer Bretagne Atlantique est un animateur de l'écosystème maritime et un promoteur de l'innovation collaborative au service de la croissance bleue. Depuis son siège brestois, il conduit de nombreuses actions événementielles et d'influence : participation à des salons et des missions internationales ou organisation d'événements thématiques en Bretagne-Pays de La Loire.

Face aux enjeux socio-économiques et environnementaux, le secteur maritime mondial se trouve confronté à un défi, celui de sa mutation vers une économie durable, innovante et partagée. Cette croissance bleue ouvre des opportunités que le Pôle Mer Bretagne Atlantique met en perspective par la labellisation de projets structurants sur son territoire. De la biodiversité au croisement des technologies numériques, spatiales et maritimes, ce sont autant de thématiques qui dessinent dès à présent les contours de l'économie maritime. Grâce à ces actions, le Pôle Mer contribue activement à faire émerger des solutions performantes et compétitives dans tous les domaines d'activité maritime, en soutenant les initiatives spontanées mais aussi en repérant les futurs besoins. Le Pôle détecte les verrous technologiques, identifie les compétences et les incite à relever le défi. Sa mission principale est ensuite l'accompagnement de ces projets vers la labellisation : conseil et expertise, mise en relation, financement, visibilité et valorisation... Depuis sa création, le Pôle Mer Bretagne Atlantique a accompagné et labellisé 500 projets innovants pour 1,28 milliards d'euros d'investissements engagés.

ENGAGER LE MARITIME DANS UN NOUVELLE ÈRE CYBER

L'informatique, les réseaux de communication et les données sont désormais omniprésents sur les navires et dans les ports, qui sont, de fait, susceptibles d'être la cible de nouvelles formes de menaces et de piratages. La piraterie informatique et les cyber-attaques sont une réalité quotidienne des opérateurs maritimes. Membre fondateur de France Cyber Maritime, le Pôle Mer sensibilise ses adhérents aux problématiques de la cybersécurisation, non seulement de leur outil de production mais aussi de leurs produits dans le cadre d'une démarche de cyber by Design. Cette sensibilisation passe par la promotion des dispositifs d'audit et de protection.
En outre, le pôle suscite et accompagne divers projets d'innovation cyber, en particulier en matière de protection des drones et navires autonomes ainsi que de cybersécurité des ports.

Contact Frédéric RENAUDEAU, Conseiller Défense - frédéric.renaudeau@polemer-ba.com



À BREST, ILS PARTICIPENT ET FORMENT À LA SÉCURISATION DES DONNÉES

LA FRENCH TECH BREST+

Depuis 2016, la dynamique French Tech est enclenchée à l'ouest de la Bretagne, sur le territoire de la French Tech Brest+. Dynamique opérée par les technopoles de Brest, Lannion et Quimper, elle vise à favoriser la création et le développement de startups sur notre territoire, favoriser la digitalisation et les interactions avec d'autres pans de l'économie, agir sur les talents et fédérer notre écosystème.

Convaincus que les startups ont besoin d'un environnement ouvert et stimulant pour s'épanouir, l'équipe opérationnelle travaille donc sur les freins rencontrés par les startups (lancement, visibilité, business, recrutement...) et développe des actions en réponse à ces besoins. Ainsi, des événements comme Ticket to Pitch, Ouest Startups, Femmes & Numérique ou encore le Job Connect viennent illustrer ces événements fédérateurs et fertiles !

L'INTELLIGENCE ARTIFICIELLE AU SERVICE DES ENTREPRISES BRETONNES : ENJEUX, SENSIBILISATION ET MARCHE À SUIVRE.

Pour la 3e année consécutive, la French Tech Brest+ a organisé les 29 & 30 juin AI DAYS.

L'évènement dédié à l'intelligence artificielle propose s'intéresse à l'incidence de l'IA dans des univers variés tels que la santé, le maritime, l'industrie, l'environnement etc. Sont également expliqués aux PME les enjeux et les bonnes pratiques pour structurer ses données et comment les faire « parler » avec de l'IA...

Des pré diagnostic ont pour objectif de d'expliquer aux entreprises de manière simple et concrète comment utiliser l'IA et évaluer leur potentiel Data pour les aider à comprendre et à envisager un plan opérationnel.

Contact Frédéric Nicolas, Délégué général - frederic.nicolas@tech-brest-iroise.fr

GACYB
bretagne

GACYB BRETAGNE

Créée en 2017 par la CCIMBO Brest et soutenue par l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Information), le GACYB Bretagne (Groupement des Acteurs en cybersécurité) est une association composée d'une trentaine d'entreprises finistériennes : informatique, cybersécurité et ESN. Son objectif est de sensibiliser l'ensemble des acteurs économiques finistériens à l'importance de la cybersécurité. Cette association a pour objet de promouvoir et œuvrer à la diffusion auprès d'un public de professionnels, d'entreprises, de collectivités et d'établissements d'enseignement de bonnes pratiques en termes de cybersécurité se rapportant au numérique et au digital. La Charte Cybersécurité des prestataires de services informatiques et numériques en constitue le socle.

Le GACYB Bretagne organise le rendez-vous annuel nommé « Breizh Cyber Show » et dont l'objectif est de réunir sur une soirée conviviale 200 à 300 entreprises du Finistère autour de la thématique de la Cybersécurité.

L'ambition est d'apporter aux chefs d'entreprise, à leurs collaborateurs, aux collectivités, une meilleure compréhension des enjeux et des solutions concrètes à mettre en œuvre. Cet évènement ambitieux qui se déroule pendant le mois de la Cyber a pour volonté de devenir un évènement majeur et récurrent en Finistère.

De plus, chaque premier mercredi du mois, l'association organise dans les CCI de Brest, Quimper et Morlaix les mercredis de la Cyber : créneaux ouverts aux entreprises du territoire pour des consultations gratuites sur le thème de la cybersécurité.

ACCOMPAGNEMENT / FORMATION(S)

Le GACYB Bretagne intègre des entreprises proposant des formations en Cybersécurité à destination des entreprises et des collectivités. Ces formations comprennent aussi bien des formations en sensibilisation que des formations de perfectionnement et de progression en compétences cyber.

Contact Sébastien Texier, Président - contact@gacyb.bzh

Datacenter Groupe Asten © Air Media 29

GROUPE ASTEN

Depuis plus de 25 ans, le Groupe Asten s'engage et investit pour le développement économique, social et numérique de la Bretagne. Nous accompagnons nos clients dans le développement, l'évolution et la sécurisation de leur système d'information et de leurs services numériques, les aidons à améliorer leurs performances en étudiant leurs besoins et métiers, en auditant et optimisant leurs infrastructures et applications, en leur conseillant les technologies les plus adaptées.

Nous intervenons notamment sur les sujets d'infogérance, sauvegarde et sécurisation des systèmes d'information et sommes propriétaire de 2 datacenters à Brest métropole. La cybersécurité est par conséquent au cœur de notre expertise.

Quelques-unes de nos offres de service :

- L'hébergement et l'infogérance des systèmes d'information des entreprises dans nos datacenters : les serveurs sont infogérés et protégés (failles de sécurité comblées par mises à jour systématiques). Nous garantissons la sécurité face aux attaques, par un très haut-niveau de protection qui freine les attaquants et les détourne vers une autre cible.
- Pour les structures qui ont des serveurs au sein de leur entreprise, nous proposons une infogérance du système d'information, comprenant les mises à jour de sécurité.
- Pour toutes les entreprises, qu'elles hébergent leur SI chez Groupe Asten ou non, nous menons des missions d'audit et de renforcement des configurations des annuaires (AD).
- Nous proposons une offre de sécurisation de la messagerie : l'objectif étant de contrôler tous les mails entrants et de ne délivrer que ceux qui ne présentent aucun risque.
- Pour renforcer la sécurité des sauvegardes, nous déployons leur hébergement dans nos datacenters, ainsi que l'étude d'un plan de secours (PRA) et le test régulier de celui-ci.

ACCOMPAGNEMENT / FORMATION(S)

Nous proposons des accompagnements à la rédaction de chartes informatiques.

Nous proposons des formations et ateliers de sensibilisation (sous forme d'échanges et serious game) des utilisateurs aux risques cyber (prêt de badge et politique de mots de passe, social engineering, tailgating, vol de matériel, verrouillage de session, USB dropping, phishing, comportement à adopter à l'extérieur et à adopter en cas de compromission, sobriété numérique).

Contact

Esther Bozec, Responsable marketing et communication
- esther.bozec@groupe-asten.fr
Philippe Hérault, Ingénieur commercial
- philippe.herault@groupe-asten.fr

<BZHunt>
EAT . SLEEP . HACK . REPEAT

BZHUNT EN DEUX MOTS ? HACKING X PASSION !

Loin du cliché hollywoodien, BZHunt repousse les limites pour défendre et valoriser la culture du hacking éthique en France et dans le monde.
Nos hackers éthiques ont fait de leur passion un métier avec pour objectif de capitaliser sur leurs travaux de recherche & innovation pour développer des solutions de cybersécurité innovantes.
De la réponse à incident aux audits et tests d'intrusion, sans oublier la sensibilisation et la formation, notre équipe challenge la sécurité des entreprises avec originalité pour identifier les vulnérabilités et évaluer leur exposition aux risques cyber.
Le métier de la cybersécurité est en constante évolution face à des menaces toujours de plus en plus sophistiquées. Nos équipes s'efforcent à offrir un service de qualité taillé aux besoins des clients avec une approche différenciante.
Si le terme hacking est principalement associé à l'univers numérique, c'est avant tout un état d'esprit. Quel que soit son champ d'activité, un hacker va user de toute sa créativité pour dépasser les limites imposées par un système et le détourner de son usage et étendre ses capacités.
Depuis sa création, BZHUNT a audité et accompagné plus d'une centaine de clients. Nous intervenons partout dans le monde quels que soient la taille ou le secteur d'activité de nos clients. Nous adressons des PME locales comme des grands groupes internationaux ou les GAFAM.
BZHUNT est aujourd'hui la 1ère entreprise française à participer à des programmes de Bug Bounty.
Nous avons obtenu le titre de champion du monde lors de la compétition organisée par Hacker One en février 2022.

ACCOMPAGNEMENT / FORMATION(S)

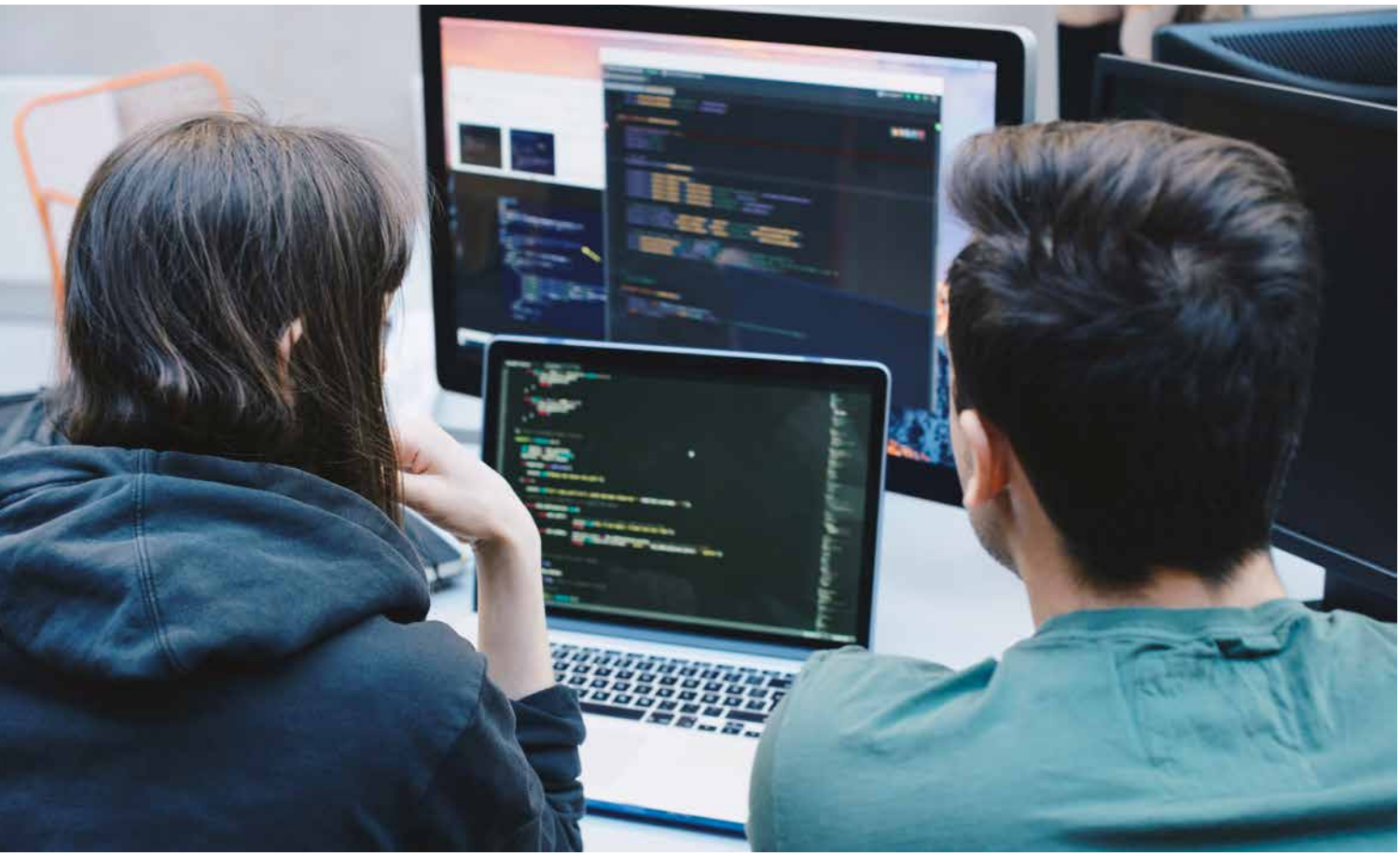
Sharing Is Caring ! BZhunt conçoit et anime des formations et conférences pour partager ses recherches et sensibiliser les professionnels au risques cyber :

- Campagne de phising
- Conférence thématique cyber
- Ateliers de sensibilisation
- Workshop de gestion de crise
- Présentation des métiers de la cybersécurité et de hacker éthique

Toutes nos formations et conférences peuvent être dispensées en français et en anglais.

Contact

Jennifer L'Azou, responsable marketing et communication - jennifer.lazou@bzhunt.fr



Crédit Mutuel
ARKEA
DE NOUVEAUX LIENS POUR CHANGER DEMAIN

CREDIT MUTUEL ARKEA

Le groupe Crédit Mutuel Arkéa est composé des fédérations du Crédit Mutuel de Bretagne, du Sud-Ouest et de leurs caisses locales adhérentes, ainsi que d'une quarantaine de filiales spécialisées (Fortuneo, Monext, Arkéa Banque Entreprises et Institutionnels, Arkéa Investment Services, Suravenir...). Il compte plus de 11 000 salariés, 2 800 administrateurs, plus de 5 millions de sociétaires et clients dans la bancassurance et affiche un total de bilan de 182,4 milliards d'euros. Crédit Mutuel Arkéa se classe parmi les tout premiers établissements bancaires ayant leur siège en région.

Au sein du Pôle Support au développement, la Direction des risques est chargée du pilotage prudentiel consolidé des risques, y compris celui des risques dits "émergents" (risque climatique, risque cyber...).

La Direction des risques doit veiller à la bonne articulation du pilotage des risques et du capital, et assurer la communication risque au niveau du Groupe Crédit Mutuel Arkea.

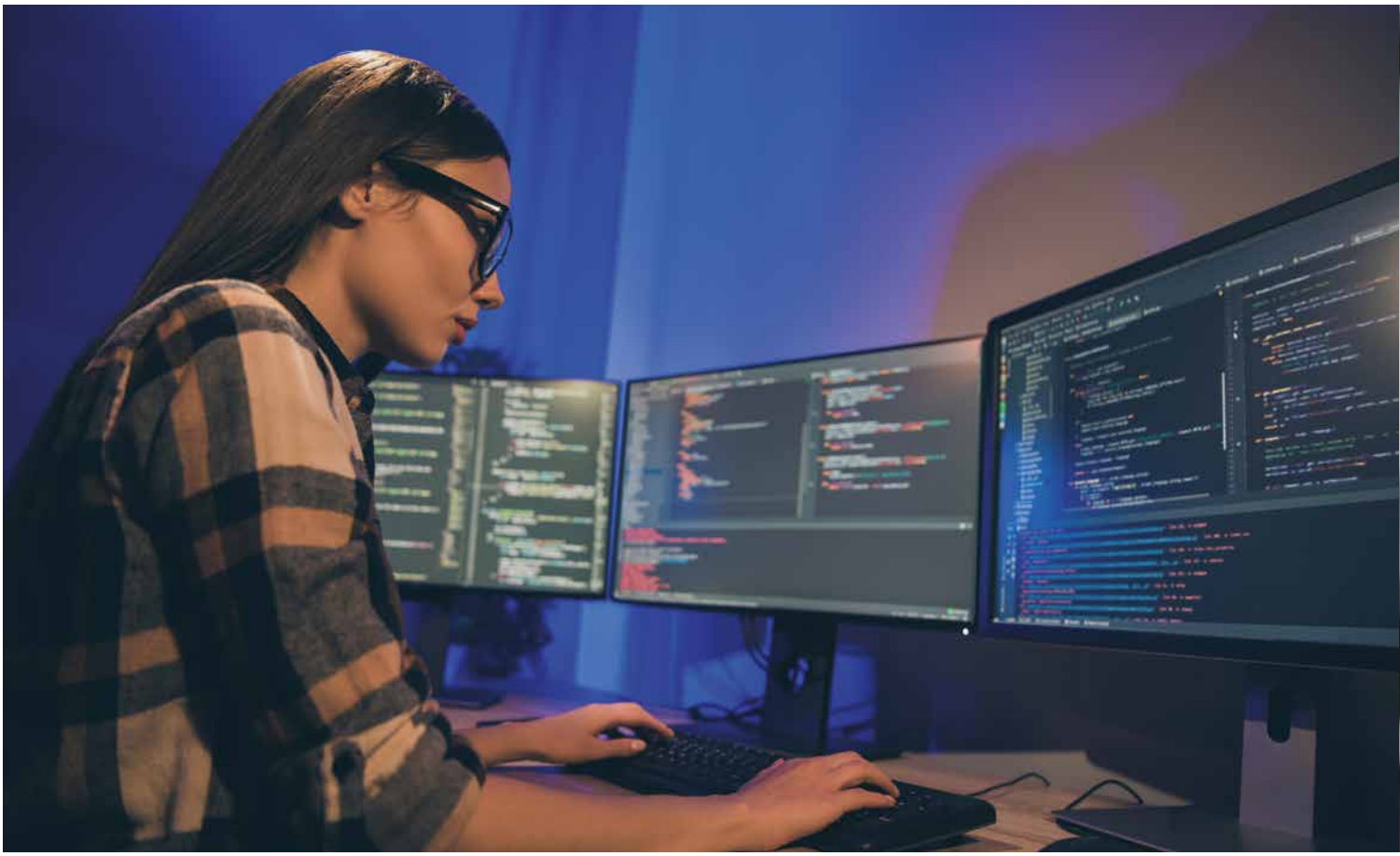
Enfin elle organise et assure la surveillance des risques de crédit et de contrepartie, marché et opérationnels y compris la fonction de Sécurité des Systèmes d'Informations et veille à la bonne application de la politique associée.

ACCOMPAGNEMENT ET FORMATION INTERNES

- E-learning de sensibilisation (une formation générale, une formation spécifique aux intervenants sur la plateforme PCIDSS) ;
- Formation EBIOS RM / ISO 27005 pour les acteurs SSI ;
- Formation DevSecOps pour les relais SSI de la DSI.

Contact

Ariane Le Berre-Lemahieu, Responsable des relations presse & contenus éditoriaux - ariane.le-berre-lemahieu@arkea.com



© Adobe Stock

ELLIDISS TECHNOLOGIES

Ellidiss Technologies est implantée dans la région brestoise depuis 18 ans. La société conçoit et distribue dans le monde entier (plus de 90 % du chiffre d'affaires à l'export) des produits et services pour la conception des systèmes critiques à prédominance logicielle. Les domaines ciblés sont essentiellement l'aéronautique et le spatial.
Les solutions proposées par Ellidiss permettent de définir, dès les phases amont du développement des nouveaux systèmes, les compromis nécessaires entre performance temps-réel, sûreté de fonctionnement et cybersécurité. Concernant la cybersécurité, il s'agit de traiter "le mal à la racine" en concevant des systèmes sécurisés par construction, en s'appuyant sur des solutions techniques et des méthodologies de développement éprouvées.

Ellidiss Technologies consacre plus de 30 % de son chiffre d'affaires à la R&D. La société contribue en particulier à des projets collaboratifs européens de l'Agence Spatiale Européenne et des programmes H2020.

Contact
Pierre Dissaux, Managing Director
- pierre.dissaux@ellidiss.com

© Adobe Stock

GROUPE PRORISK

Prorisk est une société de conseil en gestion des risques. De par sa marque PRORISK CYBER, c'est une réponse globale qui est apportée aux besoins de cybersécurité et de conformité avec le Règlement Général pour la Protection des Données (RGPD). Ceci au travers de ses 3 métiers :

1. L'Ingénierie/Conseil pour analyser les risques d'atteinte numérique et définir comment les réduire
2. La Formation afin d'accroître la culture des dirigeants et usagers pour prévenir les cyberattaques et maintenir l'activité quand elles surviennent
3. L'Assistance opérationnelle pour accompagner dans le temps en tant que Délégué à la Protection des Données (DPO) ou Responsable de la Sécurité des Système d'Information.

ACCOMPAGNEMENT / FORMATION(S)

- Management de la cybersécurité pour dirigeants d'entreprise sur une durée d'une journée.
- Sensibilisation à la cybersécurité pour collaborateurs d'une durée d'une demi-journée

Contact

Pascal Le Claire, Directeur général
- contact@prorisk-cyber.com

© Pierre-François Watras / Brest métropole

SOURCITEC

SourcITEC est une société de prestations, conseils et services, spécialisée en gouvernance Cybersécurité : - Cyberprotection - Cyberdéfense - Cybermaritime - Cyberrésilience. Nous proposons, en particulier, des prestations d'accompagnement RSSI, RSSI externe, analyses de risques, audits et sensibilisations.
Elle accompagne les professionnels pour définir les fonctions et responsabilités en matière de gestion des Cyber risques ; pour mesurer les risques et mettre en place un dispositif de prévention adapté ; pour définir un processus de gestion de crise ; pour sensibiliser les collaborateurs sur les menaces et les bonnes pratiques à adopter.

FORMATION(S) DÉLIVRÉE(S)

Depuis 2020, SourcITEC est un organisme agréé de formation et depuis le 20 octobre 2022 certifié Qualiopi (action de formation) dans le domaine de la cybersécurité et de la gouvernance :

- Cybersécurité pour les TPE et PME
- Cybersécurité maritime
- Sécuriser une infrastructure de messagerie
- introduction aux principes cryptographiques
- Prise en main de l'outil EGERIE Risk Manager avec EBIOS RM
- Management de projets
- Réussir votre projet
- Gestion de crise

Contacts

- Guillaume Basset, Président, Emmanuel Hynaux et Jocelyne Monfort, Directeurs Généraux et associés - sourcitec@sourcitec.com
- Alice Le Garrec Rivalain, Chargée communication et événementiel - alice.legarrec.rivalain@sourcitec.com

WATOO

WaToo, start-up issue de la recherche de IMT Atlantique, développe des solutions logicielles dont l'objectif est d'aider les organisations dans la détection des fuites d'information issues d'acteurs de confiance (collaborateurs, partenaires, sous-traitants, ...) et la responsabilisation (identification précise de l'origine de la fuite comme complément numérique des contrats, NDA, ...). D'après le Insider Threats Report réalisé par le Ponemon Institute et IBM, ce type d'incidents ont bondi de 44 % au cours des deux dernières années. Le coût moyen par incident a quant à lui augmenté de plus d'un tiers, pour atteindre 15,38 millions de dollars.

Basée à Plouzané, WaToo est une équipe de 4 personnes qui accompagnent leurs clients dès le démarrage de leur projet, participant à l'identification des besoins de protection.

WaToo est accompagné dans son développement par la région Bretagne et BPI et fait partie également de l'incubateur HEC à Station F.

Contact

Javier Franco Contreras, Président
- javier.francocontreras@watoo.tech

© Pierre-François Watras / Brest métropole

FORMATIONS APRÈS LE BAC

BAC +2

BTS Systèmes numériques Option Informatique et réseaux – Lycée Vauban à Brest

CONDITIONS D'ACCÈS À LA FORMATION

Après un bac :

- STI2D (Sciences et Technologies de l'Industrie et du Développement Durable),
- Professionnel,
- S (Scientifique) ou STL (Sciences et Technologie de Laboratoire).

CONTENU DE LA FORMATION

- Enseignement professionnel : informatique et réseaux (14h dont 10h de travaux pratiques en 1ère année, 17h dont 13h de TP en 2e année), sciences physiques (6h dont 3h de TP en 1ère année, 4h dont 2h de TP en 2e année).
- Enseignement général : culture générale et expression, anglais, mathématiques.
- 6 semaines de stage en entreprise.
- 180 heures de projet technique de fin d'études.

POURSUITES D'ÉTUDES & DÉBOUCHÉS

Le titulaire du diplôme peut occuper des fonctions liées aux études de conception, au développement, à l'intégration de logiciels principalement dans les domaines de l'informatique technique et industrielle et les réseaux et télécommunications. Les orientations technologiques concernent les systèmes embarqués et mobiles, les moyens de communication et l'administration de systèmes et réseaux.
Des poursuites d'études sont possibles en licence professionnelle, écoles d'ingénieurs, universités ou Prépa ATS (Adaptation Technicien Supérieur).

Contact

Lycée Vauban - Rue de Kerichen, BP 40224,
29804 Brest Cedex 09
02 98 80 88 00 - ce.0290012F@ac-rennes.fr

BTS Systèmes numériques Option Informatique et réseaux - Lycée la Croix Rouge la Salle à Brest

CONDITIONS D'ACCÈS À LA FORMATION APRÈS LE BAC

- Bac STI2D
- Bac Pro Industriel
- Bac Général

DESCRIPTIF

Le technicien supérieur en informatique sera spécialisé dans l'installation et l'administration des réseaux et infrastructures informatiques dans de nombreux secteurs d'activité :

- Les systèmes d'exploitation
- L'architecture et l'administration des réseaux informatiques tertiaires, industriels et embarqués
- La programmation d'éléments de réseaux, de télécommunication, d'applications industrielles, mobiles, embarquées, occasionnellement de gestion

POURSUITE D'ÉTUDES

- Formation BAC +3 en alternance dans le domaine de la cybersécurité (ouverture prochainement)
- Licence professionnelle.
- Licence et Master en université
- École d'ingénieur, en particulier après une classe de BTS-Prépa

Contact

Lycée La Croix Rouge La Salle,
2 rue Mirabeau, 29200 Brest
contact@lacroixrouge-brest.fr

BTS SIO (Services Informatiques aux Organisations) - Groupe scolaire Estran, Lycée Charles de Foucauld à Brest

CONDITIONS D'ACCÈS À LA FORMATION

- Titulaire du BAC + admission parcoursup
- Possibilité de formation en entreprise (alternance, apprentissage, stage...)
- 10 à 12 semaines de stages réparties sur les 2 années

DESCRIPTIF

Le BTS SIO (Services Informatiques aux Organisations) répond aux exigences des entreprises en formant des spécialistes aptes à occuper rapidement un emploi d'administrateur de réseaux locaux d'entreprise ou de développeur d'applications.
Des techniciens du numérique et de la cybersécurité capables d'évoluer et de s'adapter rapidement.

- Protéger les données à caractère personnel
- Préserver l'identité numérique de l'organisation
- Sécuriser les équipements et les usages des utilisateurs
- Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques
- Option SISR : Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service
- Option SLAM : Assurer la cybersécurité d'une solution applicative et de son développement

POURSUITE D'ÉTUDES

Poursuite vers un cursus universitaire LMD en informatique, une licence professionnelle, une formation professionnelle en alternance.

DÉBOUCHÉS PROFESSIONNELS

Toutes les entreprises, de la PME à la multinationale, disposent d'un parc, d'un réseau informatique et de nombreux logiciels qui nécessitent des compétences de gestion, d'administration ou de développement et de sécurisation.

Exemples de métiers pour la spécialité « Solutions d'Infrastructure, Systèmes et Réseaux » :

- Administrateur systèmes, réseaux et sécurité.
- Technicien support et déploiement systèmes et réseaux
- Technicien d'infrastructure systèmes et réseaux...

Exemples de métiers pour la spécialité « Solutions Logicielles et Applications Métiers » :

- Analyste programmeur
- Développeur d'application web, base de données, mobile, multimédia
- Métiers du web (Webmaster, intégrateur web...)
- Assistance aux utilisateurs...

Contacts

Contact presse : Yuna Le Breton - Chargée de communication : ylebreton@estran-brest.education
Contact formation :
Mr Eric Simon - esimon@estran-brest.education

Gestionnaire en maintenance et support informatique - CESI campus de Brest

TYPE(S) DE FORMATIONS PROPOSÉES

Formation en alternance - Bac +2

CONDITIONS D'ACCÈS À LA FORMATION

Être titulaire d'un bac (ou d'un niveau 4 équivalent).
Admission sur dossier de candidature, tests de positionnement et entretien de validation. Si vous souhaitez intégrer l'école à niveau bac, vous devez formuler vos vœux sur parcoursup.fr, avant de suivre notre processus de recrutement.
La formation est gratuite et sans aucun frais d'inscription.

DESCRIPTIF

Ce parcours comprend des projets collaboratifs qui reposent sur des cas concrets d'entreprise. Il met les élèves en situation de technicien informatique dans un service informatique et dans une ESN. Les objectifs :

- Répondre aux besoins des utilisateurs
- Installer et configurer les PC et leurs périphériques
- Mettre en place les accès aux réseaux (locaux, intranet, internet)
- Maintenir le parc-informatique
- Assister les utilisateurs dans l'utilisation de l'outil informatique. Le gestionnaire en maintenance et support informatique doit accompagner les utilisateurs dans leur mobilité (accès aux données depuis plusieurs lieux et plusieurs types de matériels) dans le respect des principes de sécurité

POSSIBILITÉ DE FORMATION EN ENTREPRISE (ALTERNANCE, APPRENTISSAGE, STAGE...)

Alternance (apprentissage et professionnalisation).
En moyenne, la formation est organisée selon un rythme d'une semaine par mois à CESI.

POURSUITE D'ÉTUDES

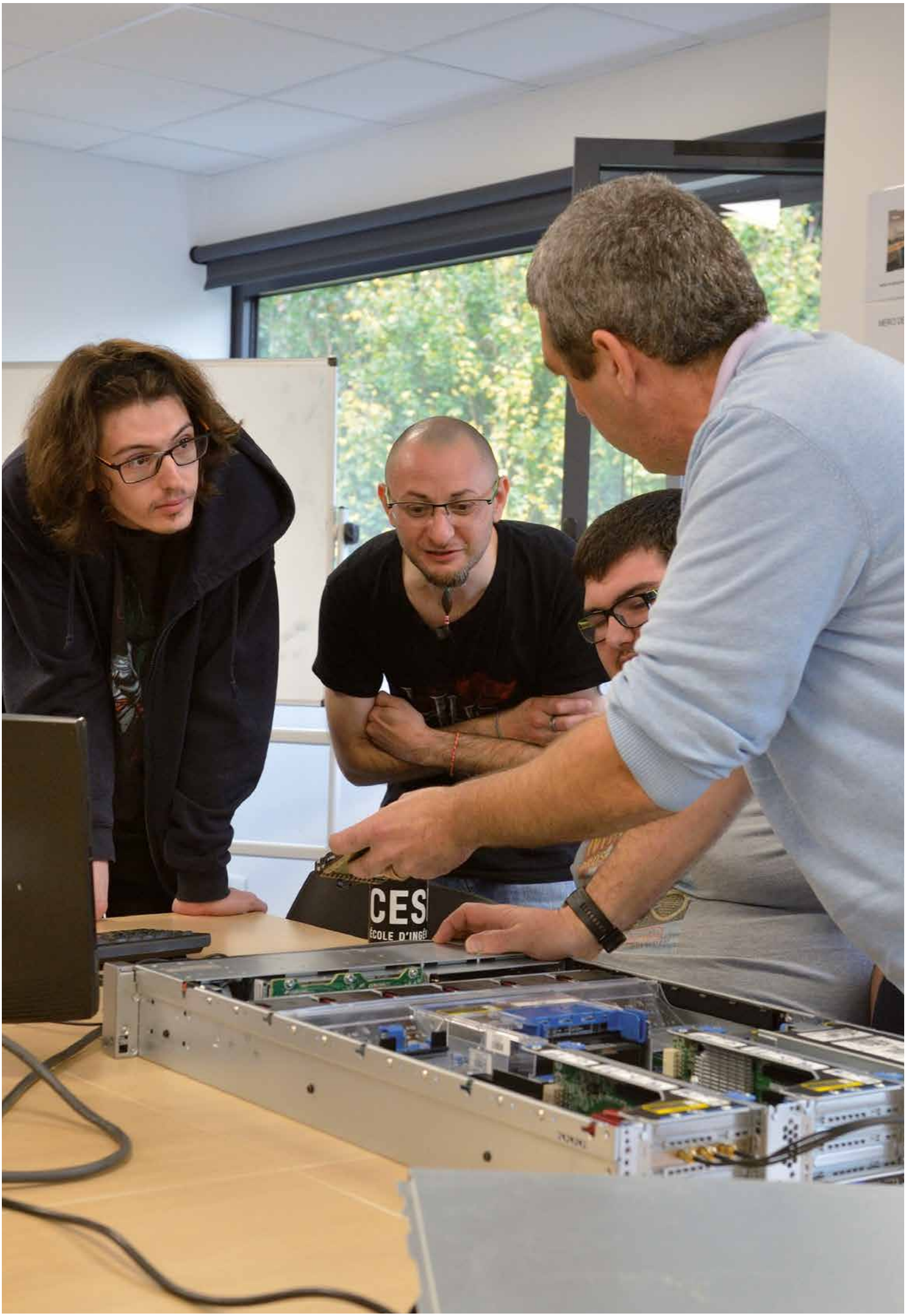
Bachelor Administrateur systèmes et réseaux (Bac +3)

DÉBOUCHÉS PROFESSIONNELS

Technicien supérieur / gestionnaire en maintenance informatique ; Technicien Help desk ;
Technicien informatique ; Technicien support / réseaux

Contact

CESI Campus de Brest
230 rue Roland Garros
29490 Guipavas
02 98 36 06 28
Chargée de relations candidats / entreprises des formations Informatique & Numérique :
Fanélie Kergil / 07 85 59 55 11 / fkergil@cesi.fr



FORMATIONS APRÈS LE BAC

BAC +3

Licence mention Informatique Parcours Ingénierie Informatique – Université de Bretagne Occidentale

OBJECTIFS

Les objectifs de la licence d'informatique sont l'acquisition des compétences fondamentales, méthodes et savoir-faire techniques représentatifs des différentes tâches de la discipline informatique. Cette formation couvre l'ensemble de la discipline informatique : fondements, architecture et matériel, systèmes, méthodes et technologies logicielles, applications informatiques, systèmes d'information.

Le parcours Ingénierie Informatique (II) est un parcours d'une année destiné tout particulièrement aux étudiants titulaires d'un DUT informatique/2ème année de BUT (ou équivalent). Le programme permet de préparer une poursuite d'étude en Master Informatique. La formation comprend des projets et des enseignements technologiques directement reliés aux besoins du marché. Ces enseignements sont complétés par une formation générale destinée à l'insertion professionnelle des étudiants (droit des entreprises, économie, anglais, communication).

Contact
UBO, 3 Rue des Archives,
29238 Brest - 02 98 01 60 00

Licence mention Sciences pour l'ingénieur Parcours ESTR – Université de Bretagne Occidentale

OBJECTIFS

L'objectif du parcours Électronique, Signal, Télécommunications, Réseaux (ESTR) est de dispenser une formation scientifique et technique générale dans les domaines de l'électronique, du Signal, des télécommunications et des Réseaux associée à l'acquisition de compétences transversales (maîtrise d'une langue étrangère, des outils de communication et informatiques).
La première année d'intégration de la Licence SPI est commune. La seconde année constitue le renforcement et permet une orientation progressive.
La troisième année est une année de spécialisation où le parcours ESTR propose trois options :

- option Électronique et Télécoms (ET)
- option Signal et Télécoms (ST)
- option Réseaux et Télécoms (RT)

Ce parcours a pour vocation principale la poursuite d'étude dans l'un des trois Master du département d'Électronique :

- Master « Électronique RadioFréquence et Télécommunication (ET) »
- Master « Signal et Télécommunications (ST) »
- Master « Cybersécurité, Télécoms, Réseaux (CTR) »

Contact
UBO, 3 Rue des Archives, 29238 Brest - 02 98 01 60 00

© École Nationale d'Ingénieurs de Brest (ENIB)

Bachelor Administrateur systèmes et réseaux - CESI campus de Brest

TYPE(S) DE FORMATIONS PROPOSÉES

Formation en alternance - Bac +3

CONDITIONS D'ACCÈS À LA FORMATION

Être titulaire d'un bac +2. Admission sur dossier de candidature, tests de positionnement et entretien de validation. La formation est gratuite et sans aucun frais d'inscription.

Possibilité de formation en entreprise (alternance, apprentissage, stage...).

Alternance (apprentissage et professionnalisation). En moyenne, la formation est organisée selon un rythme d'une semaine par mois à CESI.

DESCRIPTIF

En véritable expert des solutions techniques, l'Administrateur systèmes et réseaux a en charge la conception, la mise en œuvre de l'architecture du système d'information et sa protection.

Il prend en compte l'existant, les besoins et contraintes du client, ainsi que les évolutions technologiques dans le domaine et conçoit une architecture du système d'information adaptée et évolutive. Il propose les infrastructures réseaux, de télécommunication, les serveurs systèmes, les solutions de stockage internes ou externes, les solutions de protection du système d'information répondant aux besoins numériques des entreprises.

Il pilote la mise en œuvre des solutions systèmes et réseaux, avec méthodologie et dans le respect des normes.
Il administre et garantit le fonctionnement de l'infrastructure systèmes et réseaux dans le temps, il anticipe les évolutions nécessaires et met en œuvre les technologies de supervision et les procédures de maintenance adaptées.
Au-delà de ses compétences de conception technique et d'organisation, c'est également un communicant et un animateur, capable d'accompagner l'évolution des compétences digitales au sein de l'entreprise.
Dans le contexte actuel d'explosion quantitative des données numériques, l'Administrateur systèmes et réseaux doit concevoir des architectures performantes, solides, évolutives et sécurisées afin de garantir l'accès, la circulation et le stockage des données. Il met en œuvre les solutions nécessaires pour sécuriser son architecture dans le respect de la politique sécurité définie par le directeur du système d'information.

POURSUITE D'ÉTUDES

Manager en infrastructures et cybersécurité des systèmes d'information (bac +5)

DÉBOUCHÉS PROFESSIONNELS

Administrateur systèmes et réseaux ; Responsable/chef de projets systèmes et réseaux ; Responsable/chef de projets réseaux et télécoms ; Responsable/chef de projets systèmes d'information ; Ingénieur/consultant systèmes et réseaux ; Ingénieur/consultant réseaux

Contact

CESI Campus de Brest - 230 rue Roland Garros,
29490 Guipavas - 02 98 36 06 28
Chargée de relations candidats / entreprises des formations Informatique & Numérique :
Fanélie Kergil / 07 85 59 55 11 / fkergil@cesi.fr

Bachelor Specialized IT (Learn IT, School of Technology) - Brest Open Campus

TYPE(S) DE FORMATIONS PROPOSÉES

Bachelor / BAC+3 SPECIALIZED IT : 2 titres RNCP de niveau 6 en fonction du choix de spécialité : "Chef de projet logiciel et réseau" ou "Concepteur-Développeur d'applications".

CONDITIONS D'ACCÈS À LA FORMATION

- Titulaire du baccalauréat général, professionnel ou équivalent.
- Titulaire d'un Bac+1, toutes les filières, ayant validé 60 ECTS.
- Accès possible par la Validation des Acquis Professionnel (VAP).

DESCRIPTIF

Bachelor SPECIALIZED IT, la 1ère et la 2e année apporte des connaissances et compétences solides dans les domaines de premier niveau suivants : Administration système, Administration réseau, Administration base de données, Programmation applications & solutions. La 3e année du Bachelor IT permet aux étudiants de poursuivre leur apprentissage dans les divers domaines initiés en 1ère et 2e année. Les étudiants ont le choix parmi 2 spécialisations en lien avec leurs projets professionnels respectifs : Spécialisation IT Operations & Infrastructure Administration, ou Spécialisation IT Software & Developments

POSSIBILITÉ DE FORMATION EN ENTREPRISE (ALTERNANCE, APPRENTISSAGE, STAGE...)

- Stage 4 à 6 semaines en 1ère année de Bachelor
- Stage 8 à 10 semaine en 2e année de Bachelor
- Stage ou Alternance possible à partir de la 3e année de Bachelor. Alternance : 3 semaines en entreprise / 1 semaine en cours

POURSUITE D'ÉTUDES

BAC+5 "Manager IT" - Expert en ingénierie du développement et en architecture logicielle.

DÉBOUCHÉS PROFESSIONNELS

Administrateur système, Administrateur réseaux, Développeur concepteur d'applications, Développeur intégrateur, Chargé de projets informatiques, Administrateur bases de données, Chargé des systèmes d'information, Développeur front end, Développeur back end, Chargé de la sécurité informatique

Contact

Contact formation : 02 98 49 22 99
service.admissions@brest-opencampus.com

Barbara Réaux, Responsable des admissions et de la communication
barbara.reaux@brest-opencampus.com

© Pierre-François Watras / Brest métropole

FORMATIONS APRÈS LE BAC

BAC +5 ET PLUS

Master Réseaux et Télécommunications Parcours Télécommunications, Réseaux et Cybersécurité – Université de Bretagne Occidentale

DESCRIPTIF

Le Master Télécommunications, Réseaux et Cybersécurité permet de former des diplômés ayant acquis les connaissances théoriques et les compétences pratiques pour s'insérer aisément dans les métiers de l'informatique, des télécommunications, des réseaux et de la cybersécurité.

Ce parcours est construit sur quatre disciplines fortement techniques que sont les Télécommunications, les Réseaux, l'Informatique et la Cybersécurité. Les disciplines enseignées se composent pour moitié d'enseignement théoriques et de spécialité et pour l'autre moitié d'enseignements pratiques (travaux pratiques, mini-projets et projets longs). Les diplômés sont ainsi à même de maîtriser les technologies actuelles et de demain dans chacune de ces disciplines. Le master TRC est reconnu en tant que formation en cybersécurité au niveau national.

Le Master Télécommunications, Réseaux et Cybersécurité fait preuve d'un partenariat fort avec les industriels locaux et régionaux. **La formation est ouverte à l'alternance** permettant ainsi une professionnalisation continue entre l'entreprise et les enseignements dispensés à l'université (par période de trois à quatre semaines).

POURSUITE D'ÉTUDES

Bien que particulièrement professionnalisante, la formation offre les fondamentaux pour une poursuite d'études en doctorat. Le stage de 6 mois se déroulant en fin de cursus peut donc être effectué indistinctement en laboratoire ou en entreprise.

COMPÉTENCES ACQUISES

Cybersécurité :

- Concevoir et déployer une politique de sécurité
- Réaliser un cycle de vie sécurisé d'un développement logiciel
- Mettre en œuvre des stratégies de défense
- Réaliser des analyses de risque en suivant les normes ISO 2700X
- Détecter et réagir aux attaques
- Mettre en œuvre un plan de continuité d'activités

Contact

UBO, 3 Rue des Archives,
29238 Brest - 02 98 01 60 00

Ingénieur généraliste – IMT Atlantique

CONDITIONS D'ACCÈS À LA FORMATION

Bac + 2 Concours Commun Mines Ponts, AST GEI UNIV

Possibilité de formation en entreprise : stage, césure

Poursuite d'études : doctorat

DÉBOUCHÉS PROFESSIONNELS

Possibilité de colorer son parcours d'une expertise en lien avec votre projet d'avenir (cybersécurité, santé, intelligence artificielle, nucléaire, data, énergie...). Après une admission sur le Concours commun Mines Ponts, vous intégrez une formation d'ingénieur généraliste qui vous dote des compétences scientifiques et des soft skills indispensables aux ingénieurs agiles et responsables recherchés par les entreprises.

Contact admission@imt-atlantique.fr

Ingénieur spécialisé Informatique, réseaux et télécommunications – IMT Atlantique

CONDITIONS D'ACCÈS À LA FORMATION

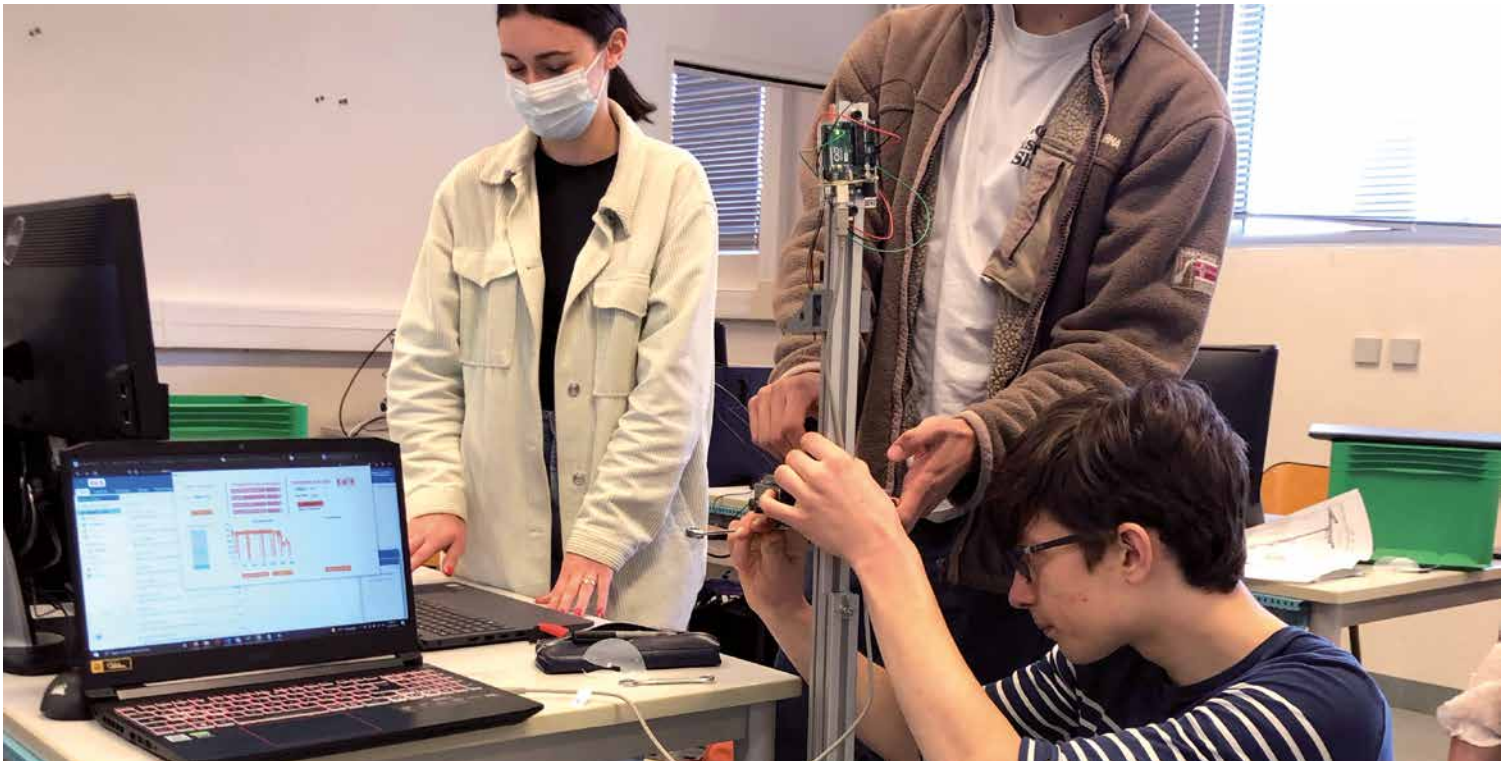
La formation est ouverte aux titulaires de BAC+2, en particulier les étudiant.e.s issu.e.s d'un DUT Réseaux et Télécoms, Informatique, Génie Electrique et Informatique industrielle, Mesures Physiques, d'un BTS Systèmes numériques, d'une L3 scientifique ou encore étudiant.e.s en classe préparatoire.

Possibilité de formation en entreprise par alternance.

DÉBOUCHÉS PROFESSIONNELS

Ce cursus par apprentissage d' IMT Atlantique vise à former des ingénieurs diplômés de haut niveau, opérationnels et à large spectre technique couvrant l'informatique, les réseaux et les télécommunications. Il prépare aux métiers d'architecture et d'ingénierie des systèmes et réseaux d'information et de communication, ainsi qu'aux fonctions managériales et à l'international.

Contact admission@imt-atlantique.fr



Manager en infrastructures et cybersécurité des systèmes d'information – CESI Campus de Brest

DESCRIPTIF

Manager en infrastructures et cybersécurité des systèmes d'information : Le Manager en systèmes d'information - Expert infrastructures et cybersécurité participe à la performance et à l'optimisation du système d'information à travers l'évolution et la gestion des priorités des projets informatiques dans le respect des orientations stratégiques de l'entreprise.

Pour mener à bien sa mission, sa fonction exige une compréhension des axes de développement stratégique de son entreprise, une bonne connaissance du système d'information, une vision globale des projets informatiques ainsi qu'une expertise technique. Il développe donc plusieurs compétences métiers et une forte expertise technique.

En tant qu'architecte du système d'information et expert en cybersécurité, il garantit la cohérence technique, la sécurité et la pérennité du système d'information. Il est amené à faire évoluer la plateforme technique d'une entreprise et la sécuriser, voire la refondre complètement notamment avec les offres cloud actuelles.

À partir du besoin client (interne ou externe), d'une analyse des risques cybers existants et dans le respect des règlementations en vigueur, il traduit les attentes en solutions informatiques et identifie les composants impactés (logiciels, matériels, processus, données). Il s'enquiert des techniques disponibles et pertinentes sur le marché auprès d'experts et de fournisseurs pour ensuite déterminer un plan d'évolution, de sécurisation et d'intégration tout en s'engageant sur une qualité et une continuité de service.

Enfin, il manage le suivi de la réalisation, apporte des modifications si besoin et garantit la cohésion de l'ensemble du système. En tant que manager d'équipes, il veille plus précisément au respect des délais et du budget, et à la gestion des équipes concernées (sous sa responsabilité hiérarchique directe ou fonctionnelle). Il est responsable au quotidien de l'avancée des projets et supervise le portefeuille de projets. Il coordonne et supervise les résultats des équipes projets informatiques et anime celles-ci.

CONDITIONS D'ACCÈS À LA FORMATION

Être titulaire d'un bac +3/+4 (ou d'un niveau 6 équivalent). Admission sur dossier de candidature, tests de positionnement et entretien de validation. La formation est gratuite et sans aucun frais d'inscription.

POSSIBILITÉ DE FORMATION EN ENTREPRISE (ALTERNANCE, APPRENTISSAGE, STAGE...)

Alternance (apprentissage et professionnalisation).
En moyenne, la formation est organisée selon un rythme d'une semaine par mois à CESI.

DÉBOUCHÉS PROFESSIONNELS

Architecte du système d'information ; Urbaniste des systèmes d'information ; Directeur/responsable informatique ; Responsable sécurité des systèmes d'information ; Ingénieur en cybersécurité ; Expert technique ; Chef de projet informatique/ maîtrise d'œuvre; Manager du système d'information ; Consultant en système d'information/sécurité

Contact

CESI Campus de Brest
230 rue Roland Garros
29490 Guipavas
02 98 36 06 28
Chargée de relations candidats / entreprises des formations Informatique & Numérique :
Fanélie Kergil / 07 85 59 55 11 / fkergil@cesi.fr

Ingénieur – École Nationale d'Ingénieurs de Brest (ENIB)

TYPES DE FORMATIONS PROPOSÉS

L'ENIB propose de nombreux double- parcours :

- Diplôme Universitaire en Entrepreneuriat, avec le PEPITE Bretagne.
- Double diplôme en Management et administration des entreprises « Ingénieur Manager », avec l'UBO.
- Quatre Masters en Informatique, Ingénierie de conception, Physique fondamentale et applications, Télécommunications (Bac + 5).

Une trentaine de parcours à l'international donnant lieu à un deuxième diplôme.

DESCRIPTIF

Volet sécurité numérique de la cybersécurité :

- Sécurisation de base des réseaux informatiques (parefeu, routage)
- Chiffrement
- règles de programmation sécurisées (C/C++/python)
- Conférence sur la sensibilisation des risques numériques en 3e année.
- 2 « Capture the flag » abordés en module optionnel MSI (Méthodologie pour le développement des systèmes d'information).
- Bases de cybersécurité dispensées dans le tronc commun du S7, via le module CRS (communication réseaux et systèmes) afin que certaines ou certains poursuivent, après l'ENIB, des études dans une formation spécialisée en sécurité des systèmes d'information.

CONDITIONS D'ACCÈS À LA FORMATION

Recrutement post-Bac sur concours Geipi Polytech

Recrutement post-Bac+2 sur concours groupe ENI (ingenieur-eni.fr), concours CPGE Banque

PT (banquept.fr) et concours L2 ou L3 Pass'ingénieur (passingenieur.scei-concours.fr).

POSSIBILITÉ DE FORMATION EN ENTREPRISE (ALTERNANCE, STAGES, APPRENTISSAGE…)

- Table ronde (intersemestre 1) – des ingénieurs en activité
- Rencontrent les élèves de première année
- Journée entreprises – La JEREE
- 15 mois de stages en 4 ans à partir de la 2e année
- Alternance sous forme de contrat de professionnalisation en 5e année
- 70 entreprises partenaires
- Établissement membre du pôle « Pépite Bretagne »

POURSUITE D'ÉTUDES

Deux parcours de Doctorats en sciences pour l'ingénieur et en sciences et techniques de l'information et de la communication (Bac + 8)

DÉBOUCHÉS PROFESSIONNELS

Le spectre des emplois accessibles aux diplômés de l'ENIB est très large : de la production au bureau d'études, de la recherche à la gestion de projet, du management d'équipe au conseil en technologies, en passant par la cybersécurité, etc.

Contact(s)

Fanny Leboucher : responsable communication - fanny.leboucher@enib.fr - Tél. 02 98 05 66 39

Ingénieur APRÈS PARCOURS « CYBERSÉCURITÉ » – ISEN Ouest

DESCRIPTIF

Ingénieur ISEN ayant suivi le parcours « Cybersécurité »
Le domaine cybersécurité est proposé aux étudiants au niveau Master 1. Il dure 2 ans.
Au préalable, les étudiants suivent généralement un cycle de 3 ans intitulé « Informatique et Réseaux ».
Pour autant, tous les cycles post-bac proposés par l'école permettent d'intégrer le domaine « Cybersécurité ».

CONDITION D'ACCÈS À LA FORMATION

Les étudiants de l'ISEN sont recrutés en très grande majorité en première année post-bac après un concours d'entrée national commun à plusieurs écoles d'ingénieurs « Concours Puissance Alpha ».

POSSIBILITÉ DE FORMATION EN ENTREPRISE

90 % des étudiants choisissent de faire leur dernière année d'études (Master 2) en contrat de professionnalisation. Il ne s'agit pas d'une obligation, mais la grande majorité des étudiants fait ce choix. Les principaux avantages de ce contrat sont que les frais de scolarité sont pris en charge par l'entreprise qui accueille l'étudiant, l'étudiant est rémunéré durant cette année et se voit généralement proposé un poste dans l'entreprise qui l'a accueilli à l'issue de son année de contrat de professionnalisation.

POURSUITE D'ÉTUDES

La poursuite d'études dans le domaine de la recherche scientifique est possible (Doctorat).

DÉBOUCHÉS PROFESSIONNELS

Tous les secteurs du numérique sont concernés par la cybersécurité. Plus largement tous les secteurs de l'industrie proposent des postes liés à la protection de leurs infrastructures et services numériques.

94 % des diplômés ISEN trouvent un emploi en moins de 2 mois. 98 % en moins de 5 mois.

92 % des étudiants ISEN travaillent ensuite dans la région où ils ont été formés.

Le salaire brut moyen 2 ans après la diplomation est de 42 000€.

(enquête indépendante de la Conférence des Grandes écoles menée sur les diplômés ISEN de la promotion 2021).

Contact

Vincent Derrien, Directeur de la Communication ISEN,
vincent.derrien@isen-ouest.yncrea.fr

Ingénieur – ENSTA BRETAGNE

L'ENSTA Bretagne propose des formations d'ingénieurs généralistes, formations d'ingénieurs par alternance (apprentissage), masters, mastères spécialisés et doctorats.

DESCRIPTIF

Plusieurs des diplômes délivrés à bac+5, bac+6 et bac+8 portent sur l'ingénierie de conception de systèmes numériques complexes à haute performance, robustes, fiables et durables :

1/ Formation d'ingénieur généraliste, sous statut étudiant ou militaire (cycle FISE), en particulier pour les spécialités "conception de systèmes numériques", "robotique mobile autonome", "systèmes d'observation et IA" (bac+5 : 3 ans de formation, après bac+2) ;

2/ Formation d'ingénieurs spécialisés en conception de systèmes embarqués (cycle FIPA), par alternance, sous statut apprenti ou salarié, (bac+5 : 3 ans de formation, après bac+2) ;

3/ Master "architecture et sécurité des systèmes électroniques et logiciels" (bac+5 : 2 ans de formation après bac+3) ;

4/ Doctorat en sciences et technologies de l'information et de la communication "software and hardware, architectures and processes" (bac+8 : 3 ans de thèse après bac+5)

CONDITIONS D'ACCÈS AUX FORMATIONS

1/ Accès sur concours (après math sup/math spé) ou sur titre (bac+3/4).

2/ Accès sur dossier après bac+2/3 (BUT, BTS ou prépa).

3/ Accès sur dossier après bac+3/4.

4/ Accès sur dossier après bac+5 (M2, diplôme d'ingénieur) ou expérience professionnelle équivalente.

5/ Accès sur dossier après bac+5 (M2, diplôme d'ingénieur).

POSSIBILITÉ DE FORMATION EN ENTREPRISE (ALTERNANCE, APPRENTISSAGE, STAGE DE LONGUE DURÉE...)

Effective pour les 5 formations :

1/ stages au cours de chacune des 3 années de formation, notamment le stage de 6 mois (projet de fin d'études) en dernière année, possibilité de contrat de professionnalisation en entreprise en dernière année et possibilité de faire une année de césure pour mener un ou plusieurs stages complémentaires ;

2/ formation de 3 ans alternant séquences académiques en école et séquences professionnelles en entreprises (sous contrat, en tant qu'apprenti ou salarié en formation continue) ;

3/ stage long (5 à 6 mois) de thèse professionnelle en 2e année

4/ stage long (5 à 6 mois) de thèse professionnelle ;

5/ Possibilité de CIFRE (convention industrielles de formation par la recherche) permettant d'effectuer 3 années de thèse dans le cadre d'un contrat avec une entreprise.

POURSUITE D'ÉTUDES

- Doubles diplômes en France et à l'international.

DÉBOUCHÉS PROFESSIONNELS

Dans tous les domaines d'application, civils et militaires, informatisés et communicants, où les systèmes logiciels doivent être fiables et robustes face aux risques d'attaques.

Exemples :
- industrie navale et énergies marines
- défense & sécurité
- numérique
- aéronautique & espace
- transports et mobilités terrestres
- recherche
- santé

Contact
admission@ensta-bretagne.fr

MBA MANAGER IT (Learn IT, School of Technology) - Brest open Campus

TYPE(S) DE FORMATIONS PROPOSÉES

BAC+5 : MBA : MANAGER IT : 1 titre RNCP niveau 7 - "Expert en ingénierie du développement et en architecture logicielle"

DESCRIPTIF

Le MBA "Manager IT" permet aux étudiants de poursuivre leur apprentissage à la suite de leur Bachelor.
Ils ont la possibilité de choisir parmi 2 spécialisations en lien avec leurs projets professionnels respectifs dès la 1ère année du MBA : Expertise IT Operations Expert (système, infrastructure, architecture et cybersécurité) ou Expertise IT Solutions Expert (applications, solutions et data management). La 2e année du MBA MANAGER IT permet aux étudiants d'approfondir encore d'avantage leurs expertises dans une approche plus globale et managériale, et de choisir parmi 2 options très demandées :
Expertise IT Operations Manager (système, infrastructure, architecture et cybersécurité). Expert IT Solutions Manager (applications, solutions et intelligence artificielle)

CONDITIONS D'ACCÈS À LA FORMATION

Titulaire d'un Bac+3, toutes filières, ayant validé 180 ECTS.
Accès possible par la Validation des Acquis Professionnel (VAP)

POSSIBILITÉ DE FORMATION EN ENTREPRISE (ALTERNANCE, APPRENTISSAGE, STAGE...)

Alternance : 3 semaines en entreprise / 1 semaine en cours ; ou stage en entreprise si parcours en initial

DÉBOUCHÉS PROFESSIONNELS

Le Cycle supérieur Ingénierie informatique prépare aux nombreux métiers de niveau bac+5, et notamment : Ingénieur(e) en informatique, Architecte en système d'information, Responsable de la sécurité des systèmes d'information (RSSI), Directeur(trice) des systèmes d'information (DSI), Directeur(trice) de projet informatique, Expert réseaux, Consultant en systèmes d'information, Manager de projet ERP, Chief Data Officer

Contact
- Margaux Nenny, Responsable des admissions
  margaux.nenny@brest-opencampus.com

- Contact formation : 02 98 49 22 99
  service.admissions@brest-opencampus.com

© Pierre-François Watras / Brest métropole

FORMATIONS SPÉCIALISÉES

Développeur-se en intelligence artificielle - École IA Microsoft By Simplon X ISEN

DESCRIPTIF

Le développeur et la développeuse en IA est un spécialiste du développement d'applicatifs informatiques autour de l'IA et de la Data Science. Intégré dans la résolution d'une problématique métier définie par l'organisation, son rôle est de développer des solutions informatiques utilisables par des spécialistes et des non-spécialistes, intégrant directement ou indirectement des briques d'Intelligence Artificielle (par exemple : algorithmes de Machine Learning). Il conçoit, teste et adapte les applicatifs intégrant tout ou partie de ces technologies.

Il/elle est donc spécialiste du développement informatique, du génie logiciel et des interfaces Hommes-Machines, avec une très bonne connaissance des technologies d'IA/Data Science, du secteur ou de la fonction d'application des données traitées.

La formation est ouverte à toute personne inscrite en tant que demandeur et demandeuse d'emploi.

Le titre RNCP à finalité professionnelle est accessible par la VAE, si vous avez déjà une expérience solide en intelligence artificielle.

Formation et passage des certifications gratuits pour les bénéficiaires grâce aux entreprises partenaires financeurs de la formation et aux fonds de financement de la formation professionnelle. (Pour les financeurs de la formation professionnelle des demandeurs d'emploi : 16 € à 25 € de l'heure selon la qualification visée et l'accompagnement à mobiliser).

Contact

Estelle Busse – ebusse@simplon.co

CONTACTS

Brest métropole
24 rue Coat-ar-Guéven
CS 73826
29238 Brest Cedex 2

Laurent Bonnaterre
Responsable de l'Unité Relations Presse
(+33)2 98 00 82 05
laurent.bonnaterre@brest-metropole.fr

Terry Guiziou
Attaché de presse
terry.guiziou@mairie-brest.fr
(+33)6 83 55 73 45

Éric Vandenbroucke
Directeur du développement économique
et international
promotion-economique@brest-metropole.fr
+33 (0)2 98 33 50 50
www.brest.fr

Unité Relations Presse Brest métropole
Photo couverture : © Pierre-François Watras / Brest métropole