

**FIC**  
**2020**  
28-29-30 JANVIER

Dossier de presse  
**Pavillon Bretagne / Pôle d'excellence cyber**  
Stand D15

**BRETAGNE**<sup>BE</sup>  
DÉVELOPPEMENT  
INNOVATION



PÔLE D'EXCELLENCE  
**CYBER**

**BRETAGNE**<sup>BE</sup>



### À propos du Forum international de la cybersécurité (FIC)

Installé depuis 11 ans dans le paysage, le FIC est devenu le rendez-vous incontournable des acteurs de la cybersécurité. Un taux de fréquentation en forte augmentation tous les ans et un visitorat de plus en plus qualitatif.

#### Les chiffres clés de l'édition 2019

- › Près de 10 000 visiteurs (+15% /2019),
- › 400 intervenants,
- › 120 conférences / ateliers / démonstrations
- › 80 pays représentés (+20% de visiteurs internationaux /2019)

## ► SOMMAIRE

- › Communiqué de presse page 4
- › Pôle d'excellence cyber page 6
- › Bretagne : La cybersécurité a son territoire page 7
- › L'offre cyber bretonne : des solutions adaptées à coût maîtrisé page 8
- › Deux métropoles qui comptent dans l'espace cyber breton page 12
- › Formation - Recherche : Acquérir de nouvelles compétences page 14
- › Europe : La Bretagne, Cyber valley européenne page 16
- › Bretagne : Point de départ vers l'international page 18
- › Mobilisation BreizhCOP page 18
- › 32 exposants bretons au Forum International de la Cybersécurité 2020 page 19

## ► COMMUNIQUÉ DE SYNTHÈSE

### **FIC 2020 : AVEC LE POLE D'EXCELLENCE CYBER, LA REGION BRETAGNE CONFIRME SON LEADERSHIP EN CYBERSECURITE DU 28 AU 30 JANVIER 2020 AU GRAND PALAIS À LILLE**

Lors de la 12<sup>e</sup> édition du Forum international de la cybersécurité (FIC), la Bretagne viendra faire valoir son rôle de leader français dans la création de startups cyber. Le pavillon collectif (D15), composé de 20 entreprises, 5 structures académiques et 2 métropoles, se distinguera par une très forte présence de jeunes pousses (13 sur les 20 entreprises exposantes).

Ces 27 exposants seront accompagnés par Bretagne Développement Innovation et exposeront leur savoir-faire aux côtés du Pôle d'excellence cyber. Toute la communauté cyber bretonne sera au rendez-vous du FIC pour un panorama des solutions, formations et briques innovantes de cybersécurité.

Du 28 au 30 janvier au FIC de Lille, le pavillon Bretagne proposera des démonstrations de solutions innovantes et des rencontres avec les acteurs qui comptent dans la cybersécurité.

Sur ce stand collectif, le public de professionnels trouvera des réponses très concrètes à des questions telles que : Comment identifier et détecter ses vulnérabilités ? Comment se protéger des cyber-attaques, que faire en cas d'incident ?

Les exposants du plateau démontreront que, quelles que soient les problématiques de sécurité, l'offre cyber en Bretagne propose des solutions adaptées à un coût maîtrisé.

#### Au FIC, le Pôle d'excellence cyber renouvelle son partenariat avec la Région

Depuis 2014, le Pôle d'excellence cyber, cofondé avec le ministère des Armées, développe une stratégie nationale autour de la formation, de la recherche et du développement industriel, dans un esprit de décloisonnement, de fédération et d'animation de la filière.

Au FIC 2020, il renouvelle son partenariat avec la Région Bretagne, pour valoriser le savoir-faire de ses membres (une cinquantaine aujourd'hui, qu'ils soient civils ou militaires, publics ou privés, académiques ou industriels) et présenter plusieurs de ses projets, au profit de la communauté nationale cyber, à l'exemple de son référentiel ou encore de sa « *Cyber Training Lab Academy* » (plateforme partagée de travaux pratiques).

#### La Bretagne au FIC 2020 : une majorité de startups et des nouveaux venus

Coordonné par Bretagne Développement Innovation, le plateau sera le lieu de convergence des enjeux de formation, de recherche et de développement industriel. Renouvelé de moitié par rapport à l'édition 2019, le stand (D15) accueillera 10 nouveaux exposants.

##### ► Le pavillon (stand D15) rassemblera les exposants suivants :

- 20 entreprises dont 13 startups : *Alcyconie*, 35 ; *Anozr Way*, 35 ; Anteo Trust & Security by Sodifrance, 35 ; *Assurable / Obdo*, 35 ; *Bloo Conseil*, 35 ; *By Stamp*, 56 ; *Cailabs*, 35 ; *Daspren*, 35 ; *Dawizz*, 56 ; *Easyliance*, 35 ; Groupe SII, 35 ; *Hogo*, 35 ; *Lorcyber*, 56 ; *Malizen*, 35 ; *Rubycat*, 35 ; *Secure-IC*, 35 ; *SIB*, 35 ; *Synacktiv*, 35 ; *Veyan*, 56 ; *WaToo*, 29.
- en italique, les startups
- en gris, les nouveaux exposants

- 5 centres de recherche ou écoles d'enseignement supérieur : Cyber Security Center de l'Université Bretagne Sud (56), IMT Atlantique (35), INRIA (35), Pôle Sup de La Salle (35), Université de Rennes 1 et la Cyberschool (35).

- 2 métropoles : Brest Métropole ; Destination Rennes Business Services

##### ► Les autres entreprises bretonnes au FIC

Cinq autres entreprises bretonnes seront présentes au FIC 2020 sur leur propre stand : Acklio, 35 (stand F19) ; Amossys, 35 (stand D1) ; Cardelya, 35 (stand G23) ; Diateam, 29 (stand B10) ; Shadline, 35 (stand D32).

#### La Bretagne ouvre les portes de l'Europe et de l'international

Pour la première fois sur le plateau Bretagne au FIC, un espace business sera consacré à l'international. Il sera matérialisé par 3 guichets représentant les pays suivants : Allemagne, Singapour, Royaume-Uni.

Cette action a un double objectif : faire rayonner l'offre cyber bretonne auprès des relais étrangers (agences de développement économique, clusters...) et ouvrir des nouveaux marchés aux entreprises régionales.

Pendant 3 jours, les entreprises exposantes et les représentants de ces pays pourront échanger sur le pavillon. Les entreprises pourront ainsi mieux comprendre les caractéristiques de ces marchés internationaux et comment y accéder : les portes d'entrée à identifier, les opportunités à saisir...

La Bretagne mettra à disposition de l'ensemble des exposants ses guichets internationaux.

#### Rennes et Brest, deux métropoles qui comptent dans l'espace cyber breton

Rennes est devenue en quelques années le haut lieu de la cybersécurité et de la cyberdéfense en France. Laboratoires, établissements d'enseignement supérieur, PME, grands groupes... Selon l'Audiar (Agence d'urbanisme de Rennes Bretagne), le territoire compte aujourd'hui plus de 3 400 emplois dans ce domaine, 1 000 étudiants formés à la cybersécurité et 150 chercheurs au sein d'un écosystème en constante évolution.

Au cœur d'une région en pointe, c'est naturellement que Brest oriente son expertise dans la cyber maritime et portuaire au service de nombreux terrains opérationnels civils et militaires : fonctions maritimes internationales, base opérationnelle de la force océanique stratégique, port civil de premier plan en matière de réparation navale, préfecture maritime, siège national du Service hydrographique de la marine (SHOM) et de l'Institut français de recherche pour l'exploitation de la mer (IFREMER).

Accompagnée d'acteurs académiques et industriels aux compétences fortes sur le sujet, Brest dispose d'atouts qui confirment son positionnement stratégique dans ce secteur.

Cette dynamique est portée par Bretagne Développement Innovation (BDI), l'agence de développement économique et d'innovation de la Région Bretagne. Sur le champ de la cybersécurité, BDI développe des actions autour de 4 axes :

- Faciliter l'accès des PME bretonnes aux marchés de la cybersécurité, en France et à l'international.
- Diffuser la cybersécurité dans des filières applicatives (industries de la mer, agroalimentaire, de la santé, mobilité...).
- Animer la communauté des acteurs.
- Garantir l'attractivité du territoire.

##### Dates-clés de la cyber en Bretagne :

- BreizhCTF 2020 : 3 avril, Rennes,
- European Cyber Week : 17-19 novembre, Rennes.

# PÔLE D'EXCELLENCE CYBER



## FAIRE CONVERGER LES COMPÉTENCES

Créé en 2014 à l'initiative conjointe du ministère des Armées et de la Région Bretagne, le Pôle d'excellence cyber porte l'ambition d'accélérer la construction d'une filière en cybersécurité-cyberdéfense souveraine par la fédération de l'ensemble des acteurs de l'écosystème français.

Le Pôle d'excellence cyber structure son action de fédération, d'animation et de décloisonnement autour de trois axes principaux :

- > La formation (initiale, continue, supérieure) ;
- > Le développement industriel ;
- > La recherche.

Le Pôle d'excellence cyber répond ainsi à trois enjeux majeurs, au profit de la communauté nationale de cybersécurité et de cyberdéfense :

- > Disposer d'une offre en formation adaptée aux besoins des services de l'État, de l'industrie et des sociétés de services ;
- > Disposer de produits et de services de confiance ;
- > Disposer d'une offre de recherche en adéquation avec les besoins des ministères et des industriels.

## UN MODÈLE ORIGINAL D'ORGANISATION HORIZONTALE, COLLABORATIVE ET EN RÉSEAU

Le Pôle d'excellence cyber regroupe des acteurs civils et militaires, publics et privés, académiques et industriels, en s'appuyant sur leurs compétences et champs d'action respectifs.

L'ensemble des membres et partenaires du Pôle d'excellence cyber se réunissent périodiquement à l'occasion de groupes de travail thématiques transversaux, permettant un haut degré de concertation dans le développement de leurs actions.

Les actions concrètes du Pôle d'excellence cyber sont :

- > La mise en place de formations (initiale, continue, supérieure) en cybersécurité ;
- > Le rapprochement des acteurs de la filière et la promotion à l'international, comme à l'occasion de la European Cyber Week ;
- > Une participation aux actions de recherche de ses membres (création de chaires industrielles de cyberdéfense, financement de thèses, post-doctorat et séminaires scientifiques).

# BRETAGNE <sup>BE</sup>

## LA CYBERSÉCURITÉ — A SON TERRITOIRE

Région numérique de premier plan, la Bretagne s'impose comme un précurseur et un acteur de référence dans le domaine de la cybersécurité en France et en Europe.

La Bretagne s'appuie sur un écosystème performant avec des entreprises reconnues internationalement, des équipes de recherche basées dans les meilleures écoles, les équipes cyber du ministère des Armées (Pôle d'excellence cyber, DGA, CALID etc.), la présence de grands donneurs d'ordre et de PME performantes.



**3 500** ÉTUDIANTS/AN  
FORMÉS À LA CYBERSÉCURITÉ



**+ DE 200**  
CHERCHEURS SPÉCIALISÉS



**150** ENTREPRISES



**50** PURE PLAYERS



**8 000** EMPLOIS

[www.bdi.fr/annuairecyber](http://www.bdi.fr/annuairecyber)

## ► L'OFFRE CYBER BRETONNE : DES SOLUTIONS ADAPTÉES À COÛT MAÎTRISÉ

Pour clarifier l'offre cyber bretonne, 3 parcours thématiques ont été imaginés pour permettre aux visiteurs du FIC d'identifier rapidement les exposants pouvant répondre à leurs besoins. L'objectif est de démontrer qu'il existe une solution bretonne à coût maîtrisé à chaque question de sécurité qui se pose, que ce soit en amont, pendant ou après un incident :

### 1/3 IDENTIFIER ET DÉTECTER POUR MIEUX ANTICIPER

**Social engineering, phishing, négligence... quand la faille vient de l'intérieur de l'entreprise et que l'humain en est le principal vecteur, comment anticiper en mettant les bonnes protections ?**

La sécurité à 100%, ça n'existe pas ! Le plus souvent, les entreprises doivent faire des choix sur ce qu'elles doivent sécuriser en priorité au sein de leur système d'information (SI).

Ces choix se font toujours dans un compromis entre la sécurité et ce qu'elle coûte à l'entreprise. Avant de faire les bons choix, l'entreprise doit d'abord identifier où elle va mettre la sécurité. Qu'est-ce qui est la donnée sensible pour elle ? Qu'est-ce qui est critique ? La réponse ne sera pas la même en fonction des métiers ou des secteurs d'application.

En moyenne, un incident de sécurité prend 100 jours avant d'être détecté par l'entreprise qui est attaquée. Pendant ce laps de temps, le SI subit des dommages qui sont hors de contrôle de l'entreprise.

**La capacité d'identifier où se trouvent ses données sensibles permet à l'entreprise de reprendre le contrôle.**

En Bretagne, sur 150 entreprises de la cyber, environ la moitié (70) peut répondre à ce besoin d'identifier et de détecter. Ces entreprises vont apporter du conseil et des solutions permettant de :

- > cartographier un système de données,
- > analyser les signaux faibles pour détecter les incidents,
- > mettre des priorités sur les données.

En cyber, ce niveau d'accompagnement correspond à la brique « *Security by design* », c'est-à-dire un accompagnement très en amont de l'incident. Car, plus on intervient en amont et plus la maîtrise des conséquences d'une attaque sera grande.

### Les entreprises bretonnes présentes au FIC 2020 sur cette thématique :

| Nom de la structure                        | Activités   | Contact   |
|--|---|---|
| Anozr Way (35)                             | ANOZR WAY est un éditeur de logiciels qui propose aux entreprises de compléter leur dispositif de sécurité, en se protégeant des risques d'attaques d'origines cyber ciblant les failles humaines. Sa technologie d'OSINT (open source intelligence) permet d'identifier et d'anticiper les scénarii d'attaques (phishing, ransomware, usurpation d'identité, fuite de données...). | <b>Philippe LUC</b><br>Chief Executive Officer (CEO)<br><a href="mailto:philippe@anozrway.com">philippe@anozrway.com</a><br>► <a href="http://www.anozrway.com">www.anozrway.com</a>                            |
| Anteo Trust & Security, by Sodifrance (35) | Le pôle Cybersecurity de Sodifrance conseille et accompagne ses clients dans : leur conformité, au regard d'obligations réglementaires (RGS, RGPD, ISO etc.), la sécurisation de leurs services et applications, la protection de leurs données.  | <b>Hervé TROALIC</b><br>Directeur de pôle Cybersecurity - Groupe Sodifrance<br><a href="mailto:htroalic@sodifrance.fr">htroalic@sodifrance.fr</a><br>► <a href="http://www.sodifrance.fr">www.sodifrance.fr</a> |
| Assurable / Obdo (35)                      | Assurable / Obdo développe une technologie brevetée de SCaaS (Secure Container as a Service) et une suite logicielle applicative permettant de fournir aux entreprises un environnement de gestion de la donnée nativement hautement sécurisé.  | <b>Frankie ALSON</b><br>CEO<br><a href="mailto:falson@obdo.co">falson@obdo.co</a><br>► <a href="https://obdo.co">https://obdo.co</a>  |
| Bloo Conseil (35)                          | Cabinet d'experts indépendants en infrastructure et cybersécurité pour accompagner les projets de transformation et de sécurisation des infrastructures informatiques.  | <b>Aurélien MAGNIEZ</b><br>Président<br><a href="mailto:amagniez@bloo-conseil.fr">amagniez@bloo-conseil.fr</a><br>► <a href="http://www.bloo-conseil.fr">www.bloo-conseil.fr</a>                                |
| Dawizz (56)                                | Dawizz est spécialisée dans la gouvernance de la donnée. Éditrice du logiciel MyDataCatalogue, une solution intelligente basée sur des algorithmes de reconnaissance sur des données structurées ou non.  | <b>Stéphane LE LIONNAIS</b><br>Co-founder<br><a href="mailto:stephane.lelionnais@dawizz.fr">stephane.lelionnais@dawizz.fr</a><br>► <a href="http://www.dawizz.fr">www.dawizz.fr</a>                             |
| Groupe SII (35)                            | Le groupe SII relève quotidiennement les défis technologiques de la transformation numérique des grands comptes, des PME-PMI et Start-Ups avec ses 8 000 collaborateurs présents sur plus de 60 implantations dans le monde.  | <b>Eric HILLY</b><br>Responsable Practice CyberSécurité<br><a href="mailto:ehilly@sii.fr">ehilly@sii.fr</a><br>► <a href="http://www.groupe-sii.com">www.groupe-sii.com</a>                                     |
| Lorcyber (56)                              | Lorcyber, spécialiste de la "sécugérance", propose aux PME et aux collectivités de co-construire leur cyber-sécurité. Lorcyber optimise la sécurité des systèmes d'information, tout en diminuant les coûts grâce à l'industrialisation.  | <b>Pierre LORCY</b><br>Président<br><a href="mailto:pierre.lorcy@lorcyber.eu">pierre.lorcy@lorcyber.eu</a><br>► <a href="http://www.lorcyber.eu">www.lorcyber.eu</a>  |
| Malizen (35)                               | Malizen a pour mission de combiner les dernières avancées en visualisation et en analyse de données pour donner aux experts en cybersécurité le pouvoir d'exercer leur savoir-faire de façon décuplée, accélérée et naturelle.  | <b>Christopher HUMPHRIES</b><br>CEO & Co-founder<br><a href="mailto:christopher@malizen.com">christopher@malizen.com</a><br>► <a href="http://www.malizen.com">www.malizen.com</a>                              |
| Synactiv (35)                              | Sécurité offensive, test d'intrusion, d'audit de sécurité et de rétro-ingénierie dans des environnements techniques les plus complexes.   | <b>Renaud FEIL</b><br>Co-founder CEO<br><a href="mailto:renaud.feil@synactiv.com">renaud.feil@synactiv.com</a><br>► <a href="http://www.synactiv.com">www.synactiv.com</a>                                      |
| Veyan (56)                                 | Sécurisation de leur patrimoine informationnel. Démarche politique et organisationnelle basée sur le sur-mesure, la proportionnalité, l'amélioration continue.  | <b>Pierre BOGENSCHÜTZ</b><br>Directeur associé<br><a href="mailto:pierre.bogenschutz@veyan.fr">pierre.bogenschutz@veyan.fr</a><br>► <a href="http://www.veyan.fr">www.veyan.fr</a>                              |
| WaToo (29)                                 | WaToo lutte contre la fuite et le détournement de données et de documents par des utilisateurs autorisés : personnel, partenaires, sous-traitants ou clients. Nos solutions dissimulent des traceurs invisibles dans les données elles-mêmes qui identifient le destinataire de manière unique.   | <b>Javier FRANCO CONTRERAS</b><br>Président/CEO<br><a href="mailto:javier.francocontreras@watootech.com">javier.francocontreras@watootech.com</a><br>► <a href="http://www.watootech.com">www.watootech.com</a> |

## 2/3 PROTÉGER POUR MIEUX PRÉVENIR

**Paralysie des services, arrêt de la production, malfaçon... comment mettre en place des protections adaptées aux risques de cyber-attaques sans alourdir les process, maintenir la mobilité et la flexibilité de l'entreprise ?**

La protection des données regroupe à la fois du service, des solutions et des briques technologiques (solutions de firewall, de chiffrement, d'authentification...).

Sur les 150 entreprises cyber installées en Bretagne, 110 apportent conseil et solutions en matière de protection face aux attaques.

La plupart des entreprises qui sont capables d'identifier et de détecter (parcours 1) proposent également des solutions de protection, dans une logique d'accompagnement sur le long terme.

### Les entreprises bretonnes présentes au FIC 2020 sur cette thématique :

| Nom de la structure | Activités  | Contact   |
|---------------------|--|---|
| ByStamp (56)        | KEYMO de BYSTAMP est la transposition du tampon encreur dans l'univers mobile. KEYMO est un tampon électronique multi-facteurs qui permet d'authentifier une personne morale ou physique sur tout type de terminal mobile, même sans connexion réseau. | <b>Yann LE BAIL</b><br>CEO<br><a href="mailto:yann@bystamp.com">yann@bystamp.com</a><br>▶ <a href="http://www.bystamp.com">www.bystamp.com</a>  |
| Cailabs (35)        | Solution de sécurisation des fibres optiques au niveau de la couche physique.  | <b>David ALLIOUX</b><br>Chef de projets et produits<br><a href="mailto:david@cailabs.com">david@cailabs.com</a><br>▶ <a href="http://www.cailabs.com">www.cailabs.com</a>                     |
| Daspren (35)        | Daspren propose aux entreprises qui souhaitent protéger leurs données face à des attaques inconnues, une solution innovante DaD (Data Aware Defense) qui est complémentaire d'un anti-virus qui protège contre les menaces connues.                    | <b>Belkacem TEIBI</b><br>CEO<br><a href="mailto:belkacem@daspren.com">belkacem@daspren.com</a><br>▶ <a href="http://www.daspren.com">www.daspren.com</a>                                      |
| Hogo (35)           | Solutions de sécurité innovantes, prêtes à l'emploi (off the shelf) pour sécuriser rapidement et efficacement tout système d'information.  | <b>Quentin RUILLERE</b><br>CTO<br><a href="mailto:hello@hogo.eu">hello@hogo.eu</a><br>▶ <a href="https://hogo.eu">https://hogo.eu</a>   |
| Rubycat (35)        | Sécurité des accès sensibles au système d'information en apportant une réponse pragmatique et simple au manque de visibilité sur les actions réalisées par les comptes à privilèges.   | <b>Cathy LESAGE</b><br>CEO/Dirigeante<br><a href="mailto:cathy.lesage@rubycat.eu">cathy.lesage@rubycat.eu</a><br>▶ <a href="http://www.rubycat.eu">www.rubycat.eu</a>                         |
| Secure-IC (35)      | Best in class protection IP cores, security evaluation solutions & consulting full set of analysis platforms   | <b>Lee ANDERSON</b><br>Marketing & Communications<br><a href="mailto:lee.anderson@secure-ic.com">lee.anderson@secure-ic.com</a><br>▶ <a href="http://www.secure-ic.com">www.secure-ic.com</a> |
| SIB (35)            | Protection et intégrité des données. Hébergement de données de santé à caractère personnel. Espace de stockage et partage sécurisé. Accompagnement Cyber (Audit, PenTest...). Accompagnement RGPD (DPO Mutualisé, SOS DPO, ...). Formations.           | <b>Nicolas JOLIVET</b><br>Responsable Pôle Cybersécurité<br><a href="mailto:nicolas.jolivet@sib.fr">nicolas.jolivet@sib.fr</a><br>▶ <a href="http://www.sib.fr">www.sib.fr</a>                |

## 3/3 PRENDRE EN CHARGE UN INCIDENT, RÉPONDRE ET REMÉDIER

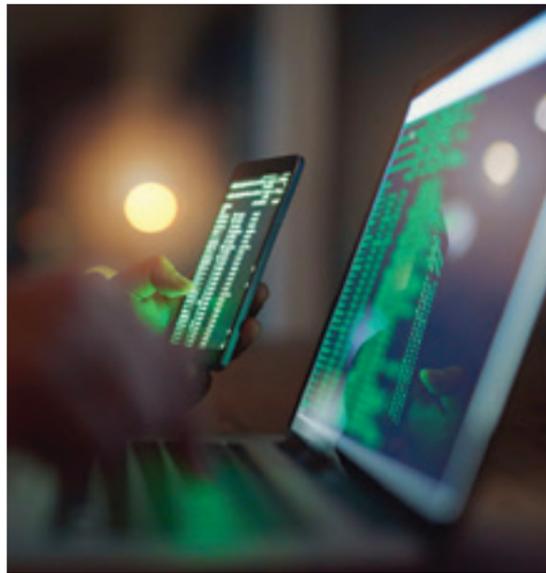
**À défaut de pouvoir tout prévenir, bien réagir est une nécessité. Comment réagir, évaluer, anticiper, sécuriser les données ciblées et remettre le système ciblé en place ?**

Comment réagir devant l'incident, comment continuer ou reprendre l'activité de l'entreprise ? Comment mettre en place les bonnes pratiques ? Comment gérer la crise ? Comment faire en sorte pour que le système redémarre le plus vite possible ? Analyse forensique, gestion de l'incident... Telles sont les compétences que les entreprises cyber doivent apporter à celles qui se sont fait attaquer. Il s'agit à la fois de compétences techniques mais pas seulement.

### Les entreprises bretonnes présentes au FIC 2020 sur cette thématique :

| Nom de la structure | Activités  | Contact  |
|---------------------|--|--|
| Alcyconie (35)      | Alcyconie est un cabinet spécialisé dans la prévention et la gestion de crise et cybercrise et la communication sensible.  | <b>Stéphanie LEDOUX</b><br>Founder & CEO<br><a href="mailto:contact@alcyconie.com">contact@alcyconie.com</a><br>▶ <a href="http://www.alcyconie.com">www.alcyconie.com</a>                           |
| Easylience (35)     | Easylience 4.0 est la 1re solution digitale en Europe dédiée aux gestionnaires de crise cyber. Système collaboratif de pilotage des crises indispensable en appui de votre SOAR (Strengths – Opportunities – Aspirations – Results / outil d'analyse forces-faiblesses-aspirations-résultats) ou de votre SIEM (Security information and event management / Gestion de l'information et des événements de sécurité). | <b>Thierry de RAVEL</b><br>Dirigeant Fondateur<br><a href="mailto:thierry.deravel@easylience.com">thierry.deravel@easylience.com</a><br>▶ <a href="http://www.easylience.com">www.easylience.com</a> |

## ▶ DEUX MÉTROPOLIS QUI COMPTENT DANS L'ESPACE CYBER BRETON



Copyright Destination Rennes Business

### RENNES

**Prenant appui sur les 2 piliers civil et militaire, la filière cybersécurité de Rennes Métropole, plaque cyber du ministère des Armées, s'est épanouie à grande vitesse et reste unique en Europe. Tous installés à moins de 20 minutes les uns des autres, les acteurs bénéficient de cet environnement riche pour se développer. Avec 3 400 emplois répartis dans 70 entreprises privées et au sein de la cyberforce du ministère des Armées, l'écosystème a à cœur de poursuivre son développement afin de consolider sa visibilité nationale et sa reconnaissance au niveau international.**

D'un point de vue académique, le territoire de Rennes Métropole dispose de classes mondiales couvrant l'ensemble de la chaîne de la cybersécurité, de la physique au droit, en passant par l'électronique, les mathématiques et l'informatique. Actuellement, le site rennais compte plus de 200 personnes en formation (dont 110 étudiants dans des formations master et mastères

dédiées à la cybersécurité) et 150 chercheurs en exercice qui travaillent spécifiquement des sujets d'excellence de la cybersécurité techniquement très avancés. Rennes est un lieu unique en matière de formation et de recherche en cybersécurité à l'échelle de la France, mais aussi en Europe.

À la rentrée 2020, Rennes accueillera la CyberSchool qui proposera aux étudiants un programme interdisciplinaire dans les domaines fondamentaux et émergents de la cybersécurité. Une formation de haut niveau, innovante et internationale, adossée à une recherche de pointe, qui vise à doubler le nombre de diplômés rennais en cybersécurité pour atteindre, à terme, un effectif de 580 étudiants.

Côté entreprises, l'Audiar recense des startups, des PME et des grands groupes sur la métropole dont le cœur de métier est majoritairement ou exclusivement dédié à la cybersécurité. L'emploi salarié privé en cybersécurité représente aujourd'hui 2 600 emplois et il a plus que doublé en 10 ans (+ 1 288 emplois salariés privés en 10 ans).

Rennes Métropole est le pôle cyber du ministère des Armées en région avec la Direction Générale de l'Armement Maîtrise de l'Information (DGA-MI) à Bruz et des composantes opérationnelles du Commandement de la cyber défense (Comcyber) dans le quartier militaire Stéphan La Maltière à Rennes / Saint-Jacques-de-la-Lande ou de formation au quartier Leschi - École des transmissions à Cesson-Sévigné (effectifs non comptés dans la présente étude). D'ici cinq ans, les armées doubleront ainsi leurs effectifs cyber à Rennes, avec 1600 personnes.

**L'observatoire de la filière cybersécurité de Rennes Métropole réalisé par l'Audiar est disponible ici :**

<https://www.audiar.org/publication/economie-et-cooperation/economie/lexcellence-cybersecurite-rennes-metropole>



Copyright Naval Group

### BREST, À LA POINTE DE LA CYBERSECURITE MARITIME ET PORTUAIRE

**Terre pionnière de coopération, la métropole brestoise accueille 220 000 habitants sur une zone d'emploi dynamique de 450 000 habitants (183 000 salariés dont 60 % sur la métropole). 400 acteurs privés et publics œuvrent à élever l'économie du territoire aux meilleurs rangs de l'attractivité et de la compétitivité.**

S'appuyant sur une communauté scientifique et des entreprises spécialisées en cybersécurité, elle impose une expertise cyber dans le domaine maritime et portuaire au service de nombreux terrains opérationnels civils et militaires : fonctions maritimes internationales, base opérationnelle de la force océanique stratégique, port civil de premier plan en matière de réparation navale, préfecture maritime de l'Atlantique, siège national du Service hydrographique de la marine et de l'Institut français de recherche pour l'exploitation de la mer, fort potentiel sur le développement des énergies marines renouvelables... Un port donc, qui au travers de ses fonctions, embrasse toutes les composantes des enjeux du monde maritime. La richesse et la puissance des réseaux locaux insufflent à la métropole une dynamique collective importante.

#### Une communauté d'acteurs aux compétences fortes

Brest est unique par sa communauté d'acteurs académiques et industriels aux compétences fortes sur le sujet de la cyber sécurité maritime et de la sûreté.

▶ **Au sein de la base de défense Brest-Lorient**, la Préfecture maritime de l'Atlantique accueille le MICA-Center, le centre MSC-HOA et le centre support cyberdéfense de la marine nationale (CSC).

▶ **Au sein de la communauté académique :** l'ENSTA Bretagne et l'École Navale sous tutelle du ministère des Armées, l'IMT Atlantique sous tutelle du ministère chargé de l'Industrie et du Numérique, l'Université de Bretagne Occidentale, l'ENIB et l'ISEN Yncréa Ouest.

▶ **Un mastère spécialisé en cybersécurité des systèmes maritimes et portuaires** à la rentrée 2020, porté par l'IMT Atlantique, l'ENSTA Bretagne, l'École navale et l'ENSM.

▶ **Des laboratoires de recherche publics :** Lab-STICC, Institut de recherche de l'École navale (IRENAV), IRDL, L@bisen et Centre Européen de Réalité Virtuelle (CERV) couvrant un large spectre thématique en lien avec la cybersécurité.

▶ **Des chaires industrielles :** la chaire industrielle de Cyberdéfense des systèmes navals (domaines civil et militaire) associant l'École navale, l'IMT Atlantique, l'ENSTA Bretagne et soutenue par Thales et Naval Group. La chaire Cyber CNI dans le domaine de la cybersécurité des infrastructures critiques. La chaire Sécurité des Objets Connectés. La chaire transnum.

▶ **Un tissu entrepreneurial dynamique :** Naval Group, Thales, Diateam/CEIS, 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, la convention ORION signée avec la DG de l'armement et le centre d'expertise des programmes navals de la marine nationale.

▶ **Le Pôle d'excellence cyber** qui a pour mission de stimuler le développement de : l'offre de formation cyber, la recherche académique, la base industrielle et technologique de cybersécurité.

**Plus d'informations :**

[economie@brest-metropole.fr](mailto:economie@brest-metropole.fr)

# ► FORMATION – RECHERCHE : ACQUÉRIR DE NOUVELLES COMPÉTENCES

## LES MEILLEURS EXPERTS, LES MEILLEURS TALENTS

### + De 200 chercheurs dans le domaine cyber

On trouve en Bretagne les meilleurs chercheurs du domaine, habitués à coopérer, garant d'une couverture de l'ensemble de la chaîne de sécurité.

De la physique, aux mathématiques, aux réseaux, à l'informatique jusqu'aux sciences humaines et sociales, la recherche en cybersécurité est multidisciplinaire. Ce leadership dans le domaine de la recherche est matérialisé par l'existence de 4 chaires industrielles spécialisées en cyberdéfense, systèmes navals, systèmes des infrastructures critiques et analyse de la menace.

Un accord de partenariat entre DGA-MI Région Bretagne et les établissements de recherche\* a été conclu pour conduire des travaux de recherche soutenus par des allocations doctorales et post doctorales.

\* Inria, CNRS, les Universités de Rennes, Bretagne occidentale et Bretagne Sud, ENS Rennes, Centrale Supélec, Insa et IMTA.

### 3 500 étudiants formés ou sensibilisés à la cybersécurité par an

L'ensemble des opérateurs de formation du territoire breton (universités, IUT, grandes écoles, CNAM...) sont mobilisés pour former en nombre suffisant les futurs spécialistes en cyberdéfense et en cybersécurité.

4 grandes écoles du ministère des Armées (Saint-Cyr Coëtquidan, École navale, ETRS, ENSTA Bretagne), Institut Mine Télécom, Centrale Supélec, l'ENSIBS, l'ISEN, l'ENSSAT... ainsi que le réseau des IUT et celui du CNAM, viennent constituer une offre cyber à tous les niveaux des cycles de formation et permet aux entreprises de trouver les compétences dont elles ont besoin. Une offre en formation continue permet d'élever encore le niveau interne des entreprises.

### CyberSchool, unique école universitaire de recherche en cybersécurité en France

À la rentrée 2020, CyberSchool proposera aux étudiants un programme interdisciplinaire dans les domaines fondamentaux et émergents de la cybersécurité. Une formation de haut niveau, innovante et internationale, adossée à une recherche de pointe, qui vise à doubler le nombre de diplômés en cybersécurité.

#### Plus d'informations :

<https://www.univ-rennes1.fr/actualites/cybersecurite-rennes-universites-ecoles-et-unites-de-recherche-reunis-pour-former-les-futurs-experts>

## Les acteurs académiques présents au FIC 2020 :

| Nom de la structure  | Points remarquables au FIC   | Contact  |
|--|--|--|
| Cyber Security Center de l'Université Bretagne Sud ENSIBS (56) | Le Cyber Security Center de l'UBS permet d'organiser la défense cyber au profit d'OIV, de détecter les vulnérabilités logicielles et de sécuriser les objets connectés.  | <b>Jack NOEL</b><br>Coordinateur Cyber Security Center UBS<br><a href="mailto:jack.noel@univ-ubs.fr">jack.noel@univ-ubs.fr</a>                                   |
| INRIA/LHS (35)   | Inria est l'institut national de recherche en sciences et technologies du numérique. La recherche de rang mondial et l'innovation technologique constituent son ADN, avec pour ambition de faire émerger et d'accompagner des projets scientifiques et entrepreneuriaux créateurs de valeur pour la France dans la dynamique européenne. | <b>Jean-Louis LANET</b><br>Conseiller scientifique<br><a href="mailto:jean-louis.lanet@inria.fr">jean-louis.lanet@inria.fr</a>                                   |
| IMT Atlantique (35)  | Des formations et une recherche d'excellence pour la sécurité des systèmes complexes de l'industrie du futur et des infrastructures critiques  | <b>Jean LE TRAON</b><br>Directeur du campus de Rennes<br><a href="mailto:contact@imt-atlantique.fr">contact@imt-atlantique.fr</a>                                |
| Pôle sup de la Salle (35)                                      | Sécurité Informatique - Formation en alternance - de BAC +3 à BAC +5   | <b>Patricia LE BOUSSARD</b><br>Référente Filière Sécurité Informatique<br><a href="mailto:p.leboussard@groupe-saintjean.fr">p.leboussard@groupe-saintjean.fr</a> |
| Université Rennes 1 (35)                                       | Leader européen en recherche et formation sur la chaîne de la cybersécurité (Cryptologie - Vie privée - Logiciel - Matériel - Réseau)  | <b>Karine CHATEL</b><br>Chargée de mission Cybersécurité<br><a href="mailto:karine.chatel@univ-rennes1.fr">karine.chatel@univ-rennes1.fr</a>                     |

# ▶ EUROPE

## LA BRETAGNE, CYBER VALLEY EUROPÉENNE

La Bretagne se positionne depuis plusieurs années comme l'une des régions françaises et européennes les plus avancées sur les enjeux de cybersécurité et la structuration de cette filière sur son territoire, en particulier grâce au Pôle d'excellence cyber et à la mobilisation de l'ensemble de l'écosystème (collectivités, enseignement supérieur et recherche, entreprises, pôles de compétitivité, ministère des Armées...).

La stratégie bretonne vise à devenir incontournable sur le sujet de la cybersécurité en France et en Europe et cela impose d'être actif et lisible sur les trois niveaux institutionnels :

- › par le soutien à un écosystème construit (recherche, formation et développement économique) breton puissant,
- › par la contribution au « Team France » de l'ANSSI, au Pôle d'excellence cyber, à la filière nationale CSF de sécurité,
- › par la participation à la gouvernance d'ECISO (European Cybersecurity Organisation)\*, au pilotage des programmes européens Interreg Europe CYBER et « cyber valleys » regroupant d'autres régions ayant un écosystème mature en cybersécurité et le soutien au centre de compétence Sparta.

### Des projets européens qui contribuent à construire l'Europe de la cybersécurité

#### › Le projet Interreg Europe « CYBER »

Porté par Bretagne Développement Innovation et le Conseil Régional de Bretagne, CYBER s'appuie sur l'échange de bonnes pratiques entre les 7 régions partenaires pour accroître la compétitivité des PME de la cybersécurité grâce à l'amélioration des politiques régionales.

<https://www.interregeurope.eu/cyber>

#### › L'action pilote « European cyber valleys »

Sous la coordination de la Bretagne, 8 régions européennes travaillent pour créer des synergies entre les régions spécialisées en cybersécurité, faciliter le développement de la chaîne de valeur cyber de l'UE, grâce au mapping des compétences disponibles sur les territoires européens, stimuler la commercialisation des produits et services existants en Europe, par la mise en place d'un programme d'accélération au niveau européen, et encourager les entreprises à investir dans la cybersécurité, au travers du déploiement d'un cyber range pan européen.

<http://s3platform.jrc.ec.europa.eu/cybersecurity>

#### › Le projet « SPARTA » :

SPARTA est un réseau de compétences en cybersécurité, soutenu par le programme européen de recherche et d'innovation (Horizon 2020), dans le but de développer et de mettre en œuvre des actions de recherche et d'innovation collaboratives de haut niveau.

Le consortium SPARTA, dirigé par le CEA, rassemble 44 acteurs issus de 14 pays membres de l'UE.

<https://sparta.eu>

#### › EEN – Entreprise Europe Network (Coopération internationale)

Un projet d'innovation peut nécessiter des compétences en dehors de l'entreprise et parfois à l'international. EEN accompagne les entreprises dans la définition du besoin, l'identification du bon partenaire et la mise en relation avec le bon interlocuteur en mobilisant son réseau de 600 contacts répartis dans plus de 60 pays à travers le monde.

[www.een-france.fr](http://www.een-france.fr)

\* Partenariat Public-Privé de l'organisation européenne de la cybersécurité.

## CONNECTION TO EUROPE

### EUROPEAN CYBER VALLEYS DEVELOP INTER-REGIONAL PARTNERSHIPS



**Interreg Europe**  
An interregional cooperation project to enhance public policies for the competitiveness of cybersecurity companies  
[www.interregeurope.eu/cyber](http://www.interregeurope.eu/cyber)

#### SPARTA

Pilot Cybersecurity Competence Network developing and leveraging cross-discipline and cross-sector capabilities to enhance European strategic autonomy.  
[www.sparta.eu](http://www.sparta.eu)

### EUROPEAN CYBER VALLEYS : PILOT ACTION

Resilience, Deterrence and Defence: Building a strong cybersecurity for the European Union  
[https://s3platform.jrc.ec.europa.eu/cybersecurity](http://s3platform.jrc.ec.europa.eu/cybersecurity)



The directory of skills of 500 European Organisations  
400 companies,  
100 research/training centres

## ► BRETAGNE : POINT DE DÉPART VERS L'INTERNATIONAL

**Pour la première fois sur le plateau Bretagne au FIC, un espace business sera consacré à l'international. Il sera matérialisé par 3 guichets représentant les pays suivants : Allemagne, Singapour, Royaume-Uni.**

La Bretagne donne accès à ses pépites à ses partenaires internationaux. Les entreprises pourront ainsi mieux appréhender les caractéristiques et les opportunités de ces marchés. La Bretagne mettra à disposition ses guichets internationaux à l'ensemble des exposants du FIC.

► **Allemagne : Pivot de la souveraineté européenne en matière de cybersécurité avec la France**

Contact : Yves Rommel - [yves.rommel@victanis.com](mailto:yves.rommel@victanis.com)

► **Royaume Uni : Malgré le Brexit, de vraies opportunités à construire**

Contact : Eric Lambert-Duverneix - [eric.lambert@victanis.com](mailto:eric.lambert@victanis.com)

► **Singapour : Stratégie cyber écrite avec le soutien de la France, Porte d'entrée du marché de l'Asie du Sud-est**

Contact : Marie Lemonnier - [mlemonnier@fccsingapore.com](mailto:mlemonnier@fccsingapore.com)

## MOBILISATION BREIZHCOP

**Bretagne Développement Innovation est fortement mobilisée dans la BreizhCOP, le programme régional d'engagement des acteurs breton.ne.s en faveur du développement durable.**

Par son rôle d'organisateur d'événements et de stands collectifs sur des salons professionnels, BDI est de fait responsable d'un impact carbone non négligeable.

Soucieux de réduire cet impact, nous avons demandé à nos fournisseurs de travailler avec nous en ce sens. Cela s'est traduit par différentes actions comme la réutilisation de mobilier, l'utilisation de matériaux bruts et recyclables ou l'impression des supports de communication avec des encres végétales.

Plus directement, nous avons limité le nombre de brochures (elles-mêmes imprimées en papier FSC et avec des encres végétales), limité l'utilisation de vaisselle jetable (Eco-cup Newcy) et favoriser l'utilisation du train pour nos déplacements.

Malgré cela, l'impact carbone d'une opération tel que le FIC est évalué à 1,7 tonnes de CO<sub>2</sub>. A partir de janvier 2020, nous avons décidé de compenser cet impact en achetant des arbres avec l'aide de la startup brestoise Ecotree (<https://ecotree.fr/>). Ecotree, forestier de métier, s'occupe de planter l'équivalent de cet impact en arbres dans les forêts bretonnes. Il faudra ainsi 80 arbres pour compenser intégralement l'opération FIC 2020.

## ► LES 32 EXPOSANTS BRETONS AU FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ 2020

| 25 entreprises                            | Stand au FIC            | Plus d'infos  |
|---|-------------------------|---|
| Acklio (35)                               | F19                     | <a href="https://www.ackl.io/">https://www.ackl.io/</a>                         |
| Alcyconie (35)                            | Pavillon Bretagne – D15 | <a href="https://alcyconie.com/">https://alcyconie.com/</a>                     |
| Amossys (35)                              | D1                      | <a href="https://www.amossys.fr/">https://www.amossys.fr/</a>                   |
| Anozr Way (35)                            | Pavillon Bretagne – D15 | <a href="https://www.anozrway.com/">https://www.anozrway.com/</a>               |
| Anteo Trust & Security by Sodifrance (35) | Pavillon Bretagne – D15 | <a href="https://www.sodifrance.fr/anteo/">https://www.sodifrance.fr/anteo/</a> |
| Assurable / Obdo (35)                     | Pavillon Bretagne – D15 | <a href="https://obdo.co/">https://obdo.co/</a>                                 |
| Bloo Conseil (35)                         | Pavillon Bretagne – D15 | <a href="https://www.bloo-conseil.fr/">https://www.bloo-conseil.fr/</a>         |
| By Stamp (56)                             | Pavillon Bretagne – D15 | <a href="https://www.bystamp.com/">https://www.bystamp.com/</a>                 |
| Cailabs (35)                              | Pavillon Bretagne – D15 | <a href="https://www.bystamp.com/">https://www.bystamp.com/</a>                 |
| Cardelya (35)                             | G23                     | <a href="https://www.cailabs.com/">https://www.cailabs.com/</a>                 |
| Daspren (35)                              | Pavillon Bretagne – D15 |   |
| Dawizz (56)                               | Pavillon Bretagne – D15 | <a href="https://www.dawizz.fr/">https://www.dawizz.fr/</a>                     |
| Diateam                                   | B10                     | <a href="https://www.diateam.net/">https://www.diateam.net/</a>                 |
| Easylience (35)                           | Pavillon Bretagne – D15 | <a href="https://www.nanocode-labs.com/">https://www.nanocode-labs.com/</a>     |
| Groupe SII (35)                           | Pavillon Bretagne – D15 | <a href="https://rennes.groupe-sii.com/fr">rennes.groupe-sii.com/fr</a>         |
| Hogo (35)                                 | Pavillon Bretagne – D15 | <a href="https://hogo.eu/">https://hogo.eu/</a>                                 |
| Lorcyber (56)                             | Pavillon Bretagne – D15 | <a href="https://www.lorcyber.eu">https://www.lorcyber.eu</a>                   |
| Malizen (35)                              | Pavillon Bretagne – D15 | <a href="https://malizen.com/">https://malizen.com/</a>                         |
| Rubycat (35)                              | Pavillon Bretagne – D15 | <a href="https://rubycat-labs.com">https://rubycat-labs.com</a>                 |
| Secure-IC (35)                            | Pavillon Bretagne – D15 | <a href="http://secure-ic.com">http://secure-ic.com</a>                         |
| SIB (35)                                  | Pavillon Bretagne – D15 | <a href="https://www.sib.fr/">https://www.sib.fr/</a>                           |
| Shadline (35)                             | D32                     | <a href="https://www.sib.fr/">https://www.sib.fr/</a>                           |
| Synaktiv (35)                             | Pavillon Bretagne – D15 | <a href="https://shadline.com/">https://shadline.com/</a>                       |
| Veyan (56)                                | Pavillon Bretagne – D15 | <a href="https://www.veyan.fr/">https://www.veyan.fr/</a>                       |
| WaToo (29)                                | Pavillon Bretagne – D15 | <a href="https://watootech/">https://watootech/</a>                             |

### 5 centres de recherche ou écoles d'enseignement supérieur

|  |                              |   |
|--|------------------------------|---|
| Cyber Security Center de l'Université Bretagne Sud ENSIBS (56) | Pavillon Bretagne – D15      | <a href="http://www-ensibs.univ-ubs.fr">www-ensibs.univ-ubs.fr</a>        |
| INRIA/LHS (35)   | Pavillon Bretagne – D15      | <a href="http://www.inria.fr">www.inria.fr</a>                            |
| IMT Atlantique (35)  | Pavillon Bretagne – D15      | <a href="http://www.imt-atlantique.fr">www.imt-atlantique.fr</a>          |
| Pôle sup de la Salle (35)                                      | Pavillon Bretagne – D15      | <a href="http://www.polesup-delasalle.fr/">www.polesup-delasalle.fr/</a>  |
| Université Rennes 1 (35)                                       | Pavillon Bretagne – D15      | <a href="https://cyber.univ-rennes1.fr">https://cyber.univ-rennes1.fr</a> |
| Université de Rennes 1 (35)                                    | Pavillon principal - D12-D25 | <a href="https://cyber.univ-rennes1.fr">https://cyber.univ-rennes1.fr</a> |
| YNCREA (29-35)   | Pavillon principal - D12-D25 | <a href="https://yncrea.fr">https://yncrea.fr</a>                         |

### 2 métropoles bretonnes

|                                      |                         |  |
|--------------------------------------|-------------------------|--|
| Brest métropole                      | Pavillon Bretagne – D15 | <a href="http://www.brest-metropole.fr">www.brest-metropole.fr</a>   |
| Destination Rennes Business Services | Pavillon Bretagne – D15 | <a href="http://www.rennes-business.com">www.rennes-business.com</a> |

## CONTACTS PRESSE

**Odile Bruley, Conseil régional de Bretagne**

02 99 27 13 55 / 06 76 87 49 57  
odile.bruley@bretagne.bzh

**Chrystèle Guy, Bretagne Développement Innovation**

02 99 84 78 76 / 07 82 21 81 35  
c.guy@bdi.fr

**Pôle d'excellence cyber**

06 63 02 36 31  
contact@pole-excellence-cyber.org



@ExcellenceCyber  
@BretagneBDI



PÔLE D'EXCELLENCE  
**CYBER BRETAGNE** 

