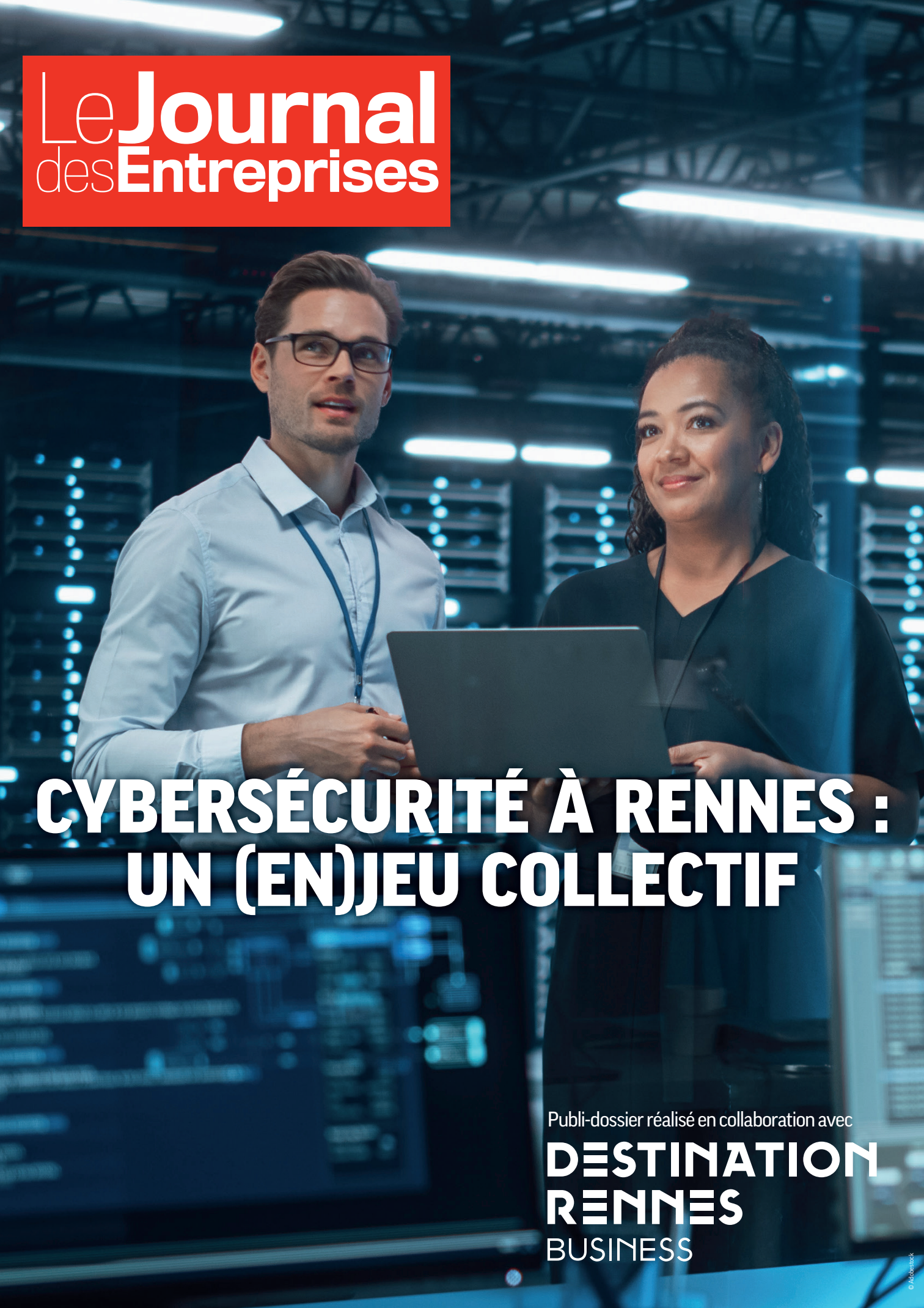
Le Journal des Entreprises



CYBERSÉCURITÉ À RENNES : UN (EN)JEU COLLECTIF

Publi-dossier réalisé en collaboration avec

DESTINATION RENNES BUSINESS

LA CYBERSÉCURITÉ À RENNES

SE FORMER, TRAVAILLER, RECRUTER

« Ici on favorise le collectif »

Une intense création d'emplois

4 242 emplois

3 377 emplois privés dans **96** entreprises privées

865 cybercombattants du ministère des Armées

Une croissance de **7,5 %** des emplois privés en un an

311 nouveaux emplois en un an

Un fort développement attendu

250 emplois par an : intentions d'embauches

220 postes à l'ANSSI

Des groupes industriels impliqués

Airbus Cybersecurity, très associé à la recherche locale

Thales Services, une « ruche » pour accueillir des startups

Le CyberSoC d'Orange Cyberdefense, place forte du groupe

Un dialogue militaro-industriel unique en France

Rennes, 1ère force cyber des Armées en région

La **Cyberdéfense Factory,** un incubateur dual civil et militaire unique

Des **chaires industrielles** mixtes

Un écosystème leader

Rennes est n°1
(hors Paris Île-de-France)

> avec **150 chercheurs** en recherche académique

> au palmarès Wavestone des startups en cybersécurité

DES SPÉCIFICITÉS UNIQUES :

« Cyberschool », école européenne universitaire de recherche

« Cyberplace », immobilier dédié en cyberdéfense

Le pôle d'excellence cyber, animateur d'innovations

French cyber booster au sein du Poool

CHIFFRES CLÉS EXTRAITS D'ÉTUDES 2020 ET 2021 DE L'AUDIAR

ÉDITO

RENNES, UN ÉCOSYSTÈME AU SERVICE DE LA CYBER

Par **Nathalie Appéré**
Maire de Rennes et
Présidente de Rennes Métropole

Chaque jour, l'actualité nous démontre toute l'importance des questions de souveraineté et de confiance numérique. Les entreprises, les collectivités, les hôpitaux sont régulièrement les cibles d'attaques cyber. Pour y faire face, la résilience des systèmes et la protection des données sont cruciales. Ce seront les thèmes des deux tables rondes organisées pendant la European Cyber Week par Rennes Métropole et le Comité Stratégique de Filière des industries de sécurité, dans le cadre de la session "Villes et territoires numériques de confiance face à la menace cyber".

Cette année, la Ville de Rennes et Rennes Métropole ont adopté leur première stratégie pour un numérique responsable. Ce plan d'actions favorise l'émergence d'un modèle où la sécurité numérique est constitutive du cadre de confiance proposé aux citoyens, aux communes et aux acteurs métropolitains. Elle fait de la transformation numérique de nos territoires une opportunité de développement économique et d'emplois, où l'innovation est vertueuse et n'entre pas en contradiction avec les enjeux du moment : enjeux d'égalité, de liberté, enjeux sociaux et écologiques.

L'industrie de cybersécurité française compte de nombreux acteurs de niveau mondial, pour beaucoup déjà implantés en Bretagne, et c'est une chance. Rennes Métropole, en partenariat avec la Région Bretagne, s'implique fortement pour le développement de cette filière, en créant les conditions de l'émergence de startups, en assurant la disponibilité de locaux, y compris sécurisés, pour les jeunes entreprises du secteur ou encore en accompagnant les acteurs académiques dans le développement des ressources humaines dans le domaine. Elle sera un partenaire actif du Campus Cyber et de sa déclinaison régionale.

SOMMAIRE

LE SECTEUR CYBER RECRUTE : DE NOMBREUSES INITIATIVES SONT MISES EN PLACE POUR SÉDUIRE TOUS LES PUBLICS

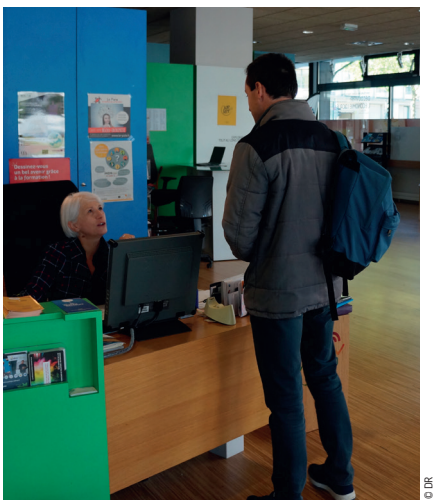
Le potentiel de recrutement dans les métiers cyber à Rennes reste important. « On estime à 250-300 les postes à pourvoir annuellement sur la métropole rennaise » précise Régine Diverrès, chargée de mission GPEC-T à We Ker, mission de service public rennais pour l'accompagnement vers l'insertion professionnelle. Des actions de recrutement, formation et reconversion se mettent en place pour des publics très divers.

« *Nous avons relancé une enquête auprès des entreprises de la cyber du territoire rennais pour identifier leurs besoins* ». L'enquête est portée par We Ker et Rennes Métropole avec le soutien de l'AUDIAR. Car les métiers recherchés sont très divers. Conseil, recherche, conception et maintien de SI sécurisés, gestion de crises de sécurité… Les recruteurs aussi sont variés, allant d'entreprises privées (Start-up, PME, grands groupes) à des structures étatiques.

Pour répondre au manque de talents, We Ker a mis en place, dans le cadre du plan de rebond de Rennes Métropole, un comité avec des employeurs, la Région, des établissements de formation pour recenser les besoins, identifier les viviers et définir les actions en fonction des publics visés.

Une matinale sur les métiers de la cyber, sous forme de webinaire, a vu le jour récemment, sous l'impulsion d'un groupe de travail réunissant l'APEC et un club de DRH. « *C'est l'occasion de mettre en avant la richesse de l'écosystème rennais, les opportunités d'emplois et de carrières à travers les témoignages de DRH et de personnes, avec des profils variés, en poste dans la cyber : un homme de 59 ans récemment diplômé du Mastère Cybersécurité de Centrale Supélec suite à une reconversion professionnelle, une jeune femme travaillant chez Amosys…* ». A l'issue de ce webinaire, des candidats se manifestent et sont orientés vers des employeurs ou la formation.

« *Dans le cadre du BreizhCTF porté par Bretagne Développement Innovation (BDI) où plus de 500 hackers éthiques se*



© DR

sont retrouvés pour participer au CTF, nous avons organisé avec BDI, Rennes Métropole, Destination Rennes et des entreprises cyber présentes sur le territoire, un premier Hack&Job ». Objectif : faciliter les rencontres entre des candidats potentiels et des employeurs. « *Ce type de rencontres met les gens en connexion, donne à voir de la diversité des acteurs de la filière cyber et l'esprit collectif qui y règne* ». Pour déclencher des envies de carrière… Opération qui devrait se renouveler le 17 mars 2023.

« *Il faut être présent dans les manifestations grand public, pour faire connaitre le plus largement possible les métiers de la cybersécurité* » insiste Régine Diverrès. Conférence au Stade de l'Emploi ouvert à un public de demandeurs d'emploi et de jeunes qui s'interrogent sur leur avenir. Rencontre « Parlons-métier hacker éthique », à l'Exploratoire centre d'information et d'orientation, avec des professionnels de la cybersécurité, qui expliquent leurs métiers. « *Ces formats d'évènements favorisent les échanges et laissent place à des questions sans jugement, dans la proximité* ».

Si le territoire rennais foisonne de ces actions variées pour faire connaitre les métiers de la cyber, c'est grâce à un collectif d'acteurs engagés et au soutien de Rennes Métropole.

Pour en savoir plus

We Ker

Régine Diverrès, rdiverres@we-ker.org

Cyberschool

Stéphane Szymanski, Chargé de formation/ reconversion Cybersécurité
stephane.szymanski@univ-rennes1.fr

© DR

CYBERSCHOOL

La CyberSchool a réalisé sa 3ème rentrée avec plus de 250 étudiants spécialisés en cybersécurité dans ses formations de Masters et d'Ingénieurs. La croissance des effectifs est particulièrement portée par ses parcours de Master (+76% vs 2020). La CyberSchool poursuit son développement avec le lancement à l'automne 2022 d'un parcours doctoral, le développement des partenariats entreprises et la préparation d'un Master qui formera en alternance au management de la sécurité des SI.
Plus d'informations sur https://cyberschool.univ-rennes.fr/en/

UNE GOUVERNANCE CYBER MÉTROPOLITAINE POUR PROTÉGER LES SERVICES DE LA VILLE

Avec le développement de nouveaux services dans les villes, rendus possibles par la numérisation, les questions de cybersécurité des métropoles deviennent cruciales.

L'utilisation de capteurs, le contrôle à distance des infrastructures, l'interopérabilité, la mobilité intelligente et la détention par les collectivités de nombreuses données à caractère personnel, prêtent le flanc à des cyber attaques.

« Il devient nécessaire de réfléchir à de nouveaux types de pilotage, transversaux à l'ensemble des activités et des organisations en particulier les Opérateurs d'importance vitale et les Opérateurs de services essentiels. Autrefois domaine exclusif des DSI, ces questions nouvelles obligent à repenser le système de gouvernance et à clarifier les responsabilités techniques et politiques. » nous explique François Bodin titulaire de la chaire « Mobilité dans une ville durable» de la Fondation Rennes 1.

À cette fin, un comité de réflexion a été mis en place. Il réunit divers acteurs, issus des secteurs institutionnel, académique comme Université Rennes 1, privé, ainsi que le PEC et un accompagnement de l'ANSSI. Sa mission consiste à proposer ce que pourrait être les responsabilités, comment pourrait être appréhendé un pilotage politique des prises de risques, évaluer ces risques, articuler l'ensemble des acteurs, identifier les coûts, la gestion de crise et les formations nécessaires.

Ce chantier, lancé en 2022, devrait pouvoir émettre de premières recommandations dès 2023. Il va inscrire le développement de territoires intelligents dans une vision et une sécurité globale. Il doit aussi préserver la confiance citoyenne, notamment en cas d'incident. Cela impose une résilience importante et une transparence vis-à-vis des usagers.

POUR UN NUMÉRIQUE RESPONSABLE ET DE CONFIANCE

Le décret précisant la stratégie numérique responsable, qui s'impose aux communes et EPCI de plus de 50.000 habitants au 1er janvier 2025, a été publié le 29 juillet 2022. Une stratégie dont la vocation est d'englober toutes les obligations ou recommandations de verdissement du numérique des administrations promues par les pouvoirs publics ces dernières années

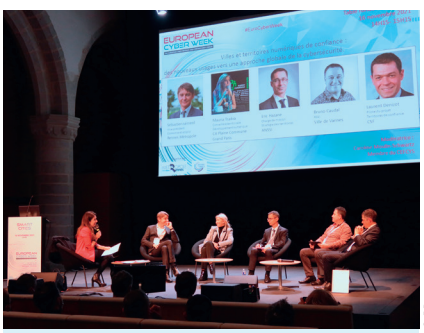
Le numérique est facteur de progrès et de création de valeur, mais ses impacts peuvent être négatifs s'ils ne sont pas encadrés : gaspillage de ressources, émission de gaz à effet de serre…

La stratégique numérique responsable s'attache donc à l'optimisation des outils numériques dans les services des collectivités, aux achats responsables, à l'allongement de la durée d'utilisation des équipements ainsi qu'à leur recyclage…

Pour des pratiques numériques responsables, les collectivités ont vocation à ne collecter que les données nécessaires au service des utilisateurs, qui respectent la vie privée (RGPD) ; et à ne développer que des usages raisonnés des données et des services.

Pour être effectif, le numérique responsable doit impérativement s'appuyer sur une plateforme technologique de confiance, qui sécurise l'ensemble. C'est l'objet du grand projet « Territoire de Confiance » du Comité Stratégique de Filière (CSF) des industries de sécurité piloté par Laurent Denizot, DG d'Egidium Technologie et dont Rennes Métropole est partenaire auprès d'autres collectivités comme Lille, Plaine Communes, Chartres ou encore Saint Quentin en Yveline.

Ce projet « Territoire de confiance », vise à bâtir avec les collectivités des plateformes cyber protégées, sobres, éthiques et résilientes. Ce mode de sécurisation numérique est si complexe qu'il s'inscrit dans un travail collaboratif d'envergure nationale, agrégeant industriels de la sécurité, l'ANSSI, et plusieurs ministères. Toutes les collectivités sont les bienvenues pour participer à cette dynamique.



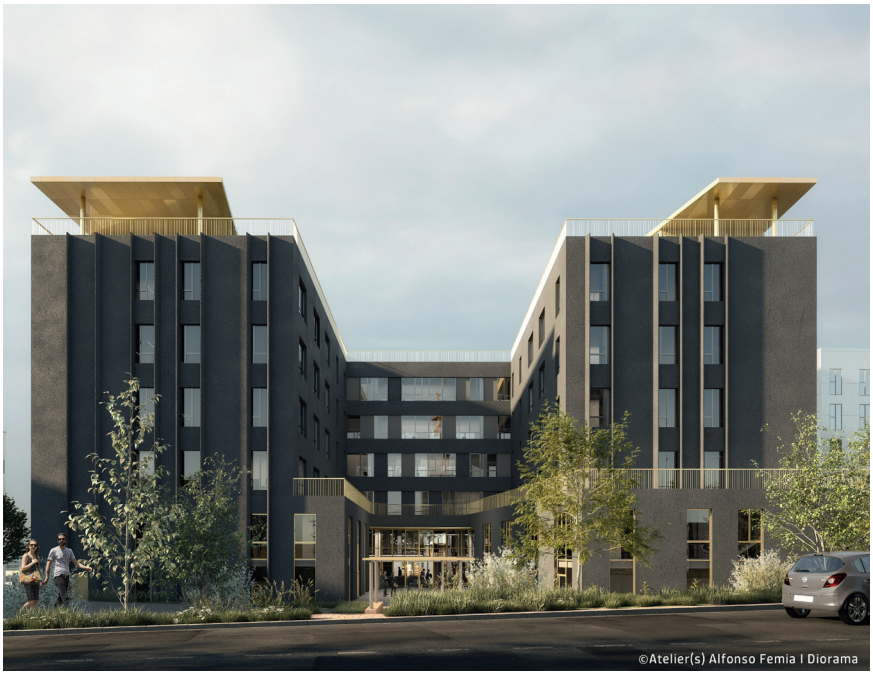
© DR

CONFÉRENCE « VILLES ET TERRITOIRES NUMÉRIQUES DE CONFIANCE FACE À LA MENACE CYBER » À LA ECW 2022

Chaque année, à l'occasion de la European Cyber Week, Rennes Métropole et Destination Rennes organisent la conférence « Villes et territoires numériques de confiance face à la menace cyber » en partenariat avec le CSF des industries de sécurité qui donne à voir les enjeux d'un numérique éthique et responsable. Une journée de réflexion et d'échanges pour œuvrer ensemble, acteurs publics et privés, au développement de « Smart-Territoires » de confiance.

LE PAYSAGE IMMOBILIER CYBER S'ÉTOFFE À RENNES

Avec une forte croissance des emplois privés (+7,5 % en un an), l'intensification des activités souveraines et la renommée de sa filière académique, Rennes Métropole s'impose comme un territoire de référence en matière de cybersécurité et de cyberdéfense en France et en Europe. Deux nouveaux bâtiments font leur apparition dans le paysage immobilier rennais et témoignent du foisonnement de la capitale bretonne en matière d'activité cyber.


©Atelier(s) Alfonso Femia I Diorama

CYBERPLACE

C'est l'immeuble des entreprises de la cybersécurité à Rennes. Avec plus de 7 600 m² de bâtiment divisés entre bureaux, espaces flex-office, pépinière d'entreprises et lieux de convivialité, la CyberPlace a tout pour favoriser l'innovation et l'émergence de projets collectifs. Et c'est l'ambition des porteurs et des partenaires du projet que sont NGE Immobilier, Rennes Métropole et la Région Bretagne.

Le bâtiment, entièrement sécurisé, accueillera une nouvelle pépinière d'entreprises de Rennes Métropole. Gérée par Citédia, cette pépinière de 1 200 m² sera dédiée à la cybersécurité et comprendra 170 m² d'espaces agréés « confidentiel défense ».

L'immeuble CyberPlace sera inauguré courant de l'année 2023. Il viendra compléter la ZAC ViaSilva, sur la commune de Cesson-Sévigné, au Nord-Est de Rennes, où sont déjà installés de grands noms de la cybersécurité (AriadNext, Secure-IC...). Ce nouveau bâtiment comptera également parmi ses voisins la pépinière Digital Square, ouverte en janvier 2017, où des entreprises comme Glimps innovent et se développent grâce à des infrastructures adaptées. Les futurs occupants de la CyberPlace, comme l'entreprise Wallix, pourront compter sur la technopole Le Poool qui s'y implante ou encore sur l'expertise et les équipements de l'Institut de Recherche Technologique b<>com qui travaille entre autres sur la sécurité des contenus et des réseaux 5G et au-delà.

ART&FACT

A l'autre bout de la ligne b du métro, dans le quartier de la Courrouze, un second pôle cybersécurité se constitue. Au Sud-Ouest de Rennes, ce quartier accueille déjà le commandement de la cyberdéfense (COMCYBER) et son incubateur unique en France, la Cyberdefense Factory, piloté conjointement avec la Direction Générale de l'Armement (DGA). D'ici fin 2022, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) inaugurera sa nouvelle antenne, première en région, dans ce même quartier. Elle installera ses équipes dans le bâtiment nommé Art&Fact sur 4 600 m². Des recrutements sont actuellement en cours pour atteindre les 200 agents à l'horizon 2026.

Du Nord-Est au Sud-Ouest, en passant par le centre-ville et les campus universitaires, il ne faut pas plus de vingt minutes pour relier les acteurs de l'écosystème cyber rennais, qu'ils soient civils ou militaires, privés ou publics, académiques ou industriels. A 1h25 de Paris en train, Rennes et la Bretagne jouent collectif pour se hisser en place forte de la cybersécurité en France et en Europe.


© Antoine Montjoin

CYBER BOOSTER

En un an d'existence, Cyber Booster peut se targuer d'un beau palmarès : pas moins de 17 startups accompagnées (ou en cours d'accompagnement), 4 partenaires premium et une équipe dédiée de 8 personnes. Le start-up studio, porté par Le Poool et Axeleo, opère dans deux écosystèmes cyber très riches que sont le Campus Cyber (Paris) et Rennes Métropole. Un deuxième appel à projet a été lancé en juillet 2022 avec pour objectif d'aider les startups à formuler une proposition de valeur claire et différenciante et concevoir un produit ou service adapté aux besoins du marché.

CYBER-TESTER LES SOLUTIONS SANTÉ

En lien avec ses filières d'excellence numériques, Rennes montre une véritable dynamique autour de la santé avec un foisonnement de start-up dédiées. Depuis 2020, elle travaille au renforcement de cet écosystème innovant pour lequel la cybersécurité est un enjeu crucial.

« *La fluidification du parcours patient est un des défis majeurs du système de santé. Elle passe par une meilleure communication entre les différents professionnels de santé qui interviennent auprès d'une même personne, pour éviter les ruptures de parcours ou une perte de temps, liées par exemple à la recherche de résultats d'examens. Or, mieux communiquer, c'est partager des données* » explique Céline Queron, chargée de la filière santé à la direction de l'économie de Rennes Métropole.

Des solutions numériques innovantes voient le jour sur la métropole pour améliorer cette fluidifié, ou encore pour mieux diagnostiquer ou assurer un suivi médical à domicile. Pour éviter que les données échangées ne soient récupérées par des organisations malveillantes, il faut éviter les failles potentielles dans les dispositifs médicaux dès leur conception.

« *En s'appuyant sur la forte concentration d'acteurs de la cybersécurité-académiques, entreprises ou institutions, la métropole a toutes les cartes en main pour offrir aux entreprises de la santé numérique un cadre pour améliorer et tester la sécurité des innovations* ». Un atout qui pourrait contribuer à inscrire le territoire dans une reconnaissance nationale, voire européenne, de la cybersécurité dont les systèmes de santé ont terriblement besoin.

UN CATALOGUE DE PRESTATION CYBER POUR ACCOMPAGNER L'ÉCOSYSTÈME DE LA SANTÉ

Un catalogue de services et de prestataires cyber, destiné aux acteurs de la santé vient de voir le jour. Dans un contexte de multiplication des attaques cyber, c'est une véritable arme de défense pour les acteurs du monde de la santé.

Aujourd'hui, la menace cyber est permanente et les données de santé sont particulièrement menacées par les cyber criminels. Avec la multiplication des objets connectés en santé et l'intégration massive du numérique, les menaces sont explosives et dévastatrices. Numérisation des dossiers patients, robotique médicale, gestion connectée des bâtiments, accroissement des métadonnées de santé : le monde médical est de plus en plus vulnérable.

« *Dans ce contexte, il existe des réponses pour prévenir, détecter et réagir face aux menaces cyber* » explique Coralie Borniambuc, chargée de projet e-santé au sein de Biotech Santé Bretagne. Cette association, centre d'innovation technologique, qui structure et anime les filières régionales des Biotechnologies et de la Santé sur le territoire breton, vient d'éditer en collaboration avec le Pôle d'Excellence Cyber un catalogue de services et prestataires cyber appliqués au domaines de la santé.

Elaboré par une équipe d'experts et destiné aux éditeurs de solutions de santé et aux établissements de santé, il alerte sur les enjeux de la cybersécurité, sur la sensibilité de la donnée en santé, détaille les différents types d'attaques et donne les clés et services pour se protéger.

B<>COM « LA CYBERSÉCURITÉ EST VITALE ! »

Les données liées à la santé sont parmi les plus sensibles que doit gérer un individu. Leur centralisation numérique en fait des cibles privilégiées et pose un problème de cybersécurité. Avec sa technologie *Serenity*, b<>com propose à dessein de nouvelles approches d'authentification multi-facteurs et sans couture, pour concilier sécurité et facilité d'utilisation pour le grand public.

© DR

#RENNES

RECRUTE

BRETAGNE

CECI N'EST PAS UNE OFFRE D'EMPLOI

C'EST UN PROJET DE VIE

WWW.RECRUTEMENT-RENNES.COM

DESTINATION RENNES BUSINESS

RENNES-BUSINESS.COM
@RENNESBUSINESS

Agence hum

CONTACT

Paul-André PINCEMIN
Délégué à la cybersécurité
et aux restructurations militaires
Rennes Métropole
pa.pincemin@rennesmetropole.fr