Focus sur les startups et les PME cyber sur le Territoire de Rennes Métropole

2025

SOMMAIRE

La cybersécurité est un enjeu sociétal dont on prend, jour après jour de plus en plus conscience. Il concerne les acteurs socioéconomiques, la nation ou encore chacun d'entre nous dans notre vie quotidienne. Elle est une brique constitutive de la confiance numérique.

La métropole de Rennes et plus globalement la Bretagne s'imposent progressivement comme territoire de référence en matière de cybersécurité à l'échelle nationale et européenne où, acteurs civils et militaires, publics et privés, industriels et académiques travaillent de concert.

Rennes Ville et Métropole prend toute sa part pour accompagner le développement de la filière, dans le cadre de Bretagne Cyber Alliance, en particulier pour voir émerger une offre de services et de produits de confiance en cybersécurité.

Afin de mettre en lumière cet écosystème, nous avons entrepris la mise à jour du recensement et descriptif des acteurs industriels cyber présents sur le territoire, et plus particulièrement des PME et des startups, depuis 2022.

Cette version, forcément incomplète et perfectible, a vocation à être complétée et actualisée régulièrement pour rendre compte, le plus fidèlement possible, du dynamisme de l'écosystème cybersécurité de la métropole rennaise.

Sébastien SEMERIL
Vice-président en charge de l'Economie et de l'Emploi
à Rennes Ville et Métropole

Ce document, qui s'inscrit dans la dynamique du campus Bretagne Cyber Alliance (www.cyberalliance.bzh), a vocation à mettre en valeur la richesse et la dynamique de l'écosystème cyber rennais et plus particulièrement celui des entreprises. Les différentes PME et Startups, classées par ordre alphabétique y sont présentées.

Le sommaire se trouve en page 2.

Leur positionnement marché, dont la segmentation inspirée de celle des radar Wavestone, est rappelé dans un tableau synthétique en fin de document, leur positionnement pour répondre aux exigences NIS2 et DORA également. L'ensemble des résultats est fondé sur l'auto déclaration.

Enfin, les différentes structures accompagnant le développement de la filière sur le territoire font également l'objet, pour certaines d'entre elles, de fiches dans lesquelles elles présentent leur offre de valeur. Elles figurent juste après cet "Note aux lecteurs".

Leur positionnement principal, non exclusif, peut se résumer ainsi :

- Être accompagné dans le montage de projets d'innovation, en particulier collaboratifs : Pôle de compétitivité Images & Réseaux : www.images-et-reseaux.com
- Approcher des marchés à l'export : Bretagne Commerce International www.bretagnecommerceinternational.com
- Être accompagné depuis l'idéation jusqu'à l'ETI : le Poool la FrenchTec Rennes Saint Malo https://lepoool.tech/ avec en particulier son dispositif CyberBooster www.cyberbooster.fr
- S'intégrer dans l'écosystème rennais et plus globalement breton, en complément de l'adhésion à Breizh Cyber Alliance : les cyber breakfast de BDI https://www.bdi.fr/fr/agenda/cyber-breakfast/
- Travailler en collaboration avec la DGA (Incubateur de startup pour expertise technique opérationnelle) : Cyber Défense Factory
- Contribuer à bâtir collectivement, public – privé, civil – militaire, académique - industriel - une autonomie stratégique en matière de cyberdéfense, n'hésitez pas à rejoindre le pôle d'excellence cyber : www.pole-excellence-cyber.org
- Disposer de locaux dans une pépinière numérique ou dédiée à la cyber avec les locaux habilitables secret : https://www.citedia-deveco.com/nos-sites/digital-square/ https://www.citedia-deveco.com/nos-sites/pepiniere-cyber/

Pour plus d'information sur la richesse et le dynamisme de l'écosystème cyber rennais où public et privé, civils et militaires, académiques et industriels travaillent de concert n'hésitez pas à consulter : www.entreprendre-rennes.fr/article/cybersecurite/ .

Et si vous souhaitez vous impliquer dans cette dynamique collective rennaise, vous faire connaître ou vous y implanter, vous pouvez contactez le délégué à la cybersécurité à Rennes Ville et Métropole Paul-André Pincemin à l'adresse suivante : pa.pincemin@rennesmetropole.fr.

Bonne lecture

FOCUS SUR Bretagne Cyber Alliance

L'ambition de Bretagne Cyber Alliance est de fédérer, soutenir, animer et développer l'écosystème breton, le faire rayonner comme une référence en France et en Europe au service d'un monde numérique plus sûr

Le BreizhCTF, la plus grande compétition de hacking en France, organisé par Bretagne Cyber Alliance.

QUI SOMMES NOUS ?

Bretagne Cyber Alliance est le campus cyber régional, créé en 2024 par six membres fondateurs : la Région Bretagne, Brest Métropole, Lannion Trégor Communauté, Lorient Agglomération, Rennes Métropole et Golfe du Morbihan - Vannes Agglomération.
Le campus cyber breton s'inscrit dans la stratégie nationale de fédération et de développement des acteurs cyber et de sécurisation de l'ensemble des acteurs économiques.
La Cyberplace est le bâtiment que Rennes Métropole a choisi pour incarner le campus cyber régional sur son territoire.

MISSIONS DU CAMPUS CYBER TERRITORIAL

Bretagne Cyber Alliance active et dynamise la communauté cyber, favorise les interactions entre les différents acteurs de la filière et fait rayonner l'écosystème cyber breton au service d'un monde numérique plus sûr. Le campus cyber breton structure son action autour de 4 missions : accompagner la croissance des acteurs économiques de la filière, conforter la performance de la recherche et de l'innovation, diffuser la cybersécurité dans toute la société bretonne et répondre aux besoins de compétences. Parmi les initiatives et résultats concrets : l'organisation des cyberbreakfast mensuels, rdv incontournable de la communauté cyber bretonne et désormais nationale ; une cartographie des aides mobilisables en Région pour engager une démarche de cybersécurité ; la réalisation d'un observatoire NIS2 permettant d'identifier les 2 000 établissements concernés par la directive européenne sur la région ; la mise en place d'un baromètre de maturité cyber des entreprises bretonnes. Rejoindre Bretagne Cyber Alliance, c'est intégrer une communauté innovante et performante, se rapprocher de ses pairs, adresser les bénéficiaires et être connecté aux enjeux nationaux et européens.
Contact : contact@cyberalliance.bzh

CHIFFRES CLÉS
175 entreprises cyber
8000 emplois
3500 étudiants formés
200 chercheurs ETP

FOCUS SUR LE POOOL x LA FRENCH TECH RENNES ST MALO

Le Poool x La French Tech Rennes St Malo est le résultat de la fusion de deux structures : Rennes Atalante et la French Tech Rennes Saint-Malo. Cette double dimension, à la fois technopole et Capitale French Tech, permet à l'association d'être profondément ancrée à l'écosystème du territoire.

La communauté est aujourd'hui composée de plus de 500 membres.

QUI SOMMES NOUS ?

Acteur central de l'écosystème de l'innovation et de l'entrepreneuriat en Ille-et-Vilaine, Le Poool accompagne les entreprises innovantes et porte la Capitale French Tech Rennes Saint-Malo. Notre mission : faire du territoire un lieu propice au développement des projets innovants, au service d'une économie durable. Pour cela, l'association s'appuie sur une vision inclusive de l'innovation. Elle a pour vocation de faire se rencontrer les différents acteurs du territoire et de coconstruire, avec eux, les conditions les plus favorables pour les entrepreneurs.

"Soutenir l'envie d'entreprendre et développer l'excellence de l'écosystème

NOTRE ACCOMPAGNEMENT

Le Poool est une communauté riche de plus de 500 membres : startups, scaleups, structures d'accompagnement, acteurs publics, ESR… et opère des programmes d'accompagnement orientés en fonction du niveau de maturité des entreprises et des filières d'excellence.
L'Intelligence Artificielle et la Cybersécurité, sont sur le devant de la scène de l'innovation sur le territoire et trouvent par ailleurs une place centrale dans l'évolution du Poool à ViaSilva, et dans son implication dans le programme national Cyber Booster : évènements dédiés à la cybersécurité et à l'IA, accompagnement des PME innovantes sur ces sujets, et accélération du développement des startups cyber sur le territoire.
En outre, L'Innovation Vertueuse, plus qu'une dynamique, fait partie de l'ADN du Poool. L'Innovation Vertueuse s'inscrit en outre dans les orientations de "transitions" au niveau national, avec France 2030, autour de la transition écologique, la parité et la souveraineté.
31 personnes œuvrent au quotidien au déploiement des actions en lien avec la French Tech.

CHIFFRES CLÉS

560 membres de l'association
255 entreprises accompagnées
28 entreprises créées avec notre accompagnement
56 sponsors et partenaires annuels

FOCUS SUR LE PÔLE D'EXCELLENCE CYBER

Créé en 2014, le Pôle d'excellence cyber (PEC) fédère un écosystème unique autour de la cybersécurité et de la cyberdéfense. Avec plus de 130 membres – entreprises, institutions, écoles et universités, laboratoires – il œuvre à la souveraineté numérique nationale en développant des synergies entre recherche, formation et innovation. Il coordonne aussi des programmes inclusifs et contribue activement au programme EDIH Bretagne.

Le Pôle d'excellence cyber est aujourd'hui composée de plus de 130 membres.

"Bâtir une autonomie stratégique durable, en phase avec les défis du monde contemporain"

QUI SOMMES NOUS ?

Le PEC est une association créée par le ministère des Armées et la Région Bretagne, structurée autour d'une ambition forte : faire de la France un leader souverain en cyberdéfense. Véritable cluster dual, le PEC s'appuie sur un écosystème dense d'acteurs civils et militaires – industriels, startups, organismes de recherche, grandes écoles et institutions – pour développer des projets concrets à fort impact.

Ses trois axes stratégiques sont :

- la recherche ;
- la formation, en lien avec France 2030 et les projets CyberSkills4All ;
- Le développement industriel.

Implanté en Bretagne mais actif à l'Europe et à l'international, le PEC défend une vision inclusive de la cybersécurité à travers des programmes sociétaux (Cadettes de la cyber, neurodiversité en entreprise) et ses publications de référence. Il organise également l'European Cyber Week, rendez-vous incontournable du secteur.

NOTRE ACCOMPAGNEMENT

Dans le cadre de l'EDIH Bretagne , le Pôle d'excellence cyber se meut en opérateur et met en œuvre une prestation de diagnostic et d'accompagnement des entreprises à sécuriser, à travers son offre de services : PACTE (Programme d'Accompagnement de la Cyber résilience des Territoires et des Entreprises). Son objectif est de relever le défi urgent de la transition numérique pour la performance, la sécurité et la pérennité des entreprises européennes et des services publics. Ce programme vise à stimuler et à accompagner les entreprises et l'écosystème en repensant leur organisation, leur modèle économique, leurs outils et méthodes, tout en plaçant le client et l'humain au cœur de cette transformation numérique. Quelle que soit leur couverture géographique (locale, régionale, nationale, européenne) ou leur mission (marché / application, technologique, RD&I…), la vision commune des partenaires de l'EDIH-Bretagne est de contribuer à la croissance économique & à la richesse des entreprises de la région Bretagne. Contact : contact@pole-excellence-cyber.org

CHIFFRES CLÉS
130 membres
2014 création du Pôle

FOCUS SUR CYBERDEFENSE FACTORY

La Cyberdéfense Factory est un espace ouvert pour favoriser l'innovation en proposant une offre de services : hébergement, accès à des données d'intérêt cyber, avis d'expertise, échange avec des utilisateurs opérationnels et capacité à tester les solutions avec des experts de la DGA et des opérationnels du COMCYBER.

"Innovez avec la Cyberdéfense Factory : l'incubateur qui transforme vos idées en solutions cyber robustes".

QUI SOMMES NOUS ?

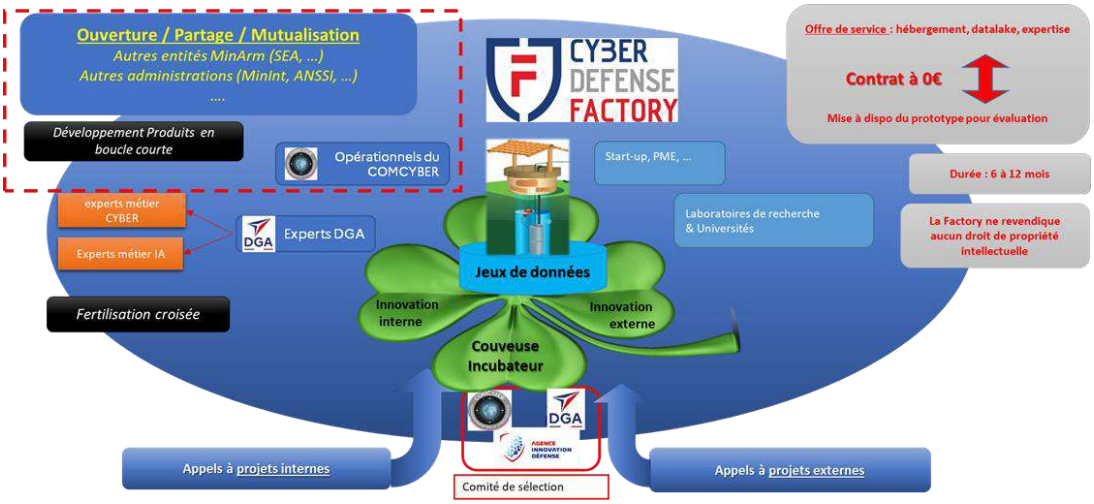
Lancée en octobre 2019 la Cyberdéfense Factory vise à favoriser l'émergence de solutions cyber innovantes, en rapprochant opérationnels des armées, startups, PME et universitaires. Elle offre un hébergement, l'accès à des données d'intérêt cyber et la capacité à développer et tester les solutions avec des experts de la DGA et des opérationnels du Ministère des Armées. L'accès aux données d'intérêt cyber permet notamment de développer des solutions faisant appel à des techniques d'intelligence artificielle,

NOTRE ACCOMPAGNEMENT

La Cyberdéfense Factory est pilotée par la Direction Générale de l'Armement (DGA), le Commandement de la Cyberdéfense (COMCYBER) et l'Agence Innovation de Défense (AID). Elle peut en particulier jouer le rôle de " couveuse d'entreprise " pour de jeunes startups prometteuses.

Ce lieu expérimental et unique en France est situé à Rennes.

La Cyberdéfense Factory travaille en étroite collaboration avec le cyberbooster, incubateur de startup créé dans le cadre de la stratégie nationale cyber et bi-localisé à Rennes et Paris (campus cyber).



MODALITÉS DE CANDIDATURES

https://www.defense.gouv.fr/aid/appels-projets/cours

FOCUS SUR CYKRED

Implantée au cœur d'un territoire reconnu comme l'un des pôles d'excellence français en cybersécurité, notre pépinière vous offre un cadre unique pour lancer et développer votre entreprise.

"Rejoignez la place forte de la cybersécurité à Rennes"

CYKRED, la pépinière dédiée à la cybersécurité à Rennes conçue spécifiquement pour les jeunes entreprises du secteur, CYKRED est aujourd'hui l'unique structure en France de ce niveau de sécurité entièrement dédiée à l'accompagnement des start-ups et jeunes pousses de la cybersécurité. Elle s'adresse également aux entreprises déjà établies souhaitant tester une équipe de préconfiguration avant de valider une implantation sur le territoire rennais.

Vous y trouverez :
- Une immersion au coeur d'un écosystème dynamique, au contact d'acteurs publics, académiques et industriels majeurs du secteur, implantés sur le territoire rennais (Pôle d'excellence cyber, Inria, DGA, Université de Rennes, entreprises spécialisées, etc.) ;
- Des bureaux clés en main et modulables, conçus avec des normes de sécurité durcie, répondant aux besoins spécifiques des métiers de la cyber ;
- Un accompagnement individualisé et gratuit, assuré par des experts du développement économique et de la filière, pour structurer votre activité, accélérer votre croissance et faciliter vos mises en relation ;
- Une communauté entrepreneuriale active, avec des temps d'échange, des événements thématiques, et une entraide entre pairs qui favorisent l'innovation et la montée en compétence.

Rennes, ville connectée et innovante, vous ouvre les portes d'un environnement stratégique pour vous ancrer durablement dans le paysage national et européen de la cybersécurité.

CYKRED est une pépinière de Rennes Métropole gérée par Citédia Métropole
Contact : deveco@citedia.com 02 30 96 30 03
Plus d'infos : https://www.citedia-deveco.com/

FOCUS SUR LE PÔLE DE COMPÉTITIVITÉ IMAGES ET RÉSEAUX

Le Pôle de compétitivité Images & Réseaux est dédié à l'innovation numérique en Bretagne et Pays de la Loire. Il fédère un écosystème de grands groupes, PME, startups, laboratoires et collectivités autour des technologies du numérique (réseaux, data/IA, cybersécurité, photonique, images et immersif, IoT...).

QUI SOMMES NOUS ?

Le Pôle accompagne ses adhérents dans la conception, le montage et la labellisation de **projets de R&D** collaboratifs ou individuels, favorisant leur financement et leur succès. Son expertise couvre l'ensemble de la chaîne de valeur numérique : réseaux, traitement et valorisation des données, cybersécurité, intelligence artificielle, et usages innovants.

La cybersécurité est au cœur des priorités d'Images & Réseaux. Le Pôle a conclu plusieurs conventions de partenariat, notamment avec le Ministère des Armées, affirmant son rôle clé dans la souveraineté numérique, la résilience cyber et le renforcement de l'innovation de Défense.

Le Pôle porte avec **Bretagne Cyber Alliance** et le **Pole d'Excellence Cyber** le dispositif EDIH Bretagne, qui propose des services de diagnostic, de formation et d'expérimentation pour accélérer l'adoption de la cybersécurité et de l'IA de confiance dans les entreprises et collectivités. Le Pôle est également partenaire de l'EDIH DIVA en Pays de la Loire dédié à l'IA, élargissant ainsi son action au niveau européen.

"ÊTRE LE MOTEUR DE LA TRANSFORMATION NUMÉRIQUE, au service des enjeux stratégiques de réindustrialisation, de souveraineté nationale et de développement durable."

NOTRE ACCOMPAGNEMENT

Images & Réseaux accompagne ses adhérents dans le montage de projets collaboratifs et leur recherche de financement, tout en assurant la labellisation des projets de R&D afin d'en accroître l'attractivité. Le Pôle anime l'écosystème numérique régional en organisant des événements et en favorisant la mise en relation entre acteurs académiques, industriels et institutionnels. Enfin, grâce à son rôle de partenaire au sein de l'EDIH Bretagne et de l'EDIH DIVA, il ouvre l'accès à des services européens qui stimulent la transformation numérique et renforcent la cybersécurité des entreprises et collectivités. Contact : pole@images-et-reseaux.com

CHIFFRES CLÉS

- 260 adhérents (grands groupes, PME, laboratoires, collectivités)
- 1100 projets labellisés, 570 M€ de financement mobilisés
- Comité de Sélection et de Validation de 50 experts indépendants

PRÉSENTATION DES ENTREPRISES CYBER

FOCUS SUR A3BC

A3BC a envisagé que l'avenir passe par la simplicité, la sécurité et la fluidité dans les activités quotidiennes, dans la vie et nous sommes arrivés avec une plateforme d'identité numérique révolutionnaire sans précédent.

Dinesh Ujoodah

"Dites adieu aux cartes, codes et mots de passe !"

QUI SOMMES-NOUS ?

Diplômé d'Audencia, de la London Business School et de l'Université de Columbia New York, Dinesh a plus de 25 années d'expérience dans le monde des institutions financières internationales passées chez Andersen Consulting, Accenture, IBM Global Business Services et à la Société Générale au sein de laquelle il a occupé notamment les fonctions de directeur du département d'Architecture d'Entreprise qu'il a créé et de Chief Data Officer. Ces fonctions ont amené Dinesh à co-diriger d'importants programmes de transformation et d'études stratégiques allant de 50 Millions à plus d'1 Milliard d'euros à travers de très nombreux pays dont la France, l'Italie, le Luxembourg, le Maroc, la Roumanie

NOTRE SOLUTION

A3BC développe et déploie une plateforme d'identité numérique pour construire un futur où la sécurité et la simplicité accompagneraient toutes les activités quotidiennes.
Nous avons réussi, grâce à notre identité numérique révolutionnaire intégrant la biométrie, à concilier ces deux exigences.
Nous mettons à disposition notre plateforme de services dédiés pour accompagner les entreprises à améliorer les interactions avec leurs clients dans lequel la confiance et la cybersécurité sont des pré-requis.
Contact : dinesh.ujoodah@a3bc.io

CHIFFRES CLÉS

2018 : création en France
CA sur Rennes Métropole : NC
Chiffres 2022

FOCUS SUR ACCEIS

Possédant des compétences de pointe dans les domaines à forte technicité ainsi qu'une grande expérience des processus de gestion du risque et de gouvernance cybersécurité, ACCEIS se positionne comme un partenaire global de la sécurité de ses clients.

Les co-fondateurs d'Acceis

"Une expertise de pointe et un engagement sans faille auprès de nos clients"

QUI SOMMES NOUS ?

Créé à Rennes en 2015, ACCEIS est doté du visa de sécurité de l'ANSSI. Et possède l'agrément CESTI software ainsi que la qualification PASSI. ACCEIS est un centre d'expertises en cybersécurité breton, vous accueille également à Paris. Son équipe d'experts pluridisciplinaires passionnés vous propose un accompagnement sur-mesure, complet qui se décline en trois grandes activités complémentaires : audits, accompagnement et conseil, études et évaluations.
ACCEIS a pour objectif d'accompagner de façon globale ses clients à la sécurisation de leurs activités en leur apportant les compétences hautement qualifiées grâce à son équipe d'experts. Intervenant sur le territoire national et à l'étranger, ACCEIS est impliqué auprès de tous secteurs d'activités, avec une présence marquée dans les domaines de l'industrie, de la santé, des services numériques et les institutionnels.

NOTRE SOLUTION

Nous proposons un continuum d'expertises entre des interventions techniques très pointues et du conseil stratégique en cybersécurité. Qualifiés PASSI, nous sommes le prestataire de confiance pour vos audits de cybersécurité. Notre agrément CESTI, nous permet de réaliser des évaluations de sécurité dans le cadre de vos CSPN.
Qualification PASSI RGS. Qualifié par l'ANSSI pour la réalisation d'audits de sécurité des systèmes d'information, sur l'ensemble des portées proposées par le référentiel. Grâce à l'excellence et la passion de ses auditeurs, ACCEIS totalise plus de 50 portées cumulées de qualifications PASSI qu'elle met à disposition pour les missions suivantes : tests d'intrusion, audits de code source, audits de configuration, audits d'architecture, audits organisationnels et physiques.
Cette qualification lui permet également d'intervenir sur des marchés réglementés. Agrément CESTI. ACCEIS dispose également de l'agrément CESTI (Centre d'évaluation de la sécurité des technologies de l'information) délivré par l'ANSSI. L'ANSSI s'appuie sur notre rapport d'évaluation pour délivrer une Certification de Sécurité de Premier Niveau (CSPN), permettant aux éditeurs et industriels d'attester du bon niveau de sécurité des produits et logiciels qu'ils développent et commercialisent. Contact : christophe@acceis.fr - 06 64 59 15 50

CHIFFRES CLÉS

25 experts hautement qualifiés -
35 collaborateurs
+ de 350 clients - 3M€ de CA

FOCUS SUR AKERVA

Akerva vous accompagne pour optimiser la sécurité de votre Système d'Information, de vos objets connectés et de vos systèmes industriels.

QUI SOMMES-NOUS ?

Fondé en 2013, Akerva est un cabinet conseil en cybersécurité et gestion des risques liés aux systèmes d'information. Fondé la même année, Orians est un groupe spécialisé dans le numérique qui intervient dans le domaine des services (Cybersécurité, Data Science et Transformation Numérique).

Le groupe Orians est détenu à 100% par des capitaux privés français, il est dirigé par Laurent Delaporte et Armand de Geoffre de Chabrignac.

"Assurer une gestion de la sécurité des Systèmes d'Information optimale et durable"

NOTRE SOLUTION

Akerva propose des services de conseil en gouvernance SSI, des prestations d'audits et de tests d'intrusion et de sécurité pour l'IoT et les systèmes industriels.
Via notre Security Lab, nos consultants experts sont en veille constante sur les cyber-menaces et disposent d'outils et de matériels innovants pour la réalisation de tests en conditions réalistes sur les objets connectés et les systèmes industriels.
Avec notre offre SOC – Centre de cyberdéfense, les entreprises peuvent désormais faire face aux menaces informatiques au quotidien grâce à un service de sécurité infogérée.
Akerva assure une gestion de la sécurité des Systèmes d'Information optimale et durable.
Contact : marketing@akerva.com

CHIFFRES CLÉS

18 M€ de CA
1 bureau à Rennes
Collaborateurs : + 170 (Chiffres 2022)

FOCUS SUR ALCYCONIE

Alcyconie est une société pure-player spécialisée en gestion et communication des crises cyber et numériques.
Son approche exclusive, cybercrisis management as-a-service, couvre l'ensemble des étapes de la gestion de crise avec son outil PIA®, une plateforme immersive de simulation.

Stéphanie Ledoux, fondatrice d'Alcyconie.

QUI SOMMES NOUS ?

Alcyconie est une société pure-player spécialisée en gestion et communication des crises d'origine cyber et numériques.
Fondé en 2018 par Stéphanie Ledoux, experte en gestion de crise avec plus de 10 ans d'expérience dans les secteurs de l'aérien, du ferroviaire et de l'industrie, l'entreprise prépare les organisations à affronter des crises et situations complexes et les accompagne, à chaud, lorsque les enjeux le nécessitent. Notre équipe est composée d'experts en sécurité, défense, droit du numérique, cybersécurité et communication de crise.
Alcyconie est en cours de qualification PACS par l'ANSSI.

"Société spécialisée en gestion et communication des crises d'origine cyber et numériques"

NOTRE SOLUTION

L'approche exclusive de la société d'Alcyconie, cybercrisis management as-a-service, couvre l'ensemble des étapes de la gestion de crise lors de l'avant-crise, pendant la crise et l'après-crise.
1. En préparation : Afin de prévenir les crises et de s'y préparer, Alcyconie propose des entraînements opérationnels (exercices de crise), abordant les différentes dimensions de la gestion des crises et crises cyber ainsi qu'un accompagnement dans la définition des dispositifs de crise et plans de continuité d'activités clients. Nos exercices de crise et entraînements opérationnels sont menés sur PIA®. Leur durée et niveau d'intensité sont adaptés aux enjeux et au niveau de maturité du client concerné et un scénario sur-mesure pour chaque exercice. PIA® est une plateforme de simulation permettant d'immerger les équipes décisionnelle et technique au cœur d'une crise en reproduisant, en temps réel, la pression des réseaux sociaux, des médias et des parties-prenantes. Notre outil SaaS a été développé avec le soutien de la Région Bretagne et de la French Tech.
2. En crise : nos consultants sont mobilisables 24/7 pour conseiller et épauler l'organisation concernée : pilotage de la crise, rédaction d'éléments de langage, veille renforcée, mobilisation d'experts cyber, élaboration de la stratégie de communication de crise adaptée…
3. En sortie et après-crise : Nous orchestrons, la phase de sortie de crise et l'organisation des retex dans une logique d'optimisation continue. Contact : contact@alcyconie.com

CHIFFRES CLÉS :
Fondé en 2018 - 20 collaborateurs -
150 exercices de crise réalisés en 2023
5% du CA sur Rennes Métropole

FOCUS SUR AMN BRAINS

Amn Brains développe des solutions logicielles de Gouvernance de la Cybersécurité, à destination des RSSI, des consultant et des auditeurs, principalement à destination des PME et ETI. Notre objectif est de libérer les professionnels de la cybersécurité des tâches mécaniques et de les laisser se focaliser sur ce qui apporte le plus de valeur ajoutée.

Rachid El Alaoui est le fondateur de la startup.

"Pour une gouvernance simple et rigoureuse de la cybersécurité"

QUI SOMMES-NOUS ?

Rachid EL ALAOUI est spécialiste de la cybersécurité, avec 12 ans d'expérience en tant que consultant, auditeur, architecte et RSSI à temps partiel.
Il est diplômé de Telecom Paristech en 2011. Il a commencé sa carrière dans le développement et l'intégration de solutions de sécurité, puis a pris de la hauteur au fur et à mesure en travaillant sur l'architecture SSI et sur les problématiques de gouvernance.
Son dernier poste avant de cofonder Amn Brains est "Responsable du pôle conseil SSI" chez AMOSSYS.
Aujourd'hui, Rachid codirige la société Amn Brains, éditeur de logiciels innovants de conception et de gestion de la cybersécurité.

NOS SOLUTIONS

Amn Auditor : Solution d'audit et de gestion de la conformité multi-référentiels, riche en fonctionnalités, conçue pour assister et guider les professionnels de la cybersécurité dans leurs activités, optimiser la qualité de leurs livrables et leur permettre de gagner un temps précieux.
Audit et Conseil en cybersécurité : Prestations à forte valeur ajoutée, visant principalement à accompagner le client dans l'établissement d'un état des lieux de sa cybersécurité, à définir les objectifs à atteindre en combinant une approche basée sur les risques et la conformité, puis à les atteindre grâce à un accompagnement complet et personnalisé.
Formation "EBIOS RM par la Pratique" : Une formation certifiante ayant pour principal objectif de rendre les apprenants pleinement autonomes et opérationnels, grâce à une expérience immersive basée sur un projet réaliste et des simulations de situations d'entretien, d'analyse, de rédaction et de synthèse.
Contact : contact@amnbrains.com

CHIFFRES CLÉS

Collaborateurs : 5 Collaborateurs
Clients : plus de 50 clients,
en France et à l'international

FOCUS SUR AMOSSYS

Afin de vous accompagner dans la sécurisation de votre espace numérique, Amossys met à votre disposition une offre globale de prestations permettant d'appréhender l'ensemble de vos problématiques de cybersécurité.

L'équipe Amossys

QUI SOMMES-NOUS ?

Nous avons fondé Amossys pour répondre aux problématiques croissantes de cybersécurité en présentant des offres variées et complémentaires.
Les valeurs qui nous animent au quotidien ? La passion pour notre métier, le sens de l'engagement vis-vis de nos parties prenantes et surtout l'expertise et l'innovation cyber qui sont au cœur même de notre ADN. Christophe Dupas et Frédéric Rémi ont co-fondé Amossys.

"Accompagner nos clients dans la sécurisation de leur espace numérique"

NOTRE SOLUTION

Amossys est engagée depuis sa création dans une démarche de labellisation afin de garantir à ses clients confiance et haut niveau d'expertise : Amossys est notamment Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) agréé par l'Agence National de la Sécurité des Systèmes d'Information (ANSSI) et Prestataire d'Audit de la Sécurité des Systèmes d'Information qualifié par l'ANSSI pour les besoins de sécurité nationale (PASSI RGS–LPM).
Audits de sécurité, conseil SSI, réponse à incident et investigation numérique, évaluation de produits de sécurité, formation, R&D…
Nous mettons à votre disposition une offre globale de prestations pour appréhender sereinement les risques et menaces de cybersécurité pesant sur votre système d'information ou votre espace numérique.
Contact : contact@amossys.fr

CHIFFRES CLÉS

20% des effectifs en R&D
2007 création à Rennes
Plusieurs récompenses cyber (Chiffres 2022)

FOCUS SUR ANOZR WAY

ANOZR WAY propose une suite logicielle pour réduire les vulnérabilités humaines et lutter contre les attaques par ingénierie sociale. Des réseaux sociaux jusqu'au darkweb, les données professionnelles et personnelles (empreinte numérique) ouvrant des vulnérabilités sont identifiées, maîtrisées et supervisées.

Philippe LUC - CEO et Alban ONDREJECK - CTO

QUI SOMMES-NOUS ?

ANOZR WAY est une startup rennaise spécialisée dans l'analyse des données exposées sur le web, dark web, et la protection des personnes face aux risques cyber.
Fondée en 2019 par Alban Ondrejeck, ancien officier des services de renseignement français, et Philippe Luc, ancien dirigeant dans le secteur de l'assurance,

"80% des incidents de sécurité dans l'entreprise sont liés à des vulnérabilités humaines. Il est aujourd'hui impératif d'adopter une approche centrée sur l'humain"

NOTRE SOLUTION

ANOZR WAY a développé une technologie propriétaire innovante souveraine. La solution ANOZR WAY est multi-récompensée : startup cyber du prix FIC 2023 et lauréate du Grand Défi Cyber 1 & 2 à titre d'exemples.
La suite logicielle ANOZR WAY permet aux dirigeants d'entreprises et à leurs collaborateurs de maîtriser leur empreinte numérique pour se protéger, eux et leur entreprise, face à des menaces d'ingénierie sociale, d'usurpation d'identité, d'espionnage, de ransomware, de vol de données etc.
Pour cela, la suite logicielle est composée de :
- Plateforme SaaS, destinée aux RSSI, Responsables Risques et Directeurs Sûreté. qui permet d'évaluer le niveau d'exposition cyber externe de l'organisation, ses dirigeants et collaborateurs, d'identifier les personnes les plus exposées/à risque, de corriger les vulnérabilités et superviser l'empreinte numérique globale et individuelle en continu.
- Application mobile : dédiée aux dirigeants et collaborateurs leur permettant de corriger eux-mêmes leurs vulnérabilités numériques et de protéger sphères professionnelle et privée. Contact : contact@anozrway.com.

CHIFFRES CLÉS

Collaborateurs : 50
+170% de croissance
8 M€ de fonds levés

FOCUS SUR APIXIT

APIXIT éclaire la cybersécurité, les infrastructures et le cloud des ETI et des grands comptes à travers ses 10 sites répartis dans toute la France. Nos équipes œuvrent au quotidien pour les projets clients par la mise en œuvre de solutions et services managés adaptés à leurs usages.

Fabrice TUSSEAU, Président d'APIXIT

"APIXIT éclaire la cybersécurité, les infrastructures et le cloud de ses clients."

QUI SOMMES NOUS ?

Depuis plus de 30 ans, APIXIT améliore la cybersécurité, les infrastructures et le cloud des ETI et des grands comptes à travers ses 10 sites répartis dans toute la France.
Expertes en solutions et services du numérique, les équipes d'APIXIT œuvrent au quotidien pour les projets clients, de l'étude des besoins, à l'élaboration de solutions adaptées jusqu'à leur déploiement et leur exploitation.
Pour préserver leurs infrastructures, nous avons élaboré des offres de services managés accessibles en 24/7 : support, supervision NOC et SOC, MCO, exploitation, infogérance.
APIXIT s'appuie sur un riche écosystème de partenaires et dispose des plus hautes certifications.
APIXIT est également engagée dans une démarche RSE récompensée.
En 2023, l'entreprise a rejoint le projet français du groupe Bechtle, renforçant ainsi sa capacité d'accompagnement des clients en France mais aussi en Europe.

NOTRE SOLUTION

Notre offre de solutions et services s'étend de la sécurité des infrastructure à celle du cloud. Nos équipes interviennent au dimensionnement, au déploiement et au suivi de solutions de protection éprouvées allant des parefeux aux passerelles de communications de nouvelle génération. APIXIT accompagne ses clients dans la protection de leurs ressources et de leurs outils. Pour cela, nos ingénieurs ont développé de fortes expertises en déploiement de plateformes de protection des postes de travail (EDR, NDR, XDR), de sécurité du cloud et des accès (CASB, ZTNA) mais aussi en gouvernance (veille cyber, EASM, CTI). Au quotidien, APIXIT s'attache à la valorisation d'une démarche de sécurité opérationnelle efficace, articulée autour de trois briques essentielles : anticiper, protéger, opérer. Pour cela, nos équipes déploient une gamme de services managés allant de la sensibilisation des utilisateurs aux bonnes pratiques de cybersécurité, à des services SOC complets opérés en 24/7. Audit, veille, test d'intrusion mais aussi remédiation ou encore réponse à incident font partie des prestations proposées afin d'assurer une sécurisation maximale des SI de nos clients.
APIXIT est certifiée ANSSI pour sa qualification PASSI. L'entreprise est également reconnue Expert Cyber,référencée sur la plateforme cybermalveillance.gouv.fr, certifiée ISO27001 et HDS. Autant de gages d'une expertise reconnue en cybersécurité. APIXIT est structurée afin d'assurer à ses clients un Maintien en Conditions de Sécurité optimal. Enfin, APIXIT étend son champs de compétence à la gestion de risque et à la conformité réglementaire (GRC). Contact : communication@apixit.fr

CHIFFRES CLÉS

Fondé en 1992
380 collaborateurs, 10 sites en France
90 millions d'euros de Chiffre d'Affaires

FOCUS SUR ASCENT

Ascent Formation, pure player de la formation IT, offre des solutions sur mesure en cybersécurité, data et IA, portées par des formateurs expérimentés. Fort d'une croissance de 100 % par an et de partenariats avec des entreprises du CAC 40 et Ministères Européens, notre expertise est reconnue à l'international.

Nicolas Duval, fondateur d'Ascent Formation

QUI SOMMES NOUS ?

Fondée en 2021, Ascent Formation est un pure player de la formation IT, spécialisé dans des domaines tels que la cybersécurité, la data, l'intelligence artificielle, les réseaux et bien plus encore.
Avec un champ d'action national et international, nous sommes titulaires d'une vingtaine de marchés publics majeurs, notamment avec le ministère des Armées, le secteur de la Santé, et le gouvernement de Belgique. Nous collaborons également avec de nombreuses entreprises, dont la majorité appartient au CAC 40.
Portée par une forte croissance de 100 % par an,
Ascent Formation continue de se développer et vient d'investir près d'un million d'euros dans de nouveaux bureaux pour accompagner cette dynamique.

"La formation au cœur de l'avenir technologique. "

NOTRE SOLUTION

Ascent Formation se distingue par la qualité de nos formateurs, tous experts techniques avec plus de 10 ans d'expérience. Ils interviennent à la fois pour des missions de formation et d'expertise en entreprise, garantissant ainsi une connaissance approfondie et actualisée des enjeux du terrain. Nos formations sont entièrement sur mesure, conçues pour s'adapter aux contraintes opérationnelles spécifiques des équipes de nos clients.
Nous avons la capacité de traiter les sujets les plus complexes dans les domaines que nous couvrons, offrant ainsi une réponse précise et performante aux besoins de nos partenaires. La qualité de notre service est reconnue et appréciée par nos clients, qui trouvent en Ascent Formation un partenaire de confiance pour accompagner leurs projets. contact@ascent-formation.fr

CHIFFRES CLÉS

100 % de croissance en 2025
100 formateurs
900 formations
+ 1 M€ du CA

FOCUS SUR AVOXA

Avoxa est un cabinet d'avocats qui dispose de spécialistes de la cybersécurité.

Jean-Nicolas Robin, avocat

QUI SOMMES NOUS ?

Concernant AVOXA CYBER, nous sommes le département droit du numérique/cybersécurité du cabinet d'avocats AVOXA.

Nos missions se placent dans deux grandes catégories :
- Accompagnement à la conformité/réglementation : de la conformité à la négociation contractuelle.
- Accompagnement à la suite d'un incident de cybersécurité : victime/notifications/responsabilités/assistance en justice.
- Lien avec les régulateurs et procédures judiciaires.

"Avoxa : la confiance se construit"

NOTRE SOLUTION

DPO, expert cyber, pénaliste… Avoxa a créé une " task force " cyber-data regroupant les talents de ses équipes pour mieux répondre à vos besoins liés aux nouveaux enjeux du numérique en amont et en aval de tout incident Cyber.
Contact : www.avoxa.fr

CHIFFRES CLÉS

+ de 15 ans d'expérience
80 personnes
365 jours de passion

FOCUS SUR BLOO CONSEIL

Bloo Conseil vous accompagne dans vos projets de transformation et de sécurisation de vos infrastructures informatiques.

Marc Housseau, Aurélien Magniez et
Mathieu Chauvin - Associés du cabinet

"Fournir une équipe sur mesure nécessaire à la bonne exécution de vos projets."

QUI SOMMES NOUS ?

Bloo Conseil est un cabinet d'experts indépendants en infrastructure et cybersécurité créé en 2016.
Bloo Conseil accompagne ses clients, grands comptes et PME, dans leurs projets de transformation et de sécurisation de leurs infrastructures informatiques ; du diagnostic au déploiement.
Pour ce faire, le cabinet réunit des indépendants autour de valeurs communes et d'expertises complémentaires en matière d'infrastructure et de cybersécurité : chef de projet, architecte, consultant certifié, référent sécurité.

NOTRE SOLUTION

Gestion de projet infrastructure et sécurité
Audit d'architecture
Expertise technique
Assistance et sensibilisation
Responsable informatique à temps partagé
Contact : www.bloo-conseil.fr

CHIFFRES CLÉS

Création en 2016
6 consultants IT/Sécurité séniors
18 ans d'expérience en moyenne
Label Expert Cyber depuis 2022

FOCUS SUR CAILABS

Cailabs est une entreprise française de deep tech, basée à Rennes, qui conçoit, fabrique et vend des solutions dans le domaine de la photonique.

L'équipe de Cailabs

QUI SOMMES-NOUS ?

Cailabs maîtrise la mise en forme de la lumière pour concevoir, fabriquer et vendre des produits photoniques innovants dans les transmissions en espace libre, les lasers industriels, les réseaux locaux et les télécommunications.

"Nous créons des produits qui aident à résoudre certains des grands défis"

NOTRE SOLUTION

Nous proposons des produits sur mesure. Par exemple, la solution TILBA améliore la fiabilité des liaisons satellitaires mais aussi navale, aéronautiques (avions, drones) ou terrestres. Elle repose sur une technologie unique au monde de multiplexage et démultiplexage spatial permettant de manipuler les formes de la lumière.
Avec cette ligne de produits, les communications optiques deviennent accessibles et facilement déployables grâce à des composants standards, embarquables et faciles d'utilisation.
Les différents produits de la gamme TILBA sont :
TILBA-ATMO, un module de compensation de la turbulence atmosphérique à la réception collectant un faisceau turbulent vers une fibre optique monomode standard.
TILBA-EMIT, un combineur de faisceau cohérent permettant d'augmenter la puissance des sources à l'émission.
Cailabs est en mesure d'accompagner vos projets de liaisons optiques à plusieurs niveaux d'intégration, du composant jusqu'à la station sol.
Contact : contact@cailabs.com

CHIFFRES CLÉS

Collaborateurs : + de 100
2013 création
44% de femmes manageuses (Chiffres 2022)

FOCUS SUR CALIDRA

Calidra est une solution de sensibilisation à la cybersécurité, offrant des modules d'e-learning sur une plateforme SaaS combinés à des simulations de phishing. Elle est entièrement personnalisable selon la maturité cyber des collaborateurs et leur criticité métier. Conçue pour toutes les tailles d'entreprises, elle accompagne l'évolution cyber des employés et vise à réduire les risques d'attaques et de fuites d'informations. Une équipe de consultants assure un suivi tout au long du programme pour garantir un accompagnement optimal.

Un des dirigeants de Calidra

"Replacer le facteur humain au centre de la stratégie cyber."

QUI SOMMES-NOUS ?

Calidra offre une solution innovante de sensibilisation à la cybersécurité, adaptée aux entreprises de toutes tailles et secteurs. Grâce à un audit de maturité en conditions réelles, Calidra évalue la vigilance de vos collaborateurs face aux attaques de phishing, permettant ainsi de définir une stratégie de prévention cyber personnalisée.
Nous proposons des formations e-learning et des simulations de phishing sur mesure, tenant compte du contexte métier et local de chaque client, afin de renforcer les réflexes de sécurité de vos équipes. Chaque collaborateur bénéficie de supports et programmes adaptés à son niveau de vigilance et à ses missions quotidiennes.
En intégrant des mesures proactives et un suivi personnalisé, Calidra offre une solution complète qui aide les DSI, DPO, RSSI et dirigeants à réduire significativement le risque de cyberattaques, notamment face à la menace numéro un : le phishing.

NOTRE SOLUTION

Une seule plateforme pour votre programme de sensibilisation cyber !
Calidra propose une plateforme complète pour gérer toutes les activités de vos programmes de sensibilisation cybersécurité : formation, sensibilisation, simulation d'attaques par ingénierie sociale (phishing,...).
Sensibiliser est devenu simple avec Calidra grâce au service managé et aux ressources mises à disposition, le contenu est totalement personnalisable et adaptable à votre structure : type, taille et activité métier.
Nous avons conçu notre plateforme pour qu'elle soit engageante et intuitive, en intégrant un système de gamification (avec des éléments comme le CyberScore, un esprit de compétition sain et des contenus interactifs). Cela permet de stimuler l'engagement des collaborateurs et de les inciter à se former efficacement tout en s'amusant.
Contacts : CEO Ayoub Sabbar a.sabbar@calidra.io / Business Manager Neïla Djermoune n.djermoune@calidra.io

CHIFFRES CLÉS

Fondée en 2023
Collaborateurs : 6
Clients : + de 20 clients tous secteurs

FOCUS SUR CEEBEX

CEEBEX est un organisme de formation en cybersécurité qui propose des formations adaptées aux entreprises et aux professionnels. Avec une équipe d'experts, CEEBEX offre un accompagnement sur mesure pour aider les organisations à développer les compétences de leurs équipes face aux défis de la cybersécurité.

"Centre de formation cybersécurité, engagé pour l'excellence."

QUI SOMMES NOUS ?

CEEBEX est un organisme de formation spécialisé en cybersécurité qui propose des formations adaptées aux besoins des entreprises et des professionnels. Avec une équipe d'experts, CEEBEX accompagne les organisations dans la montée en compétences de leurs équipes pour faire face aux défis actuels de la cybersécurité. L'organisme propose des formations sur mesure, des ateliers pratiques, et des certifications pour renforcer les connaissances et les compétences en matière de sécurité informatique.
En se positionnant comme un partenaire de confiance, Ceebex met l'accent sur la qualité de l'accompagnement, la transmission des connaissances, et la mise en pratique des compétences essentielles pour protéger les systèmes d'information.

NOTRE SOLUTION

Ceebex propose quatre pôles de formation en cybersécurité :
Sécurité Organisationnelle : Formations ISO27001 Lead Implementer/Auditor, EBIOS Risk Manager, et CISSP pour maîtriser les normes de gestion de la sécurité.
Sécurité Opérationnelle : Formations autour de la sécuriser systèmes et réseaux, de la gestion des incidents, et la protection des SI des entreprises.
Sécurité Offensive : Techniques de tests d'intrusion et évaluation de la sécurité pour anticiper et contrer les cyberattaques.
Continuité d'Activité : Mise en place de plans de continuité et de reprise d'activité.
CEEBEX propose à la fois des formations sur catalogue, et des formations sur mesure pour répondre à chaque besoin. Les formations sont disponibles en présentiel, à distance, ou en e-learning, avec des options sur mesure. Ceebex, certifié Qualiopi, garantit une expertise de haut niveau. Contact : a.sabbar@ornisec.com

CHIFFRES CLÉS

Fondé en 2023
Collaborateurs : 2
CA sur Rennes Métropole : 100k€

FOCUS SUR CLARANET

Claranet dispose d'experts de la modernisation et du run des applications critiques, des datas et de l'infrastructure en 24x7

Claranet

QUI SOMMES-NOUS ?

Claranet accompagne ses clients dans leur transformation digitale. Chaque entreprise, quel que soit son secteur d'activité, est amenée à se digitaliser et donc à manipuler des applications. Ces applications deviennent très vite critiques, elles ont besoin d'être gérées et contrôlées dans un environnement qui évolue sans cesse. C'est là que nos experts interviennent.
Nous sommes reconnus pour nos recherches sur les menaces de sécurité les plus récentes, et cette connaissance enrichit en permanence tous nos travaux en matière de cyber sécurité. Ce que nous apprenons des tests d'intrusion sur le terrain alimente nos formations, et inversement. Tout le monde y gagne !
Pour assurer la sécurité de vos applications, un management opérationnel par des experts sécurité est indispensable.

"Un pôle d'expertise dédié à la sécurité pour prévenir et protéger vos applications"

NOTRE SOLUTION

Pour vous accompagner, nous mettons à votre disposition une cellule dédiée.
Celle-ci est composée d'experts sécurité, de pentesters, de chefs de projets spécialisés dans la protection de vos données.
Certifiés, ils assurent une veille quotidienne des vulnérabilités et se forment régulièrement aux nouveaux outils afin de vous assurer le meilleur niveau de protection.
Contact : Sandrine.bajolet@fr.clara.net

CHIFFRES CLÉS

Création 1996
+ de 2500 collaborateurs (Chiffres 2022)

FOCUS SUR CLOUD IAM

Basé sur la solution open-source Keycloak, leader dans le domaine de l'IAM, Cloud-IAM supervise l'entièreté du cycle de vie des déploiements et fournit une version complète de Keycloak sans surcouche, entièrement configurable et personnalisable tout en assurant une haute disponibilité avec SLA, ainsi qu'un support 24/7.

QUI SOMMES NOUS ?

Fondé à Rennes en 2019 par Sébastien Brousse et François-Guillaume Ribreau, deux architectes cloud et dev ops avec plus de 10 ans d'expérience.
Notre objectif est de répondre aux enjeux de souveraineté numérique en fournissant à nos clients, une solution avec une réversibilité totale et un contrôle complet sur leurs données.
Notre expertise Keycloak, nous permet d'accompagner tout type d'entreprise dans leur projet de gestion des identités, tout en les soulageant de la supervision et du maintien de leur Keycloak.

"Fournisseur d'IAM SaaS entièrement managé."

NOTRE SOLUTION

Cloud-IAM fournit des déploiements Keycloak prêt à l'usage, sans surcouche, entièrement personnalisable et configurable, permettant l'ajout de plug-in, d'application custom sans contrainte et la connexion à des solutions de fédérations des utilisateurs.

Notre produit permet de répondre à trois principaux cas d'usage, l'IAM, le CIAM et l'IdP Broker. Les principaux protocoles d'authentifications (OAuth 2.0, SAML, OIDC, etc) sont intégrés nativement, ainsi que les technologies d'authentification comme le SSO, MFA, etc. L'hébergement multi-cloud est garanti par Cloud-IAM et laisse le choix du fournisseur cloud aux clients parmi deux clouds français Outscale (SecNumCloud, HDS), Sacelway ou américain GCP, AWS et Azure sur cinq continents.

Cloud-IAM expose les logs et métriques, avec la possibilité d'exporter l'intégralité des données des déploiements automatiquement via une API. Une haute disponibilité garantie des services avec des SLA de 99,95%. En cas d'incident, une équipe d'astreinte est disponible 24/7.

Les services de Cloud-IAM sont certifiés ISO 27001 de bout en bout, conforme au RGPD et permet une conformité NIS2.
Présent sur les marchés de l'UGAP et de la Canut.
Contact : support@cloud-iam.com

CHIFFRES CLÉS

Fondé en 2019
10 collaborateurs
1,3M€ du CA sur Rennes Métropole

FOCUS SUR CT SQUARE

CT-Square est une société de Cybersécurité qui propose aux PME et ETI de mesurer la résilience de leur système d'information face à une attaque informatique, puis de le superviser via un service de détection de type SOC. CT-Square propose des services d'audit (dont des tests de pénétration), de conseil, de formation et de supervision de sécurité.

L'équipe de CT Square

QUI SOMMES-NOUS ?

CT-Square se distingue par le fait qu'elle a développé en interne tous les outils techniques nécessaires et disposant d'une grande agilité pour répondre rapidement et efficacement aux besoins de ses clients comme à l'évolution de la menace.
CT-Square repose sur une équipe d'experts et d'ingénieurs confirmés provenant de différents secteurs de la société, anciens des forces armées comme universitaires, ce qui lui permet de combiner approche opérationnelle et créativité technologique.

CT-Square est lauréat du " Grand Défi Cyber " (SGPI) dans le cadre du Programme d'Investissement d'Avenir (PIA).

"L'agilité pour réagir vite"

NOTRE SOLUTION

Nous agissons au plus proche de nos clients afin d'assurer la sécurité de leur système d'information en les accompagnant grâce à nos experts et des offres de services éprouvées sur le marché.
- Diagnostic cyber : audit organisationnel et technique des systèmes d'information. L'objectif est de donner la juste visibilité sur les risques du SI au dirigeant et amorcer un plan d'action concret pour les équipes techniques.
- Remédiation : la continuité de la phase de diagnostic pour la mise en place des mesures de protections adaptées.
- Accompagnement cyber : communication avec vos équipes IT ou prestataires informatiques afin de conseiller et assurer la fiabilité du SI et son exploitation.
- SOC Managé : monitoring en temps réel de vos infrastructures par la mise en place de notre SIEM sur votre réseau et assurée par nos experts niveau 2 et niveau 3.
- Phishing & sensibilisation : sensibilisation (dirigeants, employés…) personnalisée selon votre métier ; mise en place des campagnes de Phishing.
- Réponse à Incident : nous nous tenons disponible en cas d'alerte avérée sur votre SI pour contrôler et éradiquer la menace.

CHIFFRES CLÉS

Création en 2016 + de 100 clients
12 Collaborateurs - 100% souverain
LAURÉAT DU GRAND DÉFI CYBER

FOCUS SUR CYBERMYNE

CYBERMYNE est une ESN équitable, à impact sociétal, basée sur Rennes.
Notre objectif: proposer un nouveau modèle de société, plus juste, pour une sécurité numérique accessible à tous.

Agathe Desflots Fondatrice de Cybermyne

"Nous Engager, c'est Vous Engager ! "

QUI SOMMES-NOUS ?
Société équitable, nous travaillons en transparence avec nos collaborateurs et partenaires sur les marges et tarifs pratiqués.
Les employés sont invités à rentrer au capital à partir d'un an d'ancienneté.
Nous croyons en l'intelligence collective.

Société à mission, nous intervenons bénévolement, tous les mois, dans le grand public, pour partager les bonnes pratiques d'hygiène et de sécurité numérique.
Nous pratiquons le partage.

NOTRE SOLUTION
Nos solutions s'adressent à tous types de sociétés, de la TPE (solo-entrepreneur) aux grands comptes du CAC40.
Une ESN CYBERMYNE avec l'HUMAIN au coeur :
- Délégation de personnel (collaborateurs, associés ou freelances de notre écosystème)
- Recrutement
- Sensibilisation et/ou Conseils

Des offres SERENNIS : pour une sécurité simplifiée au service de votre Autonomie
- serennis Cyberassurance (Stoïk)
- serennis Conformité RGPD (MyDPO)
- serennis Sauvegardes et stockages

Contact : https://www.cybermyne.fr/

CHIFFRES CLÉS
Création : 2023 - CA Rennes 2025 : 440K€
Collaborateurs : 6+
Clients : ENEDIS / MYTILIMER / APIXIT / ORANGE CYBERDEFENSE / CS GROUPE / ...

FOCUS SUR CY MIND

Créée en 2019, Cy Mind se distingue par une approche unique de la cybersécurité cognitive, axée sur l'humain et intégrant les sciences comportementales et les neurosciences. Ce qui fait la valeur ajoutée de Cy Mind, c'est sa capacité à transformer la manière dont les organisations abordent la gestion des risques humains en cybersécurité. Avec plus de 93% de satisfaction parmi ses clients, Cy Mind apporte une vraie expertise éprouvée, reconnue et une approche innovante, plaçant l'humain au cœur de la cybersécurité.

"HUMAN VISION FOR CYBERSECURITY
Notre objectif est de contribuer chaque jour à un monde meilleur"

NOTRE SOLUTION

Service complet de cyberprotection :
Se préparer - Gérer - Rebondir
https://www.cymind.fr
Contact : contact@cymind.fr

CHIFFRES CLÉS

2021 Lauréat Grand Défi Cyber
+ de 1000 professionnels formés grâce à notre méthodologie Cyberprotection
2025 Franchise Cy Mind & les cyberfresqueurs

QUI SOMMES-NOUS ?

Chez Cy Mind, nous accompagnons les entreprises de toutes tailles en leur proposant des solutions selon leurs temporalité : Se préparer - Gérer - Rebondir. En tant que fournisseur indépendant, notre priorité est d'adapter nos services aux besoins spécifiques de chaque client, assurant ainsi une protection complète et personnalisée. Grâce à notre méthodologie innovante, nous vous aidons à renforcer la cyberprotection de vos équipes face aux cybermenaces actuelles tout en améliorant l'engagement et la compréhension de vos collaborateurs.
Notre métier peut prendre différentes formes : Cy Mind est spécialisé dans la cybersécurité cognitive, en proposant des solutions adaptées aux besoins uniques de chaque entreprise. Nous offrons plusieurs services, notamment :
• Formation /sensibilisation : Ateliers ludiques et serious game interactifs tels que la Fresque de la Cyber et le CY-rious Game, qui sensibilisent vos équipes aux risques humains liés à la cyberprotection.
• Gestion de crise : Nous vous proposons un accompagnement expert pour renforcer la cohésion de vos équipes en période de crise cyber, tout en gérant efficacement le stress et les émotions. Nos interventions sont conçues pour aider vos collaborateurs à maintenir leur performance et à traverser les moments critiques de manière sereine et résiliente.
• Assistance post-incident : Nous offrons un soutien personnalisé pour renforcer la résilience de vos équipes après une cyberattaque, en minimisant les impacts socio-psychologiques à long terme. Profitez de notre pack initial de 6 heures en visioconférence, conçu pour apporter des solutions concrètes et un accompagnement immédiat dans la gestion de crise.

FOCUS SUR DASPREN

Daspren est une startup cyber deeptech spécialisée dans la protection des données. Elle développe une solution innovante basée sur de l'intelligence artificielle "Data-centric" pour détecter et stopper toutes les attaques sur les données : ransomware, exfiltration, destruction. Daspren est issue d'un transfert technologique de l'Inria.

Belkacem Teibi, Directeur général et Mathieu Thiery, Directeur technique.

QUI SOMMES NOUS ?

Belkacem TEIBI est cofondateur et CEO de Daspren. Il est ingénieur en sécurité informatique avec une dizaine d'années d'expérience dans l'industrialisation et le transfert de l'innovation au sein d'Inria. En 2021, il a obtenu son diplôme en Executive MBA à Rennes School Business.

Mathieu THIERY est cofondateur et CTO de Daspren. Il a obtenu son doctorat en sécurité et protection de la vie privée, délivré par l'Université de Grenoble, au sein de l'équipe Privatics (Inria). Il a notamment une expérience en développement cryptographique.

"Défendre vos données face aux cyberattaques inconnues"

NOTRE SOLUTION

Nous avons développé un logiciel de protection contre toutes les menaces ciblant les données y compris les menaces zero-day (c'est-à-dire sans antécédent connu), donc encore inconnues par les antivirus et EDRs. Les cas d'usage de la solution de Daspren sont : Cartographie des données, détection de l'exfiltration, détection de ransomware, détection de menace inconnues. Les cas d'usage à venir : Classification, conformité, protection de l'AD. Cette technologie, brevetée est indépendante de toute base de connaissance et s'appuie sur de l'intelligence artificielle avec une nouvelle approche " data-centric ".
Contact : contact@daspren.com

CHIFFRES CLÉS

+80% effectif R&D
Des millions d'accès aux données analysés par seconde
Parmi les 1% des startups mondiales retenues par Berkeley SkyDeck

FOCUS SUR EASYLIENCE

Fondée en 2016, 100% française, pionnière du pilotage des situations de crise. Notre solution et services sont à destination des institutions étatiques, OIV / OSE et grands comptes. Nos experts R&D et consultants, passionnés du pilotage, vous accompagnent dans vos projets de numérisation des dispositifs de veille, incidents et crises quelque soit votre contexte.

Les consultants dédiés aux grands comptes.

"easylience®, c'est plus qu'un éditeur de logiciel, ce sont des spécialistes du process de pilotage qui adaptent la solution à vos métiers et contraintes"

QUI SOMMES NOUS ?

Thierry de Ravel, Président de Nanocode est dirigeant d'entreprise depuis plus de 15 ans. Ses équipes interviennent comme conseillers au pilotage de crise, auprès de grands groupes, avec la solution de gestion de crise "easylience®".
easylience® est :
- Une plateforme (SaaS) no-code résiliente* 100% française. Ce dispositif couvre les processus de veille, d'incident et de crise pour chaque organisation indépendamment de son système d'information nominal.
- Une équipe d'experts du pilotage de crise, dédiée à la transposition de vos problématiques dans une solution numérique et spécialisée dans la réingénierie et l'optimisation de vos dispositifs.

NOTRE SOLUTION

Après plus de 5 ans de R&D, nous avons développé une plate-forme collaborative " tout en un " accessible sur tout type d'équipement, afin d'assurer :
- La conception et le maintien en conditions opérationnelles de vos dispositifs.
- La gestion des événements en continu : > Anticipation (veille et analyse > Gestion et qualification des alertes et incidents (manuelle et automatisée) > Activation des dispositifs exceptionnels (alerting de masse et centre de communication exclusif) > Pilotage de la situation critique (modules dédiés) > Sortie de crise (Retour d'expérience et audit).
- La formation et la réalisation d'exercices de crise.

easylience® vous propose une équipe de spécialistes pour vous accompagner sur toutes les phases de votre projet peu importe la complexité et la maturité de votre organisation. Ces experts du pilotage oeuvre à formaliser vos contraintes métiers sous forme de processus numérisés et accessibles à tous les acteurs de la gestion de crise quelel que soit leur acculturation. Notre société est certifiée ISO 27001 (Système management de la sécurité) et 22301 (Continuité d'activité) par l'Afnor. Solution accessible sans interruption et hautement redondante, nous proposons des offres certifiées SecNumCloud et HDS. Contact : contact@easylience.com

CHIFFRES CLÉS

+ 200 000 utilisateurs + 150 pays déployés + 1000 crises traitées en 2025 - 80% des effectifs à Rennes - easylience® a été utilisée par des ministères de l'état français et des OIV officiels de l'évènement en veille et en crise.

FOCUS SUR CABINET EON-JAGUIN

Le Cabinet EON-JAGUIN est un cabinet d'avocats d'affaires expert en droit des contrats, du numérique et de la santé.

Photo de Florence EON-JAGUIN, fondatrice du Cabinet

"La prise en compte des exigences réglementaires de cybersécurité "by design"est un investissement pour garantir la pérennité et la conformité de votre activité."

QUI SOMMES NOUS ?

Nous vous aidons à relever les défis juridiques de l'ère numérique, quel que soit votre statut, que vous soyez pour un industriel (hébergeur, éditeur, fabricant de produit de santé, etc.), un professionnel de santé, une structure sanitaire ou médico-sociale, ou un fonds d'investissement ou encore un acteur public de la santé.
Nous vous conseillons, nous rédigeons et négocions vos actes juridiques en intégrant les exigences légales de cybersécurité. A cet effet, nous échangeons régulièrement avec vous dans une approche simple et opérationnelle.
Nous sommes réactifs pour que vous puissiez compter sur nous à tout moment !
Nous avons aussi des partenaires fiables et compétents pour vous offrir un accompagnement complet et fluide.

NOTRE SOLUTION

Vous accompagner en étant réactif et pragmatique pour intégrer les exigences réglementaires de cybersécurité.
Contact : 06 81 29 81 43

CHIFFRES CLÉS

Création du cabinet :
2024

FOCUS SUR ERIUM

Acteur leader de l'écosystème cyber français, Erium développe des solutions de cybersécurité dont 'Cyber Investigation' une plateforme formation et la solution BlackNoise (Breach & Attack Simulation).

Florent SKRABACZ (g.) Président, Arnaud LE MEN (d.) Directeur Général

QUI SOMMES-NOUS ?

Erium est un pure-player de la cybersécurité Française. Créée en 2012 et reconnue pour son expertise sur les métiers de la sécurité opérationnelle (SOC, CERT, FIR, Hunting, Gestion de crise…), la société accompagne ses clients avec ses équipes d'experts et en développant des solutions innovantes.

Les équipes sont réparties entre les sites de Rennes (Direction Technique et R&D) et de Paris (Siège) et sont composées de ~50 collaborateurs.

"Nous créons des solutions qui permettent à nos clients de se former, s'entraîner et renforcer leurs capacités de défense pour faire face aux menaces Cyber"

NOTRE SOLUTION

BlackNoise est une plateforme de Breach and Attack Simulation (BAS) et de validation de la sécurité. La plateforme permet de reproduire, automatiquement et en toute sécurité, les modes opératoires d'attaque cyber les plus complexes (ex: APT, ransomwares, wiper, databreach, insider threat,…) sur tous les environnements informatiques, incluant le monde industriel et l'ensemble de la supply chain. Le déploiement de la solution est rapide et permet de valider en continu le bon fonctionnement des capacités de détection, de mettre en lumière les éventuels angles morts et de mesurer objectivement l'efficacité de la réaction défensive.
La mise en oeuvre de la plateforme permet de construire une lecture objective du niveau d'efficacité cyber mesuré en conditions réelles. Nos clients y voient un bénéfice pour mesurer un ROI opérationnel des investissements cyber, démontrer un niveau de conformité et entraîner les équipes techniques. CyberInvestigation est la plateforme de formation et de sensibilisation cyber de référence des RSSI et DSI. Avec des milliers de contenus, des speedquiz et des formats événementiels, CyberInvestigation positionne l'humain au cœur de la défense cyber. Disponible dans un modèle SaaS, la plateforme s'intègre complètement dans les SI d'entreprise (O365, API LMS) et intègre un tableau de bord de reporting et de conformité (NISv2, DORA, RGPD) particulièrement apprécié.

CHIFFRES CLÉS

Collaborateurs : ~50
Clients : défense, industrie, finance, public…
+20% du CA investi en R&D

FOCUS SUR FairTrust

FairTrust est un éditeur logiciel de solutions de cybersécurité : nous croyons que toutes les entreprises ont droit à la meilleure sécurité, quelles que soient leurs tailles ou leur activité.

"L'engagement d'une sécurité renforcée par l'alliance d'un contrôle d'accès moderne et d'une gestion des identités professionnelle"

QUI SOMMES NOUS ?

Issues d'horizons variés, les équipes de FairTrust bénéficient d'une expérience de plus de 25 ans dans la conception, le développement et la commercialisation de solutions de cybersécurité.
FairTrust est créée à l'image de ses dirigeants, de leurs valeurs et en réponse à une vision partagée de la nécessité d'équiper les entreprises de toutes tailles et dans tous les métiers de solutions de cybersécurité performantes, professionnelles et rapidement opérationnelles.
En mutualisant nos compétences dans les domaines de l'ingénierie, du développement, du commerce et du marketing, nous avons bâti un socle fiable et pérenne pour le développement de notre activité sur le marché Français et Européen. Notre volonté à proposer des solutions souveraines est illustré par notre engagement dans le groupement HexaTrust.

NOTRE SOLUTION

Dans le cadre de la gestion des identités (IAM) et des accès (SSO, coffre-fort numérique), nos solutions fournissent des fonctionnalités d'authentification forte des utilisateurs, de gestion du cycle de vie des mots de passe, des identités et des habilitations. En automatisant les processus, la gestion des identités renforce la sécurité et la conformité, réduit les charges administratives, minimise les erreurs humaines associées aux tâches manuelles.
Elle permet d'implémenter une séparation appropriée des tâches (SoD) et des principes de moindre privilège (Zero Trust) conformément aux réglementations comme HIPAA, NIS2, GDPR et PCI DSS.
Disponibles sur site ou en mode hébergé, nos solutions sont rapidement opérationnelles et nativement modulables et extensibles pour accompagner les évolutions des besoins et des infrastructures des systèmes d'informations modernes.
Contact : https://www.fairtrust.com/contactus

CHIFFRES CLÉS

Création en 2021
7 collaborateurs
Plus de 300 000 utilisateurs en Europe, Amérique du Sud et Asie.

FOCUS SUR FOLIATEAM

FOLIATEAM offre un catalogue complet de solutions cybersécurité et protection des données. Spécialiste du cloud privé d'entreprise, le centre de services de Pacé est certifié HDS sur les 6 domaines d'activité. Les clients bénéficient également de services SOC proposés par le groupe.

L'équipe Foliateam de l'agence de Pacé

"Plus qu'un prestataire, faites le choix d'un partenaire qui optimise votre IT"

QUI SOMMES NOUS ?

Avec plus de 20 ans d'expérience au cœur de la transformation des environnements informatiques, Foliateam accompagne les entreprises dans l'utilisation, l'optimisation et la sécurisation de leur IT : hébergement de données, performance de l'infrastructure, optimisation des réseaux, communication unifiée, infogérance, et bien sûr cybersécurité.
Avec des usages qui mutent au rythme des évolutions technologiques, l'approche 360° de FOLIATEAM s'adapte aux nouvelles habitudes de travail et de collaboration.
Ces services invitent les entreprises à se doter de solutions souples et évolutives pour soutenir le développement de leur activité. Certifié ISO27001 et HDS, FOLIATEAM est hébergeur de données sensibles et propose une large gamme de solutions : PRA/PCA, EDR/XDR, microSOC, etc...

NOTRE SOLUTION

Audit cybersécurité, plan de sauvegarde, gestion et protection des endpoints, solutions d'authentification pour la sécurité des accès et des identités, EDR/XDR, anti-spams, sensibilisation des utilisateurs.
Pour soutenir vos projets de bout en bout, Foliateam vous propose un ensemble de services portés par des experts qui vous accompagnent à chaque étape : un commercial dédié pour chaque compte, des consultants ou encore chefs de projet et ROC. Un centre des usages unique pour tester vos solutions avec nos customer success specialists ainsi qu'un catalogue de formations certifiées pour vos utilisateurs. Enfin, nos centres de services répondent à vos besoins partout en France. Ils s'assurent du bon fonctionnement de vos équipements et applications et veillent à renforcer leur sécurité. Toutes nos solutions cyber sont supportées par nos services managés et notre SOC.
Contact : chloe@foliateam.fr

CHIFFRES CLÉS

25 ans d'expertise
400 collaborateurs
5 600 clients
7M€ du CA sur Rennes Métropole

FOCUS SUR FORMIND

Formind est un leader français indépendant expert en cybersécurité qui aide ses clients à être plus résilients et à se protéger des risques numériques à travers ses trois métiers : conseils - intégration - SOC (Security Operation Center et CERT (Computer Emergency Response Team).

QUI SOMMES-NOUS ?

Qualifié PASSI, en cours de qualification PRIS par l'ANSSI et certifié ISO 27001, Formind est un pure player de près de 270 collaborateurs aux différentes expertises.

"Notre conviction : la sécurité est un levier majeur de performance des entreprises !"

NOTRE SOLUTION

- Gouvernance Cyber : stratégie, gestion des risques, pilotage et contrôle
- Continuité, gestion de crise et résilience
- Conformité légale, réglementaire et normative
- Expertise technique, architecture, Cloud, IAM, OT
- Intégration de solutions
- Audits techniques, sûreté, Redteam,
- Services managés (CERT, SOC, vulnérabilités) et gestion d'incident (FIR)
- Formation

Formind propose également une offre dédiée au tissu économique des ETI et PME-PMI, venant répondre à leurs problématiques spécifiques de cybersécurité. Créé à Paris, Formind s'est rapidement déployé à Toulouse, Bordeaux, Lyon, Rennes, Nantes ainsi qu'au Maroc, en Espagne et au Canada.
Site web : www.formind.fr - contact@formind.fr - Linkedin/company/formind

CHIFFRES CLÉS

Collaborateurs : 270+
+ de 486 clients
9 antennes sur 3 continents

FOCUS SUR GARNAULT & ASSOCIES

Spécialisée dans les secteurs des relations institutionnelles, de la transformation numérique, de la cybersécurité & de la cyberdéfense, Garnault & Associés est une agence de communication unique.

L'équipe de Garnault et associés

"Connecting people to empower Trust"

QUI SOMMES NOUS ?

Expert des réseaux, de la décision et de l'influence, Garnault & Associés accompagne ses clients grâce à son savoir-faire unique en termes d'impact et de rayonnement. Des affaires publiques aux relations institutionnelles et corporate, nous utilisons notre savoir faire stratégique pour promouvoir l'expertise et la vision de nos clients lors d'événements d'exception et sur-mesure, en nous appuyant sur un réseau robuste de décideurs publics et privés, nationaux et internationaux. Notre équipe est composée de professionnels expérimentés, réactifs et disponibles, qui ont une connaissance approfondie des rapports politiques publiques et de gouvernance. Nous travaillons en étroite collaboration avec nos clients pour comprendre leurs enjeux et développer des solutions qui leur correspondent.

NOTRE SOLUTION

L'agence a organisé de nombreuses conférences et réunions réunissant dirigeants d'entreprises et décideurs publics tels que la première Cyber Defence Pledge Conference de l'OTAN à Paris (2018), la European Cyber Week et le Paris Cyber Summit (depuis 2019) et Washington's Unplugged (depuis 2023).
Aujourd'hui, ce sont près de 300 de tables rondes, 250 réunions de travail et 30 délégations qui ont été menées en France, en Europe et aux États-Unis.
Garnault & Associés est basé en Bretagne, au coeur des capacités cyber françaises.

CHIFFRES CLÉS

10 domaines d'expertise
3 collaborateurs
45 clients - 2% du CA sur Rennes Métropole

FOCUS SUR GATEWATCHER

Leader dans la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux critiques des entreprises et des institutions publiques à travers le monde. Ses solutions associent l'IA aux dernières techniques d'analyse pour offrir une vision à 360° des cybermenaces sur l'ensemble du réseau, dans le cloud et on premise.

L'équipe

QUI SOMMES-NOUS ?

Gatewatcher couvre les techniques d'attaques les plus élaborées et identifie les éléments spécifiques à chaque type de cybermenace pour une protection maximale.
Le modèle de protection de Gatewatcher associe des technologies de pointe à une approche multi-vecteurs et cible les comportements anormaux en effectuant une analyse dynamique des signaux faibles provenant des flux du réseau. Ses solutions s'adressent tant aux grandes organisations publiques et privées qu'aux ETI, PME et collectivités à la recherche d'une capacité de détection des menaces optimale, grâce à des solutions rapidement opérationnelles et évolutives, interopérables et capables de s'intégrer rapidement et nativement dans la plupart des écosystèmes de sécurité existants.
Présent en Europe, en Afrique, au Moyen Orient et en Asie, Gatewatcher s'appuie sur un large réseau de partenaires et d'alliances technologiques pour élaborer et distribuer ses solutions innovantes.

"Cybersecurity for business serenity"

NOTRE SOLUTION

Nos solutions de Network Detection and Response (NDR) et de Cyber Threat Intelligence (CTI) analysent les vulnérabilités, détectent les intrusions et répondent rapidement à toutes les techniques d'attaque. Elles combinent des algorithmes d'apprentissage automatique avec différentes méthodes d'analyse du trafic réseau et sont conçues pour être évolutives et immédiatement opérationnelles pour une intégration facilitée dans les SOC (Security Operations Center).
Notre plateforme de NDR ouverte offre une cartographie et une analyse comportementale des menaces pour une détection augmentée et une visibilité inédite sur les attaques ciblées.
Notre solution de CTI enrichit votre détection par des informations contextuelles sur les menaces ciblant votre activité.
Parfaitement interopérables avec des équipements de type sonde, notre gamme de TAP vous permet de répliquer l'intégralité de votre trafic vers vos outils de surveillance.L'excellence technologique des solutions Gatewatcher est reconnue par les experts de la cybersécurité, ainsi que par les institutions publiques et entreprises d'industries critiques (banques, assurances, énergie, transports, retail, télécommunications, défense...). Gatewatcher est par ailleurs qualifiée par l'ANSSI. Contact : aubin.debelleroche@gatewatcher.com

CHIFFRES CLÉS

Collaborateurs : 150
Une vision à 360°
et en temps réel des cybermenaces

FOCUS SUR GEOIDE Crypto&Com

GEOIDE Crypto&Com est une société qui conçoit, fabrique et commercialise des solutions matérielles de protection de réseaux OT pour les forces armées, les opérateurs d'importance vitale, l'industrie 4.0, l'aéronautique et le monde ferroviaire.

QUI SOMMES-NOUS ?

Société française fondée en 2015 par Grégory GILLE, GEOIDE Crypto&Com a choisi d'implanter son pôle R&D dans le Pays rennais en 2022.
Installée au sein de CyberPlace début 2024, GEOIDE Crypto&Com poursuit sa croissance en s'appuyant sur la richesse de l'écosystème local.
Experte reconnue des protocoles militaires et industriels, la société se spécialise aussi dans les technologies optiques pour compléter son offre de sécurité pour les acteurs les plus critiques.

"Nos produits lèvent les verrous technologiques et organisationnels"

NOTRE SOLUTION

GEOIDE Crypto&Com conçoit et fabrique des solutions matérielles de protection de réseaux certifiées par l'ANSSI et homologuées dans les armées à destination des infrastructures critiques, civiles ou militaires.
Son offre s'articule autour de:
- Bwall, parefeu français spécialisé dans le cloisonnement de réseaux.
- GDD, diode optique qui réussit à réconcilier très haut débit et très haut niveau d'isolation.
- GOWER, passerelle multi niveau temps réel bidirectionnelle éprouvée sur les théâtres d'opérations, sur terre ou dans les airs. Contact : contact@geoide.fr

CHIFFRES CLÉS

Collaborateurs : 16
20+ Clients
700k€ de R&D par an

FOCUS SUR GLIMPS

GLIMPS développe des solutions de cybersécurité innovantes basées sur le deep learning et la conceptualisation de code. Les produits permettent de détecter, caractériser et analyser rapidement les menaces et leurs variants dans tous les fichiers.

De gauche à droite : Frédéric Grelot, Cyrille Vignon, Jérémy Bouetard et Valérian Comiti, fondateurs de GLIMPS.

"Boostez l'intelligence de vos lignes de défense !"

QUI SOMMES-NOUS ?

GLIMPS a été créée en novembre 2019 par 4 anciens ingénieurs du Ministère des Armées et compte aujourd'hui une cinquantaine de collaborateurs.

NOTRE SOLUTION

GLIMPS Malware est une plateforme de protection et d'investigation contre les fichiers malveillants incluant plus de 25 moteurs de détection et d'analyse (statique, dynamique et hybride) qui permettent de détecter et caractériser tous types de menaces et leurs variants, même les plus avancés, contenus tous les types de fichier. Les moteurs sont basés sur des technologies innovantes comme la conceptualisation de code, alimentées par le machine learning et le deep learning, ce qui différencie fondamentalement GLIMPS Malware des autres solutions du marché, en permettant de reconnaître un fichier malveillant, quelle que soit sa forme.
La plateforme GLIMPS Malware est le coeur du système, elle se décline en 3 produits :
- GLIMPS Malware KIOSK : le portail souverain d'analyse destiné aux collaborateurs de l'entreprise, qui leur permet de soumettre des fichiers pour analyse et levée de doute en toute autonomie.
- GLIMPS Malware DETECT : l'outil d'analyse et de détection avancée qui s'intègre sur tous les flux de fichiers (EDR, emails, applications métiers...) et qui fournit un verdict simplifié, transmis automatiquement aux solutions tierces pour réaliser les remédiations.
- GLIMPS Malware EXPERT : l'outil d'investigation automatique sur les fichiers pour les équipes cyber, qui offre une compréhension approfondie de la menace avec des résultats améliorés. L'exhaustivité des informations fournies aide à l'investigation, à la levée de doute et à la prise de décision, Contact : contact@glimps.re

CHIFFRES CLÉS

Ouverture d'une antenne au Canada en 2023
+100 clients protégés
1 million de fichiers analysés par jour

FOCUS SUR HOGO

Hogo est spécialiste de la cybersécurité avec des solutions sur étagères. L'entreprise innove sans cesse pour proposer à la défense et l'industrie mais aussi bien d'autres secteurs des solutions de pointe adaptées à leurs enjeux.

QUI SOMMES NOUS ?

Quentin RUILLERE est l'actuel Président de Hogo. Il fait partie des cofondateurs de la société, et y travaille depuis sa création. Précédemment, il travaillait dans l'industrie de l'énergie, au sein du groupe AREVA (SGN, Framatome) pour des projets d'envergure tels que l'usine d'enrichissement d'uranium GBII, le développement du contrôle-commande des sous-marins de classe SUFFREN, ou encore le projet de construction de réacteur EPR HPC (UK). Son expérience est axée sur la sûreté, la sécurité de fonctionnement, et la cybersécurité.

"Cybersecurity : Make it simple, keep it simple."

NOTRE SOLUTION

"Cybersecurity : Make it simple, keep it simple". Hogo développe et commercialise des Stations Blanches / Stations de Décontamination de données, permettant le traitement sûr de plusieurs types de supports (clefs et disques USB, CD/DVD, partages réseau...) et le transit de données sécurisé.
Hogo travaille principalement avec les secteurs de la Défense, de l'Industrie, et du Transport, qui recherchent le plus haut niveau de sécurité, à des coûts maîtrisés.
Contact : hello@hogo.

CHIFFRES CLÉS

7 ans de présence à Rennes
70 % du CA sur Rennes Métropole (Chiffres 2022)

FOCUS SUR ICODIA

Icodia est un hébergeur haute disponibilité certifié ISO27001:2017

QUI SOMMES-NOUS ?
Icodia est un hébergeur sécurisé haute disponibilité. Nous développons en interne des solutions nécessaires aux services d'hébergement.
Le système d'Information d'Icodia, incluant la gestion datacenter haute disponibilité, les solutions mutualisées et l'édition logicielle cybersécurité / réseau dispose de la certification ISO 27001:2017.
L'offre d'Icodia repose sur 3 axes :
- Des solutions d'hébergement très haute disponibilité, sécurisées et supervisées ;
- Des offres d'infogérance et d'audit ;
- Un pôle R&D orienté hardware, haute disponibilité, cybersécurité et informatique décisionnelle.

Un système d'Information homologable Diffusion Restreinte

NOTRE SOLUTION
Icodia a associé son savoir-faire à SanctuarIS, plateforme sécurisée de bureaux virtuels, pour proposer un Système d'Information homologable Diffusion Restreinte, en PaaS, clé en main, qui permet la gestion des informations sensibles portant la mention Diffusion Restreinte.

SanctuarIS répond aux exigences réglementaires définies par l'ANSSI dans l'Instruction Interministérielle n°901 relative à la protection des systèmes d'informations sensibles et intègre un bouquet de services capable de répondre à vos besoins, tels que le partage de fichiers, la visio-conférence, la messagerie…

Cette offre est destinée à différents secteurs, tels que les industries, les administrations publiques, les OIV, les OSE, les cabinets de conseil (PASSI, PDIS, PRIS, PACS) ou toute entité ayant un besoin de conformité SI-DR II901.

Elle est proposée par des spécialistes exigeants et reconnus, hébergée dans un datacenter sécurisé haute disponibilité et opérée en termes de MCO et de MCS par une équipe accreditée.
Cette solution entièrement "clé en main" couvre l'ensemble des besoins, depuis le poste utilisateur jusqu'au bouquet de services, ce qui permet d'en maîtriser les coûts.

CHIFFRES CLÉS

Collaborateurs : 25
Clients : 1800
CA sur Rennes Métropole : NC

FOCUS SUR IDNOW

IDnow est l'un des principaux fournisseurs européens de vérifications d'identité et d'identité numérique, dont la vision est de faire du monde numérique un endroit plus sûr. La plateforme IDnow propose une large gamme de solutions de vérification d'identité et de signature de documents, associée à une offre de services complète.

L'équipe d'IDnow à Rennes.

"Notre vision a toujours été, depuis le tout premier jour, de faire du monde numérique un endroit plus sûr"

QUI SOMMES-NOUS ?

En tant qu'acteur européen de l'identité numérique, IDnow propose à ses clients internationaux des solutions globales pour une palette d'usages toujours plus élargie, au fur et à mesure que la société se transforme et que les réglementations évoluent.
Ayant fusionné en juin 2021 avec l'entreprise rennaise ARIADNEXT, le groupe possède des bureaux en Allemagne, au Royaume-Uni et en France, et est soutenue par des investisseurs institutionnels de renom, dirigés par Corsair Capital.
Son portefeuille de plus de 900 clients internationaux couvre un large éventail de secteurs et comprend des acteurs internationaux de premier plan tels que UniCredit, Telefonica, Sixt, Crédit Agricole Personal Finance and Mobility, BNP Paribas Personal Finance, et Munich Re, ainsi que des champions du numérique comme N26, Solarisbank, Younited, BoursoBank, et Klarna.

NOTRE SOLUTION

Nous avons une méthode de vérification pour chaque besoin. Qu'elles soient automatisées ou assistées par un opérateur, purement en ligne ou sur le lieu de vente, les méthodes de vérifications d'identité sont optimisées pour garantir les normes de sécurité les plus élevées et une conversion maximale des utilisateurs.
Contact : contact@idnow.io

CHIFFRES CLÉS

Collaborateurs : 450+
Identités vérifieés p.a. : 100 millions (2023)
Nombre de clients : 900+

FOCUS SUR IMATAG

Imatag propose de protéger votre entreprise contre l'utilisation indésirable de vos images et vidéos.

L'équipe d'Imatag

QUI SOMMES-NOUS ?
Fondée en 2015, IMATAG s'est d'abord attaquée au défi de la diffusion massive de photos sans crédits sur Internet.
Notre expertise en tatouage numérique (filigrane invisible), initialement développée pour protéger les droits d'auteur, s'est naturellement étendue à la lutte contre la désinformation visuelle.

Aujourd'hui, nous sécurisons les contenus visuels tout en renforçant la cyberdéfense face aux menaces informationnelles croissantes.

"Nous sommes experts en Tatouage Numérique et Reconnaissance Visuelle"

NOS SOLUTIONS
AUTHENTICITY : Notre solution phare permet de vérifier et protéger l'authenticité des contenus visuels sur les plateformes numériques. Utilisant notre technologie brevetée de filigrane invisible, AUTHENTICITY permet l'authentification fiable des contenus visuels par les réseaux sociaux, les éditeurs et les fact-checkers, luttant ainsi contre la désinformation et les violations de droits d'auteur.

LEAKS : Le tatouage de vos contenus numériques avant diffusion permet d'identifier la source en cas de fuite. Initialement conçu pour protéger les visuels sous embargo et les contenus payants, ce système s'avère également efficace pour tracer l'origine des informations sensibles et prévenir leur détournement.

MONITOR : L'application d'un filigrane numérique à vos photos ou vidéos certifie leur provenance, même après effacement des métadonnées. Cette solution, d'abord développée pour la gestion des droits d'auteur, s'est révélée cruciale pour authentifier les contenus et détecter leur utilisation non autorisée ou leur manipulation dans des contextes de désinformation.

Contact : contact@imatag.com

CHIFFRES CLÉS
Collaborateurs : 18
Clients : Médias, Presse, Industrie Hi-Tech, Marques

FOCUS SUR IMINETI BY NIJI

Imineti by Niji fédère les activités de conseil et d'expertise en cybersécurité de Niji. Fortement intégrée au fonctionnement opérationnel des grands groupes, des ETI et PME en région, cette offre se complète naturellement avec la proposition de valeur de Niji (conseil, design et réalisation technologique).

Hervé Troalic, directeur général et Pierre Corbel, directeur cybersécurité

QUI SOMMES NOUS ?

Notre ADN c'est l'expertise en Cybersécurité ! Nos clients viennent chercher chez nous une réelle plus-value sur les domaines suivants :
- Sécurité offensive
- Accompagnement à la certification et audit
- Qualifications ANSSI
- Gouvernance et risk management cyber
- Sécurité du cloud et SecNumCloud
- Sécurité de la donnée
- Sécurité applicative

"Une expertise pointue dans le domaine de la cybersécurité et une exigence de pragmatisme pour servir nos clients"

NOTRE SOLUTION

- Red Team, test d'intrusion et audits de configuration
- Audit et conception d'architectures sécurisées (IT/OT, Cloud)
- DevSecOps, sécurité dans les projets
- Gestion des risques (cartographie des risques de l'organisation, gestion de la chaine d'approvisionnement…)
- Adaptation des plans de continuité à la crise d'origine cyber et préparation à la crise
- Accompagnement à la mise en conformité (ISO 27001/HDS, NIS, DORA, MICA, Swift, SecNumCloud
- Sensibilisation et formation

Contact : herve.troalic@niji.fr

CHIFFRES CLÉS

2021 : création de l'activité
2022 : Qualification PASSI
2025 : 40 collaborateurs, en cours de qualification PACS

FOCUS SUR IPCYB

IPCYB propose des conseils, sensibilisations, formations et entraînements des PME et usagers du numérique à l'hygiène et à la sécurité numérique. Le cabinet accompagne les personnalités dans la gestion des risques numériques et apporte les secours pour les victimes d'actes malveillants

Régis Le Guennec, dirigeant d'IPCYB

QUI SOMMES NOUS ?

Entrepreneur depuis plus de 20 ans dans le numérique, passionné par les nouvelles technologies et la création visuelle (photo/video/degsdfgssign) issue de la génération X.
Cofondateur en 1995 de l'association BUG à rennes, président de Bug et webmaster de rennet.org de 1995 à 1997.
Fondateur-directeur de l'agence de communication numérique MBA (1997-2017).
Dirigeant de l'agence IPcyb spécialisée dans le conseil et la formation cybersécurité auprès des usagers et des organisations.
J'enseigne aujourd'hui "la sécurité numérique et le hacking" dans différentes écoles, centres de formation, Universités du grand Ouest et auprès des PME et grands groupes régionaux.

"Une expérience et une culture forte de 25 ans dans le numérique"

NOTRE SOLUTION

IPcyb propose des missions de conseil et des prestations pédagogiques à l'attention des utilisateurs et organisations soucieuses de leurs pratiques de sécurité numérique. Formation en ligne (plateforme LMS et webinaire live) ou en présentiel sur le grand Ouest et sur Paris.
Spécialités : Cyber sécurité (Gouvernance/Analyse de risque, audit de maturité, sécurisation des développements web, ingénierie sociale, OSINT) & hygiène numérique (Coaching personnalisé, Sensibilisation/ ForAmation/Entrainement/Démonstration), et menaces sur les réseaux sociaux.
Je travaille également sur la sécurité des données et de l'information (RGPD, fakenews/deepfake, manipulation/influence, dérives 2.0) et la vie privée numérique
Contact : info@ipcyb.fr

CHIFFRES CLÉS

25 ans d'expérience numérique
Entrepreneur 2.0
80 % du CA sur Rennes Métropole

FOCUS SUR KEREVAL

Kereval est une entreprise française experte dans le métier du test logiciel.

L'équipe Kereval

QUI SOMMES-NOUS ?

Kereval est une PME française indépendante spécialisée dans l'ingénierie du test logiciel.
Depuis 2002, elle accompagne ses clients pour professionnaliser leur démarche de qualité logicielle. Elle les assiste dans l'élaboration de leur stratégie de test, dans la conception, l'automatisation et l'exécution de tests logiciels. Elle offre toute la gamme de tests : tests fonctionnels, tests d'interopérabilité, tests de conformité, tests de cybersécurité et tests des algorithmes à base d'Intelligence Artificielle. Elle propose également des formations certifiantes dans le domaine du test logiciel.
Basée près de Rennes, l'entreprise emploie plus de 80 collaborateurs qui interviennent aux niveaux national et international, dans les secteurs de la santé, la défense, le transport, l'industrie, les smart cities, et plus généralement de l'économie numérique.

"L'expert du test logiciel des systèmes d'information et des systèmes embarqués"

NOTRE SOLUTION

Qualifiée Prestataire d'Audit de Sécurité des Systèmes d'Information (PASSI) par l'ANSSI, Kereval accompagne ses clients à travers des prestations d'audits d'intrusion, d'architecture, de configuration, de code et d'organisation.
L'entreprise intervient sur tout système d'information et sur tout système embarqué autour des directives NIS2, RED et normes associées : ISO 62443, ETSI 303645, IEC/TR60601-1-4-5, ISO 81001-5-1, etc.
A travers son équipe dédiée " Intelligence artificielle ", Kereval accompagne les acteurs utilisant de l'IA pour les aider à sécuriser leurs solutions. Contact : contact@kereval.com

CHIFFRES CLÉS

Collaborateurs : 80+
Clients : 100+
Création 2002

FOCUS SUR LOOTUS SECURITY

Bien plus qu'une société de conseil en cybersécurité IoT et IT, LOOTUS SECURITY est également un bureau d'étude électronique. Elle assiste ses clients dans une démarche de sécurisation dès la conception.

"La sécurisation dès la conception"

QUI SOMMES-NOUS ?

LOOTUS a été fondé, il y a maintenant 5 ans par M. Julien MOINARD, expert en cybersécurité IoT et IT qui totalise plus de 12 ans d'expérience (test d'intrusion, audit, développement d'outils dédiés, conception sécurisée d'architectures électroniques et informatiques). Son expérience significative est reconnue internationalement (BlackHat, Chaos Computer Club, Hack In Paris, CanSecWest, HITB, FIC, Cap'tronic, We Network, écoles...) et repose sur des compétences techniques très pointues.

En 2023, LOOTUS devient alors LOOTUS GROUP et découpe ses activités principales en deux entreprises LOOTUS SECURITY et LOOTUS ACADEMY. LOOTUS SECURITY conserve les activités de conseils en cybersécurité IoT et IT ainsi que le bureau d'étude en électronique. Alors que LOOTUS ACADEMY développe l'activité de formation en devenant un centre de formation en cybersécurité IoT et IT certifié Qualiopi.

NOTRE SOLUTION

LOOTUS SECURITY assiste ses clients dans une démarche de sécurisation dès la conception et a la capacité d'intervenir sur des sujets très complexes, transverses et pluridisciplinaires, tout en intégrant aussi bien des équipes informatiques, qu'électroniques. Notre champ d'intervention nous permet ainsi d'intervenir sur l'ensemble de l'écosystème IoT et IT, proposant également des audits et tests d'intrusions afin d'accompagner ses clients pendant leur cycle de développement et d'évaluer leur niveau de sécurité vis-à-vis de l'état de l'art de la cybersécurité communément admis. LOOTUS SECURITY s'appuie sur des guides et normes dont le périmètre peut être national et/ou international afin de se conformer aux contraintes métiers de ses clients.
Forte de son expérience en conception de produits électroniques ou bien d'outils spécifiques dédiés à cybersécurité, LOOTUS SECURITY a conçu son écosystème " I²Cx Cyber Range " (plateforme d'entraînement à la cybersécurité des objets connectés). Disposant ainsi d'une valeur ajoutée complémentaire à son expertise, LOOTUS SECURITY accompagne alors pédagogiquement les entreprises dans l'intégration de l'état de l'art de la cybersécurité des objets connectés dès la conception, mais également de permettre aux particuliers et aux écoles de se sensibiliser à l'usage de ces technologies.
Contact : contact@lootus.net

CHIFFRES CLÉS

Création à Rennes en 2019
92 conceptions sécurisées
42 audits / tests d'intrusions
CA 2023 : 426k€

FOCUS SUR MALIZEN

Chez Malizen propose une plateforme puissante et intuitive qui permet aux experts en cybersécurité de détecter et d'investiguer efficacement les menaces complexes. Elle centralise et unifie les données hétérogènes issues de multiples sources (logs, réseau, etc.), offrant ainsi une visualisation et des outils d'analyse avancés basés sur l'IA. La plateforme s'intègre avec les standards (ECS, STIX, MITRE ATT&CK, MITRE DEF3ND, SIGMA).

Christopher Humphries - CEO.

"Les menaces cyber évoluent, les solutions technologiques se multiplient. Replaçons l'humain au cœur de la cybersécurité."

QUI SOMMES-NOUS ?

Fondée en 2020, Malizen repose sur plus de 10 ans de recherche dans des laboratoires français, combinant expertise en visualisation des données, machine learning et cybersécurité. Notre mission est d'aider les entreprises à déjouer les menaces cachées dans leurs données complexes, volumineuses et dispersées. Nous avons conçu une plateforme innovante qui associe l'intelligence humaine à la puissance des algorithmes pour identifier rapidement les anomalies et menaces qui échappent souvent aux systèmes traditionnels

NOTRE SOLUTION

Malizen centralise et unifie les données hétérogènes pour faciliter l'identification des menaces cachées. Grâce à sa flexibilité de déploiement (cloud, on-premises, ou mallette d'intervention), la plateforme s'adapte aux besoins spécifiques de chaque organisation.
Malizen s'intègre automatiquement aux systèmes existants et s'ajuste aux différentes sources de données, sans configuration complexe. Avec des visualisations interactives et des analyses alimentées par le machine learning, il permet aux équipes de détecter rapidement les menaces et d'investiguer efficacement. La collaboration est simplifiée grâce à des fonctionnalités de partage et de suivi en temps réel. Malizen transforme les processus d'investigation cyber grâce à une approche qui place l'humain au cœur des opérations tout en exploitant les avantages de l'intelligence artificielle. Nous offrons aux équipes de cybersécurité des outils qui facilitent l'investigation, unifient les données, et encouragent une collaboration efficace, le tout avec une rapidité d'action inégalée.

CHIFFRES CLÉS

+ 50 % de rapidité d'analyse par rapport à des outils traditionnels comme ELK
+ 100 % de pistes d'investigation identifiées

FOCUS SUR Neotrust

Neotrust est une société de conseil spécialisée en cybersécurité dans la gouvernance, les risques et la conformité, reconnue pour son expertise technique et son accompagnement stratégique. Nous intervenons auprès d'acteurs publics et privés pour sécuriser leurs transformations numériques avec rigueur, exigence et agilité de la stratégie à l'exécution.

L'équipe

QUI SOMMES-NOUS ?

Situé à Paris, Montréal, Rennes et Lyon, Neotrust est un cabinet de conseil indépendant spécialisé en cybersécurité : audit, gouvernance, risques et conformité.
Nous accompagnons entreprises et institutions françaises et internationales dans la maîtrise de leurs enjeux numériques, en conjuguant expertise stratégique et savoir-faire opérationnel.
Nos interventions couvrent un large spectre, allant des audits techniques (tests d'intrusion, revues de configuration, ...) jusqu'à la définition de la stratégie de cybersécurité sur mesure et son exécution opérationnelle.
Notre approche repose sur l'écoute, l'exigence et l'adaptation aux contextes spécifiques de chaque organisation.
Notre ambition : construire une cybersécurité durable, alignée avec les objectifs métiers et les obligations réglementaires (NIS2, DORA, ISO 27001, etc...).

"Neotrust, de la stratégie à l'exécution pour une cybersécurité durable."

NOTRE SOLUTION

Neotrust propose une gamme complète de services pour accompagner les organisations dans la maîtrise de leurs enjeux de cybersécurité, de gouvernance et de conformité, de la réflexion stratégique à la mise en œuvre opérationnelle.
Gouvernance, Risques et Conformité (GRC) : Diagnostic / Gap Analysis NIS2, DORA, ISO 27001; Accompagnement à la mise en conformité ISO 27001, NIS2, DORA, HDS, ...; PCA / PRA et procédures de gestion de crise.
Audits techniques et innovation :incluant des tests d'intrusion, revues de configuration, développement d'un projet CTI et audit de maturité de cybersécurité
Accompagnement opérationnel : mise en place d'experts métiers sur demande client, mise en place de dispositifs de contrôle, la gestion de projets cybersécurité, l'animation de démarches de sensibilisation, ou encore le pilotage de programmes de transformation.
Formations : Neotrust propose des formations sur mesure pour renforcer la culture cybersécurité des organisations et faire monter en compétence les équipes (intra et inter entreprises).

CHIFFRES CLÉS

Fondé en 2019 à Paris, ouvre ses bureaux à Montréal en 2023, Rennes 2025, Lyon 2025
Collaborateurs : +45
Clients: +100 en France et international

FOCUS SUR NEVERHACK

NEVERHACK offre une plateforme totale et exhaustive en termes d'offre cyber pour la performance et la sécurité de ses clients.

Le dirigeant de NEVERHACK France

QUI SOMMES NOUS ?

Créée en 2021 par une équipe de passionnés de cybersécurité, NEVERHACK a eu pour ambition de consolider les expertises de différentes structures spécialisées en cybersécurité.
Le groupe a développé son projet autour de sociétés françaises spécialisées dans les domaines de la sécurité IT, software, embarquée, et applicative, le cyber entraînement, les pentests, la gestion des identités et des comptes à privilèges, ainsi que l'accompagnement stratégique en gestion des risques et gouvernance cyber.
La vision de l'entreprise est simple : construire un monde numérique sécurisé.

"Partenaire de votre performance cyber"

NOTRE SOLUTION

L'innovation et l'expertise sont au cœur des valeurs du groupe. Cela se manifeste par une proposition de valeur forte en termes de choix de partenaires éditeurs, une exigence dans le recrutement des talents, une méthode éprouvée pour la gestion des carrières, et une offre MSSP qualitative respectant des enjeux de souveraineté pour ses clients.
Ce qui distingue véritablement NEVERHACK, c'est son approche avant-gardiste en offrant une protection proactive et réactive contre un large éventail de cybermenaces, répondant ainsi aux deux grandes problématiques de chaque RSSI : comment se protéger et comment se défendre face aux cyberattaques.

NEVERHACK propose un accompagnement 360 sur mesure pour chaque projet Cyber. Aux côtés des donneurs d'ordres Cyber pour chaque étape de leurs projets, de la conception à la mise en œuvre et maintenance, NEVERHACK adopte une approche holistique qui garantit que chaque détail des stratégies cyber de ses clients soit bien pris en compte : gestion des risques, conformité réglementaire, formation des équipes, surveillance continue. Contact : https://neverhack.com/

CHIFFRES CLÉS

1 200 collaborateurs
10 pays
1 market place cyber

FOCUS SUR NOMIOS

Créée en 2004, Nomios est née de la prise de conscience que la sécurité en entreprise nécessite une expertise spécialisée. Nous avons compris que chaque entreprise a besoin d'un accompagnement sur-mesure, avec une expertise adaptée. En effet, les défis liés à l'infrastructure et à la cybersécurité varient en fonction des applications, des données et des métiers spécifiques à chaque entreprise. Notre approche personnalisée, centrée sur les besoins précis de nos clients, est le cœur même de notre engagement depuis nos débuts.

L'équipe

"Être là pour la sécurisation globale de votre système de votre système d'information."

NOTRE SOLUTION

Service complet de cybersécurité : Gouvernance, Risque et conformité (GRC), Intégration, Support, Services Managés et SOC.
https://www.nomios.fr
Contact : info-rennes@nomios.fr

CHIFFRES CLÉS

Collaborateurs : 300 dont 9 à Rennes
Clients : + 4000, dont +50 à Rennes
CA sur Rennes Métropole : 7 M€ en 2023
(192M€ en France)

QUI SOMMES-NOUS ?

Nomios agit pour la sécurisation des réseaux informatiques d'entreprise par sa présence constante auprès des entreprises clientes. Indépendants par nature, nous choisissons des produits qui répondent aux exigences de nos clients, en tenant compte de leurs contraintes et problèmes spécifiques. Nos ingénieurs s'efforcent d'évaluer continuellement les diverses solutions disponibles sur le marché afin de pouvoir toujours proposer l'option la plus adaptée aux besoins exprimés.
Notre métier peut prendre différentes formes :
• Gouvernance, Risque et conformité (GRC) : audit technique et organisationnel de vos infrastructures réseaux et sécurité. Mise en œuvre de politique de sécurité et de performance. Analyse des textes réglementaires.
• Intégration : mise en œuvre de solutions à forte valeur ajoutée, sur-mesure, avec des projets clefs en main. FireWall, SASE, MFA, NAC, Protection des API, sécurisation IT, OT et IoT, filtrage, SIEM, Sécurisation du Cloud…
• Support : accompagnement pour l'exploitation de vos infrastructures avec des outils sur-mesure. Astreinte 24/7
• Services Managés : équipe dédiée assurant des conseils et de l'exploitation sur-mesure.
• SOC : notre service de SOC est assuré par des analystes niveau 2 et 3. Nous assurons une détection personnalisée, pour réduire les impacts et maîtriser vos risques et votre budget.
• Formation : plates-formes techniques dédiées, cursus personnalisés par des intervenants certifiés.
• Accompagnement Longue Durée : Ingénieurs experts à plus de 50% du temps dans vos équipes pour des accompagnements de plusieurs mois.

FOCUS SUR Numih France

Numih est un acteur public du numérique au service de la santé et du secteur public. Il accompagne les établissements de santé et les administrations publiques.

Une partie de l'équipe de Mipih SIB au FIC 2024

"Un acteur public au service de la sécurité de la santé et du secteur public"

QUI SOMMES-NOUS ?

Le Numih France est un groupement d'intérêt public (GIP) qui accompagne près de 1 000 hôpitaux, groupements hospitaliers de territoire, collectivités et administrations publiques dans leur transformation numérique.

En tant qu'acteur public du numérique de premier plan, le Numih France est expert dans la conception, le déploiement et l'hébergement de services numériques (certifié HDS et ISO 27001, ISO 9001, NF-461). Le pôle dédié à la protection des données et à la cybersécurité regroupe une équipe de 30 experts et propose des services à haute valeur ajoutée. Il accompagne ses adhérents dans la gestion des enjeux stratégiques liés à la sécurité des données de santé, à la cybersécurité et à la maîtrise des risques associés.

Basé à Toulouse, Rennes, Bordeaux, Lille, Amiens, Rouffach et Reims, le Numih France compte plus de 1300 collaborateurs engagés au service de l'innovation et de la sécurité dans le secteur public.

NOTRE SOLUTION :

Tout d'abord, nous accompagnons nos clients dans une démarche d'amélioration continue de leur sécurité en les guidant sur tous les aspects de la cybersécurité. Cela inclut notamment le volet organisationnel (analyse de risques, conformité au référentiel de l'ANSSI, normes ISO 27001, HDS, etc.), afin de mettre en place un système vertueux de prévention et d'amélioration.

Nous sommes aussi sollicités pour des tests d'intrusion pour identifier des vulnérabilités exploitables par un attaquant, tout en sensibilisant à la fois les agents et la direction générale. Nous conseillons nos clients sur les outils, les architectures et les pratiques à l'état de l'art pour répondre efficacement à leurs besoins en matière de protection. La sensibilisation et la formation constituent des leviers essentiels dans notre approche. Nous proposons des sessions de gestion de crise cyber intégrant des exercices de mise en situation qui plongent nos adhérents dans des scénarios de crises réalistes. Nos services incluent également la gestion de la sécurité opérationnelle via notre Centre Opérationnel de Sécurité (SOC), la gestion des identités et des accès (IAM), ainsi que des prestations de gouvernance pour garantir une gestion globale et stratégique de la cybersécurité.

Contact : contact@sib.fr

CHIFFRES CLÉS

Collaborateurs : 1 300
Clients : 1 000
CA sur Rennes Métropole : 55 M€

FOCUS SUR NYBBLE

L'ambition de Nybble est de protéger simplement et efficacement tous types d'entreprises en redéfinissant la détection et la réaction face aux menaces de cybersécurité, avec ses solutions SaaS et son approche globale unique.

Sébastien Lehuédé - Founder/SIEM Engineer
Gabriel Kropp - CTO/Cloud System Architec

"Blue Team Community
Pour une approche de la cybersécurité sans frontières"

QUI SOMMES-NOUS ?

Passionné de technologie et d'entrepreneuriat, Sébastien a suivi un cursus d'ingénieur en informatique à SUPINFO Rennes. Après une première expérience SIEM durant son contrat de professionnalisation, Sébastien rejoint le SOC du Crédit Agricole en tant qu'analyste sécurité. Intéressé par les problématiques d'architecture, il a ensuite intégré le SOC AXA en tant qu'ingénieur SIEM.
Avant de fonder Nybble, il participe à la mise en place d'un SOC externe au sein des bureaux d'Harmonic Inc à San Francisco. Initié à l'informatique et réseau par son père, Gabriel a suivi un cursus ingénieur R&T en alternance à Télécom Bretagne (via OBS). Après une expérience en SSII orienté développement, Gabriel a travaillé chez Harmonic Inc, en tant qu'ingénieur systèmes UNIX au sein de l'équipe IT L2 internationale. Curieux et impliqué, Gabriel élargit son domaine de compétences à tous les aspects d'un SI au travers de projets structurants : 2 changements d'ERP, 2 déménagements de datacenter, merge de SI, automatisation de l'IT, transition cloud.

NOTRE SOLUTION

L'offre SOC managé de Nybble est axée autour de deux plateformes. Nybble Security Analytics : est une plateforme de détection des attaques et menaces de cybersécurité (SIEM) NextGen, alliant performance et simplicité. La plateforme est distribuée en mode SaaS, déployée et gérée de façon entièrement automatisée. Elle gère nativement le format de règle générique SIGMA et dispose ainsi de centaines de règles de détection pour monitorer tous types d'équipements. Les technologies innovantes au coeur de la plateforme permettent de proposer des fonctionnalités avancées comme le rejeu d'événements après la mise en place d'une nouvelle règle ou le développement de scénario de détection complexe en mode Detection-As-Code.
NybbleHub : est une plateforme collaborative d'analyse d'alertes sécurité et de Threat Bounty. Elle permet à des analystes du monde entier de traiter et catégoriser les alertes de sécurité remontées par tous les SIEM connectés à celle-ci. De plus, des Threat Hunters identifieront des menaces et des traces de compromission au sein d'un système d'information lors de campagnes dédiées de Threat Bounty, en échange de primes. Enfin, l'aspect collaboratif de la plateforme permet aux clients et analystes de proposer de nouvelles règles de détection, des améliorations sur les procédures d'analyses, des corrections de traitement des logs afin d'optimiser les capacités de détection et de réaction globale pour les plateformes Nybble. L'équipe Nybble propose un accompagnement personnalisé à ses clients dans la définition du besoin, la mise en place de la collecte et la réponse aux incidents. Contact : sebastien.lehuede@nybble.bzh

CHIFFRES CLÉS

Fondée en 2021
10 années d'expérience SOC/SIEM
Plus de 1156 règles de détection (Chiffres 2022)

FOCUS SUR OCI

Expert de l'informatique et du digital, OCI Informatique & Digital accompagne les entreprises et collectivités sur l'ensemble de leur système d'information, le digital et notamment la sécurité informatique.

Jonathan MERAOUBI
Directeur du pôle cybersécurité "Resilience"

"Du digital OUI
mais des HUMAINS avant tout !"

QUI SOMMES NOUS ?

Expert de l'informatique et du digital à 360°, OCI accompagne les entreprises sur toute la France.
Fortes d'une organisation par pôle d'expertises, les équipes du Groupe OCI réalisent au quotidien des projets autour du cloud, la cybersécurité, le réseau, les télécoms, les applicatifs de gestion, le web ou encore le collaboratif.
Animé par le goût de l'aventure humaine et de l'innovation, le Groupe a à cœur la réussite et le confort de ses clients et l'épanouissement de ses collaborateurs au sein de l'entreprise.

NOTRE SOLUTION

L'accompagnement Resilience se traduit en 6 étapes :
- Se connaître : Auditez votre Système d'Information de façon technique et stratégique (audit organisationnel, diagnostic technique, test de vulnérabilités, audit d'architecture, test d'intrusion).
- Se préparer : Analysez les risques liés à votre activité et cadrez votre démarche en cas d'attaque (SMSI, PSSI, analyse de risques, COPIL de sécurité, gestion de crise).
- Sensibiliser : Formez et mettez en situation l'ensemble des utilisateurs en fonction de leur rôle dans l'entreprise (sensibilisation Direction, formation utilisateurs et administrateurs, campagne d'hameçonnage, e-learning).
- Renforcer : Mettez en place des outils techniques de protection en fonction des différentes composantes du SI (gestion des accès à privilèges, gestion des identités et des accès, protection des environnements collaboratifs, classification de la donnée, protection avancée des mobiles, coffre-fort de mot de passe).
- Surveiller : Monitorez en permanence le Système d'Information pour détecter et agir au plus tôt en cas d'attaque (Centre Opérationnel de la Sécurité - SOC).
- Répondre : Référencement auprès de CSIRT afin de répondre en cas d'attaque. Contact : info@oci.fr

CHIFFRES CLÉS

Fondé en 1990
12 collaborateurs
6 500 000€ de CA sur Rennes Métropole

FOCUS SUR ORNISEC

ORNISEC est un cabinet de conseil et d'audit cybersécurité, qualifié PASSI et PACS par l'ANSSI qui propose un accompagnement pragmatique à forte valeur ajoutée. À l'issue de chaque prestation, ORNISEC accompagne gratuitement ses clients, pour les aider à atteindre leurs objectifs cybersécurité.

L'équipe d'Ornisec

"Une expertise pointue dans le domaine de la cybersécurité et une exigence de pragmatisme pour servir nos clients"

QUI SOMMES-NOUS ?

ORNISEC est une société d'une quarantaine de salariés à la pointe de la cybersécurité avec un rayonnement international. Elle est née d'une passion profonde, celle de réinventer le métier du conseil en proposant systématiquement un accompagnement post prestation gratuit, pour aider nos clients à atteindre leurs objectifs. Nos valeurs sont le pragmatisme, l'accompagnement sur mesure, l'efficacité et la satisfaction client.
Notre forte expérience dans la cybersécurité et notre connaissance terrain nous permettent de répondre aux attentes de nos clients : fournir un accompagnement terrain et pragmatique (expliquer ce qu'il faut faire pour atteindre les objectifs, comment il faut le faire, avec quel outil, quelle organisation et combien cela peut coûter), assister les clients après chaque prestation pour les aider à dérouler les plans d'action proposés. Nous avons plusieurs références dans plusieurs secteurs d'activité, en France Métropole, dans les DOM/TOM/POM et à l'international.
ORNISEC est également qualifié auprès de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour réaliser les missions d'audit et de conseil en cybersécurité
- Qualification PASSI et PACS

NOTRE SOLUTION

ORNISEC décline ses activités en 6 pôles au sein desquels interviennent ses collaborateurs :
• Conseil et gouvernance : analyse de risques, EBIOS RISK MANAGER, homologations de sécurité, schéma directeur, politiques de sécurité, expertise en systèmes d'information industriels, gouvernance.
• Audit : tests d'intrusion, audit d'architecture, de configuration, de code source et d'organisation.
• Conformité : DORA, NISv2, LPM, RGS, HDS, ISO27001, RGPD, réglementation de sûreté DGAC.
• Assistance RSSI : RSSI Externe et prise en charge de la fonction de RSSI, assister le RSSI existant en lui mettant à disposition une ressource ORNISEC pour prendre une partie de sa charge de travail.
• Formation & sensibilisation : Formation des équipes techniques, Simulation de phishing et sensibilisation.
• Gestion de crise : mise en place de PCA/PRA, Procédures de gestion d'incident et de crise, Réponse à incident, simulation de crise cyber. Contact : a.sabbar@ornisec.com

CHIFFRES CLÉS

Collaborateurs : +40
Cilents : +300
CA sur Rennes Métropole : +2M€

FOCUS SUR OVALT

Ovalt apporte au marché de la cybersécurité une expertise unique issue de son ancrage industriel : protéger les systèmes de production et d'automatisation face à des menaces en constante évolution. Grâce à ses équipes spécialisées et à des partenariats stratégiques, le Groupe propose une approche complète allant du diagnostic à la mise en œuvre.

Jérôme Champenois, Julien Morel & Matéo Gallard, nos experts cybersécurité

"La cybersécurité industrielle ne peut pas être une simple transposition des modèles IT. Cela nécessite une connaissance concrète des métiers pour une réponse réellement adaptée à chaque besoin".

QUI SOMMES NOUS ?

Ovalt c'est un groupe industriel breton qui réunit plusieurs expertises au service de la performance de nos clients : automatisme, robotique, informatique industrielle, énergies et cybersécurité. Depuis 50 ans, nous accompagnons les industriels dans leurs transformations en concevant et en intégrant des solutions fiables, innovantes et durables.
Notre force : des équipes engagées, proches du terrain, qui conjuguent expertise technique et esprit collectif pour relever chaque défi.

NOTRE ACCOMPAGNEMENT EN CYBERSÉCURITÉ

Ovalt accompagne les industriels dans la protection de leurs systèmes de production et d'automatisation face aux cybermenaces croissantes. Notre démarche repose sur une approche globale et pragmatique :
Évaluation des risques et diagnostic : nous identifions les vulnérabilités, évaluons les niveaux de risque et définissons les actions prioritaires.
Recommandations et mise en œuvre : nous assurons la mise à jour sécurisée des systèmes, la segmentation des réseaux, le déploiement de plans de sauvegarde et la mise en place de solutions de détection et d'analyse des incidents.
Pilotage et gouvernance : nous aidons nos clients à structurer leur stratégie de cybersécurité, à sensibiliser leurs équipes et à se préparer à la gestion de crise.
Notre offre allie expertise industrielle de terrain et compétences cyber pointues. Notre ambition est claire : offrir aux industriels des solutions concrètes qui renforcent leur sécurité, sans compromettre leur performance opérationnelle.
Contacts : jmorel@groupe-ovalt.com, jchampenois@groupe-ovalt.com

CHIFFRES CLÉS

50 ans d'expertises
+ 480 collaborateurs
3 sites en Bretagne

FOCUS SUR OWN

Fondée en 2008 sous le nom de SEKOIA, la nouvelle marque OWN rassemble désormais les activités de services en tant que Pure-Player français de la cybersécurité. OWN, c'est la cybersécurité centrée sur la connaissance de la menace qui intervient dans les domaines de l'audit, du conseil, du renseignement cyber (Threat Intelligence), de la réponse à incident (CERT) et du SOC managé.

L'équipe de Own

"OWN a construit son cœur de compétence sur son expertise en Threat Intelligence, sans autre objectif que d'approfondir ses connaissances, ses techniques et ses méthodes pour devenir plus efficace dans la protection des actifs et des intérêts des organisations."

QUI SOMMES-NOUS ?

Pure-Player de la cybersécurité, OWN accompagne au quotidien des petites, moyennes et grandes organisations pour leur permettre d'exercer leur métier dans les meilleures conditions en proposant une amélioration en continue de leur cybersécurité et une assistance pour mieux anticiper, détecter et réagir à une menace cyber.
La cybersécurité de OWN, c'est une approche centrée sur la menace et les risques dans ses dimensions techniques, organisationnelles et géopolitiques, qui constitue son ADN dont le séquençage repose sur : Operate, Warn, Neutralize. Trois actions qui symbolisent pleinement le rôle de ses experts au quotidien : conseiller et prendre part à des actions de cyberdéfense, informer et alerter lorsque le risque est imminent, contribuer à la remédiation pour neutraliser la menace.

NOTRE SOLUTION

- Évaluation de la sécurité : nous aidons les organisations à identifier les vulnérabilités de leurs systèmes d'information, se mettre en conformité avec la réglementation (RGPD, NIS2, DORA, ...) et proposons des recommandations pragmatiques pour les aider à les corriger.
- RSSI externalisé : nous vous accompagnons dans votre cybersécurité et assurons la fonction de RSSI en mettant à disposition l'ensemble de nos expertises comme l'accompagnement à la certification ISO27001.
- Analyse de la menace : notre défi est de collecter, traiter, corréler et analyser toutes les informations techniques et non techniques (géopolitiques, économiques, métiers, etc.) pour les transformer en renseignements actionnables (utiles) et contextualisés (pertinents) dans notre Threat Intelligence Platform.
- SOC managé : nous détectons, analysons et remédions aux incidents de sécurité en continu et en temps réel de nos clients grâce à notre SOC offrant des fonctions de SIEM, EDR et XDR.
- Réponse à incident : nous vous accompagnons sur la qualification d'un incident de sécurité, sa remédiation et nous vous aidons à améliorer votre réactivité en cas d'incident de sécurité sur votre système d'information via un point de contact unique. Contact : contact@own.security

CHIFFRES CLÉS

2008 : Date de création
+ 70 Collaborateurs : Rennes, Paris, Toulouse
10 langues maîtrisées

FOCUS SUR PERSES COMMUNICATION

L'agence de communication spécialisée sur les marchés des industriels de défense et de sécurité.

L'équipe de Persés communication

"Spécialiste de la communication dans le secteur de la Défense"

QUI SOMMES NOUS ?

Hugues Collin de la Bellière est CEO. 30 ans d'expérience, de formation commerciale, marketing et communication, il est issu des meilleures agences de communication et des médias (Havas, Young & Rubicam, Euro RSCG, France 3 Publicité…). Fondateur de structures spécialisées au sein du Groupe Pégase Communication qu'il a crée : LCDM DESIGN, l'Agence Symphonie et Persès Communication. Entrepreneur dans l'âme, issu d'une famille de militaires de haut niveau. Hugues s'emploie à transmettre et s'engage bénévolement au profit de la défense comme réserviste citoyen – Terre.

Christophe Peuchaud, est en charge du développement. 27 ans d'une carrière d'Officier dans l'Armée de Terre et les Parachutistes des troupes de Marine. Il décide de fonder OENOPTIMO, acteur majeur dans l'événementiel construit autour du patrimoine œnologique. Christophe est auditeur de l'IHEDN, a suivi un parcours entrepreneurial à HEC et a fondé l'Association des Militaires Entrepreneurs (AME-France) dont il assume les fonctions de Vice-Président.

NOTRE SOLUTION

Le conseil stratégique

Une méthodologie s'appuyant sur 30 ans d'expérience pour une stratégie et un plan de communication solides et affûtés.

L'image de marque

Créer ou faire évoluer votre identité, élaborer votre plateforme de marque, votre charte graphique.

La création éditoriale.

Conception, rédaction des différents outils de communication et contenus (rapport d'activité, plaquette entreprise ou service et produit…), traduction multilingue.

Les plateformes de communication.

Édition, création de contenus, vidéos produit & corporate prises de vue.

Les médias et web design.

Médiaplanning des campagnes et stratégie numérique. Contact : hdelabelliere@perses-communication.com

CHIFFRES CLÉS

100 % disponible pour vous accompagner

FOCUS SUR QUARKSLAB

Quarkslab dispose d'un expertise qui combine la sécurité offensive et défensive dans la protection des applications et aide les organisations à adopter une nouvelle posture de sécurité : obliger les attaquants, et non le défenseur, à s'adapter en permanence.

QUI SOMMES NOUS ?

Diplômé en Management d'une École Supérieure de Commerce (MBS° et d'un Master spécialisé en Commerce International d'un Institut d'Administration d'Entreprise (IAE, Eric débute sa carrière en tant que Chef de cabinet d'un membre du Comité Exécutif de Capgemini. Il rejoint ensuite Sogeti, l'entité filiale du Groupe, leader du domaine de la Sécurité informatique.
Il y exercera pendant une dizaine d'années et occupera différents postes à responsabilités commerciales et marketing pour des grands comptes et industries stratégiques du Groupe.
Il rejoint Quarkslab en 2015 pour prendre en charge le développement et supporter la forte croissance de cette deep tech et accompagner les grandes organisations françaises et internationales dans la mise en place d'une réponse adaptée aux enjeux de la cybersécurité

"Forcer les attaquants, et non les défenseurs, à s'adapter en permanence !"

NOTRE SOLUTION

La recherche et le développement sont des piliers fondamentaux de Quarkslab depuis sa création il y a plus de 10 ans. Quarkslab a, en effet, été fondée dans le but de favoriser l'innovation en créant une jonction entre la recherche académique et une mise en pratique concrète, en intégrant par exemple les recherches en nouveaux services et logiciels de sécurité accessibles à tout type d'organisation.
L'expertise de Quarkslab combine la sécurité offensive et défensive dans la protection des applications et aide les entreprises et organisations gouvernementales à adopter une nouvelle posture de sécurité : Obliger les attaquants, et non les défenseurs, à s'adapter en permanence.
Grâce à nos services de conseil, à l'expertise de notre Lab ainsi qu'à nos logiciels, nous fournissons en France ou à l'international, des solutions sur mesure qui aident à protéger les actifs, les données sensibles et les utilisateurs contre des attaques de plus en plus sophistiquées. Contact : ehoudet@quarkslab.com

CHIFFRES CLÉS

2011 création
10 ans de R&D
Plusieurs bureaux dans le monde

FOCUS SUR RIOT

Notre mission est de faire de vos employés le meilleur atout cybersécurité de votre entreprise, en créant les outils qu'ils vont adorer utiliser.

L'équipe

"Préparez vos employés à faire face aux cyberattaques !"

QUI SOMMES-NOUS ?

Benjamin Netter est un serial entrepreneur français diplômé de l'EPITECH, co-fondateur de la plateforme de prêts aux entreprises October.

500 000 employés couverts dans 1 000 entreprises, membre du NEXT 40) et fondateur de Riot, plateforme de préparation des employés aux cyberattaques.

NOTRE SOLUTION

Riot permet de facilement déployer un programme de sensibilisation à la cybersécurité auprès des équipes.
Riot détecte automatiquement les faiblesses des employés, et permet d'y remédier par le conseil et la mise en pratique.
Contact : ben@tryriot.com

CHIFFRES CLÉS

Collaborateurs : 50
Clients : 1 000
5 ans d'existence
15 M€ de levée de fonds

FOCUS SUR RUBYCAT

RUBYCAT, éditeur de logiciels, vous apporte son expertise en cybersécurité et expérience en sécurisation des accès pour vous aider à répondre de manière simple à une problématique majeure : le manque de visibilité sur les actions réalisées par les comptes à privilèges (prestataires externes, administrateurs internes, ...) sur vos SI.

Cathy Lesage - Dirigeante

"Simplifiez-vous la gestion des accès à privilèges avec la solution logicielle rennaise de PAM/bastion, PROVE IT"

QUI SOMMES-NOUS ?

Depuis 2014, nous développons des logiciels dans le domaine de la cybersécurité avec une expertise en traçabilité des accès aux systèmes d'informations. Les déclinaisons de notre solution de PAM (Privileged Access Management) sont principalement axées sur un portail fédérateur des accès sensibles au SI (Bastion informatique). Elles sont déployées depuis plus de 10 ans chez nos clients qui apprécient notre dynamisme, notre volonté d'améliorer en permanence nos solutions, notre réactivité et notre professionnalisme. La maîtrise totale de nos développements en interne, procure à nos offres une assurance de qualité, une garantie d'adaptation de nos produits en fonction des besoins clients et une robustesse en terme de sécurité (cf. Certification ANSSI).
Notre périmètre d'intervention couvre tous les secteurs d'activité, qu'ils soient publics ou privés (PME/PMI jusqu'à ETI, collectivités locales et territoriales, hôpitaux...).

NOTRE SOLUTION

PROVE IT, solution logicielle de type " bastion-PAM " (certifiée Visa de sécurité-CSPN par l'ANSSI), renforce la sécurité des accès sensibles de votre système d'information. Elle permet de contrôler, tracer et enregistrer les actions réalisées par les comptes à privilèges sur le système d'information. Vous pourrez aussi les revoir ultérieurement sous format vidéo.
Comme le soulignent les réglementations ou recommandations en vigueur (RGPD, certification HDS, ISO 27001, guide de sécurisation du SI de l'ANSSI), quelle que soit la taille de votre établissement, il est important de tracer plus spécifiquement les accès sensibles à vos équipements critiques.
PROVE IT est une solution non invasive (aucun agent à installer), simple à déployer (installation en 30 min) et facile à administrer au quotidien. La licence est uniquement dimensionnée au nombre de connexions concomitantes vers vos ressources (les utilisateurs et équipements déclarés sont illimités).
Nous vous proposons de tester PROVE IT dans votre environnement (licence gratuite). N'hésitez pas à contacter vos intégrateurs. Vous souhaitez voir notre solution en action ? Nous organisons des webinaires hebdomadaires ; inscrivez-vous directement depuis notre site web www.rubycat.eu. (Présentation personnalisée sur demande).

CHIFFRES CLÉS

Collaborateurs : +20
+200 Clients
CA sur Rennes Métropole : 2M€

FOCUS SUR SEC-IT

SEC-IT est un cabinet d'audit et conseil spécialisé et dédié aux métiers de la cybersécurité. Créée en 2016, SEC-IT est spécialisée dans la protection des systèmes d'information et la sécurité numérique. Certifiés PASSI (Prestataire d'Audit de la Sécurité des Systèmes d'Information) depuis 2020, nous garantissons à nos clients des audits et services conformes aux plus hauts standards de cybersécurité.

QUI SOMMES-NOUS ?

SEC-IT, créé en 2016, est présent à Rennes, Paris, Toulouse, Lyon et Aix-en-Provence, et intervient sur le territoire national.
Nous accompagnons nos clients et partenaires à travers des solutions sur mesure pour répondre aux enjeux sectoriels et selon la taille des organisations (PME, ETI, Grands comptes, organismes publics). Forts de 8 ans d'expérience, nous intervenons sur des projets critiques et des secteurs variés, apportant une capacité d'adaptation au contexte de chaque entité.
Nous sommes agréés PASSI (Prestataire d'Audit de la Sécurité des Systèmes d'Information) délivré par l'ANSSI.

"Pour que la question de la cybersécurité n'en soit plus une"

NOTRE SOLUTION

Nos services adressent les besoins en audit, conseil, sécurité opérationnelle et formation :

- Audits techniques : architecture, configuration, tests d'intrusion web et infrastructure IT, OT, Cloud
- Audits organisationnels, plan de remédiation, feuille de route cyber
- Accompagnement dans la mise en oeuvre : NIS2, NIST, ISO 27001, ISO 21434, IEC 62443…
- Sécurité opérationnelle : Maintien en condition de sécurité (MCS), PCA/PRA
- Formation : Formation RSSI, RSSI Adjoint, administrateur SSI, chef de projets SI
- Préparation à la gestion de crise : Implémentation du SI de crise et des fiches réflexes, exercice de crise.

Contact : contact@sec-it.fr

CHIFFRES CLÉS

Collaborateurs : 30+
Clients : 150+ depuis 8 ans,
CA sur Rennes Métropole : 1M€ / an

FOCUS SUR SECURE IC

Avec une présence et des clients sur les 5 continents, Secure-IC est le leader en devenir et le seul fournisseur mondial de solutions de cybersécurité de bout en bout pour les systèmes embarqués et les objets connectés. S'appuyant sur une approche unique appelée PESC (Protect, Evaluate, Service & Certify), Secure-IC se positionne comme un partenaire qui accompagne ses clients tout au long du processus de conception des circuits intégrés.

Hassan Triqui - CEO et Président

Sylvain Guillet - Directeur technique

QUI SOMMES-NOUS ?

Hassan Triqui est titulaire d'un diplôme d'ingénieur de l'Institut National des Sciences Appliquées et d'un MBA de Rennes School of Business et bénéficie d'une expérience de plus de vingt ans des secteurs technologiques.
Avant de créer et de diriger Secure-IC, référence majeure du domaine des solutions de cybersécurité embarquées, il a été cadre dirigeant chez Thales et Thomson.
Sylvain Guilley est le directeur technique de Secure-IC et également professeur à TELECOM-Paris, chercheur associé à l'École Normale Supérieure (ENS, Paris), et professeur adjoint à l'Académie des Sciences de Chine. Il est rédacteur en chef de normes internationales, telles que ISO/IEC 20897, ISO/IEC 20085 et ISO/IEC 24485.
Rédacteur associé du Springer Journal of Cryptography Engineering (JCEN), il a coécrit plus de 250 articles scientifiques et déposé plus de 40 brevets d'invention.

"Les objets connectés doivent bénéficier des plus hauts niveaux de sécurité dès l'origine"

NOTRE SOLUTION

Secure-IC fournit des technologies de protection de pointe éprouvées, des éléments de sécurité intégrés et des plateformes d'évaluation de la sécurité pour satisfaire les plus hauts niveaux de certification des différents marchés (comme l'automobile, l'AIoT, la défense, les paiements et transactions, la mémoire et le stockage, les serveurs et le cloud).
Grâce à ses activités d'innovation et de recherche, Secure-IC fournit des technologies de protection de pointe et éprouvées sur silicium, des Secure Elements intégrés et des plateformes d'évaluation de la sécurité afin d'atteindre la conformité avec le plus haut niveau de certification pour différents marchés (comme l'automobile et la mobilité intelligente, la défense et l'espace, les semi-conducteurs, les infrastructures critiques, les serveurs et le cloud, la santé, l'électronique grand public). https://www.secure-ic.fr/

CHIFFRES CLÉS

Collaborateurs : 140
Clients : 200

FOCUS SUR SEKOIA

SEKOIA.IO est une solution de cybersécurité dédié pour les équipes de Security Operation Centers (SOC). SEKOIA.IO a été lancé en 2020 après 5 ans de R&D pour combler de nombreux manques en cybersécurité, en utilisant la puissance du renseignement d'origine cyber pour caractériser les menaces.

De gauche à droite : Thérèse Favet, Georges Bossert, Freddy Milesi (Président), David Bizeul, François Deruty

"One view, total control"

QUI SOMMES-NOUS ?

Entrepreneur depuis ses 19 ans, Freddy MILESI a co-fondé SEKOIA à 26 ans. Depuis 2008 il consacre tous ses efforts à des projets tech, pour créer les meilleures équipes, et leur donner l'opportunité de repenser la cybersécurité.
De background commercial et scientifique, Freddy a obtenu un Master en cybersécurité et cryptographie de la Royal Holloway University of London, un Bachelor en Management de MBS et un executive programme en management MAP à l'INSEAD. Freddy a débuté sa carrière au sein de cabinets français et US. David BIZEUL a 20 ans d'expérience dans l'industrie de la sécurité dans différents postes.
Comme principal succès, David a publié différents livres blancs sur les évolutions de la sécurité ainsi que plusieurs rapports détaillés sur des groupes d'attaquants. David a créé le CERT Société Générale puis celui d'Airbus Cybersecurity. En 2015, il fonde inThreat, startup spécialisée dans la threat intelligence maintenant fusionnée dans la plate-forme XDR SEKOIA.IO.

NOTRE SOLUTION

SEKOIA.IO se positionne comme une SOC Platform alliant l'anticipation, la détection et l'automatisation
- SEKOIA.IO apporte une capacité de supervision multi technologies et multi sources pleinement compatible avec un SI hybride
- SEKOIA.IO s'appuie sur sa base de threat intelligence exclusive pour détecter les attaques récentes
- En seulement quelques minutes, SEKOIA.IO est déployable et opérationnel
- Pour répondre efficacement, SEKOIA.IO dispose de son propre orchestrateur et de capacité d'automatisation
- SEKOIA.IO peut être opéré par vos équipes ou par votre partenaire MSSP sans complexité
- SEKOIA.IO participe activement à de multiples travaux de standardisations ou d'intérêt communautaires

Contact : contact@sekoia.io

CHIFFRES CLÉS

Collaborateurs : 110+
Clients: 1500+ / Danone, Vinci, DINUM, SNCF, OTAN, EDF, Avril, Council of Europe
CA sur Rennes Métropole : 15M€

FOCUS SUR SEKOST

Sekost est une startup bretonne experte en cybersécurité pour les petites et moyennes entreprises.

L'équipe de Sekost

QUI SOMMES-NOUS ?

Sekost propose une solution SaaS pour les ESN, permettant de tester rapidement la cybersécurité de leurs clients et de les accompagner avec des recommandations pour améliorer leur protection.

"Préparez vos clients au risque cyber"

NOTRE SOLUTION

Sekost propose une solution automatisée qui permet aux ESN et MSP de tester rapidement la cybersécurité de leurs clients et de détecter les vulnérabilités, comme le ferait un cybercriminel. Sa solution de scan teste à distance la sécurité des infrastructures et fournit un diagnostic clair avec des recommandations concrètes, particulièrement adaptées aux PME. L'ESN accompagne ensuite le client pour corriger les problèmes.
Sekost propose différents services :
- Le Flash Cyber, pour donner un aperçu de l'exposition de l'entreprise aux risques.
- Le Diagnostic Cyber, pour identifier les problèmes et obtenir un plan d'action personnalisé.
- Des ateliers de sensibilisation aux risques cyber.

Sekost noue des partenariats stratégiques avec des revendeurs en leur proposant des offres clés en main de cybersécurité à intégrer à leur catalogue. Ces partenaires peuvent ensuite accompagner leurs clients dans la mise en place des solutions et l'amélioration de leur protection contre les cybermenaces. Sekost propose également des ateliers de sensibilisation pour les clients, afin de renforcer leur compréhension des enjeux cyber et de créer une dynamique commerciale autour de ces offres. Contact : contact@sekost.fr ou 01 79 35 17 38

CHIFFRES CLÉS

200 entreprises accompagnées
6 collaborateurs
Créée en 2021

FOCUS SUR SHADLINE

Shadline est une solution de continuité numérique simple et accessible à tous. Une plateforme pour faire face à toute situation de crise cyber. Un entraînement pour préparer et former les équipes.

Olivier Wittebroodt, CEO

"Votre activité est maintenue en toute circonstances. Vous sécurisez vos exigences réglementaires et contractuelles"

QUI SOMMES-NOUS ?

Shadline permet d'outiller le PCA de ses clients pour augmenter la réactivité en cas de crise cyber, permettre une continuité de l'activité et soutenir la reconstruction de l'IT.
Les usages principaux sont :

- Garantir l'accès aux données vitales (informations clients, plan de redémarrage IT, contacts d'urgences, mallette de crise ...).

- Communiquer de manière sécurisée avec vos collaborateurs et vos partenaires.

- Entraîner régulièrement et avec un minimum d'efforts les équipes pour être toujours à jour, et prêt.

Shadline est une société rennaise d'une dizaine de collaborateurs.

Olivier W, entrepreneur de talent est le papa de la techno.

Il est accompagné par Olivier THÄERON et Patrick VALLEE pour le pilotage des opérations et le développement commercial.

NOTRE SOLUTION

Shadline se décline en deux modules :
- Une plateforme SaaS, iso fonctionnelle web et mobile, disponible en français et anglais, embarquant des solutions de communications sécurisées (chat, visio, transfert up ou down de fichier) et une sauvegarde des données essentielles. En somme, 1 war-room prête à l'emploi pour être résilient et indépendant en cas de crise.
- Un accompagnement pour identifier les besoins métiers, configurer la war room, et surtout des mises en situations régulières pour entraîner régulièrement et sans efforts les équipes et mettre à jour les process de crise.
Ainsi l'appropriation de la war room est facilitée, et les réflexes de crises améliorés.
Contact : contact@shadline.com

CHIFFRES CLÉS
2015 création
10 emplois
+ de 50 clients (Chiffres 2022)

FOCUS SUR SYLINK TECHNOLOGIE

SYLink TECHNOLOGIE est éditeur et fabricant français de solutions souveraines de cybersécurité.

SYLink Box, la solution sécurisée tout-en-un, simple et intuitive

"Une innovation de rupture contre les cybermenaces"

QUI SOMMES-NOUS ?

Entreprise française de sécurisation des réseaux, des données et des IoTs. Nous sommes éditeur et fabricant de solutions globales matérielles et logicielles, spécialisés dans la sécurisation des systèmes d'informations et dans la gestion des infrastructures informatiques critiques. Notre métier vise à répondre de manière simple à une problématique complexe : "Protéger simplement et efficacement les données sensibles des entreprises, de la plus petite à la plus grande, contre les cybercriminels tout en maîtrisant les coûts".

NOTRE SOLUTION

Les solutions sécurisées SYLink sont des technologies brevetées qui se nourrissent des cybermenaces pour les identifier et les comprendre. Ses algorithmes sont puissants, évolutifs et innovants, capables d'anticiper les risques et d'enrayer les menaces rapidement.
L'innovation est au centre de nos offres, nous permettant de fournir une protection optimale contre les cybermenaces grâce à des technologies avancées et des solutions sur-mesure développées par notre département de Recherche et Développement (R&D). Nos innovations contribuent également à la conformité aux régulations en vigueur et à l'adoption des meilleures pratiques en matière de cybersécurité.
Enfin, l'innovation chez SYLink assure une adaptation rapide face à l'évolution des menaces, garantissant ainsi la continuité et la sécurité des opérations des clients.
Contact : contact@sylink.fr

CHIFFRES CLÉS

Fondé en 2017
150 collaborateurs

FOCUS SUR SYNACKTIV

Synacktiv a pour objectif d'aider les entreprises à évaluer et améliorer le niveau de sécurité de leur système d'information. La société a été fondée en 2012 par deux experts en sécurité informatique. Ils n'ont de cesse depuis ce jour de faire de Synacktiv la référence française en matière de sécurité offensive.

Votre photo ou équipe

"Depuis 2012, Synacktiv attire et rassemble les meilleurs experts francophones dans le domaine de l'évaluation technique de la sécurité"

QUI SOMMES NOUS ?

Depuis 2012, Synacktiv attire et rassemble les meilleurs experts francophones dans le domaine de l'évaluation technique de sécurité. Nous nous différencions par la mise à disposition d'une excellence technique sur-mesure afin de répondre à vos enjeux les plus critiques. Nous intervenons auprès de secteurs d'activités divers et aux tailles de structures variées, en France et à l'international. Cette stratégie d'ultra spécialisation se décline sur l'ensemble de nos offres à valeur ajoutée :

1. L'évaluation de sécurité
2. Conception et développement de solutions sécurisées
3. Formation à la sécurité offensive
4. Accompagnement à la préparation et à la réponse aux incidents

Notre mission est d'améliorer la compétitivité de nos clients, en faisant de la sécurité un atout sans contrainte.

NOTRE SOLUTION

Comptant plus de 170 experts en sécurité offensive, l'équipe de Synacktiv s'articule autours de quatre pôles aux activités complémentaires :

1-Pôle Pentest (tests d'intrusion et audits techniques de sécurité : audit de configuration, revues d'architecture, revue de code, ...).

2-Pôle Reverse (analyse de composants complexes, recherche et exploitation de vulnérabilités, expertise couvrant l'analyse de composants électroniques, l'évaluation de composants cryptographiques, en passant par l'analyse de composants logiciels complexes avec ou sans code source).

3-Pôle Développement (développement d'outils de sécurité, assistance à la conception ou au développement de composants logiciels spécifiques à fort enjeu sécurité).

4-Pôle Incident Response (accompagnement sur l'ensemble du cycle de traitement d'un incident de sécurité, autant sur la préparation que sur sa détection). Contact : contact@synacktiv.com

CHIFFRES CLÉS

180 personnes
+26 M€ de CA
5 bureaux à travers la France

FOCUS SUR SYNETIS

Synetis conseille et accompagne les entreprises avec une offre globale conçue pour répondre efficacement aux besoins de sécurisation.

Éric Derouet, cofondateur et Président de Synetis et Rémi Fournier, cofondateur et Directeur Général.

"L'expertise Synetis au service de votre cybersécurité."

QUI SOMMES-NOUS ?

Créé en 2010, Synetis s'est imposé comme le leader des cabinets de conseil – indépendants financièrement – dans le domaine de la Sécurité des Systèmes d'Information (SSI). Cette réussite repose sur son expertise organisationnelle, fonctionnelle et technique approfondie en matière de cyber. Synetis met son savoir-faire à disposition de ses clients, qu'il s'agisse de PME, de TPE ou de grandes entreprises issues de tous les secteurs d'activité, en leur proposant des prestations sur mesure adaptées à leurs besoins.

NOTRE SOLUTION

Depuis sa création, Synetis s'engage - auprès de ses clients et partenaires - depuis des phases amonts de cadrage, de conseil ou d'audit jusqu'au déploiement et à la gestion de solutions de sécurité. Plusieurs offres, adaptables et sur-mesures, ont été imaginées pour répondre aux besoins et problématiques de votre entreprise :

- L'audit de sécurité : connaître son niveau d'exposition aux cybermenaces ;
- Le CERT - réponse à incidents : prévenir et anticiper les menaces, réagir en cas d'incident ;
- La GRC (Gouvernance, Risques et Conformité) : organiser et piloter votre cybersécurité ;
- L'Identité Numérique : maîtriser vos identités et accès ;
- La Sécurité Opérationnelle : déployer et opérer des solutions technologiques de protection des SI.

Et pour vous accompagner, toujours plus activement, Synetis met à votre disposition des offres de services de sécurité managés, sur l'ensemble de ces domaines (MSSP, SOC, Centre De Service Identité Numérique, etc.).

En outre, Synetis est qualifié Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) par l'ANSSI et en cours de qualification en tant que Prestataire de Réponse aux Incidents de Sécurité (PRIS). https://www.synetis.com/

CHIFFRES CLÉS

CA : 51,5M€
Effectifs : 350
Clients accompagnés : près de 500 clients

FOCUS SUR SYSTANCIA

Systancia est un éditeur de logiciels de cybersécurité indépendant et souverain, animé par le concept de Zero Trust.

Les équipes de Systancia

"La plateforme Zero Trust souveraine pour la sécurité des accès aux infrastructures IT et OT"

QUI SOMMES-NOUS ?

Systancia est le seul fournisseur français et même européen d'une plateforme Zero Trust de sécurisation des accès, vendue par un réseau de partenaires certifiés, qualifiés et sélectionnés pour leur expertise cyber.

Notre mission est de fournir aux organisations les éléments cyber nécessaires pour booster leur performance grâce à la confiance numérique. Pour ce faire, nous réunissons nos propres technologies dans une plateforme unique, combinant rapidité et facilité d'utilisation pour favoriser la productivité des utilisateurs et la performance des organisations.

NOTRE SOLUTION

La plateforme Zero Trust de Systancia permet de donner aux collaborateurs ou aux prestataires, quel que soit leur contexte (au bureau, en télétravail, chez un prestataire, opérateur industriel ...) un accès transparent, immédiat, sécurisé et tracé (métier ou privilégié, local ou distant, ...) à toutes les ressources dont ils ont besoin pour travailler (applications cloud ou dans le datacenter de l'organisation, postes de travail, données, infrastructures informatique ou industrielles, services).
Pour les organisations qui souhaitent :
- sécuriser l'accès de prestataires,
- surveiller les accès à privilèges aux infrastructures sensibles,
- sécuriser les accès aux infrastructures industrielles
- sécuriser le télétravail depuis des environnements non fiables,
- répondre aux enjeux de conformité réglementaires (NIS 2 , ISO 27001, DORA, TISAX ...)
- gérer leurs identités numériques de manière rigoureuse

Systancia, qui offre à la fois la gestion des accès et l'infrastructure d'accès au sein d'une expérience unifiée, vous accompagne de bout en bout dans votre stratégie Zero Trust, en commençant où vous voulez et en évoluant en fonction des besoins de votre organisation : gestion des identités, gestion des accès, accès à privilèges, accès réseaux distants.
Contact : commercial@systancia.com

CHIFFRES CLÉS

3 minutes de déploiement de votre plateforme de production
30% croissance SaaS
100 % technologie Systancia

FOCUS SUR TREEBAL GREEN

Treebal Pro est une plateforme de communication éthique et eco-responsable permettant de sécuriser les échanges entre toutes les équipes au service de la transition sociétale et environnementale.

L'équipe de Treebal Green

"Échanger dans le respect de l'Humain et de la Planète"

QUI SOMMES-NOUS ?

À l'origine de Treebal, 3 associés décidés à agir face au dérèglement climatique, mais aussi à apporter des solutions aux dérives sociales et éthiques du numérique. Ensemble, ils fondent Treebal. Treebal, c'est une messagerie qui conjugue efficacité et sobriété énergétique, protection des données et respect de l'utilisateur.
Depuis notre territoire, la Bretagne, nous contribuons au déploiement d'un numérique éthique, inclusif et responsable qui renforce la coopération

NOTRE SOLUTION

Treebal remet la question de sobriété numérique et de transition environnementale au cœur des usages dans les entreprises pour une reconquête de la souveraineté technologique.
- Treebal redéfinit les standards d'impact d'une communication efficace, éthique et durable.
- Treebal concourt à l'autonomie stratégique des organisations en France et en Europe.
- Treebal œuvre à la protection économique des organisations et à la sécurité de leurs informations.

Sécurité de la solution :
https://www.treebal.green/solution-technique.html
https://wwa.wavestone.com/fr/insight/radar-des-startups-cybersecurite-francaise-2025/
Contact : contact@treebal.green

CHIFFRES CLÉS

Collaborateurs : 10
Clients : Industrie, Transport, Agro, Collectivités
CA sur Rennes Métropole : NC

FOCUS SUR WALLACK

WALLACK est spécialisée dans la cybersécurité des PME/PMI, des ETI et des collectivités territoriales (mairies, EPCI). A partir d'une évaluation de leur maturité, la startup incarne la direction cybersécurité de ces organisations, permettant d'assurer la gestion de la sécurité numérique des clients, de la stratégie au déploiement.

Alexandre Matthey-Doret, Président et Julien YVENAT, Directeur Général, co-fondateurs.

"Adapter et innover pour rendre accessibles et réalistes les recommandations de sécurité"

QUI SOMMES-NOUS ?

Notre entreprise a été co-fondée par Alexandre Matthey-Doret et Julien Yvenat, tous deux ingénieurs en cyberdéfense.
Forte de 14 collaborateurs, Wallack est au service d'une soixantaine de clients dans le Grand Ouest.
Notre ADN est d'adapter et d'innover dans les stratégies et techniques de la cybersécurité pour que nos clients atteignent un niveau de sécurité équivalent aux plus grandes entreprises tout en respectant des budgets contraints.

NOTRE SOLUTION

Nous constituons des Directions Cybersécurité à part entière, composées d'un Responsable de la Sécurité des Systèmes d'Information (RSSI = Responsable de la Cybersécurité) et d'experts en Gouvernance, Risques, Conformité (GRC) ou en Sécurité Opérationnelle. A l'usage ou de manière récurrente, nous nous occupons de gérer complètement la cybersécurité de nos clients : stratégie, budgets, processus internes, formation/sensibilisation, contrôle interne, sécurisation du système d'information (réseau, terminaux, supervision, etc.), etc...
En cas d'attaque, nos équipes de réponse à incident prennent en charge la gestion de crise avec la direction et assurent les opérations d'investigation, de remédiation et d'échanges avec les autorités concernées.
Nous accompagnons nos clients également grâce à nos formations, en ligne comme en présentiel, destinées aussi bien aux utilisateurs qu'aux spécialistes métiers (RH, comptabilité, qualité, informatique, etc.).
La mutualisation permise par nos prestations permet d'avoir toujours une équipe pour s'occuper de votre organisation et de diminuer drastiquement les coûts de la cybersécurité, avec une division par 2 voire par 3 des coûts globaux. "Grâce à des efforts de R&D importants et une philosophie adaptée à nos clients, les petits et moyens acteurs qui font nos territoires ont aussi le droit au meilleur de la cybersécurité !"

CHIFFRES CLÉS

Collaborateurs : 14
60aine de clients dans le Grand Ouest
Ouverture d'une agence à Brest en janvier 2025

FOCUS SUR WALLIX

WALLIX est un éditeur européen de cybersécurité avec une présence internationale, qui offre aux entreprises des solutions de contrôle des identités et des accès robustes, garantissant des interactions numériques transparentes et sécurisées dans les environnements IT et OT.

Jean-Noël de Galzain, fondateur de Wallix

"Reprenez le contrôle des accès de vos utilisateurs et de vos machines dans un monde numérique !"

QUI SOMMES-NOUS ?

Fondé en 2003 par Jean-Noël de Galzain (PDG), WALLIX est aujourd'hui un leader mondial sur le marché de la sécurité des identités et des accès, reconnu par les plus prestigieux cabinets d'analystes. Sa mission est de fournir un service d'accès identifié, simple et sécurisé, pour permettre aux utilisateurs d'évoluer sans risque dans les environnements numériques et industriels.
Les solutions WALLIX sont distribuées par un réseau de plus de 300 revendeurs et intégrateurs à travers le monde et WALLIX accompagne plus de 3 100 organisations dans plus de 90 pays, dans la sécurisation de leur transformation numérique. OT.security by WALLIX est une marque dédiée à la sécurisation des accès et des identités numériques dans les environnements industriels.
La société est cotée en bourse sur Euronext Growth depuis juin 2015 (ALLIX).

NOTRE SOLUTION

Les solutions de WALLIX en matière de gestion des accès à privilèges, de gestion des accès des collaborateurs et de gouvernance protègent les actifs critiques, simplifient la conformité et améliorent l'efficacité opérationnelle.
Le portefeuille WALLIX est disponible sur site, en hybride et via la plateforme SaaS WALLIX One, dans des configurations adaptées aux besoins de chaque client.
En 2025, WALLIX figure parmi les meilleurs éditeurs mondiaux de Privileged Access Management (PAM), régulièrement salué pour sa vision stratégique et son leadership technologique. Ces rapports mettent en lumière l'expertise de WALLIX en gestion des identités et des accès, tout en réaffirmant sa capacité d'innovation, notamment dans les environnements Industriels (OT) et les solutions SaaS unifiées (WALLIX One).
Contact : info@wallix.com - LinkedIn : WALLIX Group

CHIFFRES CLÉS

+ 3100 clients dans 90 pays
+240 collaborateurs dans 16 pays
3 centres de R&D dont 1 à Rennes·
2018 création à Rennes

FOCUS SUR WAN PULSE

La société WanPulse offre son expertise auprès de toutes organisations recherchant à optimiser leur parc informatique. Nous prônons le "Made in France", en innovant, en développant au quotidien la solution proVconnect.

L'équipe de Wan Pulse

"Réduisez le temps passé à l'administration des postes par l'automatisation"

QUI SOMMES-NOUS ?

WanPulse est un éditeur de logiciels indépendant (ISV) basé en France, spécialisé dans les solutions de gestion des dispositifs. Fondée en 2009, l'entreprise s'est rapidement imposée comme un acteur clé dans le secteur des technologies grâce à son expertise et son engagement envers l'innovation. Avec une équipe diversifiée d'experts en développement de logiciels et en support client, WanPulse se consacre à aider les entreprises à optimiser leur infrastructure informatique. Nous avons établi une forte présence sur le marché, notamment dans les secteurs du retail, de l'éducation, des collectivités et de la santé, en collaborant avec des clients réputés en Europe et en Asie. Notre récente expansion sur le marché américain témoigne de notre ambition de forger des partenariats stratégiques et d'élargir notre impact à l'échelle mondiale.

NOTRE SOLUTION

proVconnect est une solution complète de gestion des parcs informatiques, spécialisée dans la supervision, le contrôle de conformité et la remédiation automatique. Conçu pour répondre aux besoins des directions informatiques, proVconnect permet de gérer efficacement les postes Windows et Linux, y compris les ordinateurs, les bornes, les serveurs et les systèmes de point de vente (POS). Grâce à son interface intuitive, les utilisateurs peuvent surveiller l'état des appareils en temps réel, automatiser les mises à jour, automatiser la détection et la résolution des incidents et garantir la conformité aux normes de sécurité. Avec proVconnect, les entreprises optimisent leurs opérations tout en assurant la sécurité et la performance de leur infrastructure IT.
Contact : info@wan-pulse.com

CHIFFRES CLÉS

Collaborateurs : 8
Licences activées : 240 000
Fonctionnalités : 200+
Taux de satisfaction : 97%

FOCUS SUR WING IT

Wing it est une entreprise spécialisée dans les services numériques dont l'expertise s'étend de la captation, du traitement des données jusqu'à leur stockage et leur sécurisation.

QUI SOMMES-NOUS ?

Après 15 ans dans le développement informatique pour Mathieu Notin et 20 ans dans le développement commercial pour Maxime Guy, ils décident en 2024 de créer leur propre société de conseil numérique. Ils puisent leurs expériences au sein des différentes expériences professionnelles pour construire une entreprise qui leur ressemble.
Le pragmatisme, le sens du service et la fiabilité définissent l'approche de Wing-it auprès des clients.

"On promeut l'approche sécurité dans nos développements pour réduire le risque de vulnérabilité"

NOTRE SOLUTION

Wing-it est une entreprise spécialisée dans les services numériques dont l'expertise s'étend de la captation, du traitement des données jusqu'à leur stockage et leur sécurisation.
Une des singularités de l'entreprise est la forte culture sécurité de ses collaborateurs qui promeuvent la cyber prévoyance.
Wing-it travaille pour différents secteurs dont certains demeurent confidentiels compte tenu des missions.
Contact : contact@wing-it.fr

CHIFFRES CLÉS

Date de Création : 2025
Collaboration des fondateurs depuis 2012

FOCUS SUR WITHLAW

Withlaw est un cabinet d'avocats spécialisé dans le domaine de la cybersécurité.

Anne-Laure Gaillard, fondatrice

"Cabinet d'avocats d'affaires expert en droit du numérique et du numérique en santé"

QUI SOMMES NOUS ?

Avocate au Barreau de Rennes, Anne-Laure a créé le cabinet Withlaw après une expérience de plus de 15 ans en tant que juriste d'entreprise, dont 10 ans au sein du cabinet international d'audit et de conseil PwC (ex PricewaterhouseCoopers et Landwell) où elle a développé et animé, au sein de la Direction juridique, les pôles contrats et protection des données / CNIL.
Elle a ainsi acquis une expérience significative en droit des affaires, et est susceptible d'intervenir pour des entreprises de toutes taille, de la TPE aux grands groupes.

NOTRE SOLUTION

Vous accompagner sur l'ensemble du territoire juridique lié à la cybersécurité.
Contact : www.withlaw-avocats.fr

CHIFFRES CLÉS

Création en 2016
1 expertise unique

FOCUS SUR YESWEHACK

YesWeHack est une plateforme globale de Bug Bounty et de gestion des vulnérabilités.

Romain Lecoeuvre, COO et co-fondateur

"Décuplez vos capacités de test et maximisez votre couverture des risques grâce à nos solutions de gestion des vulnérabilités."

QUI SOMMES-NOUS ?

Romain Lecoeuvre est un hacker éthique certifié et un spécialiste de la cybersécurité. Il a travaillé pendant plusieurs années en tant que formateur en sécurité, consultant en sécurité et responsable de département cybersécurité.
Il a co-fondé YesWeHack et l'a rejoint en tant que directeur technique en 2018. Il y occupe aujourd'hui le poste de directeur des opérations.
Pendant neuf ans, Romain a également été membre du conseil d'administration de l'association française HZV et a participé à l'organisation du plus ancien événement français de hackers underground, leHACK.

NOTRE SOLUTION

YesWeHack connecte les organisations du monde entier à des dizaines de milliers de hackers éthiques, dont l'objectif est de découvrir les vulnérabilités potentielles au sein de sites web, applications mobiles, appareils connectés et infrastructures numériques. La plateforme YesWeHack offre une gamme de solutions intégrées, basées sur des API : le Bug Bounty (recherche de vulnérabilités via une approche crowdsourcée) ; la Politique de Divulgation de Vulnérabilités, VDP (création d'un canal sécurisé pour le signalement de vulnérabilités externes) ; le Pentest Management (gestion des rapports de pentest issus de différentes sources) ; l'Attack Surface Management (cartographie continue de l'exposition numérique et détection des vecteurs d'attaque) ; ainsi que le "Dojo" (formation au hacking éthique).
Contact : contact@yeswehack.com

CHIFFRES CLÉS

Fondé en 2015
105 collaborateurs
+80 000 hackers éthiques

Offre de service et de produit
Positionnement des entreprises

2025

ENTREPRISES DE RENNES MÉTROPOLE

Signifie que l'entreprise fait l'objet d'une fiche

Entreprise	Site internet
a3bc	www.a3bc.org
abak systemes	http://www.abaksystemes.fr/jml/
acceis	http://www.acceis.fr
adaltys	https://adaltys.com/expertises/
advens	https://www.advens.fr/
airbus cyber security	www.airbus-cyber-security.com
akerva	https://akerva.com/
akka technologies	https://www.akka-technologies.com/fr
akonis	https://akonis.fr/entreprise
alcyconie	https://alcyconie.com/
alten	http://www.alten.fr/
amn brains	https://amnbrains.com/
amossys	https://www.amossys.fr/
anozr way	https://www.anozrway.com/
apave	https://oppida.apave.com/
apixit	https://www.apixit.fr/
apizee	http://www.apizee.com
arzen	https://arzen.tech/
ascent formation	https://ascent-formation.fr
astek grand ouest	https://astekgroup.fr/
atos digital security - evidens	https://eviden.com
avoxa cyber data	https://www.avoxa.fr/
axians rennes groupe vinci	www.axians.fr
bloo conseil	https://www.bloo-conseil.fr/
business & it consulting	https://www.business-and-it-consulting.com/
bretagne telecom	https://www.bt-blue.com/
cailabs	http://www.cailabs.com/technology/
calidra	https://calidra.io/
capgemini technology services	https://www.capgemini.com/fr-fr/
cardelya-gemalto	https://www.cardelya.fr/
ceebex	https://www.ceebex.fr/
cgi France	https://www.cgi.com/France/fr-fr
chapsvision	https://www.chapsvision.fr
claranet	www.claranet.fr
cloud-iam	www.cloud-iam.com
cryptovia	http://www.cryptovia.com/
ct square	https://ct-square.com
cyberpro assur	www.cyberproassur.fr
cybermyne	https://www.cybermyne.fr/
cy mind	https://www.cymind.fr/
danso	https://danso.fr
daspren	https://daspren.com/
davidson consulting ouest	www.davidson.fr
easylience	https://easylience.com/
econocom	https://www.econocom.com/fr
edsi security	https://edsisecurity.com/
eon-jaguin	https://www.eonjaguin-avocat.com/
erium alias blacknoise	http://erium.fr/ https://blacknoise.co/
experis France	https://experisFrance.fr
extia	https://www.extia-group.com/fr-fr

fairtrust	https://www.fairtrust.com/
famoco	https://www.famoco.com/fr/
foliateam a2com ex a2com	https://www.a2com.fr/
formind	http://www.formind.fr/
garnault & associes	www.garnault-associes.com
gatewatcher	www.gatewatcher.com
geoide crypto&com	https://public.geoide.fr/
glimps	www.glimps.fr
hectic	https://www.linkedin.com/company/hectic-cyber
hogo business services	http://h-b-s.fr/
icodia	https://www.icodia.com/
idemia ex morpho	https://www.idemia.com/fr/
idnow ex ariadnext	https://www.ariadnext.com/
imatag ex lamark	www.imatag.com
imineti filiale de niji	https://www.niji.fr/
inetum ex gfi	http://www.gfi.fr
ipcyb	https://ipcyb.fr/
isti	https://www.lsti-certification.fr
iswot	https://iswot.io/
it link France	www.itlink.fr
kereval	http://www.kereval.com/
lacroix lab	www.lacroix-lab.com
lamane	http://www.lamane.net/
lootus	https://www.lootus.net/fr/
lr technologies groupe	https://lrtechnologies.fr/fr/
malizen	https://malizen.com/
metsys	www.metsys.fr
nanocode marque easylience	https://easylience.com/
neo soft	https://www.neo-soft.fr/
neotrust	https://www.neotrust.io/
neverhack ex pr0ph3cy	https://neverhack.com/
nexguard labs	https://dtv.nagra.com/
nomios	www.nomios.fr
Numih France	https://numihfrance.fr/
nxo France ex nextiraone	https://www.nextiraone.eu/fr/
nybble security	https://lepoool.tech/startmeup-nybble-security
oci	https://www.oci.fr/
omr infogerance	www.omr.fr
onyphe	www.onyphe.io
orange cyberdefense	https://cyberdefense.orange.com
orange lab innovation	https://lelab.orange.fr/
orange sa	https://www.orange.com/fr
ornisec	www.ornisec.com
osytos	https://www.osytos.com/
Ovalt	https://groupe-ovalt.com/
owaltech marque shadline	https://www.shadline.com/
own	https://www.own.security/
perses communication	https://perses-communication.com/
qonfucius marque : qongzi	https://qongzi.com/
quarkslab	https://www.quarkslab.com/

Riot	https://fr.tryriot.com/
Rubycat	http://www.rubycat-labs.com
Safran	https://www.safran-group.com/
Scalian	http://www.scalian.com
Sec IT Solutions	www.sec-it-solutions.fr
Secure-IC	http://www.secure-ic.com/
Secure IT Consulting	https://secure-itconsulting.com/
Sekoia.io	https://www.sekoia.io/fr/homepage/
Sekost	https://sekost.fr/
SenseYou	http://www.senseyou.fr/
SERMA Safety & Security	http://www.serma-safety-security.com/
Sesame IT	https://sesame-it.com/
Shadline	https://www.shadline.fr/
Silicom	http://www.silicom.fr/
Situation	https://www.situation.sh/
Skild	https://skyld.io/
Sogeti	www.fr.sogeti.com
Sogitec	https://www.sogitec.fr/
Sopra Steria	https://www.soprasteria.com/fr
Squad	https://squad.fr/fr/
STMicroelectronics	https://www.st.com/content/st_com/en.html
Sylink	https://sylink.fr/
Synacktiv	https://www.synacktiv.com/
Synetis	https://www.synetis.com/
Systancia	https://www.systancia.com/
Thales	https://www.thalesgroup.com/
Treebal	https://www.treebal.green/
Viacyber	https://viacyber.fr/
Wallack	https://wallack.fr/
Wallix	https://www.wallix.com/fr/
Wan Pulse	https://www.wan-pulse.com/
Wing IT	https://www.wing-it.fr/
Withlaw Avocats	https://www.withlaw-avocats.fr/
Yeswehack	https://www.yeswehack.com/fr

Les principales mesures de NIS2 applicables aux entités concernées :

- Politiques de sécurité de l'information et de gestion des risques
- Gestion des incidents et signalement
- Continuité des activités et reprise après sinistre
- Gestion de la sécurité des tiers / chaîne d'approvisionnement
- Sécurité des réseaux et des systèmes d'information lors de l'acquisition, du développement et de la maintenance, et gestion des vulnérabilités
- politiques et procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité
- Formation et sensibilisation à la cybersécurité
- Politiques et procédures relatives à l'utilisation de la cryptographie ou chiffrement
- Politiques en matière de gestion des ressources humaines, des accès et de la sécurité de la gestion des actifs
- Politique d'utilisation de l'authentification multi-facteurs

Pour plus d'information sur NIS2, ne pas hésiter à consulter : https://monespacenis2.cyber.gouv.fr/directive/

ENTREPRISES AYANT UNE OFFRE NIS2

Entreprise	article 20 concerne les aspects généraux relatifs à la surveillance et l'exécution	L'article 21.2 intègre la maîtrise des accès physiques aux locaux, serveurs et autres matériels informatiques	L'article 21.2.a traite, à l'instar de l'article 20, de sujets de gouvernance et de mise en œuvre d'une PSSI	L'article 21.2.b est dédié à la gestion des incidents.	L'article 21.2.c traite de continuité/reprise des activités.	L'article 21.2.d porte sur " la sécurité de la chaîne d'approvisionnement ".	Email
Alcyconie				Oui	Oui		contact@alcyconie.com
ALMOND - AMOSSYS	Oui	Oui	Oui	Oui	Oui	Oui	commerce@amossys.fr
Amn Brains	Oui		Oui				rachid.elalaoui@amnbrains.com
ANOZR WAY	Oui	Oui	Oui	Oui		Oui	contact@anozrway.com
APIXIT			Oui	Oui	Oui	Oui	communication@apixit.fr
AVOXA CYBER	Oui					Oui	jnrobin@avoxa.fr
BLOO CONSEIL							contact@bloo-conseil.fr
Business & IT Consulting					Oui		contact@business-and-it-consulting.com
Cloud-IAM	Oui						support@cloud-iam.com
CT-SQUARE	Oui		Oui	Oui		Oui	contact@ct-square.com
Daspren				Oui		Oui	contact@daspren.com
Erium	Oui			Oui		Oui	contact@erium.fr
FairTrust							maiwen.simon@fairtrust.com
Foliateam	Oui	Oui	Oui	Oui	Oui		chloe@foliateam.com
Gatewatcher			Oui	Oui	Oui	Oui	aubin.debelleroche@gatewatcher.com
GLIMPS			Oui	Oui	Oui	Oui	timothee.billet@glimps.re
GUY						Oui	contact@wing-it.fr
ICODIA	Oui	Oui	Oui	Oui	Oui	Oui	contact@icodia.com
Imineti By Niji	Oui	Oui	Oui	Oui	Oui	Oui	herve.troalic@niji.fr
Malizen				Oui			hello@malizen.com
NEVERHACK	Oui	Oui	Oui	Oui	Oui	Oui	contact@neverhack.com
Niji	Oui	Oui	Oui	Oui	Oui	Oui	herve.troalic@niji.fr
NOMIOS	Oui		Oui	Oui	Oui	Oui	info-rennes@nomios.fr
Numih France	Oui		Oui	Oui	Oui	Oui	nicolas.jolivet@sib.fr
OCI Informatique & Digital			Oui	Oui	Oui	Oui	info@oci.fr

Réponses auto déclaratives

ENTREPRISES AYANT UNE OFFRE NIS2

Entreprise	L'article 21.2.e regroupe toutes les mesures techniques nécessaires à garantir la sécurité du SI.	L'article 21.2.f vient vérifier la solidité et l'efficacité de la démarche de gestion des risques, au travers d'audits si nécessaires	L'article 21.2.g traite de la formation et de la sensibilisation des personnels	L'article 21.2.h concerne l'utilisation de la cryptographie et du chiffrement.	L'article 21.2.i couvre " la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs "	L'article 21.2.j comprend l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification	Email
Alcyconie		Oui					contact@alcyconie.com
ALMOND - AMOSSYS	Oui	Oui	Oui	Oui	Oui	Oui	commerce@amossys.fr
Amn Brains		Oui					rachid.elalaoui@amnbrains.com
ANOZR WAY			Oui		Oui		contact@anozrway.com
APIXIT	Oui	Oui	Oui	Oui	Oui	Oui	communication@apixit.fr
AVOXA CYBER					Oui		jnrobin@avoxa.fr
BLOO CONSEIL	Oui						contact@bloo-conseil.fr
Business & IT Consulting	Oui						contact@business-and-it-consulting.com
Cloud-IAM	Oui				Oui	Oui	support@cloud-iam.com
CT-SQUARE	Oui	Oui					contact@ct-square.com
Daspren	Oui				Oui		contact@daspren.com
Erium	Oui		Oui		Oui		contact@erium.fr
FairTrust	Oui				Oui	Oui	maiwen.simon@fairtrust.com
Foliateam			Oui		Oui	Oui	chloe@foliateam.com
Gatewatcher	Oui				Oui		aubin.debelleroche@gatewatcher.com
GLIMPS	Oui						timothee.billet@glimps.re
GUY							contact@wing-it.fr
ICODIA	Oui	Oui	Oui	Oui	Oui	Oui	contact@icodia.com
Imineti By Niji		Oui	Oui	Oui	Oui	Oui	herve.troalic@niji.fr
Malizen	Oui						hello@malizen.com
Mipih-SIB	Oui	Oui	Oui		Oui		nicolas.jolivet@sib.fr
NEVERHACK	Oui	Oui	Oui	Oui	Oui	Oui	contact@neverhack.com
Niji	Oui	Oui	Oui	Oui	Oui	Oui	herve.troalic@niji.fr
NOMIOS	Oui	Oui	Oui	Oui	Oui	Oui	info-rennes@nomios.fr
OCI Informatique & Digital	Oui	Oui	Oui				info@oci.fr

Réponses auto déclaratives

ENTREPRISES AYANT UNE OFFRE NIS2

Entreprise	article 20	L'article 21.2 intègre la maîtrise des accès physiques aux locaux, serveurs et autres matériels informatiques	L'article 21.2.a traite, à l'instar de l'article 20, de sujets de gouvernance et de mise en œuvre d'une PSSI	L'article 21.2.b est dédié à la gestion des incidents.	L'article 21.2.c traite de continuité/reprise des activités.	L'article 21.2.d porte sur " la sécurité de la chaîne d'approvisionnement ".	Email
Alcyconie				Oui	Oui		contact@alcyconie.com
ALMOND - AMOSSYS	Oui	Oui	Oui	Oui	Oui	Oui	commerce@amossys.fr
Amn Brains	Oui		Oui				rachid.elalaoui@amnbrains.com
ANOZR WAY	Oui	Oui	Oui	Oui		Oui	contact@anozrway.com
APIXIT			Oui	Oui	Oui	Oui	communication@apixit.fr
AVOXA CYBER	Oui					Oui	jnrobin@avoxa.fr
BLOO CONSEIL							contact@bloo-conseil.fr
Business & IT Consulting					Oui		contact@business-and-it-consulting.com
Cloud-IAM	Oui						support@cloud-iam.com
CT-SQUARE	Oui		Oui	Oui		Oui	contact@ct-square.com
Daspren				Oui		Oui	contact@daspren.com
Erium	Oui			Oui		Oui	contact@erium.fr
FairTrust							maiwen.simon@fairtrust.com
Foliateam	Oui	Oui	Oui	Oui	Oui		chloe@foliateam.com
Gatewatcher			Oui	Oui	Oui	Oui	aubin.debelleroche@gatewatcher.com
GLIMPS			Oui	Oui	Oui	Oui	timothee.billet@glimps.re
GUY						Oui	contact@wing-it.fr
ICODIA	Oui	Oui	Oui	Oui	Oui	Oui	contact@icodia.com
Imineti By Niji	Oui	Oui	Oui	Oui	Oui	Oui	herve.troalic@niji.fr
Malizen				Oui			hello@malizen.com
Mipih-SIB	Oui		Oui	Oui	Oui	Oui	nicolas.jolivet@sib.fr
NEVERHACK	Oui	Oui	Oui	Oui	Oui	Oui	contact@neverhack.com
Niji	Oui	Oui	Oui	Oui	Oui	Oui	herve.troalic@niji.fr
NOMIOS	Oui		Oui	Oui	Oui	Oui	info-rennes@nomios.fr
OCI Informatique & Digital			Oui	Oui	Oui	Oui	info@oci.fr

Réponses auto déclaratives

ENTREPRISES AYANT UNE OFFRE NIS2

Entreprise	article 20	L'article 21.2 intègre la maîtrise des accès physiques aux locaux, serveurs et autres matériels informatiques	L'article 21.2.a traite, à l'instar de l'article 20, de sujets de gouvernance et de mise en œuvre d'une PSSI	L'article 21.2.b est dédié à la gestion des incidents.	L'article 21.2.c traite de continuité/reprise des activités.	L'article 21.2.d porte sur " la sécurité de la chaîne d'approvisionnement ".	Email
ORNISEC	Oui	Oui	Oui	Oui	Oui	Oui	a.sabbar@ornisec.com
Ovalt	Oui	Oui	Oui	Oui	Oui	Oui	jmorel@groupe-ovalt.com
OWN	Oui		Oui	Oui	Oui	Oui	contact@own.security
RUBYCAT				Oui			commercial@rubycat.eu
SEC-IT SOLUTIONS	Oui	Oui	Oui	Oui	Oui	Oui	contact@sec-it.fr
Sekoia.io SAS	Oui					Oui	contact@sekoia.io
SHADLINE	Oui		Oui	Oui	Oui		contact@shadline.com
SYNACKTIV		Oui		Oui		Oui	contact@synacktiv.com
Sylink	Oui	Oui	Oui	Oui	Oui	Oui	malena.moreira@sylink.com
Synetis	Oui	Oui	Oui	Oui	Oui	Oui	contact@synetis.com
SYSTANCIA						Oui	marketing@systancia.com
WALLACK	Oui		Oui	Oui	Oui	Oui	contact@wallack.fr

Réponses auto déclaratives

ENTREPRISES AYANT UNE OFFRE NIS2

Entreprise	L'article 21.2.e regroupe toutes les mesures techniques nécessaires à garantir la sécurité du SI.	L'article 21.2.f vient vérifier la solidité et l'efficacité de la démarche de gestion des risques, au travers d'audits si nécessaires	L'article 21.2.g traite de la formation et de la sensibilisation des personnels	L'article 21.2.h concerne l'utilisation de la cryptographie et du chiffrement.	L'article 21.2.i couvre " la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs "	L'article 21.2.j comprend l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification	Email
ORNISEC	Oui	Oui	Oui	Oui	Oui	Oui	a.sabbar@ornisec.com
OWN	Oui	Oui	Oui	Oui		Oui	contact@own.security
RUBYCAT	Oui			Oui	Oui	Oui	commercial@rubycat.eu
SEC-IT SOLUTIONS	Oui	Oui	Oui	Oui	Oui	Oui	contact@sec-it.fr
Sekoia.io SAS	Oui			Oui	Oui	Oui	contact@sekoia.io
SHADLINE	Oui	Oui	Oui				contact@shadline.com
SYNACKTIV	Oui	Oui		Oui	Oui		contact@synacktiv.com
Sylink	Oui	Oui	Oui	Oui	Oui	Oui	malena.moreira@sylink.com
Synetis	Oui	Oui	Oui	Oui	Oui	Oui	contact@synetis.com
SYSTANCIA	Oui			Oui	Oui	Oui	marketing@systancia.com
WALLACK	Oui	Oui	Oui	Oui	Oui	Oui	contact@wallack.fr
YesWeHack	Oui	Oui					contact@yeswehack.com

Réponses auto déclaratives

ENTREPRISES AYANT UNE OFFRE DORA

Destiné à harmoniser les règles concernant la résilience opérationnelle numérique, la gestion des risques informatiques et les normes de cybersécurité du secteur financier dans l'Union européenne, le règlement DORA a été publié au JOUE le 14 décembre 2022.

Il est entré en application depuis le 17 janvier 2025 et en cours de transposition en droit français. Le périmètre du règlement DORA inclut un grand nombre d'entités financières.

Il comprend des dispositions imposant à celles-ci de mettre en place un cadre de gestion du risque lié aux technologies de l'information et de la communication (TIC), de notifier aux autorités compétentes les incidents majeurs liés aux TIC, d'effectuer des tests de résilience opérationnelle numérique et de gérer le risque lié aux recours à des prestataires tiers de services TIC.

Il introduit également un cadre de supervision européen pour les prestataires tiers de services TIC considérés comme "critiques "

ENTREPRISES AYANT UNE OFFRE DORA

Entreprise	Audit et diagnostics à DORA	Conceptions stratégiques et procédures et impacts DORA	Gestion des risques	Tests	Gestion de la sécurité des fournisseurs de services informatiques	Email
ALCYCONIE			Oui	Oui		contact@alcyconie.com
ALMOND - AMOSSYS	Oui	Oui	Oui	Oui	Oui	commerce@amossys.fr
Amn Brains	Oui	Oui	Oui		Oui	rachid.elalaoui@amnbrains.com
ANOZR WAY			Oui		Oui	contact@anozrway.com
AVOXA CYBER	Oui	Oui	Oui		Oui	jnrobin@avoxa.fr
BLOO CONSEIL			Oui			contact@bloo-conseil.fr
Business & IT Consulting				Oui		contact@business-and-it-consulting.com
Cloud-IAM						support@cloud-iam.com
CT-SQUARE	Oui	Oui	Oui	Oui		contact@ct-square.com
Erium	Oui	Oui		Oui		contact@erium.fr
FairTrust	Oui		Oui			maiwen.simon@fairtrust.com
Gatewatcher			Oui		Oui	aubin.debelleroche@gatewatcher.com
GLIMPS		Oui	Oui	Oui		timothee.billet@glimps.re
GUY				Oui		contact@wing-it.fr
ICODIA			Oui	Oui	Oui	contact@icodia.com
Imineti By Niji	Oui	Oui	Oui		Oui	herve.troalic@niji.fr
Malizen			Oui			hello@malizen.com
NEVERHACK	Oui	Oui	Oui	Oui	Oui	contact@neverhack.com
Niji	Oui	Oui	Oui		Oui	herve.troalic@niji.fr
OCI Informatique & Digital	Oui		Oui	Oui		info@oci.fr
ORNISEC	Oui	Oui	Oui	Oui	Oui	a.sabbar@ornisec.com

Réponses auto déclaratives

ENTREPRISES AYANT UNE OFFRE DORA

Entreprise	Audit et diagnostics à DORA	Conceptions stratégiques et procédures et impacts DORA	Gestion des risques	Tests	Gestion de la sécurité des fournisseurs de services informatiques	Email
OWN	Oui	Oui	Oui	Oui	Oui	contact@own.security
RUBYCAT					Oui	commercial@rubycat.eu
SEC-IT SOLUTIONS	Oui	Oui	Oui	Oui	Oui	contact@sec-it.fr
Sekoia.io SAS			Oui			contact@sekoia.io
SHADLINE	Oui	Oui	Oui	Oui		contact@shadline.com
SyLing	Oui	Oui	Oui	Oui	Oui	malena.moreira@sylink.com
SYNACKTIV	Oui			Oui		contact@synacktiv.com
Synetis	Oui	Oui	Oui	Oui	Oui	contact@synetis.com
SYSTANCIA			Oui		Oui	marketing@systancia.com
WALLACK	Oui	Oui	Oui	Oui	Oui	contact@wallack.fr
YesWeHack			Oui	Oui		contact@yeswehack.com

Réponses auto déclaratives

Catégories	Entreprises
ANTI FRAUD	IPCYB
APPLICATION SECURITY	Acceis, Neverhack, Quarkslab, Synacktiv, Sylink, Wing IT, Yeswehack
AUTRES : FORMATION, DROIT, COMMUNICATION	Ascent, Avoxa, Cabinet d'avocats Eon-Jaguin, Garnault et associés, Perses communication, Withlaw
CLOUD SECURITY	Foliateam
CRISIS MANAGEMENT	Alcyconie, Easylience, Shadline
DATA SECURITY	Daspren, Glimps, Hogo
GOUVERNANCE & RISK COMPLIANCE	Akerva, Amn Brains, CEEBEX, Formind, Imineti by Niji, Mipih SIB, Ornisec, Ovalt
IDENTITY & ACCESS MANAGEMENT	Rubycat, Systancia, Wallix
INCIDENT RESPONSE	Malizen, Nybble security, Sekoia
IOT SECURITY	Lootus, Secure-IC
NETWORK SECURITY	CT Square, Cailabs, Gatewatcher, Geoide, Nomios
PRIVACY AWARENESS	Calidra, Cy Mind, Riot, Treebal green
SIGNATURE & KYC	A3bc, IDnow
SURVEILLANCE	Wan pulse
THREAT & ACTOR INTELLIGENCE	Erium, Synetis
TOUTES CATÉGORIES	Amossys, Apixit, Bloo Conseil, Claranet, Cybermyne, FairTrust, Kereval, OCI, Own, Sec IT, Wallack
VULNÉRABILITÉS	Anozr way, Sekost
WATERMARKING	Imatag

Réponses auto déclaratives

Accédez au site de Rennes Business pour découvrir la richesse de l'écosystème : https://www.entreprendre-rennes.fr/article/cybersecurite/

Découvrez le catalogue des formations cyber sur Rennes Métropole : https://www.entreprendre-rennes.fr/voy_content/uploads/2024/11/Catalogue-formations-f

Vous souhaitez vous implanter sur Rennes, vous faire connaître ou vous impliquer dans la dynamique collective cyber rennaise ? N'hésitez pas à contactez Paul-André Pincemin, délégué à la cybersécurité et aux restructurations militaires à Rennes Ville & Métropole, à l'adresse pa.pincemin@rennesmetropole.fr

Réalisation www.goodinfo.eu