5e édition

GUIDE
2021-2022

CYBERSÉCURITÉ

French Directory

Télétravail, Ransomware, Gestion de crise : êtes vous prêts ?

Les solutions et les services

650 éditeurs, conseils, prestataires, distributeurs, formateurs

www.solutions-numériques.com/securite
Prix : 30€ - ISSN : 2606-2860

Hors-Série SOLUTIONS numériques

En partenariat avec numeum

DELL Technologies

intel. Innovation Built-In

DÉCOUVREZ DELL EMC POWERPROTECT CYBER RECOVERY

ASSUREZ VOTRE CYBER RÉSILIENCE DÈS AUJOURD'HUI

Réduisez les risques pour votre organisation grâce à la dernière solution en matière de protection des données contre les cyberattaques.

Une cyberattaque se produit toutes les 11 secondes.

69 % des décideurs IT ne sont pas convaincus de récupérer toutes les données en cas de cyberattaque.

PROTÉGER VOS DONNÉES

IDENTIFIER LES SIGNES D'ALTÉRATION

ACCÉLÉRER LA RÉCUPÉRATION DE VOS DONNÉES

SOMMAIRE

Introduction

- **Editorial : La Cybersécurité, une affaire d'États** 4
- **Guillaume Poupard, ANSSI :** La cyber en France : Pour la construction d'un écosystème dynamique 6

Le visa de sécurité ANSSI : toutes les clés pour comprendre 8

- **Tribunes**

Cybermalveillance.gouv.fr - La cybersécurité doit intégrer la réalité de l'utilisateur 10

Cigref - Face à l'insécurité numérique, changeons de paradigme 12

Cesin - Et si on osait la sécurité logicielle ? 14

Numeum - La cybersécurité, un levier d'avenir positif et non un mal nécessaire ! 16

Clusif - La sécurité est désormais un bien commun 17

Hexatrust - Pourquoi privilégier les solutions de cybersécurité innovantes, de proximité et de confiance ? 18

AFCDP - Baromètre trimestriel : la voix des DPO 20

Les tendances et la cybersécurité

- Télétravail : la nouvelle frontière de l'accès distant 22
- Gestion de crise cyber : se préparer au pire ! 24
- Supply Chain Attack 28
- Ces multiples vulnérabilités qui menacent le SI 32
- La Cyber-assurance à l'heure du ransomware 34

Les acteurs de la Cybersécurité : Qui fait quoi ?

Editeurs, Conseils, Intégrateurs, formateurs etc. : présentation détaillée de 81 spécialistes incontournables 35

Fiches alphabétiques des entreprises spécialisées

- Fournisseurs de solutions : 160
- Prestataires de services : 173
- Formation 184
- Hébergeurs 185
- Avocats spécialisés 186
- Consultants indépendants 186
- Distributeurs 187

→

SOMMAIRE

→

Panorama : tableaux comparatifs

- Tableau des fournisseurs de Solutions 190
- Tableau des prestataires de services 204

Comprendre la technologie

Définitions : buzzword 219

IAM : La gestion des identités et accès au cœur de l'approche Zéro Trust 220

Threat Intelligence 222

La réponse à incident 225

Protection du poste de travail 226

Protection des terminaux mobiles 227

Protection de la donnée 228

Protection applicative / Audit d'architecture 229

Soc 230

Tableaux de bord/Siem 231

L'Ecosystème

Les organismes de référence :

ANSSI, AFCDP, CAMPUS CYBER, CESIN, CIGREF, CLUSIF, CNIL, CYBERMALVEILLANCE.GOUV.FR, HEXATRUST, NUMEUM

Hors Série de Solutions Numériques - Directeur de publication & rédaction : Jean Kaminsky - Conseiller de la rédaction : Jérôme Saiz - redaction@solutions- numériques.com- Publicité tel. : 01 41 77 16 03 - publicité@solutions- numériques.com - Maquette : réalisation, Pierre Sandré - Siège social : K-Now SAS, 21 rue de Fécamp 75012 Paris - Impression : Mordacq, 62120 Aire-sur-la-Lys - Dépot légal à parution

L'éditeur ne peut être tenu responsable d'éventuelles erreurs ou omissions.
Le reproduction partielle ou totale du contenu est interdite sauf autorisation expresse de l'éditeur.
Copyrigt : reproduction interdite

EDITORIAL

La Cybersécurité, une affaire d'États

Tous responsables. En 2021, la cybersécurité a été pour la première fois sous le feu de tous les projecteurs. Des spectaculaires attaques l'ont révélée au grand public.

Le risque cyber était, il y peu, encore une affaire de spécialistes. Les dirigeants d'entreprise il n'y a pas si longtemps ont pris conscience qu'il n'était plus du seul ressort de leur direction informatique ou de leur RSSI, pour les grandes entreprises, mais aussi de leur responsabilité. Le risque des sanctions de la Cnil en était une des causes. En 2021, c'est au niveau des gouvernements, et même des chefs d'états que cette prise de conscience, cette prise de responsabilité est assumée. La géopolitique s'est invitée. Les attaques sont si sophistiquées que des gouvernements étrangers sont mis en cause.

L'année 2021 aura été marquée par une explosion des ransomwares+ 64%, selon Barracuda Networks. L'exploitation de vulnérabilités des applications Orion de Solarwinds et Exchange de Microsoft ont révélé le piratage de dizaines de milliers d'entreprises et d'administrations. Ce type d'attaque utilisant la « supply-chain » logicielle, permet une dissémination du malware, au travers du cloud. La révélation de l'espionnage de responsables au plus haut niveau, par le logiciel Pegasus a également marqué les esprits.

En mai, aux Etats Unis, la cyberattaque contre Colonial Pipeline a été la goutte (de pétrole) de trop. Ce n'était pas Pearl Harbour ou le 11 septembre, mais la prise de conscience des risques cyber-terroristes. Fraîchement élu, Joe Biden a fait de la cybersécurité une préoccupation majeure de son administration.

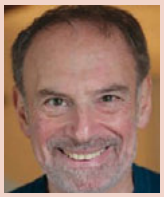
Il fait publier en mai 2021 un décret pour renforcer de façon drastique les exigences en cybersécurité des agences américaines et de leurs fournisseurs. Il annonce un plan de 20 milliards de dollars pour la sécurisation des systèmes énergétiques. Il organise un sommet avec les leaders du numérique, où notamment Microsoft s'engage à investir 20 milliards de dollars dans le domaine de la cyber-sécurité, et Google 10 milliards.

En juin, Joe Biden rencontre Vladimir Poutine et déclare à la presse : *« J'ai demandé de limiter le développement d'armements trop sophistiqués, comme des attaques de cybersécurité, pour réduire le risque de guerre accidentelle. Des infrastructures critiques devraient être préservées. J'ai donc remis une liste de 16 domaines, comme les systèmes d'eau et d'énergie. Les pays responsables doivent agir contre les criminels qui lancent des rançongiciels depuis leur territoire ».*

La France a vu des villes et des hôpitaux paralysés par des cyberattaques. Emmanuel Macron a réagi à la menace et annonce en février une stratégie nationale de cybersécurité, qui mobilise 1 milliard d'euros, dont 720 millions d'euros de financements publics*.

Il a été à l'initiative du Campus Cyber qui nait cet automne sur 26 000 m2 à la Défense (la bien nommée), concentrant sur un site unique une grande partie des industries et des recherches et des compétences nationales, et permettant notamment de mutualiser les données de cybersécurité entre les différents acteurs.

L'objectif de cette stratégie nationale est également économique et industriel : développer un écosystème national. L'Europe a perdu les batailles de l'IT et du Cloud, face aux Gafa. Positionner la France comme un leader en cybersécurité reste possible. Les objectifs fixés pour 2025 : augmenter le chiffre d'affaires de la filière à 25Md€ (contre 7,3€ en 2019), doubler la part des exportations, doubler les emplois, et faire émerger trois licornes françaises.



Réussir - en même temps - à protéger le pays et développer la filière serait un beau coup double.

Jean Kaminsky - *Editeur*

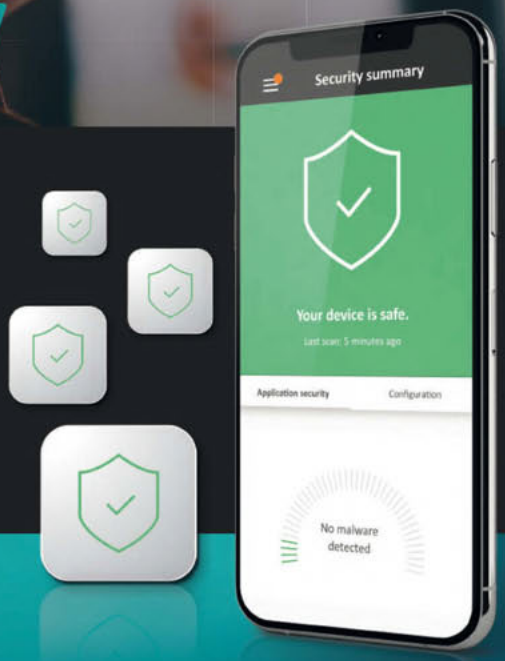
Lire aussi : *https://www.solutions-numeriques.com/strategie-nationale-en-matiere-de-cybersecurite-la-nation-va-consentir-un-investissement-important-emmanuel-macron/*

** https://www.ssi.gouv.fr/actualite/cybersecurite-faire-face-a-la-menace-la-strategie-francaise/*

SÉCURITÉ MOBILE

Protégez vos **terminaux** et **applications mobiles** avec **Pradeo Security**

- Mobile Threat Defense
- Secure Private Store
- Mobile Application Security Testing
- Mobile Application Shielding
- In-App Threat Defense



RÉCOMPENSÉ PAR LE PRIX
Global mobile security enabling technology leadership 2021
DE FROST & SULLIVAN

pradeo
MOBILE SECURITY EXPERT

Tous droits réservés - Pradeo - 2021

Par Guillaume Poupard
Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

La cyber en France : pour la construction d'un écosystème dynamique

Du particulier aux grandes administrations, en passant par les TPE/PME et les collectivités locales, la cybersécurité est désormais un enjeu majeur. La menace, criminelle, stratégique, augmente et les besoins en solutions performantes et éprouvées se multiplient.

Si l'ANSSI joue un rôle central, c'est tout l'écosystème de cybersécurité français qui doit se mobiliser pour répondre à ces défis. Des avancées encourageantes sont à noter mais l'effort doit perdurer !

Nous comptons en effet plus que jamais sur les fournisseurs de produits et prestataires de services de cybersécurité pour continuer à offrir des solutions de qualité. C'est d'ailleurs la raison pour laquelle nous valorisons ces solutions au travers des Visas de sécurité à l'issue d'un processus d'évaluation exigeant et que nous encourageons la construction du Campus Cyber pour dynamiser cet écosystème autour de projets ambitieux.

Visa de sécurité : du nouveau pour les prestataires de services

En matière de cybersécurité, la confiance dans les prestataires de services, auxquels on confie ses données, voire une partie de son système d'information, est primordiale. Aussi, la qualité des services offerts par l'écosystème cyber doit demeurer une préoccupation forte. L'ANSSI continue donc d'étoffer les catégories de Visas de sécurité pour répondre au mieux aux attentes des utilisateurs et des acteurs cyber.

Tout d'abord, l'agence a élaboré un nouveau schéma d'évaluation pour les **Prestataires de vérification d'identité à distance (PVID).** Il permet avec l'aide des centres d'évaluation habilités de délivrer un Visa de sécurité ANSSI pour attester de leur capacité à assurer la vérification d'identité à distance de manière fiable et sécurisée. Pour créer ce schéma, l'appui de l'écosystème français de la biométrie : industriels, centres d'évaluation et centres de recherche, a été extrêmement précieux. Ce schéma est déjà un succès : plusieurs industriels ont ainsi déposé des demandes d'évaluation.

Par ailleurs, pour permettre notamment aux petites structures de s'appuyer sur des prestataires de confiance pour le maintien en condition de sécurité de leurs systèmes d'information, la définition du référentiel pour les **Prestataires d'administration et de mainte-**

nance sécurisée (PAMS) progresse. Une phase expérimentale d'évaluation est en cours et permettra une adaptation du référentiel début 2022 pour coller au mieux aux besoins et à l'état de l'art. Les premiers qualifiés pourraient apparaître vers les Assises 2022 : à suivre !

Dans la même lignée, et conscients du besoin des organisations d'être accompagnées par des prestataires compétents dans leur démarche de cybersécurité, le référentiel pour les **Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS)** reste une priorité.

C'est tout l'écosystème de cybersécurité français qui doit se mobiliser pour répondre à ces défis.

Ces prestataires apporteront un soutien déterminant en matière de gestion des risques cyber et de protection des systèmes d'information. La phase expérimentale, qui nous permettra de vérifier l'applicabilité du référentiel, vient ainsi de démarrer.

Enfin, le référentiel **SecNumCloud** évolue afin de répondre aux exigences de sécurité des données et devenir le label cloud de confiance, en phase avec la stratégie Cloud de l'État. Si les solutions ayant déjà obtenu le Visa de sécurité SecNumCloud demeurent des prestations de confiance, le référentiel consolidé permettra d'attester de la protection des données face aux risques d'accès au moyen de réglementations extracommunautaires.

Des travaux similaires ont actuellement lieu au niveau européen dans le cadre de la mise en place de la certification européenne.

Nous sommes en effet fiers que la France soit l'un des pays les plus actifs dans la création de schémas de certification à l'échelle européenne. Son expertise de longue date porte aujourd'hui ses fruits. Beaucoup de schémas d'évaluation français ont ainsi déjà fait leurs preuves, tout comme nos centres d'évaluation. Le schéma *EU Common Criteria*, qui couvre la certification de sécurité de produits selon les Critères Communs, est aujourd'hui le plus avancé et devrait être validé très prochainement. Le schéma *EU Cloud Services* suivra.

Le Campus Cyber : un grand projet qui se concrétise

La première moitié de 2022 verra l'ouverture du Campus Cyber qui ambitionne d'être un « lieu totem » de la cybersécurité réunissant les acteurs principaux de notre écosystème autour de quatre thématiques : la formation pour l'amélioration des compétences, l'innovation pour le soutien de projets, l'opération pour la maîtrise du risque numérique et l'animation pour la dynamisation du secteur et le développement de synergies.

Pour l'ANSSI, le Campus Cyber est une formidable opportunité afin de développer son accompagnement de l'industrie cyber français et construire ensemble les solutions cyber de demain. Le Visa de sécurité, levier crucial, sera ainsi renforcé par de nombreuses actions pour animer et dynamiser cet écosystème performant et plein d'avenir. Nous avons hâte de vous y retrouver !

Le Visa de sécurité ANSSI, c'est :

- 246 Visas de sécurité remis en 2020
- Plus de 90 acteurs détenteurs d'une qualification
- Près de 100 certifications délivrées chaque année
- 15 centres d'évaluation/CESTI agréés

Pour en savoir plus sur le Visa de sécurité, rendez-vous sur **www.ssi.gouv.fr/visa-de-securite/** et consultez :

- le film pédagogique Visa de sécurité ;
- la brochure qualification ;
- la brochure certification.

Le Visa de sécurité ANSSI : toutes les clés pour comprendre !

A quoi sert le Visa de sécurité ?

Le Visa de sécurité que délivre l'ANSSI permet d'**identifier en un clin d'œil** les solutions ayant obtenu une certification ou une qualification, à l'issue d'une évaluation réalisée par des laboratoires agréés selon une **méthodologie rigoureuse et éprouvée**. Il permet également de repérer aisément ces laboratoires agréés qui accompagnent l'agence dans la délivrance du Visa de sécurité ! Le Visa de sécurité est l'expression directe de la certification ou de la qualification obtenue par le produit/service et de l'agrément obtenu par le laboratoire. Il signifie : « **cette solution a été évaluée selon des normes et processus reconnus par l'ANSSI**. »

Le Visa de sécurité regroupe plusieurs processus : comment les distinguer ?

Lorsqu'une entreprise utilise le Visa de sécurité ANSSI, elle doit préciser à côté pour quelle offre il a été obtenu et via quel type d'évaluation, ainsi que le niveau atteint ! Le Visa de sécurité n'est jamais délivré à une entreprise pour l'ensemble de ses offres.

A retenir : le Visa de sécurité ANSSI, gage de robustesse, ne dispense pas de vérifier ce qui a été évalué ! **Tous les détails (évaluation menée et conditions d'utilisation) sont disponibles** sur les fiches des différents produits et services sur le site internet de l'agence.

La certification de sécurité et la qualification sont les deux processus permettant à l'ANSSI d'évaluer des produits et services. Le choix de l'un ou l'autre se fait au regard des besoins des clients de l'entreprise qui souhaite faire évaluer son offre. Ils répondent à des besoins et des objectifs différents :
voir tableau ci-dessous

La certification de sécurité	La qualification
• La certification peut concerner tous les types de produits qui intègrent des fonctions de sécurité. • La certification est une évaluation de la robustesse aux attaques d'une version spécifique d'un produit, à un instant « T », selon l'état de l'art des attaques à cet instant. • **Via la certification, l'ANSSI certifie que la solution répond bien au niveau de sécurité vis-à-vis duquel elle a été évaluée**, mais ne présume pas du niveau de confiance qui peut être accordé à la solution sur les aspects non-évalués ou à l'entreprise qui la propose.	• La qualification concerne principalement les produits et les services qui représentent un intérêt pour la sécurité des administrations et opérateurs régulés : Organismes d'importance vitale (OIV), Opérateurs de services essentiels (OSE), etc. • La qualification permet de répondre à des exigences règlementaires pour la Loi de programmation militaire (LPM), le Référentiel général de sécurité (RGS) et le règlement eIDAS. • **Via la qualification, l'ANSSI atteste de l'adéquation des solutions aux besoins identifiés** et de la capacité du fournisseur ou prestataire à respecter sur le long-terme un certain nombre d'engagements pris auprès de l'ANSSI.

En quelques mots, qu'est-ce que la certification de sécurité ?

La certification est la reconnaissance par l'État de la robustesse d'un produit, éprouvée à travers une évaluation par un tiers dont la compétence est garantie par l'ANSSI. Elle est établie sur la base d'un contexte d'usage et d'objectifs de sécurité définis par un commanditaire. Une certification est assortie d'un niveau d'assurance, qui correspond à la profondeur plus ou moins importante de l'analyse effectuée par l'évaluateur, selon les objectifs de sécurité du commanditaire.

Il en existe 2 types : la certification Critères Communs (CC), standard internationalement reconnu avec plusieurs niveaux d'assurance dans la sécurité du produit, et la Certification de Sécurité de Premier Niveau (CSPN) qui est l'alternative pour estimer la résistance d'un produit en temps et ressources contraints. Ces certifications ont des durées de validité limitées dans le temps.

En quelques mots, qu'est-ce que la qualification ?

La qualification est la recommandation par l'État d'un produit ou service pour un usage donné et pour une période définie. Elle atteste à la fois de la qualité de la solution, d'un ensemble d'engagements pris par le fournisseur vis-à-vis de l'ANSSI, et de la pertinence de la solution au regard d'un besoin identifié par l'État : le sien, celui d'un Organisme d'Importance Vitale (OIV) ou celui de tout autre acteur identifié dans un cadre réglementaire. Ces solutions sont toutefois disponibles pour tous les types d'utilisateurs qui pourraient en avoir le besoin !

Pour les produits, il s'agit de s'assurer de leur robustesse en éprouvant leur capacité à résister à des attaques selon un contexte d'emploi et un niveau de menace définis. Cette évaluation s'appuie sur une certification et est graduée : qualification élémentaire, standard ou renforcée. Pour les services, il s'agit d'évaluer la compétence du prestataire afin de valider son aptitude à identifier et maîtriser les menaces et risques liés aux exigences inscrites dans les référentiels métiers. Dans les deux cas, l'ANSSI éprouve la capacité du fournisseur à respecter sur le long-terme un ensemble d'engagements pris auprès de l'agence sur la confidentialité et la protection des données, mais aussi sur la correction des vulnérabilités, le maintien des compétences, etc.

Est-il compliqué d'obtenir le Visa de sécurité ANSSI ?

Obtenir le Visa de sécurité n'est pas aisé : les évaluations sont longues et coûteuses. La durée ainsi que le coût du processus dépendent du type de produit/service évalué, de la maturité de la solution présentée, des moyens de sécurité déjà mis en place dans l'entreprise, etc. Chaque année, l'ANSSI organise une cérémonie de remise du Visa de sécurité pour distinguer les offres qui ont obtenu un nouveau Visa de sécurité depuis la précédente cérémonie. Les Visas précédemment obtenus et en cours de validité restent d'actualité !

Que va apporter la certification européenne ?

L'objectif est de créer un cadre harmonisé de certification à l'échelle européenne. Lorsqu'un schéma européen apparaîtra, il prendra le pas sur le schéma national existant. Le cadre de certification européen proposera 3 niveaux : basique, substantiel et élevé. Chacun répondra à un niveau d'assurance différent dans la sécurité du produit ou service délivré.

Est-ce que l'ANSSI délivre d'autres distinctions ?

Le terme de labellisation est utilisé par l'ANSSI pour désigner les attestations qu'elle délivre hors du cadre du Visa de sécurité. Ces labellisations attestent de la conformité à un cahier des charges, et elles n'impliquent pas l'intervention d'une entité indépendante autre que l'ANSSI pour valider cette conformité. Les labels délivrés par l'ANSSI à ce jour sont le label Ebios RM et le label SecNumEdu.

Comment me renseigner sur le Visa de sécurité ?

Plus d'informations sont disponibles sur le site internet de l'ANSSI à cette adresse :
www.ssi.gouv.fr/visa-de-securite/

La cybersécurité doit intégrer la réalité de l'utilisateur

Par Jerome NOTIN,
Directeur général du GIP ACYMA
cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Par son positionnement spécifique, Cybermalveillance.gouv.fr est un poste d'observation original et unique de la réalité de l'utilisateur. Cette observation tend à démontrer qu'il peut y avoir un fossé de compréhension et d'acceptation entre l'écosystème de la cybersécurité et les utilisateurs qu'il cherche à atteindre.

L'utilisateur ce grand méconnu et incompris

Qu'il soit dirigeant d'entreprise ou collaborateur, l'utilisateur a une appréhension du numérique et de la cybersécurité au sein de son entreprise souvent très proche de son utilisation à titre personnel. Le numérique - et a fortiori sa sécurité - demeure encore un monde obscur voire confus pour une grande majorité d'utilisateurs qui se limitent souvent à essayer d'utiliser au mieux les multiples services dont ils ont besoin, sans intégrer les contraintes liées à la sécurité.

Si on devait comparer au monde automobile, lorsqu'un conducteur prend sa voiture, sa première pensée ne va généralement pas au risque d'accident. Pour démarrer son véhicule, il n'aura qu'un nombre minimal d'opérations à réaliser comme s'installer confortablement, boucler sa ceinture et lancer le démarreur. Durant son trajet, il fera confiance aux dispositifs de sécurité de son véhicule pour le protéger au mieux en cas d'accident et respectera le code de la route, code qui vise à se protéger mutuellement contre les défaillances involontaires, techniques ou humaines. Mais il ne protège pas contre les actes malveillants, heureusement fort rares dans la vie « réelle », car on n'est que très peu confronté à des acteurs qui à chaque coin de rue veulent vous voler ou même vous détruire.

Si on revient au monde numérique, la comparaison s'arrête là. On peut en effet considérer qu'à chaque instant, des cybercriminels vont tenter de profiter de nos usages numériques pour commettre leurs méfaits et nous faire dévier de notre trajectoire. Il faut donc que l'utilisateur ait conscience des dangers et reste perpétuellement en alerte contre les risques de cybermalveillance.

Sensibiliser mais aussi éduquer et accompagner

Une mesure de sécurité n'est acceptée que si elle est, par principe, acceptable : c'est-à-dire, comprise, admise et réaliste. Cette acceptation passe en premier lieu par la sensibilisation aux risques. Mais la sensibilisation ne suffit pas. Connaître un risque est une chose, savoir s'en protéger en est une autre.

Les efforts doivent donc également porter sur l'éducation. L'éducation des plus jeunes, bien évidemment, car le cadre scolaire le permet dès le plus jeune âge et qu'ils sont sans doute la cible la plus facile à atteindre. Mais les adultes sont également des publics vulnérables à adresser : ils ont pour la plupart découvert le numérique de manière empirique et peuvent se retrouver un peu perdus pour se sécuriser. Les solutions disponibles passent trop souvent par une démarche volontaire de l'utilisateur qui ne sait pas par où commencer. Il faut donc trouver des moyens d'aller au-devant de ces publics, que ce soit dans un cadre professionnel, associatif, de service public.

Mais, même éduqués, les utilisateurs peuvent avoir besoin d'aide pratique pour faire face aux menaces ou mettre en œuvre leurs dispositifs de sécurité. Tant les particuliers que les entreprises ont aujourd'hui besoin d'un accompagnement adapté et « accessible » pour assurer leur cybersécurité. Si pour le particulier, des démarches associatives ou de services publics d'accompagnement doivent être envisagées, pour les entreprises, le coût de cet accompagnement doit être « acceptable », ce qui est encore malheureusement peu souvent le cas.

Pour que notre « monde numérique » soit un

monde de confiance et non un monde de fractures sociales, générationnelles ou même concurrentielles, la sensibilisation aux risques, l'éducation et l'accompagnement sont des leviers déterminants à considérer.

Amener la cybersécurité à la portée de l'utilisateur

Pour reprendre notre métaphore du conducteur, comment pourrait-il accepter que pour utiliser son véhicule il doive entrer - et retenir - un mot de passe de 12 caractères aléatoires, un autre pour démarrer l'autoradio, encore un autre pour ouvrir le coffre… ? Que pour s'assurer de pouvoir conduire en sécurité il doive avant de démarrer faire la mise à jour de son ordinateur de bord et de son ABS mais aussi s'assurer que leurs paramètres de sécurité sont bien cochés au fin fond de menus abscons ? Que pour pouvoir utiliser à nouveau son véhicule en cas de problème, il doive en faire des sauvegardes régulières ?
C'est pourtant ce que l'on demande aujourd'hui à l'utilisateur d'outils numériques pour assurer sa cybersécurité. Son ordinateur, sa tablette, son smartphone, son serveur domestique ou professionnel et les innombrables services auxquels ils permettent d'accéder ont chacun leurs « règles » et leur jargon spécifiques.
Considérer par exemple que « authentification à double facteur » puisse être réellement parlant pour le commun des mortels est certainement une gageure. D'autant qu'il y a quasiment autant d'appellations de cette option pourtant primordiale de cybersécurité que de services qui la proposent. Et encore faut-il savoir où la trouver pour l'activer ! Et que dire des règles de gestion des mots de passe qui sont différentes d'un service à l'autre que ce soit dans leur longueur ou leur composition ?
L'écosystème a sans doute pensé qu'il pourrait faire venir l'utilisateur à la cybersécurité, or, il vaut sans doute mieux faire venir la cybersécurité à l'utilisateur.
Éditeurs, constructeurs, opérateurs, intégrateurs, prestataires, services publics : l'ensemble des acteurs de l'écosystème de la cybersécurité doit aujourd'hui se fédérer pour apporter à l'utilisateur une cohérence et une simplification, voire une normalisation et une transparence, qui aujourd'hui font défaut, au risque de continuer à être rejeté pour son manque d'accessibilité. ■

Retrouvez le guide Cybersécurité en ligne

- Téléchargez le guide au format e-book et PDF
- Consultez les fiches des entreprises sur l'annuaire de la sécurité

Solutions-numeriques.com/securite/annuaire-cybersecurite

Face à l'insécurité numérique, changeons de paradigme !

Par Jean-Claude LAROCHE, DSI du groupe Enedis
Vice-président du Cigref

Dans le contexte de dégradation croissante de la sécurité dans l'espace numérique, le Cigref en appelle à un changement de paradigme et propose une doctrine nouvelle.

L'insécurité dans l'espace numérique n'est plus, à l'évidence, un sujet marginal, mais bien l'un des principaux risques qui pèsent sur le fonctionnement de nos sociétés contemporaines. Nous avons observé, avec une préoccupation croissante, l'augmentation quasi exponentielle des cyberattaques au cours des 18 derniers mois. Plusieurs réactions marquantes illustrent la progression de ce phénomène inquiétant. Le 19 février 2020, le Comité européen des risques systémiques, présidé par Madame Christine Lagarde, publiait un rapport sur les cyberattaques, définies comme susceptibles d'avoir de "graves conséquences négatives pour l'économie réelle". En avril 2021, le président de la FED, Jérôme Powell, confiait que la cybercriminalité constituait désormais le principal risque pour l'économie américaine, et qu'il le redoutait davantage encore qu'une crise similaire à celle de 2008. Lors du sommet de l'OTAN du 14 juin 2021, les chefs d'État et de Gouvernement des 30 membres de l'alliance ont décidé d'étendre à l'espace numérique la portée de l'article 5 de la Charte atlantique en cas de cyberattaque contre l'un d'eux.

Aucun autre secteur d'activité que celui du numérique n'accepterait de se développer dans un tel contexte d'insécurité juridique face à la cybermenace, de faiblesse du droit applicable, d'impunité des organisations criminelles qui y déploient leurs exactions. La capacité des cybercriminels croît désormais plus rapidement que la capacité de leurs victimes à se protéger. Ils ont professionnalisé, industrialisé et mondialisé leurs activités mafieuses, dans un contexte trouble de porosité ou d'adhérence avec les services spécialisés d'États qui ne partagent pas nos valeurs démocratiques. Aujourd'hui, ce sont les rançongiciels qui concentrent l'attention de la plupart des acteurs de la cybersécurité et des dirigeants. Mais les entreprises et les administrations publiques sont également confrontées à d'autres risques comme l'espionnage et le vol de données sensibles, moins visibles sans doute, mais qu'il convient de ne pas sous-estimer.

Nous savons les efforts que l'État consent déjà pour lutter contre ce fléau, et les moyens en progression constante dont l'Agence nationale de la sécurité des systèmes d'information dispose pour assurer ses missions. Mais dans le contexte de numérisation croissante des activités de la société et de son économie, cet effort n'est, hélas, pas suffisant. Les entreprises et les administrations publiques consacrent des ressources humaines, techniques et financières toujours plus élevées à la protection de leurs systèmes d'information. Dans cette dialectique

> ***« Aucun autre secteur d'activité que celui du numérique n'accepterait de se développer dans un tel contexte d'insécurité juridique face à la cybermenace, de faiblesse du droit applicable... »***

entre l'agresseur et l'agressé, entre celui qui attaque et celui qui doit se défendre, c'est toujours le criminel, parce qu'il choisit son arme et décide du moment et de l'endroit où il va frapper, qui conserve l'avantage. Il appartient pourtant aux États, et c'est une responsabilité au cœur de leur souveraineté, d'assurer la sécurité des personnes et des biens dans l'espace numérique, et des activités qui s'y déploient, au même titre que dans l'espace physique.

C'est la raison pour laquelle le Cigref propose une doctrine écosystémique de la sécurité numérique, impliquant les utilisateurs et les fournisseurs de produits et services numériques ainsi que le régulateur. Elle s'articule autour de quatre piliers. Le premier concerne la cybersécurité, dans laquelle il convient de renforcer les efforts, et, à cet égard, le plan d'accélération cyber d'un milliard d'euros présenté par le Gouvernement en février 2021 est le bienvenu. Le deuxième pilier porte sur la lutte contre la cybercriminalité et l'adaptation à celle-ci des moyens de police et de justice, lesquels souffrent dans ce domaine d'un réel retard. Le troisième relève d'une mission éminemment régalienne, la cyberdéfense en profondeur, pour identifier et neutraliser les cyberattaquants inaccessibles par d'autres moyens. Enfin, le quatrième pilier concerne la régulation, a minima à l'échelle européenne, de la sécurité par conception et la sécurité d'exploitation, des produits et services numériques, sur tout leur cycle de vie.

Le Cigref entend contribuer tout particulièrement au développement de ce quatrième pilier de la sécurité numérique. Les pratiques généralement constatées, notamment chez les éditeurs de logiciels, ne sont pas propices au renforcement de la sécurité globale des systèmes d'information. L'industrie du numérique est sans doute la seule en Europe à ne pas faire l'objet de normes minimales de sécurité. Le contexte de dégradation de la sécurité dans l'espace numérique, et de vulnérabilités croissantes des produits et services numériques, appelle un changement de paradigme et des régulations nouvelles, de nature plus systémique. Dans cette démarche, nous apportons notre soutien au rapport publié en février 2021 par l'OCDE, relatif au renforcement de la sécurité des produits et services numériques. Ce rapport propose une large « boîte à outils » des politiques publiques à mettre en œuvre pour réguler la sécurité numérique, qui a été présenté lors de notre webinaire du 5 juillet 2021, au côté d'interventions de l'ANSSI, de numeum et de l'Appel de Paris.

Soyons bien conscients que, si l'on ne modifie pas collectivement les paradigmes de la sécurité dans l'espace numérique, il est fort probable que les désordres ne cessent de croître en le vouant au chaos à l'horizon d'une dizaine d'années. Comme l'écrivait Lacordaire : « *c'est la liberté qui opprime et la loi qui affranchit* ». Aujourd'hui, l'espace numérique est un bien commun insuffisamment régulé, et les libertés qui s'y déploient servent à l'évidence les intérêts des cybercriminels de tout poil. Nous ne pouvons nous y résoudre. ■

L'actu, les dossiers de la
CYBERSÉCURITÉ
www.solutions-numériques.com/securite
Abonnez-vous à la **Newsletter** *du lundi*

Et si on osait la sécurité logicielle ?

Alain Bouillé, Délégué Général du CESIN

L'année 2021 ne nous aura pas épargnés de cyber-attaques plus ou moins ciblées avec les ravages que l'on sait pour les entreprises et les collectivités, d'actes plus sophistiqués souvent téléguidés par des états, la cyber-guerre est à nos portes nous dit-on. A cela s'ajoutent aussi des faits de cyber espionnage de plus en plus répandus, rendus sans aucun doute beaucoup plus simples par l'usage massif du cloud, avec ce qu'il comporte encore de mauvaises pratiques, par manque d'expertise, entraînant une surexposition des données sensibles des entreprises utilisatrices.

Continuer à sécuriser le périmétrique, tenter de sécuriser les usages du cloud, officiels ou non, blinder la sécurité des Endpoints, forcer le MFA, gérer les multiples alertes collectées par les services de SOC externalisés ou non, gérer des crises à répétition, tenter de recourir à la cyber-assurance quand les assureurs ne mettent pas les barres trop haut, tel est l'infernal agenda du RSSI 2021 les conduisant pour certains à des situations de surmenage voire de burn-out. Le CESIN publie en cette fin d'année une étude éloquente en la matière.

Mais si on prenait le temps de s'interroger sur la cause principale de ce marasme ? Pour qu'une attaque réussisse, il faut une conjonction de plusieurs phénomènes mais l'exploitation de vulnérabilités logicielles ou matérielles reste bel et bien, le plus souvent, le point de départ de tous ces maux. Or, les chiffres le montrent, on est dans une courbe inflationniste en matière de vulnérabilités. Si à grand renfort de briques de sécurité empilées depuis des années et de stricts processus de gestion, on a réussi tant bien que mal à gérer les vulnérabilités dites d'infrastructure, la situation concernant la qualité des codes produits et celle de l'intégrité des solutions logicielles s'aggrave de jour en jour, cette dernière donnant lieu à des attaques dites « de la supply chain ». Ce phénomène trouve ses origines dans de multiples causes mais force est de constater que le RSSI est désormais obligé de faire des choix dans la gestion de ses rustines car il ne peut plus boucher tous les trous de la grande piscine gonflable des données de l'entreprise …

Des facteurs aggravants

D'aucuns affirment que ça n'est pas la sécurité logicielle qui se dégrade mais le fait que les hackers éthiques ou non fouillent de plus en plus dans les logiciels pour y trouver la porte d'entrée idéale pour y pénétrer et extraire des données ou pour y insérer un code malveillant. Quoi qu'il en soit, plusieurs facteurs aggravants sont survenus au cours de ces dernières années :

• Tout d'abord, le recours massif au cloud et particulièrement celui du mode SAaS implique que tout le monde utilise à un instant T les mêmes solutions sans pour autant avoir la main sur leur sécurisation en cas de publication de failles importantes dont le traitement reste à la main de l'éditeur.

• Dans la kyrielle des petites solutions SaaS, beaucoup sont développées à la va-vite, mal sécurisées, et utilisées par les entreprises, y compris les plus grandes, à la marge du SI traditionnel pour tout ce qui n'est pas « core business ». Or c'est souvent-là que l'on retrouve nombre de données sensibles, souvent à caractère personnel, dont la fuite et la divulgation peuvent avoir des conséquences dramatiques pour l'entreprise.

• L'apparition du DEVOPS avec le fameux argument de l'agilité n'a pas arrangé les choses. Mais où est l'agilité quand ces développements sont confiés à des prestataires, des développeurs indépendants, voire des étudiants, qui ont souvent peu de conscience et de connaissance en matière de sécurité des développements et qu'il faut à la fin remettre une

couche de sécurité avant la mise en prod ? On a bien entendu très vite inventé le DevSecOps avec notamment ses outils d'audit de code, on a généralisé les tests d'intrusions automatisés ou non, et développé le bug bounty … mais pourquoi ne pas former tout ce petit monde à développer du code sécurisé dès le départ comme on le faisait pour les développements traditionnels ? Et finalement a-t-on vraiment calculé le ROI de ces développements dont la durée de vie est souvent assez courte ?

• Enfin on ne peut pas ne pas évoquer ici les grands éditeurs dont le nombre de vulnérabilités de leur suite logicielle fait quasiment partie de leur marque de fabrique depuis plusieurs décennies maintenant. L'industrie de la gestion des patchs, en termes de produits, mais surtout d'opérations, engloutit des sommes d'argent faramineuses si l'on additionne les budgets et les ETP que toutes les entreprises y consacrent. Que de projets de sécurisation préventive pourraient être menés à la place !

L'épisode Solarwinds, suivi de quelques autres, ont, semble-t-il, éveillé quelques consciences (mais pour combien de temps ?) et on ne compte plus les rapports, les groupes de travail à des niveaux plus ou moins élevés de l'échelle politique pour proposer des pistes pour, sinon régler ce problème (on n'atteindra jamais une sécurité à 100% du logiciel), du moins en endiguer l'inflation.

Ce qui est désarmant dans cet épisode Solarwinds et ses quelques répliques, c'est le caractère quasiment fataliste de son traitement. Que peut faire le RSSI même le mieux armé, si une société spécialisée telle que Fireye a certes détecté l'attaque mais plusieurs mois après son déclenchement et si des géants comme Microsoft n'ont rien détecté du tout ?

Partant du principe que nulle forteresse n'est imprenable, on ne peut pas s'empêcher d'envisager un Patch Tuesday porteur de ce type de maux par exemple. Et là nous serons bien dans une situation de pandémie numérique mais pas nécessairement celle que l'on envisageait.

Alors que faire ?

Si on se hasarde à une comparaison avec le monde automobile, outre les cents ans du code de la route qui vient d'être célébré, si on désosse une voiture et que l'on met de côté tout ce qui concourt à la sécurité du conducteur et des passagers, on doit arriver à environ 70 % des composants de la voiture qui contribuent à la sécurité de ses usagers. Si on fait la même chose avec un logiciel, il y a fort à parier que la part du logiciel consacrée à la sécurité sera très décevante. Pourquoi une telle disparité ? Tout simplement parce que depuis l'apparition des premiers véhicules au début du siècle dernier, on s'est très vite rendu compte que l'on avait mis en service de formidables machines à tuer et que depuis, on n'a pas cessé de progresser en matière de fiabilité des véhicules. Il semblerait que le cahier des charges de la sécurité logicielle des voitures autonomes soit tellement exigeant qu'il en paraisse inatteignable pour les constructeurs. La justification de ces niveaux de réglementation semble bien entendu indiscutable.

> « *on n'agit pas, par crainte d'impacts économiques ou pire, par manque de courage.* »

Mais alors pourquoi observe-t-on une telle médiocrité dans la sécurité logicielle au sens large ? Parce que jusqu'à une période récente l'absence de sécurité logicielle n'a pas fait beaucoup de morts ! Alors faudra-t-il attendre des victimes en grand nombre après un piratage d'une usine de distribution d'eau ou plus simplement un dérèglement des feux de signalisation dans une ville justement « connectée » ou encore un phénomène de pandémie numérique tel que décrit plus haut ?

On sait ce qu'il faut faire pour sécuriser le code ou pour empêcher que des intrus ne le détournent, mais un peu comme pour le réchauffement climatique, on n'agit pas, par crainte d'impacts économiques ou pire, par manque de courage.

On n'a jamais autant parlé de souveraineté numérique qu'en ce moment mais selon l'adage « *faites ce que je dis, pas ce que je fais* », force est de constater que l'exemple ne vient pas encore d'en haut si l'on ne retient que de récentes décisions étatiques en matière de choix de solutions américaines plutôt qu'européennes. ■

La cybersécurité, un levier d'avenir positif et non un mal nécessaire !

Etienne de Séréville, IBM,
pour la Commission Cybersécurité de numeum

Les derniers mois n'ont pas épargné nos entreprises : la longue crise sanitaire à rebond épidémique, la généralisation du télétravail, autant que faire se peut, suivant les activités de chacun et la multiplication des incidents cyber graves et opportunistes nous ont conduits à recentrer nos efforts sur l'essentiel : la santé de tous, la cohésion dans l'adversité et la poursuite de nos activités économiques pour un engagement de la filière numérique remarquable au profit de nos clients.

Cela s'est traduit par le renforcement et la mise à disposition d'infrastructure d'accès distants, l'utilisation accrue de 50% d'Internet et de 25% des services en cloud, et une assistance rapide en cas d'incidents et de crises cyber. Ces derniers ont continué à jalonner l'actualité, en particulier nos hôpitaux déjà éprouvés par l'épidémie, par leur nombre et leur impact : la multiplication des ransomwares (par 4 en 2020 d'après l'ANSSI), les fuites de données massives et la diffusion étendue par la compromission de fournisseurs (SolarWinds).

La cybersécurité, un levier d'avenir positif

Notre conviction est que la mise en commun de nos expertises et de nos ressources permet de travailler ensemble plus efficacement et de construire des réponses plus pertinentes aux questions du numérique et de la cybersécurité. En cela, nous sommes tout à fait alignés avec le Forum International de la Cybercriminalité dont la thématique de l'édition 2021 était une cybersécurité plus coopérative et plus collaborative. D'autre part, c'est aussi l'esprit qui a guidé la fusion du Syntec Numérique et de TECH IN France qui a vu la création de numeum, premier syndicat de représentation de l'écosystème numérique en France, regroupant plus de 2000 professionnels. Notre ambition à la Commission Cybersécurité est de faire en sorte que la cybersécurité soit considérée comme un levier d'avenir positif, non comme un mal nécessaire, et qu'elle apporte de la valeur au numérique par la confiance qu'elle lui procure en le sécurisant.

Informer et sensibiliser

Pour cela, nos objectifs sont de favoriser les échanges entre les membres de numeum et avec l'écosystème de la cybersécurité, faire connaître les solutions et les services de sécurité de nos membres, contribuer à rendre attractive la filière pour attirer les talents vers nos métiers et informer et sensibiliser les utilisateurs du numérique des risques potentiels pour contribuer à la confiance numérique. Ainsi, nos actions se déclinent en échanges entre professionnels sur les sujets d'intérêt cyber, tant techniques que réglementaires ou normatifs, d'innovation et d'industrialisation des technologies, ainsi que de formation vers l'école et l'enseignement supérieur. D'autre part, nous participons par exemple au rayonnement de la plateforme cybermalveillance.gouv.fr et notamment de la labellisation ExpertCyber, sommes partenaire du mois européen de la cybersécurité piloté au niveau national par l'ANSSI et nous formulons des propositions en matière de cybersécurité auprès des pouvoirs publics.

Toutes ces activités sur la cybersécurité au profit de la filière numérique française sont mues par des valeurs communes : ensemble pour un numérique de confiance au service des hommes et des innovations au service de la société. ■

La cybersécurité est désormais un bien commun

À un moment où la situation de la cybercriminalité devient critique, avec une multiplication des cyberattaques, des fraudes, des usurpations d'identité, dans un contexte de crise sanitaire, la filière de la cybersécurité risque de se disperser, façon puzzle comme aurait dit Audiard.

Par Jean-Marc Grémy,
Président du CLUSIF

Les plans de relance économique de la France et de l'Europe laissent entrevoir des financements publics de plusieurs dizaines de millions d'euros, dont des parties non négligeables pour la filière cybersécurité. Mais ces fonds seront-ils bien utilisés ? Les investissements permettront-ils une maîtrise du risque cyber à terme pour tous ? Permettront-ils que nous puissions enfin entrevoir une forme d'autonomie stratégique française, européenne pour la sécurité du numérique ? Maintes fois promise sans que nous en voyions les contours se dessiner ?
Notre crainte n'est ici pas que l'État au travers de ses ministères, ses agences et autres autorités n'ait pas les moyens de son ambition, mais bien que ces sommes d'argent ne soient finalement pas utilisées à bon escient, que leurs destinations ne servent qu'à « enrichir » des acteurs industriels et de services qui ne nourrissent d'autres rêves que d'accroître nos capacités scientifiques, industrielles et de cyberdéfense.

> ***« La cybersécurité est maintenant une nécessité quasi vitale comme la santé ou l'économie pour nos entreprises et collectivités. »***

La cybersécurité est d'utilité publique.

Si l'ANSSI est en partie à la manœuvre pour l'instruction des dossiers et du financement dans le cadre des « Parcours de cybersécurité », quelles sont les garanties d'un contrôle de l'usage des fonds ? De l'atteinte des objectifs ? Nous ne pouvons plus revivre des ratés comme les initiatives de cloud souverain ! Ce n'est pas qu'une question d'argent, mais bien de la pérennité de nos savoir-faire, de nos industries et très certainement de nos vies quotidiennes à terme.

Cette notion d'autonomie stratégique dans le monde numérique fait débat tant la mondialisation des échanges de données et de leurs infrastructures emboîte le pas à celle des échanges économiques. Cette autonomie stratégique doit être une cible qui doit dépasser la seule idée de la mise en œuvre de cyberdéfense, à l'heure où la cyberconflictualité s'invite quotidiennement dans l'analyse géopolitique.
Comme le montre le Panorama de la cybercriminalité annuel du Clusif, les menaces se sont multipliées, diversifiées, les criminels sont plus organisés et n'ont plus nécessairement besoin d'expertise technique pour agir. Face à cette industrie du crime, la cybersécurité est maintenant une nécessité quasi vitale comme la santé ou l'économie pour nos entreprises et collectivités.
Partant de cette nécessité, nous devons fixer ensemble les objectifs communs de l'écosystème cyber. Il n'est pas seulement question de moyens financiers mais bien de pérennité de nos savoir-faire, de nos industries et de notre vie démocratique. L'arrivée à l'automne du Campus Cyber est sans nul doute le premier jalon de cette longue route vers notre autonomie stratégique.
Fort de ses plus de 1 000 adhérents actifs et de ses productions à destination des entreprises, le Clusif participe activement à la mise en place de ces plans. C'est une question stratégique pour nos entreprises mais également pour nos concitoyens et dans un monde où le numérique est partout, la cybersécurité doit plus que jamais s'organiser pour réassurer notre économie et nos institutions. ■

Pourquoi privilégier les solutions de cybersécurité innovantes, de proximité et de confiance ?

Jean-Noël de GALZAIN, Président d'HEXATRUST

Une politique industrielle de cybersécurité, une vision stratégique au plus haut niveau

Les investissements Européens dans la transformation numérique, dans la modernisation de notre industrie et des usages de nos services publics sont destinés à croître de manière exponentielle dans les 10 prochaines années.

Selon l'institut IDC, « Les dépenses européennes en technologies et services qui permettent la transformation numérique des entreprises, des produits et des organisations devraient atteindre 378,2 milliards de dollars en 2022 » rien qu'en Europe, et 1800 milliards de dollars dans le monde.

L'écosystème de la transformation numérique est en effervescence, pourtant les industries européennes de la filière, matures et implantées à l'international, peinent encore à se positionner efficacement sur leur propre marché face aux concurrents mondiaux.

Ceci est, entre autres, dû à la prépondérance des solutions étrangères dans le secteur provenant d'entreprises efficacement poussées par leur propre Etat.

A juste titre c'est un axe stratégique et une politique industrielle que nous devons nous-mêmes pousser en France afin d'assurer une indépendance stratégique dans les technologies clés comme la cybersécurité ou l'Intelligence Artificielle.

Tout l'enjeu pour l'Europe, et la France est donc de se doter d'un marché national et européen actif, qui fasse le choix clair de privilégier les solutions de cybersécurité responsable et de confiance.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Le choix clair des solutions innovantes, de confiance et de proximité : un risque maîtrisé pour les donneurs d'ordre

En France, nos startups et PME industrielles qui constituent notre « FrenchTech », dont nous sommes si fiers, doivent pouvoir se reposer sur une commande nationale, des acheteurs et des prescripteurs nationaux.

Ce choix de la préférence française et européenne dans nos achats est une priorité afin de nous permettre de développer une industrie de cybersécurité leader dans le monde.

C'est à la fois la clef de la croissance de nos entreprises, véhicules d'emploi et d'avenir, mais également la maîtrise de notre dépendance numérique afin d'assurer notre propre autonomie et résilience dans un monde en perpétuelle évolution.

La nature stratégique des enjeux de sécurité informatique des organisations, publiques comme privées, doit nous pousser à faire confiance à notre industrie en premier lieu. C'est assurer la protection des actifs stratégiques de nos organisations et le respect et la mise en conformité avec notre droit.

Aujourd'hui, les acheteurs et grands donneurs d'ordres peuvent se tourner vers un écosystème industriel français de cybersécurité mature et reconnu dans le monde entier comme étant à la pointe de la technologie. La France regorge d'entreprises innovantes, avec des niveaux de croissance dépassant les 20% et implantées à l'international.

Au sein d'HEXATRUST, par exemple, nous proposons un catalogue des solutions de confiance labellisées pour leur innovations, leur confiance et répondant aux besoins du marché et respectueuses de l'intérêt européen et de la protection des individus dans un monde qui bouge.

Découvrir notre catalogue HEXATRUST

L'offre Cloud la plus complète du marché !

Bordeaux - Lille - Lyon - Nancy - Nantes - Orléans - Paris Centre - Paris Sud - Rennes - Rouen - Strasbourg - Toulouse - Tours

La gamme iCod®, votre trajectoire Cloud sur mesure avec des Services Managés personnalisés

iCod® — Energy Min Power Max !

le Cloud personnalisé pour vous

iCod® Healthcare

le Cloud pour vos données de santé

iCod In-Memory® — The Best Cloud for the Leading ERP !

le Cloud le plus performant pour vos environnements SAP Hana

iCod RCO® — The Best Red Cloud in the world !

le Cloud des environnements full Oracle

iCod 400® — The Latest Generation of Power !

le Cloud des environnements IBM power

CHEOPS SECURITY OPERATION CENTER

L'offre SOC by CHEOPS TECHNOLOGY !

3 niveaux pour s'adapter à vos besoins :

1. SOC Silver : Service SOC As A Service
2. SOC Gold : Service SOC Managé
3. SOC Platinum : Service SOC On-Premise

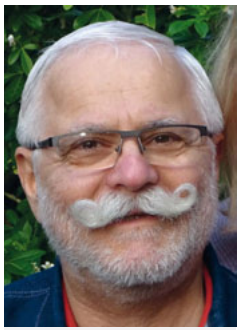
Un éventail de services pour vous apporter une réponse :

- Service d'OSINT
- Equipé de réponse sur incident, Forensic
- Backup Sécurisé, PRA / PCA
- Pentest, Audit technique & de conformité, scan de vulnérabilité
- Conseils, Formations et Sensibilisation...
- Sécurisation des infrastructures, des accès et des données

05 56 18 83 83 • www.cheops.fr • info@cheops.fr

Forte de ses 600 collaborateurs et ses 13 agences en France garantissant une relation de proximité avec ses clients, CHEOPS TECHNOLOGY propose des solutions de Cloud privé ou hybride les plus performantes du marché en fonction du type d'environnement. CHEOPS TECHNOLOGY, "The Cloud customized for you !".

Baromètre trimestriel de l'AFCDP : la voix des DPO



Patrick Blum,
Vice-Président Métiers, AFCDP

Avec son Observatoire trimestriel, l'AFCDP souhaite estimer l'évolution de la conformité des organisations, et évaluer la perception des DPO sur des sujets techniques et d'actualité.

Une confiance mitigée dans la protection des données privées

Il est manifeste que les DPO et les professionnel(le)s de la protection des données personnelles ont majoritairement (52% versus 54% au 1er trimestre) le sentiment qu'il y a encore du chemin à faire avant de considérer leurs organisations comme conformes au RGPD et autres mesures de protection des données personnelles. A noter que 13% des répondants jugent que les réglementations changeantes (invalidation du Privacy Shield, Cookies Wall, etc.) perturbent les stratégies de protection des données personnelles mises en place jusqu'ici. Cependant, il est très positif de noter que 30% des répondants se sentent écoutés et utiles, indicatif qu'il sera utile de suivre sur les prochaines éditions.

Un an après l'annulation du Privacy Shield

La majorité des répondants (52%) ne sont pas encore à l'aise avec l'impact de l'invalidation du Privacy Shield et n'ont pas encore organisé l'éventuel rapatriement du traitement de leurs données critiques ou métiers en Europe. Si le jugement de la CJUE a invalidé le « Privacy Shield », il n'a pas interdit le recours aux CCT. Il a cependant précisé comment interpréter la notion de « garanties appropriées » exigées par l'article 46 du RGPD. La Commission européenne a donc proposé de réviser ces CCT en conséquence. Cette évolution était très attendue, en particulier par les délégués à la protection des données, impatients de disposer d'un outil fiable pour assurer la conformité des transferts. Plus particulièrement vers les États-Unis d'où sont issues les multiples solutions technologiques sur lesquelles s'appuient les entreprises.

Dans une résolution adoptée le 20 mai 2021 à une très large majorité, le Parlement européen attirait l'attention de la Commission européenne sur les réserves du CEPD/EDPB (le comité des CNIL européennes) et du CEPD/EDPS (le DPO des instances européennes), et formulait des recommandations importantes. Comme la CNIL le résume dans sa FAQ sur les nouvelles CCT, celles-ci prennent en compte la législation du pays tiers de destination des transferts de données. C'est donc bien à l'exportateur, par exemple la PME ou l'association qui utilise les services d'un prestataire américain, de vérifier si la législation américaine n'est pas contraire aux obligations du RGPD et ne fait pas courir de risques aux données transférées.

Le suivi du degré de vaccination des équipes au sein des organisations

Le retour au bureau se fait au final plus rapidement qu'initialement imaginé. Nombreuses sont les mesures sanitaires déjà intégrées dans les organisations, alors comment gérer l'entrée en vigueur du passe sanitaire et la généralisation de la vaccination ? Et les enjeux de protection des données personnelles liés ? Finalement, la majorité des répondants (51%) ne considèrent pas que le suivi de la vaccination soit pertinent dans leur organisation. Mais cela dépend aussi peut-être du type d'organisation, car 12% des répondants ont tout de même confirmé effectuer un suivi. ■

Méthodologie : Dans le cadre de son Baromètre trimestriel, l'AFCDP a mené une enquête en ligne auprès de ses 6000 membres entre le 10 et le 21 juin 2021, via le réseau social privé de l'association (215 répondants) et sa page LinkedIn (60 répondants.

Les tendances

de la cybersécurité

Télétravail :
la nouvelle frontière de l'accès distant

Gestion de crise Cyber :
Se préparer au pire !

La Supply Chain Attack

Ces multiples vulnérabilités
qui menacent les SI

La cyber-assurance

Télétravail : la nouvelle frontière de l'accès distant

Ces derniers mois, le travail a connu une transformation sans précédent. Sous la pression de la pandémie de Covid-19, le télétravail a pris une place beaucoup plus importante. Les entreprises ont dû ouvrir des accès à leur système d'information. Il est temps de penser à l'avenir de ces accès distants.

Par Alain Clapaud

L'épidémie de Covid-19 a fait bouger les lignes. Le télétravail, qui restait en France un épiphénomène s'est généralisé à l'occasion des diverses périodes de confinement. Ce sont des millions de salariés qui, du jour au lendemain, ont été priés de travailler depuis leur domicile pour des raisons sanitaires et face à cette situation inédite, les entreprises sont allées au plus simple et ont ouvert des accès distants via VPN, de la même façon qu'elles le faisaient pour leurs travailleurs nomades et cadres. Les éditeurs de solution de sécurité ont accompagné les entreprises en levant temporairement les contraintes de licences, leur permettant d'installer par dizaines de milliers les clients VPN sur de nouveaux postes, la régularisation des licences n'intervenant que dans un deuxième temps, une fois l'urgence traitée.

Les 7 grands principes d'une architecture Zero Trust (ZTA) selon le NIST

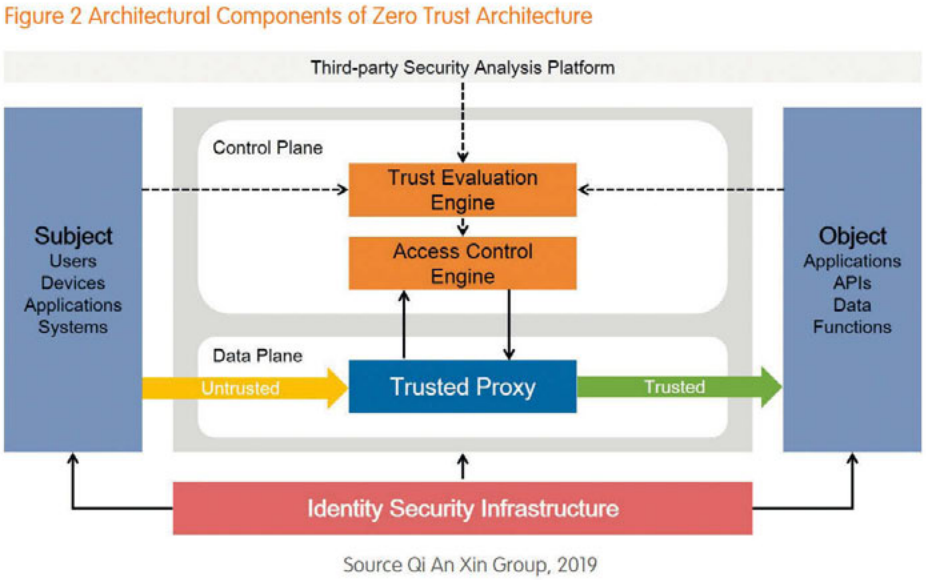
1. Toute source de données et service délivré par l'IT est considéré comme une ressource,
2. Toute communication doit être sécurisée quelle que soit son emplacement sur le réseau,
3. Les droits accordés sur une ressource ne sont validés que pour une seule session,
4. L'octroi des droits d'accès est réalisé de manière dynamique en fonction de multiples facteurs,
5. L'entreprise doit surveiller en temps réel l'intégrité de son système d'information et l'intégrité et l'efficacité de son infrastructure de sécurité,
6. L'authentification et l'autorisation de toutes les ressources sont dynamiques et strictement appliquées avant que l'accès ne soit autorisé,
7. L'entreprise doit recueillir autant d'informations que possible sur l'état de ses assets, de son infrastructure réseau et des communications afin d'améliorer sa posture de sécurité.

D'après une enquête de la Dares (Direction de l'Animation de la recherche, des Études et des Statistiques) sur la période 2017/2019, seulement 3 % des salariés étaient occasionnellement en télétravail, cette part serait passée à 24% en mars 2020 d'après un sondage Odoxa. Si la norme semble désormais s'établir à 2 jours travaillés dans les locaux de l'entreprise pour 3 jours de télétravail, la Dares estime à 12% la part des salariés qui étaient encore en télétravail en septembre 2020.

Le VPN, une architecture mature, mais pas sans inconvénients

Solution relativement simple et robuste, les liens VPN ont permis de connecter les collaborateurs à distance de manière relativement sûre, car si des attaques restent possibles sur des liaisons chiffrées, la technologie est aujourd'hui mature. Il reste bien évidemment toujours des failles à venir et à corriger sur les passerelles VPN et sur les logiciels clients mais, depuis la découverte puis le patching de la faille « Heart Bleed » dans la bibliothèque OpenSSL, le déploiement de versions récentes des logiciels permet d'écarter l'essentiel des attaques sur ces liens.

Le déploiement massif de clients VPN a néanmoins entraîné des conséquences, notamment en termes de performance. Les entreprises disposant de passerelles VPN ou de firewall dimensionnés au plus juste ont été confrontées à une chute des performances d'accès. Pour certaines ce fut l'accès Internet qui a été congestionné par toutes ces connexions inhabituelles. Outre une chute de productivité aux heures les plus actives de la journée, beaucoup de collaborateurs ont préféré accéder aux applications Cloud de l'entreprise directement sur Internet, sans transiter par le VPN afin de bénéficier d'un meilleur débit et de temps de latence réseau restreints. La conséquence de ce raccourci pris par les collaborateurs est que ceux-ci ne bé-



L'architecture ZTNA telle que la définit le Gartner.

néficient plus de l'ombrelle de sécurité apportée par l'entreprise, notamment la protection anti-malware alors que l'épidémie de Covid-19 provoquait dans le même temps une avalanche de tentatives d'attaques par ransomware et phishing. Autre conséquence de ce comportement, les collaborateurs échappaient au contrôle réalisé par le CASB (Cloud Access Security Broker) sur les accès aux applications Cloud, avec des conséquences possibles en termes d'exposition au risque de fuite de données, mais aussi quant à la conformité.

Le Cloud, une autre approche de la sécurité des accès

Face à cette évolution à la fois sociétale mais aussi technique, avec une informatique de plus en plus exploitée dans le Cloud public, un changement de paradigme est en train de s'opérer dans cette gestion des accès distants. Le nouveau modèle en train de s'imposer s'appelle le Zero Trust Network Access (ZTNA). Celui-ci s'inscrit pleinement dans l'approche SASE (Secure Access Service Edge) qui allie des briques ZTNA à un réseau de type SD-WAN.

Parmi les grands principes d'une architecture « Zero Trust », accorder des droits d'accès à une ressource doit être réalisé de manière totalement dynamique. Un droit n'est octroyé à un utilisateur ou à une application qu'en fonction de multiples facteurs dont l'identité de l'utilisateur ou de l'application qui réclame un accès, la ressource demandée mais aussi des éléments tels que la localisation géographique ou le comportement de l'utilisateur.

Mettre en place un accès de type ZTNA nécessite donc de multiples briques technologiques qui agissent de concert pour s'assurer de la sécurité des accès. Cela implique les briques de gestion des identités et des accès pour valider l'identité de l'utilisateur au moment où celui-ci veut accéder à une ressource, les firewalls pour contrôler les échanges et notamment réaliser l'inspection des flux SSL, les IPS pour détecter d'éventuelles attaques. La sécurisation des applications Cloud nécessite pour l'entreprise d'avoir une visibilité de l'activité des collaborateurs sur les services SaaS. C'est le rôle de la brique CASB qui va vérifier dynamiquement l'activité de l'utilisateur sur ces services hébergés hors de l'entreprise.

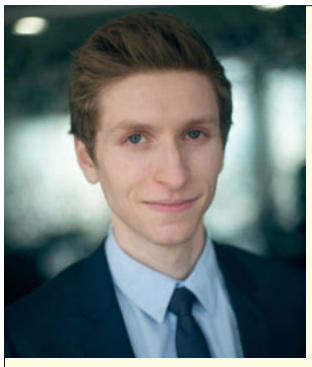
La part du Cloud étant croissante dans les systèmes d'information, l'idée de traiter cette problématique de gestion des accès dans le Cloud a fait son chemin. Cela a donné naissance aux solutions de type passerelles de sécurité Web (SWG). Utiliser une passerelle Internet pour centraliser la gestion de l'ensemble des accès aux ressources SaaS résout le problème de montée en charge des passerelles VPN. Il est beaucoup plus simple de provisionner de nouvelles ressources dans le Cloud et l'exemple de la pandémie a démontré la validité de l'approche. Depuis, les fournisseurs de passerelles SWG ont étoffé la couverture fonctionnelle de leurs offres. Celles-ci permettent non seulement de gérer les accès aux applications Cloud, mais aussi celles des utilisateurs en situation de télétravail ou nomadisme vers les applications internes de leur entreprise. Outre le volet authentification, ces plateformes sont de plus en plus universelles et offrent des fonctions de WaaF, de CASB, d'IPS, de DLP, de Sandbox, etc. Externaliser ainsi de plus en plus de briques de sécurité pour aller, pas après pas vers une informatique 100% sécurisée semble être le cours de l'histoire. Avec les passerelles SWG, le VPN semble avoir trouvé son successeur dans le Cloud. ■

Gestion de crise Cyber : Se préparer au pire !

Le risque d'une attaque informatique pèse sur chaque entreprise. Le seul moyen d'y faire face et de limiter les dégâts est de s'y préparer. Il est urgent de mettre en place une check-list à appliquer en cas d'intrusion et se maintenir prêt à la déclencher à tout instant.

Par Alain Clapaud

Tous les experts en cybersécurité le martèlent depuis des années : il ne faut pas se poser la question de savoir si son entreprise va être attaquée, mais quand. Face à cette certitude, il faut se préparer au mieux en élevant le niveau de sécurité de chaque site, de chaque endpoint, en se dotant d'outils de détection d'intrusion, en s'assurant de la fiabilité et de la protection des systèmes de sauvegarde et en segmentant au mieux son réseau interne pour limiter les dégâts. En dépit de toutes ces précautions, un attaquant finira par passer et il faudra alors réagir vite, réagir efficacement. La meilleure façon de le faire, c'est s'y préparer et mettre en place des procédures pour réagir de la manière la plus rapide et efficace possible dans l'adversité.



Eric Schmitlin,

Consultant Cybersécurité chez Cendium Cyberdefense

"Pour bien anticiper une crise cyber, il faut préparer tout ce qui ferait perdre un temps précieux pendant la crise : préparez un groupe (Signal, Telegram, WhatsApp…) avec les intervenants de la cellule de crise, préparez les messages de communication, définissez les rôles et responsabilités… Bref, si vous êtes déjà organisés lorsque la crise survient, vous pourrez directement passer à l'analyse et à la prise de décision.

Vous pouvez également faire organiser un exercice de crise par un cabinet spécialisé qui va vous placer dans l'inconfort à travers une simulation réaliste d'une journée ou moins : vous en ressortirez avec de précieux conseils et une expérience par la pratique. C'est généralement très apprécié des participants.

Enfin, n'hésitez pas à recueillir le retour d'expérience d'autres entreprises de votre secteur victimes d'attaques. On a coutume de dire qu'il existe deux types d'entreprises : celles qui se sont fait attaquer… et celles qui vont l'être !"

Chaque entreprise doit définir sa propre check-list

En 2019, Syntec Numérique (devenu en juin 2021 numeum) et **Cybermalveillance.gouv.fr** publiaient une brochure sur la question, formalisant une check-list en 5 étapes clés, chacune d'entre-elles étant à son tour déclinée en une série de conseils à appliquer. Eric Schmitlin, Consultant Cybersécurité chez Cendium Cyberdefense et l'un des auteurs de cette publication du Syntec souligne : *"Si cette méthodologie et ses grandes étapes s'appliquent à tous, leur réalisation diffère. Il faut se montrer plus pragmatique pour les petites structures. Par exemple, une grande entreprise disposera de moyens de détections perfectionnés faisant appel aux dernières technologies, alors qu'une TPE/PME se concentrera principalement sur la vigilance de ses utilisateurs pour remonter de potentiels incidents."*

Pour l'expert, la différence majeure entre un plan d'action défini par une grande entreprise et son alter ego dans une PME réside dans les moyens humains mobilisables en cas d'attaque. *"Les petites structures ne disposent pas de ressources pour gérer les incidents : il ne faut alors pas hésiter à solliciter les cabinets spécialisés en cybersécurité."* De leur côté, les grandes entreprises possèdent généralement des ressources en interne mais aussi des contrats avec des cabinets spécialisés qui vont pouvoir leur détacher très rapidement des ressources pour les épauler dans la gestion de crise et dans la phase de remédiation qui suivra. De plus, les administrations et entreprises de type OIV et OSE doivent se tourner vers l'ANSSI pour signaler l'attaque, mais aussi bénéficier du soutien du Centre opérationnel de la sécurité des systèmes d'information (COSSI).
Pour toutes les organisations, il faut se plier aux

ANATOMIE D'UN INCIDENT

Cet incident fictif s'inspire de cas réels issus d'échanges entre profesionnels du numérique.

En collaboration avec

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

TÉLÉPHONE — il y a 3 mn

Astreinte DSI HNO
Appels manqués (3)

Samedi 7:02

On a un problème, je pense que la messagerie est tombée.

C'est un problème technique ou un incident sécu ? Je t'appelle, tu peux commencer à investiguer ?

Samedi 9:09

C'est l'horreur là je pense que c'est un ransomware qui a explosé l'annuaire et pas mal de serveurs. J'ai une demande de rançon sur l'écran. Ça doit pas être répertorié car l'antivirus n'a rien vu...

J'arrive dans 10 min, je suis dans un taxi. Tu peux envoyer des échantillons contaminés à l'éditeur de l'antivirus ?

Samedi 10:32

Incident en cours (Ransomware). Messagerie indisponible, activation de la cellule de crise. Veuillez vous rendre dès que possible dans les locaux.
Le RSSI

WHATISUP — maintenant

RSSI @ Taskforce Cyber
J'ai créé un groupe Whatisup avec tout le monde pour échanger vu qu'on n'a plus de mails...

Samedi

J'ai essayé d'appliquer le patch... Là on voit des exclusions apparaître dans les paramètres... En fait on n'a plus le contrôle de la console de l'antivirus ! C'est l'attaquant qui est toujours là et il contrôle tout, je suis très serieux.
18:04

Coupez tout ! L'application des correctifs, les entrées et sorties réseaux, on coupe tout !
18:06

Nouveau message
adresseperso@fmail.com

À : monassureur@jassure.fr

Bonjour,
À la suite à notre appel, je vous confirme le déclenchement de l'assurance cyber.
Pouvez-vous me confirmer l'intervention d'experts dès cet après-midi ?

Console de supervision

https://super-vision.infra/console

Etat des services
- Annuaire
- Messagerie
- Téléphonie fixe
- Firewalls/Pare-feux
- Antivirus
- Intranet

Nouveau message
rssi@maboite.com

À : direction@maboite.com

Plan_action_v1.pptx

Vous trouverez, ci-joint, le plan d'action à la suite de l'incident informatique du mois dernier.
Quand peut-on se croiser pour parler du budget sécurité ?

SAMEDI 7H

Détection et signalement

Premiers signalements d'un incident technique impactant la messagerie.

Avoir des outils de détection et d'alerte ainsi que des **personnes disponibles pour traiter les alertes** est indispensable. Sans cette alerte du technicien d'astreinte, un weekend entier se serait écoulé sans aucune action !

SAMEDI 9H

Qualification et évaluation

Les premiers signes d'un ransomware se font savoir : une demande de rançon s'affiche sur certains écrans et l'annuaire de l'entreprise est compromis.

RANÇON : FAUT-IL PAYER ?

Non ! Pour commencer, il n'est pas assuré que vous récupériez vos données et que les hackers vous assistent dans cette tâche ! Enfin, cela contribuerait à alimenter cette forme de criminalité.
Pour finir, le caractère licite d'un paiment de rançon est plus que discutable en droit français.

SAMEDI 10H

Activation de la taskforce

Les fournisseurs de sécurité livrent leurs premières analyses qui confirment la qualification.
Le RSSI informe alors son dirigeant de l'incident et active officiellement la cellule de crise.

Savoir qui contacter chez ses prestataires et fournisseurs de sécurité. Prévoir une liste précise de personnes à contacter et des moyens de communication de crise alternatifs puisque les mails ne fonctionnent plus !

Tentatives de résolution

Les équipes travaillent à la mesure de l'étendue des dégâts et tentent de résoudre le problème. En soirée, les éditeurs mettent à disposition des correctifs de sécurité.

Laisser les équipes faire leur travail (informatique et RSSI, communication, métiers, juridique, etc.) et minimiser les égarements sur des sujets annexes.

SAMEDI 18H

Coupure et isolation du réseau

Découverte que l'attaquant est toujours présent au sein du réseau et a pris la main sur les outils de sécurité. La décision est prise d'isoler l'ensemble du réseau pour éviter des dégâts supplémentaires et stopper l'emprise du hacker sur le système d'information.

Définir des cas précis nécessitant la coupure du réseau, de façon à déporter cette prise de responsabilité sur une procédure validée et non une personne qui va forcément hésiter.

DIMANCHE 10H

Début de l'intervention de l'assurance

La cellule de crise contacte l'assurance, qui envoie des experts pour investiguer et trouver et appliquer des solutions. Les autorités (police/gendarmerie, CNIL et ANSSI) sont également contactées.

Les assurances servent aussi de pompiers et de soutien lorsque les ressources ou compétences internes ne sont pas suffisantes.

MERCREDI 17H

Premières reconstructions

La cellule de crise est activée en permanence et mène un vrai travail d'équipe ; l'annuaire est reconstitué à partir d'annuaires partiels et de sauvegardes déconnectées initialement du réseau, puis la messagerie.

Les sauvegardes sont souvent la première cible des attaques de cette nature, elles peuvent donc elles-mêmes être inutilisables.

VENDREDI 15H

Retour au nominal

Les équipements de sécurité, puis le reste, sont reconstitués. Pendant toute la semaine, l'enreprise a tenté de travailler avec des moyens informatiques limités ; et à l'issue, de nombreuses données restent perdues.

Les plans de continuité définis en amont des crises doivent prévoir les moyens de travailler avec des moyens informatiques réduits.

3 SEMAINES APRÈS

Retour d'expérience

Les investigations port-mortem des experts révèlent que l'attaquant est passé par un poste obsolète qui n'avait pas été recensé. La direction et les équipes débriefent et prévoient un plan d'action.

Disposer d'une vision claire de son parc informatique est la base de la sécurité. L'entreprise doit se nourrir de cette expérience pour capitaliser et s'améliorer.

Benjamin Leroux

Directeur Marketing d'Advens

"Anticiper une crise cyber passe principalement par la préparation et l'entrainement"

"Toute organisation peut se préparer à faire face à une crise cyber et ce avant que la crise se présente. Cette préparation repose sur différents socles. Le premier, c'est le socle organisationnel. Qu'il s'agisse de politiques internes, de procédures, de modes dégradés, la mise en place d'une organisation dédiée et d'un corpus documentaire sur la gestion de crise sera un plus pour les organisations : avoir le mode d'emploi pour monter un meuble suédois va nous aider mais ne garantit aucunement le résultat ! Le socle technique est très important en cyber et les solutions technologiques sont particulièrement nombreuses. Il nous semble essentiel de renforcer ses capacités de détection et de réaction. C'est notamment l'objectif des EDR pour protéger les postes de travail et les serveurs et, plus globalement, celui de l'XDR à l'échelle de tout le SI. Enfin, le socle humain est la dernière brique qu'il faut préparer : une crise cyber n'est pas une crise informatique : c'est une attaque humaine contre une défense humaine, c'est une bataille qui va durer, prendre du temps, épuiser, fatiguer. Il faut s'y préparer : que ce soit les équipes opérationnelles ou les équipes décisionnelles, il faut tester les procédures et les dispositifs de crise, se préparer à la prise de décision sous stress et identifier les bons réflexes à avoir.

Ces trois socles ne permettent pas d'éviter une crise cyber mais de se préparer à y faire face et à la dépasser. Les crises sont également des opportunités pour grandir sous réserve de pouvoir les gérer sereinement !"

obligations légales quant à la déclaration de l'incident de sécurité auprès de la CNIL. Si une atteinte à des données personnelles est suspectée, l'entreprise doit déclarer l'attaque dans les 72 heures. Cette déclaration se fait en ligne sur le site de la CNIL et comporte l'ensemble des éléments la caractérisant, dont le nombre approximatif d'enregistrements de données à caractère personnel concernés. En outre, si le vol de données est avéré, l'entreprise est également tenue par le RGPD (Règlement Général sur la Protection des Données) d'informer les personnes concernées.

De l'organisation, de la technique et... beaucoup d'humain

Mettre en place un plan de gestion de crise cyber implique d'instaurer une organisation qui va être chargée, le jour J, de gérer l'incident de sécurité. Chaque membre de l'équipe de gestion de crise doit avoir un rôle et des responsabilités bien précis dans le dispositif et doit pouvoir être joint très rapidement. En outre, il faut mettre en place un annuaire de crise cyber incluant l'ensemble des contacts qui seront utiles le jour où la tempête éclatera. Il faudra joindre l'ensemble des contacts internes potentiellement concernés à un moment ou les outils de communication internes de type emails, messagerie instantanée, mais aussi ToIP pourront être *off-line.* Il faut aussi pouvoir joindre des contacts chez les tiers qui sont de plus en plus présents dans le système d'information, notamment les fournisseurs d'applications SaaS, les opérateurs de services Cloud et les divers prestataires. Benjamin Leroux, Directeur Marketing d'Advens ajoute : *"L'entreprise doit bien évidemment se doter d'un Plan de Continuité d'Activité (PCA) et de procédures dédiées présentant les différents modes dégradés possibles, aussi bien pour les métiers stratégiques (Plan de Reprise d'Activité) que pour les systèmes d'information (Plan de Continuité Informatique)."* L'expert souligne l'intérêt de mener une analyse de risque pour identifier les points de fragilité du système d'information et pouvoir ainsi préparer et structurer les défenses périmétriques, de même que la rédaction de "fiches réflexes" par rôle, par fonction, par expertise, afin d'indiquer quelles seront les premières actions à réaliser par chacun.

Le volet technique de la gestion de crise est excessivement important, car les experts ont besoin d'outils sophistiqués pour définir la nature exacte puis l'étendue de l'attaque. Généralement, la pre-

mière tâche d'une équipe CERT est de déployer un EDR sur les postes de l'entreprise pour disposer de ces outils. Plus largement, le SOC doit orchestrer la lutte contre l'attaquant. Qu'il soit interne ou externe chez un prestataire, le SOC dispose de ressources Forensic habituées à intervenir dans un contexte de crise cyber et leur expérience va être extrêmement précieuse dans un contexte où chaque minute compte.

L'aspect humain est particulièrement important car gérer une crise cyber peut imposer d'importantes charges de travail et de stress nuit et jour pendant plusieurs semaines. Il faut prévoir des relèves et surtout former et préparer chacun à cet exercice. L'entrainement est capital pour former les hommes mais aussi améliorer les procédures et outillages qui seront mis en œuvre en vraie grandeur le jour de l'attaque.

Pourquoi il faut se faire aider en cas de crise

Le recours à des prestataires spécialisés est encore plus indispensable lorsque l'attaque est détectée. Le catalogue mis en place par Cybermalveillance est un point d'entrée possible si l'entreprise n'a pas déjà contractualisé avec un prestataire en cybersécurité. Il faut se tourner vers une ESN qui dispose d'une activité de CERT (Computer Emergency Response Team) qui va jouer en quelque sorte le rôle de « cyber pompiers » pour l'entreprise. L'équipe du CERT va intervenir pour gérer la crise, sur les plans techniques et organisationnels" explique Benjamin Leroux. *"La sollicitation peut être ponctuelle, avec un risque de manquer de disponibilité dans un délai court car ces équipes sont malheureusement très souvent occupées ! Elle peut aussi se faire via une forme d'abonnement, dans un modèle qui rappelle la logique de l'assurance. Le CERT peut alors aider à préparer les travaux d'anticipation et d'amélioration de la réaction."*

Pour l'expert lillois de la cybersécurité, il faut accorder une attention toute particulière au volet réponse à incident, la phase 4 dans la méthodologie proposée par Syntec Numérique. Cette étape doit se dérouler en 3 temps : La première est sans doute la plus stressante : il faut détecter puis analyser au plus vite la nature réelle de l'incident de sécurité. *"Il s'agit alors d'une véritable course contre la montre lors de laquelle il faut analyser l'incident et comprendre la situation… pour ensuite prendre les bonnes décisions."* Vient ensuite le moment de passer à l'action, la phase d'éradication. *"Il faut avant tout éradiquer la cause de l'incident et en maitriser ses effets. Ce n'est qu'après cette phase que l'on peut ensuite songer à préparer la remise en ordre de marche et remettre en place un système sain et sécurisé."* Cependant, la réponse ne doit pas s'arrêter là : une dernière étape de consolidation est nécessaire puisqu'il faut enchainer avec une phase de consolidation pour éviter de se faire attaquer à nouveau. *"Cette dernière étape vise à finaliser les chantiers constituant la première version du plan de sécurisation… jusqu'au bout !"* conclut Benjamin Leroux.

Les cinq phases d'une gestion de crise cyber

Phase 1 : Préparation

- Mise en place des processus et des outils,
- Définition de la taskforce qui va intervenir en cas d'attaque,
- Tester le dispositif.

Phase 2 : Détecter et signaler

- Faire de la veille,
- Détecter les incidents via des outils automatiques ou des remontées d'alertes par les utilisateurs et prestataires.

Phase 3 : Evaluer et décider

- Qualifier l'attaque,
- Evaluer la cause, les méthodes et ses impacts.

Phase 4 : Répondre

- Résoudre l'incident,
- Apporter un correctif technique,
- Notifier l'assureur, les autorités et déposer une plainte.

Phase 5 : Capitaliser

- Analyser pour s'améliorer,
- Créer un plan d'action à mener et en assurer le suivi.

Source : Syntec Numérique / **cybermalveillance.gouv.fr**

La Supply Chain Attack

Les attaques sur la « Supply Chain » c'est-à-dire sur la chaine de fourniture des applications, en particulier au travers des éditeurs et des prestataires IT, sont en recrudescence. Un signe des temps alors que l'externalisation des ressources informatiques est de plus en plus massive.

Par Alain Clapaud

Le recours à l'externalisation s'est généralisé dans bon nombre d'entreprises ces dernières décennies. Les grandes entreprises comptent fréquemment plusieurs milliers de fournisseurs et l'IT s'inscrit pleinement dans cette tendance. Les projets d'infogérance et d'externalisation se sont multipliés et l'essor du Cloud Computing en est certainement l'illustration la plus flagrante. Les projets d'externalisation touchent tout autant la cybersécurité avec le recours de plus en plus fréquent aux MSP et services managés proposés par certains éditeurs. SOC, Threat Intelligence ou encore la gestion des vulnérabilités sont des domaines où la mutualisation des moyens mis en œuvre par un MSP constitue un vrai atout.

Selon l'Enisa, l'agence européenne de la cybersécurité, 66% des attaques sur la Supply Chain ciblent en priorité le code des partenaires.

Des entreprises de plus en plus liées, de plus en plus interconnectées

Ce mouvement vers l'externalisation fait courir un vrai risque cyber aux donneurs d'ordres, un risque baptisé "Supply Chain Attack". Dans un contexte où les systèmes d'information des entreprises sont de plus en plus ouverts et interopérables avec ceux de leurs partenaires, l'attaque d'un prestataire ou d'un sous-traitant expose directement l'entreprise au risque de rebond. A cet égard, l'explosion du nombre d'attaques par ransomware (+93% en un an selon le rapport semestriel de Check Point Software) expose toute entreprise à ce type d'infection par rebond via les postes de travail de prestataires ou de petits fournisseurs moins sécurisés. Outre les attaques tous azimuts via des ransomware diffusés en masse, on a aussi vu des ESN et des prestataires qui travaillent pour des entreprises stratégiques plus particulièrement visées par des attaques. Les attaquants espèrent pouvoir les faire rebondir vers leurs vraies cibles.

Parfois, elles n'ont rien de technologique. Les attaquants se contentent d'usurper l'identité des partenaires de l'entreprise. Une étude menée pour Proofpoint a récemment montré que 98% (!) des entreprises interrogées avaient reçu au moins une menace émise depuis un domaine fournisseur sur une période de 7 jours. Les attaquants exploitent au maximum les domaines des fournisseurs afin de diffuser leurs campagnes de phishing et logiciels malveillants, profitant de la moindre vigilance des cibles vis-à-vis de partenaires qu'ils connaissent bien. Les attaques les plus simples restent la compromission d'emails professionnels, un type d'attaque appelée BEC (pour Business Email Compromise). L'ingénierie sociale et se faire passer pour un fournisseur est alors un moyen de faire aboutir une attaque. L'étude Proofpoint montre bien que ce sont les collaborateurs de l'entreprise qui sont la cible numéro 1 de ces attaques et non pas l'infrastructure : 74% des attaques sur la Supply Chain issue de domaines de fournisseurs sont des attaques de phishing pour moins de 30% d'attaques provenant de malware.

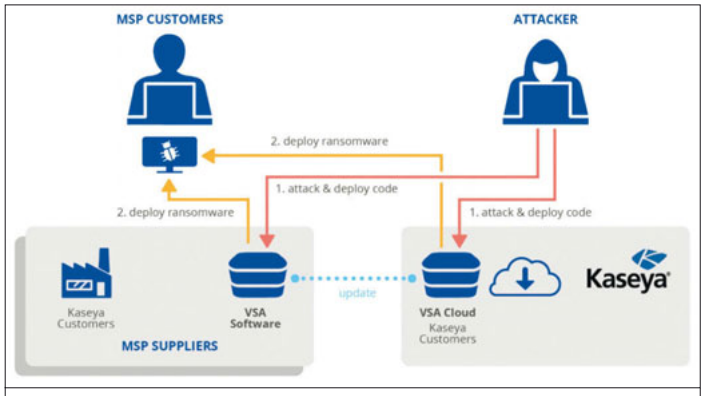
L'autre facteur qui peut potentiellement accroître le nombre d'attaques sur la Supply Chain est purement technique. De plus en plus de solutions, y compris celles déployées sur site (*on-premise*) sont connectées à Internet afin de rapatrier des données de fonctionnement auprès de l'éditeur et être mis à jour à distance et notamment appliquer des patchs de sécurité. De multiples flux de données sont ainsi échangés entre les briques d'infrastructures de tous types, depuis les appliances de stockage, les OS et les logiciels les plus divers.

C'est ainsi que ces derniers mois ont vu une augmentation sans précédent de ce type d'attaque avec l'attaque menée via SolarWinds en 2021 puis l'attaque via les outils d'audit de code source Codecov en avril 2021 et encore celle menée via l'outil de prise à distance de Kaseya.

Quelles solutions pour contrer ce risque ?

Contrer les risques d'attaques et de fuites de données liés aux attaques sur la Supply Chain n'est pas aisé. La protection périmétrique classique est sans effet lorsque l'attaquant utilise des flux de données et des adresses de partenaires autorisés pour s'infiltrer dans le système d'information. L'intelligence artificielle permet de signaler le comportement anormal d'une application ou d'un compte utilisateur qui aurait pu être compromis, mais la technologie n'est qu'une partie de la solution. Le responsable sécurité d'une grande entreprise ne peut exercer un contrôle étroit sur les briques de sécurité de l'ensemble des partenaires de son entreprise. Il lui faut adopter une autre approche pour adresser ce risque.

Philippe Proix, Expert en gouvernance de la cybersécurité-Manager de transition chez Talking Cybersecurity suggère aux grandes entreprises de mettre en place un plan d'assurance sécurité spécifique, le *PASP (Plan d'Assurance Sécurité Partenaire) : "Le PASP est habituellement composé de deux documents : Un fichier Excel de tableau de Bord et un document Word qui se basent tous deux sur l'ISO 27 001. Il s'agit de questions simples qui correspondent aux 14 thèmes de la norme et qui permettent de faire une première photographie du niveau de sécurité du fournisseur ou de la filiale."* La méthode prônée par l'expert est une démarche déclarative : le RSSI adresse le questionnaire à tous les partenaires de l'entreprise afin de disposer d'une évaluation de leur niveau de sécurité, suggérer à la direction Achat d'écarter les plus laxistes ou a minima les pousser à améliorer la sécurité de leur système d'information. *"Cette approche permet d'avoir cette photographie de l'état de l'art de la sécurité chez ce partenaire, et éventuellement de l'aider à remédier aux manques de sécurité si le questionnaire en fait apparaître. Les questions sont relativement simples mais je peux aider l'entreprise à y répondre. Après analyse des résultats, le donneur d'ordre lui accorde de 2 à 3 mois pour remédier à ces manques."* Dans certains cas, l'entreprise peut imposer un PenTest aux frais du partenaire s'il juge que cela s'impose. C'est notamment le cas de partenaires stratégiques



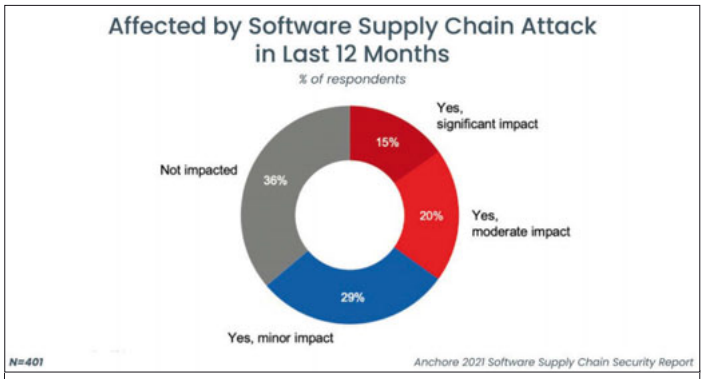
Le diagramme de l'attaque impliquant la solution VSA de Kaseya et qui a permis aux attaquants de déployer leur malware chez les clients des MSP mettant en œuvre la solution de prise de contrôle à distance. Une attaque très représentative du risque lié à la Supply Chain.

qui sont amenés à intervenir dans des processus particulièrement critiques pour l'activité industrielle ou commerciale de l'entreprise. *"Imposer un PenTest à un partenaire est une démarche bien plus coûteuse qu'un simple questionnaire mais très utile pour contrer le risque d'attaque de type Supply Chain"* souligne Philippe Proix qui ajoute : *"Cela reste une pratique exceptionnelle, car en règle générale, les entreprises font bien trop confiance à leurs sous-traitants et partenaires technologiques sur cette problématique de la cybersécurité."*

Les normes ISO sont-elles suffisantes ?

Pour les fournisseurs d'applications SaaS, l'entreprise peut se fier aux certifications de sécurité pour être certaine du sérieux de son fournisseur et surtout que celui-ci est engagé dans une démarche d'amélioration continue. A cet égard, exiger une conformité aux ISO 27001, ISO 27017 (spécifique aux services Cloud) et ISO 27018 (sur les données personnelles) est sans doute un prérequis en 2021.

Le cas des fournisseurs de services d'infrastructure dans le Cloud de type IaaS ou PaaS est un peu différent. En effet, les principaux fournisseurs Cloud affichent un impressionnant panel de certifications ISO, PCI DSS, CSA Star, SOC, etc. mais l'entreprise reste responsable de la sécurité de ses applications qu'elle déploie sur le Cloud de son partenaire et si la responsabilité de la sécurité de la plateforme est partagée entre les deux partenaires, la balance penche très largement du côté du RSSI quant à la sécurité des applications.



Selon une étude de 2021 mené par Anchore, 64% des entreprises se disent impactées de manière plus ou moins importante par des cyberattaques sur leur Supply Chain.

Témoignage Expert :

Philippe Proix,

Expert en gouvernance de la cybersécurité
Manager de transition chez Talking Cybersecurity

« Les cybercriminels visent en priorité les systèmes d'information insuffisamment sécurisés. Ceux-ci sondent les réseaux afin d'identifier les vulnérabilités de ces systèmes d'information et, s'il s'agit d'un prestataire ou fournisseur quelconque, ils s'en servent pour rebondir vers une proie plus intéressante car mieux sécurisée. C'est une démarche que l'on observe sur les attaques de ransomware depuis plusieurs années et de nombreuses entreprises sont victimes d'attaques automatiques à très large échelle et, plus récemment, par des attaques pilotées par des algorithmes d'intelligence artificielle. »
« Ce qui intéresse les attaquants, ce sont les vulnérabilités non corrigées. Un patch management insuffisamment rigoureux au niveau des applicatifs, des serveurs, des équipements réseaux et des endpoints constitue une manne pour eux. Dès lors qu'une vulnérabilité est identifiée, elle est exploitée et ceux-ci peuvent entrer dans le système d'information, explorer les ressources disponibles pour dérober des données, et éventuellement rebondir vers les systèmes des partenaires de l'entreprise. »

Vers une notation généralisée de la sécurité des entreprises

La certification est une approche qui s'est généralisée dans de nombreux domaines et imposer un label ISO 27001 de manière contractuelle à ses partenaires IT critiques est certainement une bonne pratique qui doit être étendue. Néanmoins, une telle approche a ses limites. Une certification garantit au donneur d'ordres que son partenaire dispose de processus bien définis quant à la gestion de sa sécurité, que celui-ci est engagé dans une démarche d'amélioration continue, mais ne constitue pas une garantie de l'invincibilité de ses systèmes informatiques. L'idée de noter le niveau de sécurité de chaque entreprise est née il y a quelques années, c'est ce que l'on nomme le Security Rating. Au moyen de questionnaires mais aussi de scanner de sécurité, des agences de notation réalisent un audit des ressources informatiques des entreprises afin de délivrer une note de synthèse à chaque fournisseur. Ces agences s'adressent essentiellement aux grandes entreprises mondiales qui doivent gérer des milliers de fournisseurs de par le monde et qui ont besoin de savoir où se situe leur talon d'Achille, les fournisseurs les plus faiblement protégés d'où viendra la prochaine attaque.

Les agences qui s'appuient sur des outils automatisés peuvent ajuster les notes de l'ensemble des entreprises en temps réel, en fonction des dernières vulnérabilités publiées. L'approche n'est bien évidemment pas exhaustive de la sécurité du fournisseur puisqu'outre un questionnaire déclaratif, les scanners ne peuvent auditer que les ressources IT exposées sur Internet. Néanmoins avec de tels outils, lors de la récente annonce d'une faille majeure sur Microsoft Exchange, tous les fournisseurs exploitant encore la solution et qui n'avaient pas passé de patchs correctifs ont vu leur note diminuée et le RSSI de leurs donneurs d'ordres a reçu une alerte lui indiquant la liste de ses fournisseurs exposés au risque d'attaque. Un tel outil permet à un RSSI de mettre la pression sur ses fournisseurs en leur indiquant très exactement les actions à réaliser pour remédier aux failles découvertes dans leurs systèmes informatiques.

En ce sens, la note de sécurité permet d'instaurer un cercle vertueux qui doit permettre d'élever le niveau de sécurité de l'ensemble de l'écosystème de l'entreprise et réduire ce risque d'attaque sur la Supply Chain. La cybersécurité s'affirme de plus en plus comme un différenciant compétitif pour les fournisseurs qui doivent désormais améliorer leur niveau de sécurité pour garder leurs clients et décrocher de nouveaux contrats.

LA 21

LES ASSISES

13.10.21 → → 16.10.21

/MONACO///

→ lesassisesdelacybersecurite.com

DG CONSULTANTS

COMEXPOSIUM

Ces multiples vulnérabilités qui menacent les SI

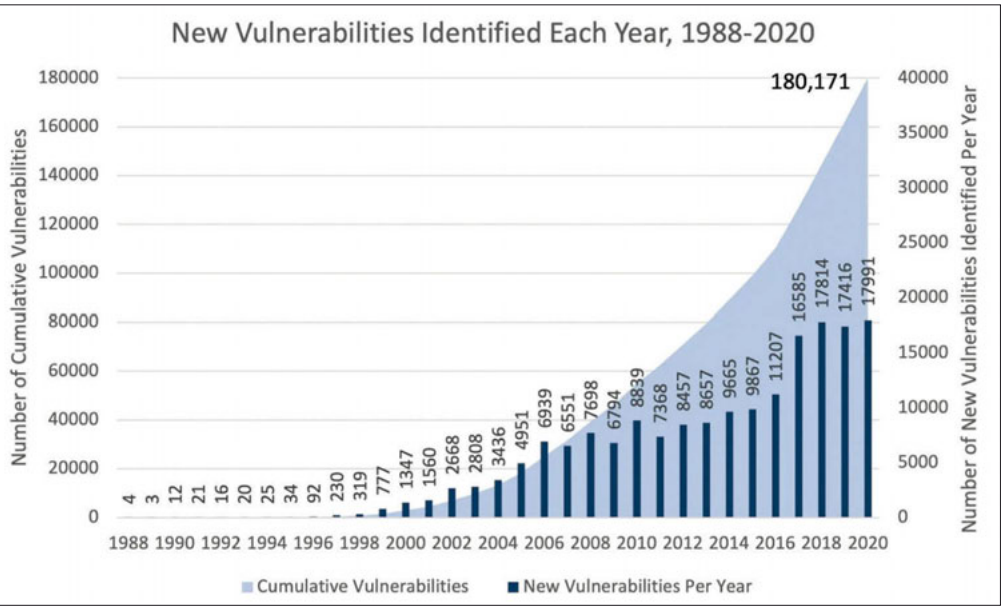
En cybersécurité, le danger est partout. Chaque équipement réseau, brique de sécurité, logiciel d'entreprise contient des failles de sécurité. Plus que jamais le RSSI doit être réactif et imposer une politique d'application des patchs de sécurité efficace et rapide pour écarter les menaces identifiées.

Par Alain Clapaud

Attaque via la messagerie et les vulnérabilités découvertes dans Microsoft Exchange, attaques par phishing, par ransomware ou encore par DDOS ou les VPN, l'actualité est particulièrement anxiogène pour le RSSI en charge de la sécurité de son entreprise. L'imagination des attaquants est infinie et nombreux sont les moyens dont il dispose pour frapper une entreprise. Contrer une attaque de type "Zero Day" est sans doute le défi le plus difficile à relever et l'entreprise ne peut compter alors que sur les mesures de prévention et son plan de gestion de crise cyber pour y faire face. Outre ce cas extrême, il est possible d'écarter de nombreuses attaques, notamment grâce à un patching ultra-réactif des briques d'infrastructures et des endpoints dès que les correctifs sont mis à disposition par les éditeurs. En outre, il faut se méfier des applications non maintenues que personne ne songe à remplacer. Celles-ci sont truffées de vulnérabilités non corrigées qui peuvent être mises à profit par un attaquant pour rebondir vers des ressources IT plus critiques.

Le nombre de CVE reste au plus haut

Au Top 10 des vulnérabilités (ou CVE pour Common Vulnerabilities and Exposures) les plus importantes publiées en 2020, les chercheurs d'IBM X-Force ont classé celle portant sur le contrôleur Citrix ADC comme la plus dangereuse, car à l'origine de 25% de l'ensemble des compromissions détectées par IBM en 2020. La seconde porte sur la plateforme PHP et plus particulièrement sur le framework ThinkPHP, notamment utilisé sur certains objets connectés. Viennent ensuite dans ce classement une faille découverte dans Apache Struts initialement constatée en 2006 (!) mais toujours exploitée, une faille sur GNU Bash, sur Microsoft Remote Desktop Services ou encore dans FortiOS, etc. Les failles sont très diverses, touchent tant les solutions d'éditeurs commerciaux que des briques Open Source, des solutions d'informatique d'entreprise mais aussi IoT. Ce classement montre aussi la difficulté des entreprises à maintenir un niveau de patching correct des solutions qu'elles mettent en oeuvre, soit par négligence mais aussi



Le nombre de vulnérabilités déclarées par les éditeurs ou des tiers reste à des niveaux très élevés. Ce qui rend le patching rapide des équipements et logiciels en production absolument indispensable.

Source : IBM X-Force Red

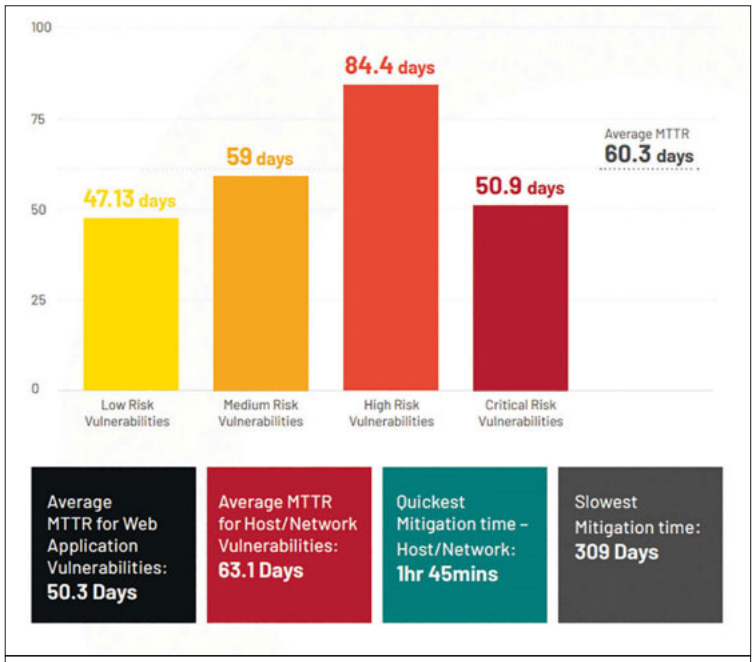
à cause des dépendances multiples liées à de vieilles versions de briques d'infrastructure, ou encore l'impossibilité de mettre à jour certains dispositifs IoT.

Des attaquants de plus en plus réactifs à l'actualité

Non seulement les vulnérabilités sont nombreuses, mais le rapport relatif aux menaces du premier quadrimestre 2021 rédigé par ESET Research, a fait apparaître l'accroissement de la rapidité d'exploitation des vulnérabilités et des erreurs de configuration. Après une grande vague d'attaques liées à la pandémie de COVID-19, les attaquants ont été très prompts à exploiter les vulnérabilités permettant la prise de contrôle des serveurs Microsoft Exchange. Les chercheurs ont ainsi identifié plus de 10 groupes de pirates différents qui ont probablement exploité cette chaîne de vulnérabilités. De même, la première partie de l'année 2021 a vu une recrudescence de détournement du protocole d'accès à distance (RDP) avec de vastes attaques par brute force pour accéder aux serveurs ainsi exposés sur Internet. En parallèle, les chercheurs d'ESET Research ont noté l'augmentation du nombre de menaces liées aux cryptomonnaies ainsi qu'une forte hausse des détections de malwares bancaires Android.

Les systèmes OT concernés à leur tour

Le système d'information est concerné dans son ensemble par cette problématique de vulnérabilités à patcher au plus vite, y compris son volet industriel, l'OT (Operational Technology). Dans son rapport biannuel "ICS Risk & Vulnerability Report" du premier semestre 2021, l'éditeur Claroty pointe ainsi la hausse alarmante du nombre de vulnérabilités signalées sur les systèmes industriels. 637 vulnérabilités ont été signalées par 76 fournisseurs au premier semestre 2021, contre 449 un an plus tôt. 70,93% de ces vulnérabilités ont été classifiées de niveau haut ou critique.
Selon les chercheurs de Claroty, plus de 80% des vulnérabilités sont découvertes par des sources externes aux fournisseurs de solutions industrielles, preuve que ces derniers doivent encore investir massivement afin d'améliorer la sécurité de leurs produits, mais aussi leur capacité à détecter et corriger les vulnérabilités qui les affligent. ■



En 2021, le délai moyen de résolution des failles de sécurité (le MTTR pour Mean Time to Remediate) dépasse encore les 80 jours lorsque le risque est jugé élevé et reste supérieur à 50 jours pour une faille critique. Un délai pendant lequel l'attaquant peut exploiter au mieux sa faille "Zero Day".

Source : Edgescan, 2021

L'actu, les dossiers de la
CYBERSÉCURITÉ
www.solutions-numériques.com/securite
Abonnez-vous à la **Newsletter** *du lundi*

La cyber-assurance
à l'heure du ransomware

Dans un contexte où les cyber-attaques contre les entreprises ne cessent de s'accroitre, la notion d'assurance cyber semble une évidence. De nombreux grands-comptes ont franchi le pas. Reste à diffuser cette couverture du risque cyber plus largement dans les entreprises françaises.

Par Jérôme Saiz

Le manifeste publié par Hexatrust en septembre 2020 explicitant 5 vœux pour une autonomie numérique pour l'Europe défend l'idée d'une Europe de la cybersécurité, d'un plan d'équipement cyber et un dispositif de soutien aux PME du secteur. Il inclut aussi un volet dédié à la cyber-assurance. Les auteurs du manifeste militent en faveur d'une couverture assurantielle du Cyber-risque, notamment afin de permettre aux TPE et PME de franchir le pas et se protéger enfin du risque cyber.

Des contrats très spécifiques

En attendant qu'une telle idée chemine, les contrats d'assurance cyber actuellement proposés sont souvent très spécifiques à l'entreprise. Souscrire à un contrat souvent complexe est un processus long qui exige une implication plus forte non seulement de la part du DSI et du RSSI, mais également du Risk Manager, du responsable assurances, du CIL (et bientôt Data Privacy Officer !), et potentiellement du responsable juridique ou de la RH. Il s'agit donc d'un projet très engageant qui doit être mené comme tel, notamment en créant une équipe pluridisciplinaire dédiée pour le mener à bien.

L'étape la plus structurante d'un tel projet est de loin la réponse au questionnaire d'assurance : l'entreprise va devoir y exposer son organisation et préciser à la fois les mesures de protection existantes mais aussi ses plans de réponse en cas de sinistre. C'est pourquoi bien que nous ayons choisi de placer cette étape assurantielle en début de processus, durant la phase d'organisation, elle exige toutefois qu'un premier travail de fond ait déjà été réalisé, tant en matière de cartographie des risques que de réponse aux incidents.

Idéalement, et puisque nous présentons la sécurité telle un processus itératif, le volet assurantiel sera donc traité au second passage par cette phase d'organisation.

Une couverture en trois volets

En cas de déclenchement d'une crise, le contrat d'assurance cyber couvrira l'entreprise sur trois volets principaux :

• Tout d'abord en prenant en charge les frais de réponse à incident et de gestion de crise (honoraires de consultants et de prestataires dans les domaines légaux, forensiques, de la communication, etc.).

• Ensuite un second volet pourra être activé en cas de réclamation de tiers à l'encontre de l'entreprise, qu'il s'agisse de clients ou d'employés. Celle-ci, en effet, pourra être mise en cause pour négligence ou non-respect de ses obligations légales et devra répondre juridiquement, ce qui entraînera des frais.

• Enfin, l'assurance pourra prendre à sa charge les frais supplémentaires induits par la poursuite de l'activité durant le sinistre, tels que la location de nouveaux locaux, de nouveaux équipements informatiques, le recours à des sous-traitants pour tenir ses engagements, etc.

A noter : le contrat d'assurance pourra également prendre en charge les frais spécifiques liés à une attaque par un ransomware, qu'il s'agisse de rembourser les frais d'un consultant en sécurité chargé de négocier avec les pirates, ou bien la rançon elle même (y compris les frais bancaires si l'entreprise a dû emprunter !). Bien entendu, et à la suite des grandes campagnes de ransomware durant 2017, ces primes spécifiques peuvent être élevées tant le risque est désormais fort.

Des clauses secrètes

Certaines clauses d'une police de cyber assurance doivent rester secrètes sous peine d'être nulles. C'est notamment le cas de la clause de protection contre les ransomwares (clause de cyber extorsion). Cela implique, pour l'entreprise, d'être en mesure de créer un groupe de travail "cyber-assurance" dont l'activité restera secrète vis-à-vis des autres collaborateurs. Seules les personnes-clés de l'entreprise pourront être mises au courant et généralement seulement au moment du déclenchement de la crise.

Au moment de la crise l'assureur sera souvent le premier partenaire extérieur alerté. Il permettra à l'entreprise de bénéficier d'une assistance immédiate pour la suite des opérations. Viennent ensuite généralement le temps des notifications légales, par exemple auprès de la CNIL s'il s'agit d'un vol de données personnelles ou des autorités si l'entreprise jouit d'un statut particulier (Opérateur d'Importance Vitale, entreprise de défense, etc.). Dans tous les cas, l'assureur sera impliqué dès le début de la crise et jusqu'à sa résolution, ce qui en fait un partenaire de premier plan de l'entreprise. A ne pas négliger, donc!

Fiches sociétés

Fournisseurs

Qui fait quoi ?

Une sélection de 81 entreprises incontournables, spécialisées dans la cybersécurité : leaders ou challengers, offreurs de solutions, de services, de formation aux entreprises et organisations.

Sociétés		Solutions	Services	Conseil	Formation	Distribution
6CURE	p.37	●				
ABBAKAN	p.38		●	●	●	●
ACCEIS	p.39			●	●	
ACTIVANOS	p.40	●	●	●		
ALLISTIC	p 41		●	●	●	
ALMOND	p.42			●	●	
ANTEMETA	p.44		●			
ARCSERVE	p.46	●				
ATEMPO	p.48	●				
AVANT DE CLIQUER	p.50	●				
AXIANS	p.49		●	●		
BITDEFENDER	p.51	●				
CHAMBERSIGN France	p.52		●			
CHECK POINT Software Technologies	p.54	●				
CS GROUP NOVALY'S	p.56	●	●	●		
CYBEREASON	p.58	●				
CYBERRES CyberRes	p.53	●				
DARK TRACE	p.60	●				
DIGITEMIS	p.62	●	●			
DYNAMIT SOLUTIONS & SERVICES	p.64		●			●
EIFFAGE Energie Systèmes-Clemessy	p.66		●	●	●	
ESET	p.67	●				
FORTINET	p.70	●	●			
F-SECURE	p.69	●				
GATEWATCHER	p.72	●				
GLOBALSIGN	p.74	●				
HOLISEUM	p.76	●	●	●		
HS2	p.78				●	
HUB ONE	p.80		●			
ILEX	p.82	●				
INFOCLIP	p.83		●	●		
INFINIGATE	p.55					●
IN GROUPE	p.84	●				
ITRUST	p.86	●	●			

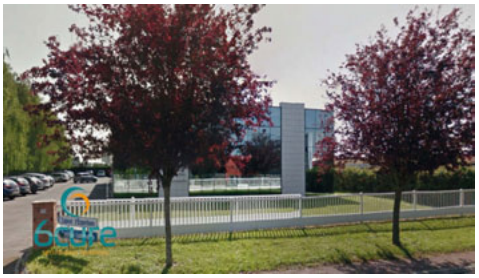
Sociétés		Solutions	Services	Conseil	Formation	Distribution
IVANTI	p.88	●				
KASPERSKY	p.90	●				
KEMP TECHNOLOGIES Ltd	p.89	●				
KEYSIGHT	p.92	●				
KUDELSKI SECURITY	p.94		●	●		
LASTPASS BY LOGMEIN	p.96	●				
MAILINBLACK	p.98	●				
METSYS	p.99		●	●		
MICROPOLE - GO CLOUD & SECURITY	p.100		●	●	●	
MIEL	p.102				●	●
NAMESHIELD	p.104	●	●	●		
NEOWAVE	p.106	●				
NETWRIX	p.108	●				
OKTA France	p.110	●				
ONE IDENTITY	p.112	●				
OODRIVE	p.114	●				
OXIBOX	p.111	●				
PING IDENTITY	p.116	●				
POST TELECOM	p.118		●			
PRIM'X	p.120	●				
QUALYS TECHNOLOGIES	p.123	●				
QUERY	p.125	●				●
QUODAGIS Digital Security	p.124	●	●	●		
RAMPAR	p.126		●	●	●	
ROHDE & SCHWARZ CYBERSECURITY	p.127	●				
RUBYCAT	p.128	●				
SANS INSTITUTE	p.130				●	
SCASSI Cybersecurity GROUP	p.132	●		●	●	
SCILLE-PARSEC	p.122	●	●			
SERMA SAFETY & SECURITY	p.134	●	●	●		
SIEMENS	p.135	●	●			
SONICWALL	p.136	●				
SOPHOS	p.137	●				
STORMSHIELD	p,138	●				
SYNETIS	p.139		●	●	●	
SYSTEMIS	p.140	●		●		
THALES	p.142	●				
THEGREENBOW	p.144	●				
TIXEO	p.143	●				
TREND MICRO	p.146	●				
UPPER-LINK	p.148	●				
USERCUBE	p.149	●				
VENAFI	p.150	●				
WALLIX	p.152	●				
WATCHGUARD	p.154	●				
WOOXO	p.158	●				
YESWEHACK	p.156	●				

Annonceurs Publicité

Les Assises p.31
Cheops Technology p.19
DELL p.2
Pradeo p.5

Notre métier : protéger les infrastructures réseau et DNS

6cure propose des solutions de protection contre les attaques informatiques, particulièrement adaptées aux « dénis de service distribués » (DDoS) et aux menaces DNS. Elles permettent de détecter et de neutraliser en temps réel les atteintes malveillantes multi formes et multi vecteurs ciblant la disponibilité et l'intégrité des services critiques. Ces outils de protection répondent aux nouvelles logiques d'attaques plus ciblées, efficaces, dévastatrices et menées de plus en plus facilement par des organisations cybercriminelles structurées et professionnalisées.



Société : 6CURE
Adresse : 701, rue Léon-Foucault
Z.I. de la Sphère
14200 Hérouville Saint-Clair
Tél. : 0 826 387 373
Mail : **contact@6cure.com**
Site web : **www.6cure.com**

Spécialisations

Lutte contre les attaques DDoS
Protection des infrastructures DNS

Chiffres clés

Effectifs : 20-25

Historique

Création en 2010

Dirigeant
Fabrice CLERC
CEO

Contacts
Direction commerciale
sales@6cure.com

Direction technique
ddos-mitigate@6cure.com

Produits / Services

- 6cure Threat Protection® : solution de protection contre les attaques DDoS de L2 à L7
- 6cure DNS Protection® : solution de mitigation des menaces DNS
- 6cure DDoS Assessment® : test de résistance aux DDoS
- Threat Intelligence

Applications

- Protection des infrastructures télécom et hébergement
- Sécurisation des infrastructures DNS
- Fourniture de services de sécurisation anti-DDoS

Certifications

- Label France Cyber Sécurité
- Label ECSO
- Référencement : fournisseur OTAN

Références clients

Liste non exhaustive
- Orange, Monaco Telecom, IMS Networks, Offratel,…
- OIV…

abbakan
an Ingram Micro Company

Société : Abbakan - Ingram Micro Security
Adresse : 11-15, quai du Président-Paul-Doumer, 92400 Courbevoie
Tél. : +33 1 55 70 21 60
Mail : **commercial@abbakan.com**
Site Web : **www.abbakan.com**

Spécialisations

Audit, Scanner de vulnérabilités, WebApplication Firewall, Web Services Firewall, Next-Gen Firewall, SSO, Endpoint Protection EDR, XDR, SASE, SD-Wan, SIEM, Sécurisation OT…

Chiffres clés

CA : 130 M€ (2020)
Effectifs : 46

Dirigeants

Steeve AHACHE
Directeur général

Franck NAVARRO
Directeur division Cybersécurité

Contacts

Sénaporak LAM
Directeur commercial

David BREBANT
Directeur commercial

Division Cybersécurité du groupe Ingram Micro, au service des revendeurs et de leurs clients

Désormais Division Cybersécurité du groupe Ingram Micro, Abbakan est un distributeur français de solutions à valeur ajoutée, expert sur le marché de la sécurité, du réseau et du eBusiness. Abbakan propose un large éventail de services destinés à aider les revendeurs et leurs clients sous la forme de partenariats permettant de bénéficier d'informations privilégiées. Outre le support technique, les services proposés par Abbakan portent sur la formation et le transfert de compétences, sur le conseil et les audits, sur l'aide à l'installation et à la configuration.

Marques distribuées

F5 Networks, Fortinet, McAfee, Forcepoint, Cisco Secure, Kaspersky, Bitdefender, FireEye, Thales, Rapid7, F-Secure, Stormshield, Keysight Technologies, Lastpass, AppviewX, Bufferzone, Sailpoint, Sealpath, Skybox Security,Thycotic, Help Systems

Services

Avant-Vente, Démo, POC, intégration, consulting (audit de sécurité…), services managés (Firewall as the service).

Acteur de bout en bout du cycle de vente

« Le développement des compétences en termes de cybersécurité constitue un axe stratégique pour le groupe Ingram Micro, que Ingram Micro France a concrétisé en mai 2019 par l'acquisition du distributeur Abbakan.

Ainsi, depuis plus de deux ans, les équipes Ingram Micro et Abbakan combinent leur expertise et leurs engagements afin d'optimiser la qualité du service qu'elles apportent à leurs partenaires respectifs. Au-delà des produits et solutions de nos partenaires éditeurs, Ingram Security est en capacité d'accompagner ses revendeurs de la génération de leads, audit de sécurité chez leurs clients jusqu'à une intégration totale ou partielle des solutions vendues, devenant ainsi un acteur de bout en bout du cycle de vente. »

Sénaporak LAM, *Directeur commercial – Abbakan*

NOTRE EXPÉRIENCE

Nos **15 ans d'expérience** nous permettent aujourd'hui de nous positionner en tant que **distributeur expert et reconnu** sur le marché de la cybersécurité. Nos éditeurs sont présents dans toutes les catégories représentées par le Gartner, ce qui nous offre **une représentation à 360°** de la sécurité informatique.

NOTRE ENGAGEMENT

Nous avons été élu à plusieurs reprises **«Best Value Added Distributor»** par nos partenaires et nous nous engageons grâce à notre **large éventail de services**, à vous accompagner dans vos projets de sécurité IT quels qu'ils soient. Nous mettons tout en œuvre pour que votre business soit synonyme de succès.

NOTRE EXPERTISE

Toujours soucieux de répondre au mieux à vos attentes, nous bénéficions d'**équipes dédiées compétentes, qualifiées et certifiées**. Nos services technique, avant-vente, marketing et commercial sont répartis par marque pour vous permettre de disposer d'interlocuteurs experts.

NOTRE VOCATION

Notre **vocation de start-up**, animée par une vision entrepreneuriale forte et le dynamisme de nos équipes, nous permet de **personnaliser notre modèle de distribution**, de façon réactive, et de nous **adapter à vos besoins et demandes**, sans contrainte et avec une connaissance du marché local renforcée.

Centre d'expertises en cybersécurité

Créé à Rennes en 2015, ACCEIS est doté du visa de sécurité de l'ANSSI. ACCEIS possède l'agrément CESTI software et la qualification PASSI.

ACCEIS s'est positionné comme un partenaire global de la sécurisation des activités auprès de ses clients et est devenu un acteur reconnu sur le plan national de la communauté cybersécurité.

Notre 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.

Société : ACCEIS
Adresse : 12 rue du Bourg-Nouveau, 35000 RENNES
Tél. : 06 64 59 15 50
Mail : **christophe@acceis.fr**
Site web : **www.acceis.fr**

Spécialisations

Audits techniques, accompagnement et conseil, gestion des incidents de sécurité, certification, gouvernance. L'équipe d'ACCEIS, composée d'experts pluridisciplinaires en cybersécurité, est capable d'intervenir à la fois sur des missions techniques exigeantes comme sur des sujets organisationnels et stratégiques à forts enjeux.

Chiffres clés

CA : 2021 : 1,2 M€
2020 : 760 K€
2019 : 566 K€

Effectifs : 20, en pleine croissance

Dirigeants

Gwenn FEUNTEUN
Président, co-fondateur

Yves DUCHESNE
Directeur général, co-fondateur

Christophe BEUCHARD
Directeur commercial & marketing associé

Contact
Christophe BEUCHARD
Directeur commercial & marketing associé
christophe@acceis.fr
06 64 59 15 50

ACCEIS est un centre d'expertises en cybersécurité fondé par deux experts du domaine, Gwenn Feunteun, Président et Yves Duchesne Directeur général et rejoints par le 3e associé, Christophe Beuchard, Directeur commercial et marketing.

ACCEIS a pour objectif d'accompagner de façon globale ses clients à la sécurisation de leurs activités et leur apporter les compétences hautement qualifiées grâce à l'équipe d'experts triée sur le volet.

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 des institutionnels.

Labels

Qualification PASSI

- ACCEIS bénéficie de la reconnaissance des plus hautes instance étatiques et est prestataire qualifié par l'**ANSSI** pour la réalisation d'audits de sécurité des systèmes d'information **(PASSI RGS),** sur l'ensemble des portées proposées par le référentiel (tests d'intrusion, audits de code source, audits de configuration, audits d'architecture, audits organisationnels et physiques).
- Cette qualification démontre notre excellence technique et nous permet également d'intervenir sur des marchés réglementés.

Agrément CESTI

- ACCEIS dispose également d'un 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 solutions qu'ils développent et commercialisent.

Références clients

Alcatel, Altenov, Arcal, Avril, Biocoop, Biosency, DGFIP, Eureden, Euro-Information, Habitat 44, Le Duff, MGDIS, NEHS, Oxyane, Kéolis, Sodexo, Société Générale, Snef…

Société : ACTIVANOS
Adresse : 128 rue La Boétie
75008 PARIS
Mail : **contact@activanos.fr**

Spécialisés dans les technologies Microsoft et matérielles les plus récentes, nous mettons notre expertise au service des gouvernements, des entreprises, des banques et des collectivités.

Nous vous aidons à mettre en œuvre les meilleures pratiques d'architectures à sécurité renforcée afin d'assurer progressivement une protection optimale évolutive de vos données et processus.

Chiffres clés

Effectifs : nc

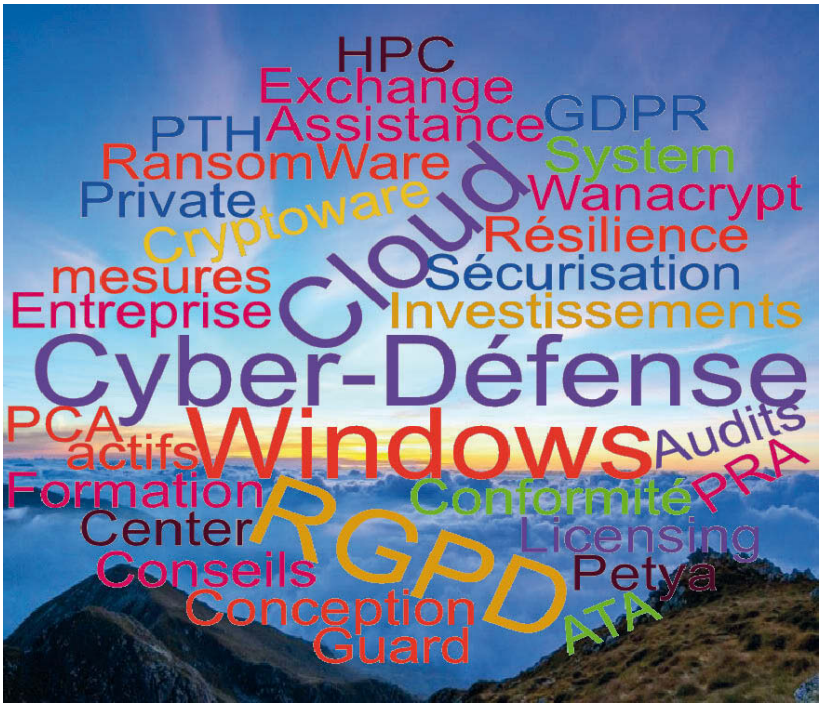
Historique

Société créée en 2004 par d'anciens constructeurs d'ordinateurs français qui n'ont cessé d'être à la pointe de l'innovation dans le numérique.

Dirigeant

Daniel BONNET
Président
daniel.bonnet@activanos.com

Jean-Daniel HENNION
Architecte systèmes senior
jeandaniel.hennion@activanos.com



Une gamme complète d'offres

Services in situ et en ligne

Nos offres de mise en sécurité conforme au RGPD se répartissent entre :

- audits multi-niveaux, à votre convenance
  - Capture de l'existant
  - Scoring, Validation, Recommandations
  - Plan segmenté d'actions prioritaires, moyen et long terme.
- mise en sécurité conforme et évolutive
  - 149 thématiques croisées : contrôles et configurations idempotentes
- formation et information continue des administrateurs et des développeurs aux meilleures pratiques internationales et aux risques émergents.

Solutions intégrées, sur mesure et clefs en mains :

Nous fournissons également des systèmes sur mesure complets, dimensionnés aux besoins réels de nos clients et sécurisés par design.

Nous concevons et intégrons :

- ses grappes HPC
- des grappes de serveurs d'infrastructure en nuage durcie, intrinsèquement conformes aux requis du RGPD, résilientes et redondantes, cryptées de bout en bout en multi-niveau, à réplications multisites synchrones et/ou asynchrones.

Ces systèmes sont fournis avec l'ensemble des services complémentaires, de la formation avancée en systèmes au support temps réel.

**Nous recherchons des sites de référence, de typologies et de tailles variées, pour assurer la qualité et l'universalité du développement « Agile » de notre robot logiciel architecte systèmes expert.*

Protéger votre activité, vos données et votre savoir-faire

Partant du constat que la meilleure protection pour une entreprise est celle qui tient compte de son contexte et de ses enjeux, Allistic accompagne des sociétés et collectivités dans leur transformation digitale en répondant à leurs enjeux de sécurisation des données.

Société : ALLISTIC
Siège social : 165 avenue de Bretagne, 59000 LILLE
Tél. : 03 74 09 61 00
Mail : **contact@allistic.fr**
Site web : **https://www.allistic.fr/**

Spécialisations

- **Gouvernance, risques et conformité**
- **Audits et tests d'intrusion**
- **Architectures sécurisées**
- **Sensibilisation et formation**

Historique

Créée en 2018 par Jean-Michel DOS SANTOS, Allistic compte plus d'une dizaine de collaborateurs qui cumulent de nombreuses années d'expériences.

Dirigeant
Jean-Michel DOS SANTOS
Fondateur et dirigeant
jmdossantos@allistic.fr
Tél. : 03 74 09 61 00

« La meilleure protection pour une entreprise est celle qui tient compte de son contexte et de ses enjeux. C'est la raison d'être d'Allistic.
En abordant la problématique de la protection de l'entreprise dans sa globalité, Allistic permet à ses clients d'aligner les investissements et les efforts sur une ambition de sécurité.
Nous avons constitué une équipe dotée des compétences nécessaires à la prise en charge des problématiques de cybersécurité pour les entreprises et les collectivités. »

Offres

Gouvernance et conformité

Maîtrisez et pilotez la sécurité des données de votre entreprise ou collectivité, gérez vos risques numériques, protégez les données personnelles.

- **Audit organisationnel :** évaluer les mesures de sécurité et de conformités face aux multiples réglementations.
- **Analyse de risque :** identifier vos risques et mettre en œuvre les mesures de sécurité adéquates.
- **Conformité :** ISO27001, RGPD, LPM, HDS, NIS etc.
- **Gestion de crise et continuité d'activité :** disposer d'un référentiel qui vous permet d'accroître la résilience de votre entreprise et maintenir votre croissance.
- **Coaching :** faire émerger vos impératifs de cybersécurité et renforcer vos compétences.
- **RSSI On-Demand :** à temps partagé ou à temps plein, disposer d'un RSSI de manière flexible et agile.

Sensibilisation et formation

Aidez vos collaborateurs à comprendre les enjeux de cybersécurité et adoptez les bons réflexes.

- **Solutions intra-entreprise**
- **E-learning**

Audits et Tests d'intrusion

Évaluez le niveau de sécurité de vos applications, sites web et infrastructures. Validez le respect des bonnes pratiques et des exigences réglementaires.

- **Pentest**
- **Audit d'infrastructure**
- **Revue de configuration**
- **Audit de code**
- **Forensic**

Architectures sécurisées

Co-construisez une architecture robuste, évolutive et simple à maintenir

- **Conception d'architectures sécurisées :** créer des infrastructures et architectures cloud (GCP, AWS, Azure…), On-premise ou hybrides sécurisées et adaptées à vos besoins.
- **Accompagnement à la mise en œuvre :** intégrer la sécurité dans vos projets.
- **Audit de l'existant :** valider et améliorer la sécurité de vos systèmes d'information

Points forts

- Cabinet indépendant
- Prestations de proximité
- Accompagnement adapté aux entreprises et aux collectivités.
- Consultants expérimentés et certifiés.

Certifications

- ISO27001 Lead Auditor, Lead Implementor
- ISO27005 Risk Manager
- CEH - Certified Ethical Hacking
- ITIL V3

CEH Certified Ethical Hacker — ITIL — PROFESSIONNEL RÉFÉRENCÉ CYBERMALVEILLANCE.GOUV.FR Assistance et prévention du risque numérique

almond

Société : ALMOND
Adresse : bât. CRISCO DUO
7 avenue de la Cristallerie
92310 Sèvres
Tél. : 01 46 48 26 00
Mail : **contact@almond.consulting**
Site web : **https://almond.consulting**

Almond est un acteur français indépendant majeur dans l'audit et le conseil, en cybersécurité, Cloud et infrastructures. De l'innovation technologique à la modernisation du Système d'information, sa mission est d'accélérer l'évolution de ses clients en apportant une vision stratégique pragmatique. Almond les accompagne sur toutes les phases de leurs projets, de la définition de la stratégie IT et métier jusqu'à la mise en œuvre de plans de transformation et l'intégration de solutions. Les équipes Almond développent pour chaque client une approche sur-mesure et garantissent un total engagement pour la réussite de leurs projets.

Spécialisations

Audits de sécurité :
d'intrusion, audits de code source, audits de configurations audits d'architecture, audits de sécurité physique et organisationnelle, *Social engineering*, Forensic

SOC / CERT CWATCH :
réponse à incidents de sécurité, services managés de détection d'incidents, scan et gestion de vulnérabilités, *Threat intelligence* conseil et audit en organisation du SOC / C-SIRT, *Security Rating.*

Sécurité des infrastructures :
architecture sécurité et réseau : hébergement, accès internet, défense en profondeur, gestion des identités et des accès (IAM et IDaaS), contrôle et sécurisation des applications SaaS, sécurisation des terminaux dans toutes les situations de mobilité.

Accompagnement RSSI – analyse de risques – sensibilisation – gouvernance de la sécurité – résilience – gestion de crise – certification PCI DSS – ANJ – conformité ISO27001 – HDS – RGPD – LPM – RGS

Chiffres clés

CA : 2020 – 19 M€
Effectifs : 180 collaborateurs
Paris, Nantes, Strasbourg, Lyon, Genève

Offres

Almond est l'un des acteurs majeurs de la sécurité en France, en accompagnant ses clients de façon transverse sur les volets organisationnels (conformité, gouvernance) et opérationnels (audit et tests d'intrusion, infrastructure de sécurité, SOC – CERT) :

Offensive Security – Utiliser les techniques des cybercriminels avec pragmatisme et méthodologie : tests d'intrusion, audits sécurité de code source, d'architecture, de configuration, physique, reverse engineering, social engineering, forensic.

Governance & Risk management – Organiser la défense du SI et maîtriser les risques : gouvernance de la SSI, analyse de risques, sensibilisation, accompagnement à la mise en œuvre de solutions de sécurité, audits organisationnels, PCA, PRA, Gestion, Tests et Exercices de Cyber-Crise, RSSI as a Service

Infrastructure Security – Concevoir et déployer les infrastructures de Sécurité : conception d'architecture technique sécurité et réseau (Cloud et sécurité des données, IAM, IDaaS, etc.), gestion de projets sécurité (AO, choix de solutions, industrialisation et pilotage, etc.), expertise technique sécurité

Compliance – Atteindre, maintenir et démontrer la conformité : mise en conformité PCI DSS, ANJ, LPM, ASIP, ISO27001, DCP. Cartographie et conformité au RGPD, audits de conformité aux référentiels internes et sectoriels, sécurité de l'Entreprise étendue (audits des fournisseurs de services)

SOC CERT CWATCH – Détecter et agir contre les attaques : services SOC/CERT, réponse à incidents de sécurité, services managés de détection d'incidents de sécurité internes et externes, service de protection (scan et gestion de vulnérabilités, gestion solutions EDR), *Threat intelligence* tactique, conseil et audit en organisation du SOC/C-SIRT

Solutions

SECURITY RATING almond

Le principe du *Security Rating* est de produire une note représentant la performance et la maturité cybersécurité d'une organisation par une évaluation automatisée, continue et reproductible sur la base de données observables publiquement.

Boost your cyber experience

BYCE est notre e-learning de sensibilisation à la sécurité de l'information, prêt à l'emploi et disponible en SaaS.

Des modules courts qui vont susciter la compréhension et l'adhésion de vos collaborateurs, écrits par nos experts et customisés par des spécialistes de la psychologie cognitive.

Certifications

- Qualifié PASSI pour les activités de tests d'intrusion, d'audits techniques (architecture, configuration, code source d'application), et d'audits de sécurité opérationnelle et physique.
- Détenteur du label France Cybersecurity.
- PCI QSA Company, qualifié pour mener les audits de certification du standard PCI DSS depuis 2010.
- Habilité en tant qu'auditeur par l'ANJ pour mener les audits de certification auprès des opérateurs de Jeux en Ligne.

Dirigeants

Olivier PANTALÉO
Associé en charge de la Cyber-sécurité
opantaleo@almond.consulting

Michael BRIQUET
Associé en charge du Commerce
mbriquet@almond.consulting

Historique

2021 – Ouverture de la première agence à l'international à Genève et ouverture d'une agence à Lyon.

2021 – Apax Partners prend une participation minoritaire dans le groupe Hifield, société mère d'Almond, afin d'accompagner son fort développement en France et en Europe.

almond

Transform, Secure & Beyond

Avec Almond, optez pour une maîtrise de vos opérations et de votre stratégie SSI

› Nos expertises

- Information Security
- Digital & Technology
- Almond Institute

› Nos services & solutions

- CWATCH
- Boost your cyber experience
- SECURITY RATING

› Nos labels, certifications et habilitations

PRESTATAIRE RÉFÉRENCÉ CYBERMALVEILLANCE.GOUV.FR – PCI DSS COMPLIANT – FRANCE CYBER SECURITY – VISA DE SÉCURITÉ – OPÉRATEUR AGRÉÉ ANJ

Paris | Nantes | Strasbourg | Lyon | Genève

https://almond.consulting

ANTEMETA

Spécialiste Infrastructure & Cloud Computing, AntemetA accompagne ses clients depuis 25 ans dans l'évolution et la digitalisation de leur système d'information. Cet accompagnement a lieu de la réflexion à la mise en place de projets de refonte d'infrastructures en environnement Datacenter, jusqu'à son maintien en condition opérationnelle tout en conservant un service de proximité au travers de nos 7 agences. AntemetA ne cesse de se diversifier pour répondre au mieux aux besoins évolutifs de ses clients. Par ces expériences, nos expertises se sont par conséquent élargies et s'articulent dorénavant autour de 5 piliers essentiels aux Systèmes d'Informations des entreprises.

Réseau & Sécurité / Infrastructure / Cyber-Sécurité / Gestion de données / Plateformes & Solution

Société : AntemetA
Adresse : 5 rue Jacqueline-Auriol, 78280 Guyancourt, France
Tél. : 01 30 62 33 22
Mail : **info@antemeta.fr**
Site web : **www.antemeta.fr**

Spécialisations :

Société française présente sur tout le territoire, AntemetA est spécialiste de projets en environnement datacenters, infrastructure et Cloud.

Chiffres clés

CA : 90 M€

Effectifs : 300 employés répartis dans 7 agences en France

Date de création : 1995

Nombre de clients : 1 000

Dirigeant

Stéphane BLANC
Président-fondateur

Contact
Ronan DACQUAY
Directeur Marketing et Communication
ronan.dacquay@antemeta.fr
01 30 62 33 22

Offres

Suivant les attentes du marché et de nos clients, nous avons développé ArcanA, un catalogue d'offres et de services à la demande cohérents, incluant une offre Cloud souverain.

De manière détaillée, les 5 piliers autour desquels s'articulent nos expertises comprennent les services et solutions suivants :

- Réseau & Sécurité :
  SD-Wan, FAI, RIPE, Telco, LAN
- Infrastructures :
  Stockage, Flash, SAN, Virtualisation, Serveurs, PRA, Réplication, IaaS, Compute, NAS, Hyperconvergence
- Cyber-Sécurité :
  ISO 27001, PSSI, SIEM, SOC, Chiffrement, Bastion
- Gestion de données :
  Sauvegarde, Archivage, Gouvernance, BaaS, PRAaaS, GDPR
- Plateformes & Solutions :
  Verticalisation, SAP, MCO, Azure

Nos différences

Maîtriser de bout en bout les technologies et ainsi concevoir et maintenir des infrastructures rentables, évolutives et au service du développement des organisations.

- Un haut niveau d'engagement : AntemetA s'engage sur les performances attendues, le niveau de service Cloud et la continuité de service.
- Un service clients guichet unique : autorité de maintenance sur les produits commercialisés, AntemetA assure le support niveau 1 et 2 en 24/7 et le MCO de ses services via un point de contact unique (accès centralisé aux services client et Cloud Hybride via un portail).

Solutions et services

Nos offres de Cloud et de services managés sont conçues pour répondre aux besoins de résilience, de sécurité et de confidentialité de nos clients. Par la contractualisation d'un niveau de service et non de la fourniture de matériel ou de puissance informatique, nos clients peuvent se concentrer sur l'essentiel : le développement de leur activité.

De plus, notre sérieuse appétence pour la cybersécurité garantit à nos clients un accompagnement global sur ces enjeux importants. Ils peuvent ainsi réduire la surface d'exposition aux risques par l'adoption des meilleures pratiques en termes de gestion du risque cyber.

Certifications

Certifié 100 % hébergée en France ; AFAQ ISO 27001 ; ITIL ; Hexatrust ; labellisé utilisé par les Armées françaises.

Références clients

Engie Cofely ; Alten ; Picard ; Société du Grand Paris ; Météo France ; Groupe Beaumanoir ; Vivendi ; Culligan ; Armand Thiery.

ANTEMETA

IL N'Y A PAS QU'EN MER QUE VOUS AVEZ BESOIN DE SECOURS ET DE PROTECTION.

ANTEMETA VOUS ACCOMPAGNE

INFRA
Réseau
Compute
Stockage

CYBER
Identification
Prévention
Détection & Réaction

DONNEE
Souveraineté
Protection
Reprise d'activité

OPS
Supervision
Exploitation
Optimisation

NOS CERTIFICATIONS ET LABELS

afaq ISO 27001 Sécurité de l'information AFNOR CERTIFICATION

Certifiée 100% HÉBERGÉE EN FRANCE

UGAP

UTILISÉ PAR LES ARMÉES FRANÇAISES

LABEL BAS CARBONE

Gartner

www.antemeta.com

arcserve®
Protect what's priceless.

Société : ARCSERVE
Adresse : Arcserve France SAS,
23 rue du Roule, 75001 Paris
Tél. : 08 05 63 83 70
Mail : **info@arcserve.com**
Site web : **www.arcserve.com/fr**

Spécialisations

Sauvegarde et restauration des données – sécurisé par Sophos –, reprise d'activité, continuité d'activité, protection des données de Microsoft 365 et Google Workspace, stockage immuable en mode Objet, archivage légal des e-mails.

Contacts

Ronan MOREAU
Territory Account Manager France
Ronan.Moreau@arcserve.com
+33 6 37 50 52 65

Joël RODRIGUEZ
Consultant Pre-Sales
Joel.Rodriguez@arcserve.com

Guillaume MAIDON
Consultant Pre-Sales
Guillaume.Maidon@arcserve.com

Priscillia OSCOSO
Marketing Manager South EMEA
Priscillia.Oscoso@arcserve.com
+34 935 48 41 17

Pour une protection des données et une sécurité de premier ordre

Arcserve, l'un des cinq premiers fournisseurs mondiaux de solutions de protection des données, propose le plus large éventail d'offres de pointe pour gérer, protéger et récupérer tous les workloads, des PME aux grandes entreprises, indépendamment de leur implantation ou de leur complexité. Les solutions Arcserve éliminent cette complexité tout en apportant une protection des données et une sécurité de premier ordre, rentable, agile et très évolutive dans tous les environnements. Cela inclut les infrastructures sur site, hors site (y compris DRaaS, BaaS et Cloud-to-Cloud), hyperconvergées et périphériques.

Produits phares

• Arcserve Unified Data Protection

Arcserve® Unified Data Protection (UDP) offre une solution tout-en-un de protection des données et de cybersécurité permettant la neutralisation des attaques de ransomwares, la récupération des données, ainsi qu'une reprise après sinistre (DR). Protégé par Sophos Intercept X Advanced, Arcserve UDP combine une protection des environnements avec cybersécurité et une continuité d'activité évolutive sur site et hors site, pour une approche multicouche qui offre une résilience informatique complète pour vos infrastructures virtuelles, physiques ou dans le Cloud.

• Arcserve OneXafe

OneXafe est une baie de stockage NAS, immuable, scale-out, en mode objet. Fonctionnant avec les différentes solutions de backup du marché, OneXafe offre un stockage évolutif pour les données non structurées et cibles de sauvegarde. Elle inclut nativement des fonctionnalités de déduplication en ligne, compression, encryption des données at rest, replication site-à-site, ainsi que d'immuabilité avec le mécanisme de snapshots intégrés, qui permet de protéger 100 % des données, même en cas d'attaques de type ranswomware.

Solutions

• Appliances Séries 9000 et Séries X

Basées sur les technologies de protection avancées Arcserve Unified Data Protection (UDP) et Sophos Intercept X Advanced, les Appliances Arcserve combinent la protection des points de terminaison et la continuité des activités sur site et hors site par le biais d'une approche multicouche garantissant une résilience informatique complète.

• Appliance Arcserve N-series

Basées sur la technologie Arcserve UDP, les appliances sont alimentées par Nutanix et sécurisées par Sophos, et offrent aux infrastructures hyperconvergées Nutanix une protection unifiée des données, une évolutivité et une sécurité inégalées.

• Arcserve UDP Cloud Hybrid Secured by Sophos

Sauvegarde dans le cloud, avec cybersécurité entièrement intégrée, extension de reprise après-sinistre avec les logiciels de protection de données et les Appliances Arcserve.

• Arcserve Cloud Backup for Office 365 Secured by Sophos

Sauvegarde et cybersécurité de Cloud à Cloud pour les données Microsoft 365, tout en protégeant des cyberattaques avec les technologies anti-ransomware et la prévention des menaces de Sophos.

• OneXafe Solo – Protection des données « zéro configuration »

OneXafe Solo est une appliance qui transfère des données directement dans le Cloud ou NAS.vers StorageCraft Cloud Services pour la continuité des activités.

La première et dernière ligne de défense contre les cyber-attaques

CRÉEZ UNE STRATÉGIE UNIQUE POUR LA REPRISE APRÈS SINISTRE, LA SAUVEGARDE, LA CYBERSECURITE ET LA DISPONIBILITE DES APPLICATIONS AVEC ARCSERVE!

Les solutions best-in-class d'Arcserve gèrent, protègent et restaurent toutes les charges de travail des données des PMEs, ETIs et Grandes Entreprises. Elles intègrent toutes les fonctionnalités de produits indépendants, de la prévention des cyber-menaces, la sauvegarde et restauration après sinistre, et la disponibilité des applications. Protégé par Sophos Intercept X Advanced for Server, Arcserve combine de façon unique la protection des serveurs, le stockage immuable et la continuité d'activité évolutive sur site et hors site. Arcserve offre une résilience complète des données pour la nouvelle génération de data centers hybrides.

arcserve.com/ransomware

arcserve®

Société : ATEMPO
Adresse : 23, avenue Carnot
91300 Massy – France
Tél. : 33 1 64 86 83 00
Mail : **info@atempo.com**
Site web : **www.atempo.com**

Spécialisations

Éditeur de solutions pour la protection des données et le Data Management, Atempo dispose d'une expertise éprouvée pour sauvegarder, archiver et déplacer les grands volumes de données dans les secteurs pétavores tels que la finance, l'assurance, les médias, le design industriel, les sciences de la vie et de la Terre, les véhicules intelligents et les systèmes d'information géographique.

Contact :
Thanom MARI
Marketing Manager
thanom.mari@atempo.com

« Nos solutions 100 % souveraines et " Privacy and security by design " répondent à la fois aux exigences des entreprises et des citoyens en matière de sécurité, confidentialité et conformité réglementaire, mais aussi à la volonté du gouvernement de renforcer la souveraineté numérique en Europe. Au quotidien, nous œuvrons aux côtés d'acteurs reconnus de la filière cybersécurité pour reprendre le contrôle sur notre destin numérique et ainsi, bâtir une troisième voie européenne garantissant aux organisations professionnelles le meilleur du monde numérique. »

Luc d'Urso, PDG du groupe Atempo.Wooxo

Présentation de l'entreprise

Avec plus de trente années d'expérience au service de nombreux ministères régaliens, organisations publiques et grands comptes exigeants, Atempo propose une gamme de solutions éprouvées pour protéger les entreprises contre tout risque de perte de données et d'interruption d'activité en cas de sinistre.

Atempo a fait le choix de développer des offres souveraines sans recours à la sous-traitance étrangère. La R & D s'organise autour d'un laboratoire d'Intelligence artificielle, à Orléans (45), et de trois centres de développement en région parisienne (91), Vannes (56) et La Ciotat (13).

Sélectionnée dans le cadre du programme gouvernemental French Tech 120-Alumni 2020 destiné à faire émerger 25 licornes d'ici à 2025, l'entreprise dispose d'un puissant réseau de grossistes à valeur ajoutée, de revendeurs, constructeurs, intégrateurs, et fournisseurs de services managés.

Atempo se positionne comme un fervent défenseur d'une Europe numérique. Engagée dans la lutte contre la cybercriminalité, elle est membre d'Hexatrust, *d'European Champions Alliance*, du groupement Acyma qui soutient le programme gouvernemental cybermalveillance.gouv.fr. et de l'association européenne GAIA-X.

En août 2021, Atempo a obtenu la certification ISO 9001 : 2015 pour son système de Management de Qualité.

Offres

Partenaire technologique de nombreux constructeurs de stockage de pointe, tels que DDN, Qumulo, Nutanix, Wasabi ou encore Huawei et d'acteurs souverains du Cloud Computing, tels que OVHcloud, Outscale, Scaleway, ASP Serveur, Jaguar Networks etc., Atempo propose des offres qui s'articulent autour de trois solutions :

- Miria : plateforme de nouvelle génération pour migrer ou synchroniser des gros et très gros volumes de données non structurées entre stockages hétérogènes et les protéger
- Tina : solution de sauvegarde de serveurs physiques et virtuels
- Lina : solution de sauvegarde en continu des postes de travail fixes et portables.

Ces solutions sont proposées sur site ou en mode cloud.

Labellisées **Utilisé par les Armées Françaises** et **France Cybersecurity**, les solutions Atempo sont exclusivement développées en France au sein des centres de R & D du groupe, et bénéficient d'une solide réputation auprès de grands comptes publics et privés.

Ces solutions sont référencées au catalogue GouvTech de la Dinum (Direction interministérielle du numérique). Ce catalogue permet aux administrations d'identifier plus facilement les solutions numériques répondant à des critères de qualité et de fiabilité en matière de protection des données et de conformité aux grands principes du numérique public.

Points forts des solutions Atempo

- Indépendance vis-à-vis des constructeurs
- Facilité/rapidité et fiabilité de restauration grâce au concept de « Navigation temporelle "
- Hétérogénéité des environnements supportés
- Qualité du support, basé en France, accessible 24/7, assuré par des spécialistes
- Système de licences adapté aux segments de marché : collectivités, hôpitaux, éducation, recherche…
- Fonction de *Disaster Recovery* pour lutter efficacement contre la recrudescence des cyberattaques
- Solution « airgap » pour protéger les données sauvegardées des attaques cybercriminelles
- Solutions capables de répondre aux enjeux liés à l'explosion des volumes de données – à l'échelle du pétaoctet
- Juridiction européenne

Société : Axians
Adresse : 4 rue Jacques Daguerre
92500 Rueil-Malmaison
Mail : **contact-cybersecurity@axians.com**
Site web : **www.axians.fr**

Axians accompagne ses clients – entreprises privées, secteur public, opérateurs et fournisseurs de services – dans l'évolution de leurs infrastructures et de leurs solutions digitales. Axians maîtrise l'ensemble des technologies de l'information et de la communication : solutions applicatives et data analytics, réseaux d'entreprises et espaces de travail digital, datacenter et Cloud, infrastructures télécoms, cybersécurité. Au travers d'activités de conseil, de conception, d'intégration et de services, Axians développe des solutions sur-mesure afin de transformer la technologie en valeur ajoutée. Axians est une marque de VINCI Energies.

Chiffres clés

12 000 collaborateurs dans le monde

Présent dans 25 pays

2,6 Md € d'activité

Dirigeant

Guillaume GARRIC
Directeur Général

Quand vous choisissez Axians, vous bénéficiez :

- d'une assistance complète tout au long de vos projets, du conseil à l'exploitation
- d'un réseau dense d'entreprises de proximité pour répondre à vos besoins
- de solutions sur-mesure.

Offres

Spécialiste de la cybersécurité, Axians propose à ses clients de modéliser leur propre trajectoire cybersécurité et de l'implémenter dans les meilleures conditions tout en tenant compte des spécificités métiers et des secteurs d'activité.

Notre offre de cybersécurité s'articule autour de 3 pôles d'expertise et apporte à nos clients un service sur-mesure et une expertise on-demand :

Audit & Conseil : nos consultants interviennent sur 3 aspects que sont la cybersécurité IT, la cybersécurité ICS et le Privacy Management et accompagnent les clients sur les thématiques suivantes : gouvernance, gestion des risques (PIA), DPO, certification ISO 27001, audit de maturité (RGPD, ISO 27001, IEC 62443), référentiels de sécurité, assistance RSSI, sensibilisations et formation.

Solutions de Sécurité : nos ingénieurs proposent un accompagnement dans la réalisation de missions d'audit technique d'architecture et de configuration, d'analyse d'écarts et recommandations et dans l'intégration de solutions de sécurité. Nous nous appuyons sur un écosystème de partenaires stratégiques, afin de couvrir au plus près la sécurité des infrastructures, des données, des accès ainsi que la sécurité du contenu et du Cloud.

Services Opérationnels (SOLAR) : notre offre de services opérationnels se compose de 5 briques de sécurité permettant de détecter, d'explorer et de traiter les événements malveillants et les vulnérabilités : Red Team, SCAN, CERT, SOC, CSIRT.

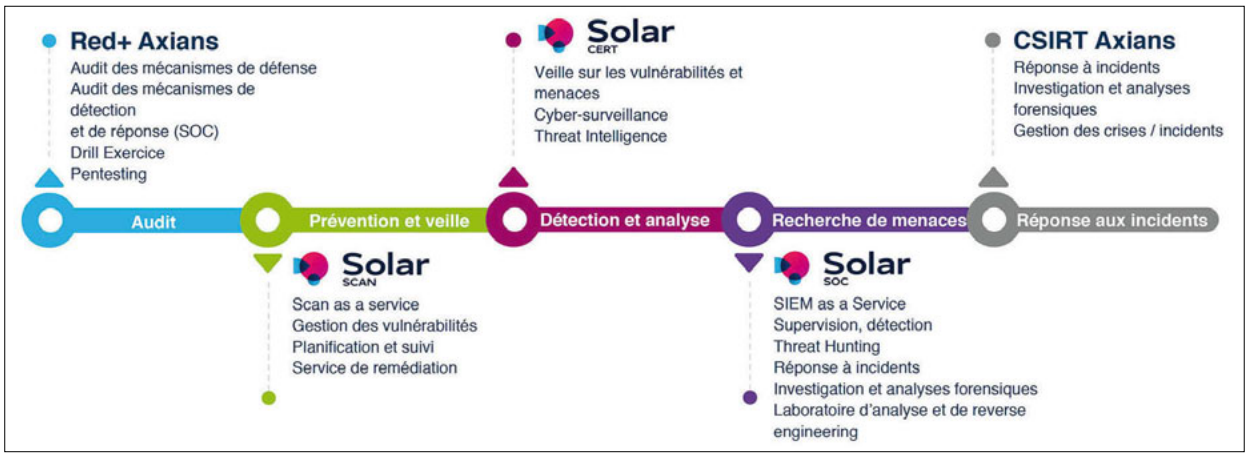
Qualifications et labels

Axians Cybersecurity Paris est qualifié PASSI et reconnu comme un prestataire de confiance recommandé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Axians Cybersecurity Paris est en mesure de proposer les prestations suivantes conformément au référentiel RGS (Référentiel Général de Sécurité) :

- audit organisationnel et physique
- audit de configuration
- audit d'architecture
- audit d'intrusion

Axians a obtenu le label Expert Cyber, délivré par Cybermalveillance.gouv.fr et destiné à valoriser les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients. Cette labellisation fait preuve de l'implication d'Axians dans la cybersécurité comme un acteur leader et moteur.

Le CERT Axians a obtenu l'agrément en tant que membre à part entière (Full Member) du FIRST, le Forum for Incident Response and Security Teams en novembre 2015.



Société : AVANT DE CLIQUER
Adresse : 9, rue Georges-Braque, 76000 ROUEN
Tél. : 02 78 77 53 86
Site web : **avantdecliquer.com**
Mail : **contact@avantdecliquer.com**

Spécialisations

Avant de Cliquer permet aux DSI, RSSI, DPO et dirigeants de réduire le risque de cyberattaque de manière drastique à l'aide d'un programme de sensibilisation au phishing basé sur l'apprentissage par l'action, créé sur mesure pour chaque utilisateur et animé sur la durée. La solution est entièrement autonome.

Impact

Plus de 200 000 utilisateurs actuellement sensibilisés.

Objectifs

Diviser par 10 le risque de cyberattaques

Notre solution en vidéo

Dirigeant
Carl HERNANDEZ
CEO
carl@avantdecliquer.com
Tél. : 02 78 77 53 86

Conçu, créé et hébergé en France

Pour en finir avec le Phishing !

Développez la vigilance de vos utilisateurs et gagnez en sérénité

L'audit de vulnérabilité
Réalisé en situation réelle. Mesure le niveau de maturité de vos utilisateurs face à une attaque par phishing. Votre rapport de vulnérabilité présenté en visioconférence permet de définir votre stratégie de prévention cyber.

Sensibilisation en continu
- Parce que le mode opératoire des fraudeurs évolue, les simulations de phishing ne sont donc pas faites sous la forme de campagnes ponctuelles mais d'envois constants, ce qui est bien plus efficace.
- Parce que les fraudeurs ne préviennent pas, à chaque instant, chaque utilisateur est susceptible de recevoir un mail malveillant.

Personnalisation de l'apprentissage
Les utilisateurs peu vigilants sont sensibilisés autant de fois que nécessaire jusqu'à ce que chaque point de faiblesse détecté soit comblé.

Des mises en situation
Les mises en situation peuvent prendre plusieurs formes :
- mails comportant des liens
- SMS
- attaques par rebond
- clé USB…

Amélioration des remontées d'information de vos utilisateurs
- En 1 clic, à l'aide d'un bouton "Alerte Phishing", intégré au client mail, vos utilisateurs signalent tout mail douteux.
- Le mail potentiellement frauduleux est automatiquement transmis pour analyse à votre équipe informatique.
- L'utilisateur est félicité pour son comportement positif.

Documentation des actions mises en place
Les actions de sensibilisation menées, les améliorations constatées, les axes de progression sont documentés. Ces actions sont conformes à l'article 32 du RGPD, imposant la mise en place de mesures organisationnelles de protection des données personnelles.

E-learning
Sensibilisation initiale, couvrant des éléments de contexte et techniques liés à l'hameçonnage (30 minutes sous forme de 15 modules).

Vous n'avez rien à faire. Tout est automatique.
Les envois ciblés sont réalisés sans action de votre part : vous n'avez pas à créer ou choisir des templates, à planifier des envois, à analyser les résultats pour sensibiliser les utilisateurs qui en ont le plus besoin.

Un accompagnement personnalisé
Chaque mois vous échangez avec un spécialiste sur les améliorations constatées et les axes de progrès, les menaces actuelles, de nouveaux modules d'e-learning et supports de communication personnalisés.

Lauréat de l'intelligence économique — Trophées de l'agroalimentaire
Référencé CAIH — Centrale d'Achat de l'Informatique Hospitalière
Bpi France — Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité
Éditeur référencé UGAP-SCC — Référencé UGAP — L'achat public responsable
Finaliste du prix de l'innovation — Salon des Maires et les Collectivités Locales

Bitdefender®
BUILT FOR RESILIENCE

Société : BITDEFENDER
Adresse : 49 rue de la Vanne, 92120 Montrouge, France
Tél. : +33 1 47 35 72 73
Mail : **enterprise_france@bitdefender.fr**
Site web : **www.bitdefender.fr**

Spécialisations

Protection des endpoints physiques et virtualisés, sécurité du Cloud et des conteneurs, eXtended Detection and Response (XDR/XEDR), SOC managé (MDR), Threat Intelligence, Forensics, Machine Learning

Chiffres clés

Effectifs : 1 600

Historique : société européenne créée en 2001

Bitdefender Labs : +30 milliards de requêtes de menaces chaque jour et +400 nouvelles menaces découvertes par minute

Le saviez-vous ? Les technologies Bitdefender sont utilisées par plus de 150 éditeurs sous licence

Dirigeant

Fondateur et PDG de Bitdefender : Florin TALPES *est un entrepreneur technologique visionnaire qui a fondé l'une des premières sociétés privées d'édition de logiciels, qui allait plus tard devenir Bitdefender. Sous sa direction, Bitdefender est devenu un leader mondial de la cybersécurité protégeant des millions de clients dans le monde.*

Contact

Laurent TOMBOIS
Country Manager France
ltombois@bitdefender.fr

Bitdefender est un leader de la cybersécurité qui fournit des solutions de pointe en matière de prévention, de détection et de réponse aux menaces. Protégeant des millions d'environnements de particuliers, d'entreprises et de gouvernements, Bitdefender est reconnue comme étant un expert de confiance au sein de l'industrie pour l'élimination des menaces, la protection de la vie privée et des données, et la cyber-résilience. Grâce à des investissements importants dans la recherche et le développement, les Bitdefender Labs découvrent 400 nouvelles menaces chaque minute et répondent à 30 milliards de requêtes de menaces par jour. La société a été la première à innover dans le domaine des malwares, de la sécurité de l'IoT, de l'analyse comportementale et de l'Intelligence artificielle. Sa technologie est utilisée sous licence par plus de 150 éditeurs parmi les plus reconnus au monde. Fondée en 2001, Bitdefender a des clients dans 170 pays et possède des bureaux dans le monde entier.

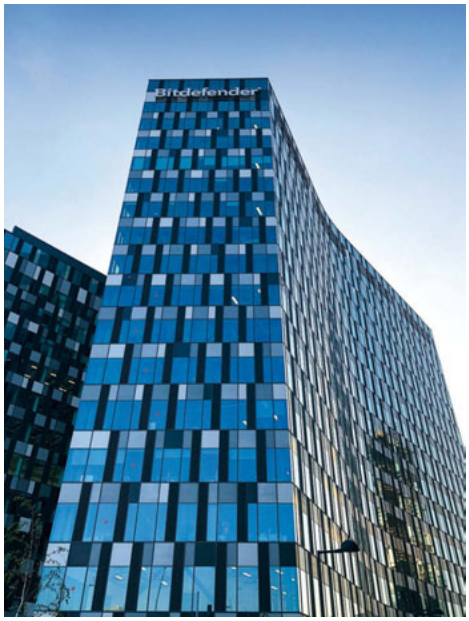
Offres

Bitdefender ambitionne de toujours mieux protéger ses clients entreprises en renforçant leur cyber résilience. Pour cela, Bitdefender répond à des besoins concrets en matière de cybersécurité.

• **Réduire le nombre d'outils utilisés et améliorer la visibilité.** Bitdefender GravityZone est une solution unifiée pour la protection et l'analyse des endpoints. Elle sécurise tous les endpoints de l'infrastructure et les charges de travail dans le Cloud via une seule console, un seul agent et un déploiement unifié (physique/virtuel/conteneurs, Cloud). Tous les modules de sécurité sont regroupés au sein d'un seul et unique outil : anti-malware Next-Gen, EDR, XEDR, analyse des risques, contrôle des applications et du Web, Patch Management, chiffrement, sécurité contre les attaques réseau, sandbox cloud, Machine Learning, etc.

• **Bénéficier de la meilleure prévention possible.** Bitdefender est l'éditeur ayant été le plus grand nombre de fois à la première place des tests AV-Comparatives depuis 2018 en matière de Protection dans le monde réel, de Performances et de Protection contre les malwares. Bitdefender a aussi reçu la récompense « Best Protection 2020 » de la part d'AV-Test.

• **Résoudre les problématiques liées au manque de compétences internes.** Les organisations ne disposant pas des ressources nécessaires à la gestion quotidienne d'une solution de cybersécurité, à l'analyse des alertes et à l'investigation sur les attaques, elles peuvent se reposer sur le service Bitdefender Managed Detection and Response (MDR). Celui-ci



exécute 24h/24, 7j/7, des mesures avancées de prévention et de remédiation des cyberattaques, depuis le SOC Bitdefender.

• **Améliorer son ROI.** Bitdefender améliore le retour sur investissement de la cybersécurité en fournissant une solution unifiée qui intègre à la fois le renforcement, l'évaluation des risques, la prévention, la détection, la réponse et l'investigation.

Récompenses

« Strong Performer » Forrester Wave Endpoint Software Security As a Service (Q2 2021), « Top Player » Radicati Advanced Persistent Treat Protection (2021), « Best Protection » AV-Test (2020)

Certifications

SOC2 Type 2, ISO 9001, ISO 27001, Nutanix AVH/VMware/Citrix Ready.

ChamberSign
Autorité de certification

Pionnière dans son domaine, ChamberSign est une autorité de certification et un tiers de confiance. Elle propose un ensemble d'outils d'identités numériques et de signatures électroniques conforme aux réglementations en vigueur.

Société : CHAMBERSIGN FRANCE
Adresse : Le cours du Midi
10, cours de Verdun-Rambaud
69002 Lyon
Tél. : 0892 230 252
(0,45 € TTC la minute France Métropolitaine uniquement)
Mail : **commercial@chambersign.fr**
Site web : **www.chambersign.fr**

Spécialisations

ChamberSign est une autorité de certification. Tiers de confiance, elle est qualifiée par l'Anssi et LSTI pour délivrer des identités numériques professionnelles à destination des personnes physiques et des entités morales. Elle fournit des certificats numériques émis et délivrés dans le respect des normes les plus strictes de la profession (notamment eIDAS et RGS) afin de garantir des échanges électroniques authentifiés et sécurisés.

Chiffres clés

Effectifs : + 20

+40 bureaux d'enregistrement répartis sur le territoire français (Guyane et Dom inclus)

+de 500 opérateurs habilités à délivrer des certificats électroniques

Dirigeant
Stéphane GASCH
Délégué général
sgasch@chambersign.fr
tél : 06 07 73 46 06

Experte dans son domaine, ses missions sont nombreuses :

• fournir des certificats électroniques émis et délivrés dans le respect des normes les plus strictes de la réglementation (notamment RGS et eIDAS), garantissant ainsi l'identité numérique professionnelle de la personne physique ou de la personne morale ;

• proposer des solutions permettant la gestion des identités numériques en web service afin de s'adapter aux besoins de ses clients, grands comptes ou partenaires ;

• accompagner les organisations et les usagers à l'utilisation du certificat électronique dans leurs échanges dématérialisés sécurisés et adapter les processus et produits aux nouveaux usages ;

• participer à la réflexion et au développement des échanges électroniques sécurisés (membre de la FNTC, du club PSCO, ou encore de l'ACN).

Offres

Les identités numériques de la personne morale.

Se protéger entre autres des usurpations d'identité, de modifications ou d'altérations de données et de documents pendant les échanges ou l'archivage devient une nécessité pour toutes les organisations.

Le certificat **Certiserv serveur client RGS*** permet de garantir la confidentialité des données transmises et d'authentifier fortement le serveur et son propriétaire. Il est utilisé lors de la transmission sécurisée de flux.

Les certificats numériques de type cachet tel que **Negocio** (Conforme RGS* pour la piste d'audit fiable en particulier) ou **Eurocomercio** (répondant aux obligations fiscales de la facture électronique qualifié RGS** & eIDAS) scellent les données afin d'en garantir leur origine, leur authenticité et leur intégrité. Ainsi, les documents deviennent opposables entre les acteurs et durables pendant leur archivage.

Les identités numériques personne physique

Les certificats numériques pour personnes physiques offrent une multitude d'usages. Ils permettent une authentification forte de son propriétaire (Windows, applications métiers, comptes utilisateurs…), la certification des e-mails ou encore la signature électronique conforme RGS* (**Initio**), avancée eIDAS (**Eiducio**), qualifiée eIDAS (**Eiducio+** / **Europrobatio**). C'est ainsi l'assurance d'une dématérialisation à valeur légale où l'identité du signataire, son engagement et l'intégrité des documents sont prouvés de manière certaine.

Qualifications et distinctions

ChamberSign s'est vu décerner le visa de sécurité de l'Anssi pour ses services de certification électronique et a également obtenu le label France Cybersecurity.

• Ses certificats électroniques sont qualifiés eIDAS et RGS.

• Elle est certifiée ISO 9001 version 2015 pour ses procédures internes et celles de délivrance de certificats.

Conformément à ses obligations d'AC, ses processus et son système d'information ont fait l'objet d'un audit de conformité RGPD conclu positivement et dont le renouvellement périodique est inclus dans sa politique interne.

Historique

ChamberSign fournit en France ses premiers certificats numériques en 2000. Le marché vient de se créer. La directive 1999/93/CE relative au cadre communautaire pour les signatures électroniques et sa transposition en France avec la promulgation de la loi du 13 mars 2000 consacre la signature électronique et l'acte authentique électronique. L'État français impose alors le certificat numérique à de nombreuses entreprises et collectivités pour les téléprocédures ou les accès aux espaces usagers. Depuis sa création le 20 septembre 2000 par les Chambres de Commerce et de l'Industrie et CCI France, ChamberSign France demeure aujourd'hui l'un des précurseurs en la matière.

CyberRes
A Micro Focus Line of Business

Renforcez votre cyber-résilience

CLUSIF Adhérent 2021

Société : CYBERRES
Nom des marques :
FORTIFY, VOLTAGE, NETIQ,
ARCSIGHT, INTERSET
Adresse : Tour Carpe Diem
31 place des Corolles
92098 Paris La Défense Cedex
Site web : **www.cyberres.com**

Spécialisations

- **DevSecOps**
- **Conformité RGPD**
- **Chiffrement**
- **Sécurité de l'information**
- **Collecte et traitement des logs**
- **SIEM & SOC**
- **IAM, IGA, Authentification forte**

Chiffres clés

12 000 employés dans 48 pays
40 000 clients
7 500 partenaires
$ 3 milliards de revenus
Création : 1976
Sièges sociaux : Newbury (Royaume-Uni) et Santa Clara (Californie – États-Unis)

Dirigeants
Stephen MURDOCH
CEO Micro Focus

John DELK
Senior VP & General Manager – CyberRes

Christophe GAULTIER
Sales Director France & BeLux - CyberRes
christophe.gaultier@microfocus.com
Tel : +33 6 29 17 83 67

CyberRes regroupe les solutions de sécurité de Micro Focus. Nous apportons l'expertise de l'un des plus grands portefeuilles de sécurité au monde pour aider nos clients à faire face à l'évolution des menaces en renforçant la cyber-résilience de leurs équipes et organisation. Nous aidons les entreprises à renforcer la confiance, à gagner en fiabilité et à survivre en cas de conditions difficiles, de crise et de volatilité du marché. Notre portefeuille fait partie d'un ensemble plus large de solutions de transformation numérique qui permettent de lutter contre les conditions défavorables afin que les entreprises continuent à fonctionner pour répondre à leurs obligations tout en tirant parti des opportunités de demain.

Offres

ArcSight

Next-Gen Security Operations & Analytics

Fort de plus de 20 années dans le monde du SIEM, la plateforme ArcSight propose une solution complète pour capturer, stocker, corréler, et effectuer du machine learning. Dans une interface modernisée, nous proposons une catégorisation des incidents et des contenus remontés selon le Framework MITRE ATT&CK et un système de SOAR intégré.

Fortify

Application Security

Leader sur le marché de la sécurité applicative, notre gamme Fortify propose des solutions de SAST (scan de code) et de DAST (scans dynamiques) afin de réduire les risques de mauvaise utilisation du code applicatif.

Notre plateforme de sécurité des applications automatise les tests tout au long du CI/CD afin que les développeurs puissent résoudre rapidement les problèmes.

Voltage

Data Security & Governance

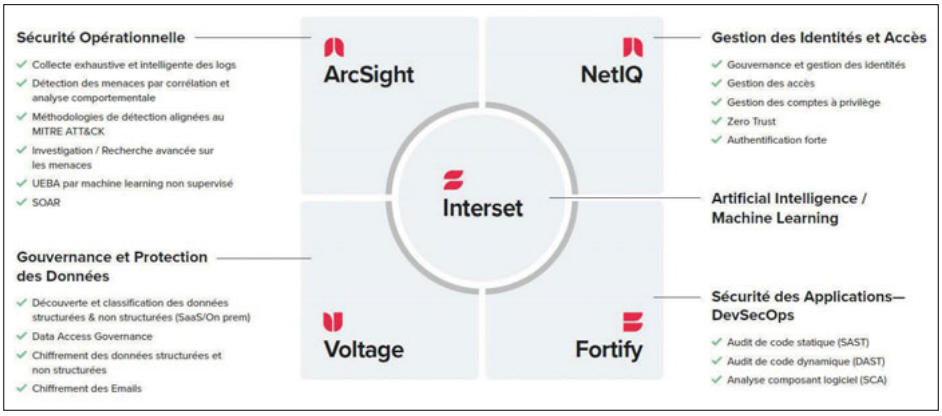
Découvrez, analysez et protégez vos données sensibles, structurées et non structurées dans le respect des exigences réglementaires, type RGPD.

Présent dans la sécurité de données (dans le monde de la carte de paiement notamment) depuis une quinzaine d'années, la plateforme Voltage propose de sécuriser vos e-mails, vos documents, mais aussi vos données structurées, pour améliorer votre posture de sécurité.

NetIQ

Identity and Access Governance

De la gouvernance des identités à l'authentification forte, en passant par la gestion des accès et la sécurisation des comptes à privilèges, CyberRes propose la gamme complète et modulaire NetIQ de solutions IAM à déployer chez vous ou dans le Cloud.



Société : CHECK POINT SOFTWARE TECHNOLOGIES Ltd
Adresse :
43-47, avenue de la Grande-Armée
75116 Paris
Tél. : +33 (0) 7 82 97 19 00
Mail : **contact@checkpoint.com**
Site web : **http://www.checkpoint.com/**

Spécialisations

NextGen Firewall, sécurisation des postes de travail, accès à distance via VPN, protection des Iaas privées, orchestration de la sécurité Cloud, protection SaaS.

Chiffres clés

CA : $ 2 milliards
Effectifs : 5 400

Dirigeants

Michael TECHER
Country Manager
France

Xavier DUROS
SE manager
France

Contacts

Kinnie ANDRÉ
Field Marketing Manager
kandre@checkpoint.com

Ilona TUCA
Business Developper
Ilona.tuca@infinigate.fr

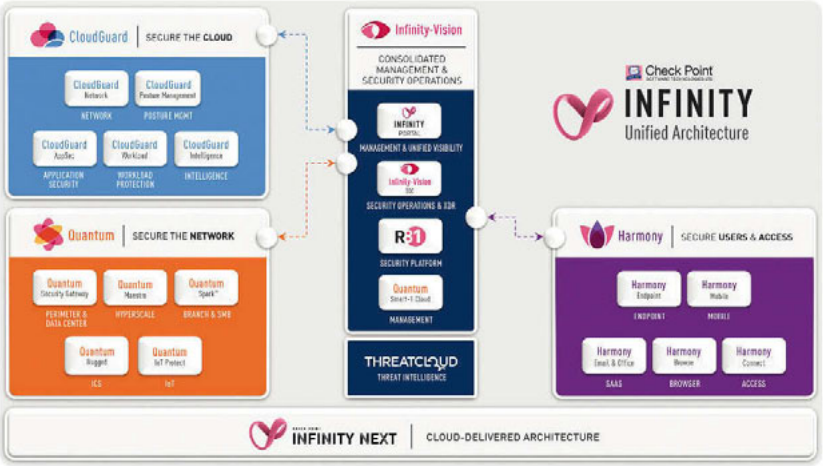
BU dédiée chez Infinigate
checkpoint@infinigate.fr

Check Point Software Technologies est l'un des principaux fournisseurs de solutions de cybersécurité dans le monde pour les gouvernements et les entreprises. Ses solutions protègent les clients des cyberattaques grâce à un taux de blocage inégalé des logiciels malveillants, des logiciels rançonneurs et autres types d'attaques

Check Point propose une architecture de sécurité multi-niveau qui défend les données des entreprises sur leurs réseaux, leurs Cloud et leurs endpoints. Les solutions disposent d'un système complet et intuitif d'administration unifiée de la sécurité. Check Point protège plus de 100 000 entreprises de toute taille. Depuis plus de 20 ans, des clients dans le monde entier comptent sur Check Point pour protéger leur marque, leurs actifs et leurs données contre les cyberattaques, et pour accélérer leur activité de manière productive en toute sécurité.

Check Point est distribué par Infinigate qui collabore depuis de nombreuses années pour accompagner les revendeurs et clients dans leurs projets de cybersécurité. Une équipe Infinigate dédiée épaule Check Point sur toutes les demandes de projet et apporte son soutien grâce à ses experts en marketing et avant-vente et ses commerciaux. Infinigate est également un centre de formation qui est habilité à vous recevoir et vous faire passer les certifications Check Point

Offres



Références clients

Les références publiques de clients sont mises à jour sur
https://www.checkpoint.com/customer-stories/

Historique

- Check Point a été fondée en 1993 par Gil Shwed (PDG), Marius Nacht et Shlomo Kramer.
- La société a lancé FireWall-1 en 1994, premier pare-feu au monde équipé de la technologie Stateful Inspection (au cœur de tous les pare-feu modernes).
- Check Point est cotée à la Bourse du NASDAQ depuis 1997 sous le symbole « ChKP ».
- La société est basée à San Carlos, en Californie, et à Tel Aviv, en Israël.
- Possède des bureaux dans 42 pays.
- Protège plus de 100 000 entreprises de toute taille et des millions d'utilisateurs à travers le monde.

INFINIGATE
.... Adding Value to Distribution

LE MEILLEUR DE LA CYBERSÉCURITÉ **POUR VOS CLIENTS**

Infinigate est le 1er Distributeur à Valeur Ajoutée Européen 100 % dédié à la Cybersécurité.

Infinigate propose des solutions de sécurité IT innovantes et performantes pour les revendeurs, intégrateurs et fournisseurs de services managés.

Le groupe **Infinigate** compte plus de 500 employés répartis dans 11 filiales en Europe.

L'ÉCOSYSTÈME CYBER INFINIGATE

- PROTECTION ENDPOINT & MOBILE
- CYBER INTELLIGENCE
- SÉCURITÉ DE L'EMAIL
- SERVICES & SUPPORT
- FORMATIONS TECHNIQUES
- ORCHESTRATION & AUTOMATISATION
- SÉCURITÉ DU RÉSEAU
- AUDIT & GOUVERNANCE
- SOLUTIONS MSP & MSSP
- SÉCURITÉ DU CLOUD
- SAUVEGARDE & PRA
- GESTION DE L'IDENTITÉ

frhead.fr

A10 Acronis BACKBOX Barracuda Check Point ENTRUST HID
kaspersky netwrix okta radware N-ABLE SONICWALL yubico

Tel : 01 80 73 04 25 • **Email :** info@infinigate.fr • www.infinigate.fr

Société : CS-NOVIDY'S
Adresse : immeuble Energy-2,
4 rue Paul-Dautier,
78140 Vélizy-Villacoublay
Site web : **https://www.csnovidys.com/**

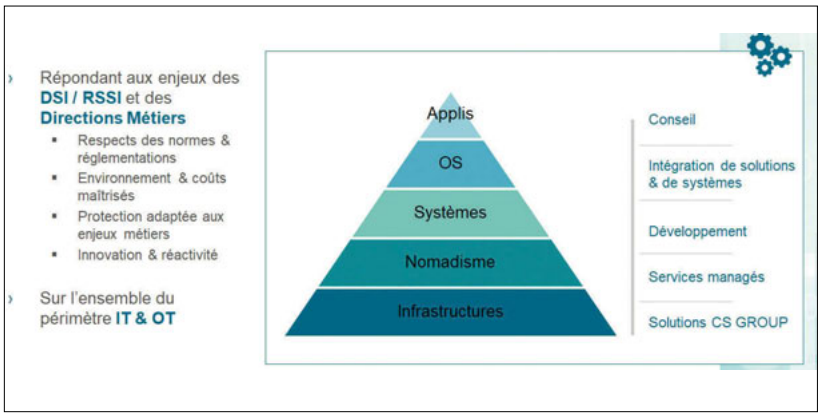
À travers sa filiale CS-NOVIDY'S, CS GROUP se positionne dans le Top 5 des sociétés de services françaises sur le marché de la cybersécurité

Notre positionnement nous permet de couvrir l'ensemble des enjeux de la cybersécurité sur les SI d'entreprise (IT), et les SI industriels (OT), du Conseil aux services managés en passant par l'intégration de solutions et de systèmes.

L'enjeu est de déployer une sécurité au juste niveau pour permettre une maîtrise optimale de l'ensemble des infrastructures et systèmes. Nous concilions ainsi l'approche des DSI, RSSI et des directions opérationnelles métiers.

UNE EXPERTISE du plus haut niveau

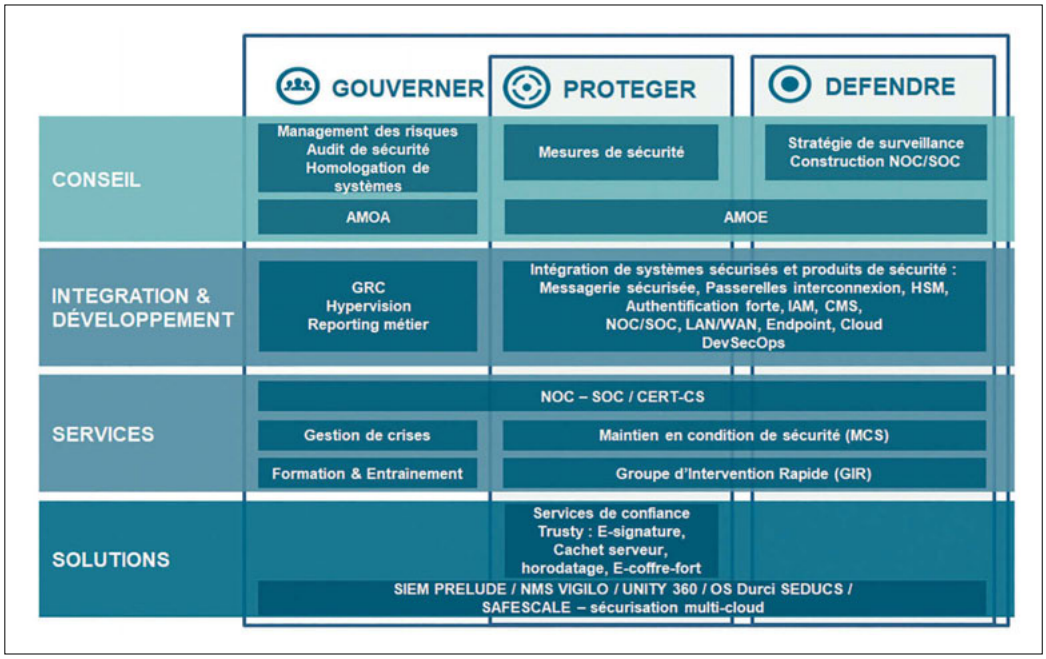
- **CERT - CS GROUP**
- **Qualification PASSI & PASSI LPM**
- **Produits certifiés EAL3+**
- **NOC/SOC externalisé / hybride**
- **Laboratoire de Lutte informatique**
- **La R&D au profit d'une sécurisation forte & flexible**



Offre

Une approche holistique de la cybersécurité :

- la sécurité des infrastructures et des communications (Lan, Wan, Cloud…)
- des systèmes d'exploitation sécurisés
- l'intégration de systèmes et d'applications sécurisés
- l'homologation de système d'informations sensibles…



Par ailleurs, expert en Data Intelligence, nous maîtrisons totalement les aspects de sécurisation, de confidentialité et d'intégrité de la donnée, enjeu majeur des entreprises en environnement cloud et collaboratif, et proposons une approche « security by design ». Nous intervenons sur des secteurs stratégiques : la défense, la sécurité publique, le nucléaire, le spatial, l'aéronautique ou encore l'énergie. En tant que ETI française, nous proposons à nos clients qui opèrent dans ces secteurs d'importance vitale des solutions souveraines.

Dans le domaine de la valorisation et de la sécurisation des données, nous sommes particulièrement impliqués dans des initiatives nationales et européennes et auprès de nos grands clients pour contribuer à garantir la souveraineté numérique européenne.

NOVIDY'S

WWW.CSNOVIDYS.COM

CS-NOVIDY'S, filiale de CS GROUP

ACTEUR LEADER

POUR LA SÉCURISATION DE VOS SYSTÈMES D'INFORMATION D'ENTREPRISE & INDUSTRIELS

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY · CERT · AUTHORIZED TO USE CERT

VISA DE SÉCURITÉ · AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI

FRANCE CYBER SECURITY

SYSTÈMES CRITIQUES INTELLIGENTS CYBERPROTÉGÉS

CS GROUP

Société : CYBEREASON
Adresse : 54-56 avenue Hoche, 75008 Paris, France
Tél. : +33 1 87 39 90 00
Site web : **www.cybereason.com/fr**
Demo: : **https://www.cybereason.com/fr/request-a-demo**

Chiffres clés :
Effectifs : +1 000

Dirigeants

Lior DIV
CEO & co-fondateur

Yossi NAAR
CVO & co-fondateur

Tonatan Striem AMIT
CTO & co-fondateur

Contacts
Joël MOLLO
RVP France
joel.mollo@cybereason.com
Julien BILLOCHON,
SE Lead France:
julien.billochon@cybereason.com

Prévenir, détecter et remédier aux attaques les plus avancées

Cybereason a été créée en 2012 et a délivré sa plateforme de sécurité après deux ans de développement. Opérant dans plus de quarante pays, Cybereason est une société internationale à capitaux privés dont le siège se situe à Boston, aux États-Unis. Notre solution complète, basée sur le comportement, comprend des moteurs Antivirus, NGAV, Anti-Ransomware, Anti-Fileless Malware Prevention, EDR, XDR, et des capacités forensics complètes. Nous vous donnons une visibilité sans précédent et fournissons la puissance nécessaire pour prévenir, détecter et remédier aux attaques les plus avancées.

Offres

EPP (AV / NGAV) / EDR / XDR / Forensics & Incident Response

Services

Managed Detection & Response / M-XDR

Une visibilité approfondie de vos systèmes et de l'activité qui s'y déroule est impérative pour une sécurité robuste. Cybereason collecte des informations brutes sur les machines, les connexions, les processus, les utilisateurs et d'autres événements (+400 types de données), et les envoie au moteur de corrélation CMC *(Cross-Machine Correlation engine)* pour analyse.

Le moteur de corrélation CMC enrichit les données brutes en corrélant des millions d'événements au sein de votre organisation et en appliquant l'Intelligence artificielle, l'apprentissage automatique, l'analyse comportementale et les informations provenant de sources de renseignements sur les menaces *(Cybereason Threat Intelligence)*.

Grâce à une analyse centralisée en mémoire, le moteur de recherche peut identifier en temps réel les menaces connues et inconnues. Finalement, une fois que tout le bruit a été filtré et que la vraie réalité d'une opération malveillante peut être vue, alors Cybereason alertera votre équipe et déclenchera un MalOp *(Malicious Operation)*. Un MalOp inclut l'histoire complète de l'attaque en fournissant un contexte dans les techniques MITRE ATT&CK spécifiques détectées, la cause première, un calendrier d'attaque et des détails supplémentaires pour aider à accélérer la compréhension, la portée et la réponse.

Lorsqu'un analyste lit un MalOp, il est immédiatement prêt à agir. Cybereason n'émet pas d'alertes redondantes pour des événements individuels et n'envoie pas plusieurs alertes pour chaque machine affectée par le même événement.

Cybereason génère donc peu d'alertes, de meilleures qualités et avec un très faible taux de faux positif.

L'intérêt majeur de Cybereason est de proposer une solution EDR et XDR afin d'étendre la détection au-delà du Endpoint (Cloud, réseaux, identité, etc.) et de proposer une remédiation sur l'intégralité de ce périmètre.

Certifications

Gartner	Forrester	NSS Labs	MITRE ATT&CK
Cybereason Named a **Visionary** in Gartner's 2021 EPP Magic Quadrant Report	Cybereason Named a Strong Performer With the **Highest Current Offering Score** in Forrester's 2020 EDR Wave	Cybereason Received the **Highest Overall 'AA' Product Rating** in NSS Lab's 2020 Advanced Endpoint Protection Test	Cybereason Leads the Pack in **Protection, Linux, and Real-Time Coverage** in the 2020 MITRE ATT&CK Evaluation

cybereason

REPOUSSEZ LES CYBERATTAQUES.

DEPUIS L'ENDPOINT ET SUR TOUS LES FRONTS.

Rejoignez les Défenseurs, en repoussant les cyber-attaques de toute part.

Cybereason vous aide à reprendre l'avantage sur les cyber-attaquants. Nous fournissons une visibilité sans égal de l'ensemble des menaces qui pèsent sur votre entreprise en vous procurant une vision globale et corrélée des opérations malveillantes, sans rester limités aux simples remontées d'alertes, vous permettant ainsi de contrer toutes les attaques dans leur intégralité.

www.cybereason.com/fr/request-a-demo

Société : DARKTRACE
Adresse : 38 avenue des Champs-Élysées, 75008 Paris
Tél. : +33 1 40 73 84 85
E-mail : **info@darktrace.com**
Site web : **www.darktrace.fr**

Spécialisations

Détection, réponse et investigation des cybermenaces – IA Auto-Apprenante – Réponse Autonome – Investigation autonome des menaces – Sécurité Réseau – Sécurité Cloud – Sécurité SaaS – Sécurité E-mail – Sécurité des systèmes industriels

Chiffres clés

Effectifs : 1 500 employés
Plus de 5 600 clients dans le monde

Dirigeant

Emmanuel MERIOT
VP Europe du Sud (basé à Paris)

Contact commercial
+33 1 40 73 84 85
info@darktrace.com

Contact RP :
Wendy ROLTGEN
Fabriq PR
+33 1 85 08 43 46
darktrace@fabriqpr.com

Historique

Fondée en 2013 par des mathématiciens de l'université de Cambridge et des experts de l'information au sein des gouvernements des États-Unis et du Royaume-Uni, Darktrace est aujourd'hui reconnue comme la première entreprise d'IA au monde dans le domaine de la cybersécurité.

Leader Mondial en IA Auto-Apprenante

Darktrace (DARK:L), un leader mondial de l'IA en cybersécurité, protège plus de 5 600 organisations dans le monde contre les menaces avancées, notamment les ransomwares et les attaques vers le Cloud et le SaaS. Son approche fondamentalement différente applique son IA Auto-Apprenante pour permettre aux machines de comprendre l'entreprise et de les défendre de manière autonome.

Darktrace compte plus de 1 500 employés et 30 bureaux dans le monde, son siège social est à Cambridge (Royaume-Uni). Darktrace a été désignée par le magazine TIME comme l'une des « entreprises les plus influentes » en 2021.

Offres

À défaut d'utiliser d'importants volumes de données d'entraînement, **l'IA Auto-Apprenante de Darktrace** apprend sur le tas à partir de données en temps réel. Appliqué à la cybersécurité, cela signifie que l'IA Auto-Apprenante peut identifier et arrêter les attaques zero-day puisqu'elle ne se base sur aucune base de données d'attaques historiques.

Que ce soit dans le Cloud et les systèmes de messagerie, à travers les technologies opérationnelles ou les réseaux et infrastructures traditionnels, l'IA Auto-Apprenante de Darktrace est installée au cœur de ces systèmes, et ne nécessite aucune migration de données. Son apprentissage sur mesure évolue constamment au fur et à mesure que l'environnement des données change.

L'IA Auto-Apprenante regroupe de manière autonome les appareils des utilisateurs en groupes de pairs en fonction de sa compréhension du comportement de chacune de ces entités. La technologie combine un certain nombre de méthodes de clustering différentes, elle peut ainsi déterminer lorsqu'un appareil se comporte de manière inhabituelle par rapport au reste de son groupe de pairs, ce qui lui permet de détecter les cyber-perturbations déjà présentes au sein de votre organisation.

Dans cette nouvelle ère de cyber-menaces, les équipes de sécurité humaine sont dépassées. Nous avons maintenant besoin de machines pour penser par elles-mêmes et réagir aux attaques rapides. Grâce à **Darktrace Antigena,** l'IA Auto-Apprenante permet une prise de décision autonome, ce qui est si critique lorsqu'une attaque ou un incident se déroule. Elle est capable de déterminer, par elle-même, l'action appropriée requise pour contenir immédiatement la menace et arrêter sa propagation, sans perturber inutilement les activités.

Cette prise de décision autonome donne aux humains un temps précieux pour reprendre le contrôle face aux incidents à évolution rapide et ainsi se concentrer sur un travail stratégique à plus forte valeur ajoutée.

Le **Cyber AI Analyst** est la première technologie au monde capable de parcourir un réseau informatique, d'enquêter sur les menaces potentielles et de produire des rapports écrits compréhensible. Il fonctionne comme un analyste humain de sécurité, enquêtant sur les signes avant-coureurs d'une attaque, consultant des sources tierces et utilisant son intuition pour parvenir à une conclusion sur une certaine menace, mais à la vitesse de la machine. Ce produit de pointe est le résultat de plus de trois ans de recherche et de perfectionnement.

Références clients

McLaren, Autodistribution, PCIS LVMH, Allianz, Tessi, OpinionWay, Bourse Direct, Porcher Industries, AmSty, Ville de Las Vegas, Ebay Classified, Librairie Éditrice du Vatican, Hôpital Américain de Paris

Combattre les ransomwares à l'aide de l'IA

Darktrace est la seule technologie capable d'interrompre une campagne de ransomware de manière autonome, sans perturber les opérations normales.

Pour en savoir plus, visitez
darktrace.com/fr/ransomware/

DARKTRACE

DIGITEMIS
CYBERSECURITY & PRIVACY

Société : DIGITEMIS
Nom de marque : MAKE IT SAFE

MAKE IT SAFE
by DIGITEMIS

Tél. : 09 72 46 39 78
Mail : **contact@digitemis.com**
Site web : **www.digitemis.com**

Spécialisations

Solution logicielle innovante. Make IT Safe : pilotage de la conformité (RGPD, PSSI, LPM, ISO 27001, Sapin 2…), évaluation et pilotage des risques (filiales, sous-traitants, fournisseurs…), audit management, intégration de la sécurité dans les projets (ISP), plans d'assurance sécurité (PAS), plans d'action collaboratifs…
Services d'expertises :

- **expertises uniques en cybersécurité et en protection des données personnelles (RGPD)**
- **externalisation de la fonction DPO et RSSI**
- **audit, conseil et formation**
- **tests d'intrusion complexes (Active Directory, ERP, AS/400, Red Team, IoT…)**

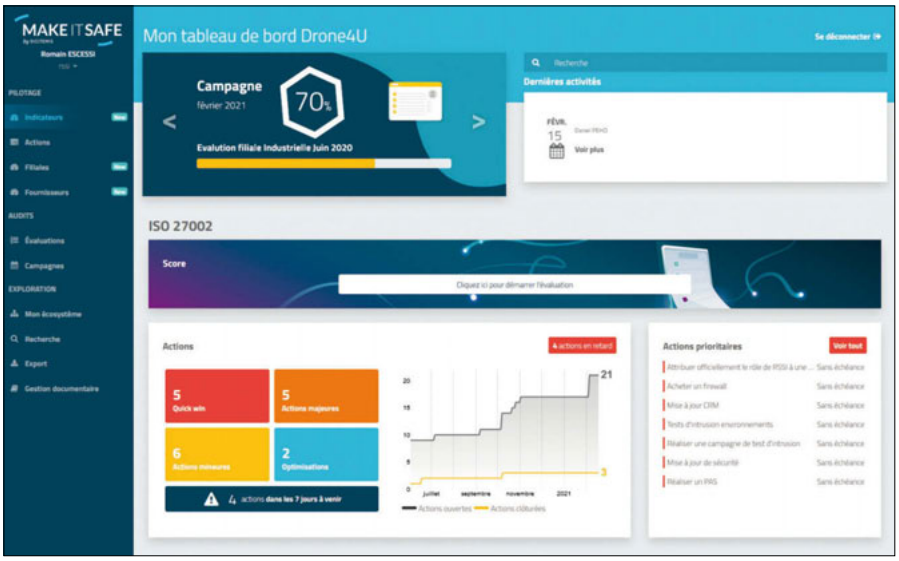
Chiffres clés

Effectifs : 48
Historique : création de l'entreprise en 2014

Dirigeant
Ludovic
de CARCOUËT

« 56 % des attaques proviennent de l'écosystème d'une entreprise, il est fondamental d'analyser et de réduire l'exposition interne comme l'externe »

Depuis 2014, DIGITEMIS conçoit des solutions intuitives et collaboratives pour aider ses clients à se protéger contre les nouvelles menaces. Tenant une place à part dans le paysage des pépites de la French Tech, l'entreprise réunit de façon inédite des experts en cybersécurité, des juristes et ingénieurs en conception de logiciels. Cette alliance lui a permis de devenir un leader reconnu, qui continue d'innover différemment.



Offres

Connaître ses vulnérabilités et réduire ses risques sont deux enjeux de cybersécurité qui nécessitent une action collaborative et pragmatique. Make IT Safe permet de maîtriser son exposition en analysant l'ensemble de son écosystème (filiales, sous-traitants, fournisseurs) selon des référentiels standard ou personnalisables.

Automatisez la création de vos plans d'actions en priorisant les ressources à affecter selon l'importance des risques identifiés ; la plate-forme permet d'assurer leur réussite en pilotant efficacement et collaborativement leur suivi.

Make IT Safe accélère la transformation des organisations en améliorant leur cyber maturité par la digitalisation de processus, tels que les plans d'assurance sécurité (PAS) et l'intégration de la sécurité dans les projets (ISP).

Certifications

- Qualification PASSI par l'Anssi
- Référencement UGAP
- Bpifrance Excellence
- France Cybersecurity
- Pass French Tech

Références clients

Cour des comptes
Sodebo
Ligue Nationale Rugby
Vinci Energies
MAIF assureur militant
EDF
Suez environnement

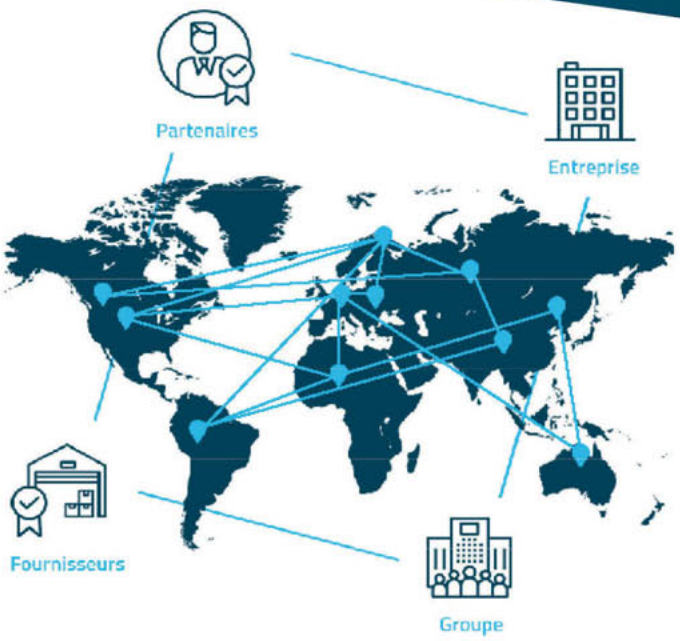
MAKE IT SAFE
by DIGITEMIS

Devenez acteur de votre cybersécurité avec Make IT Safe

Les **cyberattaques** et les risques liés à l'absence de **mise en conformité** peuvent provenir de diverses sources (vos filiales, vos fournisseurs...).

Pour réduire **ces risques** il devient primordial de vérifier l'ensemble des points de contrôle et de réussir le pilotage de **vos plans d'action**.

Make IT Safe est LA solution qui accompagne la transformation de votre organisation en améliorant **sa cybermaturité**.



La seule plateforme 100% française, collaborative et modulaire qui améliore votre maturité en matière de cybersécurité.

COMPLIANCE & RISK MANAGEMENT

- PILOTAGE DES FILIALES
- PILOTAGE DES FOURNISSEURS
- AUDIT MANAGEMENT
- INTÉGRATION DE LA SÉCURITÉ DANS LES PROJETS
- PLANS D'ASSURANCE SÉCURITÉ
- PLANS D'ACTION COLLABORATIFS

Éditeur référencé UGAP-SCC

UGAP

Lauréat du PASS FRENCH TECH

bpifrance EXCELLENCE 2019

PARTENAIRE de la DEFENSE — RESERVE MILITAIRE

SAS Digitemis 800 891 848 00015

Société : DYNAMIT SOLUTIONS & SERVICES
Activités : Services - Intégration - Formation
Adresse : 131-151 rue du 1er-Mai 92000 Nanterre
Tél. : +33 1 80 03 85 23
Mail : **contact@dynamit.fr**
Site web : **www.dynamitservices.fr/**

Spécialisations

- **Protection des données (sauvegarde, chiffrement, stockage, archivage)**
- **Analyse des vulnérabilités (réseau, empreinte numérique, site web)**
- **Protection du parc informatique (Endpoint, MDM, Antiphishing)**
- **Audit de sécurité et conformité Hybrid cloud (AWS, Azure, Kubernetes et VMware)**
- **Formation utilisateur sur la cybersécurité en entreprise**
- **Gestion unifiée de terminaux**

Chiffres clés

CA : 25 M€
Effectifs : 49 employés
Création : 1992
Siège social : Nanterre - France

Dirigeant
Jonathan HAYOUN
PDG

Contacts

Benoît AMSELLEM
Directeur commercial et opérations
benoit.amsellem@dynamit.fr

Arnaud MILLARD
Cybersecurity Pre-Sales Specialist
arnaud.millard@dynamit.fr

Boostez la puissance de votre cybersécurité

Le nombre d'attaques informatiques augmente de façon dramatique : vol de données, demandes de rançon, atteinte à l'image ou sabotage, sont autant de risques qui pèsent sur les organisations avec des conséquences souvent graves, parfois irréversibles.

Avec son approche novatrice de la sécurité des entreprises, DynamIT Solutions & Services vous aide à sécuriser ce qui compte le plus : vos données, l'espace de travail de vos collaborateurs ainsi que votre identité sur Internet.

Nos solutions

Solution Saas de sécurité et de gestion des postes

DynamIT propose une offre de gestion du parc informatique basée sur la **Persistance,** une technologie unique qui **ne peut être altérée ni supprimée** mais aussi des solutions unifiées de gestion des terminaux qui permet de gérer depuis un emplacement centralisé :

- les serveurs
- les ordinateurs portables
- les ordinateurs de bureau
- les smartphones
- les tablettes

Sauvegarde des données dans le Cloud

Sauvegarder n'aura jamais été aussi simple.

DynamIT Backup propose plusieurs options de restauration sécurisées de bout en bout dans le Cloud français.

Crucial pour se prémunir des ransomware, cette solution est une sauvegarde glissante sur 28 jours et un archivage mensuel des données afin de rendre possible leur récupération à tout moment.

Protection proactive face aux menaces

Face aux nouvelles menaces, nous proposons une nouvelle solution de cybersécurité qui intègre **l'Intelligence artificielle et le Deep Learning** dans son système de détection de menace.

Contrairement aux solutions de détection et de réponse attendant qu'une attaque soit exécutée pour réagir, notre approche de prévention basée sur le Deep Learning protège les entreprises par l'analyse anticipée des menaces.

Confidentialité et vulnérabilité

Nous proposons également une large gamme de solutions disruptives pour garantir une confidentialité maximale au sein de l'entreprise grâce à l'authentification multi-facteur pour les postes utilisateurs mais aussi le filtrage web, **des tests de vulnérabilité, l'identification des données présentes sur le darkweb,** l'anonymisation des données de l'entreprise ou encore le hacking visuel.

deepinstinct
BEFORE YOU KNOW IT

Nous écartons ce que les autres ne peuvent pas détecter

DynamIT Cybersecurity

Contactez-nous :
contact@dynamit.fr

TOUTE MENACE

- Malwares
- Ransomwares
- Spywares
- Chevaux de Troie
- Adversaires actifs

N'IMPORTE OÙ

- Périmètre NW
- Terminal
- Mobile
- Centre de données
- Cloud

TOUT SYSTÈME D'EXPLOITATION

- Windows
- macOS
- Android
- IOS et iPadOS
- Chrome OS

TOUT ENVIRONNEMENT

- VDI
- Cloud / On-Premise
- Multi-Tenancy
- En ligne / Hors ligne

EIFFAGE
ÉNERGIE SYSTÈMES

Société : Eiffage Énergie Systèmes – Clemessy
Marque : CLEMESSY
Adresse : 18 rue de Thann
Bp 54299 - 68057 Mulhouse Cedex 2
Tél. : +33 (0) 3 89 32 32 32
E-mail : **contact.clemessy@eiffage.com**
Site web : **www.clemessy.com**

Spécialisations

Partenaire de référence de nombreuses industries, connaissance des systèmes industriels et techniques permettant d'intégrer la cybersécurité sur tout le cycle de vie des installations des clients :

- **Conception**
- **Diagnostic**
- **Sécurisation**
- **Maintien en conditions de sécurité**

SÉCURITÉ ACCRUE À TOUS LES NIVEAUX

Connaissance des enjeux et des failles de cybersécurité propres aux systèmes industriels et techniques pour une sécurité efficace.

OPTIMISATION DES COÛTS

Intégration et adaptation des solutions de sécurisation pour des coûts optimisés et des systèmes plus performants.

SÉCURITÉ TOUT AU LONG DU CYCLE DE VIE

Intégration des règles et mesures de cybersécurité dès la conception des systèmes et jusqu'à la maintenance-exploitation.

Chiffres clés

Présents dans la cybersécurité depuis 20 ans

Dirigeant
Pierre GUILLEMINOT
Directeur général

Contact
Jocelyn ZINDY
Directeur commercial Cybersécurité
03 89 32 37 08 - 06 24 90 18 94
Jocelyn.zindy@eiffage.com

Eiffage Énergie Systèmes conçoit, réalise, exploite et maintient des systèmes et équipements en génies électrique, industriel, climatique et énergétique dans le respect des Hommes et de l'environnement. Eiffage Énergie Systèmes propose une offre sur mesure pour les marchés de l'industrie, des infrastructures et réseaux, des villes et collectivités et du tertiaire.

Au sein d'Eiffage Énergie Systèmes, toutes les offres sont pilotées de manière transverse afin d'intégrer toujours plus de valeur ajoutée et de favoriser l'innovation pour vous proposer la meilleure des réponses.

Ces offres sont portées par différentes marques expertises, parmi lesquelles, Clemessy, la marque dédiée à l'industrie.

Dans le domaine de la cybersécurité, Clemessy répond aux besoins des industries les plus exigeantes et s'engage à leur côté pour leur permettre :

- ***d'exploiter en toute sécurité leurs installations***
- ***de protéger leurs données essentielles***
- ***de répondre aux obligations légales***

Offres

Audit, diagnostic, et conseils	Sécurisation des systèmes	Maintien en conditions de sécurité
• Diagnostic • Analyse de risque • Support à l'homologation LPM • Inventaire, cartographie • Évaluation niveau de sécurité / référentiel ANSSI • Tests de vulnérabilité • Définition des mesures SSI	• Étude, intégration de solutions matérielles et logicielles (détection et protection) • Simulation d'attaques • Remédiations et durcissement • Sécurisation des architectures industrielles, réseau, données, logiciels, postes et équipements • Évaluation des risques résiduels	• Maintenance • Veilles de vulnérabilité • Mises à jour • Formation de sensibilisation

« Eiffage Énergie Systèmes travaille sur la sécurité dans le domaine industriel depuis plus de 30 ans. Nous sécurisons les systèmes existants en débutant par une phase de diagnostic. Nous évaluons les vulnérabilités, identifions les systèmes obsolètes et analysons les risques. Cette phase permet ensuite de planifier et prioriser les interventions nécessaires. Nous procédons enfin à la remise en état en réduisant les indisponibilités du système. Notre expertise nous permet également d'intervenir sur des sites industriels neufs. La cybersécurité est ainsi intégrée dès la conception. »

Jocelyn Zindy,
directeur commercial Cybersécurité et Transformation numérique

Certifications

Connaissance approfondie des nombreux référentiels (loi de Programmation Militaire, PIMSEC ANSSI, IEC 62443)

Références Clients

Automobile / Environnement / Défense / Agro-alimentaire / Chimie / Pharmacie / Nucléaire / Spatial / Aéronautique

Premier éditeur européen de solutions de sécurité*

Indépendance, intégrité, connaissance et expertise sont les fondements qui guident et motivent nos collaborateurs depuis plus de 30 ans. Située au coeur de l'Europe et présente dans plus de 200 pays, la société ESET est détenue majoritairement par ses quatre fondateurs. Pionnier en matière de détection proactive des menaces, ESET est aujourd'hui le leader dans ce domaine et protège plus d'un milliard d'internautes dans le monde.

Société : ESET
Adresse : 20 allée Louis-Calmanovic
93320 Les Pavillons-sous-Bois
Tél. : 01 55 89 08 85
Site web : **www.eset.com/fr**

Spécialisations

- **Protection Endpoint (postes, serveurs, mobiles, données)**
- **Protection des serveurs de messagerie et des outils collaboratifs**
- **Endpoint Detection and Response (EDR)**
- **Sandbox Cloud**
- **Managed Detection & Response**
- **Health Check**
- **Déploiement & Upgrade**

Chiffres clés

Effectif mondial : plus de 2 000 collaborateurs et chercheurs
R&D : 13 laboratoires

Twitter : **@ESET_France**
LinkedIn : **esetfrance**
Blog : **welivesecurity.com/fr**

Contacts
Thierry DEFOIS
Directeur commercial
thierry.d@eset-nod32.fr

Nicolas CHAUBARD
Directeur clients finaux
nicolas.c@eset-nod32.fr

Références *

**Liste non exhaustive*

spie batignolles
Gendarmerie nationale
HONDA
Musée de l'Armée Invalides
Allianz Suisse
Canon

Partenaires

MEMBRE DU DISPOSITIF
CYBERMALVEILLANCE.GOUV.FR
RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Offres

Légère, efficace et actuelle, ESET propose une gamme complète de solutions pour protéger le patrimoine numérique des entreprises, en prenant en compte les contraintes liées au télétravail et nomadisme grandissant. S'appuyant sur le moteur maintes fois primé NOD32, nos clients nous recommandent pour notre simplicité de déploiement, d'administration et notre capacité à assurer une protection contre les menaces courantes autant que les menaces ciblées (APT) et ransomwares. Proches de nos clients, nos 11 implantations France et Afrique francophone vous accompagnent pour garantir la réussite de vos projets.

Protégez vos postes de travail, serveurs et terminaux mobiles
Les solutions de sécurité ESET endpoint réunissent technologie multi-couche, machine learning et expertise humaine pour offrir un juste équilibre entre performance, détection et faux positifs.

Pilotez la sécurité de vos terminaux depuis un point central
Offrant une visibilité complète et des fonctionnalités d'administration puissantes, ESET PROTECT (sur site ou dans le Cloud) simplifie le déploiement, l'administration et la gestion au quotidien. Bénéficiez d'un contrôle granulaire aisé de vos stratégies depuis la console.

Contrez les attaques ciblées (APT) et prévenez les menaces zero-day
Détectez en temps réel les comportements anormaux et réagissez immédiatement grâce à ESET Enterprise Inspector. Identifiez les menaces inconnues avec ESET Dynamic Threat Defense grâce à une Sandbox Cloud qui simule le comportement d'un utilisateur pour contrer les techniques d'évasion.

Protégez vos données et sécurisez vos moyens d'accès
Protégez vos données en les chiffrant avec ESET Endpoint Encryption et renforcez leurs accès avec une double authentification assurée par ESET Secure Authentication.

Services

Professional Services
Des techniciens experts sont d'astreinte pour répondre aux besoins en cybersécurité des entreprises avec une assistance 24h/24, 7J/7, proposant également Déploiement, Upgrade et Health Check.

Security Services pour Endpoints & EDR
ESET Security Services pour Endpoints fonctionnent avec vos produits de sécurité ESET afin de fournir une solution de sécurité complète qui agit de manière préventive, réactive et proactive. Accélérez également la détection et la remédiation des incidents liés à l'EDR grâce à la recherche proactive et la surveillance des menaces avec ESET Threat Monitoring et ESET Threat Hunting..

**Source : Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019.*

LANCEMENT D'UN NOUVEAU SERVICE :

LES TABLES RONDES DE LA RÉDACTION

SOLUTIONS numériques

WEBCAST AUTOUR D'UNE THÉMATIQUE

En live ou en replay

Télétravail, Cybersécurité, RGPD, etc
Découvrez nos évènements en ligne

SÉCURITÉ D'ACTIVE DIRECTORY : POURQUOI ÉCHOUONS-NOUS ET QUELS DÉTAILS ÉCHAPPENT AUX ADMINISTRATEURS ?

REPLAY du 7 Octobre 2021
AvecTenable

CLOUD DE CONFIANCE : LE PROJET DE L'ETAT, AVEC KPMG

REPLAY du 21 Septembre 2021
Evènement Thales, en partenariat avec Solutions-Numeriques

LA SÉCURITÉ APPLICATIVE À L'ÈRE DU DEVSECOPS : DÉTECTER ET CORRIGER LES FAILLES DE VOS APPLICATIONS WEB

REPLAY du 16 Septembre 2021
Avec Rohde-Schwartz Cybersecurity et Yes We Hack

CYBERSECURITE DES ENVIRONNEMENTS INDUSTRIELS

REPLAY du 1er Juillet 2021
Avec Keysight et Advens

CISCO CYBERSECURITY DAY
Visionnez chacune des conférences

REPLAY du 29 juin 2021
Evènement Cisco, en partenariat avec Solutions-Numeriques

Replay : solutions-numeriques.com/webinar

30 ans d'expérience en cybersécurité avec toujours le même moteur : l'innovation

Société : F-Secure
Adresse : immeuble Seine-Way - bât G
12-14 rue Louis-Blériot
92500 Rueil-Malmaison
Tél. : 01 41 29 23 23
Site web: **www.f-secure.com**
Mail : **sales-france@f-secure.com**

Spécialisations

F-Secure couvre tous les aspects de la cyber sécurité. Nous disposons de 30 années d'expérience dans le domaine de la sécurité, au cours desquelles nous avons conçu les outils les plus performants pour lutter contre la cybercriminalité.
Nos solutions et services permettent de :

- **bloquer les attaques avant qu'elles ne pénètrent le réseau**
- **réduire le potentiel des malware en minimisant les vulnérabilités**
- **empêcher les applications malicieuses d'être exécutées sur le périphérique**
- **détecter & répondre aux événements inhabituels générés par une attaque ciblée**

Chiffres clés

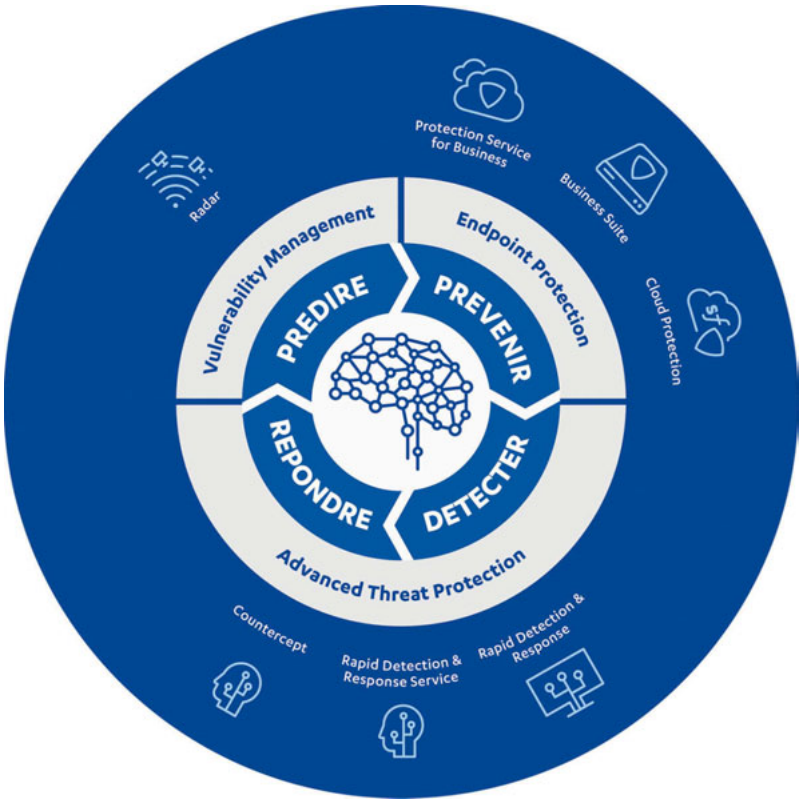
CA : 2020 (NC)
Croissance à +20 % à date
2019 : 217,3 M€
Effectifs : 1 700 employés dans le monde.

Dirigeants

Juhanni INTIKKA
Juhanni Intikka est CEO de F-Secure depuis le 20 novembre 2020. Il a occupé des postes de direction dans diverses industries telles que les télécommunications, les logiciels et la manutention des matériaux et possède une expérience de conseil d'administration dans les secteurs de l'aviation et de la construction.

Guillaume GAMELIN
Guillaume Gamelin est Country Sales Manager France chez F-Secure et possède une expérience de plus de 15 ans sur le marché de la sécurité informatique.

Les offres



Fondée en 1988, F-Secure est une entreprise finlandaise spécialisée en cybersécurité et cotée au Nasdaq OMX Helsinki Ltd. Depuis plus de trente ans, nous protégeons des dizaines de milliers d'entreprises et des millions de particuliers grâce à notre réseau de partenaires de distribution, et plus de deux cents fournisseurs de services. Des solutions de protection des postes de travail à la détection et réponses aux menaces avancées, nous veillons à ce que nos utilisateurs puissent compter sur une cyber sécurité de haut-niveau. L'alliance unique de l'expertise humaine de solutions logicielles et d'Intelligence artificielle nous permet d'être reconnu comme un acteur incontournable du marché européen.

Récompenses

F-Secure a remporté ses huitième et neuvième awards *« Best Protection »* d'AV-Test – pour ses solutions pour les particuliers et les entreprises – ainsi qu'un award *« Best Performance »* pour les particuliers. Grâce à sa technologie de pointe, F-Secure est la seule entreprise à avoir remporté au moins un prix *« Best Protection »* de AV-TEST lors de sept des dix derniers comparatifs annuels au cours de ces dix dernières années. Une régularité dans les performances inégalée à ce jour.

Références clients

Société : FORTINET FRANCE Sarl
Adresse : Tour Atlantique, 24e étage
1 place de la Pyramide,
92911 Paris La Défense Cedex
Tél. : +33 (0) 1 80 42 05 40
Mail : **france_marketing@fortinet.com**
Site web : **www.fortinet.fr**

Nom des marques
Les marques de Fortinet incluent, sans s'y limiter : Fortinet, FortiGate, FortiGuard Labs, FortiCare, FortiManager, FortiAnalyzer, FortiOS, FortiASIC, FortiMail, FortiClient, FortiEDR, FortiSIEM, FortiSandbox, FortiWiFi, FortiAP, FortiSwitch, FortiWeb, FortiADC, , FortiCloud, FortiNAC, FortiAI, FortiSASE…

Spécialisations

Next Generation Firewall, Data Center&IPS, Endpoint Security, Virtualized Next-Generation Firewall, Secure Wi-Fi, Application Delivery Controllers, Security Subscriptions, Sandbox, Web Application Firewall, AWS/Azure/GCP Security, DDoS, Management, Email Security, SIEM, Cloud Access Security Broker, Identity and Access Management, Network Access Control, SD-WAN, Endpoint protection, SASE, Zero Trust

Chiffres clés

CA 2020 : $ 2.59 milliards
Effectifs : 9000 employés

Dirigeant
Entrepreneur expérimenté, Ken XIE a débuté sa carrière en créant sa première entreprise de sécurité réseau, Stanford InfoSystem, Inc. en 1993. Quelques années plus tard, il créera NetScreen (NASDAQ: NSCN), avant de fonder Fortinet en 2000, dont il est l'actuel PDG.

Contact
Le bureau de représentation français est dirigé par Mme Claire SOUHAUT, Country Manager, qui possède plus de trente années d'expérience sur le marché IT français.

Fortinet (NASDAQ : FTNT) protège les personnes, les appareils et les données, et permet à plus de 530 000 clients de toutes tailles, d'accélérer en toute sécurité leurs échanges numériques. Fortinet est classé au 1er rang pour le nombre d'appliances sécurisées délivrées dans le monde. La plateforme Fortinet Security Fabric sécurise les appareils, les données, les applications et les connexions critiques du Data Center au Cloud en passant par le travail à domicile. Le Fortinet NSE Training Institute propose l'un des programmes de formation les plus vastes et les plus larges du secteur afin de rendre la formation à la cybersécurité et les nouvelles opportunités de carrière accessibles à tous. Pour en savoir plus, consultez le site https://www.fortinet.com/fr***, le*** blog Fortinet ***ou*** FortiGuard Labs***.***

Offres

Des réseaux filaires/sans fil aux plateformes de messagerie, applications web, bases de données et davantage, les solutions Fortinet sécurisent les infrastructures réseau et les données d'entreprise, dans leur intégralité, permettant ainsi aux organisations utilisatrices de garder la main sur leurs réseaux, leurs utilisateurs et leurs données. En parallèle, les solutions de reporting et de gestion centralisées de Fortinet permettent de gérer et de surveiller tous les environnements, de quelques équipements à plusieurs milliers d'appliances et d'agents sur les postes clients. Les utilisateurs bénéficient ainsi d'une administration simplifiée et d'une visibilité précise sur leur statut de sécurité en temps réel.

Services

Le FortiGuard Labs est l'organisme de renseignement et de recherche sur les menaces de Fortinet. Sa mission est de fournir aux clients de Fortinet les meilleurs renseignements sur les menaces de l'industrie afin de les protéger contre les activités malveillantes et les cyber- attaques sophistiquées. Il est composé de chasseurs de menaces, chercheurs, analystes, ingénieurs et spécialistes des données parmi les plus compétents de l'industrie, travaillant dans des laboratoires de recherche spécialisés dans le domaine de la menace dans le monde entier. Le FortiGuard Labs surveille en permanence la surface d'attaque mondiale en utilisant des millions de capteurs réseau et des centaines de partenaires de partage de renseignements. Il analyse et traite ces informations en utilisant l'Intelligence artificielle (IA) et d'autres technologies innovantes afin d'exploiter ces données pour détecter de nouvelles menaces.

Ces efforts se traduisent par des renseignements sur les menaces qui peuvent être exploités en temps utile, sous la forme de mises à jour des produits de sécurité Fortinet, de recherches proactives sur les menaces pour aider les entreprises à mieux comprendre les menaces et les acteurs auxquels ils sont confrontés, et en fournissant des services de conseil spécialisés pour aider nos clients à identifier et à renforcer leur exposition à la sécurité.

Solutions

• Certifications, labels ou Points Forts
Fortinet possède plus de certifications produit que n'importe quel autre constructeur d'appliances de sécurité. Ces certifications délivrées par des tiers démontrent la capacité de l'entreprise à consolider de nombreuses technologies de sécurité dans un seul système tout en respectant les plus hauts standards de performances et de précisions.

La qualité des fonctions de sécurité est également certifiée par des organisations indépendantes telles que ICSA Labs, NSS Labs et Virus Bulletin 100. Plusieurs certifications gouvernementales ont également été obtenues telles que FIPS 140-2, Common Criteria eAL2 et eAL4+ et d'autres certifications majeures liées à IPv6 et à ISo9001. Fortinet a également reçu plus de 785 brevets et a plus de 220 brevets en cours de validation.

• Références Clients
Fortinet possède de nombreuses références clients dans tous les secteurs d'activité et dans toutes les catégories d'entreprises parmi lesquelles en France, Lagardère Group, le CG 92, Pierre&Vacances, Lyreco, HR Path, VGRF, Vinci Park, Vinci Energies, Cerna Santé, L'Edhec Business School…

Votre réseau n'est pas bien protégé? Rencontrez Fortinet

La Fortinet Security Fabric
sécurise les bordures
partout où vous en avez besoin

FORTINET®

www.fortinet.fr

Copyright © 2021 Fortinet, Inc. All rights reserved.

GATEWATCHER

Société : GATEWATCHER
Adresse : 75, boulevard Haussmann
75008 Paris
Tél. : 01 44 51 03 93
Mail : **contact@gatewatcher.com**
Site web : **www.gatewatcher.com**

Spécialisations

- **Network Detection & Response (NDR)**
- **Cyber Threat Intelligence (CTI)**
- **Networks Intrusion Detection System**
- **Détection des APT's**
- **Sécurité IOT et OT**

Chiffres clés :

Effectifs : plus de 60 collaborateurs

Dirigeants
Jacques
de LA RIVIÈRE
Fondateur – CEO

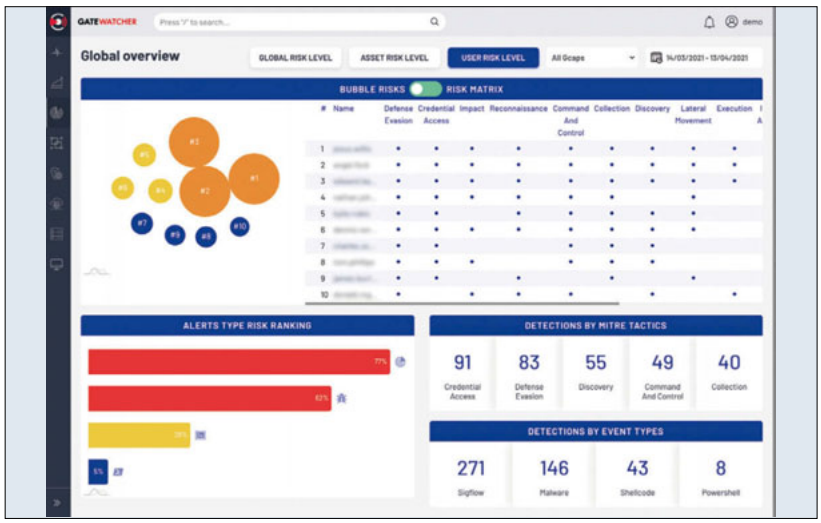
Philippe GILLET
Fondateur - CTO

Historique

2015 : création de Gatewatcher
2016 : label France Cybersécurité
2017 : lauréat du Prix spécial du jury FIC
2018 : lauréat du Silicon Cybersecurity Awards (Meilleure solution de détection)
2019 : qualification élémentaire de l'Anssi pour la plateforme Trackwatch
2020 : rachat de LastInfoSec, acteur spécialisé en Cyber Threat Intelligence. Lauréat du prix Com Cyber décerné par le ministère des Armées
2021: Gatewatcher lance Aioniq, son offre *Network Detection and Response*
2022 : membre fondateur du Campus Cyber

Révéler les cybermenaces avant qu'elles n'assombrissent votre activité

Gatewatcher est un leader européen de la cybersécurité spécialisée dans la détection des intrusions et menaces avancées ainsi qu'en Threat Intelligence. Il édite notamment la plateforme Trackwatch® qualifiée par l'Anssi. Développé en France par une équipe pluridisciplinaire d'experts en sécurité de haut niveau, son modèle de protection associe des technologies de pointe à l'IA pour répondre à toutes les techniques d'attaque en identifiant les éléments propres à chaque cybermenace.



Offres

Gatewatcher s'adresse aux OIV et OSE dans leur mise en conformité à la Loi de Programmation Militaire ainsi qu'à toute entreprise, organisation ou institution à la recherche d'une capacité de détection optimale tout en disposant de solutions rapidement opérationnelles et offrant une forte interopérabilité avec leur infrastructure.

- **Aioniq®** est une nouvelle plateforme de détection et de réponse qui permet d'identifier avec certitude les actions malveillantes et les comportements suspects par une cartographie de l'intégralité des assets présents sur le SI. L'association de cette capacité avec des performances inédites d'analyse des flux réseau chiffrés permet d'offrir une modélisation complète et précise du niveau de risque cyber associé à chaque connexion entre assets et utilisateurs, pour un niveau de détection et de visibilité inégalé.
- **Dualwatch®** est un IDS Next-Gen qui analyse statiquement et dynamiquement votre réseau et prévient d'un large panel d'attaques, des plus simples aux plus complexes. Facile à déployer, la solution contribue à réduire immédiatement le risque cyber au sein de votre organisation
- **Trackwatch®** garantit une détection à 360° en temps réel de tous les types d'attaques et intrusions grâce à la combinaison d'algorithmes d'apprentissage automatique et de différentes méthodes d'analyse du trafic et de détection contextuelle des anomalies. Qualifiée par l'Anssi depuis 2019, la plateforme est déployée au sein des organisations les plus critiques et les plus exposées (banque, industrie, énergie...)
- **LastInfoSec®** est une plateforme de Threat Intelligence visant à fournir une amélioration immédiate de votre niveau de protection. Sa technologie exclusive associe machine learning et traitement Big Data pour générer en un temps très court un flux d'information de haute qualité sur les cybermenaces.

Certifications

GATEWATCHER

AIONIQ

Augmented Detection

100%
assets
cartography

100%
NDR

100%
cyber-risks
modeling

www.gatewatcher.com

GlobalSign, fournisseur leader en solutions d'identité et de sécurité

Société : GLOBALSIGN
Tél. : +33 9 75 18 32 00
Mail : **sales-fr@globalsign.com**
Site web : **www.globalsign.fr**

Créée en 1996 et première Autorité de Certification européenne, GlobalSign est un prestataire de services d'identité qui fournit des solutions PKI hautement évolutives sur le Cloud pour les entreprises ayant besoin de gérer la sécurité de leurs transactions commerciales, communications, offres de contenu et interactions au sein des communautés. Au service d'entreprises, grands groupes, fournisseurs de services cloud du monde entier et innovateurs dans le domaine de l'IoT, elle permet de sécuriser les communications en ligne, de gérer des millions d'identités numériques vérifiées et d'automatiser les processus d'authentification et de chiffrement. Ses infrastructures PKI de pointe et solutions d'identités répondent aux besoins des milliards de services, de terminaux, de personnes et d'objets qui composent l'IoT.

Spécialisations

- **Contrôles d'accès authentifiés**
- **Sécurité des réseaux & infrastructures**
- **Sécurité applicatives & des données**
- **Sécurité des e-mails & documents**
- **Sécurité mobile**
- **Sécurité de l'IoT**
- **Conformité eIDAS**

Chiffres clés

25 millions de certificats reposent sur notre racine de confiance

Effectifs : 130 en Europe / 530 dans le monde

Références clients

Edenred, Monext, Petit Bateau, Avril, Groupe BPCE

Dirigeant
Henry KRUMINS
PDG de GlobalSign zone EMEA
Directeur des Ventes et du Marketing EMEA/AMER

Contacts

Olivier MARSET
Chargé de compte France
olivier.marset@globalsign.com

Arnaud VANDERROOST
VP des ventes EMEA
arnaud.vanderroost@globalsign.com

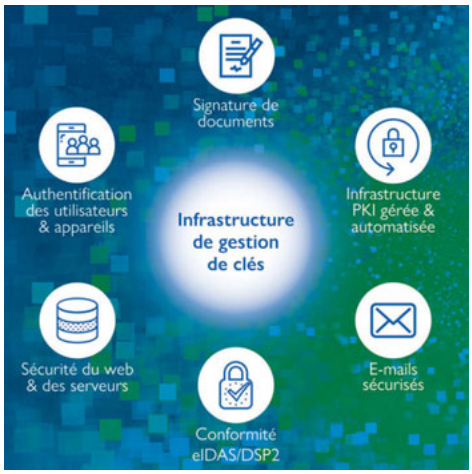
Ronald de TEMMERMAN
VP des ventes Stratégiques - EMEA
ronald.detemmerman@globalsign.com

Offres

- Avec nos solutions de certificats numériques, des milliers de clients authentifiés effectuent, grâce à la sécurité SSL, leurs transactions en ligne, transfèrent des données, distribuent du code inviolable et protègent leurs identités en ligne pour sécuriser leurs e-mails et contrôles d'accès.
- **Produits et services qualifiés :** Prestataire de services de confiance qualifié (PSCQ), GlobalSign fournit des certificats qualifiés de signatures électroniques, de cachets électroniques (certificats QSealC) et d'authentification de site internet (certificats QWAC), ainsi que des sceaux d'horodatage qualifiés conformes à l'eIDAS. Nos certificats QWAC et QSealC conformes à la DSP2 permettent notamment d'identifier de façon unique le prestataire de services de paiement, son numéro d'autorisation, son rôle et le nom de l'autorité nationale compétente auprès de laquelle il s'est enregistré.

Solutions

- **Portail AEG :** solution d'infrastructure à clé publique gérée et évolutive conçue pour les environnements hétérogènes des entreprises. Il sert de passerelle directe entre **Atlas, AC cloud nouvelle génération de GlobalSign,** et l'annuaire *Active Directory*, élargissant sa portée à l'ensemble des terminaux de votre réseau. Prise en charge des protocoles SCEP et ACME v2.
- **Plateforme Managed PKI :** service de gestion du cycle de vie sur le Cloud qui centralise la gestion de la facturation, des certificats et utilisateurs pour réduire le TCO et simplifier les déploiements.
- **Service de signature numérique sur le Cloud (GMOSign) :** élargit l'accès aux signatures numériques à toutes les entreprises. En plus de l'intégration aux solutions de workflow documentaire, il lève les freins sur les questions de coûts, de maintenance et d'expertise technique. Disponible sur la plateforme Atlas dès septembre 2020.



Certifications

- Accréditation WebTrust depuis 2001
- Membre fondateur du CA/B Forum
- Membre du Conseil de sécurité des autorités de certification (CASC)
- Membre de la liste AATL (Adobe Approved Trust List) et Microsoft Root Trust List
- Accrédité PSCQ au titre de l'eIDAS et figure à ce titre sur la liste de confiance de la Belgique et du Royaume-Uni
- Certifications ISO27001 (management de la sécurité de l'information) et ISO22301 (management de la continuité d'activité) du British Standards Institute

GlobalSign®
GMO INTERNET GROUP

Facilitez le déploiement de vos signatures numériques grâce à notre service cloud évolutif disponible sur Atlas, notre nouvelle plateforme PKI

Service de signature numérique à la volée

- Intégration transparente aux workflows existants
- Respect de la conformité (directive sur la facturation électronique)
- Sur Atlas : processus d'achat simplifié, capacités d'automatisation et de gestion du cycle de vie étendues, interruptions de service évitées
- Identités de signature au niveau individuel ou de l'organisation
- Horodatage fiable, intégrité du contenu, non-répudiation
- Matériel et expertise en PKI non requis

1ère Autorité de Certification établie en Europe depuis 1996, **GlobalSign** est un fournisseur leader de solutions de confiance pour la **sécurité** et la gestion des **identités** aux innovations uniques autour de l'automatisation. Elle est reconnue comme **Prestataire de services de confiance qualifié eIDAS** pour les signatures et services qualifiés sur le marché numérique en Europe.

www.globalsign.fr | +33 9 75 18 32 00 | ventes@globalsign.com

Spécialiste de la Cybersécurité des Infrastructures Critiques et Industrielles

Société : HOLISEUM
Adresse : 5, place de la Pyramide
92088 Paris La Défense
E-mail : **contact@holiseum.com**
Site web : **https://www.holiseum.com**

Spécialisations

Cybersécurité industrielle, infrastructures critiques, Maritime, SCADA, SI de sûreté, IT, IoT, LPM, NIS, etc.

Notre approche globale, dite holistique, de la sécurité nous confère un point de vue privilégié pour adresser efficacement les risques multifactoriels de nos clients :

- ***Couverture de l'ensemble de la chaîne de valeurs des services en cybersécurité,***
- ***Adresser de manière transverse les processus d'une organisation et ses environnements (IT/OT/SI Sûreté/IoT),***
- ***Pluridisciplinarité faisant converger les disciplines Cybersécurité, Sûreté et Intelligence Économique.***

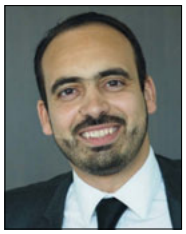
Nos secteurs d'interventions de référence :

Maritime

Industrie

Énergie

Banque/Finance



Dirigeants
Faïz DJELLOULI
Co-fondateur et Président

An NGUYEN
Co-fondateur et Directeur général

Conseil et services

Nos consultants interviennent sur des missions à forte valeur ajoutée et sur des problématiques et contextes complexes au travers de nos cinq rôles :

- **CONSEILLER**
Aider votre organisation à établir ou développer une stratégie globale de sécurité.
- **AUDITER**
Une gamme complète d'audits, du plus élémentaire au plus complexe (Audit 360 de sites industriels, pentests…)
- **SÉCURISER**
Mise en œuvre de projets de sécurisation et intégration de solutions cybersécurité.
- **FORMER**
Sensibiliser les utilisateurs de votre entreprise aux problématiques de la cybersécurité.
- **INVESTIGUER**
Faire la lumière sur les compromissions avérées ou supposées.

VISA DE SÉCURITÉ — ANSSI

« La qualification PASSI de Holiseum sur les cinq portées d'audit du référentiel de l'Anssi témoigne de la diversité de nos expertises et de notre approche holistique de la cybersécurité, consistant à aborder les problématiques de cybersécurité dans toute leur complexité et leur dimension multifactorielle. »

Faïz DJELLOULI

Éducation

SENSIBILISATION ET FORMATION

Nous organisons des sessions de **Sensibilisations** et/ou **Formations** dans divers domaines (Cybersécurité industrielle, Blockchain, IoT, Radio, etc.) adaptables à tout niveau d'expérience.
Nous développons également nos propres démonstrateurs industriels dans les domaines de la cybersécurité, la sûreté, le maritime etc.

WEB-SERIE ÉDUCATIVE

CYBER VOX est une chaîne dédiée à la vulgarisation des menaces cyber et de la cybersécurité.
Le but : faire de l'éducation populaire centrée sur la cybersécurité, mais aussi fédérer les professionnels autour d'une vision partagée.
https://bit.ly/31RPWOV

SERIOUS GAME

CYBER WARGAME est un serious game qui plonge vos collaborateurs dans un contexte d'attaque – défense cyber portant sur les actifs d'une organisation. Le jeu Cyber Wargame est disponible en version **physique** et **numérique.**
www.cyber-wargame.com

HOLISEUM

Holiseum lance le premier Tir à Blanc de Ransomware du marché !

Problématique :

« Comment connaître le niveau de résilience de mon SI face au risque particulier du Ransomware? »

Le Tir à Blanc de Ransomware est une solution qui s'appuie sur un Ransomware de notre conception - **inoculé volontairement dans le SI client** - qui permet de tester en conditions réelles l'étendue des actions pouvant y être réalisées.

Bien qu'il soit **démuni de sa charge malfaisante**, ce ransomware déploie les techniques les plus sophistiquées utilisées par les attaquants.

BÉNÉFICES ATTENDUS :

1 TEST

Tester les défenses en place (antivirus, EDR, sonde IDS/IPS, réactivité du SOC etc.)

2

Cartographier les actifs compromis, les chemins de propagation et les vulnérabilités exploitées

3

Identifier un plan d'actions permettant de cibler la menace des ransomwares

Réservez dès maintenant votre créneau de présentation avec nos experts : contact@holiseum.com

PROGRAMME

Introduction à la cybersécurité

ESSCYBER
Essentiels techniques de la cybersécurité
SECUCYBER
Fondamentaux techniques de la cybersécurité

Sécurité des réseaux et des infrastructures

SECUARCH
Sécurité des architectures
SECUWIFI
Sécurité et Red Team Wi-Fi moderne
SECUPKI
Infrastructures de clés publiques
SECUPKIWIN
Infrastructures de clés publiques Windows

Sécurité défensive

SECUWIN
Sécurisation des infrastructures Windows
SECULIN
Sécurité Linux
SELinux
Comprendre SELinux et savoir modifier la politique de sécurité
SECUWEB
Sécurité des serveurs et des applications Web
SECUINDUS
Cybersécurité des systèmes industriels
SECUOBJ
Sécurité des objets connectés
SECUMOBILE
Audit sécurité d'applications mobiles Android et iOS

+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

HS2
Hervé Schauer Sécurité

Formation cybersécurité technique

DÉTECTION ET RÉPONSE • INFORENSIQUE • SÉCURITÉ OFFENSIVE

PROGRAMME

Détection et réponse aux incidents

OSINT
Formation OSINT/CTI
SECUSOC
Surveillance, analyse et corrélation
SECUBLUE1
Surveillance, détection et réponse aux incidents de sécurité
SECUBLUE2
Surveillance, détection et réponse avancée aux incidents de sécurité
SPLUNK
Formation SPLUNK
ELASTICSEARCH
Formation ELASTICSEARCH

Inforensique

FORENSIC1
Analyse inforensique Windows
FORENSIC2
Analyse Inforensique avancée
REVERSE1
Rétroingénierie de logiciels malfaisants
REVERSE2
Rétroingénierie avancée de logiciels malfaisants

Sécurité Offensive

PENTEST1
Tests d'intrusion
PENTEST2
Tests d'intrusion et développement d'exploits
PENTESTWEB
Tests d'intrusion sur applications Web
PENTESTINDUS
Tests d'intrusion des systèmes industriels

+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

Société : HUB ONE
Adresse : Continental Square Mercure
2 place de Londres
93290 Tremblay-en-France
Tél. : 01 70 03 85 00 / 01 78 76 58 00
Site web : **https://hubone.fr/**
Mail : **cyber@hubone.fr**

Dirigeant
Guillaume
de LAVALLADE
Directeur général
Hub One

Chiffres clés

136 M€ de CA en 2020
570 collaborateurs
+ de 5 000 entreprises clientes
10 agences en France

Notre vision

L'anticipation et la surveillance des menaces sont aujourd'hui maîtres mots. Il est indispensable de connaître à la fois son niveau de sécurité tout en étant sensibilisé et formé face au risque cyber. Le pôle cybersécurité d'Hub One vous accompagne pour renforcer votre système d'information, votre organisation et vous rapprocher du risque zéro.

Stand #165
#Assises de la Sécurité

Hub One est membre associé du Campus Cyber

CAMPUS CYBER ASSOCIÉ

Accompagner les entreprises dans la protection de leurs systèmes d'information

Hub One est l'opérateur de technologies digitales pour les entreprises et organisations publiques. Acteur de référence de la transformation numérique en univers contraints, Hub One s'appuie sur ses trois expertises : connectivité haut-débit, traçabilité et cybersécurité. Hub One propose le meilleur des technologies au travers de solutions éprouvées et adaptées aux besoins et usages des professionnels.

Hub One se positionne comme un acteur de référence de la cybersécurité au travers de plusieurs domaines : la formation et le cyber-entraînement, le conseil/audit, l'intégration, l'édition et le SOC. Cette expertise s'est construite au travers de ses filiales **Sysdream** *et* **Oveliane.**

Hub One est une société membre du Groupe ADP, filiale à 100 % d'Aéroports de Paris SA.

Nos Solutions

SOC

Supervisez en continu la sécurité de votre système d'information afin d'anticiper, d'identifier et de réagir face aux menaces cyber. Notre Centre opérationnel de sécurité (SOC) est hébergé en France et il est en cours de qualification PDIS.

Intégration & conseil

Obtenez tous nos conseils dans le choix des outils les plus adaptés, leur mise en place et leur intégration. Nous assurerons le maintien en condition opérationnelle et condition de sécurité de vos solutions.

Formation sensibilisation (cyber entrainement)

Améliorez la compréhension des enjeux en cybersécurité. Formez et fédérez vos collaborateurs autour de l'un de nos 42 programmes de formation et grâce à notre plateforme de cyber-entrainement MALICe en mode Attaque ou Défense.

Audit

Nos experts vous aident à évaluer le niveau de maturité de la sécurité de vos systèmes d'information. Une démarche d'accompagnement allant du diagnostic à l'analyse, jusqu'à la proposition d'un plan de transformation adapté à votre activité et vos contraintes.

Contrôle de conformité et prévention d'attaques

Outillez votre système d'information, avec notre solution Oveliane, afin d'assurer en continu le contrôle de conformité et d'intégrité de vos systèmes (respect de votre politique de sécurité, des préconisations de l'Anssi…).

Hub One
Digital Technologies

CYBERSÉCURITÉ

LUTTEZ EFFICACEMENT **CONTRE LES ATTAQUES CYBER** ET PROTÉGEZ VOTRE ENTREPRISE

HUB ONE VOUS PROPOSE UNE OFFRE GLOBALE EN CYBERSÉCURITÉ

- Audit organisationnel et technique
- Formation sensibilisation
- Contrôle de conformité et surveillance en continu des serveurs
- Intégration et expertise
- SOC (Centre Opérationnel de Sécurité)

AVEC HUB ONE ANTICIPEZ LES RISQUES POUR MIEUX PROTÉGER VOTRE ENTREPRISE

Hub One, filiale du groupe ADP, acteur de référence de la cybersécurité a construit son expertise au travers du rachat de Sysdream acteur phare de la cybersécurité et des sociétés Oveliane et OïkiaLog.

cyber@hubone.fr
01.78.76.58.00
https://hubone.fr

VISA de sécurité

OVELIANE Division Cybersécurité Hub One

SYSDREAM Division Cybersécurité Hub One

Hub One adopte une démarche responsable et engagée

Une plateforme IAM globale

Fournisseur de la plupart des grands comptes, Ilex International a su développer, depuis plus de 30 ans, une réelle expertise sur le contrôle d'accès logique et la gestion des identités et des habilitations.

Nos solutions répondent aux exigences de toutes les entreprises et organisations soucieuses de la sécurité de leur système d'information, en France comme à l'international.

Société : ILEX INTERNATIONAL
Adresse : 51 boulevard Voltaire
92600 Asnières-sur-Seine
Tél. : 01.46.88.03.40
Mail : **info@ilex-international.com**
Site web : **www.ilex-international.com**

Spécialisations

Éditeur de logiciels de gestion des identités et des accès

Dirigeants

Olivier MOREL
Directeur général

Fabrice BÉROSE
Directeur commercial & marketing

Offres

En tant que 1er éditeur français de solutions de gestion des identités et des accès, notre objectif est de proposer une plateforme IAM globale, capable de répondre à l'ensemble des besoins de nos clients grands comptes et ETI, et de couvrir tous leurs cas d'usage utilisateurs, qu'il s'agisse de leurs collaborateurs, leurs partenaires et prestataires, ou de leurs clients finaux (CIAM).

Notre plateforme permet de couvrir à la fois tous les domaines de la gestion des accès mais également de traiter toutes les problématiques de la gestion des identités et des habilitations.

- **Suite Ilex Identity :** solutions dédiées à la gestion des identités et des habilitations parfaitement adaptées aux besoins de tous types d'organisations.
- **Suite Ilex Access :** offre complète et modulaire de gestion des accès permettant de gérer l'intégralité des problématiques d'authentification renforcée et adaptative, de Web Access Management, de fédération d'identité, de eSSO et de Mobile SSO.

Notre offre est disponible en modes On-Premise & SaaS.

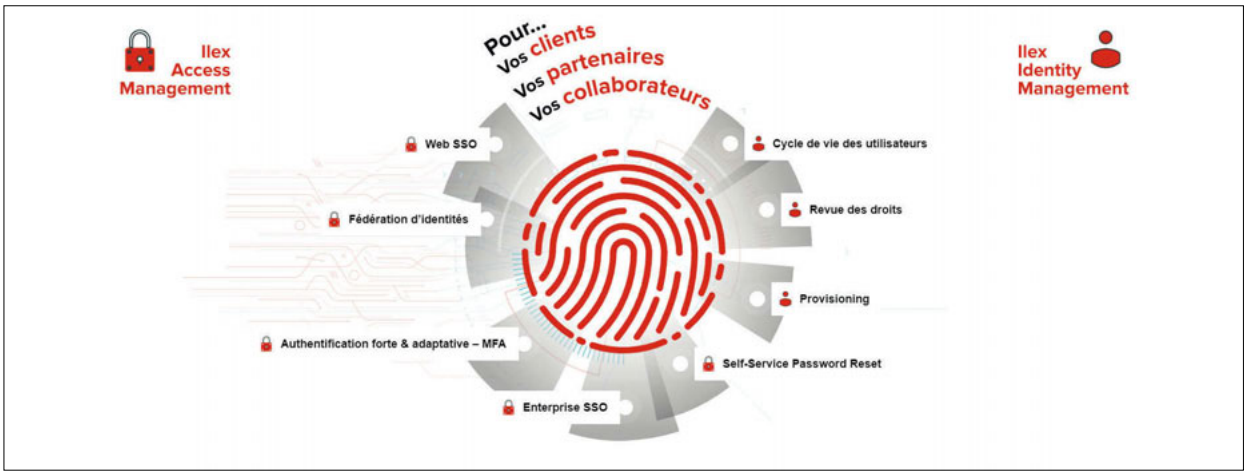
Afin de garantir une mise en œuvre optimale de leur projet IAM, nos clients peuvent compter sur nos partenaires intégrateurs, ainsi que sur nos équipes Professional Services. Notre mission est de contribuer à la réussite du déploiement de nos solutions comme à la satisfaction client. Nous restons également impliqués dans la durée pour fournir le support éditeur adéquat et accompagner nos clients pour que leur plateforme IAM puisse évoluer en fonction de leurs besoins.

Vos enjeux sont les nôtres

- Sécurité
- Conformité réglementaire
- Expérience utilisateur
- Transformation digitale
- Ouverture du système d'Information
- Retour sur investissement (ROI)

Références clients

En accompagnant nos clients issus de nombreux secteurs d'activité tels que les banques et assurances, la défense, la santé, les médias, les énergies et la distribution, ce sont aujourd'hui plus de 14 millions d'utilisateurs en France et à l'international qui bénéficient de nos solutions IAM.



infoclip

Société : INFOCLIP
Adresse : 20 rue de La Michodière, 75002 PARIS
Tél. : 01 43 18 19 20
Mail : **contact@infoclip.fr**
Site web : **www.groupe-infoclip.com**

Spécialisations

- **CyberSécurité**
- **Cloud souverain**
- **Infogérance**

Historique

Fondé en 1989, le Groupe INFOCLIP se classe aujourd'hui comme un prestataire global et incontournable de solutions cloud et sécurité pour les PME et ETI

Dirigeant
Éric MELKI
Co-fondateur & Dirigeant

E-mail : **emelki@infoclip.fr**

La Cyber Sécurité est l'enjeu majeur des PME et ETI pour 2022.

En effet, selon l'Anssi, le nombre d'attaques sur les PME et ETI a été multiplié par quatre ces douze derniers mois.

En Europe, la moyenne hebdomadaire sur 2021, des attaques par organisation est de 777, en augmentation de 36 %. (CheckPoint Research). En France, en cas d'attaque par ransomware, 25 % des entreprises optent pour le paiement d'une rançon qui s'élève en moyenne à 130 000 €.

Notre objectif est d'accompagner les PME et ETI à relever ce défi pour assurer la continuité de leur business. Nous avons souhaité créer une offre simple, lisible et accessible : CyberExcellence qui s'accompagne d'un indicateur de mesure et suivi de l'exposition, CyberRésistance©.

Évaluez votre Score CyberRésistance© et renforcez votre cyber résilience

La sécurité est généralement considérée comme une charge et non comme un investissement. On peut considérer que c'est vrai… tant que l'entreprise n'est pas victime d'une attaque. Mais alors le prix à payer est considérable et l'on comprend pourquoi la cybersécurité est une composante incontournable au service du business de l'entreprise.

Le Score CyberRésistance© permet à l'entreprise de connaître son niveau d'exposition face aux attaques ; c'est un outil stratégique pour mesurer l'efficacité des mesures de sécurité mises en place.

Offre CyberExcellence

Scoring CyberRésistance©

- Installation des sondes et outils de tests et de scoring
  – analyses des données collectées
- Formalisation du rapport et établissement de votre score
- Élaboration des recommandations
- Plan d'actions et propositions d'amélioration

Sécurisation

- Mise en place des comités de suivi
- Mise en place de la charte informatique / conformité RGPD
- Sensibilisation des collaborateurs
- Déploiement des solutions antivirales / firewall / DLP / Authentification renforcée / Durcissement des solutions cloud

Détection

- Mise en place d'un SOC pour détecter en temps réel les menaces pesant sur vos actifs
- Identification de la menace et de sa gravité potentielle en fonction du métier et des actifs
  – aide à la décision et conseil de classification sur la menace
- État des services de production
  – blocage de l'attaque et nettoyage
- État des services de production
  – supervision 24h/24 des services critiques pour vos activités et alertes automatiques. Traitement proactif

Cellule de crise

- Gestion de crise
  – déclenchement et gestion de la cellule de crise.
  – quel que soit le système présentant une défaillance (interne/ partenaire / fournisseur)
- Communication interne et externe
  – préparation d'un plan de communication et outils éventuels pour communiquer auprès des équipes internes et des parties prenantes externes (clients / fournisseurs / Autorités)
  – gestion 24h/24 de l'évènement
  – maintien d'une équipe de gestion et fourniture d'outils
  – suivi des parties prenantes
  – suivi des jalons et des communications des parties prenantes au traitement et à la résolution de l'incident

Retour au nominal et remédiation

- Pilotage
- Remédiation
- Restauration des données et systèmes le cas échéant
- Reprise des activités
- Retour à la normale
- Capitalisation

CyberAssurance

- Accompagnement
  – prise en compte des contraintes liées aux contrats de Cyber assurance
  – analyse et mesure des écarts entre les attendus et l'existant
  – proposition d'adaptations
  – mise en place des correctifs
  – assistance à la sélection des contrats et compagnies d'assurance
- Questionnaire Cyber
  – accompagnement au questionnaire Cyber de l'assureur
- Suivi contractuel
  – fourniture de liste des éléments à superviser pour assurer la conformité

Certifications

ISO 27001 — ISO 9001:2015 — ITIL

Société : IN GROUPE
Nom des marques : NEXUS SMART ID
Adresses :
Nexus France : *104 avenue du Président-Kennedy – 75016 Paris*
Nexus Sweden :
Telefonvägen 26, Hägersten
Stockholm – Sweden
Mail : **contact@ingroupe.com**
contact.fr@nexusgroup.com
Site web : **www.ingroupe.com**

Spécialisations

Identités électroniques, Authentification forte, Credential Management, Sécurité IoT, convergence logique et physique.

Chiffres clés

CA : 427 M€
Effectifs : 1 700 personnes

Historique

Date de création : 1538

Dirigeants

Philippe FONTON
Country Manager France-Benelux-South
01 40 07 06 06

Olivier DUSSUTOUR
CEO Nexus Group

Contacts :
Tél. : 01 40 07 06 06

IN Groupe, entreprise de souveraineté numérique, procure des solutions d'identité et des services numériques sécurisés pour accompagner les États dans l'exercice de leur souveraineté, protéger l'identité des citoyens et préserver l'intégrité des entreprises.

S'appuyant sur les technologies de Nexus, IN Groupe sécurise la société en permettant la production et la gestion d'identités de confiances pour les personnes et les objets. La plate-forme Nexus Smart ID intègre une gamme de produits permettant la mise en œuvre d'un environnement fluide, centralisé et automatisé pour des identités de confiance sécurisées. Cette solution contribue à l'émission et la gestion du cycle de vie d'identités électroniques de confiance pour les employés et devices ainsi que pour l'Internet des objets (IoT). IN Groupe compte 1 700 employés à travers le monde, répartis sur 6 sites principaux en Europe et plus de 10 bureaux dans le reste du monde.

Nexus Smart ID

Notre solution **Nexus Smart ID** intègre l'essentiel de notre technologie, et offre des modules standardisés, simples d'utilisation, permettant aux organisations :

- de générer et gérer les identités logiques et physiques centralement
- de dériver les identités vers des usages mobiles
- d'utiliser les identités électroniques en environnements multiples
- de sécuriser l'ensemble des accès et communications workforce, workplace, IoT

Offres

Smart ID Identity Manager
Portail de production et gestion de cartes & credential, RFID, workflows, Self-Services.

Smart ID Certificate Manager
Solutions PKI pour les utilisateurs, les devices, l'IoT.

Smart ID Digital Access
Authentification multi facteurs, Gestion des identités et des accès, ID fédération

Smart ID Mobile APP
Mobile Virtual SmartCard pour authentification, signature et chiffrement mobile.

Smart ID Desktop APP
Virtual Smartcards pour authentification, signature et chiffrement

Certifications

ISO 27001, Critères Communs EAL4+, TISAX

Références clients

Orange, Electrolux, Airbus, Vinci, ministère des Finances, Banque de France, BMW, Vodafone, Volkswagen, Siemens.

SPÉCIALISTE MONDIAL DE L'IDENTITÉ ET DES SERVICES SÉCURISÉS

IN Groupe, entreprise de **souveraineté numérique,** contribue à faire valoir pour chacun un droit fondamental : le Droit d'être soi.
Nous procurons des solutions d'identité et des services numériques sécurisés pour accompagner les **États** dans l'exercice de leur souveraineté, protéger l'identité des **citoyens** et préserver l'intégrité des **entreprises**.

IN GROUPE

LE DROIT D'ÊTRE SOI

ITrust éditeur de solutions innovantes en cybersécurité

Société : ITRUST
Adresses : 118 route d'Espagne – 31100 Toulouse
Paris : 6 rue du 4-Septembre, 92130 Issy-les-Moulineaux
Tél. : 0567 34 67 80
Mail : sales@itrust.fr
Site web : www.itrust.fr

Depuis 14 ans, ITrust réunit une équipe d'experts en architecture sécurité et tests d'intrusion. Nous vous accompagnons dans votre démarche de sécurisation, en vous proposant nos conseils, audits, pentests, MSSP, ainsi qu'une suite d'outils innovants et souverains, développés par nos équipes à Toulouse et à Paris. Notre technologie d'analyse comportementale, Reveelium, détecte les signaux faibles et les anomalies grâce aux algorithmes d'IA, de Machine learning et de corrélation qui vont analyser vos logs.

Spécialisations

Audit, Pentests, Scanner de vulnérabilité, EDR, SIEM UEBA, SOC, Machine Learning

Chiffres clés

Effectif : 60

Dirigeant
Jean-Nicolas PIOTROWSKI
Président fondateur
jnpiotrowski@itrust.fr

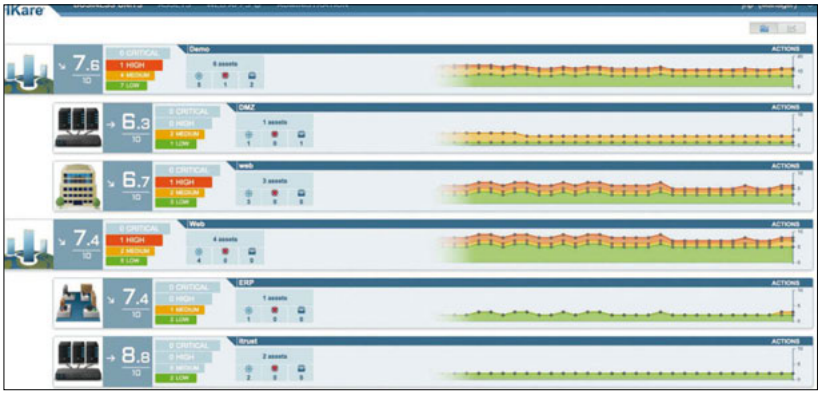
Offres

Notre activité s'articule en trois pôles :

- expertise et conseil : audit intrusif, audit organisationnel, audit de code, audit forensic, accompagnement PSSI/PRA et PCA, accompagement ISO 2700x / LPM / RGPD
- solutions de cybsersécurité : scanner de vulnérabilité IKare, EDR ACSIA, SIEM & moteur d'analyse comportementale Reveelium
- centre de contrôle de sécurité (SOC) : nous assurons totalement ou partiellement la supervision de la sécurité de votre système d'information

Solutions

- Label France Cybersécurité
- CIO Applications pour Reveelium



Interface du scanner de vulnérabilités IKare
Scoring des vulnérabilités par B.U.

Labels & prix

- Label France Cybersécurité
- TOP 25 Machine Learning Providers par CIO Applications (Reveelium)
- TOP 10 Most Valuable Cyber Security Solution Provider 2019 par CEO VIEWS
- Champions de la Croissance 2021par *les Echos & Statista*
- Certifié ISO 9001 sur l'ensemble des activités de l'entreprise

Interface du SIEM UEBA Reveelium
Classification des alertes selon la Matrice Mitre

ITrust
IT Security Services

L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE VOTRE SÉCURITÉ

Solutions Souveraines

ITrust est un acteur français, non soumis aux Patriot Act & Cloud Act

Veille sur les Vulnérabilités

IKare monitore votre SI en continu et automatise la détection des vulnérabilités.

Facturation Fixe & Adaptée

ITrust adapte sa facturation selon la taille de votre entreprise et le périmètre à surveiller

Threat Intelligence

La technologie Reveelium détecte les menaces avancées : Ransomwares, APT, Phishing...

UNE SOLUTION POUR CHAQUE BESOIN

IKare **Scanner de Vulnérabilités**	Reveelium **SIEM UEBA**
ACSIA **E.D.R**	Professional Services **Expertise & Conseil**

ITrust

ÉDITEUR DE SOLUTIONS INNOVANTES
ET EXPERT EN CYBERSÉCURITÉ

www.itrust.fr

Société : IVANTI
Adresse : Tour CBX – 15e étage
passerelle des Reflets
92400 Courbevoie
Tél. : +33 (0)1 76 40 26 20
Mail : **contact@ivanti.fr**
Site Web : **www.ivanti.fr**

Spécialisations

- **Gestion des terminaux mobiles et clients – physiques et virtuels**
- **Priorisation des correctifs basée sur les risques**
- **Gestion des correctifs OS et applications tierces**
- **Gestion des vulnérabilités basée sur les risques**
- **Contrôle des applications**
- **Whitelisting**
- **Gestion des privilèges**
- **Contrôle des périphériques**

Chiffres clés

Effectif : 3 100 collaborateurs dans 23 pays
Les solutions Ivanti sont disponibles dans 12 langues

Historique

Fondée en 2017 à la suite du rachat de LANDESK par la société d'investissement en fonds privés Clearlake Capital Group, l'entreprise combine les technologies, les biens et le personnel de LANDESK (créée en 1985 sous le nom LANSystems) et de HEAT Software (créée en 1989 sous le nom de FrontRange Solutions). Le siège social est basé à Salt Lake City – Utah (États-Unis). En juillet 2017, Ivanti acquiert RES Software.
En août 2020, TA Associates rejoint l'investisseur existant en tant qu'actionnaire d'Ivanti. La société acquiert MobileIron et Pulse Secure en 2020, puis RiskSense en 2021.

Dans l'Everywhere Workplace, les collaborateurs utilisent une multitude de périphériques pour accéder aux données et applications IT sur différents réseaux. La plateforme d'automatisation Ivanti Neurons réunit les solutions Ivanti de gestion unifiée des terminaux (UEM), de sécurité Zero Trust et de gestion des services d'entreprise (ESM), leaders du marché, afin de créer une plateforme IT unifiée permettant l'autoréparation et l'autosécurisation des périphériques, et le self-service des utilisateurs.

Solutions

Ivanti Security Controls combine les fonctionnalités essentielles dont les entreprises ont besoin pour limiter leur exposition aux risques de sécurité. Elle simplifie les processus complexes d'application des correctifs, de création de listes blanches et de gestion des privilèges. Ivanti Security Controls aide également les entreprises à passer des CVE à la correction par application de correctifs en quelques heures ou minutes.

Ivanti Neurons offre aux équipes IT le renfort de bots d'automatisation leur permettant d'anticiper les menaces de sécurité et d'autosécuriser les périphériques grâce à la cybersécurité adaptative : collecte, découverte et détection en continu des problèmes de sécurité, définition d'un ordre de priorité et correction proactive.

Ivanti Neurons for Zero Trust Access crée une connexion sécurisée entre l'appareil et les applications web sur site et dans le Cloud, ce qui renforce la sécurité, la productivité et la conformité tout en améliorant considérablement l'expérience de l'administrateur et de l'utilisateur final.

Ivanti Neurons for Vulnerability Management (de RiskSense) offre un spectre complet de gestion des vulnérabilités basé sur les risques. En quelques secondes, vous savez quelles sont les actions à entreprendre et vous accélérez la remédiation des points d'exposition aux vulnérabilités les plus importants sur votre surface d'attaque, votre infrastructure, vos applications et vos cadres de développement.

Ivanti Patch for MEM est un plug-in SCCM/Intune qui automatise la découverte et le déploiement de vos correctifs d'applications tierces via la console SCCM. Vous pouvez déployer manuellement les correctifs à l'aide des paquets de mise à jour logicielle SCCM, ou bien combiner l'automatisation Patch for MEM et les règles de déploiement automatique MEM pour automatiser entièrement la mise à jour des applications tierces.

Patch for Endpoint Manager détecte rapidement les vulnérabilités de Windows, Mac OS, Linux et de centaines d'applications tierces (Acrobat Flash/Reader, Java, navigateurs Web, etc.), et déploie des correctifs prétestés par des experts partout où vous en avez besoin.

Avec **Ivanti Neurons for Patch Intelligence,** vous collectez et réunissez dans un seul tableau de bord, les données essentielles vous facilitant la gestion, la hiérarchisation et la distribution des correctifs dans votre environnement IT.

La solution Ivanti Application Control combine 2 fonctionnalités : le blocage de tous les malwares zeroday et l'élévation des privilèges. Avec Application Control, vous gérez l'exécution des seules applications installées par un utilisateur de confiance (technologie Trusted Ownership) tout en bloquant celles non reconnues et gérez les privilèges de l'utilisateur à un niveau granulaire et contextuel (suppression des droits administrateurs et élévation à la demande).

Sales Contacts

Jean-Michel TAVERNIER
Regional Sales Director, ESG
jean-michel.tavernier@ivanti.com

José FERNANDES
Country Manager France, SSG
jose.fernandes@ivanti.com

Kemp Flowmon : Scellez les écarts de sécurité

Société : KEMP TECHNOLOGIES Ltd
Adresse : Mary Rosse Centre, Holland Road, Limerick, Ireland
Tél. : +353 61-260-101
Mail : **france-na-emea@kemp.ax**
Site web : **www.flowmon.com**

Dans un monde où la technologie est au service de l'humain, des environnements numériques sécurisés et sains sont essentiels. C'est pourquoi Kemp Flowmon a développé une solution de réseau intelligent qui permet aux entreprises de s'assurer que leurs services fonctionnent correctement et en toute sécurité, et que leur main-d'œuvre est productive.

Spécialisations

- **Détection des rançongiciels**
- **Détection des menaces internes**
- **Détection des menaces inconnues**
- **Analyse du trafic crypté**
- **Dépannage réseau et enquête d'incident**
- **NDR, NPMD, DPI, APM, DDoS**

Dirigeant
Jiri TOBOLA
VP Flowmon Business Unit

Contact
Michael MERTA
Business Development Manager
mmerta@kemp.ax

Historique

- *+10 ans de présence sur le marché ; au service d'industries telles que ISP/télécom, centre de données, entreprises de taille intermédiaire, grandes entreprises, gouvernement.*
- *+1 200 clients internationaux validant le leadership de Flowmon.*
- *4,9 étoiles sur 5, évaluation de la solution chez Gartner Peer Insights.*
- *Inclus dans le Guide du marché de Gartner pour la détection et la réponse du réseau (NDR) et le Guide du marché de la surveillance et du diagnostic des performances du réseau (NPMD).*

Offres

La solution Kemp Flowmon sert comme une plate-forme partagée où les équipes réseau et sécurité parlent le même langage. Cela favorise la coopération, un partage optimal des ressources ainsi qu'une résolution plus rapide des problèmes rencontrés. Flowmon permet aux professionnels de l'informatique d'améliorer la performance et de réduire les risques de sécurité dans les environnements sur site, de centre de données et de Cloud.

Services

Scellez l'écart entre la protection du périmètre et celle des terminaux

La sécurité est un élément clé des opérations commerciales et donc une priorité absolue pour les DSI d'aujourd'hui. Cependant, une nouvelle tendance émerge en raison du télétravail et des changements technologiques vers le mobile, le Cloud et l'IoT, remettant en cause les outils de sécurité traditionnels et créant une nouvelle surface d'attaque.

Flowmon Anomaly Detection System (ADS) est une solution de sécurité qui détecte les anomalies cachées dans le trafic réseau. La solution fournit une large gamme de méthodes de détection, y compris l'apprentissage automatique, l'heuristique, les méthodes statistiques, politiques et basées sur les signatures, qui analysent le trafic sous plusieurs angles pour contrer des comportements malveillants.

Avec Kemp Flowmon ADS, les entreprises créent un système de protection multicouche capable de détecter les menaces à chaque étape de la compromission, y compris les **rançongiciels,** les attaques contre les applications critiques, les violations de données et un éventail d'indicateurs de compromission.

Cas d'utilisation

Détection des menaces inconnues

Grâce à la reconnaissance des modèles de comportement, Flowmon peut découvrir les menaces inconnues à un stade précoce avant que tout dommage ne soit causé, offrant une zero-day protection.

Détection des menaces internes

Que les incidents soient causés par un utilisateur imprudent ou une intention malveillante, protégez votre réseau de l'intérieur.

Dépannage et enquête

La surveillance du réseau de nouvelle génération fournit des informations exploitables sur le réseau afin de trouver, analyser et résoudre facilement les problèmes. L'apprentissage automatique et l'analyse des données fonctionnent à l'unisson pour fournir aux administrateurs une intelligence contextualisée afin de réduire le temps de réponse.

Pourquoi Kemp Flowmon ?

- Du déploiement aux informations du tableau de bord en 30 minutes
- PoC facile et rapide avec un ingénieur Kemp dédié
- Excellent support et guidage intégré au produit
- Disponible en tant que matériel HW, appliance virtuelle (VMware, KVM, hyper-V) et instance de Cloud public (AWS, Azure, Google Cloud)
- Localisé dans six langues du monde, dont le français

Références clients

kaspersky

Société : KASPERSKY
Adresse : 2 rue Joseph-Monier, 92500 Rueil-Malmaison
Tél. : 01 41 39 04 44
Mail : **info@kaspersky.fr**
Site web : **www.kaspersky.fr**

Spécialisations

Protection contre les attaques ciblées, EDR, MDR, Threat Intelligence, sécurité des environnements industriels

Chiffres clés

Effectif : + de 4 000 professionnels dont 1/3 au département Recherche et Développement

Dirigeant
Bertrand TRASTOUR
Directeur général

Contacts

Stéphane FICHERA
Head of enterprise sales, France
Stephane.fichera@kaspersky.com

Catherine OUDOT
Head of Channel, France
catherine.oudot@kaspersky.fr

Pascal NAUDIN
Head of B2B Sales North, West & Central Africa
pascal.naudin@kaspersky.fr

Prenez le contrôle des cyber-incidents complexes

Depuis près d'un quart de siècle, Kaspersky a joué un rôle important dans la sécurisation de ses clients et partenaires en les aidant à protéger leurs données les plus importantes et à contrer des menaces croissantes en nombre et en complexité.

Kaspersky dispose aujourd'hui d'un portefeuille de produits et de services à l'avant-garde de la cyber sécurité de nouvelle génération, qui permet à ses clients de tirer le meilleur parti de la technologie en toute sécurité.

Mondialement reconnu pour son expertise et son leadership technologique, Kaspersky fournit des solutions de sécurité pour plus de 270 000 entreprises et 400 millions d'utilisateurs à travers le monde.

Offres

Kaspersky EDR

Kaspersky Endpoint Detection and Response est un outil performant et doté de nombreuses fonctionnalités pour les experts en sécurité informatique, offrant une visibilité totale, une détection des menaces performante et une analyse efficace, avec un accès rapide aux données recueillies. Votre processus d'enquête bénéficie de l'analyse rétrospective, d'indicateurs d'attaque propriétaires et du mappage MITRE ATT&CK, ainsi que de la recherche proactive des menaces et de l'accès à Kaspersky Threat Intelligence. Découvrez la séquence de l'intrusion dans son intégralité, comprenez les attaques complexes à plusieurs niveaux qui ciblent les terminaux et réagissez rapidement et de manière appropriée !

Kaspersky MDR

Kaspersky *Managed Detection and Response* offre des fonctionnalités de cybersécurité matures via un déploiement clé en main, rapide et évolutif sans qu'il soit nécessaire d'investir dans du personnel ou des compétences supplémentaires.

Grâce aux modèles de Machine Learning brevetés, à une Threat Intelligence continue et unique, à la recherche automatisée de menaces avec indicateurs d'attaque propriétaires, votre organisation est protégée en permanence contre les menaces complexes.

Laissez à Kaspersky le soin de se charger des processus de triage et d'enquête des incidents, coûteux en temps et en ressources. Profitez de tous les avantages d'un centre d'opérations de sécurité (SOC) sans avoir à créer le vôtre !

Certifications

Kaspersky a obtenu plus de premières places que tous les autres fournisseurs de sécurité lors de tests indépendants. Et c'est une performance que nous répétons année après année.
www.kaspersky.com/top3

Reconnu.
Transparent.
Indépendant.

Prenez le contrôle des cyber-incidents complexes

Renforcez la puissance de votre équipe cybersécurité avec des technologies de pointe enrichies par des renseignements de haut niveau sur les menaces, des connaissances et les conseils des meilleurs experts.

kaspersky.fr/enterprise-security

kaspersky BRING ON THE FUTURE

© 2021 AO Kaspersky Lab. Bring on the future : Bienvenue dans le futur.

Société : KEYSIGHT TECHNOLOGIES
Adresse : France Parc Technopolis – bâtiment Olympe – ZA Courtaboeuf
3 avenue du Canada CS 50035
91941 Les Ulis Cedex
Tél. : (toll free) 0805 980333
Mail : **contactcenter_france@keysight.com**
Site web : **https://www.keysight.com/**

Keysight est à la pointe de l'innovation technologique, dans les domaines de la sécurité des réseaux, de la conception électronique, du test, de la fabrication électronique et de l'optimisation des processus de réponse aux incidents IT.

Nos 15 000 employés créent des solutions de classe mondiale sur les marchés de la sécurité, des communications sans fil, de la 5G, de l'automobile, du quantique, de l'aérospatiale, de la défense et des semi-conducteurs dans plus de cent pays.

Notre activité de mesure électronique a vu le jour en 1939, qui était à l'origine de la création de Hewlett Packard. Notre histoire s'appuie sur plus de 80 ans d'innovation, d'expertise en science de la mesure et le développement de relations étroites avec nos clients. Nous travaillons chaque année avec environ 30 000 clients dans le monde entier, dont la plupart appartiennent au Fortune 1000.

Spécialisations

- **Tests et sécurité (IT/OT, CLOUD)**
- **Breach and Attack Simulation pour vérifier la sécurité opérationnelle**
- **Réseaux sans fil (4/5G)**
- **Solutions pour l'Automotive**
- **Solutions pour l'IOT**
- **Solutions pour l'Aerospace/ defense**

Chiffres clés

CA : $ 4,3 Mds en 2020
Effectifs : +15 000
Historique : création de HP en 1939, création de Keysight en 2014 suite au spin off d'Agilent

Contact

Roxana MAGDO
Business development director – industrial solutions
roxana.magdo@keysight.com

Offres

En 2016, Keysight a transformé la structure de l'entreprise, passant de divisions axées sur les produits à des organisations de solutions axées sur l'industrie, permettant un alignement plus étroit avec les clients.

Solutions pour les industries

SECURITE INDUSTRIELLLE OT/IT

FULL VISIBILITY

La solution de visibilité de Keysight est conçue pour les environnements IT et OT, du Datacenter au Cloud, et couvre, avec des produits dédiés, les sites OT soumis à des conditions de température et d'humidité extrêmes, ce qui fait de nous la seule société capable d'offrir une VISIBILITÉ TOTALE sur les réseaux industriels 4.0.

THREAT SIMULATOR

BREACH AND ATTACK

La sécurité n'est jamais statique. De nouvelles cyberattaques apparaissent constamment et les erreurs de configuration sont monnaie courante. Comment se préparer à des menaces en constante évolution ?

Le seul moyen est de vous attaquer avant que les pirates ne le fassent.

Plate-forme SaaS de simulation de brèches et d'attaques (BAS), Threat Simulator teste en permanence vos défenses en simulant des attaques sur votre réseau de production et vos postes de travail.

SCADA AND IT NETWORK TESTING

TEST YOUR DESIGN

BreakingPoint de Keysight peut créer une simulation de réseaux SCADA complexes et distribués comprenant des dizaines ou des milliers de points d'extrémité, de applications telles que Modbus, IEC et Bacnet, ainsi que des exploits et des logiciels malveillants. Ces simulations aident les organisations à mesurer la résilience des systèmes, à prendre des décisions d'achat, à former les équipes d'exploitation sur les incidents de sécurité SCADA et à prendre des décisions sur le déploiement de nouvelles technologies.

Références clients

Keysight compte parmi ses 30 000 clients des sociétés technologiques les plus innovantes ainsi que des opérateurs de services essentiels les plus importants au monde, notamment Apple, Amazon, Google, Microsoft, Facebook, NVIDIA, Qualcomm, la NASA, Thales, EDF, Airbus, RITP, TOTAL, ENEDIS, RENAULT, LA POSTE pour n'en citer que quelques-uns.

KEYSIGHT TECHNOLOGIES

abbakan
an Ingram Micro Company

Eliminate the blind spots!

ACCELERATE INNOVATION TO CONNECT AND SECURE THE WORLD

Keysight enhances your security with total visibility solutions, from IT Cloud down to extreme conditions OT/ICS environments.

KEYSIGHT TECHNOLOGIES

www.keysight.com

KUDELSKI SECURITY

Société : KUDELSKI SECURITY
Adresse : route de Genève 22
CH-1033 Cheseaux-sur-Lausanne
Suisse

86, rue Henri-Farman
92130 Issy-les-Moulineaux
France

Tél. : +41 21 732 01 01
Mail : **info@kudelskisecurity.com**
Site web : **www.kudelskisecurity.com**

Spécialisations

- **Services de sécurité managés pour environnements IT, Cloud, Endpoints et OT 24 h/24, 7 j/7**
- **Services managés de détection et de réponse aux menaces (MDR)**
- **EDR managé**

Chiffres clés

Revenus bruts 2020 (Kudelski Security) : 140 millions de dollars

Revenus 2020 (Groupe Kudelski) : 741,35 millions de dollars

Effectifs Kudelski Security : 350+

Dirigeants
Andrew HOWARD
CEO

David CHETRIT
VP Sales EMEA

Kudelski Security est une entreprise leader dans le domaine de la cybersécurité, dont l'objectif principal est de remettre en cause le statu quo. Nous collaborons avec nos clients afin de renforcer leur confiance en matière de cybersécurité, leur résilience aux menaces et la protection de leurs données grâce à un ensemble unique de solutions comprenant conseils, technologies, services de sécurité managés et innovation personnalisée. Avec des bureaux en Europe (Suisse, France – Paris, Allemagne, Royaume-Uni) et à travers les États-Unis, nous sommes forts d'une longue tradition d'ingénierie et d'innovation, qui nous permet de développer des solutions à même de résoudre les défis de cybersécurité les plus complexes auxquels sont confrontés nos clients.

Services

Services de sécurité managés

- Services de sécurité managés pour infrastructures IT, Cloud, Endpoints et OT. 24 h/24 et 7 j/7
- Services managés de détection et de réponse aux menaces (MDR)
- Surveillance et chasse proactives des menaces
- EDR managé
- Services de réponse aux incidents
- Services de sécurité du Cloud

Conseil

- Audits et conformité
- Tests d'intrusion avancés
- Évaluation stratégique de programmes de cybersécurité
- Conception et développement de programmes de cybersécurité
- Programme d'accompagnement des CISO/RSSI

Technologies

- Évaluations de technologies
- Conception et architecture de cybersécurité
- Implémentation et migration de technologies

Innovation

- Sécurité des produits connectés
- Services de sécurité IoT
- Évaluation et validation de la sécurité logicielle et matérielle et analyse forensique
- Sécurité des blockchains

Certifications

- Certifié ISO 27001:2013
- Certifications CERT *(Computer Emergency Response Team)*
- Membre actif du FIRST *(Forum of Incident Response and Security Teams)*
- Nos laboratoires avancés sont accrédités par l'Anssi pour délivrer la certification de sécurité CSPN

Distinctions

- Reconnu comme *Strong Performer* dans le rapport de Detection et Réponse Managés (MDR) : *« The Forrester Wave™: Managed Detection And Response, Q1 2021 »*
- Reconnu comme Leader dans le rapport *« The Forrester Wave™: Midsize MSSPs, Q3, 2020 »*
- Reconnu comme l'un des principaux fournisseurs sur le segment *Managed Detection and Response* (MDR) du *« Gartner Market Guide for Managed Detection & Response Services 2017-2021 »*
- Nommé comme l'un des fournisseurs les plus connus en Europe dans le rapport de Frost & Sullivan : *« European Managed & Professional Security Services Market, 2021 »*
- Reconnu comme l'un des 10 principaux fournisseurs MSS au niveau européen dans le *« Magic Quadrant for Managed Security Services Worldwide, 2019 »*

Références clients

Pernod Ricard, L'Oréal, Canal+, Suez, Apicil

En France, un nombre croissant d'entreprises nous font confiance

« Kudelski Security connaît un solide développement en France depuis 2018. Un nombre croissant d'entreprises fait appel à nos services de sécurité managés innovants, et notamment à nos services managés de détection et de réponse aux menaces pour les environnements IT, Cloud, Endpoints et OT/ICS, fournis à travers notre Cyber Fusion Center basé en Suisse. Nos services de sécurité managés et de réponse aux incidents ont d'ailleurs été distingués par de nombreux analystes tels que Gartner, Forrester et IDC. »

Philippe BORLOZ,
EMEA General Manager, Kudelski Security

KUDELSKI SECURITY
Services managés de détection et de réponse aux menaces
Des services MDR personnalisés, rapides et disponibles 24 h/24 et 7 j/7.
Cloud
OT
IT
Endpoints
Quel que soit votre environnement, nos services MDR vous protègent.
www.kudelskisecurity.com

Société : LASTPASS BY LOGMEIN
Adresse : The Reflector, Hanover-Quay, Dublin Docklands, Dublin, D02 R573, Irlande
Tél. : +353 1 254 1490
Mail : **www.lastpass.com/lastpass-enterprise-contact-sales**
Site web : **www.lastpass.com/business-solutions**

Spécialisations

Gestion d'identité et d'accès (IAM)

Chiffres clés

CA : 1,2 billion $
Effectifs : 4 000
Historique : créé en 2003

Contacts
Patrick BRENNAN
Country Channel Manager France
Patrick.Brennan@logmein.com
+33 6 10 24 51 96

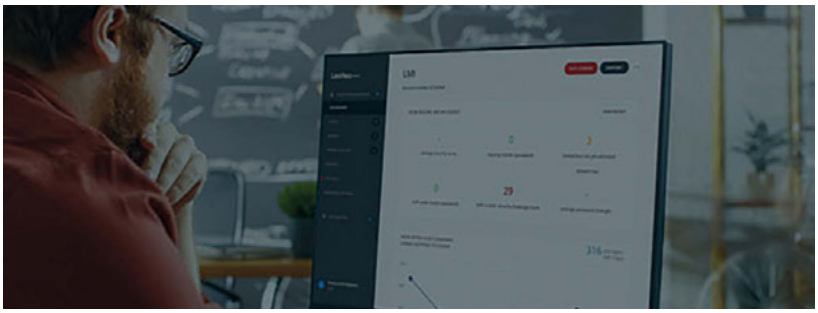
Nicolas MARRIMPOEY
Responsable Grands comptes
Nicolas.Marrimpoey@logmein.com

Vincent GHIOTTI
Responsable Grands comptes
Vincent.Ghiotti@logmein.com

LastPass pour l'entreprise

Permettez à vos employés d'effectuer leurs tâches en toute sécurité

De l'authentification à l'accès aux mots de passe, LastPass gère tous les points d'accès de votre entreprise afin que vous puissiez minimiser les risques tout en améliorant la productivité de vos employés.



Solutions

Accès sécurisé, centralisé
Avec sa solution intégrée d'authentification unique et de gestion des mots de passe, LastPass Enterprise offre un contrôle de chaque point d'accès.

- **Authentification unique (SSO)**
Un catalogue de +1 200 apps pré-intégrées et des intégrations personnalisées offrent un accès transparent sans mot de passe.
- **Gestion des mots de passe**
Simplifiez l'accès à toutes les apps en créant, capturant, et remplissant automatiquement les identifiants pour n'importe quel site.
- **Accès simple et intégré**
Apps dans le nuage, mobiles, anciennes ou internes : centralisez les accès des employés à l'aide d'une solution intégrée.

Points forts

Déploiement simple à l'échelle de tous les utilisateurs
LastPass Enterprise automatise des processus informatiques clés et simplifie l'accès des employés pour favoriser la productivité du personnel.

Console d'administration performante
Quel que soit le point d'entrée, la visibilité des accès par le SI à l'échelle de l'entreprise est fondamentale pour assurer la sécurité.

Diminution de la friction pour les utilisateurs
LastPass Enterprise fournit aux employés un accès simple et rapide à leur travail ainsi qu'une solution unique pour se connecter à tout.

Poste de sécurité renforcé
Du modèle zéro connaissance aux fonctionnalités de sécurité en option, LastPass Enterprise assure la sécurité de votre activité.

Fonctionnalités de sécurité performantes :

- Conformité SOC 2 Type 2
- Authentification multifacteur
- Gestion des points d'accès
- Solution d'identité tout en un
- Contrôle informatique centralisé

Offres

LastPass Enterprise, LastPass Identity, LastPass MFA
https://www.lastpass.com/fr/business-solutions

« 80 % des failles de sécurité en entreprise sont liées aux mots de passe. LastPass est une solution tout-en-un pour la gestion des identités et des accès. Concrètement, cela signifie qu'il n'est nécessaire de se souvenir que d'un seul mot de passe maître, et LastPass s'occupe du reste. Une fois les individus débarrassés de la nécessité de se souvenir de leurs mots de passe, le risque pour l'entreprise est réduit et les collaborateurs peuvent ainsi augmenter leur productivité. LastPass s'adresse à tout le monde et chacun peut télécharger une version personnelle. Nous proposons aussi une offre professionnelle pour les entreprises de toutes tailles et issues de tous les secteurs d'activités. »

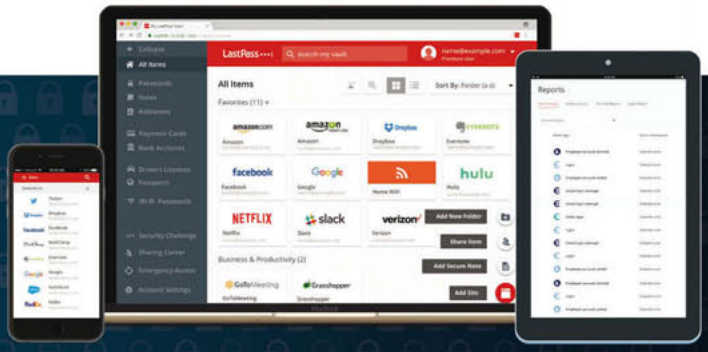
Patrick BRENNAN - *Country Channel Manager France*

LastPass ••• | by LogMeIn

Une hygiène des mots de passe sécurisée et simplifiée

Ne plus jamais réinitialiser un mot de passe

- Authentification unique
- Gestion des mots de passe
- Accès simple et intégré



Pour en savoir plus :
lastpass.com/fr/business-solutions

©2021 LogMeIn, Inc. Tous droits réservés.

MAILINBLACK

Fondée en 2003, Mailinblack est la pépite française qui rend la cybersécurité accessible à toutes les organisations. Ses équipes, constituées de 70 collaborateurs basés à Marseille, conçoivent, développent et hébergent en France ses solutions de cybersécurité. Parmi elles, la solution de protection de messagerie Protect ou encore l'outil de sensibilisation et de formation aux cyber-risques Phishing Coach. Lauréate du Grand Défi Cyber et forte de plus de quinze années d'expertise en sécurité, R&D et Intelligence artificielle, Mailinblack recense aujourd'hui 1 million d'utilisateurs et 14 000 clients dans les secteurs public et privé.

Spécialisations

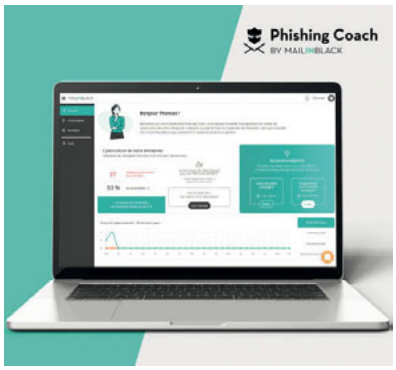
Sécurité e-mail, audit des vulnérabilités humaines, formation et sensibilisation aux cyber-risques

Chiffres clés

CA entre 5M€ et 10M€
Effectifs : 70

Solutions

Protect – Produit historique de Mailinblack, Protect sécurise les boîtes mail professionnelles contre les cyberattaques, grâce à des technologies propriétaires couplées à de l'Intelligence artificielle. Ses solutions anti-malware, anti-phishing, anti-spearphishing et anti-spam puissantes garantissent une messagerie propre et sécurisée. Ses interfaces de gestion, simples et intuitives, permettent à l'administrateur de garder le contrôle sur les paramètres de sécurité et d'avoir un aperçu du nombre de menaces interceptées au quotidien, tout en laissant 100 % d'autonomie aux utilisateurs.



Phishing Coach – Dernière innovation Mailinblack, Phishing Coach sensibilise et forme les collaborateurs aux risques cyber grâce à des simulations d'attaques de phishing réalistes. Basée sur un système d'apprentissage par la répétition, Phishing Coach permet d'évaluer le niveau de vulnérabilité humaine dans les organisations et de proposer des contenus de formation adaptés et personnalisés, au moment de l'erreur, afin de réduire considérablement les risques. L'outil permet également de piloter la progression.

Société : MAILINBLACK
Nom des marques :
Protect BY MAILINBLACK
Phishing Coach BY MAILINBLACK

Adresse : 4 place Sadi-Carnot
13002 Marseille
Tél. : 04 88 60 07 80
Mail : **contact@mailinblack.com**
Site web : **www.mailinblack.com**

Dirigeant

Thomas KERJEAN
Directeur général
tkerjean@mailinblack.com

Contacts
Justine GRETTEN
Responsable communication
jgretten@mailinblack.com

Certifications

- Hexatrust, French Tech, Solainn
- Solution Phishing Coach référencée au catalogue Gouv tech

Points forts

- Société française et hébergement des données en France
- 100% RGPD
- Solutions accessibles aux PME, ETI, collectivités et santé
- Référencées aux centrales d'achat (UGAP, RESAH, UNIHA, CAIH, SIPPEREC)
- Disponibles en SaaS ou On Premise
- Facilité d'installation et d'administration
- Certifiées HDS

Prix : Lauréat du Grand Défi Cybersécurité

Références clients

OpenClassrooms, la ville de Lens, Grand-Frais, Louis Roederer, le CHU de Toulouse, le Domaine national de Chambord.

Historique

2003 : *création de l'entreprise*
2006 : *commercialisation du produit historique Protect (anciennement Mailinblack Anti-Spam)*
2019 : *levée de fonds de 14 millions, arrivée de Thomas Kerjean comme nouveau DG*
2020 : *sortie de nouvelles fonctionnalités sur Protect (exemple : Secure Link qui analyse les liens présents dans les e-mails) et lancement de Phishing Coach (solution de sensibilisation et de formation aux cyberattaques).*

Société : METSYS
Adresse : 121 rue d'Aguesseau, 92100 Boulogne-Billancourt
Tél. : +33 181 891 970
Mail : **contact@metsys.fr**
Site web : **www.metsys.fr**

Spécialisations

Partenaire de grands éditeurs comme Microsoft, Varonis, One Identity, Tenable/Alsid ou encore EfficientIP, Metsys investit massivement dans le domaine de la cybersécurité afin d'accompagner ses clients pour protéger leur Système d'Information. La valeur ajoutée de Metsys est la maîtrise de bout en bout de la cybersécurité, depuis les infrastructures on-premise jusqu'au Cloud. Nos collaborateurs spécialisés dans leurs domaines de compétences respectifs nous permettent de traiter aussi bien les sujets liés aux identités des utilisateurs que ceux liés aux infrastructures systèmes. Ils interviennent également sur les outils collaboratifs ainsi que sur la détection des incidents de sécurité au travers de notre Centre Opérationnel de Cybersécurité (SOC). Metsys propose une offre de cybersécurité complète permettant d'accompagner nos clients depuis la mise en œuvre jusqu'à la supervision des infrastructures.

Chiffres clés

CA prévisionnel 2021 :
50 millions d'euros

Effectif à la fin 2021 :
350 collaborateurs
300 clients actifs

Acteur incontournable des services du numérique, présent sur l'ensemble du territoire, (Paris, Lille, Rennes, Nantes, Tours, Bordeaux, Toulouse, Aix-en-Provence, Lyon et Strasbourg), Metsys dispose d'une offre globale de services allant de la phase d'audit et de conception, jusqu'à l'implémentation et le support.

En s'engageant vers une transition digitale, les organisations font face à des failles de sécurité de plus en plus nombreuses. Afin d'apporter une réponse efficace à leurs besoins, elles doivent considérer la sécurité selon une approche globale. Sécuriser les infrastructures ne suffit plus, il s'agit d'anticiper les cybermenaces tout en assurant la gouvernance et la conformité des données. De plus, et malgré toute la prévention, les cybercriminels sont encore capables de contourner les systèmes de protection. Les entreprises doivent être en mesure de réagir efficacement en cas d'attaque.

Metsys s'appuie sur la mise en œuvre de moyens informatiques et humains pour anticiper les menaces et sur son SOC pour anticiper, surveiller et réagir aux attaques. Nous nous appuyons sur 4 piliers pour garantir la résilience des SI de nos clients :

- Prévenir et détecter (Identification des risques potentiels, collecte et analyse des alertes détectées par le Centre Opérationnel de Cybersécurité,…)
- Sécuriser vos Systèmes d'Information (sécurisation native de vos infrastructures, sécurisation du passage au Cloud…)
- Assurer la gouvernance et la mise en conformité des données
- Réagir et intervenir (accompagner la mise en œuvre des processus de gestion de réponse aux incidents)

Offres

- **Security Excellence Center by Metsys :** premier service de sécurité managé autour des briques de Microsoft 365 (Office 365/eM+S/Windows10), Varonis, Tenable/Alsid, Tehtris, Coreview, etc. Metsys Security Excellence Center permet aux entreprises d'exploiter le plein potentiel des briques de cybersécurité intégrées à leurs abonnements.
- **Gestion des Identités et des données :** Metsys vous accompagne dans la mise en place et la gouvernance des outils de gestion des identités et des accès, vous permettant ainsi de garantir un accès et une authentification sécurisée à vos Systèmes d'Information.
- **Centre Opérationnel de Cybersécurité :** L'offre SOC de Metsys est destinée à superviser les différents outils de sécurité et à offrir les niveaux d'analyses et d'alertes adéquats. Cette offre aide les entreprises à exploiter au mieux les outils de sécurité qu'elles ont acquis. Le SOC se chargera d'analyser les signaux à risques, d'émettre des alertes et de répondre ou de proposer des réponses sur incident comme, par exemple, bloquer immédiatement tout poste de travail réalisant de l'extraction de données.

« Notre ambition est de proposer à nos clients une offre de sécurité, dite, de bout en bout, capable d'anticiper les cybermenaces en assurant une gouvernance renforcée et une meilleure maîtrise des données au travers d'une approche sécuritaire globale. Depuis la détection et l'anticipation des menaces jusqu'à la remédiation, la mise en conformité et la gouvernance des données, Metsys accompagne ses clients dans une démarche globale de maîtrise de la sécurité des SI, avec l'aide de ses spécialistes formés et certifiés. La construction du Centre Opérationnel de Cybersécurité de Metsys permet d'apporter aux clients la supervision, la détection d'événements anormaux/non désirés, et la réactivité de réponse sur incident ainsi que l'analyse post mortem. »

Nicolas VERDIER,
RSSI et Directeur de l'agence Metsys Centre-Val de Loire

Dirigeant
Laurent CAYATTE
Président et fondateur de Metsys

Contact
Nicolas VERDIER
RSSI et directeur de l'agence Centre-Val de Loire
Tél. : +33 762 793 608
nicolas.verdier@metsys.fr

Société : MICROPOLE
Marque : GO CLOUD & SECURITY

Adresse : 91-95 rue Carnot
92300 Levallois-Perret
Tél. : +33 (0)1 74 18 74 18
Mail : **contactGCS@micropole.com**
Site web : **https://www.micropole.com/fr-fr/offres/security-cloud-data/go-cloud-security**

Spécialisations

- **Cloud : conseil, assistance technique, expertise migration cloud**
- **Cybersécurité : offensive, défensive, cloud et GRC (Gouvernance, Risk, Compliance)**
- **Quelques domaines d'interventions : conseil et architecture cloud, *Cloud Security*, audit sécurité, scan de vulnérabilités, Pentest, Shadow IT…**

Chiffres clés

CA : 111 M€ dont BU 2,5 M€
Effectifs : 1 110 employés répartis en Europe dont 26 consultants GC&S en France
Date de création : 1987
Date de création de GC&S : 2020

Dirigeants

Christian POYAU
Co-fondateur et PDG du Groupe Micropole

Christophe LEVIER
Directeur de l'entité Go Cloud & Security Micropole
contactGCS@micropole.com
Tél. : +33 (0)1 74 18 74 18

Go Cloud & Security accompagne les entreprises, dans le cadre de leur transformation digitale, dans leur migration vers le Cloud & dans la sécurisation défensive et offensive globale de leur SI.

Go Cloud

Cloud First est au cœur de la stratégie IT des entreprises de taille intermédiaire (ETI) et grandes entreprises. Avec nos partenaires, AWS, Microsoft Azure et Google Cloud, nos équipes accompagnent les clients dans cette transition qui leur apportera agilité, performance, résilience et optimisation financière

Security

La transformation digitale rapide à base de Cloud, IA, IoT ou encore de BYOD expose les entreprises aux cyberattaques qui ne cessent de progresser. Face à ces menaces, nos experts aident les entreprises à procéder à une mutation de leurs sécurités défensive et offensive et à mettre en place gouvernance, stratégie et des technologies innovantes.

Offres

Go Cloud & Security réunit les 2 expertises pour vous proposer des services sans couture et adaptés à l'évolution de vos problématiques SI et gouvernance.

Consulting

- Governance, Strategy, Compliance, Architecture, Audit, Risk…

Architecture & Technology

- Migration, POC, Design, DevOps…

Managed Services

- Infrastructure, Support, Monitoring, Continuous Improvement…

Solutions & Tools

- Monitoring, Management, Connectivity, Finops…

Cloud Security

- Security for Public Cloud Platforms…

Defensive Security

- Architecture, Social Engineering, DevSecOps, Training

Offensive Security

- Access, Apps, Data, Risk, Cloud Security, Forensic…

Trois bonnes raisons de nous faire confiance

- Plus de trente ans d'expérience dans les solutions d'infrastructures, de management et de valorisation de la donnée et d'analytique d'entreprises (Business Intelligence, Big Data, Machine Learning, Data Visualisation, Data Science…).
- Nos experts Cloud vous conseillent et vous accompagnent dans la migration de vos infrastructures, vos applications, vos données et vos services IT. Nos partenaires technologiques vous offrent les solutions les plus avancées dans les domaines du Cloud et de la Cybersécurité.
- Nous vous guidons à travers chaque étape de votre projet en vous apportant les bonnes pratiques et expériences pour vous permettre de gagner rapidement en agilité, de lancer de nouveaux services et d'adresser n'importe quel nouveau cas d'usage et surtout, de gagner en compétitivité !

Référence clients

BNP Paribas, MACIF, Gras Savoye, Unibail Rodamco Westfield, Groupe Bouygues, Suez, Engie…

- Partenaire certifié des Cloud Provider : Microsoft Azure, AWS, Google Cloud
+100 consultants formés/certifies
- Principaux partenaires technologiques : Vectra, Yubico, CloudHealth, InterCloud, Varonis, DataDog, Paloalto, Tenable…

Membre associé de Cyber Campus

Portrait de Christophe LEVIER

Plus de 25 années d'expérience dans le développement d'activités dans les domaines des infrastructures, du datacenter, du Cloud et de la cybersécurité à travers des éditeurs de logiciels, ESN, intégrateurs et DSI de Grands comptes et à travers des postes de direction du Développement, direction de Business Unit ou direction-générale.

Depuis 2019, il a rejoint le Groupe Micropole pour développer l'entité nommée Go Cloud & Security, dont la mission est d'accompagner les clients dans leurs projets de migration vers le Cloud public et dans les opérations de sécurisation de leur SI.

GO CLOUD & SECURITY

VOUS ACCOMPAGNE DANS VOTRE MIGRATION VERS LE CLOUD ET DANS LA SÉCURISATION DEFENSIVE ET OFFENSIVE GLOBALE DE VOTRE SI.

CONSULTING

> Governance, Strategy, Compliance, Architecture, Audit, Risk...

MANAGED SERVICES

> Infrastructure, support, monitoring, continuous improvement...

ARCHITECTURE & TECHNOLOGY

> Migration, POC, Design, DevOps...

CLOUD SECURITY

> Security for Public Cloud Platforms...

OFFENSIVE SECURITY

> Access, apps, data, risk, Cloud security, Forensic...

DEFENSIVE SECURITY

> Architecture, Social engineering, DevSecOps, Training center...

SOLUTIONS & TOOLS

> Monitoring, management, connectivity, Finops...

+100 CONSULTANTS FORMÉS/CERTIFIÉS

- Advanced partner AWS
- Gold partner Microsoft
- Google cloud partner

+10 PARTENAIRES

Vectra • Yubico • InterCloud CloudHealth • Datadog Paloalto...

CAMPUS CYBER ASSOCIÉ

MICROPOLE

Christophe Levier — contactGCS@micropole.com — micropole.com — +33 1 74 18 74 18

Société : MIEL
Adresse : Parc Burospace 5, 91570 Bièvres
Tél. : +33 1 60 19 34 52
Mail : **reseausecu@miel.fr**
Site web : **www.miel.fr**

Spécialisations

- **Cybersécurité Zero Trust**
- **Digital Workplace**
- **Data centers multi-clouds**
- **Réseaux du Cloud & IoT**

Chiffres clés

55 collaborateurs, 400+ personnes formées chaque années, 1000+ partenaires revendeurs nous font confiance.

- 1985 : création par Roger BONINI
- 1992 : partenariat Citrix
- 2008 : partenariat Palo Ato Networks
- 2021 : 12+ éditeurs partenaires dans le domaine de la cybersécurité

Dirigeant
Jean-Baptiste POMMÉ
Directeur général
jean-baptiste.pomme@miel.fr

Contact
Kamel MOUHOUBI
Directeur pôle produits cybersécurité
kamel@miel.fr

Tél. : 01 73 23 66 20

Créée en 1985, MIEL introduit sur le marché français, via un réseau de revendeurs qualifiés, les nouvelles technologies à l'attention des DSI et des Cloud providers. MIEL a connu les débuts de l'ère du PC et accompagné son développement dans les entreprises en lançant en précurseur en France les technologies mémoire Flash, Wi-Fi, client léger, optimisation WAN, virtualisation, NAC, switching 10GbE, hyperconvergence, cybersécurité Zero Trust…

MIEL propose un éventail complet et complémentaire de technologies pour sécuriser l'informatique d'entreprise à l'ère du Cloud : de la protection du endpoint à la sécurité du Cloud et des accès SaaS, en passant par le réseau, la messagerie, les identités, les données. Visibilité, Machine-learning, menaces connues et inconnues, la sécurité dernier cri pour la transformation numérique.

Distributeur des nouvelles technologies pour la cybersécurité des entreprises

Cybersécurité opérationnelle (SOC) : Zero Trust, next-gen firewall piloté par Machine-learning, SASE, SOAR, EDR, Micro-segmentation

Solutions SIEM et UEBA unifiées, collecte et corrélation de logs temps réel.

Contrôle de tous les accès au LAN. **NAC moderne**. Convergence de sécurité IT et OT.

Prise de main à distance ultra-sécurisée (PMAD). Gestion des **comptes à privilèges**.

Protection prédictive de la messagerie. Anti-spear-phishing, sécurité intégrée O365.

Détection des vulnérabilités, évaluation des risques, automatisation SecOps

Analyse réseau temps réel, Nord-Sud et Est-Ouest. NDR.

Passerelle de sécurité : VPN SSL, filtrage d'accès, SSO.

Simulation de cyberattaques as-a-Service, sur tous les vecteurs d'attaque.

Authentification forte sans mot de passe. Biométrique.

Gestion des accès et identités dans le Cloud. IAM.

Back-up des données O365.

Adoptez et maîtrisez la CYBERSÉCURITÉ dernière génération

avec

MIEL

Votre **DISTRIBUTEUR**, centre de compétence, de **SUPPORT** et de **FORMATION** pour :

BeyondTrust
CARBONITE an opentext company
citrix
Cymulate
ExtraHop
FORESCOUT
illumio
LOGPOINT
paloalto NETWORKS
RAPID7
vade
VERIDIUM TRUSTED DIGITAL IDENTITY

MIEL vous présente les réponses innovantes aux projets actuels

Nos ingénieurs rencontrent au quotidien les équipes informatiques, DSI et RSSI, partenaires revendeurs et cloud providers partout en France pour expliquer, démontrer, répondre aux questions, organiser des PoC.

Contactez-nous dès aujourd'hui pour organiser la prochaine démo !

Appelez le 01 60 19 02 30

www.miel.fr

Haute disponibilité des services critiques en ligne

Société : NAMESHIELD
Adresse : 37 bd des Capucines
75002 Paris
Tél. : +33 2 41 18 28 28
Mail : **commercial@nameshield.net**
Site web : **https://www.nameshield.com/**

Avec plus de 25 ans d'expérience au service de ses clients et partenaires, Nameshield garantit la haute disponibilité des services stratégiques en ligne d'une entreprise/administration et assure la surveillance et la défense de leurs noms de domaine.

Nameshield est le registrar français de référence en gestion et sécurisation de portefeuille de noms de domaine et services associés. Nameshield propose une solution globale de management, de surveillance et de défense des noms de domaine. Ses services de détection des menaces et remédiation garantissent la cyber-sécurité des marques en ligne de ses clients. Son authentificateur d'URL (breveté) permet d'agir en anticipation des fraudes.

Chiffres clés

Date de création : 1994
Effectifs : 100
Actionnariat : détenue à 100 % par ses salariés et par le fonds de dotation Esperancia

Dirigeants

Gérard GOURJON
DG

Aymeric de VACHON
DG / DAF

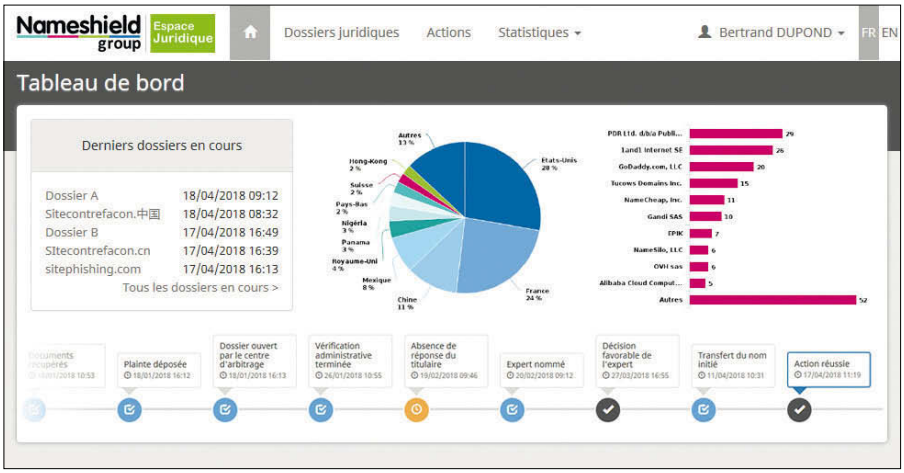
Florent BLONDEAU
DG / Dir. Études et Développements

Contact

Murielle BOCHATON
Directrice commerciale
murielle.bochaton@nameshield.net

Points forts

- **Gestion des risques** ciblant les noms de domaine et services associés
- Adaptation aux **environnements complexes**
- Politique de **développements internes / solutions propriétaires**
- Certifié **ISO 27001**
- **Conformité Anssi**
- **Support dédié et équipes expertes**
- **Service juridique internalisé**
- Solution **DNS Premium labellisée France Cybersecurity**
- **Hébergement des données sur le sol français**
- **Engagement sociétal** avec le fonds de dotation Esperancia



Offres

Nameshield met à disposition de ses clients une équipe d'experts pour les accompagner **sur tous les aspects de la gestion des noms de domaine et des menaces associées :**

- gestion et sécurisation de portefeuille de noms de domaine pour éviter le vol de données, le détournement d'un nom de domaine, la non-conformité de zones DNS (SSO, Filtrage IP, Double Auth, gestion scope et droits…)
- solution de haute disponibilité DNS : filtrage anti-DDoS – réseau anycast – Failover – GeoIP – DNSSEC – DMARC
- CTI permettant la détection des menaces en ligne : phishing, usurpation d'identité, contrefaçon, sites contrefaits, faux comptes réseaux sociaux, etc.
- solutions de remédiation et service juridique internalisé
- mise en place d'une politique de sécurité et gouvernance noms de domaine
- cartographie des risques sur les actifs numériques / audit
- sécurité technique : certificats TLS/SSL, etc.

Certifications

Registrar français certifié **ISO 27001,** intégrant un **CERT** et disposant du Label **France Cybersecurity sur sa solution DNS Premium.**

Nameshield évolue au cœur de l'écosystème cybersécurité et participe à son évolution au travers d'associations et d'organismes, tels que **Hexatrust, First, Cesin, Clusif, DNS Oarc, ACN.** Nameshield est également présent au sein des groupes ICANN registry et registrar stakeholder**.**

Références clients

Administrations / Pure player du web / Banque / Energie / Industrie / Pharmaceutique / Retail / etc.

nameshield
Online Assets Security

GARANTIT LA HAUTE DISPONIBILITÉ DE VOS SERVICES STRATÉGIQUES EN LIGNE, ASSURE LA SURVEILLANCE & LA DÉFENSE DE VOS NOMS DE DOMAINE.

Téléchargez nos plaquettes avec ce code :

www.nameshield.com
blog.nameshield.com

Le BASTION DNS : Tout le savoir-faire de Nameshield pour protéger vos noms de domaine stratégiques

Votre trafic web, vos emails et de nombreuses applications clés de l'entreprise dépendent de certains de vos noms de domaine. Ce sont vos **noms de domaine stratégiques**. La moindre indisponibilité prive d'accès vos clients et utilisateurs avec des conséquences irrémédiables sur les données, le chiffre d'affaires, l'image de marque et la fidélité.
Malheureusement ces noms de domaine attisent les convoitises et leur **surface d'attaque** est importante, entre l'exposition à des **risques administratifs**, tels que les tentatives d'usurpation du nom, et à des **risques techniques**, tels que les attaques DDoS sur l'hébergement DNS.
Garantir leur **intégrité** et leur **disponibilité**, les **surveiller**, les **analyser** et **être alerté** en cas d'attaque est primordial. Pour répondre à ces impératifs, Nameshield, fort de son savoir-faire reconnu par ses pairs et d'une expérience de près de 30 ans dans la gestion de noms de domaine critiques, a créé le Bastion DNS : service unique de protection, surveillance et d'alerte.

Les 5 piliers du Bastion DNS Nameshield :

Intégrité
Protection totale contre les tentatives d'accès, d'usurpation, de transfert, de modification ou de suppression de vos noms de domaine.

Disponibilité
Vos noms de domaine toujours disponibles, rapides et résilients face aux tentatives de cyber-attaques DDoS, DNS spoofing ou DNS cache poisoning.

Surveillance
Surveillance dédiée et continue de la disponibilité de vos noms de domaine et équipe d'astreinte 24/365.

Analyse
Analyse mensuelle du trafic de la zone et sous-zone(s), rapport d'optimisation technique et de conformité aux préconisations de l'ANSSI.

Alerte
Système d'alerte en cas de détection d'anomalie de trafic basé sur le monitoring permanent du trafic du nom de domaine.

Opérateur français

Certifié ISO 27001 depuis 2017

Labellisé France Cybersecurity

Membre Hexatrust

Membre First

Membre de l'ACN

Membre du Conseil d'Administration de l'Afnic

Membre du groupe ICANN Stakeholder

Crédit images : Nameshield | Freepik Storyset

INFORMER
pour transformer l'entreprise

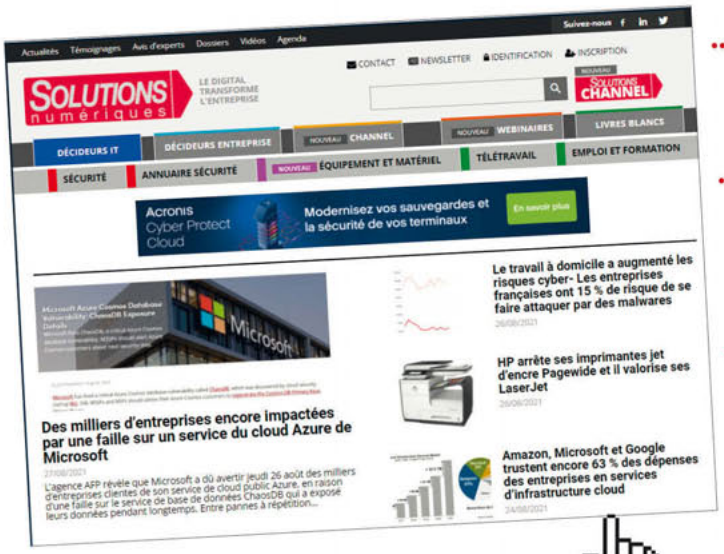
La dématérialisation, le Cloud,
les communications unifiées,
les nécessités de la cybersécurité
transforment le travail et toute l'entreprise,
les services publics.
Le magazine, le site, ses newsletters
vous informent sur cette actualité mouvante
et vous aident à décoder les tendances

Abonnez-vous

www.solutions-numeriques.com/abonnement/

Toutes les ressources et newsletters en ligne

Pour répondre à vos besoins d'information



- La cybersécurité vous concerne ? Cliquez sur l'onglet. Vous trouverez les infos, l'annuaire, le lexique, etc
- L'emploi, les salaires, les formations, les offres vous intéressent ? Le site sur l'Emploi dans le numérique est à votre disposition
- Votre site Télétravail. Infos et bonnes pratiques pour le travail à distance et le travail hybride
- Solutions Channel. L'info des partenaires, intégrateurs, distributeurs

www.solutions-numeriques.com

NEOWAVE

Société : NEOWAVE
Noms des marques : WENEO, WINKEO, BADGEO, LINKEO, HOLDEO

Weneo Winkeo Badgeo Linkeo Holdeo

Adresse : Pôle d'activités Y.-Morandat
1 480, avenue d'Arménie
13120 Gardanne (France)
Tél. : +33 (0) 4 42 50 70 05
Mail : **contact@neowave.fr**
Site web : **www.neowave.fr**

Spécialisations

- **Authentification forte Windows**
- **Authentification forte Web / SSO**
- **Chiffrement de données**
- **Signature électronique**
- **Sécurité des cryptoactifs**
- **Contrôle d'accès physique et gestion des temps**
- **VPN**

Chiffres clés

CA : € 500 000
Effectifs : 7

Historique

- **NEOWAVE a été fondée en 2007 à Gardanne par Bruno BERNARD avec les Smart Objects comme cœur de métier.**
- **À partir de 2012, l'entreprise a recentré son activité sur le marché de la sécurité numérique.**
- **En 2020, NEOWAVE propose trois grandes familles de produits : les solutions ID 2.0, les produits FIDO et les lecteurs de carte à puce.**

Dirigeant
Bruno BERNARD
Président : **bruno.bernard@neowave.fr**
Tél. : 04 42 50 70 05

Contacts :
Corinne JOACHIN
Responsable Marketing & Communication
corinne.joachin@neowave.fr
Tél. : 04 42 50 70 05

Le spécialiste de l'authentification forte et des transactions sécurisées

NEOWAVE est une entreprise innovante spécialisée dans l'authentification forte et les transactions sécurisées. Notre mission principale est de protéger le patrimoine numérique des entreprises et des usagers grâce à des technologies d'authentification forte à base de composants sécurisés et de certificats numériques. Nos solutions adressent les marchés de la cybersécurité, de la confiance numérique et de la gestion des identités. Notre expertise et notre agilité permettent d'accompagner et conseiller nos clients sur des projets spécifiques.

Offres

Les produits de NEOWAVE combinent le haut niveau de sécurité offert par la carte à puce avec les avantages des technologies de stockage et de connectivités : USB, RFID / NFC et Bluetooth Low Energy (BLE). Conçus et fabriqués en France, ils répondent aux exigences de sécurité des agences européennes.

Solutions ID 2.0

Les solutions ID 2.0 de NEOWAVE sont des cartes à puce et des tokens USB avec leur Middleware – sécurisation des accès logiques et physiques. Elles constituent des solutions évolutives permettant d'héberger des certificats pour le chiffrement, la signature électronique et l'ensemble des services liés à la dématérialisation. Elles sont compatibles avec la majorité des logiciels et des équipements déployés dans les entreprises, organisations professionnelles et collectivités.

Afin de concilier confort et sécurité, nos solutions ID 2.0 permettent de gérer de manière centralisée tous les droits d'accès logiques ou physiques.

Gamme FIDO

Les standards FIDO U2F (Universal Second Factor) et FIDO2 sont adoptés par des leaders mondiaux de l'Internet.

Ces produits sont adaptés aux acteurs de la confiance numérique – signature électronique, chiffrement, lettre recommandée, consentement, services financiers, assurances, santé…– et permet de se mettre en conformité avec la règlementation eIDAS (Identification, Authentification et Services de Confiance Electroniques) et le RGPD.

Lecteurs de carte à puce

La gamme de lecteurs carte à puce de NEOWAVE, à contact et/ou sans contact (RFID/NFC), facilite la mise en œuvre des applications sécurisées. Les produits de la gamme sont facilement installés, mis en œuvre et intégrés dans un environnement bureautique, grâce à leur compatibilité PS/SC CCID.

Références Clients

Certinomis, Crédit Agricole, Ministère de l'Intérieur, CertEurope, Allianz, AR24, ChamberSign

Distributeurs européens

ProSoft, Atlantis Software, Probitas, idpeople, Openseas

Certifications

Cybersecurity Made in Europe – Solutions 100 % *Made in France*, en conformité avec les règlements et standards européens de sécurité numérique

Ministère de l'Intérieur – Validé par le ministère de l'Intérieur (sécurisation des postes d'accès nomade)

Composants sécurisés certifiés EAL5+ par l'Anssi Produits FIDO qualifiés par l'Anssi

France Cyber Security – Labélisation France Cyber Security 2016, 2017 et 2019

Société : NETWRIX
Adresse : 300 Spectrum Center Drive, Suite 200 Irvine, CA 92618 - États-Unis
Tél. : +33 9 75 18 11 19
Mail : **netwrix.emea@netwrix.com**
Site web : **www.netwrix.fr**

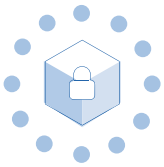
Spécialisations

Sécurité des données – identité et infrastructure, gouvernance des accès aux données, évaluation des risques IT, assainissement des données, détection des menaces internes, gouvernance de l'information, analyse des fichiers, demande d'accès aux données, conformité

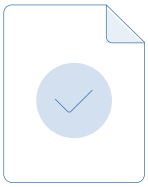
Dirigeant

Pierre-Louis LUSSAN
Country Manager
South-West Europe
Pierre-louis.Lussan@netwrix.com

CONNAISSEZ VOS DONNÉES



PROTÉGEZ CE QUI COMPTE



PROUVEZ LA CONFORMITÉ

Netwrix est un éditeur de logiciels qui permet aux professionnels de la sécurité et de la gouvernance de l'information de reprendre le contrôle des données sensibles, réglementées et stratégiques, quel que soit leur emplacement. Plus de 10 000 organisations du monde entier s'appuient sur les solutions Netwrix pour sécuriser leurs données sensibles, tirer pleinement parti des contenus d'entreprise, réussir les audits de conformité en déployant moins d'efforts tout en dépensant moins et améliorer la productivité de leurs équipes informatiques et de leurs travailleurs du savoir.

Offres

Data Security Platform

La sécurité de l'entreprise ne peut plus s'appuyer sur des solutions de sécurité informatique ponctuelles. Les organisations se concentrent sur leurs actifs les plus essentiels : les données clients et les données d'entreprise. Netwrix vous permet d'adopter une approche de sécurité centrée sur les données. Il identifie les contenus sensibles dans les données structurées ou non structurées, sur site ou dans le Cloud, pour réduire les risques et détecter à temps les comportements suspects des utilisateurs afin de bloquer toute violation.

Auditor

De plus en plus d'organisations, de toutes tailles et de tous secteurs, reconnaissent l'importance des audits IT internes et externes. Les avantages sont nombreux : Les audits informatiques vous permettent d'améliorer la sécurité, de réussir les audits de conformité et d'optimiser les opérations informatiques. Mais, trop souvent, ce processus est bien plus fastidieux et chronophage que nécessaire. Découvrez comment le logiciel Netwrix Auditor facilite les audits et vous permet d'atteindre vos objectifs en mobilisant moins d'efforts.

Data Classification

Les données en constante croissance de votre organisation vous causent-elles des tracas ? Netwrix Data Classification, la solution de classification des données Netwrix résout vos défis en matière de données, tels que l'atténuation des risques de violation de données, l'exploitation optimale de vos contenus, l'accroissement de la productivité des employés et la réussite des audits de conformité au prix de moins d'efforts.

Sécurité des données

Netwrix propose un riche portefeuille de solutions pour protéger la sécurité des données. Notre solution permet d'identifier et de réduire les risques relatifs aux données sensibles, et de détecter en temps réel les menaces qui pèsent sur les informations sensibles. Nous avons aussi une solution dédiée pour NetSuite et Salesforce qui permet de sécuriser les données sensibles dans NetSuite ou Salesforce en effectuant un suivi des modifications et des personnalisations.

Protection de l'identité

Notre solution dédiée à la protection des identités permet d'accorder à la demande des accès privilégiés sécurisés et de protéger les comptes en gérant les mots de passe en libre-service. De plus, elle permet de renforcer la sécurité avec des politiques de mots de passe forts et peut détecter en temps réel les attaques contre l'Active Directory pour empêcher les modifications et les accès malveillants et, enfin, annuler les modifications et les suppressions non désirées dans Active Directory.

Sécurité de l'infrastructure

Les solutions dédiées à la protection de l'infrastructure permettent de veiller à ce que les systèmes informatiques soient sécurisés à tout moment, pour identifier les vulnérabilités de l'infrastructure informatique avant qu'elles ne soient exploitées.

Points forts

- Plus de 10 000 clients dans plus de 100 pays
- Une assistance à la clientèle bénéficiant de 97 % de satisfaction client
- Plus de 150 distinctions sectorielles
- Sélectionnée dans les listes Inc. 5000 et Deloitte Technology Fast 500, comme une des entreprises à la croissance la plus rapide

netwrix

LE MONDE PROTÉGÉ CONTRE LES CYBERMENACES

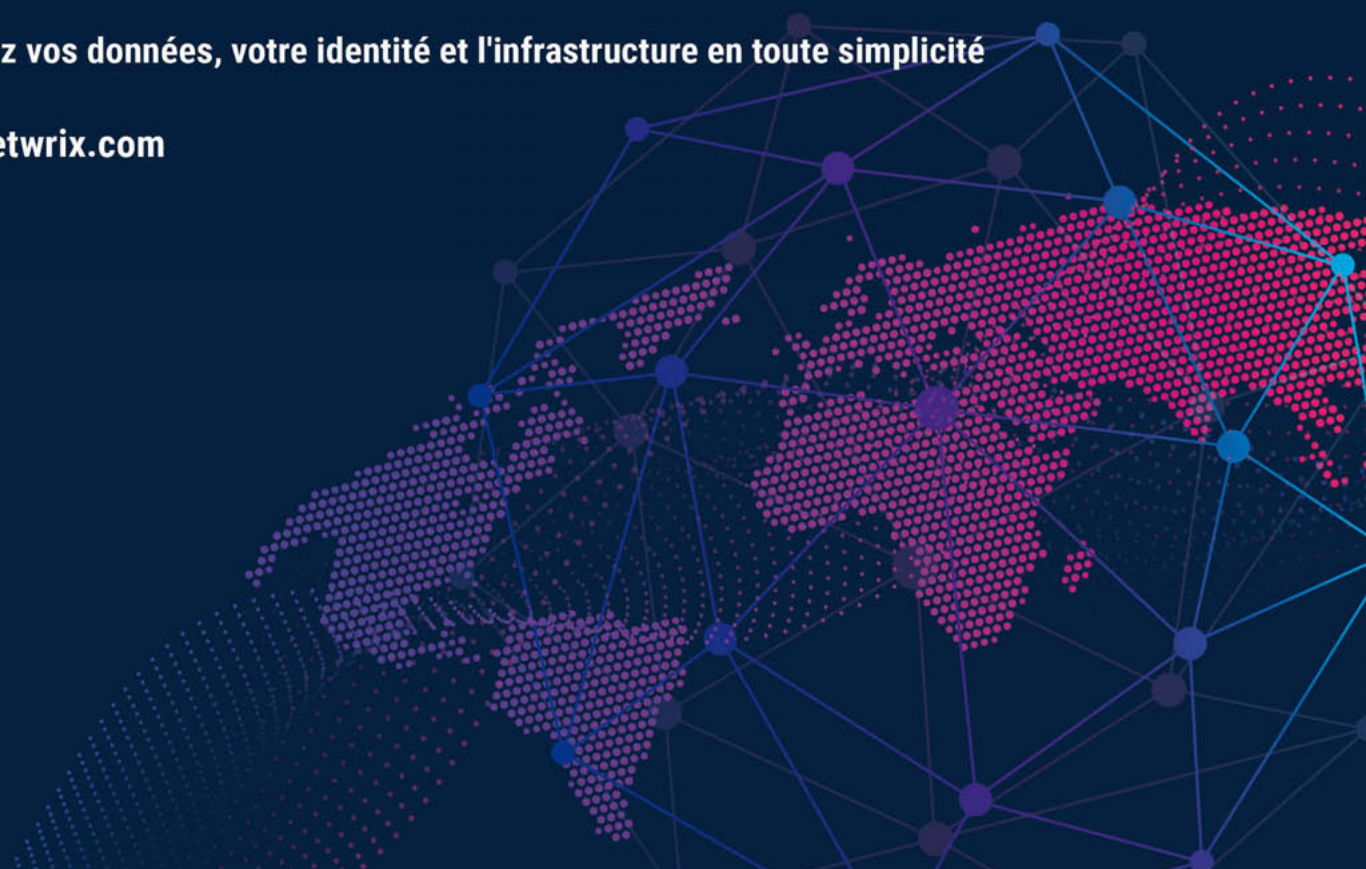
Dans une époque de cybermenaces constantes, comment pouvez-vous vous assurer que votre entreprise sera encore plus sécurisée demain qu'elle ne l'est aujourd'hui ?

Netwrix aide plus de 10 000 organisations dans le monde à:

- Surmonter la sécurité cloisonnée pour éliminer les angles morts
- Suivre les meilleures pratiques de l'industrie pour identifier, gérer et réduire les risques de cybersécurité

Protégez vos données, votre identité et l'infrastructure en toute simplicité

www.netwrix.com



Société : OKTA FRANCE
Adresse : 9-11 allée de l'Arche - 92400 Courbevoie
Tél. : 01 85 64 08 80
E-mail : **paris@okta.com**
Site web : **www.okta.com/fr**

Spécialisations

Solutions de gestion des identités et des accès (Identity & Access Management, Customer Identity & Access Management)

Chiffres clés

- *Créée en 2009 par Todd McKinnon (CEO) & Frederic Kerrest (COO)*
- *Entrée en Bourse en 2017 (OKTA)*
- *Chiffre d'affaires : $ 835 M pour l'année fiscale 2021*
- *3 850 collaborateurs dans le monde*
- *+ de 10 600 clients*
- *Acquisition d'Auth0 en mai 2021*

Dirigeant

Nicolas PETROUSSENKO
Country Manager France
nicolas.petroussenko@okta.com

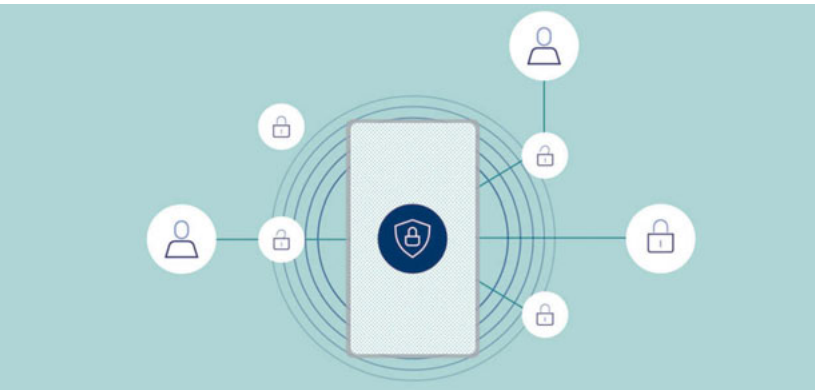
Contact
Infinigate France

Tony CILIBRASI
Business Developper
Tony.cilibrasi@infinigate.fr

Business Unit dédiée Okta
okta@infinigate.fr

Okta, l'identité numérique pour tous

Okta est le leader indépendant des services de gestion des identités et des accès. Okta Identity Cloud permet aux organisations de connecter aux technologies pertinentes les individus adéquats, au moment opportun.



Okta vous accompagne dans votre transformation digitale pour faire de l'identité le pilier de votre stratégie Zero Trust, sécuriser les modes de travail hybride, accélérer la migration vers le Cloud, réduire les points de frictions IT, améliorer l'engagement client et renforcer la confiance des utilisateurs.

Sa plateforme Okta Identity Cloud permet de sécuriser l'accès des collaborateurs, partenaires et prestataires grâce à ses solutions d'**Identity & Access Management** (IAM) et d'offrir une expérience de connexion fluide et sécurisée aux applications clients avec ses solutions **Customer Identity & Access Management** (CIAM).

Agnostique et évolutive, la plateforme Okta possède le plus vaste portefeuille d'applications pré intégrées du marché. Les clients d'Okta ont ainsi la possibilité de se connecter aux intégrations prêtes à l'emploi de plus de **7 500 applications cloud, on-premise et mobiles,** en quelques minutes et en toute sécurité.

Okta est distribué par Infinigate France qui accompagne les revendeurs, intégrateurs et clients dans leurs projets de cybersécurité.

Solutions

Identity Access Management (IAM)

Facilitez et protégez les accès de vos collaborateurs, partenaires et prestataires.

- Single Sign-On
- Universal Directory
- Advanced Server Access
- Multi-Factor Authentication
- Lifecycle Management
- Access Gateway
- API Access Management

Customer Identity Access Management (CIAM)

Offrez des expériences d'enregistrement et d'authentification fluides à vos clients

- Multi-Factor Authentication
- Lifecycle Management
- Access Gateway
- API Access Management
- Authentication
- User Management
- B2B Integration

Pourquoi choisir Okta ?

Pour la quatrième année consécutive, Okta figure parmi les leaders du Gartner Magic Quadrant for Access Management 2020. Comme le souligne Gartner dans son rapport complémentaire consacré aux fonctionnalités critiques, Okta est « l'un des outils de gestion des accès les plus avancés et matures du marché, capable de répondre aux exigences d'accès des utilisateurs internes comme externes ».

Références Clients

Plus de 10 650 organisations à travers le monde – dont Engie, JetBlue, Nordstrom, Siemens, Slack, T-Mobile, Takeda, ou encore Twilio – font confiance à Okta pour protéger les identités de leurs personnel, partenaires et clients.

Société : OXIBOX
Adresse : 15 boulevard des Chênes
78280 Guyancourt
Tél. : 01 30 54 45 79
Mail : contact@oxibox.fr

Spécialisations

- **Résilience des données.**
- **Enclaves sécurisées à immutabilité garantie.**
- **Solution conforme aux recommandations de l'ANSSI.**
- **Restauration instantanée d'un fichier ou d'une machine virtuelle.**
- **Compatibilité étendue : Windows, MacOs, Linux, environnements virtualisés.**
- **Tarification à la volumétrie sans frais de licence.**

Chiffres clés

+ de 1 200 clients
+ de 2,5 Po protégés chaque jour
100 partenaires distributeurs

Certifications

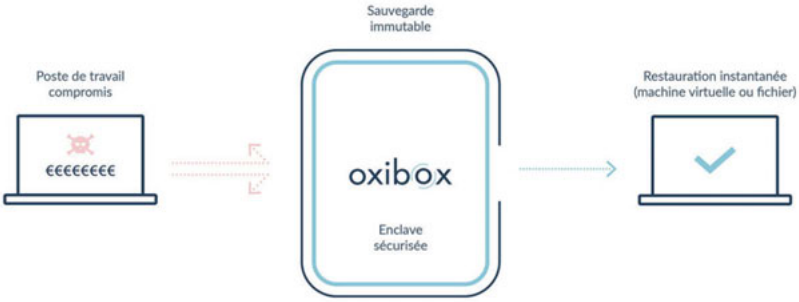
- Solution référencée DINUM.
- Cloud français certifié HDS et ISO 27001/ 50001 et Tier III.
- Oxibox Fireproof : ASTM E119.

Historique

- **2014 : Lancement Oxibox Backup-as-a-Service**
- **2016 : Lancement Oxibox Plug-and-Protect**
- **2017 : Solution d'orchestration cloud Oxiadmin full multi-sources**
- **2018 : Rachat de la société Infosecure**
- **2019 : Référencement UGAP / Sélection par l'European Cyber Security Organisation / Rachat de la société IDS Box / Intégration du classement FrenchWeb 500**
- **2020 : Membre CyberTaskForce / Classement Early Metrics Top 20% / Lancement d'Oxibox Data Protection / Prix de la Startup Innovante Airbus**
- **2021 : Référencement DINUM / Vainqueur du prix Techinnov / Sélection SPRING50**

Résilient face aux ransomwares

Les solutions de sauvegarde et de protection des données ne suffisent plus à garantir la pérennité des systèmes face à l'explosion des menaces cyber.
La technologie innovante d'Oxibox permet de répondre à cet enjeu par la création d'enclaves sécurisées qui garantissent l'immutabilité des sauvegardes.



Répondre à la menace par l'innovation

Oxibox permet aux entreprises de redémarrer leurs systèmes immédiatement après une cyberattaque grâce aux sauvegardes rendues résilientes.
La solution inclut la sauvegarde des données sur site, celle des postes nomades ainsi que les services cloud. Les offres sont adaptées aux besoins complexes des grands comptes comme des petites entreprises à partir de 1 To.

Oxibox Data Protection permet le déploiement instantané d'enclaves sécurisées, compatibles avec la plupart des solutions de sauvegarde.
Oxibox Plug-and-Protect est une solution clé en main, permettant la mise en conformité immédiate avec les recommandations de l'ANSSI : sauvegarde automatique déconnectée, répliquée à distance "3-2-1".

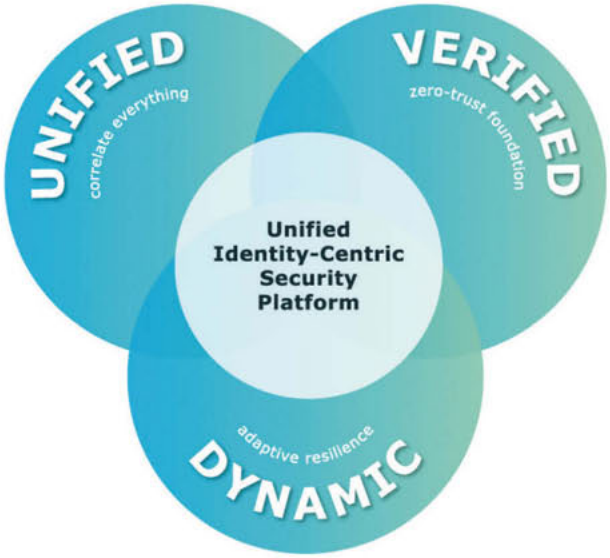
Dirigeant
François ESNOL-FEUGEAS
CEO et fondateur

Qui sont les cibles des ransomwares ?

« Les victimes des attaques sont peu enclines à communiquer, il est donc difficile de disposer de chiffres précis. Ceux publiés par les prestataires ne révèlent que la partie émergée de l'iceberg. Grâce à des organismes tels que cybermalveillance.gouv.fr, le recensement des attaques permet de faire un état de la menace plus réaliste.
Les modes opératoires évoluent très vite. Les cybercriminels sont passés d'une approche de masse à un ciblage intelligent frappant les organisations les plus sensibles et les plus vulnérables.
Très souvent, les entreprises qui prennent contact avec nous ont déjà été victimes d'un sinistre. C'est pourquoi nous appuyons le travail de sensibilisation sur le terrain avec nos partenaires distributeurs : leur rôle de conseil est clé pour les dirigeants qui n'ont pas identifié le risque ou ne savent pas comment anticiper. Très révélatrice de nos lacunes en matière de gestion de risque, l'année 2020 a provoqué une prise de conscience. Bousculés dans l'organisation du travail, dans nos usages, nous faisons face aux vulnérabilités des systèmes avec une mise en danger de la continuité du service public quand hôpitaux et collectivités sont pris pour cible. »

Pourquoi les leaders avant-gardistes choisissent One Identity

Nos différenciateurs



One Identity fournit une cybersécurité centrée sur l'identité qui protège les personnes, les applications et les données essentielles à l'entreprise. Nous vérifions tout, afin que chaque utilisateur ait les bons accès, au bon moment, pour les bonnes raisons. Notre plate-forme de sécurité unifiée centrée sur l'identité rassemble les meilleures capacités de gestion des comptes à privilèges (PAM), de gouvernance et d'administration des identités (IGA) et d'Active Directory et d'Azure Active Directory (AD/AAD) pour assurer la cybersécurité. One Identity est un éditeur de confiance de renommée mondiale, gérant plus de 250 millions d'identités pour plus de 5 000 organisations dans le monde.
Pour plus d'informations, visitez http://www.oneidentity.com/fr-fr.

- **Comblez les failles** de sécurité
- **Arrêtez les menaces** (internes et externes)
- **Sécurisez** l'accès à distance
- **Ouvrez** les silos de données
- Adoptez une **approche holistique** de la sécurité
- Redonnez le **sourire aux RSSI et aux utilisateurs**

Des solutions primées:

- Gestion des comptes à privilèges - PAM
- Gestion du cycle de vie des comptes Active Directory
- Gouvernance et administration des identités - IGA

Essais gratuits (Cloud, virtuels et installés)
www.oneidentity.com/fr-fr

Alors pourquoi les leaders avant-gardistes choisissent-ils One Identity ? Il y a trois choses importantes qui nous différencient :

Unified

Avec notre plateforme de sécurité unifiée centrée sur l'identité vous pouvez corréler toutes les identités, utilisateurs, applications et comptes à travers votre informatique multigénérationnelle.

- **Des solutions primées :** les analystes du marché de l'IT reconnaissent systématiquement l'excellence de nos solutions UAM , IGA et PAM
- **Fonctionne de manière transparente dans votre environnement :** API, notamment Microsoft Office, SAP, Salesforce, ServiceNow, Workday, Epic et plus encore
- **Intelligence et analyse intégrées :** source unique de vérité avec connaissance contextuelle, améliorations automatisées.

Verified

Notre plate-forme de sécurité unifiée centrée sur l'identité est la base Zero Trust pour protéger et fournir l'accès aux personnes, aux applications et aux données.

- **Privilège just-in-time :** accordez le bon accès au bon utilisateur au bon moment pour une raison précise
- **Surveillance contextuelle et suivi de session :** minimisez les zones de vulnérabilité grâce à une visibilité et une vérifiabilité totales
- **Analyse comportementale :** optimisez les décisions et automatisez les actions dans votre écosystème de cybersécurité centré sur l'identité

Dynamic

Notre plateforme de sécurité unifiée centrée sur l'identité offre une résilience adaptative aux changements organisationnels, à l'évolution technologique et aux menaces émergentes de cybersécurité.

- **Cloud sans compromis :** fonctionnalités complètes fournies via SaaS ; intégrations avec Microsoft Azure, Amazon Web Services, Google Cloud, Docker et plus
- **Solutions flexibles et personnalisables :** commencez là où vous êtes et renforcez votre posture de cybersécurité centrée sur l'identité graduellement
- **Niveau entreprise :** évolutivité sans limites, testée en combat live par les plus grandes entreprises mondiales sensibilisées à la cybersécurité

Comment nous aidons à combler les failles de cybersécurité

1. **Corrélation holistique :** unification de bout en bout des identités et des comptes
2. **Orchestration automatisée :** processus moderne et gouvernance frictionless à travers l'identité et les privilèges
3. **Enrichissement intelligent :** ne donner à chacun des privilèges qu'avec une conscience contextuelle – continuum de droits
4. **Adaptation continue :** aux changements dans les rôles/responsabilités des utilisateurs, l'infrastructure informatique, les nouvelles menaces
5. **Vérification continue :** zéro confiance, maintenant ! droits just-in-time avec connaissance de la situation et surveillance du comportement

« One Identity a pour vocation de fournir agilité et efficacité aux entreprises en matière de cybersécurité, quelle que soit sa taille ou son secteur d'activité tout en sécurisant les actifs numériques de l'entreprise. »

Sébastien de LA TULLAYE, Directeur Général France de ONE IDENTITY

LE PARTENAIRE DE CONFIANCE POUR LA GESTION DES CONTENUS ET DOCUMENTS SENSIBLES

Société : OODRIVE
Nom des marques :
OODRIVE_SHARE – OODRIVE_SIGN – OODRIVE_MEDIA – OODRIVE_MEETING

Adresse : 26, rue du Faubourg-Poissonnière – 75010 Paris
Tél. : +33 (0)1 46 22 07 00
Site web : **www.oodrive.com/fr**

Contact
Maxime GEFFRAY
Communication Project Manager
m.geffray@oodrive.com

Spécialisations

SaaS, gestion des contenus et documents sensibles, solutions cloud sécurisées, plateforme collaborative, signature électronique, partage et synchronisation

Chiffres clés

CA : 49 M€ en 2020
Effectifs : 400 collaborateurs
Utilisateurs : + de 1M
Clients : + de 15 000 professionnels
International : solutions utilisées dans 90 pays

Oodrive propose aux entreprises des solutions de partage de documents, de sauvegarde et de signature électronique répondant aux certifications françaises et internationales les plus exigeantes en termes de sécurité et de confidentialité.

Créé en 2000, le groupe français est aujourd'hui le leader européen de la gestion des données sensibles. Présent en Europe, oodrive compte plus de quatre cents collaborateurs. Ses solutions équipent plus de 1 million d'utilisateurs de tous secteurs d'activité.

Pour satisfaire aux besoins de souveraineté et de confidentialité, et conformément aux réglementations en vigueur, la sécurité des données clients est garantie par les qualifications SecNumCloud et eIDAS, les certifications RGS***, ISO 27001:2013 et HDS.

Conscient que chaque action a un impact sur la société et l'environnement, Oodrive est engagé en matière de responsabilités sociétales des entreprises (RSE). Le groupe met en œuvre des mesures écoresponsables afin de réduire son empreinte carbone et compense chaque année la part résiduelle de ses émissions de gaz à effet de serre*.

**Certifié par ERM et compensé par Judo CARES.*

«Aujourd'hui, l'actif principal d'une entreprise, ce sont ses données, et particulièrement les données sensibles. La Chine et les États-Unis exercent une hégémonie sur ces sujets et leurs législations font loi en Europe. C'est pourquoi nous nous positionnons comme l'alternative européenne aux solutions collaboratives américaines.»

Stanislas de REMUR
Co-fondateur et CEO d'Oodrive

Offres

oodrive _share

Avec l'offre de partage, vous consultez, modifiez et annotez vos documents au sein d'un espace numérique entièrement sécurisé, accessible partout et à tout moment.

oodrive _sign

Cette solution vous garantit une signature électronique sécurisée en règle avec la conformité, selon vos besoins et exigences.

oodrive _media

L'offre de Digital Asset Management permet de centraliser et gérer tous vos actifs de marque. Tirez le meilleur profit de vos ressources numériques grâce à une solution sécurisée et intuitive.

oodrive _meeting

Avec ce module, vous dématérialisez vos réunions de gouvernance, sécurisez vos données critiques et prenez des décisions importantes en gardant les idées claires.

FOCUS : la signature électronique, un outil plébiscité

Acquéreur en 2021 de l'entreprise française SELL&SIGN, Oodrive a enrichi son offre de signature électronique oodrive_sign pour se présenter comme *la* référence européenne du marché. En effet, la signature électronique s'est largement démocratisée ces deux dernières années. Elle est de plus en plus adoptée par les organisations puisqu'elle est parfaitement adaptée aux nouveaux modes de travail enclenchés par la crise sanitaire, et permet également de répondre aux enjeux de transformation digitale des entreprises, déjà présents avant la pandémie.

Avec oodrive_sign, les clients signent un document sur tout support, partout, avec ou sans réseau. Ils bénéficient d'une protection juridique optimale garantie et d'un dossier de preuve renforcé grâce à divers éléments comme l'horodatage, la certification et l'archivage légal des documents signés sur oodrive_sign. Enfin, la solution permet à ses utilisateurs de personnaliser leurs parcours de signatures en fonction de leur métier ou de leur secteur d'activité. La solution permet également de collecter des informations sur les signataires de façon consentie grâce aux champs personnalisables Smartfields©.

oodrive — NO LIBERTY WITHOUT SECURITY

SELL&SIGN — SOLUTION DE SIGNATURE ÉLECTRONIQUE INTELLIGENTE

Certifications

VISA DE SÉCURITÉ — SecNumCloud — CERTIFIED ISO 27001:2013 COMPANY — ISO 27701 — HDS

Société : PING IDENTITY
Adresse : 7 rue Léo-Delibes, 75116 Paris
Tél. : 01 86 26 43 16
Mail : **sales@pingidentity.com**
Site web : **https://www.pingidentity.com/fr**

La solution d'identité intelligente pour les entreprises

Ping Identity est la solution d'identité intelligente pour les entreprises. Nous aidons les organisations à mettre en œuvre un modèle de sécurité Zero Trust défini par l'identité et des expériences utilisateurs plus personnalisées. La plateforme PingOne Cloud fournit l'accès aux applications cloud, mobiles, SaaS et on-premises pour les collaborateurs, clients et partenaires. Nos solutions permettent d'accélérer les initiatives de transformation numérique, satisfaire les clients et sécuriser les entreprises grâce aux fonctions d'authentification multifacteur, single sign-on, la gestion des accès, protection intelligente des API, annuaire et gouvernance des données.

Spécialisations

Gestion des identités et des accès pour les environnements IT hybrides

Chiffres clés

CA : 244 M$ en 2020
Effectifs : 1 200 dans le monde
Historique : création en 2002

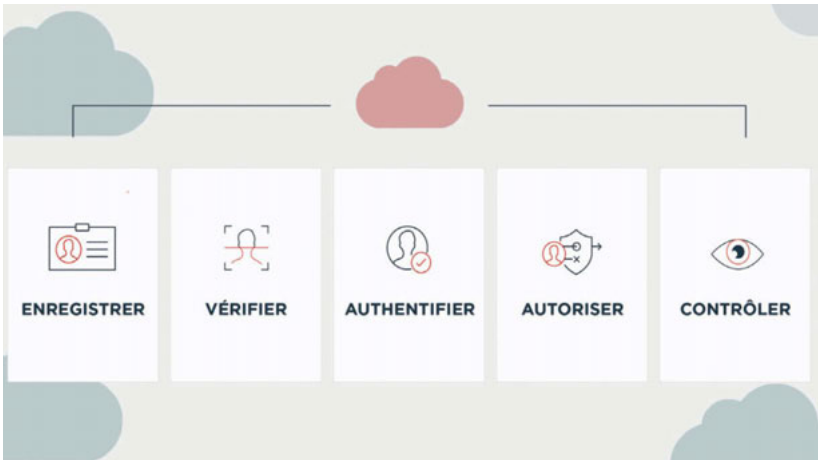
Dirigeant

André DURAND
CEO et co-fondateur de Ping Identity

Références

Plus de la moitié des 100 plus grandes entreprises au monde nous font confiance pour notre expertise et partenariats avec des sociétés comme Microsoft et Amazon.

Un Hub d'authentification et de contrôle d'accès



Offres

IDENTITÉ POUR LES EMPLOYÉS

La solution d'identité cloud de Ping pour les collaborateurs fournit des services d'authentification et d'autorisation centralisées pour connecter les employés vers n'importe quelle application, n'importe quel directory et via n'importe quel appareil. Ping élimine les silos d'authentification qui entravent la productivité et la sécurité des utilisateurs.

En mettant en œuvre un hub d'authentification géré de manière centralisée et des contrôles d'accès, les organisations peuvent accéder à des expériences utilisateurs transparentes, fluides et sécurisées pour démarrer l'adoption du modèle Zero Trust.

IDENTITÉ POUR LES CLIENTS

Plus que jamais, l'expérience client et la sécurité ont le potentiel d'aider les organisations à acquérir de nouveaux clients et fidéliser les clients existants pour accélérer les revenus via le digital.

La gestion des identités et des accès clients (CIAM) peut aider les marques à fournir l'expérience client sécurisée et transparente nécessaire pour dégager un avantage concurrentiel considérable et gagner la confiance des clients.

Points Forts

- Leader du Gartner Magic Quadrant 2021 pour l'Acces Management
- Leader du KuppingerCole Leadership Compass pour le CIAM
- Net Promoter Score (NPS) de 65 - leader du marché

La Plateforme PingOne Cloud

Une plateforme unique pour améliorer la sécurité et l'agilité dans votre organisation

ENREGISTRER

VÉRIFIER

AUTHENTIFIER

AUTORISER

CONTRÔLER

Société : POST TELECOM
Département POST Cyberforce
Adresse : 20 rue de Reims,
L-2417 Luxembourg
Tél. : 8002 4000
Mail : **commercial.telecom@post.lu**
Sites web : **www.cyberforce.lu**
www.post.lu

Spécialisations

- **Développement et intégration de solutions en cybersécurité**
- **Pentesting**
- **Conseil**
- **SOC & CSIRT**
- **Gestion des risques**
- **Conformité**
- **Data Science**
- **Sécurité Telecom**

Dirigeants

Claude STRASSER
Directeur général de POST Luxembourg

Pierre ZIMMER
Directeur général adjoint de POST Luxembourg & Chief Strategy Officer

Mohamed OURDANE
Chef du département POST Cyberforce de POST Luxembourg

POST Luxembourg est le premier opérateur de services postaux et de télécommunications du pays et propose ses services aux clients résidentiels et professionnels.

En tant que fournisseur majeur en termes de services de télécommunications et intégrateur ICT, POST Luxembourg accompagne activement la transformation digitale du Luxembourg. Ainsi, afin de centraliser toutes les compétences en cybersécurité au sein du Groupe en une seule équipe, le département « POST Cyberforce » a été créé en 2019. Conscient de l'importance que revêt la cybersécurité, POST Cyberforce, avec son centre d'expertise étayé, propose des services complets afin de mieux anticiper et contrer les cybermenaces.

Services

POST Cyberforce propose une gamme complète de services personnalisés en cybersécurité et accompagne ainsi les entreprises de toute taille, tant au Luxembourg qu'à l'international.

Offensive security

Afin de vérifier qu'un système d'information soit bien sécurisé et que les équipes opérationnelles aient les réflexes adaptés en cas d'incident, POST Cyberforce propose divers services de sécurité offensive :

- Adversary simulation
- Pentesting
- Red team & Purple team exercises
- Physical Intrusion
- Vulnerability research & application robustness testing
- Advanced phishing campaign…

Advisory services

Avec son entité « Risk & Business Advisory », POST Cyberforce répond aux défis posés par la transformation digitale, notamment à travers une offre de conseils spécifiques appelée « Trusted Advisory Services ». Cette activité de conseil couvre la gestion de la continuité d'activité, la cyber-résilience, la transformation informatique, l'audit des centres de données ainsi que tout le spectre de la gouvernance, du risque et de la conformité.

Security professional services

POST Cyberforce conçoit et met en œuvre des solutions (design, architecture et intégration) de sécurité complètes pour une protection optimale d'une entreprise ou structure avec un large panel de partenaires technologiques et en assurant, en cas de besoin, la gestion opérationnelle :

- Gestion des vulnérabilités et des menaces
- Protection des données et des identités
- Sécurité périmétrique
- Protection des devices, serveurs et applications.

Cyberdefense

Grâce à son SOC 24/7 et son CSIRT, POST Cyberforce détecte en temps réel les incidents de sécurité et intervient instantanément. Un SOC local unique permet ainsi de détecter aussi bien les menaces informatiques directes, que celles qui utilisent les réseaux télécoms de POST. La conformité réglementaire est garantie et l'utilisation de l'IA et de l'automatisation (SOAR) permet des réponses efficaces et proportionnelles, selon le type de menace.

Les services du CSIRT POST Cyberforce comprennent les prestations suivantes sur les incidents de sécurité :

- Assistance 24/7 avec intervention sur site possible
- Analyse et remédiation rapide
- Analyse forensique post-mortem
- Renseignements sur les menaces (Threat intelligence).

CyberLabs

POST Cyberforce dispose d'une équipe dédiée qui conçoit des solutions innovantes contribuant à renforcer le niveau de sécurité des filiales du Groupe POST Luxembourg, ainsi que de ses clients. Dans une démarche d'innovation ouverte, cette équipe d'experts fait progresser le développement de produits de sécurité de pointe et soutient ainsi la promotion d'initiatives de sécurité dans les domaines des télécoms, du big-data et tiers de confiance, de l'informatique, de l'IoT, etc.

We ensure you Focus your
CYBERFORCE
security on your business

Get in touch with our experts
CYBERFORCE.lu

POST
LUXEMBOURG

PRIMX
MAKE ENCRYPTION HAPPEN

Société : PRIM'X
Adresse : 21 rue Camille-Desmoulins
92130 Issy-les-Moulineaux
Tél. : 01 40 95 24 80
Mail : **business@primx.eu**
Site web : **www.primx.eu**

Spécialisations

Éditeur de logiciels de chiffrement pour la confidentialité des données :

- **Postes de travail et environnement utilisateur**
- **Disques et laptops**
- **E-mails et échanges de données**
- **Cloud et bibliothèques de partage**

Dirigeants

Serge BINET
Président et co-fondateur
Nicolas BACHELIER
Directeur général adjoint

Contact

Vanessa de CHAMBRUN
Directrice commerciale France
business@primx.eu

PRIM'X, éditeur de logiciels depuis plus de 15 ans, met son expertise du chiffrement au service de la protection des données sensibles des entreprises. Ses logiciels, qui s'adressent majoritairement aux administrations, aux grands-comptes et plus récemment aux PME, permettent de gérer la confidentialité des données stockées et échangées.

L'objectif de PRIM'X est d'apporter une nouvelle manière d'appliquer le chiffrement dans une organisation pour une meilleure protection des données sensibles contre la perte, le vol, la publication (disclosure), et l'espionnage économique.

L'information est un asset précieux de l'entreprise, et sa valeur réelle n'est pas celle qu'on lui attribue mais celle qu'un ennemi lui donne. Les données sont partout et disséminées à la fois, ce qui rend leur classification fastidieuse. Pour ces raisons, il est nécessaire d'adopter une politique globale : Encrypt Everything, Everywhere, and Always.

Alors que les produits de chiffrement du marché sont souvent très partiels et d'un maniement assez complexe, la vision de PRIM'X est que le chiffrement doit être global, simple et transparent, automatique et dirigé par une politique de sécurité.

La sécurité ne doit pas uniquement se limiter à une simple protection contre l'extérieur, mais permettre un cloisonnement interne.

La confidentialité ne peut pas être laissée à l'appréciation des utilisateurs, avertis ou non, mais dirigée par l'entreprise à 360° : une protection globale et de bout-en-bout.

Offres

Les solutions de PRIM'X permettent un cloisonnement cryptographique des données entre utilisateurs et interdisent aussi les accès non autorisés aux données par des tiers.

ORIZON : chiffrement des environnements utilisateurs et des espaces partagés dans le Cloud.

ZONECENTRAL : protection des fichiers stockés sur les postes de travail, les périphériques et les serveurs.

CRYHOD : protection des postes nomades avec authentification préboot et chiffrement de la totalité du disque dur.

ZED! et ZEDMAIL : échange de conteneurs ou de messages électroniques chiffrés.

ZONEPOINT : chiffrement des documents partagés sur MS SharePointTM, sécurité de l'archivage documentaire.

Et notre offre packagée en partenariat avec Synetis et Yubico : GO ENCRYPT (logiciel de chiffrement + matériel d'authentification + intégration + accompagnement).

Certifications

PRIM'X a fait de la certification de sécurité de ses solutions une politique stratégique d'éditeur. Les certificats sont entretenus, repassés pour les différentes versions et les différentes plates-formes pour suivre l'évolution des technologies, de l'état de l'art en cryptographie, et des menaces. Les solutions passent des contre-évaluations nationales, transnationales, ou spécifiques à un marché donné : certification EAL3+, qualification Anssi, visa de sécurité, agrément UE et Otan.

Reconnus au niveau international, ces certificats apportent une confiance dans la robustesse du produit.

CERTIFIED CC EAL3+

EU UE RESTRICTED

VISA DE SÉCURITÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI

NATO OTAN RESTRICTED

PRIMX

MAKE ENCRYPTION HAPPEN

Encryption solutions for data confidentiality*

CRYHOD

ZED!

ORIZON

ZONEPOINT

ZONECENTRAL

ZEDMAIL

Rendre le chiffrement possible - *Solutions de chiffrement pour la confidentialité des données - **ZoneCentral, Cryhod, Zed!

CERTIFICATION CC EAL3+

VISA DE SÉCURITÉ** QUALIFICATION ANSSI

AGRÉÉS POUR LA PROTECTION D'INFORMATION MARQUÉE DIFFUSION RESTREINTE

www.primx.eu

Société : SCILLE
Nom de marque : PARSEC
Adresse : 11 chemin de Jalès
33160 Saint-Médard-en-Jalles
Mail : **parsec@scille.fr**
Site web : **www.parsec.cloud**

Spécialisations

Solution de partage et de stockage sécurisé des données sensibles dans le Cloud.

Chiffres clés

Effectifs : 11 salariés

Historique

Scille est une start-up créée en 2014 par Thierry Leblond (CEO) et Emmanuel Leblond (CTO). En 2016, avec le soutien de la DGA et en collaboration avec le LaBRI, nous avons lancé le développement de la solution de cybersécurité Parsec, dont la commercialisation a débuté en 2020.

Dirigeants

Thierry LEBLOND
Co-fondateur et CEO /
Thierry.leblond@scille.fr

Emmanuel LEBLOND
Co-fondateur et CTO /
emmanuel.leblond@scille.fr

SCILLE est une Jeune entreprise innovante (JEI) créée en 2014 spécialisée dans :

- *la sécurité du partage des données sur le Cloud,*
- *la transformation numérique et la dématérialisation de processus complexes et sécurisés.*

SCILLE, membre de Systematic Paris Région et du GICAT, est une start-up d'une dizaine d'ingénieurs de haut niveau sur Bordeaux et Paris, qui édite le navigateur de données sensibles PARSEC.

Offres

Parsec est un logiciel open source de distribution décentralisée de la confiance en mode **ZeroTrust et Zero-knowledge**. Certifiée **CSPN par l'Anssi,** Parsec est une solution collaborative ergonomique permettant le stockage souverain des données. La solution Parsec assure aux entreprises une sécurité « anti-ransomware » grâce à des fonctionnalités innovantes telles que la double authentification, la traçabilité et l'historisation des fichiers, accessibles à tout moment en cas d'attaque du serveur par des personnes malveillantes.

L'axe principal du développement de Parsec repose sur le fait que la confiance du secret donnant accès aux données chiffrées de bout en bout ne doit être confiée qu'à l'utilisateur final. Le modèle de sécurité de Parsec s'appuie donc sur cinq nouveaux paradigmes de sécurité qui sont :

- la confiance nulle ou « Zero Trust »,
- la diffusion de connaissance nulle ou « Zero Knowledge »,
- la sécurité centrée sur l'utilisateur ou « User-centered Security Model ».
- la « micro-segmentation » des données sensibles,
- le fonctionnement en mode « WORM (Write Once, Read Many) ---> fonction **ANTI-RANSONWARE**

Certifications

- Certification CSPN délivrée par l'Anssi
- Partenariat 3D Outscale sur la marketplace
- Partenariat Airbus développement
- Autres références et prix : Partenaires - Parsec

Références Clients

Nous comptons parmi les utilisateurs de notre solution Saas à seulement 5 euros/user/mois des start-up, PME et cabinets d'avocats particulièrement sensibles aux questions de sécurité des données. De l'autre côté du spectre, nous proposons une offre On Premise personnalisable afin de répondre aux exigences des grands groupes. À ce titre, nous travaillons actuellement avec plusieurs acteurs OIV, étatiques et de la défense.

« Parsec fait confiance à ses collaborateurs comme à ses utilisateurs. La confiance structure littéralement la société, aussi bien dans sa conception que dans sa gestion quotidienne. Si Parsec livre strictement, à l'utilisateur propriétaire, les clés d'accès à ses données sensibles sans en garder un double, c'est justement parce que nous sommes convaincus que votre autonomie vous responsabilise et vous sécurise. Cette foi, nous l'avons également en nos collaborateurs. Nous leur faisons pleinement confiance, en fonctionnant en télétravail à 100 % depuis la création de Parsec. Nous sommes ainsi les premiers utilisateurs de notre propre solution et comprenons parfaitement ce que peuvent en attendre nos clients. » Thierry LEBLOND

Société : QUALYS TECHNOLOGIES
Adresse : Maison de la Défense,
7, place de la Défense,
92400 Courbevoie
Tél. : 01 41 93 35 70
Mail : **tam-fr@qualys.com**
Site Web : **www.qualys.com**

Spécialisations

- **Gestion des actifs IT**
- **Sécurité du SI**
- **Protection du Cloud**
- **Protection des applications web**
- **Conformité**
- **Gestion des certificats**

Chiffres clés

CA 2020 : $ 363 millions

CA 2019 : $ 321,6 millions

Historique

- Qualys, fondée en 1999, est l'un des premiers fournisseurs de services dans le Cloud, et c'est aujourd'hui le principal fournisseur de solutions de sécurité et de conformité.
- L'entreprise compte aujourd'hui plus de 19 000 clients dans plus de 130 pays et elle est cotée au Nasdaq depuis 2012 sous le symbole QLYS.
- Qualys est également l'un des fondateurs de la Cloud Security Alliance (CSA).
- Quelques chiffres : + de 1 000 milliards d'événements de sécurité traités, + de 3 milliards de scans IP/audits par an, 99,9996 % de précision d'analyse.

Dirigeant
Sumedh THAKAR
Président et CEO
Qualys

Née dans le Cloud et avec une approche novatrice de la sécurité, Qualys Cloud Platform et ses applications intégrées aident les entreprises à simplifier leurs opérations de sécurité et à réduire le coût de la conformité. Notre plateforme fournit en continu de précieux indicateurs de sécurité, et elle automatise le spectre complet des audits, de la conformité et de la protection des systèmes d'information et des applications Web.

Offre

Qualys aide les entreprises à rationaliser et fédérer leurs opérations de sécurité et de conformité IT au sein d'une seule et même plateforme, et à intégrer la sécurité à leur transformation numérique pour leur garantir davantage de souplesse, une activité plus dynamique et des économies substantielles. Qualys Cloud Platform et ses applications Cloud intégrées fournissent en permanence aux entreprises un service de renseignement sur la sécurité afin qu'elles puissent automatiser le spectre complet de l'audit, de la conformité et de la protection des systèmes d'information et des applications Web aussi bien sur site, sur les points d'extrémités et dans la plateforme Elastic Cloud.

Services

La Qualys Cloud Platform, c'est aujourd'hui plus de 20 applications regroupées en 7 catégories :

- Asset Inventory
- Infrastructure Security
- Cloud Infrastructure security
- Endpoint security
- DevSecOps
- Compliance
- Web App Security

Solutions

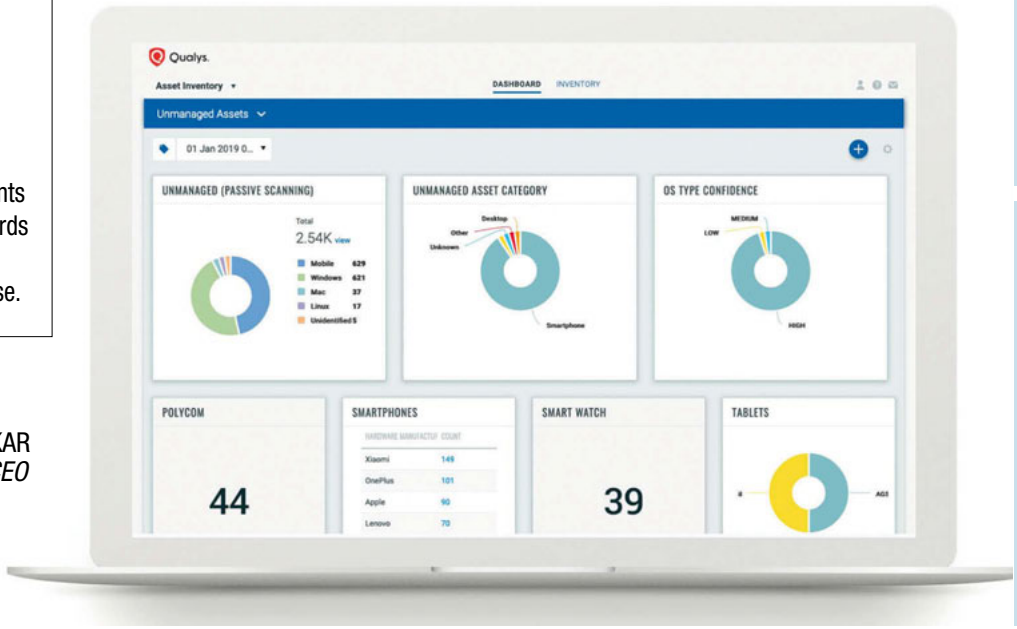
Points forts de la Qualys Cloud Platform

- Aucun matériel à acheter ou à gérer
- Des coûts d'exploitation réduits
- Des analyses faciles à lancer
- Une plateforme évolutive
- Des ressources actualisées
- Des données stockées en toute sécurité
- Une solution disponible dans le Cloud public, privé ou sur site

Références Clients

Clients internationaux : Microsoft, Apple, EBay, Amazon, Google, Bank of America, General Electrics, PWC…

Clients en France : Accor, Adeo, Air Liquide, Altran, Axa, BPCE, Carrefour, CDC, Danone, Groupama, Kering, Orange, RATP, Rexel, Société Générale, Sodexo, Saint-Gobain, Suez, Veolia…



QUODAGIS Digital Security : Conseils et expertises en cybersécurité

QUODAGIS Digital Security est la filiale sécurité du groupe français QUODAGIS.

Spécialistes en cybersécurité, nous avons pour vocation d'aider les entreprises à améliorer la sécurisation de leur système d'information et son adaptation aux nouveaux besoins et usages.

Société : QUODAGIS Digital Security
Adresse : 64 rue de Miromesnil
75008 Paris
Tél. : +33 1 55 06 11 91
Mail : **digital-security@quodagis.fr**
Site web : **digital-security.quodagis.fr**

Spécialisations

Audit, conseil, intégration, IAM, sécurité du Cloud, gestion des risques, Security Operation Center

Chiffres clés

Effectifs : 120 collaborateurs
CA 2020 : 10,8 M€

Localisation

Paris, Toulouse, Aurillac, Barcelone, Monaco

Dirigeant

Christophe LEROY
Directeur
QUODAGIS
Digital Security

Produits / services

Nos clients peuvent ainsi s'appuyer sur l'expertise de nos équipes dans les domaines suivants :

- **Audit et Pentest,** pour évaluer et contrôler le niveau de sécurité de leurs infrastructures.
- **Conseil et accompagnement** dans la gouvernance de leur cybersécurité,la gestion des risques, de la conformité et de la conduite de projets.
- **Identity Access Management** pour maîtriser la gestion des accès et des droits utilisateurs, et la conduite de leurs projets d'évolution de leur SI.
- **Formation et sensibilisation** afin de permettre à leurs collaborateurs de mieux appréhender les risques et de contribuer à la chaîne cybersécurité.
- **Security Operation Center** afin de bénéficier de l'ensemble de nos expertises dans la surveillance et la protection des actifs et équipements.
- **Délégation d'expertises**pour accompagner et renforcer vos équipes dans le domaine de la cybersécurité.

La synergie entre les entités du groupe QUODAGIS (intégration, services managés, accompagnement et transformation vers les services Cloud, assistance technique) permet à nos clients d'intégrer leur démarche cybersécurité dans leur stratégie IT globale.

Nous sommes convaincus que la cybersécurité doit s'inscrire naturellement dans les projets et services IT et répondre ainsi à l'ensemble des enjeux et contraintes des entreprises.

La maîtrise du groupe QUODAGIS dans les différents aspects de la gestion et de l'évolution des systèmes d'informations, nous permet de proposer à nos clients la démarche la plus adaptée à leurs contextes métiers, structurels et budgétaires.

Ainsi le groupe QUODAGIS accompagne depuis plus de dix ans des centaines de clients dans leurs projets de transformation de leur système d'information, de déploiement de technologies et de sécurisation des services.

Société : **QUERY INFORMATIQUE**
Adresse : 1 bd Charles-de-Gaulle
92700 Colombes
Tél. : 01 49 97 33 00
Mail : query@query-informatique.com
Site web : www.query-informatique.com

Spécialisations

Protection des postes de travail et des données, prise de main à distance sécurisée, connexion automatisée sans mot de passe, anonymisation des données de tests, environnements Windows et Mainframe IBM z/OS

Historique

Création en 1991

Nos solutions protègent vos données de façon optimale sur les environnements Windows et Mainframe z/OS au travers de solutions logicielles faciles à mettre en œuvre et des supports externes sécurisés, autonomes et multi plates-formes. Toutes ces solutions s'adaptent parfaitement aux besoins des clients, qu'ils soient grands comptes ou PME.

Solutions

Protection des postes de travail

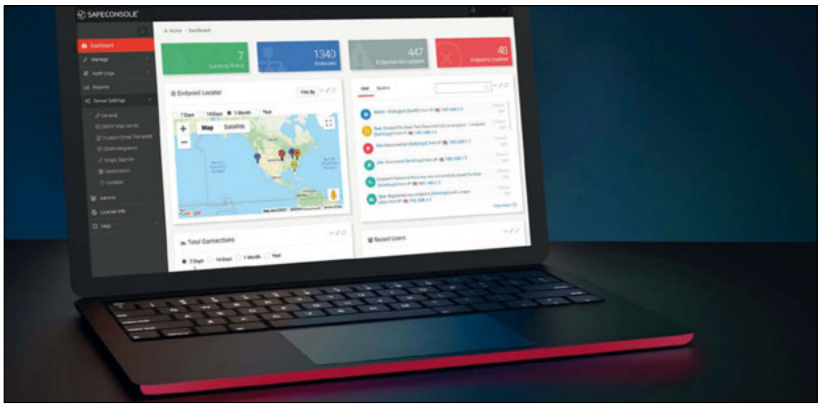
Sécurisez l'accès aux postes de travail grâce à une solution logicielle facile à mettre en œuvre et très flexible. Depuis une console centralisée, mettez en place vos stratégies de sécurité en fonction du type d'utilisateur pour le contrôle des périphériques externes, le filtrage des applications, le chiffrement partiel ou complet, etc. Suivez également l'activité de votre parc informatique et le mouvement des données.

Et plus besoin de mots de passe du fait de leur gestion automatisée et centralisée, la connexion aux sessions se faisant à l'aide d'un jeton de connexion, avec aussi la possibilité de générer des mots de passe dit « forts » pour l'ensemble des utilisateurs, et plus encore…

Protection des données

Nos clés USB et disques durs externes, chiffrés au niveau matériel, sont multi plates-formes (Windows, Mac Os et Linux) et très robustes. Avec des capacités de stockage allant de 8 Go à 15,3 To, ils s'adaptent aux sociétés de tous types et de toutes tailles. Les utilisateurs disposent ainsi d'un coffre-fort numérique leur permettant de transporter des données sensibles en toute sécurité, voire d'une machine virtuelle grâce à une clé USB sécurisée bootable.

Une solution logicielle optionnelle permet de plus la gestion centralisée de ces périphériques externes, sur site ou dans le Cloud. Différentes politiques de sécurité y sont paramétrables en fonction de vos besoins : politique de mot de passe, protection en écriture, restriction par type de fichiers, verrouillage d'inactivité, distribution de contenu, géolocalisation, blocage des ports USB…



Points forts

- Gestion centralisée
- Contrôle des périphériques
- Filtrage des applications
- Chiffrement partiel ou complet
- Périphériques sécurisés
- Connexion sans mot de passe
- Audits et rapports
- Prise de main à distance multi plate-forme sécurisée
- Création de jeux de tests sélectifs et anonymisés

Société : RAMPAR
Adresse : Bâtiment CRISCO DUO
7 avenue de la Cristallerie
92310 Sèvres
Tél. : 01 46 48 26 00
Mail : **contact@rampar.com**
Site web : **https://www.rampar.com**

Spécialisations

Sécurité :
- **Architecture sécurité**
- **Intégration de solutions de sécurité**

Cloud :
- **Architectures Cloud**
- **Replatforming d'applications**

Ops :
- **Hébergement Cloud**
- **DevOps**
- **MCO des infrastructures & applications**

Chiffres clés

CA 2020 : 14,6 M€
CA 2019 : 11 M€
Effectifs : 50 collaborateurs
Paris, Nantes

Dirigeants

Marc BERGER
Associé en charge des services managés
mberger@rampar.com

Benoît VÉROVE
Associé en charge de l'intégration
bverove@rampar.com

Olivier CRAIGNOU
Associé en charge du commerce
ocraignou@rampar.com

Rampar est un acteur majeur français sur les métiers de l'intégration, du Cloud et des Services managés dans les domaines de la cybersécurité et des infrastructures. Il apporte des solutions aux enjeux du numérique omniprésents chez ses clients. Dans un environnement technologique en perpétuelle évolution, ses experts réseau, sécurité et Cloud assurent une veille permanente animée par la passion de la technologie.

OFFRES :

Security

- Conception d'architecture
- Intégration de solutions de sécurité (Network, Cloud, Endpoint, applications)

Cloud

- Modèle MSP
- Conception, intégration et gestion des environnements Cloud publics (Azure, AWS)
- Replatforming d'applications

Ops

- Hosting en cloud privé et public
- Infogérance de SI
- Infogérance spécialisée
- Centre de support

Sécurité : nos experts cybersécurité conçoivent et mettent en œuvre les architectures de sécurité pour protéger vos données. Nous avons trié sur le volet un ensemble de partenaires et de solutions de sécurisation pour faire face aux menaces d'aujourd'hui.

Cloud : à nouvel horizon, nouvelles méthodes ! L'agilité et la créativité qu'offrent le Cloud imposent de nouvelles dynamiques projet. Forte de nos partenariats Azure et AWS, notre équipe MSP Cloud vous aide dans la construction d'applications cloud natives, le replatforming et vos projets lift & shift.

Ops : expertise technique pointue, réactivité d'intervention et souplesse de fonctionnement nous permettent d'infogérer et d'héberger vos applications et infrastructures critiques en toute sécurité.

Les SI de plus en plus ouverts et répondant à une tendance forte de travail collaboratif induisent des changements profonds des architectures chez nos clients, notamment en termes de «cloudification» des SI et bien entendu d'évolutions de la sécurisation des données de l'entreprise.
Rampar met au service de ses clients toute son expertise dans un contexte très souvent international pour répondre à ces nouveaux enjeux, depuis la conception d'architecture jusqu'au maintien en conditions opérationnelles, en passant par la fourniture et l'intégration de solutions technologiques.

Historique

2021 – Rampar obtient la certification Microsoft Linux and Open Source Databases Migration to Azure

2021 – Apax Partners prend une participation minoritaire dans le groupe Hifield, société mère de Rampar afin d'accompagner son fort développement en France et en Europe.

ROHDE&SCHWARZ
Make ideas real

Société : ROHDE & SCHWARZ CYBERSECURITY
Adresse : Parc Tertiaire de Meudon, 9-11 rue Jeanne-Braconnier, 92366 Meudon
Tél. : +33 1 46 20 96 00
Mail :
sales-fr.cybersecurity@rohde-schwarz.com
Site web :
www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz Cybersecurity est l'un des leaders en sécurité informatique qui protège les ressources numériques des entreprises et des institutions publiques au niveau mondial contre les cyberattaques. La société fournit des solutions innovantes de protection des données pour les environnements Cloud, une sécurité avancée pour les sites web, les applications Web et les Web services, ainsi que le chiffrement réseau, la sécurité des postes de travail et des appareils mobiles. Pour prévenir les cyberattaques de manière proactive plutôt que réactive, nos solutions informatiques de confiance sont développées selon l'approche de la sécurité by design.

Spécialisations

Pare-feu applicatif (WAF) in app, on-premises, dans le Cloud et en mode SaaS. Solution de protection des applications Cloud native.

Offres

R&S® Trusted Gate

- Chiffre et sécurise les données dans les Clouds publics
- Portefeuille de solutions adéquates pour les outils de Cloud et de collaboration
- Sécurité maximale pour Microsoft® SharePoint™ et Office 365™
- Échange de données sécurisé, respect de la protection des données et conformité.

R&S® Web Application Firewall

- Sécurise les applications web, services web et API
- Bloque les attaques sur la couche applicative y compris celles du Top 10 OWASP
- Surveille l'utilisation des applications web pour prévenir toute menace interne
- Intègre de multiples moteurs de sécurité et un workflow graphique et intuitif
- On-premises et multi-Cloud

R&S® Cloud Protector

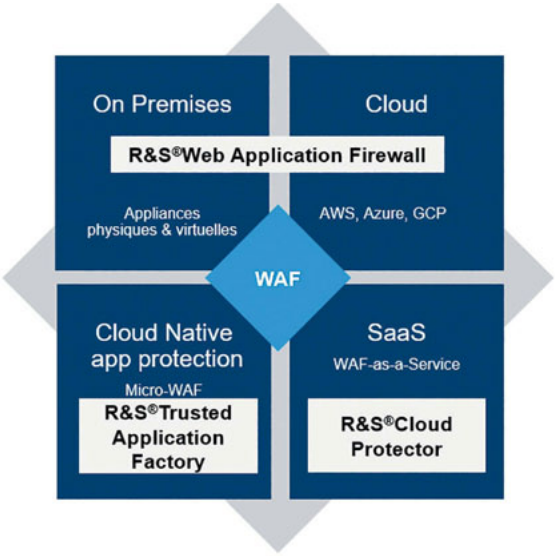
- Protège les sites et applications web avec un WAF en mode SaaS
- Sécurise les applications web en toute simplicité et de manière évolutive
- Empêche les attaques par déni de service distribué (DDoS)

R&S® Trusted Application Factory

- Solution déployée en tant que Micro-WAF au plus proche de l'application
- Protection des applications cloud native
- Permet aux équipes DevOps de produire du code sécurisé
- Sécurité intégrée au pipeline CI/CD
- Apporte la visibilité sur la sécurité de vos services numériques

THE BRIGHT SIDE OF CYBERSECURITY

- **Contrôle**
  Gardez la maîtrise des clés d'accès à vos données sensibles
- **Haute sécurité**
  Automatisez la sécurité de vos API, services critiques et Web
- **Facilité**
  Déployez rapidement une sécurité adaptée à vos enjeux numériques
- **Confiance**
  Appuyez-vous sur un expert européen certifié



Dirigeant
Stéphane de SAINT ALBIN
Vice-président, Application & Cloud Security
Président, Rohde & Schwarz Cybersecurity SAS

Contacts

Gilles d'ARPA
VP Sales Application & Cloud Security
gilles.darpa@rohde-schwarz.com

Manuela JOULAGEIX
Head of Marketing SEMEA
manuela.joulageix@rohde-schwarz.com

Gérez simplement vos comptes à privilèges - PAM

Société : RUBYCAT
Adresse : Digital Square
1137A avenue des Champs-Blancs
35510 Cesson-Sévigné
Tél. : 02 99 30 21 11
Mail : **sales@rubycat-labs.com**
Site web : **www.rubycat.eu**

Nom des marques :
PROVE IT
PROVE IT ADVANCED
PROVE IT CLUSTER

Retrouvez nos webinaires sur :
www.rubycat.eu/webinaires

Spécialisations

- **Contrôle et traçabilité des accès sensibles au SI**
- **Gestion des comptes à privilèges (PAM)**

Dirigeante
Cathy LESAGE
Dirigeante – CEO

Contact
Thomas CRIBIER
Ingénieur avant-vente
thomas.cribier@rubycat.eu

Basé à Rennes, Rubycat est un éditeur français de logiciels, spécialisé dans la traçabilité et le contrôle des accès sensibles au système d'information. Fort d'une expertise reconnue dans le domaine de la sécurité des accès au SI, Rubycat apporte avec PROVE IT une réponse pragmatique et simple au manque de visibilité sur les actions réalisées par les comptes à privilèges.

Solutions

PROVE IT : la solution de PAM qui sécurise vos accès sensibles

Solution logicielle française certifiée par l'ANSSI, PROVE IT s'intègre facilement dans votre environnement pour fédérer les accès sensibles au SI (Sans agent - installation en moins d'une heure).

Elle contrôle et trace les accès tiers et utilisateurs à privilèges aux ressources critiques, avec enregistrement et visualisation des sessions.

PROVE IT intègre un coffre-fort sécurisé d'identifiants secondaires (non-divulgation des identifiants des ressources critiques).

Interfaçage natif avec les solutions de gestion d'événements (SIEM) et d'authentification forte (MFA).

PROVE IT ADVANCED : pour aller plus loin dans la sécurisation de votre SI

La gamme de PROVE IT s'est élargie avec PROVE IT Advanced et Cluster et offre de nouvelles fonctionnalités :

- la segmentation des droits d'administration par profil – auditeurs / opérateurs / administrateurs – à périmètre variable
- l'API Rest qui facilite les opérations d'administration les plus courantes
- Résilience / répartition de charge

Références clients

- Ministères (DGFIP…)
- Mairie de Vincennes
- CHU de Nîmes
- Proginov
- Semitan
- SHV Energy SRM
- Limagrain
- NEOVIVO
- Port Boulogne-Calais

Certifications

PROVE IT est une solution certifiée Visa de sécurité – CSPN par l'ANSSI.

PROVE IT éligible dans le cadre du Plan France Relance

La gestion des accès à privilèges (PAM) est un maillon essentiel dans la gouvernance du SI, elle fait partie des dix différentes ***solutions identifiées par l'ANSSI*** *comme pouvant faire l'objet d'un projet d'acquisition dans le cadre du* ***Plan France Relance.***

Pour rappel, l'objectif du volet cybersécurité de France Relance piloté par l'ANSSI est de ***renforcer la sécurité*** *de l'État, des administrations, des collectivités territoriales, des établissements de santé et des organismes au service des citoyens (social, santé, formation, audiovisuel, sécurité), tout en dynamisant l'écosystème industriel français.*

Notre solution PROVE IT est éligible dans le cadre d'un appel à projets de France Relance. Si vous faites partie d'un organisme éligible, ***n'hésitez pas à nous contacter*** *pour échanger ensemble sur votre projet. Un apport minimal de 30 % sera attendu de la part du bénéficiaire. Le montant du cofinancement de l'ANSSI sera défini suivant la maturité du projet et les objectifs du plan de relance. Plus d'informations disponibles sur le site de l'ANSSI.*

PROVEIT by rubycat

Le **groupe Limagrain** a choisi **PROVEIT**

Hervé LAUTARD, Directeur Infrastructures et Opérations, revient sur la mise en place de **PROVEIT** **pour gérer ses accès à privilèges.**

Limagrain de la terre à la vie

Limagrain *est un groupe coopératif agricole français spécialisé dans les semences de grandes cultures, les semences potagères et les produits céréaliers et comprend des marques connues telles que Vilmorin & Cie, Jacquet, Brossard,...*

Le **contexte métier** du groupe

Enjeux dans le domaine de l'industrie agroalimentaire :

- Pour garantir le fonctionnement et la continuité des process de production, il est essentiel d'assurer l'intégrité et la disponibilité de son SI.
- Pour offrir le respect du secret industriel, l'établissement doit s'assurer de la confidentialité de la chaîne d'information et se prémunir de toute fuite de données, et empêcher les accès non maîtrisés au SI.
- Pour assurer la sûreté de fonctionnement, l'entreprise doit respecter les contraintes métiers et réglementations via notamment un contrôle rigoureux des actions opérées sur le SI.

Le **besoin**

Compte tenu de notre activité, nous utilisons principalement des ERP et applicatifs métiers sur l'ensemble de nos sites. Certaines alertes remontées sur le SI nécessitent une intervention rapide et sécurisée **7 jours sur 7 et 24h sur 24**.

Lorsque la **gestion globale de notre maintenance** a été confiée à un prestataire, la mise en place d'une solution de PAM/bastion s'est avérée nécessaire.

Nous recherchions donc une solution facile à mettre en œuvre qui nous permettrait de **sécuriser les accès externes à notre SI** et d'**auditer simplement les actions effectuées lors des interventions**.

> *« Nous souhaitions une solution qui ne nécessite pas une équipe dédiée pour sa mise en œuvre.*
>
> *Notre équipe s'est approprié rapidement et facilement l'administration de **PROVE IT**. »*

Solution mise en œuvre

PROVEIT by rubycat

Le bastion d'administration **PROVE IT** de **Rubycat** se positionne directement sur le SI. Il vient fédérer l'ensemble des connexions internes et externes au SI que ce soit sur les réseaux bureautiques ou industriels.

Son approche non invasive permet de le déployer rapidement et simplement dans des environnements hétérogènes.

La solution **PROVE IT** s'est révélée idéale pour nous. En effet, elle a pu répondre parfaitement aux trois critères que nous nous étions fixés :

- **Attentes techniques :** les fonctionnalités de PROVE IT permettent de fédérer l'ensemble des accès des prestataires externes, de sécuriser leur connexion, mais également d'auditer facilement une intervention en revisionnant l'enregistrement vidéo de celle-ci.
- **Simplicité de mise en place, d'utilisation et d'administration :** PROVE IT ne nécessite pas une équipe dédiée pour son administration et à sa mise en œuvre. Ici n'importe qui peut prendre en main rapidement et facilement l'administration de PROVE IT.
- **Budget limité :** Enfin nous avions un budget limité, et nous ne pouvions pas envisager des solutions plus complexes et souvent très coûteuses à mettre en œuvre dans une organisation comme la nôtre

Hervé LAUTARD
Directeur Infrastructures et Opérations chez LIMAGRAIN
10/05/2021

SANS | GIAC CERTIFICATIONS

Société : SANS INSTITUTE
Adresse : 11200 Rockville Pike, Suite 200
North Bethesda, MD 20852, USA
Tél. : +44 203 384 3470
Mail : **emea@sans.org**
Site web : **www.sans.org**

Spécialisations : formations dans le domaine de la cybersécurité

Cyberdéfense, Inforensique, réponses aux incidents, management, tests d'intrusion, systèmes de contrôle industriel (SCI), fondamentaux de la sécurité, sécurité du Cloud et audit.

Chiffre clé

Effectifs : 500

Contact
Axelle SAIM
Business Development Director France & Luxembourg
asaim@sans.org
+ 33 (0)7 67 82 75 52

SANS Institute est la référence mondiale en matière de formation depuis plus de 30 ans dans le domaine de la cybersécurité.

Notre mission fondamentale consiste à partager les connaissances et compétences de pointe en matière de cybersécurité des entreprises, institutions militaires et gouvernementales pour une protection optimale des personnes et des biens.

Une formation de pointe
Les formations SANS préparent les stagiaires à faire face aux menaces d'aujourd'hui et à relever les défis de demain. Pour ce faire, nos cours et nos supports pédagogiques sont constamment mis à jour afin d'enseigner les dernières techniques et outils qui assurent la sécurité des réseaux et des données. Conçues pour être pratiques, nos formations immergent les stagiaires en laboratoire, pour qu'ils appliquent leurs nouvelles connaissances et affinent leurs compétences. Les stagiaires seront en mesure de mettre en œuvre leurs nouvelles compétences dès leur retour au bureau. C'est la promesse SANS.

Une force humaine
Enseignants hors normes de par leur compétences, les formateurs SANS sont actifs auprès de nombreuses organisations influentes ; passionnés, ils animent nos formations avec dynamisme et efficacité.

La communauté mondiale
SANS Institute est un membre éminent de la communauté mondiale de la cybersécurité. Nous exploitons l'Internet Storm Centre – un système d'alerte précoce pour Internet. SANS développe, met à jour et publie gratuitement une vaste collection de documents de recherche sur de nombreux aspects de la sécurité de l'information.

Services

Formation ciblée
Nous proposons plus de 70 cours SANS spécifiques, qui s'alignent sur les rôles, responsabilités et disciplines majeurs des équipes de sécurité. Cyberdéfense, inforensique, réponses aux incidents, management, tests d'intrusion, développeur, systèmes de contrôle industriel (SCI) et audit. Chaque programme offre une progression de cours qui conduit les professionnels des bases fondamentales du sujet jusqu'aux spécialisations de haut niveau.

SANS propose ses formations en présentiel, OnDemand (en ligne à votre rythme), Live Online (live streaming) ou en intra-entreprise.

Security Awareness Training
Formations de sensibilisation à la sécurité, qui se présentent sous forme de vidéos interactives, préparant vos salariés à reconnaître et à réagir correctement aux cybermenaces prédominantes d'aujourd'hui.

Cyber Academy
SANS Cyber Academy identifie des candidats à fort potentiel pour les former de façon intensive à la certification GIAC, avant de les affecter à des postes clés.

Cyber Start
Une suite de défis, d'outils et de jeux conçus pour initier les enfants et les jeunes adultes au domaine de la cybersécurité.

NetWars
Une série de défis pratiques conçus pour tester les compétences et l'expérience des participants : Core NetWars (fondamentaux de la sécurité) et DFIR Netwars (l'inforensique et la gestion d'incidents).

Certifications

De nombreux cours SANS s'alignent sur les examens GIAC *(Global Information Assurance Certification)*. GIAC valide les compétences des professionnels de la sécurité des informations, attestant que les personnes certifiées possèdent les compétences et connaissances techniques nécessaires. Plusieurs certifications GIAC sont accréditées ANSI / ISO / IEC 17024.

- Un ciblage spécialisé, adapté à un poste particulier
- Des connaissances approfondies du monde réel
- La certification dont le concept est réputé être le plus fiable

GIAC CERTIFICATIONS

SANS

CLOUD SECURITY

SANS believes that the cloud is a transformative technology that will define the technology landscape for many years to come. Given the unmitigated growth of Cloud, we have launched the Cloud Security Curriculum to give you the training and skills you need to become a cloud security expert. Our curriculum provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and applications in the cloud against the most dangerous threats.

LONG COURSES

SEC488: Cloud Security Essentials
Learning the language of Cloud Security.

SEC510: Public Cloud Security: AWS, Azure, and GCP
Multiple clouds require multiple solutions.

SEC522: Defending Web Applications Security Essentials
Not a matter of "if" but "when". Be prepared for a web app attach. we'll teach you how.

SEC540: Cloud Security & DevOps Automation
The cloud moves fast. Automate to keep up.

SEC557: Continuous Automation for Enterprise and Cloud Compliance

SEC588: Cloud Penetration Testing
Aim your arrows to the sky and penetrate the Cloud.

SEC584: Cloud Native Security: Defending Containers and Kubernetes
Deliver securely at the speed of cloud native.

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud
Stop treating the symptoms. Cure the disease.

FOR509: Enterprise Cloud Forensics and Incident Response

SHORT COURSES

SEC534: Secure DevOps: A Practical Introduction
Principles! Practices! Tools! Oh My! Start your journey on the DevSecOps road here.

SEC541: Cloud Security Monitoring and Threat Hunting
Attackers Can Run But Not Hide. Our Radar Sees All Threats.

MGT520: Leading Cloud Security Design & Implementation
Building and leading a cloud security program.

NEW GIAC Cloud Security Certifications

Recently released GIAC Cloud Security Essentials (GCLD) affiliated with SEC488 and GIAC Public Cloud Security (GPCS) affiliated with SEC510

To find out more about Cloud Security Courses, visit sans.org/cloud-security-courses

SANS | GIAC CERTIFICATIONS

SCASSI. cybersecurity GROUP

Toulouse
Paris
Madrid
Valencia

Notre job :
Sécuriser les systèmes critiques et embarqués

Spécialisations : **cybersécurité des systèmes critiques et SI métiers, e-learning cybersécurité, sensibilisation, faux-phishing, logiciels d'audit, pentest et IoT cybersécurité**

Chiffres clés : *CA :* 5 M€ (2020) - *Effectifs :* 50 collaborateurs

SCASSI. be secure

EXPERTISE

GOUVERNANCE ET CONFORMITÉ

- Analyse de risques de système de communication du trafic aérien
- Mise en conformité LPM, I SO 27001, HDS, RGPD (ESN, Datacenter), SSI (industriels)
- Accompagnement à la conception d'architecture logicielle sécurisée

ARCHITECTURE ET INFRASTRUCTURE SI

- AMOA/AMOE Cyber de systèmes critiques
- Sécurité opérationnelle des SI
- Intégration logiciels et composants SSI experts

ÉVALUATION TECHNIQUE

- Pentest
- Audit technique, mobiles, IOT
- COTS assessment sur composants avioniques, spatiaux et défenses

VISA DE SÉCURITÉ

CENTRE D'EXPERTISES

AÉRO & CONTRÔLE AÉRIEN
DÉFENSE ET SPATIAL
AUTOMOTIVE
IOT INDUSTRIEL
FORENSIC
SANTÉ ET SECTEUR PUBLIC

phosforea

SENSIBILISATION

E-LEARNING - CYBERSÉCURITÉ

- Catalogue de +50 contenus dans 8 langues
- Contenus sur étagère ou à façon avec accompagnement chefferie de projet
- 12 000 heures de formation dispensées en 2020

SIMULATION DE PHISHING

- Déploiement de campagnes e-mail
- Base de +50 modèles d'e-mails frauduleux
- Statistiques avancées de campagnes

PRODUITS

- Learning Management System
- Plate-forme de Faux Phishing
- Mobile Learning

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

FORMATION

ISO 27001
ISO 27005
EBIOS
CEH
CRITÈRES COMMUNS
SÉCURITÉ DÉVELOPPEMENTS

june cybersec factory

AUDITOOL

LOGICIEL D'AUDIT POUR PILOTER SIMPLEMENT LA CONFORMITÉ SSI D'UNE ORGANISATION.

Organiser et réaliser ses audits techniques, organisationnels et métiers dans un environnement sécurisé.

Le seul logiciel français de pilotage d'audit avec chiffrement des données. En local ou sur un Cloud national, vos travaux d'audits sont en sécurité.

LABEL SMART & SECURE IOT
Digital113

MIOT

IOT cybersécurisé pour un pilotage des engins de chantier en confiance

L'offre MIOT est composée d'un device et d'une plate-forme de visualisation des données.

Références clients : Airbus Defence & Space, ESSP, CNES, Thales Alenia Space, Airbus, Rockwell Collins, DGAC DSNA, GCB, MAAF, La banque Postale, Groupe BPCE, Groupama, Generali, Continental, Renault, Actia, Saint Gobain, Naval Group, Michelin, Hôpitaux de Toulouse, EFS, Groupe Rocher, GIFI

Laurent PELUD
Fondateur groupe

Pierre NICOLAS
DG SCASSI FR

Jesus FRIGINAL
DG SCASSI ES

Laëticia MAYNARD
DG PHOSFOREA

Auditool.

Standardiser la production d'audit SSI est un levier de croissance.

Organisez, réalisez et restituez tous vos audits sans perdre de temps :

- Génération automatisée de rapport d'audit
- Référentiels intégrés de normes techniques et organisationnelles
- Mode pentest
- Mode collaboratif / déconnecté
- Statistiques avancées de mission

Mode saaS ou on premise.

Données hébergées sur cloud français.

Logiciel cybersécurisé.

June factory est une filiale de Scassi Group
En savoir plus : **www.june-factory.com**
contact@june-factory.com
05 61 17 08 54

june | cybersec factory

SERMA SAFETY & SECURITY

Société : SERMA SAFETY & SECURITY
Adresse : 14, rue Galilée
CS10071 33608 PESSAC
Tél. : 05 57 26 08 88
Mail : **contact-s3@serma.com**
Site Web : **www.serma-safety-security.com**

Spécialisations

Audit, intégration de solutions de sécurité (détection des menaces, visibilité - automatisation – orchestration infra & cloud, protection des données, sécurité de l'infrastructure – Firewall-NAC, protection des identités et accès, sécurité de l'application-gestion des vulnérabilités, réseau et virtualisation), SOC, infogérance de solutions de sécurité, laboratoire de sécurité, CESTI, sûreté de fonctionnement.

Chiffres clés

CA : +21 M€
Effectifs : +200 ingénieurs
Historique : +20 ans d'expérience
150 clients actifs industrie et service providers (dont 30 comptes du CAC 40)

Dirigeants

Xavier MORIN
Directeur général

Nathalie MONEY
Directrice commerciale
n.money@serma.com

Michel DUFRESNE
Responsable BU Sûreté de fonctionnement
m.dufresne@serma.com

Lionel AGULHON
Responsable BU Laboratoire de sécurité
l.agulhon@serma.com

Xavier MORIN, *Directeur général*
«SERMA Safety and Security est aujourd'hui représenté par près de 200 experts des métiers de la sécurité.
SERMA Safety and Security est ainsi un des rares acteurs capables d'adresser les problématiques sécuritaires sur les systèmes d'information, industriels, embarqués et IoT.»

SERMA Safety and Security est un interlocuteur unique pour la sécurité et la sûreté de fonctionnement des produits et systèmes IoT, embarqués, industriels ou d'information. L'expertise développée depuis plus de 20 ans lui permet d'intervenir sur toute la chaîne de valeur des systèmes : depuis la conception jusqu'au maintien en conditions opérationnelles/supervision des équipements.

• **Expertise et conseil en cybersécurité**
Les consultants de SERMA Safety and Security spécialisés en cybersécurité accompagnent les concepteurs, intégrateurs et utilisateurs de systèmes dans la maîtrise de la sécurité de leurs produits, tant dans leur fonctionnement que dans leur sécurisation au regard des risques de malveillance et d'intrusion. Le panel d'offres de services couvre l'ensemble des besoins en sécurité : audit, conseil, GRC, services managés, SOC et intégration de solutions.

• **Expertise et conseil en sûreté de fonctionnement**
Les études menées par nos experts portent sur des systèmes ou des logiciels ayant des contraintes de sûreté de fonctionnement. SERMA Safety and Security propose son expertise aux industriels, donneurs d'ordres et autorités de certification qui doivent élaborer, valider, homologuer ou certifier leurs systèmes et logiciels.
Ce processus d'étude de sûreté de fonctionnement est axé autour de quatre points principaux : fiabilité, disponibilité, maintenabilité et sécurité.

• **Laboratoire d'évaluation sécuritaire**
Le laboratoire d'évaluation sécuritaire évalue annuellement plus de 200 produits sécuritaires complexes, allant de la puce électronique au système hardware/software complet. Il dispose de nombreuses accréditations (critères communs, EMVCo, GlobalPlatform, PCI, FIPS…) qui lui permettent de réaliser des évaluations selon différentes normes internationales, publiques ou privées. Le laboratoire est agréé CESTI (Centre d'évaluation de la sécurité des technologies de l'information) par l'Anssi.

Parallèlement à ces diverses activités, la société propose des formations couvrant les phases de sensibilisation, d'utilisation opérationnelle, de test, de design, d'exigence de sécurité, de sûreté et de conception.
Présente sur cinq sites en France, la société compte près de deux cents collaborateurs et réalise un chiffre d'affaires de plus de 21 millions d'euros. Elle est une filiale du Groupe SERMA.

Offres

CONSEIL
- Études prospectives et cadrage
- Schémas directeurs, conformités, PSSI, PCA/PRA
- Analyses de risques et audit de maturité
- Architecture sécurisée
- Accompagnement sûreté de fonctionnement
- Préparation à la certification
- Conseil en design sécurisé

EXPERTISE
- Identification des cibles de sécurité
- Intégration de solutions de sécurité
- Étude de sûreté de fonctionnement
- Analyse de modules cryptographiques
- Infogérance des équipements de sécurité
- Reverse engineering
- Formations et sensibilisation

ÉVALUATION ET CONTRÔLE
- Audits : tests intrusion, audits archi/conf/ code, PASSI, Redteam
- Détection des alertes de sécurité (SOC)
- Audit du code logiciel (qualité/sécurité/sûreté)
- Audit et évaluation sûreté de fonctionnement
- Évaluations sécuritaires (nombreux schémas publics et privés)
- Outils de test IoT (Hardsploit)

Certifications

Qualifié PASSI RGS (audit de configuration – Audit d'architecture – Audit de code source – Audit d'intrusion) depuis 2017 – Accrédité CESTI Critères communs et CSPN depuis 1998

SIEMENS
Ingenuity for life*

Société : SIEMENS SAS
Adresse : 40, avenue des Fruitiers
93210 Saint-Denis (France)
Tél. : +33 1 85 57 00 00
Site web :
https://new.siemens.com/fr/fr/entreprise/thematiques/la-cybersecurite-chez-siemens.html

Spécialisations

Grâce à son approche holistique, Siemens est le partenaire de référence et de confiance pour répondre aux enjeux de la digitalisation et de la cybersécurité des systèmes industriels. En effet, Siemens est le premier équipementier – le seul à ce jour – à avoir obtenu en France la qualification de l'Anssi pour une gamme complète d'automates programmables (Simatic S7-1500).
Par ailleurs, Siemens accompagne la sécurisation des installations au travers d'un large portfolio de services : cartographie, conseil (IEC 62443, analyse de risques, référentiels Anssi…), durcissement des configurations, cloisonnement des réseaux, automates industriels sécurisés, switch industriels sécurisés, accompagnement à l'homologation et maintien en condition de sécurité.

Contact :
Fabien MIQUET
PSSO Siemens Digital Industries France
fabien.miquet@siemens.com

Depuis plus de 170 ans en France, le nom de Siemens est synonyme de performance technique, d'innovation, de qualité et de fiabilité. Siemens opère dans les domaines de l'électrification, de l'automatisation et de la digitalisation et compte parmi les principaux fournisseurs de technologies à haute efficacité énergétique, qui contribuent à préserver les ressources naturelles. L'entreprise est pionnière en matière d'équipements d'automatisme, de systèmes d'entraînement et de solutions logicielles destinées à l'industrie. Avec plus de 7 000 collaborateurs, 8 sites industriels et 11 centres de R&D, dont huit à responsabilité mondiale, Siemens France s'engage activement dans les filières stratégiques pour l'industrie française. Depuis 2017, Siemens est le seul équipementier dont les process de développement sont certifiés sur la base de la norme internationale IEC 62443-4-1 par le TÜV Sud, et également le seul à offrir des automates programmables industriels qualifiés par l'Anssi.

Excellence par ailleurs renouvelée :

- avec le maintien en qualification obtenue en 2019 pour la gamme des automates S7-1500 ;
- avec la qualification Anssi de trois nouvelles références (CPU 1500 redondantes) décrochées en octobre 2020 ;
- avec la labellisation SecNumEdu de sa formation Cybersécurité des systèmes industriels (SITRAIN DI-CYBER) ;
- avec notre SCADA WinCC Open Architecture (WinCC OA) doublement certifié, autant côté process de développement que côté produit.

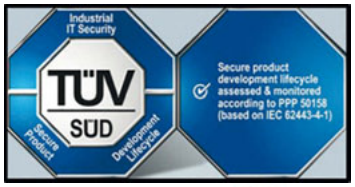
L'ensemble de ces distinctions montre combien le sujet cybersécurité est un enjeu stratégique pour le groupe. Associant la parole aux actes, Siemens est l'initiateur de la *Charter of Trust* pour promouvoir le sujet cybersécurité au plus haut niveau au sein des entreprises.

Suivez-nous sur Twitter
@Siemens_France

Offre

Gamme complète d'automates industriels sécurisés, switch industriels sécurisés, surveillance de la sécurité des systèmes industriels.

Certifications



Gamme complète d'automates industriels S7 1500 qualifiée.

Switch industriel SCALANCE XM400, certifié.

Services

Un ensemble de services pour un accompagnement personnalisé :

- Diagnostic (cartographie, analyse de risques, évaluation de la maturité…)
- Conseil (gouvernance, formation…)
- Déploiement (cloisonnement réseau, durcissement des configurations…)
- Contrôle, validation, conformité (préparation à l'homologation, audit de conformité…)
- Maintien en condition de sécurité (mise à jour, gestion des vulnérabilités…)

« La certification TÜV SÜD IEC62443-4-1 de nos sites de développement, associée à la certification Anssi, permet à Siemens d'atteindre le niveau le plus exigeant préconisé par l'ICCF Framework issu du groupe de travail de la Commission Européenne JRC dans le cadre de ses propositions pour une certification européenne des produits pour les systèmes industriels. Nous nous félicitons de cette nouvelle avancée. »

Vincent JAUNEAU, directeur Digital Industries chez Siemens France. ℗ photo Vincent Jauneau

SOLUTIONS
SERVICES
CONSEIL
INDUSTRIE

* L'ingéniosité au service de la vie

SONICWALL®

Société : SONICWALL
Adresse : 17 rue du Colisée
75008 PARIS
Tél. : +33 (0)800 91 55 61
Site web : **www.sonicwall.com**
Mail contact : **france@sonicwall.com**

Spécialisations

Firewalls (physiques ou virtuels), Switch, bornes Wifi, administration centralisée, protection avancée des terminaux (End Point), protection avancée de la messagerie, sécurisation des applications et des accès distants (VPN-SSL), sécurisation du Cloud, Sandboxing ATP, sécurités Zero-Trust et Least-Privilege.

Chiffres clés

Effectifs : 1 600

Contact IdF et Est
Bertrand GARS
Tél. : +33 6 14 49 32 06
bgars@sonicwall.com

Contact Ouest et DOM-TOM
Sylvain STAHL
Tél. : +33 7 84 43 58 70
sstahl@sonicwall.com

Avec trente, années d'expertise, SonicWall est reconnu comme un leader mondial de la sécurité des réseaux dans la course au Cyber Armement. Grâce à la plateforme Capture Labs, nos solutions bénéficient d'une forte performance pour la détection & la prévention des menaces. Chaque jour, nos équipements permettent de bloquer plus de 30 millions d'attaques.

Offres

NGFW Série TZ – TPE/PME : des firewalls permettant de sécuriser efficacement les réseaux, plateforme SD-WAN, avec la possibilité d'avoir une analyse approfondie via un Sandboxing dans le Cloud.

NGFW Série NSa – Entreprise : efficacité et performance de sécurité pour les entreprises ou sites de taille moyenne.

NGFW Série NSsp – Datacenter et MSSP : des firewalls conçus pour les grandes entreprises multi-sites, les datacenters et les fournisseurs de services managés (MSSP), offrant une protection haute vitesse, une densité de ports élevée et un débit d'inspection allant jusqu'à 100 Gbit/s

NGFW Série NSv : des firewalls virtuels permettant de sécuriser des réseaux, des datacenters ou des applications hébergées dans les Clouds publics ou privés (Aws, Azure…).

Secure Switch : une gamme de switchs manageables dans le Cloud ou directement via un pare-feu SonicWall.

SonicWave : sécurité et performances intégrées pour offrir une connectivité sans fil au sein des entreprises. Les AP peuvent être gérés via le Cloud (WNM) ou le pare-feu.

Capture Client : sécuriser les terminaux avec un anti-virus comportemental permettant un retour en arrière (rollback), Une diffusion simplifiée des certificats SSL, une détection des vulnérabilités et une analyse Sandboxing dans le Cloud.

E-mail Security : filtrer efficacement les e-mails via des appliances physiques ou virtuelles, ou dans le Cloud (compatible Office365), avec la possibilité d'avoir une analyse Sandboxing dans le Cloud des pièces jointes aux mails.

Cloud App Security : sécurisation d'App Cloud, d'Office 365, G-Suite via un déploiement en 5 mn grâce aux API. Sécurité et détection de malveillances au niveau de la messagerie, des fichiers partagés, des connexions, des drives…

Secure Mobile Access : pour une sécurisation centralisée des applications (situées dans l'entreprise ou dans le Cloud) pour des utilisateurs (locaux ou distants), via une double authentification et une vérification de l'intégrité du poste. en appliance physique ou virtuelle.

NSM et Analytics : des consoles pour superviser et manager les différents produits, et bénéficier d'un reporting complet et centralisé. Solution dans le Cloud ou via une appliance virtuelle.

Cloud Edge Zero Access : une application SaaS puissante qui fournit un *Network-as-a-Service* simple pour une connectivité de site à site et hybride vers AWS, Azure et Google Cloud. Elle combine des approches de sécurité Zero-Trust et Least-Privilege

Certifications

- Critères Communs EAL4+
- Programme partenaire noté 5* par CRN Partner Program Guide (2021)
- Score de 100 % au test ICSA Labs (2021)
- Note de 4.6/5 Gartner Peer Insights (2021)

SOPHOS

Un écosystème de Cybersécurité adaptatif

Sophos ACE s'appuie sur l'automatisation et les analystes, ainsi que sur la contribution collective des produits, partenaires, clients et développeurs Sophos pour créer une protection qui s'améliore en permanence.

C'est un système étendu conçu pour optimiser la prévention, la détection et la réponse. Il protège la nouvelle réalité des systèmes d'entreprise interconnectés et se défend contre le paysage changeant des cyberattaques qui combine désormais l'automatisation et le piratage humain en direct.

Siège social de Sophos à Abingdon (Oxfordshire), Royaume-Uni

Société : SOPHOS
Adresse : 80, quai Voltaire
95870 Bezons
Tél. : 01 34 34 80 00
Site web: **www.sophos.fr**
Mail contact: **sales@sophos.fr**

Spécialisations

Protection Endpoint NextGen (Postes, Serveurs, Mobiles, Données, Cloud)

Protection réseaux NextGen (Firewall, E-mail, Web, WAF, WiFi, UTM)

Chiffres clés

CA 2021 : $ 938,4 M
Effectifs : 3 700 employés

Emmanuel GOSSELIN
Responsable des Ventes
emmanuel.gosselin@sophos.fr

Un leader mondial de la Cybersécurité

Sophos protège plus de 500 000 entreprises et des millions d'utilisateurs dans plus de 150 pays, contre les cybermenaces actuelles les plus avancées. Alimenté par les renseignements sur les menaces, l'IA et l'apprentissage automatique des SophosLabs et SophosAI, Sophos propose un large portefeuille de produits et services innovants afin de garantir la sécurité des utilisateurs, des réseaux et des terminaux contre les ransomwares, les malwares, les exploits, le phishing et de nombreuses autres cyberattaques toujours plus sophistiquées.

Sophos Portofolio

Bénéficiant d'une administration centralisée, cohérente et intégrée à travers la console Sophos Central, les solutions de protection Sophos associent des technologies éprouvées avec des innovations issues des toutes dernières avancées de protection NextGen.

Sophos Extended Detection and Response (XDR) vous permet de détecter et d'enquêter sur les points d'extrémité, les serveurs, les pare-feu et d'autres sources de données, le tout étayé par le Data Lake de Sophos. Vous obtenez une vue exhaustive de la posture de cybersécurité dans votre organisation avec la possibilité d'explorer les détails granulaires si nécessaire.

Sophos XGS Firewall

La nouvelle série de pare-feu XGS offre des performances inégalées et fournit une protection avancée contre les cybermenaces. Les nouveaux dispositifs matériels sont dotés des meilleures fonctionnalités d'inspection de la couche de transport sécurisée (ie : TLS : Transport Layer Security) du marché, intégrant un support natif du protocole TLS version 1.3. Ces modèles sont jusqu'à cinq fois plus rapides que ceux actuellement disponibles sur le marché.

Sophos Managed Threat Response

Sophos est l'un des plus importants fournisseurs de détection, avec plus de 5000 clients actifs. Avec Sophos MTR, votre organisation est soutenue par une équipe d'élite de chasseurs de menaces et d'experts qui vous apportent une remédiation en plus de la détection face aux menaces les plus sophistiquées.

Sophos MSP Connect

Le programme MSP Connect de Sophos permet à tout partenaire de proposer depuis une seule et même console une facturation mensuelle et sans engagement. L'offre MSP de Sophos s'intègre parfaitement au budget OPEX des entreprises.

STORMSHIELD

La cybersécurité européenne de confiance

Société : STORMSHIELD

Noms des solutions :
Stormshield Network Security
Stormshield Endpoint Security
Stormshield Data Security

Adresse : 22, rue du Gouverneur-général-Éboué
92130 Issy-les-Moulineaux
Tél. : + 33 (0)9 69 32 96 29

Site Web : **www.stormshield.com**
Mail contact : **commercial@stormshield.eu**

Spécialisations

Firewall, UTM, IPS, VPN
Device control, APT Detection protection réseau, Cloud, Endpoint, EPP, EDR, infrastructures virtualisées, chiffrement de données, accès distant sécurisé, sécurité OT

Chiffres clés

CA : non communiqué
Effectifs : plus de 400 collaborateurs

Dirigeant
Pierre-Yves HENTZEN
Président

Contacts
Eric HOHBAUER
Directeur des Ventes - Directeur général délégué
eric.hohbauer@stormshield.eu

Alain DUPONT
Directeur des Services Clients
Directeur général délégué
Alain.dupont@stormshield.eu

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Nos technologies répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités.

Notre mission : cyber-séréniser nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations.

Une protection innovante de bout en bout

Stormshield, premier éditeur français pure-player en cybersécurité, associe trois grandes expertises pour protéger durablement les entreprises et les organisations contre les menaces les plus avancées :

- Protection des infrastructures informatiques et industrielles ;
- Protection des postes de travail, des serveurs et des terminaux ;
- Protection des données (on-premise, Cloud et mobilité).

Certifications

Les technologies Stormshield sont certifiées au plus haut niveau européen pour garantir une protection optimale (UE - OTAN Restreint - Visas ANSSI - EAL3+/ EAL4+ - Producto CCN Aprobado - Producto CCN Cualificado).

Stormshield s'est engagé dans un process de qualification continue de ses produits Stormshield Network Security, au niveau Standard de l'Anssi, et est le seul éditeur de pare-feux à obtenir à la fois les qualifications espagnoles « Producto CCN Aprobado » et « Producto CCN Cualificado ».

« La notion de confiance n'est pas un vain mot en cybersécurité. C'est un critère de choix, au même titre que la richesse fonctionnelle, les performances ou le prix.

En effet, un environnement informatique est à risque dès lorsque ses systèmes de protection ne présentent pas eux-mêmes des garanties de sécurité et de robustesse et donc ne sont pas de confiance. Les solutions de cybersécurité sont positionnées à des endroits stratégiques et ont souvent des droits élevés. Toute faiblesse de ces solutions, introduite volontairement ou non, offre un point d'accès direct aux ressources protégées. Le contexte de cyberguerre latent accentue bien évidemment la criticité de cet enjeu.

S'appuyer sur des technologies européennes de confiance permet aux entreprises et organisations de l'UE de garder la maîtrise de leur protection. Les qualifications délivrées par l'Anssi vont dans ce sens. Elles attestent de la robustesse des produits face aux attaques mais aussi de la confiance qu'à l'État envers l'éditeur, par une analyse de code source et un audit de l'environnement de développement.

Et si une technologie extra-européenne apporte une couverture fonctionnelle plus adaptée, appliquer le principe de double-barrière étatique permet de concilier confiance et usage. »

Pierre-Yves HENTZEN - *Président*

Société : SYNETIS
Adresse : 19 rue du Général-Foy
75008 PARIS
Tél. : +33 01 47 64 48 66
Mail : **contact@synetis.com**
Site web : **www.synetis.com**

Spécialisations

Fondée en 2010, Synetis est un cabinet de conseil indépendant, devenu le partenaire de référence pour les entreprises désireuses de sécuriser leurs actifs.

Chiffres clés 2020

CA : 21,5 M€
Effectifs : 160

Dirigeants
Éric DEROUET
Cofondateur & Président
eric.derouet@synetis.com

Rémi FOURNIER
Cofondateur & Directeur général
Remi.fournier@synetis.com

Contact :
Michael LECLERCQ
Responsable marketing et communication
michael.leclercq@synetis.com

Prévenir les menaces et renforcer sa cyber résilience

À l'heure où les organisations poursuivent leurs stratégies de transformation numérique, la sécurité doit être une priorité pour tous. SYNETIS vous accompagne dans tous vos projets de sécurisation et vous aide à faire face aux nouveaux enjeux de la cybersécurité.

Les offres et périmètres d'expertise

L'offre globale de SYNETIS est conçue pour répondre efficacement aux besoins de ses clients, grâce à de larges compétences technologiques et de nombreuses expertises qui lui permettent de proposer une grande variété de solutions :

- **Le Conseil SSI :** permet aux clients de faire face aux règlementations ou aux nouvelles menaces et d'en assurer la gouvernance.
- **L'identité numérique :** facilite la confiance que l'on peut avoir dans la mise à disposition de services digitaux.
- **L'audit SSI :** identifie les menaces Cyber pesant sur une organisation.
- **La sécurité opérationnelle :** propose des actions concrètes de protection des données et des infrastructures.
- **Le C-SIRT (labellisé Expert Cyber)** pour prévenir (à travers une veille et de la Threat Intelligence) et réagir (réponse à incident, investigation numérique)
- **La formation et la sensibilisation** qui participent toutes les deux à la bonne application de la SSI.
- **Services managés de sécurité :** pour des services de sécurité externalisés clés en main (identité numérique, gestion de vulnérabilités, surveillance, etc.)

Antoine COUTANT

Practice Manager Audits SSI et CSIRT

« Se préparer pour mieux réagir à une cyberattaque ! »

« Aujourd'hui, il est important de comprendre que la sécurité des SI est avant tout un moyen de protéger son outil de travail. Le risque d'intrusion informatique est réel, même pour les SI les plus sécurisés, et les incidents de sécurité sont quotidiens pour la plupart des organisations.

Nos interventions CSIRT augmentent exponentiellement surtout depuis le début de la crise sanitaire. En 2020, les cyber-attaquants ont amélioré leurs capacités à s'adapter et à cibler plus efficacement leurs victimes. Il est donc primordial de s'y préparer, de s'entraîner et avant tout, de se connaître. À titre illustratif, Synetis est en capacité de s'intégrer à une équipe interne afin d'intervenir rapidement en cas de cyberattaque (investigation numérique, levée de doute, etc.).

En parallèle, il faut, bien sûr, continuer à sensibiliser les utilisateurs. Rappeler régulièrement les bonnes pratiques, en restant le plus pragmatique possible. Un équilibre difficile à trouver, mais essentiel pour que chacun comprenne que c'est avant tout un moyen de protéger ses actifs. »

SYSTEMIS
Cybersecurity Services

Anticipez les attaques et maîtrisez votre cyberdéfense

Société : SYSTEMIS
Adresse : 108 avenue de Fontainebleau, 94270 Le Kremlin-Bicêtre
Tél. : (0) 820 222 302
Mail : **contact@systemis.eu**
Site web : **https://www.systemis.eu/**

Spécialisations

Pure Player Cybersécurité, audit, conseil, expertise, intégration et solutions

Chiffres clés

CA : 10 M€ (e) en 2021

Effectifs : 75 collaborateurs

Historique : fondée en 2009, SYSTEMIS est une société 100 % autonome. Spécialisée en cybersécurité, elle s'engage dans la durée auprès de ses clients (Grands comptes, ETI et PME).

Implantations : France, Benelux, Canada

Centre de cyberdéfense français dédié aux PME/ETI

« Toutes les entreprises, quelles que soient leur taille et leur maturité, doivent avoir accès, en toute autonomie, à une cybersécurité de qualité »
Cyril Magliano

Les **PME/ETI** concentrent près de **60 % des attaques de logiciels malveillants** entraînant un fort risque de disparition. SYSTEMIS met donc à leur disposition un **moyen unique de construire leur protection** en toute autonomie : le Centre de cyberdéfense français.

Ce centre, **uniquement dédié aux PME/ETI,** repose sur un partenariat étroit avec les **acteurs français de la cybersécurité** qui leur permet d'anticiper et de répondre de manière automatisée aux **menaces** les plus récurrentes.

Les **solutions souveraines** proposées et l'accompagnement à la carte font de ce centre un **guichet unique de la cybersécurité** qui aide les entreprises à construire leur propre trajectoire vers une plus grande **cyber résilience**.

Dirigeants

Yohann COHEN
Directeur des opérations
ycohen@systemis.eu

Cyril MAGLIANO
PDG et fondateur
cmagliano@systemis.eu

Fayçal KHALOULI
Directeur du Business Development
fkhalouli@systemis.eu

Notre expertise

Gouvernance – Risque – Conformité : évaluation des risques et mise en œuvre opérationnelle nécessaire à leur gestion rigoureuse et pérenne.
- Analyse des risques
- Schémas directeurs SSI
- Assistance RSSI

Confiance numérique : gestion des habilitations, des flux et des accès.
- Gouvernance des identités et des accès
- Contrôle des accès (SSO, authentification forte…)
- Accès à privilège

Sécurité opérationnelle : mise en œuvre de la sécurité dans les systèmes, les réseaux et les applications.
- Solutions de sécurité (SIEM, SOC, antivirus)
- Fuites de données
- Audit et tests d'intrusions

Nos prestations

Assistance technique : mise à disposition d'un ou de plusieurs consultants expérimentés.

Prestations forfaitaires : mise en place d'une équipe de professionnels de la sécurité pour la réalisation intégrale d'un projet.

SYSTEMIS
Cybersecurity Services

VOUS VOULEZ LE SECRET DE PIERRE ?

IL NOUS A CONFIÉ SA **CYBERSÉCURITÉ**

LA CYBERSÉCURITÉ DE QUALITÉ ACCESSIBLE À TOUS

THALES

Société : Thales
Adresse : 4, avenue des Louvresses – 92622 Gennevilliers Cedex – France
Tel : +33 (0) 1 46 13 20 00
Site Web : **www.thalesgroup.com/cic**
Mail contact :
cyberdefencesolutions@thalesgroup.com

Spécialisations :

Leader européen de la cybersécurité et leader mondial de la protection des données, Thales contribue à la transformation digitale sécurisée de ses clients grâce à sa maîtrise des systèmes d'informations critiques. Ses 2000 spécialistes en cybersécurité répondent aux exigences les plus poussées des clients du Groupe, publics et privés, dont les opérateurs d'importance vitale, en matière de sécurisation des systèmes d'information et de protection des données. Ils comptent plus que jamais sur Thales dans leurs moments décisifs. Couvrant l'ensemble du référentiel du NIST (National Institut of Standards and Technology), les solutions proposées par Thales protègent l'intégrité des technologies qui font avancer le monde en conservant une avance sur toutes les formes de menace numérique.

Chiffres clés :

CA Groupe : 17 milliards d'euros (2020)
Effectifs Groupe : 81 000
Présence mondiale : 68 pays

Dirigeant

Pierre-Yves Jolivet
Directeur général Solutions de CyberDéfense

Thales est l'un des leaders européens de la cybersécurité et le leader mondial de la protection des données.

Fort de 81 000 collaborateurs dans 68 pays, Thales a réalisé en 2020 un chiffre d'affaires de 17 milliards d'euros. Thales offre une capacité unique pour créer et déployer des équipements, des systèmes et des services répondant aux besoins de sécurité les plus complexes. Son implantation internationale exceptionnelle lui permet d'agir au plus près de ses clients partout dans le monde. S'appuyant notamment sur ses compétences fortes en cryptographie, Thales est l'un des leaders mondiaux des produits et solutions de cybersécurité pour la défense, les organismes gouvernementaux, les opérateurs d'importance vitale et les opérateurs de services essentiels, l'internet des objets, notamment du monde industriel et plus largement des systèmes critiques de secteurs d'activité clés (bancaire, transport, spatial, industrie, etc).
Présent sur l'ensemble des prestations de Cybersécurité, Thales propose une plateforme complète de solutions, de produits et de services, pour des environnements souverains ou critiques, depuis le conseil et les audits de sécurité, la protection des données, l'analyse des menaces, la confiance numérique, la conception, la mise au point, l'intégration, la certification et le maintien en conditions de sécurité (MCS) des systèmes, jusqu'au dépistage des cybermenaces, à la détection d'intrusions et à la supervision de la sécurité (centres opérationnels de cybersécurité en France, au Royaume-Uni, aux Pays-Bas, au Canada et à Hong Kong).

Offres

PRODUITS :

Cybels Protect :
- Passerelles de sécurité (Cybels elips-SD et Elips Gateway)
- Protection des réseaux (Cybels Mistral)
- Gestion des accès et authentification multi facteurs (SafeNet Trusted Access)
- Protection de données cloud et serveurs, Gestion d'infrastructures PKI, (Cybels Authenticate, hSM Luna, CipherTrust Data Security Platform)
- Sécurisation des communications mobiles (Cryptosmart), du partage et du stockage de données (Cryptobox), des applications collaboratives de messagerie (Citadel)

Cybels Detect & Respond :
- Sonde de détection d'intrusion (Cybels Sensor)

Services

Cybels Risk & Threat Evaluation :
- Conseil et audit cyber (qualification PASSI)
- Evaluation de la Sécurité des Technologies de l'Information (CeSTI),

Cybels Train & Experiment :
- Formation et entraînement contre les attaques cyber et test des infrastructures IS/IT/OT grâce à des scénarios d'attaque virtualisés (Cybels Train & Experiment),

Cybels Detect & Respond :
- Service de renseignements sur les menaces (Cybels Threat Intelligence)
- Plateforme big data pour la recherche d'attaques avancées (Cybels Analytics)
- Détection et réponse aux menaces (Cybels Security Operation Centres, qualification PDIS)
- Service d'alerte et de réaction rapide aux attaques informatiques (CSIRT/CeRT-IST, qualification PRIS).

Qualifications

Visas de sécurité de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour les qualifications de :
- Prestataire d'Audit de Sécurité des Systèmes d'Information (PASSI)
- Prestataire de détection d'incident de sécurité (PDIS)
- Prestataire de Réponse aux Incidents de Sécurité (PRIS)
- La sonde de détection Cybels Sensor.
- La protection des réseaux
- CeSTI qualifié.
- Critères Communs, CSPN, Bancontact.
- Cryptosmart, agréée Diffusion Restreinte

Société : TIXEO
Adresse : 244 rue Claude-François, 34080 Montpellier
Tél. : +33(0)4 67 75 04 31
Mail : **contact@tixeo.com**
Site web : **www.tixeo.com**

Spécialisations

Solutions de visioconférence collaborative sécurisée

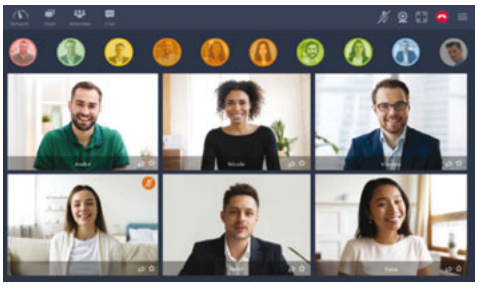
Historique

- **2003 : création de la société**
- **2017 : certification CSPN et Qualification par l'Anssi**

Dirigeants :
Renaud GHIA
Président, co-fondateur

Sébastien JEANJEAN
Directeur général, co-fondateur

« Tixeo s'appuie sur plusieurs années d'expertise dans la conception de solutions innovantes de vidéo-collaboration hautement sécurisée prenant en compte la sécurité à tous les niveaux, dès la conception (Secure by design). De plus, et contrairement à la plupart des autres éditeurs, nous ne sommes soumis à aucune législation étrangère imposant des capacités d'écoute susceptibles d'être exploitées. » Renaud GHIA, *Président de Tixeo*



Créée en 2003, Tixeo est leader européen de la visioconférence sécurisée. Unique acteur français proposant des solutions de vidéo-collaboration labellisées par l'Anssi, Tixeo a conçu sa technologie de visioconférence sur la base d'un ensemble de mécanismes innovants permettant d'assurer un niveau de sécurité encore jamais atteint pour des réunions en ligne. Le siège, la R&D, l'hébergement et le support sont exclusivement localisés en France et sa technologie est non-soumise aux législations étrangères.

Solutions

Tixeo propose une approche simple et conviviale de la visioconférence tout en offrant de nombreuses fonctionnalités de collaboration depuis n'importe quel équipement. Ses trois modes de communication avancée offrent une nouvelle approche de la collaboration et du télétravail en équipe.

La technologie Tixeo, labellisée Anssi, se base sur des mécanismes innovants qui assurent un niveau de sécurité encore jamais atteint dans le domaine de la visioconférence. Tixeo propose un réel chiffrement de bout-en-bout des flux audio, vidéo et data dans une visioconférence multipoint tout en gardant une grande adaptabilité aux variations réseau. Une innovation rendue possible grâce à la technologie unique « SVC on Demand » de Tixeo. Même en cas d'attaque ciblant le serveur Tixeo, la confidentialité des communications est garantie.

Contrairement aux solutions traditionnelles de visioconférence (H.323/SIP), la solution Tixeo ne nécessite l'ouverture que d'un seul port – pas d'impact sur la politique de sécurité du réseau.

À ce jour, contraint par leur architecture technologique, aucun autre acteur de visioconférence ne propose un tel niveau de sécurité.

Offres

Toutes nos offres intègrent la technologie Tixeo certifiée CSPN et qualifiée par l'Anssi et sont 100 % conformes au RGPD

TixeoCloud : la visioconférence sécurisée Tixeo est disponible en mode Cloud pour un déploiement simple, rapide et sécurisé. L'hébergement des serveurs Tixeo se répartit en France métropolitaine selon une stratégie multi-cloud pour garantir une haute disponibilité de service.

TixeoPrivateCloud : le Cloud privé Tixeo vous offre votre propre serveur de visioconférence hébergé dans le Cloud, sans passer par de lourdes étapes de déploiement. Ce Cloud dédié, infogéré par Tixeo, offre une connectivité optimale en supprimant les désagréments de maintenance.

TixeoServer : l'approche on-premise du serveur de visioconférence Tixeo permet de répondre aux exigences les plus strictes en matière d'intégration. En installant TixeoServer au cœur de votre infrastructure vous gardez une totale maîtrise de votre installation et bénéficiez d'une sécurité optimale pour vos visioconférences

Certifications

- Technologie certifiée (CSPN) et qualifiée par l'Anssi
- Labellisé FRANCE CYBERSECURITY et CYBERSECURITY MADE IN EUROPE

Tixeo est membre de : HEXATRUST, ALLIANCE POUR LA CONFIANCE NUMERIQUE, CLUSIF

Tixeo intègre l'offre de visioconférence SFR Business sélectionnée par l'UGAP

Références Clients

Société : THEGREENBOW
Adresse : 14 rue Auber
75009 Paris
Tél. : +33 1 43 12 39 30
Mail : **sales@thegreenbow.com**
Site web : **www.thegreenbow.com**

Spécialisations

Éditeur de logiciels de sécurité des communications et de solutions VPN de confiance

Dirigeants

Roger SIMON
CEO

Mathieu ISAIA
Directeur général

TheGreenBow Vos connexions protégées en toutes circonstances

Pour les communications avec des collaborateurs nomades, des télétravailleurs, d'autres organisations comme vos clients et vos fournisseurs, ou encore avec des objets connectés, vous avez besoin de connexions sécurisées et fiables. Pionnier des technologies VPN depuis 1998 avec plus de 2 millions d'utilisateurs à travers le monde, TheGreenBow protège vos connexions en toutes circonstances.

TheGreenBow est un éditeur de logiciels VPN de confiance. Nous aidons les organisations et les individus à devenir cyber-responsables. Pour cela, nous concevons et développons des solutions fiables et faciles d'utilisation.

Nous protégeons les accès et les connexions à votre système d'information et assurons l'intégrité et la confidentialité des données échangées en toutes circonstances : que ce soit entre des organisations, des collaborateurs nomades, des télétravailleurs ou des objets connectés.

Avec plus de deux millions de licences distribuées dans plus de 70 pays et l'obtention de plusieurs Visas de Sécurité Anssi, les logiciels TheGreenBow s'adressent à tous les types d'organisation : TPE/PME, grands comptes, Opérateurs d'importance vitale (OIV) et Opérateurs de services essentiels (OSE) ou encore administrations et collectivités territoriales.

Nos engagements

ACN, Cercle de l'Arbalète, partenaire Réserve – Entreprise – Défense, Clusif, Cybertaskforce, ECSO, F.I.R.S.T., Hexa-Trust, label « Utilisé par les Armées françaises », Pôle System@tic, TechInFrance.

Notre Offre

Produits

- La gamme **Endpoint Secure Connection** (Client VPN qui comprend l'offre Le VPN Français)
- La gamme **Secure Connection Management** (solutions serveurs)

Services

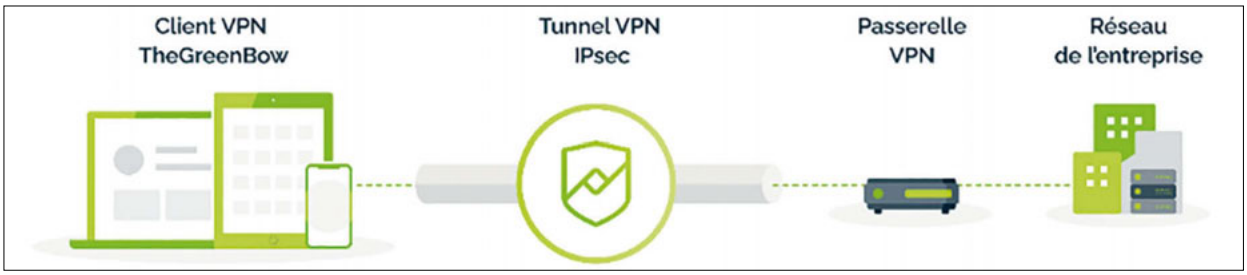
- Formations
- Assistance technique pour des besoins ponctuels
- Technical Account Manager (TAM) pour un accompagnement à long terme

Nos points forts

- Sécurité : premier fournisseur à obtenir une certification Critères communs EAL3+ et un agrément Diffusion restreinte Otan et UE pour ses logiciels VPN (démarche de certification continue auprès de l'Anssi)
- Simplicité d'utilisation : interfaces ergonomiques
- Facilité d'installation : intéropérables avec toute passerelle VPN

Historique

1998 : création de TheGreenBow
2001 : premier client VPN TheGreenBow
2004 : premiers contrats ODM
2013 : première Certification du client VPN Windows TheGreenBow par l'Anssi
2015 : client VPN universel (Windows, Linux, iOS, MacOS
2019 : obtention du label « Utilisé par les Armées françaises »
2020 : certification de deux versions Linux et d'une version Windows



Vos connexions protégées en toutes circonstances avec le VPN de confiance.

Rencontrez TheGreenBow
Du **13 au 16 octobre 2021** aux **Assises de la Cybersécurité** à Monaco sur le stand n° 11, niveau DIAGHILEV

Pour en savoir plus, découvrez toutes nos solutions sur **www.thegreenbow.com**

THEGREENBOW

Trend Micro

Leader mondial de solutions de cybersécurité, Trend Micro contribue à créer un monde plus sûr en sécurisant les échanges d'informations numériques. S'appuyant sur plus de 30 ans d'expertise en matière de sécurité, de recherche sur les menaces et d'innovation continue, Trend Micro permet au grand public, aux entreprises et aux organisations gouvernementales de faire preuve de résilience grâce à des solutions de sécurité connectées pour les environnements Cloud, les Endpoints, la messagerie, l'IIoT et les réseaux.

Contacts
Tél. : 01 76 68 65 00
Mail : **marketing@trendmicro.fr**
Site web : **www.trendmicro.fr**
Twitter : **@TrendMicroFR**
LinkedIn : **https://www.linkedin.com/company/trend-micro-europe**

Spécialisations

Solutions de sécurité connectées pour les environnements Cloud, les Endpoints, la messagerie, l'IIoT et les réseaux, renforcées par une plateforme XDR de défense contre les menaces fournissant une visibilité centralisée des risques.

Chiffres clés

CA Monde : $ 1,515 milliard
Effectif Monde : plus de 6 700 collaborateurs

Dirigeant
Jean-Marc THOUMELIN
VP Europe du Sud

Historique

Depuis 1988, Trend Micro a lancé des technologies et services de sécurité innovants pour protéger les entreprises contre l'évolution de menaces de plus en plus nombreuses et complexes. Trend Micro a été le premier à étendre la protection contre les menaces du poste de travail au serveur, puis à la passerelle Internet. Trend Micro continue d'innover dans la gestion de dispositifs mobiles, les technologies d'évaluation de réputation d'applications mobiles, le chiffrement des données, la détection de menaces avancées et l'optimisation de la sécurité pour les environnements de Cloud et de virtualisation.

Offres

Les solutions Trend Micro sont conçues pour faire face aux problématiques rencontrées au sein du paysage informatique actuel :

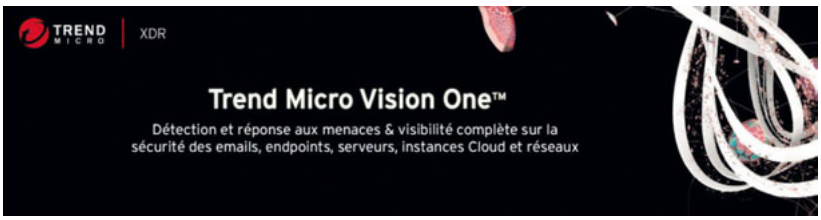
- **Cloud One™** propose des services sur mesure pour le Cloud (serveurs, applications, réseau, stockage de fichiers, conteneurs et conformité).
- **Apex One™**protège l'ensemble des dispositifs (PC fixes, portables & équipements mobiles) & applications des utilisateurs.
- **Network One™** fournit une protection réseau contre les menaces connues, inconnues et non divulguées.

Trend Micro met également au service de ses clients :

- **Trend Micro Vision One™, sa plateforme de défense contre les menaces**, qui permet de réagir plus rapidement à travers l'ensemble des couches de sécurité (messagerie, endpoints, réseau, serveurs et instances Cloud). Capitalisant sur les bénéfices offerts par la technologie Trend Micro XDR, celle-ci fournit une visibilité centralisée des risques et hiérarchise les alertes pour une détection et une réponse aux menaces encore plus rapides.
- **Smart Protection Network™ (SPN), son infrastructure mondiale de renseignements sur les menaces basée sur le Cloud.** Offrant une gestion unifiée de la sécurité, celle-ci optimise l'ensemble des solutions Trend Micro et permet de protéger les données sensibles où qu'elles se trouvent. Chaque jour, SPN collecte et analyse près de 8 milliards de requêtes, bloque près de 180 millions de menaces et identifie près de 18 millions de nouvelles menaces.
- **Son programme Zero Day Initiative (ZDI),** reconnu comme la référence mondiale en matière de détection et de recherche de vulnérabilités depuis 13 ans. Incontournable en ce qui concerne l'identification des bugs très sévères et critiques, ce dernier a identifié et rendu publiques 60 % des vulnérabilités signalées dans le monde en 2020.
- **Les Trend Research, son réseau international de plus de 450 chercheurs en sécurité à travers le monde, disponible 24h/24, 7j/7.** Cette équipe d'experts et ingénieurs spécialisés est chargée de surveiller les menaces, de prévenir les attaques et fournir des solutions rapides afin d'aider les clients à sécuriser leurs données.

Références clients

Trend Micro compte parmi ses clients 9 des 10 premières entreprises du Fortune® Global 500 dans les secteurs de l'automobile, de la banque, de la santé, des télécoms et de l'industrie pétrolière.



TREND MICRO | XDR

TREND MICRO VISION ONE™

VOIR PLUS.
RÉAGIR PLUS VITE.

Les menaces évoluent, c'est pourquoi vous devez pouvoir réagir rapidement à celles qui compromettent vos lignes de défense en place.

Aujourd'hui, la messagerie, les endpoints, les serveurs et les services Cloud sont souvent protégés par des couches de sécurité distinctes. Jusqu'à faire proliférer des alertes non corrélées, susceptibles de masquer une attaque en cours.

Capitalisant sur **notre technologie XDR éprouvée**, la nouvelle plateforme **Trend Micro Vision One™** offre une visibilité centralisée des risques et hiérarchise les alertes pour une détection et une réponse aux menaces encore plus rapides.

Vous accélérez ainsi la détection et la réponse aux menaces.

Pour plus d'informations, rendez-vous sur www.trendmicro.fr/VisionOne

TREND MICRO

UPPER-LINK
DIGITAL TRANSFORMATION & CLOUD SOLUTIONS

Société : UPPER-LINK (Cloud Solutions)
Adresse : 7 mail Barthélémy-Thimonnier – 77185 Lognes
Tél. : 01 81 80 07 70
Mail : **sales@upper-link.com**
Site web : **www.upper-link.com**

Pour s'informer et comprendre comment sécuriser votre système d'information, rendez-vous www.upper-link.com/securite.

Dirigeant :
René-Louis ADDA
Président d'Upper-Link

« Dire que la sécurité est un enjeu majeur du SI devient dérisoire. Avec la croissance importante des cyber-attaques, la sécurité du SI est devenue un enjeu de survie des entreprises et un enjeu de sécurité économique nationale.

La sécurité qui représentait un coût très important devient, par l'existence de nouvelles offres sur le marché, bien plus abordable pour les entreprises, chacune à leur niveau. »

René-Louis ADDA,
Président d'UPPER-LINK

Certifiés ISO 27001 et professionnel en sécurité informatique référencé par Cybermalveillance.gouv.fr, Upper-link, ESN spécialisée dans la transformation digitale et les solutions intervient sur tout le territoire français et européen. Pour les besoins de certains clients, nous gérons des projets à l'échelle mondiale.

Avec plus de quinze ans d'expérience, Upper-Link vous accompagne dans la transformation et la sécurisation de votre système d'information.

Pour y répondre, nous nous sommes organisés en quatre départements, le Digital Workplace (poste de travail), l'infrastructure (Cloud/Hybride), le développement d'applications spécifique, le CRM & DATA/BI.

Cloud Solution Provider Microsoft et multi Gold Partner, vous bénéficiez outre de notre expertise du support prioritaire Microsoft et de conditions tarifaires avantageuses sur les abonnements Cloud (MS 365, AZURE, DYNAMICS…) et sur tous les outils de sécurité associés.

Nous avons développé un système de facturation détaillé et flexible offrant à nos clients la possibilité d'ajuster le nombre de licences au mois le mois et d'analyser le coût par entité.

Pour un système performant, sécurisé et au juste coût, Upper-Link fait l'architecture, intègre et manage tout ou partie de votre système.

Offres

- Audit et Sécurisation du poste de travail
- Audit et sécurisation de l'infrastructure (serveur & réseau)
- Audit et sécurisation des applications
- Mise en place des sauvegardes et PRA
- Formation et accompagnement des utilisateurs à un comportement sécuritaire

Services

- Audit et conseil pour sécuriser les systèmes
- Intégration de solutions de sécurité
- Surveillance et gestion 24/7 disponibilité et sécurité du SI (Infogérance/supervision)

Solutions

- Microsoft Endpoint Manager (MDM)
- Microsoft Defender Security Center (SOC)
- Azure Information Protection (chiffrement)
- Microsoft Defender for Office 365 (anti-phishing)
- Microsoft Defender for Azure (antivirus)
- Conditionnal Access
- Multi-Factor Authentication
- Azure Sentinel (SIEM)
- Azure Backup (sauvegarde & PRA)
- Microsoft Cloud App Discovery (SIEM)
- Microsoft Cloud App Security (CASB)

Certifications

- **Professionnel en sécurité informatique référencé par Cybermalveillance.gouv.fr**
- **Certifiés ISO 27001**
- **Cloud Solution Provider Microsoft**
- **Multi Gold-Partner Microsoft**

USERCUBE

IGA by design

Usercube, la solution de gouvernance et d'administration des identités (IGA) adaptée à votre organisation.

Les entreprises doivent aujourd'hui s'adapter au travail à distance. Elles doivent **réduire leurs coûts** informatiques tout en **augmentant leur sécurité**.

La gouvernance des identités et des accès permet de se **conformer** à des **réglementations** et des **politiques de sécurité** de plus en plus exigeantes.

Usercube est la **solution SaaS** la plus adaptée aux entreprises, offrant un ensemble complet de **fonctionnalités** et une expérience utilisateur optimisée.

3M
Identités managées

500M
Rôles supervisés

100%
SaaS multitenant

150
Clients dans le monde

- **Catalogue de connecteurs**
- **Modèle de rôles multidimensionnel capable de gérer les droits fins**
- **Automatisation de la mise à jour des données de l'organisation et des workflows d'arrivées, mutations, sorties.**
- **Fonctionnalités de SoD, reporting et recertification**

ISO 27001
BUREAU VERITAS
Certification

BUREAU VERITAS 1828

NOS CLIENTS EN TÉMOIGNENT

INTÉGRATION RAPIDE

" Grâce à cette solution entièrement personnalisable et sans code, nous avons déployé une gouvernance complète des identités et des accès aux applications en moins de 9 mois portant sur plus de 4 500 rôles applicatifs et plus de 500 000 rôles techniques. "

Top 10 mondial des banques de détail

SECURISÉE & ADAPTÉE

" Usercube prend en charge nos exigences en matière de confidentialité des données ainsi que nos normes de sécurité les plus strictes grâce à la certification ISO 27001. La solution a directement généré 1,3M€ d'économies annuelles tout en supprimant toutes les failles de sécurité des comptes utilisateurs non contrôlés. "

Top 5 mondial de fournisseurs de pétrole gaz

FACILE D'UTILISATION

" L'interface moderne et intuitive d'Usercube a été un avantage clé dans l'accélération du déploiement de la solution auprès de nos utilisateurs internationaux très exigeants. Les certifications d'accès aux applications n'ont jamais été aussi facilement acceptées et réalisées par les équipes commerciales. "

Groupe de défense européen

www.usercube.com / sales@usercube.com

VENAFI®

Leader de la protection et de la gestion des identités machine

Société : VENAFI
Adresse : 175 E 400 S, Suite 300
Salt Lake City, UT 84111 USA
Tél. : +1.801.676.6900
Site web : **https://www.venafi.com**

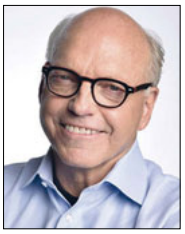
Spécialisations

Notre plateforme logicielle gère et sécurise les clés et certificats dont dépendent toutes les entreprises privées et tous les organismes publics pour sécuriser l'authentification et l'accès des machines, le chiffrement des communications et l'intégrité du code généré. Les solutions Venafi protègent les communications, les transactions commerciales, les systèmes et données critiques, les accès des utilisateurs et l'environnement mobile.

Chiffres clés

Effectifs : +300 collaborateurs

Plus de 500 entreprises du G2000 utilisent VENAFI pour se protéger



Jeff HUDSON,
CEO

Stéphane DORCHIN
Directeur Europe continentale

Machine Identity Management : cette catégorie de marché a été récemment reconnue par les analystes, dont le Gartner.
Venafi en est l'inventeur et le leader. Venafi propose aujourd'hui une seule et unique plateforme pour gouverner les identités machine et assurer l'automatisation de leur cycle de vie.
Selon le Gartner : *« La gestion de l'identité des machines vise à établir et à gérer la confiance dans l'identité d'une machine – appareils mobiles, objet connectés, containers, applications, code entre autres – interagissant avec d'autres entités, telles que des appareils, des applications, des services cloud ou des passerelles. »*

Il y a deux acteurs majeurs sur le réseau : les humains et les machines.

Les humains utilisent leurs identifiants et des mots de passe pour s'authentifier auprès des machines et ainsi accéder au réseau et aux informations.

Les machines ont également besoin de s'identifier les unes aux autres, mais elles n'utilisent pas d'identifiants et mots de passe. Pour ce faire, elles utilisent des identités machine matérialisées par des certificats et clés.

Nous savons tous que le nombre de machines sur les réseaux augmente de manière exponentielle, en lien avec la transformation digitale qui elle-même dépend des machines et non des humains.

Plus de 10 milliards de dollars sont dépensés chaque année pour protéger les identités des personnes, mais nous investissons trop peu pour protéger les identités des machine.

Les cyber criminels sont bien au fait de cela, et eux concentrent des ressources de plus en plus importantes pour voler des identités machine et accéder impunément aux réseaux des organisations.

Venafi a inventé la technologie qui permet d'avoir la visibilité, l'intelligence, l'automatisation et les intégrations nécessaires pour protéger de manière globale les identités machine des sociétés soucieuses d'augmenter leur maîtrise du risque cyber.

Solutions

La transformation digitale, la cloudisation, l'avènement des DevOps et la création en interne d'usines digitales poussent les organisations à créer et déployer de plus en plus de machines, de plus en plus variées, de plus en plus rapidement.

Cette accélération du nombre de machines sert en premier les métiers de l'entreprise en leur permettant d'être plus accessibles pour les clients, plus véloces, plus intégrés, plus innovants. Mais en contrepartie la multiplication des machines les expose plus grandement et profondément aux cyber attaques.

en effet, l'accroissement du nombre de machines et donc des identités machines entraine une perte de visibilité et de contrôle de la part des équipes de sécurité tout en apportant une charge de travail supplémentaire aux équipes opérationnelles. Cela offre une surface d'attaque importante aux hackers tant sur le nombre que sur le niveau cryptographique souvent faible, alors que l'organisation est moins agile pour y répondre.

Par exemple, il n'est pas rare de voir des certificats de plus de 3 ans installés sur des machines. Est-ce acceptable ? Est-ce que la machine est sécurisée ? Est-ce qu'il est facile de changer cette identité ? La réponse est trois fois « Non ! ». Mais comment sommes-nous arrivés à ce stade et comment y remédier ?

Les méthodes de gestion traditionnelles des identités machine – très souvent manuelles – sont dépassées et ne savent pas répondre aux besoins de la transformation digitale. Les équipes de sécurité, très axées sur les utilisateurs, ont délaissé les machines. Il est en tout premier lieu, nécessaire de reconsidérer les machines et leur identité comme des actifs critiques qu'il faut savoir bien sécuriser à leur création et surtout pouvoir gérer tout au long de leur vie. Puis en reprendre le contrôle.

Pour ce faire, les équipes de sécurité doivent pouvoir avoir la visibilité sur les identités actives sur le réseau afin de mieux mitiger les risques, anticiper les problèmes et identifier leurs priorités.

De plus, ces mêmes équipes doivent repenser la mise à disposition d'une identité machine quelle qu'elle soit, pour en faire un service automatisable et intégrable dans les processus et technologies des nouveaux départements IT aussi bien que dans le legacy. L'identité machine doit être « consommée » facilement, son accès doit être simplifié.

Enfin l'intégration d'une identité machine dans un processus IT doit devenir la norme. L'automatisation des tâches d'administration doit être proposée aux diverses équipes.

Visibilité, facilité, automatisation, intégration des identités à l'échelle de l'organisation permettent à celle-ci de devenir crypto agile et répondre aux défis de la sécurité des identités machine, de la conformité interne et réglementaire et des opérationnels, tout en réduisant drastiquement ses coûts et augmentant la fiabilité de son SI.

Plus de sécurité, plus vite, pour tout le monde et moins cher : c'est ce que les clients de Venafi ont pu démontrer dès les premiers mois d'utilisation de notre plateforme.

Comment Venafi peut-il vous aider à protéger les identités de vos machines?

Venafi propose une gamme de solutions pour aider les grandes entreprises à sécuriser leurs clés et certificats

- Éliminer les arrêts de production liés aux certificats
- Gouverner l'usage des clés SSH
- Rationnaliser sa PKI
- Simplifier la sécurisation des DevOps
- Éviter les constats d'audit
- Sécuriser les appareils mobiles

venafi.com

VENAFI®

©2020 Venafi, Inc. All rights reserved.

WALLIX
CYBERSECURITY SIMPLIFIED

Société : WALLIX GROUP
Adresse : 250 bis, rue du Faubourg-St-Honoré 75008 PARIS
Tél. : +33 1 53 42 12 81
Site web : **www.wallix.com**

Dirigeant
Jean-Noël de GALZAIN
Président – Directeur général

Contact
Jean-Pierre BARRE
Directeur commercial France
jpbarre@wallix.com

Témoignage client

d'un DSI du secteur de la communication – 2020 Gartner Peer Insights :

« Wallix simplifie la gestion des identités et des accès. Je contrôle les différents accès à mon SI et j'ai maintenant des tableaux de bord pertinents »

Twitter : **@wallixcom**
Linkedin : **WALLIX Group**

Essayez gratuitement nos solutions pendant 30 jours !

Sécurisez votre avenir numérique

WALLIX protège les identités et les accès aux infrastructures informatiques, aux applications et aux données. Spécialisées dans la gestion des accès à privilèges, les solutions WALLIX garantissent la conformité aux dernières normes de sécurité informatique et protègent contre les cyber-attaques, les vols et les fuites de données liés aux identités volées et aux abus de privilèges.

Produits

WALLIX Bastion : solution leader européenne de *Privileged Access Management*, facile à utiliser et à déployer, Bastion offre une sécurité et une surveillance robustes des accès à privilèges aux infrastructures informatiques critiques. Solution certifiée CSPN par l'Anssi.

WALLIX BestSafe : solution de *Endpoint Privilege Management* pour une gestion du moindre privilège innovante. Éliminez le besoin d'élévation de privilèges sur les comptes utilisateurs et garantissez une sécurité hors pair sur tous les terminaux avec des autorisations contrôlées au niveau des processus et applicatifs.

WALLIX Trustelem : solution *d'Identity as a Service* (IDaaS) pour unifier et simplifier l'accès aux applications métier. Améliorez l'expérience utilisateur et augmentez la productivité des administrateurs.

WALLIX Authenticator : solution d'Authentification multi-facteurs pour protéger l'accès aux actifs informatiques, aux applications et aux données, avec une connexion de haute sécurité où que vous soyez.

Usages métiers

- **Transformation digitale :** automatisez la sécurité pour garantir la productivité de vos équipes IT et DevOps et sécurisez votre transformation digitale quelle que soit la localisation de vos ressources IT.
- **Audit & Conformité :** relevez le défi de la conformité en répondant aux exigences des standards et réglementations sectorielles, nationales et européennes (RGPD, PCI DSS, Directive NIS, ISO 27001).
- **Gestion des risques et sécurité :** assurez-vous que vos systèmes les plus vulnérables sont protégés des utilisateurs (internes et externes) pour garantir la continuité d'activité et la productivité de votre société.
- **Cybersécurité à la conception :** renforcez la sécurité de vos solutions en intégrant les technologies de gestion des accès et des identités de WALLIX dès leur conception avec **WALLIX Inside**. Concentrez-vous sur votre métier en toute sécurité.

À propos de WALLIX

- Leader européen du PAM
- Solutions certifiées CSPN par l'Anssi
- Un réseau mondial de partenaires technologiques et commerciaux
- Coté en Bourse sur Euronext Growth (ALLIX)

Cybersécurité : RESTEZ INFORMÉ

L'actualité quotidienne
News, avis d'experts, témoignages, livres blancs, etc.
https://www.solutions-numeriques.com/securite/

La newsletter
Chaque lundi, comme 40 000 professionnels et décideurs, recevez la synthèse des informations.
C'est gratuit, inscrivez vous :
https://www.solutions-numeriques.com/securite/inscription/

L'annuaire : Guide papier et en ligne
Trouvez l'éditeur de solution, le prestataire de services qu'il vous faut.
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

033CRI

Société : WatchGuard® Technologies
Adresse : 22 Boulevard de Stalingrad
92320 Châtillon
Tel : +33 97 755 4336
*Mail : **france@watchguard.com***
*Site Web : **www.watchguard.fr***

Chiffres clés :
Effectifs : 1 200 collaborateurs

Historique :
Société créée en 1996

Dirigeants
Prakash PANJWANI
CEO

Contacts
Pascal Le DIGOL
Country Manager France
Email: **pascal.ledigol@watchguard.com**
Tél.: 06 20 20 58 35

Une solution idéale pour les PME et les entreprises dites distribuées

Depuis 25 ans, WatchGuard Technologies s'attache à développer des technologies de cybersécurité de pointe afin de proposer des solutions faciles à déployer et à gérer. La société est aujourd'hui leader mondial en matière de sécurité et d'intelligence réseau, de Wi-Fi sécurisé, d'authentification multifacteur et de protection avancée des endpoints.
Près de 18 000 revendeurs et fournisseurs de services de sécurité font confiance aux produits et services primés de l'entreprise dans le monde entier pour protéger les actifs de plus de 250 000 clients dans un monde où le paysage de la cybersécurité est en perpétuelle évolution. La mission de l'éditeur est de rendre la sécurité d'entreprise accessible aux entreprises de tous types et de toutes tailles, en toute simplicité, faisant de WatchGuard une solution idéale pour les PME et les entreprises dites distribuées.

Offres

- **Sécurité et intelligence réseau**
- **Sécurité des endpoints**
- **Authentification multifacteur (MFA)**
- **Wi-Fi sécurisé**

Points forts

Protection intelligente
De multiples services collaborent intelligemment à la prévention, la détection et la réponse instantanée aux cyberattaques à l'aide de politiques automatisées. Ils surveillent en outre la santé de votre infrastructure informatique, tout en vous tenant à tout moment informé(e).

Visibilité exploitable
Des outils de visibilité exploitables vous permettent d'identifier proactivement les menaces, tout en vous proposant des mesures correctives pour les problèmes connus.

Gestion simplifiée
Grâce à notre plateforme de gestion basée dans le Cloud, vous pouvez déployer, configurer et maintenir rapidement et facilement votre sécurité sur plusieurs produits de sécurité, entreprises et sites.

SMART SECURITY, SIMPLY DONE.

SÉCURITÉ RÉSEAU • AUTHENTIFICATION MULTIFACTEUR • WI-FI SÉCURISÉ • SÉCURITÉ DES ENDPOINTS

PROTECTION INTELLIGENTE

De multiples services collaborent intelligemment à la prévention, la détection et la réponse instantanée aux cyberattaques à l'aide de politiques automatisées. Ils surveillent en outre la santé de votre infrastructure informatique, tout en vous tenant à tout moment informé(e).

VISIBILITÉ EXPLOITABLE

Des outils de visibilité exploitables vous permettent d'identifier proactivement les menaces, tout en vous proposant des mesures correctives pour les problèmes connus.

GESTION SIMPLIFIÉE

Grâce à notre plateforme de gestion basée dans le Cloud, vous pouvez déployer, configurer et maintenir rapidement et facilement votre sécurité sur plusieurs produits de sécurité, entreprises et sites.

PIONNIER DEPUIS 25 ANS DANS LE DÉVELOPPEMENT DE TECHNOLOGIES DE CYBERSÉCURITÉ DE POINTE

25 ANNIVERSARY WatchGuard

+33 97 755 4336

france@watchguard.com

©2021WatchGuard Technologies, Inc. Tous droits réservés.
Part No.WGCE67463_081921

La première plateforme européenne de Bug Bounty et de *Vulnerability Disclosure Policy* (VDP)

Société : YESWEHACK
Adresse : 14 rue Charles-V
75004 PARIS
Mail : **contact@yeswehack.com**
Site web : **https://www.yeswehack.com**

Fondée en 2015, YesWeHack est la première plateforme européenne de Bug Bounty et de Vulnerability Disclosure Policy (VDP). YesWeHack connecte plus de 30 000 hackers éthiques répartis dans 170 pays et des organisations de toutes tailles et de tous secteurs pour rechercher les vulnérabilités (bugs) de leurs sites web, applications mobiles, infrastructures et objets connectés, et sécuriser leurs périmètres exposés.

Spécialisations

Bug Bounty et VDP

Chiffres clés

Effectifs : 60 salariés – 30 000+ hackers éthiques

Historique

Fondée en 2015, YesWeHack est la première plateforme européenne de Bug Bounty et VDP. Avec des bureaux en France, Allemagne, Suisse et à Singapour, YesWeHack sécurise des organisations de toutes tailles et de tous secteurs dans plus de 40 pays.

Dirigeants

Guillaume VASSAULT-HOULIÈRE
CEO & co-fondateur, YesWeHack

Romain LECOEUVRE
CTO & co-fondateur, YesWeHack

Popularisé dans les années 90 par Netscape, le Bug Bounty devient une pratique courante d'un nombre croissant d'organisations, des start-up aux administrations, en passant par des entreprises du CAC40.

Le Bug Bounty consiste, pour une organisation, à récompenser – avec des primes, ou *Bounties* – des chercheurs, ou « hackeurs éthiques », pour les vulnérabilités – les « bugs » – qu'ils lui rapportent.

Le Bug Bounty se déroule dans le cadre d'un programme qui définit les règles à respecter par l'organisation et les chercheurs. Ces règles précisent principalement :

- le(s) périmètre(s) du programme : sur lequel les vulnérabilités peuvent être recherchées. Il s'agit le plus souvent d'applications web ou mobiles, d'API ou d'infrastructures, mais également – de plus en plus fréquemment – d'objets connectés
- les types de vulnérabilités à rechercher ou « vulnérabilités qualifiantes », et qui donnent droit à une prime
- la grille de primes applicable – en fonction de la gravité de la vulnérabilité remontée
- toute autre spécificité du programme, que l'organisation souhaite préciser

Offres

Les services YesWeHack

- **Programmes de Bug Bounty privés :** sélectionnez, pour chaque programme, des chercheurs selon vos critères d'expertise, de compétence, de nationalité. YesWeHack gère à ce jour plus de 350 programmes privés en Europe et en Asie.
- **Programmes de Bug Bounty publics :** mobilisez l'intégralité de la communauté YesWeHack et communiquez sur votre stratégie de sécurité.
- **Vulnerability Disclosure Policy (VDP) :** offrez aux chercheurs un canal sécurisé et structuré pour remonter les vulnérabilités de vos systèmes d'information, avant qu'elles ne soient découvertes et exploitées par des personnes malveillantes.

Un accompagnement complet et personnalisé

En complément d'une communauté de confiance et de qualité, ainsi que d'une interface puissante et conviviale, la plateforme YesWeHack intègre un support client avancé, gérant vos programmes de bout en bout : définition et mise à jour des règles, sélection et rotation des chercheurs, triage des rapports des vulnérabilités, suivi des budgets et indicateurs des programmes en ligne avec les objectifs du client, etc.

Références Clients

- Plus de 350 programmes privés dans plus de 40 pays
- Programmes publics : Blablacar, SwissPost, Lazada, Deezer, OVHcloud, ZTE, Dailymotion, TousAntiCovid, Prestashop, Cybermalveillance.gouv.fr, Aéroport de Paris, Olvid…

COORDONNEZ VOTRE REMONTÉE DE VULNÉRABILITÉS

AVEC

YES WE HACK

#1 PLATEFORME EUROPÉENNE DE SÉCURITÉ CROWDSOURCÉE

WWW.YESWEHACK.COM

BUG BOUNTY YES WE HACK		VDP YES WE HACK*
APPROCHE ACTIVE		**APPROCHE PASSIVE** *Politique de Divulgation de Vulnérabilités
Encourager la recherche de vulnérabilités.	**POURQUOI**	Recueillir des vulnérabilités potentielles.
Création d'un programme de Bug Bounty publié sur YesWeHack. Définissez le périmètre, les règles et la grille de récompenses.	**COMMENT**	Mise à disposition d'un canal de communication sur une page web dédiée. Centralisez les remontées grâce à la plateforme YesWeHack.
À une sélection de chercheurs de la plateforme (privé) ou à la totalité de la communauté YesWeHack (public).	**QUI**	À toute personne souhaitant signaler un bug.
RECHERCHE ACTIVE, LES CHERCHEURS SONT ATTIRÉS PAR UNE RÉCOMPENSE FINANCIÈRE.		**DÉCOUVERTE FORTUITE, AUCUNE ATTENTE DE RÉCOMPENSE FINANCIÈRE.**

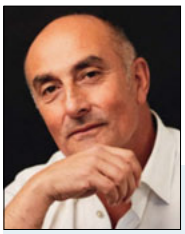
BUG BOUNTY

VDP

Société : WOOXO
Adresse : 515 avenue de la Tramontane – Bat. A
13600 La Ciotat – France
Tél. : 0811 140160
Mail : info@wooxo.fr
Site web : www.wooxo.fr

Spécialisations

Éditeur de solutions pour la protection des données, Wooxo aide les entreprises de toute taille à préserver leurs écosystèmes de données numériques, essentiels à leur activité. Son credo : zéro perte de données, zéro interruption d'activité !



Dirigeant
Luc d'URSO
PDG du groupe Atempo.Wooxo

« En tant qu'éditeur de solutions 100 % souveraines et membre de la sélection French Tech 120, Alumni 2020, nous avons un devoir d'exemplarité. Nos offres s'inscrivent dans la droite ligne du Plan France Relance orchestré par le gouvernement et plus particulièrement son volet Cybersécurité. Le pack Cybersécurité répond en tous points aux attentes des organisations : sécurité et confidentialité des données protégées, conformité réglementaire, réversibilité, transparence tarifaire et bien entendu performance », déclare Luc d'Urso, PDG du groupe Atempo.Wooxo.

Éditeur français de solutions pour la protection des écosystèmes numériques professionnels et constructeur de matériel informatique, Wooxo s'adresse aux TPE/PME à la recherche de solutions concrètes, clé en main et abordables pour protéger leurs systèmes d'information contre tous types de risques – cyberattaques, vols, incendies, etc.

Depuis 2010, Wooxo assure la reprise d'activité informatique des organisations professionnelles en France, en Europe et au Maghreb à travers un ensemble de services de protection des données (le « Pack Cybersécurité ») qui répondent aux exigences du RGPD en matière de sauvegarde et restauration. En 2017, Wooxo s'associe à Atempo, géant international de la sauvegarde et de l'archivage professionnel pour les gros volumes de données. Le Groupe Atempo.Wooxo vient ainsi se placer au 50e rang du *Truffle 100* des éditeurs de logiciels français.

Wooxo intègre au Pack Cybersécurité la solution YooShield, son anti-malware exclusif de prévention des cyberattaques. Associant désormais la reprise d'activité à la protection préventive contre les différentes formes de malwares, le Pack Cybersécurité de Wooxo devient le premier service de protection 360° à destination des TPE/PME. Wooxo, acteur incontournable de la lutte contre la cybercriminalité, est la seule entreprise de son marché à proposer au sein d'une même offre ce niveau de service et d'expertise pour les organisations de taille modeste.

Récompenses

Le Pack Cybersécurité de Wooxo est une solution labellisée France Cybersecurity.

Wooxo fait partie des 120 entreprises françaises, dotées d'un potentiel d'hyper-croissance, sélectionnées dans le cadre du programme d'accompagnement gouvernemental FT 120. L'entreprise a été élue *Best SME Data Protection Company 2019 & Leading Provider of Backup Software* en 2019.

L'éditeur assure la vice-présidence d'Hexatrust, groupement qui réunit plusieurs éditeurs français œuvrant ensemble pour promouvoir l'excellence cyber et le Cloud de confiance.

Wooxo fait également partie du groupement Acyma qui soutient le programme gouvernemental cybermalveillance.gouv.fr, et l'entreprise est membre du Pôle mondial des Solutions Communicantes Sécurisées, de Medinsoft et de la French Tech Aix-Marseille.

En août 2021, Wooxo a obtenu la certification ISO 9001 : 2015 pour son système de Management de la Qualité.

Le Pack Cybersécurité est une solution souveraine de prévention des cyberattaques et de reprise instantanée d'activité, spécialement conçue pour les TPE/PME. Simples et efficaces, ses services clé en main et packagés garantissent zéro perte de données et zéro interruption d'activité en s'adaptant à tous les budgets :

- sauvegarde sécurisée contre les ransomwares et opérationnelle 24/24
- respect de la règle essentielle du 3-2-1
- reprise d'activité instantanée
- restauration sur site ou hors site, online ou offline
- restauration *Bare Metal Restore* autonome en moins d'une minute

Les acteurs du marché

Panorama des offreurs de solutions et de services de cybersécurité en France

- **Fournisseurs de solutions** fiches alphabétiques p160
- **Prestataires de services** fiches alphabétiques p174

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.
L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Consultez le site web, qui peut comporter des mises à jour :
www.solutions-numeriques.com/securite/annuaire-cybersecurite/.

Les éditeurs et sociétés de services peuvent se référencer ou mettre à jour leur fiche existante sur la même page.

E C Label ExpertCyber N Adhérents Numeum (ex Syntec Numérique) H Adhérents Hexatrust

Fournisseurs de solutions

3D-OXIDES

Nous développons un chip sécuritaire couplé à une blockchain user-centric pour faire des identités physiques et digitales pour tous types d'utilisateur incluant aussi les objets.

01630 Saint-Genis Pouilly France

http://www.3d-oxides.com

3M FRANCE

Notre promesse : travaillez sereinement grâce à des appareils protégés du piratage visuel avec les filtres de confidentialité 3M.

95006 Cergy-Pontoise France

6CURE H

Éditeur français de solutions de réactions aux attaques informatiques.

Threat Protection®: détection et neutralisation des attaques DDoS / DNS Protection® : mitigation des menaces DNS.

14200 Hérouville-Saint-Clair France

http://www.6cure.com

8MAN

Suite intégrée permettant de visualiser la structure de l'annuaire et des ressources informatiques afin de le modifier dynamiquement pour prévenir en temps réel de toute faille de sécurité.

10555 Berlin France

A10 NETWORKS

A10 Networks fournit des solutions ADC, FIREWALLS, PROXY, ANTIDDOS, DECHIFFREMENT DE FUX SSL/TLS pour les Data-Centers et Multi-Clouds (privés/publics) aux formats Appliance, VM, BareMetal, Container.

92974 Paris-La Défense France

https://www.a10networks.com

ACG CYBERSECURITY

Conseil en sécurité de l'information, conseil en cybersécurité, gouvernance SSI, diagnostic cybersécurité, analyse de risques, audits de sécurité & tech, mise en conformité.

92800 Paris Île de France France

https://acgcybersecurity.fr

ACRONIS

Acronis édite des solutions de protection des données Cloud hybride : sauvegarde, reprise d'activité après sinistre et synchronisation et partage sécurisés des fichiers.

92300 Levallois-Perret France

http://www.acronis.com

ADVANCED TRACK & TRACE

ATT développe des solutions d'authentification, de traçabilité et de sécurité documentaire. SealCrypt, cachet électronique visible, permet de protéger tout document, à la fois physique et numérique.

92500 Rueil-Malmaison France

AF SOFTWARE

2 modules principaux : - MySUSI : « Sensibilisation des utilisateurs à la sécurité informatique » - GRC : « GDPR Registry Console ». Outil numérique novateur pour la tenue des registres imposée par la GDPR.

13100 Aix-en-Provence France

https://www.afsoftware.fr

AFFINION INTERNATIONAL

Nous proposons une approche 360° de la cyber protection en réponse aux nouveaux risques auxquels s'exposent les consommateurs. Cette offre s'adresse aux banques, assurances et télécoms.

75002 Paris France

https://affinion.fr

AIRBUS CYBERSECURITY

Airbus CyberSecurity fournit des produits et des services de sécurité de confiance sur mesure, permettant d'anticiper, détecter, analyser et répondre aux cyber-attaques les plus sophistiquées.

78990 Élancourt France

https://www.cybersecurity-airbusds.com/fr

ALGOSEC

Aligner la gestion de la politique de sécurité réseau sur vos processus métiers avec AlgoSec Security Management Suite.

EC2R 5 BJ Londres Royaume-Uni

ALHAMBRA SYSTEMS SA

OneseQ (Alhambra, Groupe PROLOGUE) apporte et intègre des solutions blockchain et de cybersécurité, pour proteger les données, la continuité des processus et la sécurité des procédures de décision.

28037 Madrid Espagne

https://oneseq.es

ALINTO

Alinto sécurise et optimise les Emails des organisations. À la fois éditeur et opérateur nous assurons un service premium aux entreprises désireuses de travailler avec des spécialistes.

69002 Lyon France

https://www.alinto.com

APICEM SARL

APICRYPT, messagerie sécurisée en santé, facilite la communication entre les professionnels de santé tout en préservant la confidentialité des informations transmises par un cryptage de haut niveau.

59412 Coudekerque Cedex 2 France

https://www.apicrypt.org

AQUA SECURITY

Aqua propose une solution permetttant de sécuriser tout le cycle de vie des applications Cloud Natives (du pipeline CI/CD au runtime et à la micro segmentation) quel que soit le type d'environnement.

75000 Paris France

https://www.aquasec.com

ARCSERVE

Nos solutions de protection des données, PRA/PCA, sur site et dans le Cloud, ainsi que notre stockage immuable offrent une récupération instantanée, fiable et complète.

75001 Paris France

https://www.arcserve.com/fr/

ARS NOVA SYSTEMS

TinyMDM : logiciel français de gestion d'appareils mobiles professionnels dédié à Android et partenaire Android EMM. Il possède trois modes de gestion : mode kiosque, 100 % managé et profil de travail.

44300 NANTES France

https://www.tinymdm.fr/

ARX ONE

Sauvegarde en ligne professionnelle : service de sauvegarde assurant la protection des données et le respect de leur confidentialité. Flexibilité, polyvalence et reprise rapide après sinistre.

44300 Nantes France

www.arxone.com

ATEMPO H

Éditeur de solutions de protection de données, Atempo dispose d'une expertise forte pour sauvegarder, archiver, restaurer et déplacer les gros volumes de données critiques de milliers d'entreprises.

91300 Massy France

http://www.atempo.com

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction. Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

ATOS

N H

Services et produits : Evidian (gestion identités/accès), Trustway (chiffrement - HSM), IDnomic (sécurité de l'IoT, infrastructures de confiance), SOC, conseil, intégration, MDR, CERT, audit, infogérance.

95870 Bezons France

https://atos.net/en

AVANT DE CLIQUER

N

Solution intelligente et automatique de sensibilisation des utilisateurs à la cybersécurité et au phishing. Montée en compétence par le biais d'un programme d'apprentissage par l'action individualisé.

76000 Rouen France

https://www.avantdecliquer.com

AVAST SOFTWARE

Avast fournit des solutions de sécurité digitale pour protéger ordinateurs, terminaux mobiles et IoT, utilisant le machine learning et l'IA pour détecter et contrer les menaces en temps réel.

14000 Prague 4 République tchèque

http://www.avast.com

AVIRA

Avira protège les individus en leur permettant de gérer, de sécuriser et d'améliorer leur vie numérique via toute une gamme d'applications de sécurité et de performance (Windows, Android, Mac, et iOS).

88069 Tettnang Allemagne

https://www.avira.com/fr

AXWAY SOFTWARE

N

La gamme comprend deux offres : « API Gateway » pour gérer le cycle de vie des API et protéger l'accès aux services Web, et « Syncplicity » pour la synchronisation et le partage sécurisés des fichiers.

92085 Paris-La Défense France

https://www.axway.com/fr

B<>COM

N

b<>com est un centre d'innovation privé conçu pour accélérer l'innovation dans les technologies numériques.

35530 Cesson-Sévigné France

http://www.b-com.com

BALABIT

Éditeur de solutions de gestion des accès privilégiés et de gestion des logs, Balabit permet aux entreprises de réduire les risques de failles de données liées à des comptes privilégiés.

92300 Levallois-Perret France

http://www.balabit.com

BARRACUDA NETWORKS

Sécurité Réseau/Infra avec protection complète du périmètre sur tous les vecteurs d'attaques. Firewall Next Gen - Web Application Firewall - Sécurité Email - VPN - Reverse Proxy - Etc.

92974 Paris-La Défense France

https://barracuda.com

BEEMO TECHNOLOGIE

N

Beemo Technologie propose des solutions complètes et fiables pour assurer la sauvegarde des données et la reprise d'activité en cas de sinistre. Solution 100 % française.

34470 Pérols France

http://www.beemotechnologie.com

BERTIN IT

H

Bertin IT propose des solutions d'anticipation des menaces cyber et de détection de fuites de données (MediaCentric) et une passerelle de sécurisation des interconnexions de réseaux (CrossinG).

78180 Montigny-le-Bretonneux France

http://www.bertin-it.com

BETA SYSTEMS

Logiciels de gestion des data-centers et de la sécurité informatique : sécurisation des procédures de traitement des données et de la gouvernance d'entreprise basée sur l'identité & l'accès utilisateur.

94200 Ivry-sur-Seine France

BEWARE CYBERLABS

Solutions de formation et d'entraînement à la cybersécurité, de cyber-déception, de génération de trafic, de scan de vulnérabilités et de pentesting développées en France.

33000 Bordeaux France

https://www.beware-cyberlabs.eu

BEYONDTRUST

BeyondTrust propose une offre PAM intégrée alliant sécurité et productivité : gestion des sessions, des comptes privilégiés et des droits sur endpoints/serveurs, cartographie des comptes & assets etc.

75012 Paris France

https://www.beyondtrust.com/fr

BE-YS SOFTWARE

Nous proposons une gamme outils en SAAS : de Customer Identity Access Management (Be-e IAM) ; d'échanges et traitement de données (Be-e Exchange) ; d'Api Management (GexRT).

63967 Cedex 9 Clermont-Ferrand France

https://www.be-ys-software.com

BITDEFENDER

Bitdefender est un leader mondial de cybersécurité qui fournit des solutions de pointe en matière de prévention, de détection et de réponse aux menaces.

92120 Montrouge France

https://www.bitdefender.fr

BLOCKPROOF

Blockproof est un logiciel en ligne pour la mise en conformité RGPD qui convient à différents types de profils.

31400 Toulouse France

https://blockproof.fr

BMC SOFTWARE

N

BMC SecOps réunit grâce à un portail intégré et automatisé, la Sécurité et les Opérations IT pour réduire les risques, cerner les priorités et les vulnérabilités et répondre à toutes les violations.

92931 Paris-La Défense Cedex France

http://www.bmc.com/it-solutions/secops-security-operations.html

BOLDON JAMES

Boldon James est un éditeur de logiciels leader dans le domaine de la classification de données et de la sécurisation de messagerie, applicable pour la conformité aux réglementations RGPD, LPM, II 901.

92400 Courbevoie France

http://www.boldonjames.fr

BOX

Box, l'entreprise de gestion de contenu dans le cloud qui permet de révolutionner la façon de travailler en connectant en toute sécurité les personnes, leurs informations et leurs applications.

75008 Paris France

http://www.box.com

BRAINWAVE GRC

H

Brainwave Identity GRC, solution d'Identity Analytics, est dédiée à l'audit et au contrôle des droits d'accès ainsi qu'à l'analyse des cyber risques dans les systèmes d'information.

92600 Asnières-sur-Seine France

CA TECHNOLOGIES

N

Les solutions de sécurité de CA Technologies permettent d'assurer la sécurité du digital tout en ouvrant les portes à l'expérience utilisateur.

92914 La Défense France

http://www.ca.com

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique) H Adhérents Hexatrust

CAILABS

Solution de sécurisation des liaisons en fibre optique très haut débit (10 Gb/s ou plus), par une technique unique d'obfuscation modale des données et détection innovante des tentatives d'intrusion.

35200 Rennes France
http://www.cailabs.com

CECURITY.COM N

Avec ses offres de dématérialisation, d'échanges sécurisés et de conservation, Cecurity.com garantit à ses clients la sécurité, la confidentialité, l'intégrité et la traçabilité de leurs données.

75009 Paris France
https://www.cecurity.com

CERTIGNA

CERTIGNA, prestataire de service de confiance et autorité de certification propose des solutions d'authentification, de chiffrement, de signature et d'horodatage électronique conformes eIDAS et RGS.

59650 Villeneuve d'Ascq France
https://www.certigna.con

CERTINOMIS N

Solution complète pour externaliser votre PKI : à partir de 50 identités, pilotez par une IHM Web et/ou des webs services la gestion de vos certificats, logiciels ou sur carte à puce et clef USB.

94673 Charenton-le-Pont Cedex France
https://www.certinomis.fr

CHAMBERSIGN FRANCE

Autorité de certification, ChamberSign garantit l'identité numérique des personnes physiques et morales. Tiers de confiance, elle délivre des certificats électroniques conforme eIDAS et RGS.

69002 Lyon France
https://www.chambersign.fr

CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies fournit exclusivement des solutions de sécurité de pointe qui protègent les entreprises des cyberattaques.

92200 Neuilly-sur-Seine France
http://www.checkpoint.com

CHECKMARX

Éditeur de solutions de sécurité applicative permettant la conception d'applications sécurisées sans retarder le cycle de développement. Reconnu leader par le MQ Gartner 2020 en AST.

92200 Neuilly-sur-Seine France
https://www.checkmarx.com

CISCO SYSTEMS FRANCE

Cisco propose une offre réseau et de sécurité à la fois intégrée, automatisée, ouverte et facile d'utilisation.

92130 Issy-les-Moulineaux France
https://www.cisco.com/c/fr_fr/index.html

CITALID

Citalid propose un produit permettant aux RSSI et Risk Managers de quantifier leurs risques cyber, puis de construire une politique d'investissements de défense rationalisée, efficace et rentable.

92300 Levallois-Perret France
https://www.citalid.com

CLOUD ECO

Spécialiste des PME, Cloudeco vous conseille dans la sécurisation de vos équipements fixes (PC/serveur) et mobiles (téléphones/tablettes) grâce à ses solutions de sauvegarde, d'antivirus et firewall.

93210 Saint-Denis France
http://cloudeco.fr

COFENSE

Cofense® fournit des solutions de détection et de réponse au phishing. Nous misons sur un réseau de personnes de 25M rapports Phish suspects, et la technologie, aux attaques d'arrêt rapide.

365x24x7 Londres Royaume Uni
https://www.codefense.com

CYBELIUS

Première société française dédiée à la cybersecurité des systèmes industriels, nous proposons plusieurs offres de produits et de services et notamment CyPRES solution de détection des cyberattaques.

69002 Lyon France

CYBERARK

Entreprise spécialiste de la sécurité des accès à privilèges, les infrastructures et les outils dans l'entreprise, le cloud et à travers le réseau DevOps.

92400 La Défense France
https://www.cyberark.com

CYBEREASON

Cybereason propose une solution complète de prévention et de détection basée sur l'analyse comportementale, et intégrant des moteurs Antivirus, NGAV, Anti-Ransomware, Anti-Fileless Malware Prevention, EDR, XDR, et des capacités forensics complètes. Nous donnons une visibilité sans précédent et fournissons la puissance nécessaire pour prévenir, détecter et remédier aux attaques les plus avancées.

75008 Paris France
www.cybereason.com

CYBERNETECH SAS

CyberDetection SIEM propose la surveillance de l'activité interne et externe du système d'information de votre entreprise, à travers son logiciel software as a service (SAAS).

6210 Mandelieu France
http://www.cyberdetection.net

CYBERRES MICRO FOCUS

Application Security - DevSecOps : Fortify. Security Operations & Analytics : ArcSight & Interset. Data Governance & Protection: Voltage. Identity and Access Management - Zero Trust : NetIQ.

92098 Paris La Défense Cedex France
http://www.cyberres.com

CYBERWATCH H

Éditeur français, notre logiciel comporte 2 modules : supervision de vulnérabilités (CVE) ; gestion des conformités (règles de durcissement, PSSI...). On Premise, avec/sans agent ou déconnecté.

75008 Paris France
https://www.cyberwatch.fr

CYBONET

Cybowall, une plate-forme de détection et de réponse aux menaces conçue pour les petites et moyennes entreprises (PME). Combinant à la fois l'accessibilité et la fonctionnalité.

3190501 Haifa Israël
http://www.cybonet.com

CYNET - HOLISTIC SECURITY SIMPLIFIED

Cynet est une plateforme de sécurité qui protège les organisations contre les violations par découverte et atténuation automatiques des menaces,- durant toutes les étapes d'attaque dans tout le SI.

92200 Neuilly-sur-Seine France
https://www.cynet.com

DANTOOIN

Solution d'anticipation, prévision et lutte en Cyber-sécurité/Cyber-défense liant l'IA et les Données.

44000 Nantes France
http://dantoo.in

DARKTRACE

l'Enterprise Immune System utilise des algorithmes d'intelligence artificielle qui imitent le système immunitaire humain et permettent de défendre les réseaux d'entreprise de tout type et toute taille.

75008 Paris France
https://www.darktrace.com

DELL TECHNOLOGIES

Pour garantir la disponibilité des données où qu'elles se trouvent, Dell Technologies propose des solutions, des logiciels et des appliances pour protéger, sauvegarder et restaurer les données.

34000 Montpellier France

www.delltechnologies.com/fr-fr/

DHIMYOTIS N

Tiers de confiance et autorité de certification reconnue au niveau européen, Dhimyothis sous Certigna sécurise les transactions électroniques, protège et authentifie les identités et informations.

59650 Villeneuve-d'Ascq France

http://www.dhimyotis.com

DIGITAL GUARDIAN

Digital Guardian est la seule plateforme de sécurité véritablement axée sur les données conçue pour empêcher le vol de ces dernières.

EC3V 1LP London Royaume-Uni

https://digitalguardian.com/fr

DIGITEMIS SOFTWARE N H

Make IT Safe est une plateforme modulaire (hébergée en France) qui s'adapte à tous vos besoins en cybersécurité et conformité, ainsi qu'à divers référentiels (RGPD, CCPA, Sapin 2, ISO 27001, HDS, LPM).

44400 Nantes France

https://www.digitemis.com

DISKYVER

Diskyver propose des solutions SaaS de machine learning qui vous permettent de faire les bons choix pour vous protéger contre les risques planant sur la voix sur IP.

59800 Lille France

https://www.diskyver.com

DMARC EXPERT

Le protocole DMARC permet de lutter contre la fraude au président et contre l'usurpation de marque ou de l'identité d'un de vos utilisateurs. Nous simplifions sa mise en place qui peut être complexe.

76000 Rouen France

https://www.dmarc.com

DOCAPOSTE ARKHINEO N H

Nous proposons un service d'archivage électronique à valeur probante en mode SaaS. Leader depuis 20 ans, nous garantissons l'intégrité, la pérennité et la conformité des documents électroniques.

75009 Paris France

https://www.arkhineo.com

DOCTOR WEB FRANCE

Éditeur des solutions antivirus Dr.Web, sécurisant postes, serveurs, passerelles Internet, messageries, appareils mobiles. Expertise Linux, Android, Windows. Recherche en déchiffrement. Mode Saas.

67100 Strasbourg France

http://www.drweb.fr

EDSI N

EDSI est spécialisée en sécurisation des développements embarqués reposant ou non sur du HW dédié à la sécurité : Cartes à puce, Hardening logiciel, Cryptographie, etc.

35510 Cesson-Sévigné France

http://edsisecurity.com

EFFICIENTIP H

EfficientIP, fournisseur français de solutions DDI (DNS, DHCP, IPAM), aide les organisations à accroitre leur efficacité à travers des réseaux agiles, sécurisée et fiables.

92250 La Garenne-Colombes France

http://www.efficientip.com/fr

EGERIE SOFTWARE H

EGERIE est éditeur de logiciels spécialisés dans la gestion intégrée des cyber-risques et le pilotage de la cybersécurité.

83000 Toulon France

https://www.egerie-software.com

EM2B

BotProtector est une solution de détection et de protection contre les attaques des bots malveillants.

44000 Nantes France

https://www.botprotector.io

ENTRUST DATACARD

Solutions on-premise, cloud, as a service pour la PKI, les certificats numériques, la signature électronique, l'IAM, les HSM, l´IoT et l´émission de titres d´identification.

45400 Semoy France

https://www.entrustdatacard.com

EQUISIGN N

Equisign propose 2 solutions : une offre de transfert sécurisé de fichiers utilisée par plus d'un million d'utilisateurs ; une offre de Lettre recommandée électronique qualifiée par l'Anssi.

92057 Paris La Défense France

http://www.equisign.fr

ERCOM H

Ercom, société française filiale du groupe Thales, développe des solutions simples et certifiées pour sécuriser les terminaux, communications mobiles, messageries instantanées et échanges de données.

78140 Vélizy-Villacoublay France

https://www.ercom.fr

ESET FRANCE

Au-delà du simple antivirus, ESET propose une gamme complète de solutions pour protéger le patrimoine numérique des entreprises : Machine learning, SandBoxing, EDR et Cyber Threat Intelligence.

93320 Les Pavillons-sous-Bois France

http://www.eset.com/fr

ETAS SAS

Premier fournisseur au monde de solutions de sécurité dans le domaine des systèmes embarqués, des communications M2M, de l'Internet des objets et des véhicules connectés.

93404 Saint-Ouen France

https://www.escrypt.com/en

EURAFIBRE

Solutions d'interconnexion de sites distants via MPLS/VPN jusqu'à 10 Gb/s en fibre optique (AS35625). Sécurisation des données et qualité de service (QoS).

59650 Villeneuve d'Ascq France

https://www.eurafibre.fr

EUROEDI N

Éditeur spécialisé dans l'EDI et la facturation électronique, nos solutions logicielles et services sont conçus en France pour traiter, transférer et archiver légalement vos données B2B ou B2G.

33840 Captieux France

http://www.euroedi.com/

EVINA

DCB protect est une solution SaaS protégeant les opérateurs télécom & annonceurs de paiements frauduleux sur la facture opérateur. - ProxyPony est un réseau mondial de proxys 4G disponible dans 17 pays.

78000 Versailles France

https://www.evina.fr

EXER

Grâce à un catalogue de solutions unique et à une équipe d'experts qualifiés, Exer est le distributeur qui vous soutiendra dans tous vos projets sécurité, wifi et réseau.

59160 Lille France

https://www.exer.fr/

EC Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique) H Adhérents Hexatrust

F5 NETWORKS

F5 offre des solutions de sécurité et Cloud qui permettent aux entreprises d'adopter l'infrastructure applicative de leur choix sans pour autant sacrifier la vitesse ni le contrôle de leurs opérations.

92150 Suresnes France

https://f5.com/fr

FACTORYTHINGS N

VigiCenter est un boitier IP destiné au monitoring et à la sécurisation des datacenters. VigiLock est une solution logicielle permettant de coordonner les règles d'accès et de gestion du datacenter.

45430 Checy France

http://www.vigilock.com

FEEDER

Offre vidéosurveillance, écosystème et les acteurs du marché de la vidéosurveillance.

13127 Vitrolles France

http://www.feeder.fr

FEITIAN TECHNOLOGIES

Sécurité digitale comprenant PKI, Java Cards, Lecteurs de carte à puce, OTP, Fido U2F, Dongles de protection logicielle.

06560 Valbonne France

http://www.ftsafe.com

FIREEYE

FireEye est spécialisé dans la cybersécurité axée sur la cyberveille. La plate-forme de FireEye combine des technologies de sécurité innovantes, des services de cyberveille d'envergure internationale.

92120 La Défense France

http://www.fireeye.fr

FLASHPOINT

La plateforme Flashpoint Intelligence permet l'accès aux rapports de renseignements et aux données du Deep & Dark Web Forum data.

États-Unis

http://www.flashpoint-intel.com

FLEXERA

Évaluez votre logiciel via une base de données de 23 000+ applications pour identifier vos vulnerabilities et obtenez des correctifs de sécurité personnalisables pour votre logiciel tiers.

92671 Paris France

https://www.flexera.com

FORECOMM

BlueFiles permet de transmettre des documents sensibles en ligne avec simplicité. Transfert sécurisé, envoi chiffré et contrôle distant : une solution zero knowledge pour une confidentialité garantie.

93160 Noisy-le-Grand France

ps://mybluefiles.com

FORGEROCK

ForgeRock, le leader sur le marché de la gestion de l'identité numérique, transforme la manière dont les entreprises établissent des échanges sécurisés entre les personnes, les services et les objets.

75008 Paris France

https://www.forgerock.com

FORTINET

Fortinet offre à ses clients une sécurité sans compromis pour relever les défis de sécurité les plus critiques au sein des environnements réseaux, applicatifs, cloud ou mobiles.

92911 Paris-La Défense Cedex France

http://www.fortinet.fr

F-SECURE

Fondée en 1988, F-Secure est une entreprise finlandaise spécialisée en cybersécurité, qui protège depuis plus de trente ans des dizaines de milliers d'entreprises et millions de particuliers.

92500 Rueil-Malmaison France

https://www.f-secure.com/fr_FR/web/business_fr/home

FULL IP SOLUTIONS

Représentant exclusif pour la France & autres pays francophones de éditeurs/constructeurs spécialisés sécurité & cybersécurité : Clavister, MobilityGuard, Cryptshare, Yubico, OnlyOffice, Feitian, etc.

78306 Poissy France

http://www.fullipsolutions.com

G DATA SOFTWARE

La solution multi-couche G DATA intègre tous les éléments nécessaires à la protection des entreprises. Antimalware, gestion des endpoints, filtrage Internet et email sont réunis dans une même console.

92120 MONTROUGE France

GATEWATCHER N H

Gatewatcher est l'éditeur du système de détection d'intrusions et de menaces avancées Trackwatch®. Cette solution a obtenu le Visa de Sécurité pour la Qualification Elémentaire délivré par l'ANSSI.

75008 Paris France

http://www.gatewatcher.com

GEMALTO

La gamme de solutions SafeNet de Protection des Données et des Identités de Gemalto offre des solutions de chiffrement, de gestion de clés et d'authentification forte et gestion des accès.

92190 Meudon France

http://safenet.gemalto.com

GFI N

Keenaï est un SIEM, développé en France, permettant de couvrir les cas d'usage que sont la Cyber Défense, la lutte contre la Fraude, les contrôles RGPD et la défense des installations industrielles.

93400 Saint-Ouen France

gfi.world/fr-fr

GLOBALSIGN

Prestataire de services d'identité aux solutions PKI évolutives sur le cloud pour les entreprises devant gérer la sécurité de leurs transactions commerciales, communications et offres de contenu.

75010 Paris

https://www.globalsign.com

GROUPE IMPRIMERIE NATIONALE N

Pass'IN est un service clé en main de gestion des identités professionnelles. Pass'IN protège le patrimoine, les systèmes, les applications et les données contre tout accès non autorisé.

75116 Paris France

http://www.imprimerienationale.fr

GS2I

i-Guard est le premier logiciel EDR (Endpoint Detection & Response) Européen et Français. Son intelligence artificielle agit seule et bloque menaces connues et inconnues directement sur les Endpoints

75010 PARIS France

https://www.gs2i.fr

GUARDICORE

Guardicore Centra assure la sécurité des Datacenters et du cloud de votre entreprise en contrôlant par de la micro segmentation et une visibilité en temps réel jusqu'au niveau des process applicatifs

78150 Rocquencourt France

http://www.guardicore.com

GUIDANCE SOFTWARE INC

Editeur d'EnCase, déployé sur 35 millions d'Endpoints à travers le monde, Guidance Software est le leader du marché de l'Endpoint Détection Response (EDR) et l'acteur de référence de l'investigation.

92400 Courbevoie France

HACKUTY

RISK BASED VULNERABILITY MANAGEMENT COCKPIT

Hackuity's platform aggregates and normalizes all your security assessment practices, whether automated or handmade.

69009 Lyon France

https://www.hackuity.io

HAREL SYSTEMS

Protection des données de gestion commerciale.

75116 Paris France

https://www.helloharel.com

HARFANGLAB N H

HarfangLab, le seul EDR français Full On Premise ou en Cloud qui préserve la souveraineté numérique de ses clients.

75008 Paris France

https://www.harfanglab.fr

H-IAPPS

NBH est une solution SaaS de formation en continu sur le comportement des utilisateurs face aux risques informatiques qu'encours les entreprises. Nous agissons en cybersécurité et RGPD.

80440 Boves France

https://neverbehacked.com

HID GLOBAL

Leader mondial des solutions d'identité sécurisée, HID Global délivre des solutions de contrôle d'accès et des transactions, d'impressions, de suivi (RFID…), d'authentification, de protection, etc.

92150 Suresnes France

https://www.hidglobal.fr

HP INC

HP Wolf Security est une approche disruptive de la sécurisation des postes de travail. Elle renforce votre sécurité tout en s'intégrant dans votre écosystème de sécurité en place.

92190 Meudon France

https://hp.com/fr/wolf

HYPERVISION TECHNOLOGY N

Yuno, plate forme d'orchestration de réponse aux menaces ou attaques afin d'accélérer le traitement d'incident et de protéger la continuité d'exploitation. Pas de programmation requise, drag and drop.

75008 Paris France

http://www.hypervision-technology.com

IBM FRANCE N

Notre offre est développée autour de 3 axes, contrôler et améliorer la sécurité du SI. Le 1er, l'écosystème mondial d'IBM. Le 2e, les solutions de sécurité. Et, le 3e, notre offre de services.

92275 Bois-Colombes France

https://www-03.ibm.com/security/fr-fr/solutions

IDACTIS

La suite logicielle ID>Security permet de contrôler et sécuriser les accès aux postes de travail et aux applications en sécurisant la gestion des mots des mots de passe des utilisateurs.

14400 Maisons France

http://www.idactis.com

IDECSI

Solution experte de la sécurité des données dans les outils collaboratifs Microsoft 365 et on premise. Une plateforme de Monitoring, Detection, Alerting, Remediation et un engagement utilisateur fort.

75008 Paris France

https://www.idecsi.com

IDNOMIC N H

IDnomic est le leader européen de la protection et la gestion des identités numériques. IDnomic fournit des services de PKI pour l'identification des personnes, des terminaux et des objets connectés.

92130 Issy-les-Moulineaux France

http://www.idnomic.com

I-GUARD

Fondée en 2014 à Paris, i-Guard est une société française innovante. Créateur du premier logiciel EDR européen et intelligent, idéal pour les TPE, PME et organismes désirant protection et simplicité.

75010 Paris France

https://www.i-guard.eu/

ILEX INTERNATIONAL N H

Suite Ilex Identity : offre de gestion des identités et des habilitations - Suite Ilex Access : offre de gestion des accès (authentification renforcée, WAM, fédération d'identité, eSSO, Mobile SSO).

92600 Asnières-sur-Seine France

https://www.ilex-international.com

IMPERVA

Les solutions d'Imperva permettent de détecter les risques et vulnérabilités, protéger l'information là où elle est utilisée (sur site et Cloud) et d'être en conformité avec les réglementations.

92800 Puteaux-La Défense France

http://www.imperva.com

IN GROUPE

IN Groupe, entreprise de souveraineté numérique, s'appuie sur les technologies de Nexus pour la production et la gestion d'identités de confiance sécurisées pour les personnes et les objets.

75016 Paris France

INFOBLOX

Infoblox delivers Control and Security from the Core.

Increase business speed, agility, and efficiency by taking charge of your core network services and security.

1019 GM Amsterdam Pays Bas

http://www.infoblox.com

INVENIS N

Invenis est un logiciel d'analyse Big Data, permettant l'exploration de données, la détection de signaux faibles et le reporting. Experts en Data Science, nous proposons également un accompagnement.

75011 Paris France

https://invenis.co

INWEBO TECHNOLOGIES N H

Service d'authentification forte français pour la sécurisation des accès et des transactions. Nous protégeons les applications VPN, SSO, PAM, IAM, métier et grand public.

75009 Paris France

https://www.inwebo.com

ISIT

ISIT offre une stratégie cybersécurité globale (produits & services) pour les systèmes Temps Réel Critiques, couvrant aussi bien les logiciels développés en interne que les codes Open Source.

31830 Plaisance du Touch France

http://www.isit.fr

ITRUST H

ITrust propose des services et solutions en cybersécurité : IKare (scanner de vulnérabilités) ; Reveelium (SIEM, UEBA) ; ACSIA EDR (surveillance locale des événements) ; SOC souverain a la demande.

31100 Toulouse France

https://www.itrust.fr

IVANTI

Les solutions de sécurité Ivanti offrent une protection multiniveau : gestion des correctifs et vulnérabilités, whitelisting, contrôle des applications, gestion des privilèges, protection des données.

92979 Paris-La Défense France

http://www.ivanti.fr

IXIA

Ixia propose des solutions de test, de visibilité et de sécurité afin de valider, renforcer et optimiser vos produits, applications et réseaux physiques et virtuels.

91300 Massy France

http://www.ixiacom.com

JUNE-FACTORY

AUDITOOL, un logiciel d'audit pour piloter simplement la conformité SSI d'une organisation. MIOT, une solution d'IOT cybesécurisé (device et dashboard) pour gérer un parc d'engins de chantier.

31670 Labège France

http://www.june-factory.com

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique) H Adhérents Hexatrust

JUNIPER NETWORKS

SDSN est une plateforme réseau sécurisée, associée à des services cloud à la fois flexibles, évolutifs et sécurisés qui facilite la mise en place de politiques de sécurité axées sur le workflow métier.

92200 Neuilly-sur-Seine France
https://www.juniper.net

KASPERSKY LAB FRANCE

Kaspersky Lab propose des solutions de « Threat Intelligence » et de sécurité informatique pour protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs.

92500 Rueil-Malmaison France
https://www.kaspersky.fr

KAZEKO

Welcomr est la nouvelle solution de gestion des accès pour les smart buildings : accueil holistique des visiteurs, expérience utilisateur sans contrainte, 100 % dématérialisée et de haute sécurité !

37000 Tours France
https://welcomr.fr

KEEEX N

KeeeX offre la signature numérique embarquée universelle. Tout format de fichier porte preuves d'intégrité, signatures, dates, liens externes. Confidentialité ultime et conformité RGPD, eIDAS.

13013 Marseille France
https://keeex.me

KEMP FLOWMON

Kemp Flowmon offre une solution innovante pour la sécurité et visibilité réseau. La solution Flowmon peut être deployée comme matériel, comme appliance virtuelle (VMware, KVM, Hyper-V) ou même en Cloud.

61600 Brno République tchèque
http://www.flowmon.com

KEYSIGHT

Keysight offre des solutions pour la sécurité des réseaux IT et OT, de la conception électronique, du test, de la fabrication électronique et de l'optimisation de réponse aux incidents IT.

9141 Les Ulis Cedex France
https://www.keysight.com

KIUWAN

Solution d'analyse statique du code en mode SaaS ou On Premise pour détecter les failles de sécurité, les défauts de qualité et surveiller les composants externes embarqués.

78000 Versailles France
http://www.kiuwan.com

KIWI BACKUP N

Kiwi Backup propose deux solutions de sauvegarde de données externalisée : Kiwi Backup et Kiwi Santé (données de santé avec hébergement HDS). Disponible en marque blanche. Linux, Windows et Mac.

68200 Mulhouse France
http://www.kiwi-backup.com

KOBIL

Fondé en 1986, KOBIL est présent en France. KOBIL sécurise l'identité sur l'ensemble des plateformes, avec mAST, et supporte la directive DSP2. Parmi nos clients : Migros Bank, Société Générale, USB.

67547 Worms Allemagne
http://www.kobil.com

KONTROL SAS

Plateforme d'Encryption As A Service pour éditeurs SaaS qui souhaitent faire certifier Anssi leur service cloud en garantissant sécurité, confidentialité et intégrité des données à leurs utilisateurs.

75017 Paris France
https://www.tanker.io

KUB CLEANER H

KUB-CLEANER appartient au Groupe RAS, il est leader sur le marché de la sécurisation des échanges de données entre vos périphériques USB et vos réseaux internes. En cours de qualif ANSSI.

92110 Clichy France
http://kub-cleaner.com

LINAGORA N

Des solutions clés en main pour : authentifier les personnes et les machines, assurer la confidentialité au sein de votre SI, dématérialiser vos documents grâce à la signature électronique sécurisée.

92800 Puteaux France
https://linagora.com

LMBA / GEDIX N

La solution GEDIX, conçue en France, permet la communication et l'acquisition de données sécurisées avec les moyens industriels dans les réseaux industriels. #DNC #MDC.

69003 Lyon France
https://www.gedix.fr

LOGMEIIN

LastPass - Coffre Fort + Single Sign-On (SSO) + MFA. Gestion des mots de passe en toute simplicité. Améliorez la sécurité et l'hygiène des mots de passe de vos employés sans compliquer l'utilisation ni augmenter la charge administrative.

75018 Paris France
https://www.lastpass.com/fr

LOGPOINT

Solution européenne de SIEM et Log Management, LogPoint permet d'assurer la mise en conformité réglementaire, de déployer une défense contre les menaces de sécurité et d'optimiser les opérations IT.

92500 Rueil Malmaison France
https://www.logpoint.com/fr

LOOKOUT

Lookout, alimentée par plus de 160 millions de mobiles, identifie les risques (Phishing, Malware, Sideloading, Conformité applicative...) et s'intègre parfaitement aux standards du marché.

75016 Paris France
https://www.lookout.com/fr

LYBERO.NET

CryptnDrive, partage web de fichiers intégrant un séquestre numérique. Chiffrement de bout en bout, aucun logiciel client nécessaire; Lybcrypt SDK pour intégrer le chiffrement dans votre appli web.

54603 Villers-lès-Nancy Cedex France
https://lybero.net

MAILINBLACK N H

La solution MailInBlack permet de protéger efficacement la messagerie des spams/virus et de retrouver une boîte mail propre. Elle offre une sécurité maximale et un gain de temps et de productivité !

13006 Marseille France
https://www.mailinblack.com/

MALWAREBYTES

Malwarebytes, ENDPOINT PROTECTION et INCIDENT RESPONSE, technologie multicouche, protège les entreprises contre les attaques et répare les dommages non détectés par les autres solutions de sécurité.

75009 Paris France
https://fr.malwarebytes.com

MAPREUVE

MaPreuve est le premier site de confiance permettant de protéger et certifier juridiquement et immédiatement un document numérique.

59650 Villeneuve d'Ascq France
https://www.mapreuve.com

MARKET ESPACE

TrackUp est une solution qui permet de surveiller des adresses emails pièges certifiées insérées dans une base de données. Le déclenchement d'alertes automatiques permet de détecter le vol des données.

59290 Wasquehal France
https://www.track-up.com

MCAFEE S

McAfee Security Connected sécurise les postes de travail (ENS), données (DLP), réseaux (IPS NSP); la gestion du SOC (SIEM ESM); Web filtering (MWG), Sandbox (ATD) interconnectés via OpenDXL.

92800 Puteaux France

https://www.mcafee.com/fr

MICROSOFT N

L'offre Microsoft assure la sécurité globale du Système d'information sur les aspects détection, protection et réponse en s'appuyant sur la puissance du Cloud et de l'Intelligence artificielle.

92130 Issy-les-Moulineaux France

https://www.microsoft.com/fr-fr

MOBILE PROCESS

Solutions pour l'ensemble des terminaux mobiles de l'entreprise : push mail sécurisé ; Mobile Device Management ; sécurisation des terminaux ; accès sécurisé aux données de l'entreprise.

57070 Metz France

http://www.mobile-process.com

MOBILEIRON

MobileIron est le leader en UEM. Notre offre a bien évoluée depuis plusieurs années par le rajout de solutions de sécurité du mobile, de sécurisation des applications cloud et de ZSO.

92200 Neuilly-sur-Seine France

http://www.mobileiron.com

MOSKITOS

Moskitos est l'éditeur de Crosscut®, plateforme d'intégration et d'APIs management pour connecter rapidement et en toute sécurité la data, les API, les applications et accélérer l'innovation numérique

92300 Levallois-Perret France

https://www.moskitos.fr

MYDPO N

myDPO participe de manière active à la création du patrimoine informationnel des entreprises, en rendant accessible la gestion des données personnelles pour la mise en conformité RGPD des entreprises.

75009 Paris France

https://mydposolution.com

MYQ FRANCE

7 solutions en 1 : Gestion de périphérique, gestion des systèmes, gestion d'impression, impression mobile (BYOD), gestion des scans, panneau de contrôle, et gestion de parcs.

75010 Paris France

https://www.myq-solution.com/fr/home

NAMESHIELD H

DNS Premium est une infrastructure robuste et fiable, basée en France, couplée à un réseau anycast, aux diverses fonctionnalités : DNSSEC - filtrage anti-DDoS - Failover - GeoIP - Statistiques fines.

75002 Paris France

https://www.nameshield.com

NANOCODE

Easylience® est une solution numérique dédiée aux métiers de la gestion de crise. Accompagnement sur l'évolution des pratiques opérationnelles (ISO 223xx) et dans la conduite d'exercices de crise.

35510 Cesson Sévigné France

https://www.nanocode-labs.com

NCIPHER SECURITY

Les modules de sécurité matériels (HSM) nShield sécurisent les processus de traitement cryptographique, de génération de clés, de protection, de chiffrement et autres.

CB1 2GA Cambridge Royaume-Uni

https://www.ncipher.fr/

NEOWAVE H

Les solutions ID 2.0 sont des tokens USB et des cartes à puce avec leur middleware pour le contrôle d'accès logique.

Les produits FIDO U2F sont des dispositifs 2FA pour sécuriser les accès Web.

13120 Gardanne France

http://www.neowave.fr

NETHEOS

La solution SaaS de Netheos sécurise et automatise les parcours de souscription fortement réglementés des banques et des assurances, en conciliant notamment KYC et expérience utilisateur.

34000 Montpellier France

https://www.netheos.com

NETSCOUT

Défense anti DDoS automatique intelligente pour les réseaux d'opérateurs et d'entreprise, dans le Cloud ou sur site, virtualisée ou boitiers. Defense contre les APT rapide et automatisée. Forensic.

91300 Massy France

http://www.arbornetworks.com

NETSKOPE

Netskope Security Cloud: Les services informatiques peuvent localiser, comprendre et sécuriser leurs données sensibles présentes dans leurs environnements SaaS, IaaS et Web (Web Proxy).

EC1V 4JP London Royaume-Uni

https://www.netskope.com

NETWORK USERS INSTITUTE

Notre solution de Cybersécurité met en scène le DNS RPZ comme le premier rempart à la Cybercriminalité, soit 95 % de couvert en quelques minutes.

76100 Rouen France

https://nui.fr

NETWRIX

Une visibilité omniprésente sur le comportement des utilisateurs, les configurations système et la sensibilité des données sur les infrastructures informatiques hybrides afin de protéger les données.

75000 Paris France

https://www.netwrix.fr

NEXTDAY.VISION

Mieux sécuriser sans mot de passe- OtpOne API est la solution clé en main pour remplacer les mots de passe dans les applications d'entreprise par un login simple ou multi-facteur sans mot de passe.

2822 Courroux Suisse

https://www.otpone.com

NEXUS GROUP

Nexus est un groupe suédois, filiale de IN Groupe. Nos solutions Nexus Smart ID couvrent l'ensemble des besoins pour une gestion complète des identités numériques et des accès logiques et physiques.

75016 Paris France

http://www.nexusgroup.com

NIS

NIS offre le portefeuille de Gemalto/SafeNet de protection des identités et des données, permettant aux organisations d'être protégées, conformes et en contrôle, où que leurs activités les mènent.

13420 Gemenos France

http://www.nis-infor.com/fr

NORMASYS

NUMERISQUE est une solution cyber-sécurité hybride IDS/IPS qui applique les technologies de l'Intelligence Artificielle aux processus décisionnels.

75009 PARIS France

https://www.normasys.com

NORMATION H

Solution de management des configurations systèmes : configuration automatique du socle système ; audit continu des configurations et des règles de sécurité ; correction automatique des écarts.

75003 Paris France

https://www.rudder.io/fr

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique) H Adhérents Hexatrust

NOZOMI NETWORKS

Nozomi Networks est un spécialiste des solutions de Visibilité et de Sécurité en environnements Industriels (OT & IoT).

6850 Mendirisio Suisse

https://nozominetworks.com

NTX RESEARCH

Solutions : XCA (authentification forte des personnes et objets par tables de codage), PKI2.0 (certificats clients).
Logiciels : Win RGPD Manager (conformité RGPD), Win Security Manager, Smart City.

75116 Paris France

https://ntx-research.com/fr

NUCLEON SECURITY

Nucleon Security, spécialiste de la cybersécurité qui redéfinit la protection des endpoints et la gestion de vulnérabilité grâce à sa plateforme Nucleon Smart Endpoint.

921706 Vanves France

https://nucleon-security.com

NXO

Bénéficiez d'experts pour vous aider à définir une stratégie de sécurité de votre SI et vous accompagner de bout en bout sur les solutions de sécurité les plus pertinentes en phase avec vos objectifs.

92500 Rueil Malmaison France

https://www.nxo.eu

OKTA

Okta est le leader de la gestion des identités et des accès. La plateforme Okta Identity Cloud offre des fonctionnalités de SSO, MFA, Workflows, sécurisation des APIs, fédération d'annuaires, PAM, IGA.

92800 Puteaux France

http://www.okta.com/fr

OLFEO

N H

Olfeo est le leader français de la sécurité web. Nous accompagnons depuis plus de 17 ans les entreprises exigeantes dans la sécurisation, l'analyse et l'optimisation de leur flux web.

75001 Paris France

https://www.olfeo.com

ONE IDENTITY

Gouvernance des identités et des accès, gestion des données non structurées, gouvernance et gestion des comptes à privilèges, sécurisation et administration de l'Active Directory, Log Management.

92200 Neuilly-sur-Seine France

https://www.oneidentity.com/fr-fr

ONELOGIN

OneLogin, leader de l'Unified Access Management, rend simple et sécurisé l'accès des entreprises à leurs applications et à leurs données, qu'elles soient dans le cloud ou sur site.

W1F 8BH London Royaume-Uni

https://www.onelogin.com

ONETRUST

H

Leader des logiciels de gestion des programmes de protection/confidentialité des données personnelles, de sécurité, de conformité et de gouvernance, OneTrust propose des programmes de confiance dans ces domaines.

75017 Paris France

http://www.onetrust.com

OODRIVE

N H

En tant que partenaire de confiance pour la gestion des données sensibles, Oodrive propose aux professionnels des solutions Cloud de partage, de sauvegarde et de signature électronique.

75010 Paris France

https://www.oodrive.com

OPENIP

S N

Le SIP Trunk Touch permet aux entreprises de téléphoner sur Internet, en bénéficiant d'une gestion simplifiée, des sécurités anti-piratage dernières générations et de forfaits d'appels illimités.

92110 Clichy France

https://www.openip.fr

OPSWAT

Créée en 2002 OPSWAT propose 2 solutions: MetaDefender pour la prévention des menaces et MetaAccess pour le contrôle d'accès au cloud et la conformité des terminaux.

75019 Paris France

http://www.opswat.com

ORACLE

N

Construire une infrastructure Cloud et une plateforme de services offrant à ses clients une sécurité opérationnelle et efficace pour stocker leurs données et héberger leurs applications critiques.

92715 Colombes Cedex France

https://www.oracle.com/fr/security

ORSEC TECHNOLOGIES SAS

OORIGIN Audit est une sonde passive de monitoring réseaux conçue pour le Cyber Threat Hunt que l'on développe à Bordeaux ; avec intégration de la technologie Deep Packet Inspection de « Rohde & Schwarz ».

33700 Mérignac France

https://www.oorigin.fr

OVELIANE

Solution française de prévention d'attaques par le contrôle en continu de l'hygiène de la sécurité du parc de serveurs (conformité et intégrité).

92300 Levallois-Perret France

http://www.oveliane.com

OXIBOX

Oxibox est une solution de cyber-résilience qui garantit, en une seule installation, la pérennité de toutes les données de l'entreprise : postes de travail, serveurs, machines virtuelles, Cloud.

78280 Guyancourt France

https://www.oxibox.eu

PALO ALTO NETWORKS

Spécialiste de la sécurité réseau de nouvelle génération, Palo Alto Networks joue un rôle moteur dans la sécurisation des applications et la prévention des cyberfailles.

92130 Issy les Moulineaux France

https://www.paloaltonetworks.com

PARSEC

Collaborez en confidentialité et intégrité dans le Cloud grâce à PARSEC, « solution sécurisée anti-ransomware et ergonomique certifiée ANSSI », disponible en Saas et On Premise.

33160 Saint-Médard-en-Jalles France

http://www.parsec.cloud

PHISHME

PhishMe : solution humaine de lutte contre le phishing. Collecter, analyser et intervenir, nos solutions : PhishMe Simulator, PhishMe Reporter, PhishMe Triage, PhishMe Intelligence.

VA 20175 Leesburg États-Unis

https://phishme.com

PHOENIX CONTACT FRANCE

La gamme de pare-feux industriels - mGuard - permet de protéger les machines / le réseau OT des cybermenaces et de faire de la télémaintenance en toute sécurité (via des tunnels VPN).

77436 Marne la Vallée France

https://www.phoenixcontact.com/online/portal/fr

PING IDENTITY CORPORATION

Plateforme Ping Identity : Offre de gestion des Accès (Authentification Forte, SSO, Fédération d'identité, WAM, API Security) et Offre de Gestion des Identités Clients CIAM. Solutions OnPrem et Cloud.

75116 PARIS France

https://www.pingidentity.com/fr.html

PRADEO H

Leader européen dans le domaine la sécurité mobile, Pradeo propose des services innovants pour protéger les applications et les terminaux mobiles (smartphones, tablettes et objets connectés).

75116 Paris France

https://www.pradeo.com

PRIM'X TECHNOLOGIES N H

Basés sur des technologies puissantes et avancées, les logiciels de chiffrement développés par Prim'X assurent une protection globale des données contre la perte, le vol et l'espionnage économique.

69444 Lyon France

https://www.primx.eu

PROMISEC H

Promisec Endpoint Manager est une solution sans agent exclusive qui offre des fonctionnalités de visibilité intégrale, de détection, analyse et correction des anomalies.

75019 Paris France

http://www.promisec.com

PROOFPOINT

Proofpoint, spécialisé dans la cybersécurité nouvelle génération, permet aux organisations de protéger leurs données contre les menaces avancées, et de se conformer aux réglementations en vigueur.

75009 Paris France

https://www.proofpoint.com/fr

PROVE & RUN H

Prove & Run vend des briques logicielles de sécurité formellement prouvées pour protéger les systèmes connectés contre les cyberattaques à distance : ProvenCore, ProvenVisor et ProvenFilter.

75017 Paris France

http://www.provenrun.com

PYDIO N

Pydio est un logiciel de partage de fichiers pour les entreprises qui permet de gérer les accès à la donnée ainsi que ses autorisations d'accès et de partage. Pydio est conforme à la RGDP.

75003 Paris France

https://www.pydio.com

QUALYS

Qualys, Inc. (NASDAQ : QLYS) aide les entreprises à rationaliser et fédérer leurs opérations de sécurité et de conformité au sein d'une seule et même plateforme.

92400 Courbevoie

https://www.qualys.com

QUERY INFORMATIQUE

Nos solutions modulables protègent de façon optimale vos postes de travail, votre parc informatique et vos données numériques.

92700 Colombes France

https://www.query-informatique.com

QUEST SOFTWARE

L'ensemble du portefeuille de solutions logicielles Quest couvre la gestion de l'information, des terminaux, des identités et des accès, de la plateforme Microsoft, et la protection des données.

75116 Paris France

https://www.quest.com/fr-fr

RADWARE

Radware propose des solutions ADC (loadbalancing, reverse proxy, WAF) et des solutions anti-ddos on prem et cloud (detection et mitigation automatique & trafic legit garanti).

92400 Courbevoie France

http://www.radware.com

ROHDE & SCHWARZ CYBERSECURITY H

Rohde & Schwarz Cybersecurity produit des solutions pour la sécurité de l'information et des réseaux, comme des pare-feu de nouvelle génération et des logiciels pour l'analyse des réseaux.

92360 Meudon France

https://rohde-schwarz.com/cybersecurity

RSA

Cybersécurité : détection et réponse aux attaques avancées. Gestion des identités et accès utilisateurs. Réduction des risques en termes de business, fraude et cybercriminalité. GRC.

95876 Bezons France

https://www.rsa.com/en-us

RUBYCAT

PROVE IT solution de contrôle d'accès et d'audit renforcé pour les connexions sensibles au SI (prestataires, utilisateurs à privilèges…) - PAM - avec enregistrement & visualisation des sessions.

35510 Cesson-Sévigné France

https://www.rubycat.eu

SAILPOINT TECHNOLOGIES

En tant que pionnier de l'industrie et leader sur le marché de la gouvernance des identités, SailPoint assure la sécurité, l'efficacité opérationnelle et la conformité des entreprises de tout secteur.

92931 Paris-La Défense France

https://www.sailpoint.com/fr

SCASSI SOLUTIONS N

Scassi Solutions est l'éditeur des solutions HoneyNet, Auditool, Passed et de la plateforme RGPD.

31670 Labège France

http://www.scassi.com

SCHLEUPEN AG

Nos logiciels : R2C_GRC, pour la gestion des risques et GRC ; R2C_Security, pour la sécurité de l'information, aide à la mise en conformité et facilite le pilotage ISO 27001, 27005, GDPR…

76275 Ettlingen Allemagne

https://grc.schleupen.de/fr

SCPTIME N

SCPTime® met en œuvre un service de diffusion de l'heure légale (UTC) sécurisée, certifiée, précise et traçable pour « cybersécuriser » le temps (Adm, Finance, Digital, Transprt, Énergie, Ind4.0…).

38350 La Mure d'Isère France

https://www.scptime.com/fr/

SEALD

Solution de chiffrement d'emails et de documents simple et intégrée aux clients mails, utilisable même si le destinataire n'a pas la solution, et permet un contrôle a posteriori des données envoyées.

75014 Paris France

https://www.seald.io/

SEC'IT

La solution de cyberdéfense des entreprises autonome et automatisée.

34000 Montpellier France

http://www.secit.fr

SECKIOT

Seckiot, éditeur de logiciel français, sécurise les systèmes industriels & IOT grâce à ses 3 modules : cartographie des équipements, scan des vulnérabilités et détection des intrusions.

75008 Paris France

https://www.seckiot.fr

SECLAB H

DENELIS sécurise les interconnexions réseaux en masquant et isolant votre infrastructure critique, tout en permettant des échanges de données bidirectionnels. SCOOP applique cette technologie à l'USB.

34000 Montpellier France

http://www.seclab-security.com

SECLUDIT

Elastic Workload Protector protège vos applications (workloads) et données en continu avec une approche DevOps. Analysez automatiquement toutes vos failles de sécurité.

06560 Sophia Antipolis France

https://secludit.com

SECRET DOUBLE OCTOPUS

Secret Double Octopus est une solution d'authentification primée, qui remplace les Token, OTP et au final le mot de passe lui-même.

75009 Paris France
https://doubleoctopus.com

SECURE2BROWSE

Navigation Internet a distance. Laissez à vos utilisateurs un accès à distance vers un navigateur cloud ou on-premise dont seul le rendu graphique est envoyé. Supporte le filtrage URL et SSO.

CH-6312 Steinhausen Suisse
http://www.secure2browse.com

SECURE-IC

Secure-IC est spécialisée dans le domaine de la sécurité des systèmes embarqués. Notre offre tourne autour de 4 Business Lines : Threat Analysis, Threat Protection, Think Ahead et Content Protection.

35510 Cesson-Sévigné France
http://www.secure-ic.com

SEKOIA

Produits : SEKOIA.IO, solution XDR s'appuyant sur la Threat Intelligence.
Services : accompagnement et expertise (CERT, audit, Pentest, Threat Intel, Forensic, investigation).

75008 Paris France
https://sekoia.fr

SENTINELONE

L'agent unique SentinelOne EPP,EDR,MDR combine prévention, détection et réponse afin d'assurer la protection des postes de travail et serveurs contre tous les vecteurs de menaces.

75008 Paris France
http://sentinelone.com

SENTRYO

La solution Sentryo ICS CyberVision est une plateforme de surveillance réseau qui fournit visibilité, intégrité et sécurité pour les systèmes de contrôle industriel.

69100 Villeurbanne France
https://www.sentryo.net/fr

SERENICITY

Serenicity propose des solutions de sécurité performantes destinées aux petites, moyennes et grandes entreprises ainsi qu'aux collectivités pour lutter contre les cyberattaques et prévenir les risques.

42000 Saint-Étienne France
https://www.serenicity.fr

SESAME IT

Sesame IT édite des sondes de détection d'attaques durcies développées en France. Ces dernières sont entre autres adaptées pour la mise en conformité des OIV avec la Loi de programmation militaire.

75006 Paris France
http://www.sesame-it.com

SHADLINE

Shadline est une plateforme d'échange et de stockage totalement immunisée contre les ransomwares, offrant des communications sécurisées et un accès aux données critiques même en cas de cyberattaque.

75003 Paris France
http://www.shadline.com

SIEMENS

Pionnier en cybersécurité industrielle, Siemens dispose entre autre des automates SIMATICS S7-1500, seule gamme au monde certifiée et qualifiée, dont l'Etat recommande l'achat, notamment pour les OIV.

93527 Saint-Denis France
http://www.siemens.fr/ingenuity-for-life

SILVER PEAK

Silver Peak, le leader mondial des réseaux SD-WAN, se positionne à la pointe de la transformation du cloud avec un modèle de réseau avant-gardiste.

92300 Levallois-Perret France
https://fr.silver-peak.com

SKYBOX SECURITY

Skybox est une suite logicielle dans le domaine de la cyber sécurité traitant à la fois la gestion de la politique de sécurité et de l'analyse les risques de manière innovante.

95110 San Jose États-Unis
http://www.skyboxsecurity.com

SKYHIGH NETWORKS

Cartographie des Services Cloud utilisés, monitoring et sécurisation d'applications Cloud critiques et/ou home made, protection des données et prévention des fuites d'informations vers le Cloud.

http://www.skyhighnetworks.com

SOFT EXPANSION

Distributeur des solutions de stockages sécurisées Kanguru, Clefs USB et disques durs cryptés administrables à distance.

77920 Samois-sur-Seine France
http://www.softexpansion.com

SONICWALL

Depuis 30 ans SonicWall propose des solutions de sécurité informatique : firewalls (physiques, virtuels, Cloud Azure/Aws), messagerie, terminaux, accès distants, wifi, protection Cloud O365, switchs.

75008 Paris France
https://www.sonicwall.com

SOPHOS

Premier éditeur européen de solutions de sécurité professionnelles, Sophos propose une gamme complète de protections: NextGen Endpoint, serveurs, mobiles, chiffrement, Firewall, Email, Web et WiFi.

95870 Bezons France
https://www.sophos.com

SPIRENT COMMUNICATIONS

Notre offre de cybersécurité (logiciel, matériel & service) : validation sécurité & performance réseau en prod ; service de sécurité & tests d'intrusion ; test de sécurité & performance en lab.

78280 Guyancourt France
http://www.spirent.com

SPLUNK N

Splunk permet de mettre en place une sécurité basée sur l'analyse. Notre mission est de rendre les données machine accessibles, exploitables et utiles à tous.

75009 Paris France
http://www.splunk.fr

STIMSHOP N

Notre technologie exclusive Wi-Us de communication sans fil par ultrason permet l'échange de données sécurisé entre deux devices, sans onde radio. Pertinent pour une authentification forte en local.

75020 Paris France
http://www.wi-us.eu

STORMSHIELD N

Stormshield délivre des solutions de protection des réseaux, des postes de travail et des données certifiées au plus haut niveau de confiance européen, pour une sécurité de bout en bout.

59650 Villeneuve d'Ascq France
http://www.stormshield.eu

STRATON IT

Corrium découvre le réseau et ses composants, la cartographie générée est analysée par huits experts automatisés. Le diagnostic est complété par un plan d'action exhaustif, suivi hebdomadairement.

59000 Lille France
http://www.straton-it.fr

SYMANTEC

Symantec Corp., leader mondial de la cyber sécurité, aide les entreprises, les gouvernements et les particuliers à sécuriser leurs données les plus importantes, quelle que soit leur localisation.

92617 Courbevoie Cedex France

https://www.symantec.com/fr/fr

SYNOPSYS NORTHERN EUROPE LTD.

Synopsys propose aux organisations une offre complète de solutions et services permettant de détecter et de remédier à des défaillances, vulnérabilités et problèmes de conformité tout au long du SDLC.

RG7 4SA Reading Royaume-Uni

https://www.synopsys.com/software

SYSPERTEC N

L'offre JVL de SysperTec permet de renforcer la sécurité des systèmes informatiques Legacy (IBM z Systems et IBM i) et distribués depuis plus de 20 ans.

92210 Saint-Cloud France

https://www.jvl.fr

SYSTANCIA N

Systancia propose des solutions de sécurité des accès externes au SI, de surveillance des utilisateurs à pouvoirs (PAM), d'authentification unifiée (SSO) et de gestion des identités (IAM).

68390 Sausheim France

http://www.systancia.com

TANIUM

Tanium propose une plateforme de visibilité et de contrôle des terminaux qui transforme la façon dont les entreprises gèrent et sécurisent leurs systèmes d'information.

92200 Neuilly sur Seine France

https://www.tanium.com/fr

TEAMVIEWER GMBH

Avec la combinaison de ITbrain Surveillance, Anti-Malware et Backup, vous obtenez une solution complète pour votre infrastructure informatique ! En plus c'est complètement intégré dans TeamViewer.

73037 Goeppingen Allemagne

https://www.itbrain.com

TEHTRIS

TEHTRIS OPEN XDR Platform & ses modules EDR, EPP, SIEM, NTA, MTD, Honeypots, DNS FW & ZTR assurent une défense hyper automatisée en temps réel contre le cyber espionnage & le cyber sabotage 24 h/24, 7 j/7.

75009 Paris France

https://tehtris.com

TENABLE

Tenable est la société de Cyber Exposure. Plus de 30 000 entreprises dans le monde font confiance à Tenable pour comprendre et réduire les cyber-risques.

75008 Paris France

https://www.tenable.com

TEXPLAINED

Logiciel de rétro-conception des puces électroniques. Analyses de sécurité de tous types de composants. Solutions de sécurisation des données contenues dans les puces.

06560 Valbonne France

http://www.texplained.com

THALES N

Thales propose des services et solutions qui couvrent l'ensemble de la chaine de valeur cybersecurité, intègrant dans ses solutions des technologies innovantes comme AI, Analytics, IOT, Automation.

78141 Vélizy Cedex France

https://www.thalesgroup.com/en/activities/security/critical-information-systems-and-cybersecurity

THEGREENBOW H

Le Client VPN TheGreenBow garantit la sécurité des connexions distantes au Système d'Information. Disponible pour ordinateur et smartphone, il est le seul logiciel VPN fiable, ergonomique et certifié.

75009 Paris France

http://www.thegreenbow.com

THREATQUOTIENT INC.

ThreatQ (TIP) permet de disposer du contexte, de la personnalisation et de la priorisation nécessaires pour prendre de meilleures décisions, accélérer la détection et la réponse aux incidents.

20191 Reston États-Unis

https://www.threatq.com

TIXEO H

La visioconférence sécurisée Tixeo (certifiée/qualifiée ANSSI) s'adapte à toutes les infrastructures avec les solutions TixeoCloud, TixeoServer (serveur en interne) et TixeoPrivateCloud (infogéré)

34080 Montpellier France

https://www.tixeo.com

TRANSFERTPRO

Société 100 % française: échange de fichiers volumineux ; stockage, partage, collaboration ; CFN ; HDS ; OP/Saas ANSSI ; CSPN ; qualification élémentaire ; SecNumCloud (wip).

75017 Paris France

https://www.transfertpro.com

TRANSMIT SECURITY

Fournisseur de solution innovante – 1er service d'authentification biométrique Passwordless Omni-Device et Omni-Canal – 0 Mot de passe – 0 Login – 0 Application – 0 Phishing – 0 Fraude – 100 % sécurisé.

75000 Paris, Nantes, Toulouse, Nice France

http://www.transmitsecurity.com

TREND MICRO

Notre offre protège les activités des utilisateurs, toutes les applications, tous les dispositifs, en tout lieu, les environnements virtuels, Cloud et hybrides, le réseau face aux attaques ciblées.

9250 Rueil-Malmaison France

http://www.trendmicro.fr

TRUSTINSOFT N H

TrustInSoft propose des outils et des services déjà reconnus mondialement : TrustInSoft Analyzer, un outil d'analyse de code source permettant de garantir mathématiquement la conformité du code.

75014 Paris France

https://trust-in-soft.com

TRUSTWAVE

Trustwave aide les entreprises à lutter contre la cybercriminalité avec ses offres de technologies sécurité réseau, application et données en mode licence ou SAAS également disponibles en mode gérés.

80807 Munich France

http://www.trustwave.com

TUFIN

Tufin permet aux entreprises d'automatiser la visibilité de leurs politiques de sécurité, la gestion des risques, la mise en œuvre et la conformité dans tout leur environnement hybride.

75017 Paris France

https://www.tufin.com/fr

UNISYS

Unisys a développé une solution 0 Trust (leader selon Forrester, Gartner) avec les fonctionnalités suivantes: invisibilité de l'infrastructure, accès distant, micro segmentation, isolation dynamique.

92250 La Garenne Colombes France

http://www.Unisys.com

USERCUBE

Usercube est une solution de gestion des identités et des habilitations de nouvelle génération, leader sur le marché du SaaS (certifié ISO27001) mais aussi disponible en mode On Premise.

13825 La Penne sur Huveaune France

http://www.usercube.com

VADE SECURE H

Notre solution de protection de l'email predictive utilise l'IA et les données du milliard de boîtes mail que nous protégeons, pour bloquer les attaques ciblées dès le premier email.

59510 Hem France

https://www.vadesecure.com

VARONIS

Varonis est une plate-forme innovante de sécurité des données qui permet aux entreprises de gérer, d'analyser et de sécuriser les données d'entreprise contre les menaces internes et les cyberattaques.

92400 Courbevoie France

VECTRA NETWORKS

Vectra est une société qui utilise l'intelligence artificielle pour détecter et traiter les cyber-attaques en temps réel.

75017 Paris France

https://www.vectra.ai

VEEAM

Fournisseur innovant de solutions de disponibilité assurant la continuité d'activité des entreprises (Availability for the Always-On Enterprise™).

92800 Puteaux France

https://www.veeam.com/fr

VENAFI

Acteur majeur du marché de la sécurité dans le domaine de la protection de l'identité des machines, des connexions et des communications sécurisées entre machines. Venafi protège l'identité des machines en orchestrant la gestion des clés cryptographiques et des certificats numériques.

UT 84111 CARRY-LE-ROUET

Salt Lake City États-Unis

https://www.venafi.com/fr

VERACODE

Veracode est le précurseur de la sécurité applicative en mode DevSecOps. Offre 100 % Cloud, Veracode traite l'appSec sous toutes ses formes : statique, dynamique, composants Open Source, containers…

EC4 Londres Royaume-Uni

https://www.veracode.com

VERIZON

Fournisseur mondial de solutions de communications : plateformes sécurisées de mobilité, Cloud, réseau stratégique, Internet des objets, communications avancées, UCC, SOC, NOC, SIEM, SDN, SDP, Forensics, IAM.

92042 Courbevoie France

http://www.verizonenterprise.com/fr

VMWARE N

VMware, un leader mondial des infrastructures Cloud et de la mobilité d'entreprise, aide les organisations à accélérer leur transformation numérique.

92042 Paris La Défense France

https://www.vmware.com/fr.html

WALLIX N H

Le Bastion WALLIX est une solution de gestion des accès à privilèges intègrant la gestion des mots de passe, un portail d'accès web, la gestion des accès et l'enregistrement des sessions.

75008 Paris France

WASACA

WaSaCa est le distributeur référent en France des solutions Endpoint Protector by CoSoSys by Invintia. Certificateur exclusif en France, il recrute, forme, certifie et anime un réseau de revendeurs.

75008 Paris France

htt://www.wasaca.fr

WATCHGUARD

WatchGuard est un acteur majeur dans le domaine de la sécurité et l'intelligence réseau, du Wi-Fi sécurisé, de l'authentification multifacteur et de la protection avancée des Endpoints.

92320 Châtillon France

https://www.watchguard.com

WOLEET

Woleet sécurise vos documents avec une preuve universelle horodatée d'existence ou de signature grâce à la Blockchain.

35577 Cesson-Sévigné France

https://www.woleet.io

WOOBE

Identité numérique & Signature électronique sans fichier central des données - Irrévocable - Supranational.

95300 Pontoise France

http://www.woobe.fr/w1

WOOXO N

Wooxo édite des solutions pour éliminer les risques d'interruption d'activité et la perte potentielle de données informatiques consécutifs à tout type de sinistre informatique.

13600 La Ciotat France

https://www.wooxo.fr

WRAPTOR N

Une protection antispam efficace à 100%, sans aucune perte de messages, grâce à une méthode de vérification de la relation entre vous et vos contacts de courrier électronique.

13400 Aubagne France

http://www.spamwars.fr

YAGAAN N

YAGAAN développe et commercialise un scanner de code source de nouvelle génération. Grâce au machine learning, la YAG-Suite est une solution pertinente et abordable pour vos audits de code.

35 510 Rennes - Cesson Sévigné France

http://www.yagaan.com

YESWEHACK H

YesWeHack est la 1re plateforme européenne de Bug Bounty et de VDP. La plateforme met en relation des organisations avec 18 000+ hackers éthiques pour sécuriser leurs périmètres exposés.

75004 Paris France

https://www.yeswehack.com

ZERTIFICON SOLUTIONS GMBH

Solutions logiciels On-Premise et Cloud d'automatisation de la signature et du chiffrement des e-mails avec certificats de norme internationale S/MIME et PGP, ainsi que par mots de passe.

12347 Berlin Allemagne

https://www.zertificon.com/france

ZIWIT N

Scanner de vulnérabilité web garanti zéro faux positif. Audits automatisés, rapports de failles, correctifs à appliquer et simulation d'attaques. Suivi technique personnalisé inclus.

34000 Montpellier France

https://httpcs.com

ZSCALER

Zscaler apporte à chaque utilisateur une expérience Internet productive et sécurisée, quel que soit le terminal utilisé et l'endroit où il se trouve, en mode SaaS et 100 % Cloud.

92400 Courbevoie France

https://www.zscaler.fr

ZYXEL FRANCE

Zyxel propose une gamme de solutions de sécurité destinées aux entreprises, pour les aider à protéger et faciliter la gestion de leurs réseaux. Elle comprends les gammes Zywall USG, ATP et VPN.

69760 Limonest France

http://www.zyxel.fr

Prestataires de services

2SI CONSULTING

2SI Consulting est un cabinet de conseils et de services spécialisé dans la cybersécurité et la protection des données personnelles qui vous accompagne dans votre transformation digitale.

97160 Le Moule France

https://www.2siconsulting.com

ABAKUS SÉCURITÉ

N E C

Abakus Sécurité est un intégrateur de solutions de sécurité, expert des SIEM (QRadar), SIRP (Resilient), logiciels d'investigation (i2) et de la protection des appareils mobiles (MaaS360).

75008 Paris France

http://www.abakus-securite.fr

ABINGTON ADVISORY

Accompagnement (AMOA et expertise) au niveau : organisationnel ; technologique (architectures et hardening de composants) ; conformité (RGPD, NIS, LPM, ISO 27K...).

75800 Paris France

https://www.abingtonadvisory.com/fr/cybersecurite-confiance-numerique

ACCEIS

ACCEIS est une entreprise d'expertise en cybersécurité créée par deux experts techniques, proposant une offre transverse d'audits, de conseil et de formations sur le plan techniques et organisationnel

35000 Rennes France

http://www.acceis.fr

ACCENTURE

N

L'offre sécurité d'Accenture couvre 5 domaines : Cyberdefense, Identité Numérique, Stratégie & Risk, Sécurité Applicative et Services Managés. Accenture a acquis Arismore et Memority.

75636 Paris France

https://www.accenture.com/fr-fr

ACELYS SERVICES NUMÉRIQUES

E C

Conseil et expertise. Analyse Risques. Gouvernance (RSSI/DPO, ISO 27001, PSSI). Audits (organisationnels et techniques), pentests. Ingénierie de la sécurité (architecture, solutions, configuration...

34000 Montpellier France

https://www.acelys.fr

ACESI GROUP

N

Fournir à nos clients un accompagnement global, aussi bien sur des aspects organisationnels que techniques. Nos prestations vont du test d'intrusion jusqu'à la mise en œuvre d'un Système de Management

67960 Strasbourg - Entzheim France

http://www.ace-si.com

ACTIVANOS SAS

Spécialiste en architecture Microsoft Active Directory et Cloud

34500 Béziers France

http://www.activanos.com

ACTIV'INFO

Nous accompagnons et mettons en oeuvre dans les TPE/PME (max 50 users) une informatique sécurisée, documentée, conforme RGPD. Des méthodes issues des grands comptes à la portée des plus petits.

33360 Camblanes et Meynac France

https://www.activinfo.fr

ADENIUM

Adenium est une société spécialisée dans la mise en œuvre de Plan de continuité d'activité (PCA) selon ISO 22301 et la résilience des organisations.

75020 Paris France

https://www.adenium.fr

ACTUELBURO

E C

Nos collaborateurs vous assistent dans l'optimisation et la gestion de vos systèmes d'information et votre mobilité de façon efficiente et concurrentielle. Audit de sécurité, pentest, maintenance, etc.

64300 Orthez France

https://www.actuelburo.fr

ADACIS

E C

Qualifiée PASSI par l'ANSSI pour audits : test d'intrusion /configuration /architecture /organisationnel et physique. Solution d'Analyse de risque labélisée conforme à la méthode Ebios RM par l'ANSSI.

33150 Cenon France

https://www.adacis.net

ADENIUM

N

Adenium est une société spécialisée dans la mise en œuvre de Plan de continuité d'activité (PCA) selon ISO 22301 et la résilience des organisations.

75020 Paris France

https://www.adenium.fr

ADIKTS

Adikts est un cabinet de conseil IT spécialisé sur la Sécurité Applicative (DevSec, DevSecOps), le cloud AWS (Architecture) et la conception d'applications autour de stacks techniques opensources.

78360 Paris France

https://www.adikts.io

ADVENS

Advens est le premier pure-player français de la cybersécurité. Nous avons développé une offre globale, proposant des réponses adaptées à chaque secteur, à chaque acteur, à chaque besoin.

75009 Paris France

https://www.advens.fr

ADVENTIUM TECHNOLOGIES

N

Cellule de CyberSécurité en cours de création.

75005 Paris France

http://www.adventium.fr

ADVISO

Adviso, expert en sensibilisation à la cybersécurité, vous accompagne de l'élaboration à la mise en œuvre de votre stratégie de sensibilisation. 2019 : 100 000 collaborateurs formés, dans 15 pays.

92048 Paris La Défense Cedex France

http://www.adviso.fr

AGENCEE

Audit, Conseils, Analyse, Implémentation, Controle pour PME PMI sur la sécurité informatique. Sensibilisation à la sécurité informatique.

31600 Eaunes France

http://www.agencee.fr

AKAMAI TECHNOLOGIES

En assurant une protection contre les attaques les plus sophistiquées, Akamai vous aide à protéger vos sites Web et applications en ligne des risques d'indisponibilité et de vol de données.

75008 Paris France

https://www.akamai.com/fr/fr

AKERVA

N

Société de conseil spécialisée en sécurité du SI et Cyberdéfense : Audits et Tests d'intrusion. Gouvernance & Sécurité du SI. Formation & E-Learning. SOC & Centre de cyberdéfense.

75008 Paris France

https://akerva.com

AKKA

N

AKKA allie son expérience de l'électronique automobile, des réseaux, de l'architecture et des TI et son expertise en matière de cybersécurité pour lutter contre les risques.

92977 Paris-La Défense France

https://www.akka-technologies.com

ALASTAR

E C

Sécurisez votre SI grâce à l'expertise Alastar, votre partenaire ExpertCyber. Cybersécurité. Gestion de l'infra. Sauvegarde. RGPD.

56800 Ploermel France

https://www.alastar.fr

ALEKSO

QUIVIV développe et opère des solutions de cybersécurité en SaaS reposant sur les principes de simplicité et d'efficacité, centré sur les usages et mis en œuvre dans une interface unique de pilotage.

92350 LE PLESSIS-ROBINSON France

http://www.alekso.fr

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique)
H Adhérents Hexatrust

ALENATEC

Société de services et de conseils en informatique spécialisé en sécurité informatique : Audits techniques et organisationnels, Conseil, ingénieries, expertise technique, Intégration et développement.

75008 Paris France

https://www.alenatec.com

ALGOSECURE

AlgoSecure est un cabinet de conseil spécialisé en sécurité informatique. Nous réalisons des audits de sécurité et des tests d'intrusion pour vous aider à sécuriser votre système d'information.

69120 Vaulx-en-Velin France

ALLISTIC N

Allistic, pure player de la cybersécurité, accompagne ses clients dans leur stratégie cybersécurité, la gestion de la confiance numérique, la protection des menaces digitales et la sensibilisation.

59000 Lille France

https://www.allistic.fr

ALMOND

Nous sommes spécialisés en Cybersécurité et nos savoir-faire reposent sur 5 expertises : Offensive Security, Defensive Security, Infrastructure Security,Compliance et SOC-CERT CWATCH.

92310 Sèvres France

http://almond.consulting

ALTRAN TECHNOLOGIES N

Nos services couvrent l'IT, l'IOT, les syst. industriels, les systèmes embarqués et s'appuient sur nos labs, nos partenariats et nos centres d'expertises internes (Analytics, IOT, Industrie 4.0…).

92807 Puteaux France

http://www.altran.com

AMBICIO

Nous proposons d'auditer et-ou d'accompagner les entreprises dans l'évaluation et la sécurisation de leur SI. Nous bénéficions d'une solide expérience d'audit des SI adaptée au RGPD.

92100 Boulogne-Billancourt France

https://www.ambicio.fr

AMBIONICS SECURITY

Notre approche réaliste et offensive éprouve la sécurité de vos applications web en continu. Leurs vulnérabilités sont détectées et qualifiées, et l'efficacité des correctifs validée.

75009 Paris France

AMOSSYS

Société de conseil et d'expertise en cybersécurité, AMOSSYS propose une offre globale de services pour sécuriser ses SI : audit PASSI, conseil SSI, réponse à incident, évaluation CSPN ou CC, LID…

35000 Rennes France

https://www.amossys.fr

ANEXIS

Stratégie pour une meilleure cyber-résilience, conformité RGPD, organisation agile, transition numérique... nous accompagnons les TPE - PME dans leur démarche de développement et de sécurisation.

33000 Bordeaux France

https://www.anexis.fr

ANTEMETA

Spécialiste infrastructure et Cloud Computing, Antemeta accompagne ses clients depuis 25 ans dans l'évolution de leur système d'information.

78280 Guyancourt France

https://www.antemeta.fr

APIXIT N

APIXIT est expert dans la transformation numérique des entreprises en Cybersécurité, Infrastructures et Cloud : audit, conseil, intégration, MCO et services managés, assistance technique.

91940 Les Ulis France

https://www.apixit.fr

APSIDE N

Apside : Conseil, ingénierie SI, ingénierie industrielle, ingénierie infrastructure.

92100 Boulogne-Billancourt France

https://apside.com

ARMATURE TECHNOLOGIES N

Cabinet de conseil indépendant spécialisé en sécurité des systèmes d'informations : test d'intrusion, cybersécurité, cyberdéfense, risque, conformité et gouvernance, architecture orientée sécurité.

75008 Paris France

http://www.armaturetech.com

ASSYSTEM

Conseil en gouvernance de la sécurité, accompagnement à l'homologation, Intégration, MCS.

78180 Montigny le Bretonneux France

http://www.assystem.com

ATE

Expert français en hébergement et infogérance de systèmes d'information stratégiques. Solutions Cloud sur mesure ultra sécurisées. Hébergeur certifié de données de santé (HDS) et ISO 27001.

59650 Villeneuve d'Ascq France

https://www.ate.info

ATN GROUPE

ATN Groupe est une ESN fondée en 1997, spécialisée dans les infrastructures informatiques, les applications cloud ainsi que les réseaux et télécoms qui est reconnu dans le domaine de la cybersécurité.

38240 Meylan France

AUTICONSULT N

Auticonsult est la 1re ESN française à employer des consultants informaticiens autistes. Nous intervenons dans les domaines de la Cybersécurité, de la Data, du Développement et du Test.

92400 Courbevoie France

https://auticonsult.fr

AVITI E C

Aviti fournit des prestations de services autour de l'infrastructure systèmes et réseaux et des solutions d'infogérance. Aviti propose aussi du Cloud Computing à travers sa propre marque CloudDirect.

44300 Nantes France

https://www.aviti.fr

AXEL IT

Spécialiste de l'intégration IT des Entreprises, nous combinons 8 centres de compétences pour servir votre transformation digitale au travers des Infrastructures et de l'Outillage des processus IT.

92800 Puteaux France

https://www.axelit.fr

AXIANS N E C

Axians, marque de VINCI Energies dédiée à l'ICT, vous accompagne dans vos projets de cybersécurité, dans l'intégration et l'infogérance de votre système d'information.

69200 Vénissieux France

https://www.axians.fr

AXIANS C&C MARSEILLE-NICE-MONACO E C

Axians accompagne ses clients et propose son savoir-faire pour couvrir l'ensemble des besoins de sécurité numérique des entreprises: conseil et conformité, audits, intégration, services managés.

13011 Marseille France

https://www.axians.fr/fr

AXICOM-SECURITE

Société d'intégrateur,d'audit et conseils solution orienté sécurité périmètre et terminaux ainsi qu'audit Rgpd et gestion de risque.

75002 Paris France

Https://axicom-security.com

AZERI BEGI CYBERSÉCURITÉ

Azeri begi est spécialisé en cybersécurité des entreprises dans les départements du pays basque et des landes. Nous effectuons des audits, formations, interventions (en cas d'attaques).

64240 Macaye France

https://www.azeri-begi.fr

BEA INFORMATIQUE E C

BEA est labellisées ExpertCyber et se distingue par une approche en Cybersécurité à 360°. Nous traitons le volet autant technique qu'organisationnel et couvrons de la Gouvernance jusqu'aux Pentests.

30100 Ales France

https://www.bea-informatique.fr

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction. Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

BEARINGPOINT

BearingPoint a développé ses activités de conseil en cyber sécurité autour de 3 grands axes : stratégie et sensibilisation, gestion des risques et gestion de crise, conformité règlementaire.

92907 Paris-La Défense Cedex France

http://www.bearingpoint.com

BEIJAFLORE

Cabinet de conseil en cyber sécurité, qualifié PASSI, Beijaflore accompagne ses clients nationaux et internationaux dans l'évaluation des risques cyber et le déploiement des systèmes de protection.

75016 Paris Gabon

https://www.beijaflore.com/fr

BLUESCREEN

E C

BLUESCREEN est un MSP qui apporte à ses clients une offre d'infogérance sans engagement et illimitée sur poste utilisateur, serveur et CLOUD.

69760 Limonest France

https://bluescreen.fr

BOCK CONSEIL

Cybersécurité des SI industriels : formation, transfert de compétences, assistance à maîtrise d'ouvrage et maîtrise d'œuvre. Expérience de 8 ans à plein temps sur tous types de procédés.

69100 Villeurbanne France

https://www.bockconseil.fr

BRIGHTWAY

Brightway est un cabinet proposant une offre complète en cyber sécurité et gouvernance des données: audit, conseil, alerte et avertissement (SOC/CERT), réponse à incident et formation certifiante.

92310 Sèvres France

https://www.brightway.fr

BSI FRANCE

BSI France organisme de certification et de formation, vous propose des solutions de cyber sécurité, sécurité de l'information et de conformité au Règlement général sur la protection des données.

75017 Paris France

BSSI CONSEIL ET AUDIT

Conseil et audit en cybersécurité.

75009 Paris France

https://www.bssi.fr

BUG BOUNTY ZONE

Bug Bounty Zone est la première plateforme professionnelle de bug bounty proposant plusieurs niveaux d'expertise en cyberdéfense.

13014 Marseille France

https://www.bugbountyzone.com

CALYPT CYBERSÉCURITÉ

Calypt est une société de cybersécurité basée à Lyon opérant sur tout le territoire français. Nous proposons audits, formations agréées, conseils, développement… pour entreprises de toute taille.

69003 Lyon France

https://www.calypt.com

BY THE WAY

E C

By The Way assure des missions d'audit, d'étude, de définition & de mise en œuvre d'architectures systèmes et réseaux dans les domaines de la sécurité, de la mobilité et des infrastructures systèmes.

59175 Vendeville France

https://www.bytheway.fr

CAPGEMINI - SOGETI

N

Nous proposons des services de sécurité de bout en bout intégrant conseil, protection et surveillance pour protéger votre entreprise.

92130 Issy les Moulineaux France

https://www.sogeti.com/services/cybersecurity

CAPGEMINI TECHNOLOGIE SERVICES - SOGETI

N E C

Notre offre inclut de l'audit/pentest (PASSI & PASSI LPM), du conseil stratégique et opérationnel, de l'intégration/run, de la surveillance (SOC PDIS) et de la réponse à incidents (CERT et SWAT).

92130 Issy les Moulineaux France

https://www.fr.sogeti.com/expertise/nos-activites/cybersecurite

CEGEDIM OUTSOURCING

N

Cegedim Outsourcing, spécialiste dans les métiers de l'infrastructure IT, délivre aux entreprises de toutes tailles des services d'intégration, d'infogérance et des prestations en assistance technique.

78457 Vélizy Cedex France

http://www.cegedim-outsourcing.fr

CEIS

H

CEIS Cyberdéfense propose une offre complète et intégrée à 360 degrés à destination des entreprises ne disposant pas d'une organisation dédiée à la cybersécurité ou souhaitant la renforcer.

75015 Paris France

https://www.ceis.eu

CGI FRANCE

N

Notre offre sécurité et gestion des risques s'étend aux métiers de CGI : conseil, intégration, services managés. Nos domaines d'interventions sont : gouvernance SSI, IAM, SOC, PCA, audit et tests…

92400 Courbevoie France

http://www.cgi.fr

CLARANET

N

Expert en infogérance d'applications critiques et en sécurité. Hébergement sécurisé et conforme (PCI DSS & 27001). Offre sécurité : pentests/audits, Soc as a Service, Services managés.

75011 Paris France

http://www.claranet.fr

CNPP CYBERSECURITY

Audit, conseil et formation en sécurité des systèmes d'information.
Gouvernance, risques et conformité : ISO 27001, PCI DSS, ISO 22301... Technique et sécurité opérationnelle. Forensic.

75017 Paris France

http://www.cnpp-cybersecurity.com

CO-C

Expert en sécurité intrusive indépendant : tests d'intrusion (physique, externe, interne) ; Audit de sécurité (LAN, datacenter, cloud) ; Audit de configuration ; Formation sécurité et sensibilisation.

69160 Tassin France

http://www.co-c.net

COESSI

N

Qualifiée PASSI RGS, reconnue pour ses travaux innovants en sécurité des systèmes industriels et de l'IoT, CoESSI intervient tant en Cybersecurité qu'en protection de la vie privée (RGPD) des SI.

92000 Nanterre France

https://www.coessi.com

COGITAL

N

Cogital est spécialisé en Cybersécurité. Nos activités portent sur l'Audit, le Conseil, l'intégration et les Services Managés. Nous sommes certifiés techniquement auprès de nos partenaires éditeurs.

75014 Paris France

https://www.cogital-it.com

CONIX

Expertise technique : audit / test d'intrusion, SOC managé, réponse à incident. Expertise conseil : référentiels SSI, analyses de risques, sensibilisation, tableaux de bord.

92130 Issy-les-Moulineaux France

http://www.conix.fr

CONSORT

N

Consort intervient sur l'ensemble du cycle de sécurisation et de protection des accès, des données, des tentatives d'intrusions, des tests de vulnérabilité.

75017 Paris France

http://www.consort-group.com

COREYE

N

COREYE se positionne comme un MSSP (Managed Security Service Provider), accompagne ses clients avec son offre de sécurité CoreTrust (SOC externalisé, WAF, Anti-DDos, SIEM) et est certifié ISO27001.

59262 Sainghin-en-Mélantois France

http://www.coreye.fr

CORTEXERA

E C

Avec plus de 25 ans d'expertise, nous proposons pour toutes les entreprises. Conseil, intégration, formation et RSSI à temps partiel. Certifié ISO27001, Label ExpertCyber, CISSP, CoBIT.

13008 Marseille France

https://www.cortexera.com

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique)
H Adhérents Hexatrust

CS NOVIDY'S N

CS Novidy's propose une offre globale : Conseil (PASSI LPM), Intégration, Services (CERT-CS/GIR, NOC/SOC), éditeur (Prelude - SIEM, Vigilo - NMS, Trusty - IGC, horodatage, coffre-fort, SEDUCS - OS durci).

92350 Le Plessis Robinson France

http://www.c-s.fr

CYBER-EGIDE

Cyber-Egide propose un audit sur mesure de votre entreprise pour trouver et résoudre les vulnérabilités de votre réseau. Nous proposons aussi un logiciel qui protège tous vos pc, téléphones et réseau.

75005 Paris France

https://www.cyber-egide.fr

CYBERENS

Conseil en ingénierie de sécurité sur la base d'analyses de risque.
Édition de logiciels de protection des données : client sécurisé de messagerie (SET) pour Windows, bibliothèque cryptographique.

33000 Bordeaux France

https://www.cyberens.fr

CYBERGLOBAL

Cyber accompagnés (suivi) – Cyber formés (formation) – Cyber assurés (assurance).

1700 Miribel France

https://cyberglobal.fr

CYBERSEC&YOU H

Cybersec&You est le distributeur à valeur ajoutée de l'ensemble des produits et services des membres d'Hexatrust. Nous proposons un guichet unique pour les organisations publiques et privées.

78750 Mareil-Marly France

https://www.cybersecandyou.com

CYBERZEN

Conseil stratégique, audit fonctionnel et organisationnel pour due dilligence ou accompagnement, prestation de conseil sur le moyen terme et offre de sensibilisation innovante.

75001 Paris France

https://www.cyberzen.com

DATA PRIVACY PROFESSIONALS N

Services de DPO externe et de mise en conformité RGPD à l'international (fr, eng, ger). Formations B2B (Datadock, OPCO) et B2C (Mon Compte Formation) : cybersécurité, RGPD, transformation numérique.

67114 Eschau France

https://www.dataprivacy.pro

DAVID INFORMATIQUE N

Offres de services proactives incluant direction de SI, infogérance niveau 1-2-3 physique / Cloud, sécurité (système de reprise d'activité, firewall…) avec engagement de temps de reprise d'activité.

21200 Beaune France

http://david-informatique.com

DBM PARTNERS

Cabinet de conseil à taille humaine, nous aidons nos clients à maîtriser leurs risques numériques sur les domaines Cybersécurité, Digital Workplace, Gouvernance de l'information et Projets.

75116 Paris France

http://www.dbm-partners.com

DELOITTE

Deloitte est classé numéro 1 mondial des services de conseil en cyber sécurité par Gartner pour la 5e année consécutive. Une offre pluridisciplinaire au service de toutes les organisations.

92200 Neuilly-sur-Seine France

https://www2.deloitte.com/fr/fr.html

DEVELOPPEMENT CONSEIL COMMUNICATION N E C

ESN spécialisée en cybersécurité, réseau et transformation digitale. prestations de conseil, d'intégration, infogérance dans le domaine de la sécurité. opérations de prévention et remédiation en cyber.

59710 Merignies France

https://www.dc-communication.eu

DEVOTEAM N

Transformer le risque en opportunité Business. Devoteam soutient les entreprises dans leur transformation digitale en intégrant la sécurité dans les projets, et veille au maintien de leur résilience.

92300 Levallois-Perret France

http://www.devoteam.fr

DIGITAL SECURITY N

Digital.security est une société de services spécialisée en sécurité numérique. Premier CERT™ IoT, digital.security emploie 250 experts certifiés PASSI, ISO 27001, ISO 27005, CISSP, CMMI, ITIL.

75012 Paris France

https://www.digital.security/fr/

DIGITEMIS CYBERSECURITY & PRIVACY N H

Prestataire qualifié PASSI par l'ANSSI. 7 labels CNIL (audit & formation). Tests d'intrusion, audit architecture, gouvernance. Focus : Iot, sécurité des fournisseurs, systèmes industriels, Phishing.

44400 Nantes France

https://www.digitemis.com

DIGORA N

Analyse des mesures et évaluation des risques liés aux bases de données en 3 étapes : identifier des actifs SGBD, analyse des mesures en fonction d'un référentiel, cartographie des mesures de sécurité.

67000 Strasbourg France

https://www.digora.com/fr/expertises/securite/analyse-risques

DILITRUST N

DiliTrust offre une gamme de solutions et services dédiés à la Gouvernance : Gestion des Conseils et Comités, des Data rooms, transfert sécurisé de données sensibles ou volumineuses.

92059 La Défense France

http://ww.dilitrust.com

DPO CONSULTING N

DPO Consulting est une société de conseil spécialisée en protection des données personnelles qui a pour objet d'accompagner les entreprises dans la mise en conformité au RGPD.

75009 Paris France

https://dpo-consulting.fr

EBRC H

Cyber-Resilience services : conseil en gestion des risques ICT, Business Continuity, ISO27001-22301, PCI DSS, Pentests, DC Tier IV ; SOC, Gestion des vulnérabilités, Cyber-Securité & Forensics.

2453 Luxembourg Luxembourg

http://www.ebrc.com

E-CATALYST N

Formation en cybersécurité, audit en cybersécurité, création de sites web, campagne de communication digitale, appui à la mise en conformité au RGPD, maintenance informatique.

59600 Maubeuge France

https://e-catalyst.fr

ECO HARDWARE SAS

Contrat de maintenance, infogérance informatique. Solutions Cloud. Société spécialiste en sécurité informatique. Entreprise de cybersécurité. Récupération de données disque dur NAS.

75015 Paris France

https://www.eco-hardware.fr

EIFFAGE ENERGIE SYSTÈMES - CLEMESSY

Clemessy, la marque dédiée à l'industrie du groupe Eiffage répond aux besoins des industries les plus exigeantes dans le domaine de la cybersécurité, pour exploiter en toute sécurité les installations.

68100 Mulhouse France

https://www.clemessy.com

EIGHT TECH E C

Infogérance des systèmes informatiques professionnels. Sécurisation, optimisation et performance des systèmes et des réseaux. Conseil, déploiement et accompagnement.

34170 Castelnau le Lez France

https://8tech.fr

EITA CONSULTING N

Conseil, ingénierie SI, ingénierie industrielle, ingénierie infrastructure, Installation Fibre Optique (D1, D2, D3), Antenne G5, IoT, IA.

78360 Montesson France

https://www.eitaconsulting.fr

ETELCOM S.A.S.

Société de services d'ingénierie informatique spécialisée dans la sécurité informatique. Audit, conseil, surveillance, installation, maintenance et infogérance informatique et Télécom.

56400 Auray France

https://www.etelcom.fr

EXAPROBE - GROUPE ECONOCOM N

Exaprobe est un opérateur souverain de sécurité augmentée, intervenant autour de quatre axes: le conseil, l'intégration, les services managés & l'infogérance et les offres packagées en mode SAAS.

92350 Le Plessis-Robinson France

http://www.exaprobe.com

EXCELLIUM SERVICES

With its headquarter in Luxembourg and more than 90 security professionals, Excellium is the leader of Cybersecurity services regarding Application Security and Security Incident management.

L-5326 Contern Luxembourg

https://www.excellium-services.com

EXPONENS

Audit et conseil en gouvernance et sécurité des SI.

75107 Paris France

http://www.exponens.com

EXTERN IT N

Service informatique externalisé pour PME et assos, nous avons développé une offre de services cybersécurité adaptée à ces structures pour leur permettre de se protéger et se relever d'un incident.

59118 Wambrechies France

https://www.extern-it.fr

EXTREMIT

extremIT est une Entreprise de Services du Numérique qui accompagne les PME des Hauts-de-France dans leur politique de cybersécurité (audit préalable, résolution d'incidents, prévention et formation).

59650 Villeneuve d'Ascq France

http://www.extremit.fr

FIDENS

FIDENS à la pointe de l'expertise de la cybersécurité depuis plus de 15 ans, nos équipes réunissent des professionnels aguerris et certifiés, experts des techniques, méthodes et standards du domaine.

75009 Paris France

https://www.fidens.fr

FORMIND H

Formind est un cabinet de conseil indépendant spécialisé en sécurité de l'information, gestion des risques et conformité, qui intervient aussi bien en engagement de moyens que de résultats.

92130 Issy-les-Moulineaux France

http://www.formind.fr

G-ECHO N

Diagnostic, conseil, audit, expertise,
Accompagnement (formation, recrutement),
Solutions (gestion des risques et vulnérabilités, tests de sécurité, DLP…).

31380 Garidech France

http://www.g-echo.fr

GFI INFORMATIQUE N

Gfi propose des solutions logicielles novatrices et des services pour surveiller vos données. Keenaï, SIEM 100 % français avec une IA supervisant la sécurité IT, tout comme les environnements OT.

93400 Saint Ouen France

http://www.gfi.world

GPLEXPERT E C

Conseils & Services en Ingénierie Informatique spécialiste du Système d'Information Sécurisé. Système, Réseaux, Open source, Hébergement, Supervision, Cybersécurité, Gestion de crise. ISO27001 & HDS.

91290 Arpajon France

https://gplexpert.com

GRAND E NOV

Accompagnement suite Diagnostic Compétitivité Région Grand Est

67100 Strasbourg France

http://www.grandenov.fr

GROUPE SII N

Le Groupe SII apporte une expertise sur la confiance numérique dans les domaines de l'informatique industrielle, du système d'information et de l'IoT à travers son offre SECURE DIGITAL FACTORY.

35510 Cesson-Sévigné France

http://www.groupe-sii.com

HACKNOWLEDGE SA

Hacknowledge est une solution de monitoring sécurité de type MDR (managed detection response). Notre rôle est d'identifier les anomalies/problèmes sécurité et de vous conseiller pour leur résolution.

1028 Préverenges Suisse

http://www.hacknowledge.com

HARMONIE TECHNOLOGIE N

Partenaire des Grands Comptes, nous couvrons l'ensemble de la cybersécurité : la stratégie SSI, le management des identités et des accès, et la gouvernance et la protection des données.

75008 Paris France

https://www.harmonie-technologie.com

HELIX SECURITY SAS

Conseils, formations et accompagnement dans la sécurité. Prestataire de Service proposant SOC et une gamme étendue de services.

97460 Saint Paul France

https://www.helixsecurity.cloud

HEXANET E C

Opérateur télécom, hébergeur et fournisseur de services managés certifié ISO27001 et HDS. Hexanet-Soluceo vous conseille et vous accompagne sur tous vos projets de modernisation et de sécurisation SI.

51100 Reims France

https://www.hexanet.fr

HIRMES

Hirmes est une entreprise qui œuvre pour la confiance numérique. Nous proposons des services de conseil et d'audit dans le domaine de la sécurisation des systèmes d'information.

63122 Ceyrat France

https://www.hirmes.fr

HOLISEUM H

Holiseum vous aide à mieux appréhender vos risques cyber en adoptant une approche globale, dite holistique. Nous pouvons ainsi intervenir sur l'ensemble de la chaîne de valeur cybersécurité.

92088 Paris-La Défense

https://www.holiseum.com

HUB ONE N

Hub One propose une offre globale de sécurité : Audit, Conseil, Formation, Cyber-entraînement, Intégration, Edition, SOC.

93290 Tremblay en France France

https://www.hubone.fr

I.S. MANAGEMENT

MA-SAUVEGARDE spécialisée dans la sauvegarde externalisée depuis plus de 10 ans, propose une solution fiable et robuste personnalisable en marque blanche. ISO27001 et HDS.

69360 Sérézin-du-Rhône France

https://ma-sauvegarde.com

IBC DIALOG E C

Ibc Dialog réalise des mises en place de réseaux et la sécurisation des postes. IBC propose aussi l'hébergement de données avec des prestations d'infogérance globale ou partielle.

14120 Mondeville France

https://www.ibc-dialog.fr

IDAXIO

Nous assurons la connectivité des données grâce aux meilleures solutions API, pour partager en toute sécurité vos informations avec vos clients, partenaires et fournisseurs.

78230 Le Pecq France

https://www.idaxio.com

IDENTO H

Idento est le cabinet de conseil et d'intégration, leader de la gestion de l'identité et des accès (IAM, IAG, PAM, CIAM, DAG, Fédération, Authentification forte, MFA…).

92600 Asnieres sur Seine France

https://idento.fr

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique)
H Adhérents Hexatrust

ID-LOGISM N

Cabinet de conseil sécurité/protection données strat & perso. Analyse de risques ISO27005. Gouvernance sécurité ISO27001 PSSI RSSI CLOUD. Conformité RGPD DPO externe. IAM. Classification données. DLP.

75005 Paris France

http://www.id-logism.fr

IDNA E C

iDNA, conseil expert en Cybersécurité, Réseaux, Datacenter et Cloud, vous accompagne dans vos projets de sécurisation et de transformation IT. #Gouvernance #Expertise #Opérations #ExpertCyber.

75003 Paris France

https://www.idna.fr

IMS NETWORKS N

IMS Networks aide les organisations à optimiser la performance et la sécurité de leurs infrastructures IT en leur proposant des services RÉSEAU & CYBERSÉCURITÉ certifiés ISO 27001.

81100 Castres France

http://www.imsnetworks.com

INDATABLE N

Indatable est une société de conseil spécialisée dans l'accompagnement à la mise en conformité numérique et réglementaire. Nous proposons des prestations de sécurité informatique, RGPD et SAPIN II.

13014 Marseille France

https://indatable.com

INET SYSTEM N

Spécialiste de la sécurité sur les plates-formes Apple (postes de travail et terminaux mobiles).

92310 Sèvres France

http://www.inet-system.com

INFOCLIP N

Le Groupe Infoclip propose d'accompagner ses entreprises clientes dans l'exécution de leurs projets de transformation digitale. Infoclip met en place et infogère les systèmes de sécurité.

75019 Paris France

http://www.infoclip.com

INFORSUD TECHNOLOGIES N

INFORSUD Technologies accompagne les entreprises/collectivités dans l'optimisation, la performance de leur système d'information et en assure la cybersécurité - audits/pentests/sensibilisation.

31500 Toulouse France

https://inforsud-technologies.com

INFOSYS N

Nous aidons à gouverner, à opérer, à surveiller, à détecter et à réagir aux attaques, avec une suite de cybersécurité evolutive, pour transformer, automatiser et orchestrer, On-Prem ou sur Cloud.

92914 Paris-La Défense Cedex 9 France

https://www.infosys.com/services/cyber-security.html

INOPS N

Société spécialisée dans la prestations intellectuelles d'experts du digital et conseil métiers.

75017 Paris France

http://www.inops.fr

INQUEST E C

INQUEST propose une offre complète de réponse à incident de cybersécurité ainsi qu'une offre d'audit (organisationnel et technique) et conseil SSI.

92800 Puteaux France

http://www.inquest-risk.com

INTEGRALE IP

ESN spécialisée en Infrastructure Réseau & Sécurité Informatique : audit, conseil, expertise technique, intégration de solutions LAN / WLAN / MAN / WAN / SDWAN.

93400 Saint-Ouen France

https://integraleip.fr

INTERDATA E C

Interdata a l'expérience et l'expertise certifiée pour vous apporter des services intégrés ou managés afin de sécuriser vos réseaux, vos applications et vos identités.

91940 Les Ulis France

https://interdata.fr

INTRINSEC N E C

Intrinsec propose un portfolio d'expertises & services en cybersécurité pour accompagner de la définition de la stratégie à la fourniture de services managés pour en maintenir le niveau.

92000 Nanterre France

http://www.intrinsec.com

IRON MOUNTAIN

Iron Mountain votre partenaire de confiance : solutions digitales, Cloud, restauration de données archivées, externalisation des bandes de sauvegarde, destruction sécurisée de matériel informatique.

91420 Morangis France

https://www.ironmountain.fr

ISATECH N

Notre offre consiste en l'identification des processus métiers critiques, l'audit, la cartographie des systèmes d'information et l'accompagnement dans la sécurisation des données d'entreprise.

56000 Vannes France

https://www.isatech.fr

ISE SYSTEMS H

Audits d'infrastructures, d'applications, du SMSI, de conformité (ISO 27001), analyse de risques. Mise en place SOC/SIEM, Veille CERT, PRA/PCA, PSSI. Gouvernance, contrôle de la conformité, risque.

92300 Levallois Perret France

http://ise-systems.fr

IT&M REGIONS N

Assistance dans le domaine de la cybersécurité : Antivirus / Firewall / Sauvegarde / Gestion poste de travail, RGPD/DPO (volet sécurité).

45000 Orléans France

http://www.it-m.fr

IT3 INFORMATIQUE

Audit de cybersécurité. Certification infrastructure. Tests d'intrusion. Infogérance. Accompagnement RGPD. Matériel. Logiciels.

67201 Eckbolsheim France

https://it3.fr

I-TRACING

I-TRACING est un leader français du conseil & de l'ingénierie en cybersécurité : audit, forensic, intégration, développements sécurisés, conformité, SOC, services managés, formation...

92800 Puteaux France

https://www.i-tracing.com/fr

ITS GROUP

ITS Group est une ESN qui accompagne les entreprises dans les domaines de la sécurité, aussi bien sur du conseil que dans l'intégration et l'infogérance de solutions.

92100 Boulogne Billancourt France

http://www.itsgroup.com

IVISION

Sensibilisation utilisateurs, outils de protection, audits de sécurité, PCA / PRA, décontamination, RGPD / DPO, sauvegarde hébergée, messagerie hébergée, infogérance, ingénierie…

92600 Asnières-sur-Seine France

https://www.ivision.fr

JANUA N

Consulting, implémentations, déploiement et support de solutions de gestion des identités open source (annuaires LDAP, SSO, Provisioning).

06650 Le Rouret France

http://www.janua.fr

JLLNET E C

Vous accompagner sur les domaines d'infrastructure (réseau/ système/ stockage/ virtualisation/ sécurité/ supervision) mais aussi sur le MCO, l'évolution de votre SI et sur vos projets métiers.

13127 Vitrolles France

https://www.jllnet.fr

K SECURITY

Audit de sécurité informatique, mise en place firewall infogéré, mise en conformité RGPD.

85500 Les Herbiers France

https://www.k-security.fr/

KATANA DIGITAL SA

Destruction physique, sur site, sécurisée de supports informatiques (disques durs, tapes, SSD, mobiles) selon la norme DIN66399 et utilisation d'une application pour tracer les n° de série des médias.

75001 Paris France

http://www.katanadigital.com

KPMG

Maitriser les risques cyber en dialoguant avec toutes les fonctions, en intégrant les problématiques business/conformité/risques tout en s'appuyant sur des expertises techno et investissements majeurs.

92066 Paris-La Défense France

https://home.kpmg.com/fr/fr/home.html

KUDELSKI SECURITY

Fournisseur indépendant de solutions et services innovants de cybersécurité pour les entreprises privées et le secteur public : conseils, technologies, services managés, innovation personnalisée.

1033 Cheseaux sur Lausanne Suisse

https://kudelskisecurity.com

KYRON SI

E C

Kyron propose des solutions de cybersécurité IT/OT en s'appuyant sur l'expertise reconnue de ses collaborateurs à travers de multiples certifications (ISA62443,CISSP,CCSP,CEH,ISO27001,ISO27005...).

31100 Toulouse France

http://www.kyron.fr

LECPAC CONSULTING

Nous sommes une société de conseil dans les domaines du cloud (Partenaire OVH) et en cybersécurité. Nous proposons des accompagnements sur la démarche ISO 27001 et des audits d'infrastructure cloud.

91170 Viry Chatillon France

https://lecpac-consulting.com

LEXFO

LEXFO est un cabinet indépendant d'expertises techniques en sécurité des SI. L'activité de LEXFO se décline en 5 offres de service : Audit de sécurité, Réponse à incidents, Surveillance des SI, R&D.

75009 Paris France

https://www.lexfo.fr

LISIS CONSEIL

Lisis Conseil est un cabinet de conseil indépendant spécialisé dans la gouvernance de la sécurité des systèmes d'information, la gestion des risques, la continuité des activités et la conformité.

78170 La Celle Saint Cloud France

http://www.lisis-conseil.com

LOGIFORM CONSEIL

N

L'informatique, plus simplement : intégration d'ERP, CRM Mobile et logiciels de gestion pour PME ; Divalto ; Gestimum ; administration de réseaux et serveurs.

69300 Caluire et Cuire France

http://logiform-conseil.com

LOGIN SECURITE

N H

Login Sécurité accompagne les DSI dans la définition et la mise en œuvre de leur stratégie de Confiance Numérique en s'appuyant sur deux leviers : la Cybersécurité et le Réseau.

92210 Saint-Cloud France

https://www.login-securite.com

MANIKA

N

MANIKA est un cabinet indépendant de conseil, d'audit et de formation spécialisé dans la protection et le renforcement du système d'information.

92200 Neuilly-sur-Seine France

https://www.manika-consulting.com

MASTER SECURITY CONSEIL

MASTER SECURITY CONSEIL société de spécialistes, à fort potentiel, travaillant sur de la sécurité, cybersécurité, RGPD, intelligence artificielle & machine learning,big data & science de la donnée.

92100 Boulogne France

http://www.mastersecurityconseil.fr

MATILAN

Matilan est une ESN spécialisée dans les services informatiques destinés aux PME, ETI et grands comptes. Notre expertise s'appuie sur des compétences en sécurité, services Cloud et infogérance.

75008 Paris France

https://www.matilan.com

MEDIANE SYSTEME

N

R&D externalisée. Systèmes embarqués sécuritaires. Temps réel. Objets connectés. IIoT. LINUX Secure. OPC UA…

78230 Le Pecq France

https://medianesysteme.com

METANEXT

N

Conseil en Gouvernance, Risque et Conformité, et en Conception et Intégration de solutions de sécurité des réseaux, sécurité périmétrique, firewalling, PRA/PCA, solutions SIEM et solutions Idaas.

92100 Boulogne-Billancourt France

http://www.metanext.com

METSYS

N H

Acteur incontournable des services du numérique, Metsys vous offre un accompagnement sur mesure tout au long de vos projets de transformation numérique.

92100 Boulogne Billancourt France

https://www.metsys.fr

MHCONSEIL

E C

Conseil, accompagnement et mise en service de solutions IT (matériels, logiciels, mise en production et assistances).

75017 Paris France

https://www.mhconseil.fr

MICROPOLE

Go Cloud & Security est la structure au sein du Groupe Micropole spécialisée dans le Conseil et l'assistance technique dans les domaines du Cloud Public et de la Cybersécurité.

92300 Levallois France

https://www.micropole.com

MIXCOM

N

Diagnostic rapide de problèmes informatiques grâce à notre service innovant OptimIS d'analyse comportementale simultanée de l'ensemble des composants d'une architecture informatique complexe.

35760 Saint-Grégoire France

http://www.mixcom.fr

MODIS

N

Modis, acteur mondial du conseil en ingénierie, services numériques et sciences de la vie, déploie une offre dédiée à la sécurité avec un focus réglementaire (RGPD).

92800 Puteaux France

http://www.modisfrance.fr

MPTCONSEIL

Je vous accompagne dans votre digitalisation de confiance.

37000 Tours France

http://www.mptconseil.fr

NAXIOS

Infogérance globale de PME. Conseil et Installation de pare-feu. Équipe de réponse aux incidents cybersécurité.

92100 Boulogne-Billancourt France

https://www.naxios.fr

NBS SYSTEM

NBS System est créateur et infogérant de l'offre Cerberhost, un système de très haute sécurité, disposant de plusieurs dizaines de couches de sécurité, disponible sur AWS et sur nos Clouds privés.

75017 Paris France

http://www.nbs-system.com

NDA-SECURITY

N

NDA-Security réunit EXPERTISES SSI indépendantes(FR)et SOLUTIONS LOGICIELLES européennes uniques sélectionnées pour répondre aux enjeux techniques, assurantiels, organisationnels et réglementaires.

91230 Montgeron France

https://www.nda-security.fr

NET FREED

N

Net Freed est un cabinet de conseil en cybersécurité. Nous accompagnons nos clients dans le choix et la mise en œuvre de réponses adaptées aux enjeux de leurs métiers, avec agilité et pragmatisme.

13340 Rognac France

http://www.netfreed.com

NETFORMATIC

E C

Prestataire spécialisé dans les services informatiques destinés aux PME : conseil, sécurité, intégration, infogérance. Accompagnement RGPD, audit fonctionnel, analyse de risques. Labellisé ExpertCyber.

69340 Francheville France

https://www.netformatic.com

NEWLODE

Newlode est un fédérateur de sociétés de service expertes sur les grandes thématiques qui composent les Systèmes d'Informations actuels : Sécurité, Cloud, Big Data, Virtualisation, Containerisation.

92038 La Défense France

http://www.newlode.io

NOMIOS

Nomios agit pour la sécurisation des réseaux informatiques d'entreprise par sa présence constante auprès des entreprises clientes.

92100 Boulogne-Billancourt France

https://www.nomios.fr

NOVENCI E C

Nous préconisons et mettons en place des solutions pour renforcer la sécurité informatique des entreprises et contrer les cyberattaques (rançongiciel ou ransomware).

1340 L'Îsle d'Espagnac France

https://www.novenci.fr

NOVIDY'S

Intégrateur Sécurité & Réseaux, Novidy's offre à ses clients des solutions, prestations et services basés sur l'écoute, la personnalisation et l'excellence technique.

78140 Vélizy Villacoublay France

https://www.novidys.com

NTT LTD.

Leader mondial des services technologiques. NTT Ltd aider les entreprises à mieux performer grâce à des solutions technologiques intelligentes - orientées données, connectées, numériques et sécurisées.

92160 Antony France

https://hello.global.ntt

NXO FRANCE N

Leader indépendant de l'intégration pour les entreprises et les administrations, NXO conçoit, déploie et exploite des solutions de Communication & Collaboration, Infrastructures digitales et Sécurité.

92500 Rueil Malmaison France

https://www.nxo.eu

OFISS

Nous sommes consultés pour auditer et préconiser des solutions cyber.

75008 Paris France

OÏKIALOG

Conseil, intégration et maintient en condition opérationnelle de solutions de sécurité des systèmes d'information, avec une très forte expertise sur les SIEM.

92300 Levallois-Perret France

http://www.oikialog.com

ON-X N H E C

ON-X, cabinet français indépendant de conseil et d'expertise, spécialisé en CyberSécurité : gouvernance, Risques et Conformité ; SecOps et Managed Detection & Response ; audits de sécurité PASSI.

92800 Puteaux France

https://www.on-x.com

OPEN GROUPE N

Éditeur de solutions digitales en mode SaaS.

92300 Levallois-Perret France

http://open.global

OPENMINDED N H

Pure player français en cybersécurité, nous réalisons des prestations de conseil, de vente et d'intégration de solutions, d'audit, de contrôle et de mise à l'épreuve de la sécurité du SI

75009 Paris France

http://www.opmd.fr

OPENSPHERE N

Cabinet de conseil international crée en 2005. OpenSphere est l'expert indépendant en cyber sécurité des DOM-TOM : Conseil, Audit de sécurité, Forensic, RSSI délégué, SOC, ISO 2700x et Formation.

97490 Sainte-Clotilde La Réunion

https://www.opensphere.fr

OPTRIUM

Créée en 2004, la société Optrium est Distributeur-Conseil-Intégrateur de solutions logicielles axées sur Gouvernance des SI (Systèmes/Données/Utilisateurs).

92000 Nanterre France

http://www.optrium.fr

OPTYMA SARL

Conseillers à la protection des données, on-demand CSO, GAP analysis, Finma, CH LPD, GDPR.

1204 Genève Suisse

https://www.optyma.ch

ORANGE CYBERDEFENSE N

Fort de son expérience d'opérateur télécoms, Orange Cyberdefense propose une approche complète de la sécurisation des actifs numériques : audit, pilotage quotidien de la sécurité, gestion de crise.

92983 Paris-La Défense France

https://www.cyberdefense.orange.com

OSINX - GROUPE ACTIMAC E C

osinx est un ESN qui propose des solutions et des services spécialisés dans la cybersécurité pour les PME, ETI et collectivités : sensibilisation, audit, mise en conformité, protection et remédiation.

14200 Hérouville Saint Clait France

https://osinx.fr

PCL ASSISTANCE INFORMATIQUE E C

Créée depuis 1994 dans les Alpes Maritimes, PCL Assistance Informatique s'est développée à partir d'une idée simple. Apporter une qualité de service adaptée aux nouvelles exigences des PME-PMI.

06800 Cagnes sur Mer France

https://www.pcl-assistance.com

PHOEBE N

PHOEBE propose un "Pré-Diagnostic", une rapide analyse de risque déclinée à partir de la méthode EBIOS et dont le résultat est un rapport commenté abordant objectivement vos risques Cyber.

83200 La Valette du Var France

https://www.phoebe

PICTIME GROUPE N

PICTIME GROUPE propose des services managés de sécurité pour les acteurs du retail, sous la marque PICTIME, et les acteurs de la santé sous la marque COREYE.

59262 Sainghin-en-Mélantois France

https://www.pictime-groupe.com

PINSENT MASONS FRANCE LLP

Cabinet d'avocat disposant d'une expertise en droit des nouvelles technologies et tout particulièrement sur les questions de cybersécurité et de réglementation applicables aux données.

75008 Paris France

http://www.pinsentmasons.com

POST LUXEMBOURG

Fournisseurs télécom et intégrateurs informatique, POST et sa filiale EBRC ont uni leurs compétences autour d'une marque unique « POST Cyberforce », pour offrir une gamme complète de services en cybersécurité.

L-1235 Luxembourg

https://www.cyberforce.eu

PPP-CONSEIL N

Consultant sécurité. Architecte réseau. Conduite de projets. Étudier la fiabilité de votre système d'information (certifier ISO 27001 27005). Audit de lignes industrielles (certification Sentryo).

56370 Le Tour du Parc France

http://www.ppp-conseil.fr

PRIAMOS

Le cabinet Priamos accompagne ses clients en proposant 4 offres différentes : Conseil, Audit et Formation en interventions courtes, et son offre Ingenierie pour un renfort au quotidien.

Toulouse 31000 France

https://www.priamos.fr

PRIVACY IMPACT

Privacy Impact - audit conseil formation - intègre les enjeux techniques et juridiques pour proposer des solutions concrètes et efficaces dans la protection des données et le respect de la vie privée.

75017 Paris France

http://www.privacyimpact.fr

PROBE I.T

Conseil en gouvernance, analyse de risque, architecture sécurisée, pentesting. Assistance MOA, pilotage de projet. Audit, conformité. Impact GDPR/RGPD.

30900 Nîmes France

PRODWARE

Une expertise au service des clients

Créé en 1989, Prodware est un Groupe international spécialisé dans l'édition-intégration et l'hébergement de solutions de gestion pour les entreprises.

75019 Paris France

https://www.prodware.fr

QUIETIC N E C

L'entreprise est spécialisée en services managés et cybersécurité, avec des solutions et méthodes pour lutter contre les risques, et intervention en cas d'attaques, sinistres ou erreurs humaines.

44300 Nantes France

https://www.quietic.fr

QUODAGIS N

Experts des services aux infrastructures, QUODAGIS vous accompagne dans votre transformation digitale dans le respect des bonnes pratiques et des contraintes de sécurité (modes projet, AT, MSP).

75008 PARIS France

http://www.quodagis.fr

QUODAGIS INTEGRATION N

QUODAGIS Integration est intégrateur spécialisé dans les solutions ITSM, ITAM et ITOA. Nous accompagnons les DSI de moyennes et grandes entreprises dans le choix des outils et leur mise en œuvre.

75008 Paris France

https://integration.quodagis.fr

QUONEX

Partout où l'Information et la Communication sont des enjeux décisifs, Quonex déploie avec précision et engagement toute son expertise.

93300 Aubervilliers France

http://www.quonex.fr

RAMPAR

Rampar se positionne comme un acteur majeur français sur les métiers de l'intégration, du Cloud et des services managés dans les domaines de la cybersécurité et des infrastructures.

92310 Sèvres France

https://www.rampar.com

REALSOFT INFORMATIQUE

Société de Service lié aux developpements de solutions spécifiques (du cahier des charges à la mise en place formation du personnel), specialiste réseaux, solutions de location serveurs.

06250 Mougins France

http://www.realsoft.fr

RECOVEO

Recoveo Forensics comprend 2 catégories : Vente d'outils et logiciels de forensics ; Service de récupération de données sur téléphone, disque dur et tous autres supports numériques.

42300 Roanne France

http://recoveoforensics.com

RISK&CO

Notre groupe déploie une offre globale de sécurisation des systèmes informatiques complexes et industriels.

92300 Levallois Perret France

https://www.riskeco.com

RLG INFORMATIQUE N

Sécurisation des comptes utilisateurs et comptes Office 365. Sécurisation des PC et serveurs. Mise en place de coffre-forts de mots de passe. Sensibilisation des utilisateurs à la sécurité.

44100 Nantes France

https://www.rlginformatique.com

SAVANE CONSULTING N

Savane-Consulting intervient de l'étude de faisabilité au délivery sur les problématiques de : Sécurité des systèmes et infrastructures informatiques ; Gouvernance sécurité du SI ; Cybersécurité.

75008 Paris France

http://www.savane-consulting.com/

SCASSI N

SCASSI, ingéniérie - conseil en cybersécurité des SI Métiers et Systèmes Critiques est basée en France et en Espagne. L'offre se compléte par le e-learning de Phosforea et les produits June-Factory.

31670 Labège France

https://www.scassi.com

SCC FRANCE N

SCC accompagne ses clients dans leur transformation IT(conseil, intégration, maintenance, financement). Nos offres : Réseau et Sécurité, Workspace, Software Asset Management, Infogérance et Maintenance.

92000 Nanterre France

http://france.scc.com/

SCHNEIDER ELECTRIC H

Prestataire d'intégration et de maintenance spécialisé en Cyber industrielle. Conforme au référentiel d'exigences PIMSEC de l'ANSSI. Intégrateur certifié Stormshield, Wallix, Sentryo. Formateur Cyber agréé.

69792 Saint-Priest France

http://www.schneider-electric.com

SCIURUS CONSEIL

SCIURUS Conseil est un cabinet de conseil français spécialisé en Cyber Sécurité.

34770 Gigean France

http://www.sciurusconseil.com

SEC-IT SOLUTIONS

Audit organisationnel et technique, tests d'intrusion, conseil, sécurité opérationnelle, formation - SEC-IT est qualifiée PASSI et accréditée CIR - Agences : Aix, Lyon, Rennes.

13290 Aix-en-Provence France

https://www.sec-it-solutions.fr

SECTOR

Accompagnement dans la mise en place de process en conformité avec les normes sectoriels.

38230 Tignieu France

http://www.sectorgroup.net

SECUREWARE E C

SecureWare est composée d'ingénieurs expérimentés, pluri-compétences capables d'accompagner nos clients dans toutes les phases d'un projet. Intégration, Conseils, Formation. Missions à l'étranger.

21600 Fenay France

https://www.secureware.fr

SECUREWORKS

SecureWorks propose des services de gestion et de surveillance sécurité (SOC), threat intelligence, réponse aux incidents au travers d'une plateforme propriétaire (CTP) ainsi que du conseil.

95870 Bezon France

SECURIVIEW SAS

Securiview offre des services SOC - Log Management- Détection d'intrusion-Réponses à incidents - Vulnerability Management - Forensic - Tests d'intrusion.

93400 Saint-Ouen France

http://www.securiview.net

SEKOIA

SEKOIA EST UNE STARTUP DÉDIÉE À LA CYBERSÉCURITÉ. Une approche globale de la sécurité et une équipe multidisciplinaire de professionnels passionnés pour (ré)inventer la sécurité avec nos clients.

75008 Paris France

https://sekoia.fr

SERMA SAFETY & SECURITY

SERMA Safety & Security est un interlocuteur unique pour la sécurité et la sureté de fonctionnement des systèmes d'information, embarqués et industriels.

75008 Paris France

https://www.serma-safety-security.com

SERVAL-CONCEPT

La société Serval-Concept est spécialisée dans les tests d'intrusions ainsi que les audits des systèmes d'information (architectures systèmes et réseaux, application, systèmes industriels, etc).

59250 Halluin France

http://serval-concept.com

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique)
H Adhérents Hexatrust

SFR BUSINESS N

Opérateur/Intégrateur de solutions et services en cybersécurité pour grands comptes, ETI & PME : conseil, audit, Pentest, Scan Vuln / protection sur mesure & packagées / exploit, services managés, SOC.

75015 Paris France

http://www.sfrbusiness.fr

SII N

Assistance au entreprise en mode régie ou forfait.

75016 Paris France

http://www.groupe-sii.com

SILICOM N

SILICOM, outre une offre basée sur le conseil (audits et préconisations), s'appuiera en 2018 sur des produits de sécurité Internet et de mobilité.

78280 Guyancourt France

http://www.silicom.fr

SMARTPOINT N

Dans un monde en constant changement, en embrassant constamment la nouveauté, Smartpoint se positionne en tant que conseiller sur la protection de vos technologies, vos données, et vos collaborateurs.

75013 Paris France

http://www.smartpoint.fr

SNS SECURITY

SNS SECURITY est une société de services indépendante, spécialisée dans la sécurité informatique défensive et offensive (pentest). Expert partner FORTINET, Gold SENTINELONE et partenaire SEKOIA.IO.

34070 Montpellier France

https://www.sns-security.fr

SOCOA SÀRL

Gérez votre entreprise, nous gérons votre (cyber) sécurité !

1025 Saint Sulpice Suisse

http://www.socoa.ch

SODIFRANCE N

Offre de conseil et d'intégration en Cybersécurité incluant un SOC, une activité d'infogérance et de formation. Réalisation d'audits (Pentest, Bug Bounty…). Expertise certifiée ISO 27001 et PASSI.

44000 Nantes France

http://www.sodifrance.fr

SO-IT E C

Intégrateur Cybersécurité

Solution de sécurité : Palo Alto Firewall et Endpoint (Cortex), SIEM LogPoint, Forescout (NAC et 802.1x), Vade (AntiSpam).

Service : Managed Detection And Response.

31100 Toulouse France

https://www.so-it.fr

SOLUCEO DGPF

Partenaire intégrateur national reconnu pour notre expertise et nos réalisations. Focus sur les projets de transformation et de modernisation des Réseaux et de la Sécurité.

38170 Seyssinet-Pariset France

https://www.soluceo.fr

SOPRA STERIA N

Acteur majeur de la cybersécurité, reconnu par l'ANSSI, Sopra Steria s'appuie sur 750 experts en Europe et propose une offre globale de services (GRC, sécurité applicative et du Cloud, SOC).

92360 Meudon la Forêt France

https://www.soprasteria.com/fr

SOSATOUTPC

L'ingénierie des systèmes : audit de l'existant ; étude de l'architecture des systèmes ; analyse des besoins réels et des pôles d'évolution ; préconisation des matériels et des logiciels.

22160 Callac France

http://www.sosatoutpc.com

SPIE ICS N

Au travers de son centre d'expertise dédié et de son partenariat avec Airbus Cybersécurity, SPIE ICS délivre un accompagnement global sur l'ensemble sujets de Cybersécurité

92240 Malakoff France

http://www.spie-ics.com

SQUAD

Protéger le patrimoine informationnel. Surveiller le cycle de vie de l'information dans et en dehors de l'entreprise. Réagir à un incident de sécurité sur les plans technique et légal.

75001 Paris France

https://www.squad.fr

STEEL PC E C

Un besoin de maintenance, de matériel, d'hébergement ou de solutions de sauvegarde? L'expérience acquise par Steel PC vous assure expertise, performance et réactivé dans vos projets IT !

57140 Norroy-le-Veneur France

https://steel-pc.fr

STRATEGY & GOVERNANCE

Strategy & Governance offre des services autour de la cyber sécurité depuis plus de 10 ans, nous intégrons la sécurité dans les organisations en vue de les aider à préserver leur patrimoine.

41170 Baillou France

http://www.strategy-and-governance.eu

SYC CONSULTANTS

Audit informatique, gouvernance informatique, assistance MOA projet ERP GED BI, commissaire aux comptes et expert comptable.

75017 Paris France

https://www.sycconsultants.fr

SYNACKTIV

Synacktiv est une société d'expertise en sécurité des systèmes d'information fondée en 2012 par des consultants ayant plus de 12 ans d'expérience dans le conseil et l'audit de systèmes informatiques.

75015 Paris France

http://www.synacktiv.com

SYNCHRONE N

Synchrone certifié ISO27001 dispose d'une communauté d'expertise constituée de plus de 160 consultants susceptibles d'intervenir sur l'ensemble du territoire national.

75002 Paris France

http://www.synchrone.fr

SYNETIS N H E C

Synetis est un cabinet de conseil et d'expertise exclusivement dédié au domaine de la Cybersécurité avec une offre globale conçue pour répondre à l'ensemble des besoins de sécurisations des SI.

75008 Paris France

https://www.synetis.com

SYNEXIE E C

Synexie expert en cybersécurité accompagne ses clients dans l'évolution et le maintien en condition opérationnelle des infrastructures systèmes et réseaux sécurisés.

83000 Toulon France

https://www.synexie.fr

SYSDREAM N

Sysdream division Cybersécurité de Hub One propose une gamme de solutions axées sur l'audit, la formation et le cyber-entrainement.

92300 Levallois-Perret France

https://www.sysdream.com

SYSTEMIS N

Maîtrisez en toute autonomie vos risques cyber grâce aux talents de SYSTEMIS et aux solutions de cybersécurité souveraines françaises (Gouvernance, Audit, Identité, Intrusion, DevSecOps, Formation).

94270 Le Kremlin-Bicêtre France

https://www.systemis.eu

TALC SI E C

Talc SI est une société de service spécialisée dans la gestion, l'optimisation et la sécurisation des systèmes d'information (serveur, stockage, sauvegarde/restauration, virtualisation,cybersécurité).

95130 Franconville France

https://www.talcsi.com

TECODATA

Créée en 2003, nous sommes spécialisés dans le déploiement de matériel ainsi que dans la mise à disposition de ressources techniques (de Technicien Itinérant à Consultant Big Data & Cybersécurité).

79270 Frontenay Rohan Rohan France

http://www.tecodata.fr

TEOS CYBERSECURITY

Gouvernance (RSSI de transition / à temps partiel, sous-traitance RSSI, politiques SSI, analyses de risques…). Audit & conformité (TI, audits, conformité RGPD). Sécurité IoT & industrielle.

17000 La Rochelle France

http://www.teos-cybersecurity.com

TGS FRANCE INFORMATIQUE

E C

Une offre complète de solutions et de conseils : logiciels de gestion, ERP, Paie & RH, BI & DATA, infrastructure, maintenance, infogérance, conseil en systèmes d'information et en cybersécurité.

49070 Beaucouze France

https://www.tgs-france.fr

TIBCO

N

Chez Tibco, nous mettons l'humain au cœur de la sécurité de l'information: Des hommes, des process, des outils et de la gouvernance pour vous aider à agir au plus près des métiers et des utilisateurs.

44860 Saint-Aignan de Grand Lieu France

http://www.tibco.fr

TNP CONSULTANTS

N

Stratégie & Gouvernance SSI, Protection des données, Audit de sécurité, Tests d'intrusion Analyses de risque, Privacy & Security by design, Certification Privacy & Security, Forensics, SOC, Formation.

92200 Neuilly-sur-Seine France

https://www.tnpconsultants.com/fr

TRAX

N

Trax est une agence de conformité digitale, qui accompagne les entreprises à la certification ISO 27001 (sécurité des systèmes d'information), via des prestations d'audit, de formation et de conseil.

92300 Levallois-Perret France

http://www.trax.solutions

TRÈFLE SOLUTION

Nous sommes spécialisés dans la protection de l'information et la sécurité des systèmes d'information. Nous intervenons sur des problématiques en cybersécurité de type technique et organisationnel.

92100 Boulogne-Billancourt France

http://www.groupetrefle.com/solution

TRSB

N

L'offre TRSb s'articule autour de quatre expertises métiers : le conseil, la stratégie & l'innovation, le développement & l'intégration de solutions, les services managés et l'expérience utilisateurs.

75008 Paris France

http://www.trsb.net

T-SYSTEMS

N

T-Systems propose les compétences des 1 400 experts de sa Division Magenta Security, des opérations de solutions périmétriques et SIEM/SOC au Consulting sur le protection et les réponses.

92500 Rueil-Malmaison France

http://www.t-systems.com

UBCOM SA

Préparer et organiser nos clients à la cybersécurité avec une gouvernance, des outils, du comportement, du juridique, de l'innovation et de l'intelligence. Analyse du risque cyber.

1920 Martigny Suisse

http://www.ubcom.ch

UBG. CYBER

UBG. Cyber est un cabinet indépendant spécialisé dans l'audit, le conseil et la formation en Cyber Threat Intelligence, Cyber-défense, cybersécurité et cybercriminalité.

69002 Lyon France

https://cyber.ubg-interactive.com

UNUMKEY

Labellisée France Cybersecurity, UnumKey propose des prestations de conseil, d'audit et de formation à destination des entreprises privées et publiques.

51100 Reims France

https://www.unumkey.fr

UPPER-LINK

Certifiés ISO 27001 et professionnel en sécurité informatique référencé par Cybermalveillance.gouv.fr, Upper-link est spécialisée dans la transformation digitale et les solutions cloud.

77185 Lognes France

https://www.upper-link.com

URAEUS CONSULT

N

Spécialisée en Cybersécurité : Audit de SI, Évaluation du risque, Accompagnement à la certification ISO27001, Conformité RGPD et ISO27002. Risk Managers certifiés ISO27005 LSTI Grade.

06560 Sophia-Antopolis France

http://www.uraeus.fr

UTIKXO

UTIKXO est un cabinet de conseil en organisation et processus spécialisé dans la protection et la conformité du patrimoine numérique de l'entreprise: cybersécurité, intelligence économique, privacy.

75017 Paris France

https://www.utikxo.com

VAADATA

Vaadata est une entreprise spécialisée en tests d'intrusion. 3 types d'audits: black box, grey box, ingénierie sociale. Périmètre des tests: plateformes web/mobile, objets connectés, facteur humain.

69009 Lyon France

https://www.vaadata.com

VEYAN

N

VEYAN est une société de conseil, organisationnel et politique, en cybersécurité. Notre gamme d'accompagnement porte sur la gouvernance de la sécurité de l'information et sur la conformité au RGPD.

56520 Guidel France

https://www.veyan.fr

VFLIT OMR INFOGÉRANCE

44230 Saint-Sébastien-sur-Loire France

https://vflit.fr

VNEXT

N

vNext est une société de conseil. Nous intervenons dans trois domaines d'activités : Business Consulting, IT Consulting et Managed Services.

75014 Paris France

http://www.vnext-group.com

WALLACK

E C

Wallack intervient comme Responsable de la Cybersécurité de ses clients. De la construction d'une feuille de route jusqu'à la conformité terrain, nous intégrons la cybersécurité à votre organisation.

35135 Chantepie France

https://www.wallack.fr

WANCORE

Nous délivrons notre expertise en ingénierie Réseaux (architectures LAN/WAN) et CyberSécurité selon 3 modes d'intervention : Conseil, Intégration et MCO N3. Clientèle CAC 40 à ce jour.

75008 Paris France

http://www.wancore.fr

WANNATH

E C

WANNATH est un cabinet de conseil spécialisé dans l'efficience des Systèmes d'Information et plus particulièrement dans le domaine de la cybersécurité : Conseil, audit et accompagnement.

75008 Paris France

https://www.wannath.com

WAPLI INFORMATIQUE

E C

Accompagnement des PME pour l'ensemble de leurs besoins informatiques/numériques : audit, conseil, intégration, réseaux, infogérance, sauvegardes et cybersécurité. Certifié ZyXEL Security Specialist.

82000 Montauban France

https://www.wapli-informatique.fr

WAPSI

Accompagnement de clients dans le choix de solutions outillées et de solutions à la régie et au contrat d'assistance, sur les éléments vecteurs de failles de sécurité (utilisateur, application, Cloud).

75008 Paris France

https://www.aerow.group

WAVESTONE

N

Wavestone est le leader du conseil en cybersécurité et confiance numérique en France avec plus de 500 consultants dédiés et la capacité à adresser des grands projets internationaux.

92042 Paris-La Défense Cedex France

http://www.wavestone.com

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique)
H Adhérents Hexatrust

WEODEO

Notre approche est ou peut être globale au regard du parcours du dirigeant. notre offre est donc sur mesure… en fonction de votre contexte, de vos besoins.

75013 Paris France

http://www.weodeo.com

WISE PARTNERS

WISE Partners est un Cabinet de conseil indépendant, spécialisé en cyber-sécurité et confiance numérique.

75116 Paris France

http://www.wise-partners.fr

XMCO

Cabinet de conseil en SSI, XMCO intervient dans de projets au forfait. Fondé en 2002 et dirigé par ses fondateurs, XMCO s'est imposé grâce à son expertise et son discours transparent.

75002 Paris France

http://www.xmco.fr

XPERIZ N

Analyse de risques (EBIOS, ISO 27005). Posture permanente de sécurité : intégration de la sécurité dans les projets, et comportements. Pilotage des plans d'actions issus des audits. Gestion de crise.

75004 Paris France

http://www.stratops.fr

YEC'HED MAT CONSEIL

Yec'Hed Mat est un cabinet de conseil et de formation dans la mise en conformité avec le RGPD et appliqué spécifiquement à la santé auprès des cliniques, start-up, CRO et industrie pharmaceutique.

33800 Bordeaux France

https://yeched-mat.com

YOGOSHA SAS N H

Yogosha est une plateforme de Bug Bounty qui permet à ses clients de mettre en œuvre une recherche de vulnérabilités en rémunérant les chercheurs à la faille découverte.

92514 Boulogne Billancourt France

https://www.yogosha.com

YOURAX E C

Yourax et son équipe de consultants hautement certifiés en cybersécurité, vous accompagne dans la mise en place de solutions informatiques : Sécurité, Cloud, Infrastructure, Réseau & Wifi.

59223 RONCQ France

https://www.yourax.fr

ZENIKA N

Zenika s'inscrit dans une démarche d'amélioration continue et de mise en place de la sécurité chez ses clients en leur apportant conseil et expertise dans les grands domaines.

75009 Paris France

http://www.zenika.com

ZERO TRUST SAS

Spécialiste des environnements Cloud, pure player sur le conseil en sécurité Cloud 2.0, avec une réelle indépendance. Conseil de solution et intégration, Conseil et audit, SOC de nouvelle génération

93200 Saint Denis France

https://zerotrust.fr

ENTREPRISES SPÉCIALISÉES, RÉFÉRENCEZ-VOUS SUR L'ANNUAIRE EN LIGNE

Les informations de ce guide sont issues de l'annuaire en ligne. Les sociétés spécialisées en cybersécurité doivent se référencer et mettre à jour régulièrement leur fiche.

Attention, l'annuaire est réservé aux entreprises réellement spécialisées en cybersécurité. La rédaction valide la création des fiches.

Inscription et mise à jour :

https://www.solutionsnumeriques.com/securite/ annuaire-cybersecurite/

Formation

2600 H

L'École 2600 est un organisme de formation spécialisé dans la cybersécurité; notre but est de remédier à la pénurie d'experts opérationnels en cybersécurité. Nous recrutons à Bac+3 pour 3 ans d'études.

78180 Montigny le Bretonneux France

https://ecole2600.com

4CYSEC N

4CYSEC vous accompagne dans vos projets liés à Cybersécurité et à la protection des données : FORMATION - AUDIT - FORENSIC - COMPLIANCE (RISK MANAGEMENT, ISO, EBIOS, PENTEST, ISO2700x, GDPR, DPO...).

75012 Paris France

https://4cysec.io

AASTERIA N

Face aux menaces de vol de données en entreprise Aasteria forme vos salariés à identifier les risques et postures à adopter. Dotez vous des capacités de confiance indispensables à votre développement.

92400 Paris-La Défense France

http://aasteria.com

APPSECFR

Formation en Sécurité des Applications. Nous formons dans les cadres réglementaires PCI-DSS chapitre 6. Ainsi qu'autour des référentiels de type OWASP.

79000 Niort France

https://www.appsec.fr

BLUECYFORCE

Premier centre d'entraînement opérationnel à la cyberdéfense en France, BLUECYFORCE propose des parcours immersifs, individuels ou collectifs, afin d'intensifier l'apprentissage « par la pratique ».

75015 Paris France

https://www.bluecyforce.com

CLÉON CONSEIL

Conseil et formation : RGPD sensibilisation, formation des DPO/DPD, CODIR ; assistance à maitrise d'ouvrage DSI ; conseil DSI ; diagnostic numérique EHPAD.

31700 Cornebarrieu France

http://www.cleon.cc

CONSCIO TECHNOLOGIES H

Conscio Technologies est le spécialiste des solutions de sensibilisation des utilisateurs. Son offre est constitué de contenus de sensibilisation et des solutions logicielles de gestion de campagnes.

75002 Paris France

http://www.conscio-technologies.com

DMR N

DMR (Développement Multimédia et Réseaux), centre de formation, forme au niveau régional, national et international les RSSI, DPO, Experts Cyber sécurité, Analyste SOC, Architectes sécurité, Administrateurs et Développeurs, etc.

13170 Les Pennes-Mirabeau France

http://www.dmr-formation.fr

ÉCOLE DE GUERRE ÉCONOMIQUE

L'École de guerre économique (EGE) propose des formations en intelligence économique, cyber et sûreté. Elle est l'organisme certifiant pour l'obtention du Titre « Expert(e) en intelligence économique ».

75007 Paris France

http://www.ege.fr

EDUGROUPE

EduGroupe accompagne les entreprises dans leurs projets de formations liées à la Sécurité informatique, Cybersécurité, Management des risques, ISO, EBIOS, Développement sécurisé, Sécurité cloud, IOT.

75016 Paris France

https://www.edugroupe.com

EXPERNET N

Expernet est un centre de formation Informatique, une école informatique et formation e-learning. Domaines : Bureautique, Système et Infrastructure réseaux, Infographie, Gestion de projet, CAO, PAO.

97420 Le PORT France

http://www.expernet.fr

GLOBAL KNOWLEDGE

Notre offre de formations et de certification couvre les solutions techniques éditeurs et les référentiels métiers de la cybersécurité (Normes ISO, CISSP, CRISC, CISM, CCSP, sans oublier le RGPD).

92500 Rueil-Malmaison France

https://www.globalknowledge.fr/securite

HS2 N

HS2 (Hervé Schauer Sécurité) propose un programme complet de formations inter-entreprises en cybersécurité technique et organisationelle, droit de la cybersécurité, protection des donnéesl (DPO/RGPD) et continuité d'activité.

92200 Neuilly-sur-Seine France

http://www.hs2.fr/

IPSSI

L'IPSSI, grande école d'informatique, Web et Digital Marketing implantée à Paris, Marne-la-Vallée, Brest et Nice forme les étudiants du Bac au Bac+5 en alternance, aux métiers des technologies.

75012 Paris France

https://www.ecole-ipssi.com

PHOSFOREA N

PHOSFOREA est experte en sensibilisation et formation à la cybersécurité en e-learning et présentiel. PHOSFOREA a créé la première application mobile de sensibilisation à la cybersécurité.

31670 Labège France

https://www.phosforea.com

ŒIL POUR ŒIL CRÉATIONS

Œil pour Œil CRÉATIONS propose formations à distance, e-learnings et Serious Games pour acculturer les collaborateurs d'une entreprise à la la protection des données ou GDPR - RGPD, la cybersécurité, ou la lutte anticorruption, grâce à la puissance de la gamification.

59000 Lille France

https://www.oeilpouroeilcreations.fr

PÔLE FORMATION UIMM BRETAGNE

L'École supérieure du numérique appliqué propose, en intra ou inter entreprise, des formations continues selon les 7 modules de l'ANSSI (3 en tronc commun et 4 spécialisés).

35170 BRUZ France

https://www.esna.bzh/esna/cyberdefense

SANS INSTITUTE

SANS, référence mondiale en matière de formation dans le domaine de la cybersécurité, propose plus de 60 cours, qui s'alignent sur les rôles, responsabilités et disciplines des équipes de sécurité.

20852 North Bethesda, MD États-Unis

https://www.sans.org

SECURESPHERE BY EPITA

SECURESPHERE by EPITA propose des formations professionnelles à la cybersécurité pour tous les collaborateurs. Ces modules couvrent aussi bien la sensibilisation que l'approfondissement technique.

94270 Le Kremlin Bicêtre France

https://www.securesphere.fr/index.php

TERRANOVA SECURITY

Chef de file mondial en sensibilisation à la sécurité, nous aidons les RSSI à mettre en place des programmes de simulation de phishing, de sensibilisation à la cybersécurité et de formation RGPD.

H7S 2N5 Laval Canada

https://terranovasecurity.com/fr

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique)
H Adhérents Hexatrust

Hébergeurs - Data Center

3DS OUTSCALE N H

Fondé en 2010 et filiale de Dassault Systèmes, 3DS OUTSCALE fournit un Cloud Nouvelle Génération qui offre des services évolutifs, performants et sécurisés partout dans le monde.

92210 Saint-Cloud France
https://fr.outscale.com

AZNETWORK N

Réalisation d'analyses de risque et de plans de traitement des risques.

61000 Alençon France
https://aznetwork.eu

BRETAGNE TÉLÉCOM

Bretagne Télécom vous propose un hébergement sur mesure dans notre Data Center certifié ISO 27001 et HDS. Plusieurs solutions sont disponibles : Cloud privé, hébergement de données de santé, Housing…

35220 Châteaubourg France
https://www.bretagnetelecom.com

CELESTE

Baies 15 kVA, Suites 100 kVA
Fibre optique 1 à 10 Gb/s
6 opérateurs
Taux de disponibilité 100 %
Double chaîne électrique jusqu'à la baie
Surveillance 24/7
P.U.E. 1,3"

77420 Champs-sur-Marne France
https://www.celeste.fr

COREYE N

Avec CoreTrust, COREYE (MSP et MSSP) propose des services managés de sécurité (Anti-DDoS, Waf, SIEM, Scan de vulnérabilité, SOC externalisé) pour sécuriser vos données. COREYE est ISO 27001 et HADS.

59262 Sainghin-en-Mélantois France
https://www.coreye.fr

DATA4 GROUP

DATA4, opérateur de data centers en Europe, dispose de réserves foncière et électrique (121 ha et 146 MW disponibles) uniques sur le marché européen pour accompagner la croissance de ses clients.

91460 Marcoussis France
https://www.data4group.com

ESPRIT H

Gamme de Firewalls, SOC,SIEM, exploitation des failles, Kali Linux.

2037 Ariana Tunisie
http://www.esprit-tn.com

EXODATA

Exodata est un MSP qui place la sécurité au cœur de son offre. Elle accompagne ses clients dans leur transformation digitale, avec un support 24/5 sans surcoût grâce à un positionnement Follow the Sun.

75001 Paris France
https://www.exodata.fr

FULLSAVE N

Opérateur Cloud et télécom indépendant, FullSave propose des solutions IaaS de type Cloud privé.
FullSave a construit et mis en service en 2014, le datacenter TLS00 (1 600 m²).

31670 Labège France
http://www.fullsave.com

GROUPE CYLLENE N

Cyllene.Cyber planifie, organise, déploie, pilote et mesure tout en satisfaisant aux obligations réglementaires et aux exigences juridiques et assurantielles.

92000 Nanterre France
https://www.groupe-cyllene.com

IBO

Les services d'hébergement, les services d'infogérance, les services liés à la sécurité informatique, IBO est agréé depuis 2013 par le Ministère de la Santé en tant qu'Hébergeur de Données de Santé.

63014 Clermont-Ferrand Cedex 2 France
http://www.ibo.fr

IKOULA

Ikoula spécialiste, des serveurs dédiés et du Cloud depuis 1998. Propriétaire de 2 DataCenters en France et présent à l'international (filiale aux Pays-Bas), Cloud disponible sur 3 continents.

92100 Boulogne-Billancourt France
https://www.ikoula.com/fr

INFOCLIP N

Le Groupe Infoclip propose d'accompagner ses entreprises clientes dans l'exécution de leurs projets de transformation digitale.
Infoclip met en place et infogère les systèmes de sécurité.

75019 Paris France
http://www.infoclip.com

JAGUAR NETWORK H

Jaguar Network est un opérateur cloud souverain qui accompagne plus de 1.000 clients pour valoriser leurs données grâce à 15 ans d'expertise en Cloud, Telecom, Big Data, IoT et services nanagés.

13321 Marseille France
https://www.jaguar-network.com

KABIA N

Services d'hébergement, Kabia est un opérateur Cloud souverain français fournissant des services managés à haute valeurs ajoutées tout en respectant les contraintes et processus métier des nos clients.

06100 Nice France
https://www.kabia.eu

LEVEL 3 COMMUNICATIONS

Level 3 dispose d'un portefeuille complet de services de sécurité basés sur son réseau international qui permet d'avoir une vision complète de la cartographie des menaces au niveau mondial.

92000 Nanterre France
http://www.level3.com/en

NEOJEDI

Clood le cloud à la française est une solution de stockage, de sauvegarde et de partage en ligne pour tous types & formats de documents, ultra sécurisée et entièrement localisée en France.

31500 Toulouse France
https://clood.co

OT GROUP

OT Group fait de la protection des données de ses clients son enjeu n°1 et propose : architecture Cloud, infogérance SI ; SaaS ; Web, interconnexion réseaux, SecOps, DevOps et sécurité informatique.

44800 Saint Herblain France
https://www.ot-group.com

RÉSEAU CONCEPT N

Pionnier de l'Internet, fondée en 1995, Réseau Concept dispose de ses propres data center. Nous infogérons plusieurs centaines de PME/PMI et ETI.

21000 Dijon France
https://www.reseau-concept.com

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction. Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

SYNAAPS

SynAApS fournit des services d'hébergement Cloud souverain (PaaS-IaaS, PRA-PCA, infogérance et Housing) haute qualité, doublement certifiés sécurité (ISO 27001:2013) et agréés Santé (HADS).

69603 Villeurbanne Cedex France

https://www.synaaps.com

TDF

TDF propose des services d'infrastructures sur l'ensemble du territoire : Datacenter, connectivité haut débit (fibre optique, faisceau hertzien), transit IP, liaison sécurisée vers les Clouds publics.

92120 Montrouge France

http://www.tdf-telecom.fr

T-SYSTEMS FRANCE N

T-Systems opère des solutions de « Security as a Service » pour les protections, analyses et réponses aux risques et attaques. Ses 1 200 experts ont intégré et opèrent le Best-of-Breed des solutions.

93200 Saint-Denis France

VENDOME SOLUTIONS

Vendôme propose à ses clients la conception de data center sur-mesure et un hébergement dans ses locaux, en plein cœur de Paris.

25000 Besançon France

https://www.groupetenor.com

XEFI

XEFI - Leader des services informatiques auprès des TPE / PME.

63170 Aubière France

http://www.xefi.fr

YULPA N

YULPA propose des services d'hébergements et vous accompagne sur la sécurisation et l'audit de vos infrastructures hébergées chez YULPA ou en interne. Infrastructure intégralement en France.

75008 Paris France

https://yulpa.io

Avocats spécialisés

CABINET SFEZ AVOCATS

Domaines d'expertise : droit des Data et des technologies avancées, et Propriété intellectuelle. Prestations : rédaction et négociation de contrat, audit juridique, étude de faisabilité et formation.

75009 Paris France

https://www.avocats-sfez.fr

CHRISTIANE FERAL-SCHUHL SAINTE-MARIE AVOCATS

Depuis près de 30 ans, Christiane Feral-Schuhl éxerce dans le secteur du droit de l'informatique, des nouvelles technologies, des données personnelles et de la propriété intellectuelle, dont elle est un acteur reconnu.

75016 Paris France

www.feral-avocats.com

ITEANU AVOCATS

Société d'Avocats composée de 13 professionnels à l'activité quotidienne dédiée droit du numérique, conseil et défense de ses clients, depuis 28 ans. La cybersécurité est au coeur de sa pratique.

75008 Paris France

http://www.iteanu.com

LE NINIVIN AVOCAT

Le cabinet dispose d'une solide expérience dans la prévention des risques, la rédaction des contrats, la gestion des litiges associés, y compris les expertises techniques et la défense pénale.

75008 Paris France

LEXING ALAIN BENSOUSSAN AVOCATS

Le cabinet a été fondée 1978 par Aain Bensoussan, avocat à la Cour d'Appel de Paris et est spécialisé dans le droit de l'informatique.

75017 Paris France

https://wwww.alain-bensoussan.com

MATHIAS AVOCATS

MATHIAS Avocats vous accompagne tant en conseil qu'en contentieux de manière dédiée dans votre conformité juridique (contrats, conformité RGDP, droit des affaires).

75017 Paris France

http://www.avocats-mathias.com

PINSENT MASONS FRANCE LLP

Cabinet d'avocat disposant d'une expertise en droit des nouvelles technologies et tout particulièrement sur les questions de cybersécurité et de réglementation applicables aux données.

75008 Paris France

http://www.pinsentmasons.com

Consultants indépendants

CONSEILPREV

Christophe CERF, 30 years expertise mutli-sectors, multi-projects (OilGas, Power, Renewables, Automotive, Buildings).
Cybersécurité des Systèmes Industriels IT/OT, Architect & Design.

75014 Paris France

https://conseilprevup.com

CYBERWORKS

Conseil et audit autour des normes ISO 27001/27701/HDS et des référentiels de l'ANSSI : PASSI, SecNumCloud, PDIS, PRIS, PAMS.

44100 Nantes France

https://www.cyberworks.fr

LE NET EXPERT

Expert informatique formé par la CNIL.
Spécialisé en cybercriminalité et en protection des données personnelles.
Audits. Accompagnements. Formations. Forensic.

84300 Cavaillon France

https://www.lenetexpert.fr

TANCO & CO

Agence Technologique. Consulting sureté et sécurité informatique. Expert cybersécurité. Design et intégration de solutions sur mesure. Alarme, contrôle d'accès et vidéoprotection. Éditeur de logiciel.

06250 Mougins France

https://www.tanco.fr

TRANSFERTPRO

Nous simplifions et sécurisons l'envoi, le stockage et le partage de fichiers en entreprise grâce à nos solutions.
Certification CSPN et la Qualification élémentaire délivrées par l'ANSSI.

75017 Paris France

https://www.transfertpro.com

E C Label ExpertCyber
N Adhérents Numeum (ex Syntec Numérique)
H Adhérents Hexatrust

Distributeurs

ABBAKAN
Distributeur à valeur ajoutée spécialisé dans la commercialisation de solutions de cybersécurité à destination des intégrateurs, revendeurs et Telecoms du secteur des technologies de l'information.
92400 Courbevoie France
http://www.abbakan.com

ARROW ECS FRANCE
Spécialiste de la distribution de solutions d'infrastructure et de services dans les domaines des serveurs d'entreprise, stockage, logiciels et virtualisation pour les professionnels de l'informatique.
92600 Asnières sur Seine france
http://www.arrowecs.fr

CERBERIS
Forte de son expérience, la société Cerberis a su nouer des partenariats forts avec les plus grands acteurs du marché, lui permettant aujourd'hui de proposer à ses clients et partenaires des solutions.
38100 Grenoble France
https://www.cerberis.com

CONFIG
CONFIG propose des solutions par le biais de partenariats avec des acteurs reconnues de l'IT. Ceux-ci dispensent des formations et des compléments de compétences pour assurer leur savoir-faire.
75019 Paris France
https://www.config.fr

D2B INFORMATIQUE
Distributeur de solutions d'infrastructure, spécialisé dans les domaines de la protection des données, du Data Management et de la sécurité informatique.
93100 Montreuil France
http://www.d2b.com

DYNAMIT
Société de services et de distribution informatique nous fournissons, en plus du matériel et des logiciels, de l'assistance, de la maintenance, des services de protection et de cybersécurité.
92000 Nanterre France
https://www.dynamitservices.fr

EXCLUSIVE NETWORKS
Spécialiste mondial de la cybersécurité de confiance pour les infrastructures numériques, dispose de bureaux dans 40 pays, propose « Solution Zone » et le PowerLab pour une démonstration technique des intégrations en temps réel.
92100 Boulogne Billancourt France
https://www.exclusive-networks.com/fr

FEEDER
Offre vidéosurveillance, écosystème et les acteurs du marché de la vidéosurviellance.
13127 Vitrolles France
http://www.feeder.fr

GROUPE DFM
Groupe DFM accompagne les entreprises avec ses 4 expertises : informatique (infogérance & réseaux), télécoms, impression & solutions documentaires, et sécurité électronique.
94000 Créteil France
https://groupe-dfm.fr

INFINIGATE
Infinigate est un distributeur spécialisé dans la fourniture de solutions de sécurité informatique. Pare-feu, Endpoints, authentification forte, audit… notre catalogue répond à tous les besoins.
92100 Boulogne-Billancourt France
http://www.infinigate.fr

INGRAM MICRO
Grossiste en produits technologiques, Ingram Micro offre aux partenaires un accès aux dernières technologies et solutions gérées, notamment le cloud, la configuration, la chaîne d'approvisionnement et le cycle de vie des actifs.
59810 Lesquin France
https://fr.ingrammicro.eu

MIEL
MIEL propose un éventail complet et complémentaire de technologies pour sécuriser l'informatique d'entreprise à l'ère du Cloud, protégeant endpoints, IoT, accès SaaS, réseaux, e-mails, identités…
91570 Bièvres France
https://www.miel.fr

NEOVAD
NeoVAD est distributeur de solutions innovantes autour du (DEM) Digital Experience Monitoring, du SASE (Secure Access Service Edge), et de la sécurité.
92100 Boulogne-Billancourt France
http://www.neovad.fr

TECH DATA FRANCE
Tech Data est un leader européen de la distribution de produits et services technologiques pour les réseaux de revendeurs.
776111 Bussy St Georges Marne-La-Vallée
https://fr.techdata.com

WATSOFT DISTRIBUTION
Watsoft propose une gamme complète de solutions de cyber-sécurité qui permet de minimiser et d'anticiper sensiblement les menaces, les cyber-attaques, les ransomwares, etc.
33600 Pessac France
https://www.watsoft.com

WESTCON-COMSTOR FRANCE
Distributeur à valeur ajoutée de solutions de pointe dans les domaines de la sécurité, la collaboration, les réseaux et les Data Centers, disposant d'un réseau mondial de revendeurs spécialisés.
92600 Asnières sur Seine France
https://www.westconcomstor.com/fr/fr.html

Recrutement

UVU GROUP
Cabinet de recrutement et management de transition spécialisé dans la gestion des risques d'entreprise et Cybersécurité pour le compte des grandes PME, ETI et groupes internationaux.
92000 Nanterre France
https://www.uvu-group.com

Cyber-assurance

BESSÉ
Bessé est conseil en assurances des entreprises. Le transfert à l'assurance du risque cyber renforce la chaîne de valeur de la cybersécurité. Nos experts vous accompagnent dans vos démarches.
44000 Nantes France
https://www.besse.fr/fr

CNC-EXPERTISE
CnC Expertise est un cabinet d'expertise en assurance spécialisé dans les réponses à incident cyber et les sinistres liés aux technologies de l'information.
78600 Maisons-Laffitte France
https://www.cnc-expertise.com

Les acteurs du marché

Panorama
Solutions et Services
Tableaux Comparatifs

- **Panorama des solutions** tableaux comparatifs p190
- **Panorama des services** tableaux des prestataires p204

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.
L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Consultez le site web, qui peut comporter des mises à jour :
www.solutions-numeriques.com/securite/annuaire-cybersecurite/.

Les éditeurs et sociétés de services peuvent se référencer ou mettre à jour leur fiche existante sur la même page.

Éditeurs de

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
3D-OXIDES						●	●	●							
3M FRANCE	●			❊											
6CURE			●												
8MAN	●					●					●				
A10 NETWORKS		●	●	●		●									
ACG CYBERSECURITY	●	●	●	●		●	●		●						
ACRONIS	●							●							
ADVANCED TRACK & TRACE	●			❊	●	●									
AF SOFTWARE		●	●												
AFFINION INTERNATIONAL	●	●		●		●			●			●			
AIRBUS CYBERSECURITY	●		●		●				●			●	●		
ALEKSO	●	●	●	●		●			●						
ALGOSEC											●	●	●		
ALHAMBRA SYSTEMS SA	●	●	●		●	●	●	●				●	●	●	●
ALINTO	●	●	●	●										●	
APICEM SARL	●	●		●					●						
AQUA SECURITY		●										●	●		
ARCSERVE	●	●							●	●					
ARS NOVA SYSTEMS	●	●		●											
ARX ONE	●														
ATEMPO	●								●						
ATOS	●	●	●	●		●	●	●	●	●	●	●	●	●	●
AVANT DE CLIQUER									●			●	●		
AVAST SOFTWARE		●	●			●	●		●				●		
AVIRA	●	●	●	●		●	●		●			●	●		
AXWAY SOFWARE	●	●													
B<>COM	●		●	●		●	●	●							
BALABIT	●		●			●									
BARRACUDA NETWORKS	●	●	●				●						●		
BEEMO TECHNOLOGIE	●														
BERTIN IT	●		●	●	●				●			●	●		
BETA SYSTEMS	●	●				●	●				●	●		●	
BEWARE CYBERLABS			●		●	●	●		●		●		●		
BEYONDTRUST	●	●		●	●	●	●		●		●		●		
BE-YS SOFTWARE	●	●				●		●							
BITDEFENDER	●	●	●	●	●		●		●			●	●		
BLOCKPROOF	●														
BMC SOFTWARE		●	●						●			●	●	●	●
BOLDON JAMES	●			●					●	●					
BOX	●	●		●					●	●					
BRAINWAVE GRC	●	●				●	●			●	●	●			

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Solutions

Protection							Exploitation							Saas	Adhérent	
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	HEXATRUST
	●	●					●		●							
		●		●												
			●		●					●						●
	●	●					●	●		●	●	●	●			
			●		●		●			●	●	●	●	●		
		●														
	●											●	●			
	●	●	●	●	●	●	●									
		●		●		●										
●		●		●	●				●		●					
			●		●		●		●	●	●					
●	●	●	●	●	●		●	●	●		●	●		●		
●		●	●		●		●		●	●	●			●		
	●	●					●							●		
			●				●									
		●		●	●		●							●		
		●				●								●		
		●												●		
		●	●	●	●											●
●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●
		●		●						●				●	●	
●	●	●	●	●	●	●										
●		●		●		●	●			●	●		●			
	●	●								●				●	●	
	●	●			●									●	●	
	●				●			●	●	●						
●	●	●	●		●					●			●			
		●													●	
●		●			●											●
	●	●					●			●		●	●			
●					●					●		●	●			
	●	●	●	●	●	●				●						
	●															
●		●	●	●	●	●	●		●	●	●	●	●	●		
●			●	●	●		●	●		●	●	●	●	●	●	
		●					●			●			●			
		●				●								●		
	●									●		●	●			●

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
CA TECHNOLOGIES	●	●	●	●		●	●			●		●			●
CAILABS			●												
CECURITY.COM	●	●		●		●								●	
CERTIGNA	●	●		●		●									
CERTINOMIS						●									
CHAMBERSIGN FRANCE						●									
CHECK POINT SOFTWARE TECHNOLOGIES	●	●	●	●	●	●	●		●	●	●	●	●	●	
CHECKMARX	●	●											●		
CISCO SYSTEMS FRANCE			●				●					●	●	●	
CITALID	●	●	●	●	●	●			●		●	●	●		
CLOUD ECO	●		●	●					●						
COFENSE	●		●												
CYBELIUS					●						●				
CYBERARK	●	●				●	●		●		●	●	●		
CYBEREASON	●	●	●	●	●				●		●		●	●	
CYBERNETECH SAS	●	●	●						●						
CYBERRES MICRO FOCUS	●	●				●			●	●	●	●	●	●	●
CYBERWATCH		●	●		●				●		●	●	●		
CYBONET	●		●				●		●			●	●	●	
CYNET - HOLISTIC SECURITY SIMPLIFIED									●			●	●		
DANTOOIN	●	●				●				●		●	●		
DARKTRACE		●	●		●		●		●				●	●	
DELL (CYBER RECOVERY)	●	●				●			●	●	●				
DHIMYOTIS	●	●				●	●		●						
DIGITAL GUARDIAN	●	●	●	●						●					
DIGITALSACE	●	●	●	●					●			●	●		
DIGITEMIS (SOFTWARE)	●	●	●	●	●		●		●		●	●			
DISKYVER		●	●	●					●			●	●		
DMARC EXPERT		●				●									
DOCAPOSTE ARKHINEO	●	●													
DOCTOR WEB FRANCE	●	●	●	●					●						
EDSI	●	●		●			●								
EFFICIENTIP	●		●						●			●	●		
EGERIE	●	●	●	●	●	●	●	●	●		●	●			
EM2B	●														
ENTRUST	●					●	●	●							
EQUISIGN	●	●							●	●					

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent	
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	HEXATRUST
	●	●	●			●	●			●				●	●	
		●			●											
		●												●	●	
	●	●												●		
	●													●	●	
	●															
●	●	●	●	●	●	●	●	●	●	●	●	●	●			
			●				●			●				●		
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		
●							●		●	●				●		
		●		●	●	●										
●									●		●			●		
														●		
	●	●	●	●	●		●				●		●	●		
●		●	●	●	●	●	●	●	●	●	●	●	●	●		
	●	●	●	●	●			●						●		
●	●	●	●	●	●		●	●	●	●	●	●		●		
				●	●				●	●						●
●				●	●			●		●	●	●	●			
●		●		●	●				●		●	●				
●	●	●	●										●	●		
●					●				●	●	●	●	●	●		
●	●	●	●	●		●		●	●	●	●	●	●			
	●	●		●											●	
		●									●			●		
		●		●	●						●		●			
		●												●	●	●
●			●	●	●		●		●	●				●		
		●		●										●		
		●												●	●	●
		●		●	●	●							●	●		
		●				●								●	●	
		●			●		●	●	●				●	●		●
									●	●	●			●		●
		●			●									●		
	●	●			●	●								●		
		●												●	●	

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
ERCOM (THALES)	●	●	●	●		●	●		●						
ESET FRANCE	●	●	●	●	●		●		●			●	●		
ETAS SAS		●	●		●		●					●	●		●
EURAFIBRE			●												
EUROEDI	●														
EVINA		●											●		
EXER	●	●	●	●	●				●		●	●	●	●	
F5 NETWORKS		●	●	●		●	●						●	●	
FACTORYTHINGS		●							●						
FEEDER									●						
FEITIAN TECHNOLOGIES	●	●		●		●	●	●	●						
FIREEYE		●	●		●				●					●	
FLASHPOINT	●		●			●	●		●			●			
FLEXERA		●							●			●	●		●
FORECOMM	●	●	●	●		●			●						
FORGEROCK						●									
FORTINET	●	●	●	●	●	●	●		●			●	●		
F-SECURE		●	●	●			●		●			●	●		
FULL IP SOLUTIONS	●	●	●			●				●	●	●	●	●	
G DATA SOFTWARE	●	●	●	✣											
GATEWATCHER	●	●	●		●	●		●	●				●		
GEMALTO	●	●		●		●	●	●							
GFI	●	●	●	●	●	●	●	●	●				●	●	
GITGUARDIAN		●											●		●
GLOBALSIGN	●		●	●		●	●								
GROUPE IMPRIMERIE NATIONALE	●			●		●			●						
GS2I	●	●	●		●		●		●						
GUARDICORE		●	●		●										
GUIDANCE SOFTWARE INC	●	●		●	●		●				●	●	●		
HACKUITY	●	●											●		
HAREL SYSTEMS	●	●					●								
HARFANGLAB									●						
H-IAPPS	●		●									●	●		
HID GLOBAL						●						●	●	●	
HP INC		●							●						
HYPERVISION TECHNOLOGY	●	●	●		●	●	●		●			●	●	●	
IBM FRANCE	●	●		●		●			●	●		●	●	●	●
IDACTIS						●			●						
IDECSI	●	●		●		●				●				●	
IDNOMIC	●			●	●	●	●		●						

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent	
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	HEXATRUST
	●	●	●	●	●	●										●
●	●	●	●	●		●		●	●					●		
	●	●	●		●		●	●						●		
					●											
		●												●	●	
●			●			●				●		●		●		
●	●	●	●	●	●	●										
●	●	●	●		●		●	●	●	●	●			●		
	●			●	●		●								●	
	●	●	●	●		●										
●			●	●	●			●	●		●	●	●			
●										●	●	●		●		
			●	●	●		●			●				●		
	●	●	●											●		
●	●	●														
●	●	●	●	●	●	●	●				●		●			
●		●	●	●	●		●	●	●	●	●	●	●	●	●	
	●	●		●	●	●								●	●	
●		●	●	●	●	●	●			●	●	●	●	●		
●										●				●		
	●	●		●	●	●								●	●	
●		●	●	●	●	●	●			●	●	●	●	●		
●		●	●	●						●	●	●		●		
●							●		●	●				●		
				●							●	●			●	●
													●	●		
●	●	●					●			●				●		
				●		●						●				
●	●	●	●	●	●			●	●		●		●	●	●	
●	●	●	●	●	●		●	●	●	●	●	●		●	●	
	●			●		●										
●	●	●	●					●	●	●		●	●	●		
	●	●		●	●	●	●							●	●	●

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
I-GUARD	●	●	●	●					●					●	
ILEX INTERNATIONAL		●		●		●			●						
IMPERVA	●	●								●		●	●	●	
IN GROUPE	●			●		●	●		●						
INFOBLOX	●		●	●	●		●		●		●				
INVENIS	●		●				●			●	●				
INWEBO TECHNOLOGIES		●	●	●		●	●	●	●						
ISIT	●	●	●	●	●		●		●	●		●	●	●	●
ITRUST	●	●	●								●	●	●	●	●
IVANTI	●	●		●		●	●		●			●	●		
IXIA	●	●	●				●			●	●				
JUNE-FACTORY	●				●		●					●	●		
JUNIPER NETWORKS			●							●			●	●	
KASPERSKY LAB FRANCE	●	●	●		●				●				●		
KAZEKO		●		●			●								
KEEEX	●	●		●		●	●	●	●	●				●	
KEMP FLOWMON		●	●		●				●						
KEYSIGHT	●	●	●	●	●		●		●	●		●	●	●	
KIUWAN		●											●		●
KIWI BACKUP	●	●		●					●						
KOBIL	●	●		●		●									
KONTROL SAS	●	●		●			●								
KUB CLEANER	●				●		●		●						
LINAGORA	●	●	●	●		●									
LMBA / GEDIX	●	●	●	●	●		●		●						
LOGMEIN	●	●		●		●			●						
LOGPOINT	●	●	●	●	●				●					●	
LOOKOUT				●					●			●	●		
LYBERO.NET	●														
MAILINBLACK															
MALWAREBYTES				●					●			●	●		
MAPREUVE	●														
MARKET ESPACE	●					●									
MCAFEE			●				●		●			●	●	●	
MICROSOFT	●	●	●	●		●	●	●	●	●			●	●	
MOBILE PROCESS				●											
MOBILEIRON				●											
MOSKITOS	●	●					●							●	
MYDPO	●														
MYQ FRANCE	●					●	●		●						
NAMESHIELD	●		●				●							●	

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent	
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	HEXATRUST
●		●	●	●	●											
	●														●	●
●	●	●	●		●		●		●	●	●	●		●		
	●	●												●		
●		●		●	●	●			●	●	●	●		●		
										●		●		●	●	
	●			●	●		●							●	●	●
	●	●	●	●	●		●	●								
●	●	●	●	●	●		●	●	●	●	●	●		●		●
		●	●	●	●	●	●			●	●			●		
					●		●		●				●			
													●	●		
●	●	●	●		●		●	●	●	●	●	●				
●		●	●	●	●	●				●	●	●		●		
	●									●				●		
	●	●		●				●						●	●	
●					●		●	●	●	●	●	●	●	●		
●	●	●		●	●	●	●	●	●		●	●	●	●		
							●			●			●	●		
		●	●	●		●									●	
	●	●	●													
		●	●				●							●	●	
		●	●	●	●											●
	●	●			●										●	
					●										●	
	●													●		
								●	●	●	●	●	●			
●		●	●			●								●		
		●												●		
																●
●				●		●		●	●	●	●	●		●		
		●														
		●											●	●		
●		●		●	●			●	●	●	●	●	●		●	
●	●	●	●	●	●	●	●	●		●	●	●		●	●	
						●	●			●						
						●										
	●	●	●			●				●	●		●	●		
															●	
	●	●														
	●	●			●			●								●

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
NANOCODE		●		●							●	●			
NCIPHER SECURITY	●						●								
NEOWAVE	●					●									
NETHEOS						●				●					
NETSCOUT								●				●	●		
NETSKOPE	●	●	●	●	●	●			●		●	●	●	●	●
NETWORK USERS INSTITUTE	●	●	●	●			●		●	●		●	●		
NETWRIX	●	●				●				●	●	●	●	●	
NEXT DECISION	●												●		
NEXTDAY.VISION		●			●	●			●						
NEXUS GROUP						●	●								
NIS	●	●	●	●		●	●		●						
NORMASYS	●	●	●						●	●			●		
NORMATION					●		●		●		●	●	●	●	●
NOZOMI NETWORKS					●		●				●	●	●		
NTX RESEARCH	●					●	●			●	●				
NUCLEON SECURITY	●			●		●			●						
NXO		●	●	●		●			●			●			
OKTA	●	●		●		●	●		●						
OLFEO	●		●	●					●	●				●	
ONE IDENTITY						●						●	●	●	
ONELOGIN	●	●				●			●						
ONETRUST	●					●									
OODRIVE	●	●		●		●			●						
OPENIP		●	●	●					●						
OPSWAT	●			●					●				●		
ORACLE	●	●	●	●		●	●	●		●			●	●	
ORSEC TECHNOLOGIES SAS			●							●					
OVELIANE	●	●	●	●								●	●		
OXIBOX	●	●	●	●	●	●	●	●	●			●	●		
PALO ALTO NETWORKS	●	●	●	●	●	●	●		●	●	●	●	●	●	
PARSEC															
PHISHME	●	●							●	●	●	●	●		
PHOENIX CONTACT FRANCE	●	●	●	●	●				●						
PING IDENTITY CORPORATION						●									
PRADEO		●		●			●						●		
PRIM'X	●		●	●					●						
PROGENIA	●	●									●	●	●		
PROMISEC		●							●				●		
PROVE & RUN				●	●		●								

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

	Protection							Exploitation							Saas	Adhérent	
	Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	HEXATRUST
		●	●									●			●		
			●												●		
		●	●		●	●	●										●
		●													●		
	●		●	●		●	●	●		●	●	●	●		●		
	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		
	●	●	●	●	●	●	●			●	●		●		●		
	●	●	●								●						
					●							●					
		●						●							●		
		●				●	●										
		●	●												●		
			●	●	●	●		●	●		●						
	●	●			●	●	●	●			●	●		●			●
	●								●	●	●		●	●	●		
		●	●														
		●		●	●	●	●			●							
	●											●					
		●			●	●											●
		●	●						●		●			●	●		
		●	●	●	●										●		
			●														●
		●	●												●	●	●
		●			●	●									●		
			●		●		●							●			
	●	●	●	●		●	●	●	●		●				●	●	
	●					●		●	●	●	●		●	●			
			●			●				●							
	●	●	●	●	●	●	●	●		●	●			●	●		
	●	●	●	●	●	●	●	●	●	●	●	●			●		
	●		●		●	●			●	●	●	●		●	●		
			●	●		●											
		●		●											●		
	●		●	●			●	●	●	●	●				●		●
			●		●	●	●									●	●
					●							●			●		
	●				●					●	●	●	●	●	●		●
			●	●		●											●

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
PYDIO	●			●					●						
QUALYS	●	●	●	●	●		●		●		●		●		
QUERY INFORMATIQUE	●								●						
QUEST SOFTWARE	●	●	●	●		●	●		●		●	●	●	●	
RADWARE	●	●	●				●								
ROHDE & SCHWARZ CYBERSECURITY	●	●	●	●					●				●		
RSA	●	●	●	●	●	●			●			●	●		
RUBYCAT	●	●	●		●	●									
SAILPOINT TECHNOLOGIES						●									
SCASSI SOLUTIONS	●	●	●		●		●				●	●	●		
SCHLEUPEN AG	●	●	●						●	●	●	●	●		
SCPTIME	●	●	●		●		●	●							
SEALD	●	●				●									
SEC'IT	●	●	●	●	●		●		●				●		
SECKIOT			●		●		●				●		●		
SECLAB	●		●		●	●			●						
SECLUDIT	●	●	●		●							●	●		
SECRET DOUBLE OCTOPUS				●		●									
SECURE2BROWSE		●							●						
SECURE-IC	●						●					●	●		
SEKOIA	●	●	●									●	●		●
SENTINELONE									●						
SENTRYO			●		●		●				●		●		
SERENICITY	●		●						●			●			
SESAME IT	●	●	●		●	●			●		●	●	●	●	
SHADLINE	●				●		●								
SIEMENS					●										
SILVER PEAK		●	●												
SKYBOX SECURITY	●	●	●	●	●		●	●	●		●	●	●		
SKYHIGH NETWORKS	●	●	●	●							●	●		●	
SOFT EXPANSION	●								●						
SONICWALL	●	●	●	●					●	●	●	●	●	●	
SOPHOS	●	●	●	●											
SPIRENT COMMUNICATIONS	●	●	●	●			●						●		
SPLUNK	●	●	●	●	●		●					●		●	
STIMSHOP			●	●	●		●		●						
STORMSHIELD	●		●	●	●								●	●	
STRATON IT	●	●	●		●				●	●	●	●	●		

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent	
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	HEXATRUST
		●													●	
		●	●	●	●	●	●			●			●	●		
●	●	●	●	●	●	●	●			●	●	●	●	●		
			●		●		●		●	●						
	●	●	●		●		●							●		●
●	●			●	●	●		●	●		●		●	●		
	●				●		●			●	●		●			
	●	●												●		
			●		●		●						●		●	
		●								●	●		●			
		●			●		●	●	●	●				●	●	
	●	●												●		
					●								●			
●					●	●				●	●	●	●			
●	●	●		●	●		●	●	●							●
							●			●			●			
	●		●			●	●	●						●		
		●		●										●		
●		●	●													
●								●	●	●	●	●		●		
				●							●	●				
●					●					●	●	●	●	●		
		●		●	●					●	●		●			
●		●	●	●	●		●	●	●	●			●			
		●									●			●		
					●									●		
					●		●						●			
●	●	●	●	●	●	●	●		●	●	●	●	●	●		
●	●	●	●							●				●		
		●		●												
●	●	●	●	●	●	●	●			●			●	●		
	●	●	●	●	●											
					●					●			●			
							●	●	●	●	●	●	●	●	●	
	●			●	●	●										
●	●	●		●	●		●							●	●	
										●			●	●		

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
SYMANTEC	●	●	●	●	●	●	●		●	●	●	●	●		
SYNOPSYS NORTHERN EUROPE LTD.		●										●			●
SYSPERTEC		●				●			●				●		
SYSTANCIA	●	●		●		●			●						
TANIUM		●	●		●				●		●	●	●		
TEAMVIEWER GMBH	●	●							●				●	●	
TEHTRIS	●	●	●	●	●	●	●		●			●	●	●	
TENABLE		●	●		●	●					●	●	●		
TEXPLAINED	●												●		
THALES	●	●	●	●	●	●	●	●		●	●	●	●	●	●
THEGREENBOW	●		●	●											
THREATQUOTIENT INC,	●	●	●												
TIXEO		●	●												
TRANSFERTPRO	●	●		●						●					
TRANSMIT SECURITY						●									
TREND MICRO			●	●	●		●		●			●	●		
TRUSTINSOFT	●	●	●		●	●	●	●				●	●		●
TRUSTWAVE	●	●	●	●		●	●		●			●	●	●	●
TUFIN		●	●			●						●	●	●	
UNISYS						●									
USERCUBE	●		●			●				●		●			
VADE	●						●			●		●			
VARONIS	●	●	●		●										
VECTRA NETWORKS	●	●							●			●			
VEEAM						●					●				
VENAFI	●		●	●	●	●	●	●		●	●	●	●	●	●
VERIZON	●	●	●	●	●							●			
VMWARE	●				●	●	●								
WALLIX	●	●								●	●	●	●	●	
WASACA		●	●	●		●			●						
WATCHGUARD TECHNOLOGIES	●					●		●							
WOLEET						●									
WOOBE	●	●							●						
WOOXO	●	●		●					●				●		
WRAPTOR	●	●										●	●		●
YAGAAN	●	●	●			●	●					●	●		
YESWEHACK	●					●									
ZERTIFICON SOLUTIONS GMBH	●	●									●		●		
ZIWIT	●	●	●	●											
ZSCALER			●												
ZYXEL FRANCE															

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent	
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	HEXATRUST
●	●	●	●	●	●	●			●	●	●	●	●			
		●	●				●						●			
	●				●			●							●	
	●	●	●	●	●	●								●	●	
				●			●		●	●	●	●	●			
			●	●	●						●		●	●		
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		
			●		●			●	●	●	●		●	●		
		●														
●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	
		●			●	●										●
●									●	●	●					
		●														●
	●	●												●		
	●													●		
●		●	●	●	●	●								●		
		●	●		●		●							●	●	●
●		●	●	●	●	●	●	●	●	●	●	●	●	●		
●					●		●	●			●		●	●		
	●	●	●	●	●	●								●		
	●													●		
●				●									●			●
		●					●			●	●	●	●			
		●	●	●	●				●	●			●			
		●		●	●											
●	●						●									
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		
		●	●	●	●	●	●	●		●	●				●	
	●	●									●		●	●	●	●
	●	●	●	●	●	●	●	●		●		●	●	●		
●	●		●	●	●					●		●		●		
	●	●														
		●		●												
		●	●	●		●									●	●
				●			●							●	●	
		●	●				●			●					●	
	●	●	●		●		●		●	●			●	●		●
	●	●														
		●	●							●			●	●	●	
●		●	●		●	●	●			●				●		
					●											

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
2SI CONSULTING	●	●	●	●		●	●		●				◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲
ABAKUS SÉCURITÉ	●		●	●								◆	◆▮▲	◆▮▲		◆▮▲✖		◆▮
ABINGTON ADVISORY	●	●	●	●					●	◆	◆	◆	◆	◆	◆	◆	◆	◆
ACCEIS	●	●	●	●			●		●	◆	◆	◆	◆		◆		◆	◆
ACCENTURE	●	●	●	●	●	●	●	●	●	◆▮	◆▮	◆▮▲	◆▮▲✖	◆▮▲	◆▮	◆▮▲✖	◆▮▲✖	◆▮▲
ACELYS SERVICES NUMÉRIQUES	●	●	●	●					●	◆	◆▮▲	◆▮▲	◆▮▲				◆▮	◆▮▲
ACESI GROUP	●	●	●	●		●			●	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮	◆▮	◆▮	◆▮▲	◆▮▲
ACTIVANOS SAS	●		●			●					◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲
ACTIV'INFO			●										◆					◆▮
ACTUELBURO	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
ADACIS	●	●	●						●			◆✖	◆					
ADENIUM	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆			◆	◆	◆
ADIKTS	●	●											◆					
ADVENS	●	●	●	●	●	●	●		●	◆▮	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮	◆▮▲
ADVENTIUM TECHNOLOGIES	●	●								◆	◆	◆		◆		◆	◆▮▲	▮▲
ADVISO																		
AGENCEE	●		●	●					●		◆	◆	◆				◆	◆
AKAMAI TECHNOLOGIES	●	●		●		●							◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲
AKERVA	●	●	●		●	●	●			◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆	◆▲
AKKA	●	●	●	●	●					◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		◆▮	◆▮
ALASTAR	●		●						●	◆▮	◆▮		◆▮					
ALEKSO	●	●	●	●		●			●				▲✖	▲✖		▲✖	▮▲✖	▮▲✖
ALENATEC	●		●	●	●	●		●	●		◆▮	◆	◆	◆▮		◆	◆▮	◆▮
ALGOSECURE	●	●	●							◆	◆	◆	◆	◆	◆	◆	◆	◆
ALLISTIC	●	●	●	●		●	●		●	◆	◆	◆	◆▲	◆▮▲	◆▮▲	◆▲	◆	◆
ALMOND	●	●	●	●		●	●		●	◆	◆	◆	◆▲	◆▲	◆	◆▲	◆	◆
ALTRAN TECHNOLOGIES	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
AMBICIO	●	●		●		●	●		●	◆	◆	◆		◆			◆	◆
AMBIONICS SECURITY	●	●	●															
AMOSSYS	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆	◆	◆	◆	◆
ANEXIS	●	●							●	◆	◆	◆						
APIXIT	●		●	●		●			●	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲
APSIDE	●	●	●								▮		▮					◆▮
ARMATURE TECHNOLOGIES	●	●	●			●		●	●									
ASSYSTEM					●					◆	◆	◆	◆				◆	◆
ATE	●	●	●							▲	▲	▲	▲	▲	▲	▲	▲	▲
ATN GROUPE	●			●		●					◆		◆▮▲	◆▮▲			◆▮▲	◆▮▲
AUTICONSULT	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			Labels		Adhésion		
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT (Computer Emergency Response Team)	Organisme de Formation **	Adhérent NUMEUM	Adhérent Hexatrust	Label ExpertCyber
◆▮	◆▮	◆▮			◆		◆			◆▮▲	◆	◆	◆	◆	◆	◆					
	◆▮	◆▮	◆▮▲		◆▮	◆▲	◆▮	◆▮	◆▮✖	◆	◆▮▲	◆		◆▮▲	◆				●		●
	◆	◆	◆		◆	◆	◆	◆			◆	◆	◆	◆	◆	◆					
◆	◆	◆	◆	◆	◆			◆			◆	◆	◆	◆	◆	◆		●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆	◆	◆	◆	◆		●			
◆▮▲	◆▮▲	◆▮▲			◆▮▲		◆▮▲	◆	◆	◆▮▲	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮					●
	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮	◆▮▲				◆▮	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲			●		
	◆▮▲	◆▮▲			◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲		◆▮▲	◆▮▲		●			
	◆▮	◆▮			◆			◆▮		◆▮	◆▮	◆	◆	◆▮	◆	◆		●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
		▮▲			◆						◆	◆	◆	◆	◆	◆					●
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆					
◆		◆▮		◆							◆	◆		◆	◆						
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮▲	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		●			
◆		◆▮			◆	◆	◆	◆	◆	◆		◆	◆		◆	◆		●	●		
	◆	◆			◆			◆	◆	◆	◆	◆	◆	◆	◆	◆					
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲											
◆▲	◆▲	◆		◆	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲		●	●		
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●		
	◆▮▲	◆▮▲	▮		◆▮						◆▮▲	◆▮	◆▮	◆▮▲	◆▮	◆▮					●
▮▲✖	▮▲✖	▮▲✖	▲✖	▮▲	◆▮▲✖	▲	▲✖	▲	◆	▲		◆	◆		◆	◆					
◆▮✖	◆▮	◆▮✖	◆	◆	◆	◆	◆▮✖	◆		◆▮	◆▮	◆		◆▮	◆						
◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆		●			
◆	◆	◆	◆	◆▮	◆	◆	◆				◆▲	◆	◆	◆▲	◆	◆			●		
◆	◆	◆	◆	◆	◆	◆▲	◆▲	◆▲	◆▲	◆✖	◆	◆	◆	◆	◆	◆	●	●			
◆	◆	◆▮	◆	◆	◆	◆	◆✖	◆	◆	◆	◆▲	◆	◆	◆▲	◆	◆			●		
	◆		◆	◆	◆			◆				◆	◆		◆	◆					
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆					
					◆								◆			◆					
◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲		◆▲	◆▲				●		
◆▮				◆▮	◆▮			◆▮											●		
																			●		
		◆			◆								◆			◆					
▲		▲		▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲					
◆▮▲	◆▮▲	◆▮▲			◆					◆▮▲	◆	◆		◆	◆						
◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			●		

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
AVITI	●		●			●			●	◆	◆▮▲			▮			◆▮▲	
AXEL IT			●	●		●	●		●		◆▮	◆▮	◆▮	◆▮		◆▮	◆▮	◆▮
AXIANS	●		●		●					◆	◆▮	◆	◆▮▲	◆▮▲		◆	◆▮▲	◆▮▲
AXICOM-SECURITE	●	●	●	●		●			●			◆▮					◆▮	◆▮
AZERI BEGI CYBERSÉCURITÉ	●	●			●	●			●			◆					◆	
BEA INFORMATIQUE	●	●	●	●					●	◆	◆▮▲	◆▮▲	◆▮▲					◆▮
BEARINGPOINT	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
BEIJAFLORE	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
BLUESCREEN			●						●								▲	▲
BOCK CONSEIL			●		●						◆	◆						
BRIGHTWAY	●	●	●	●					●									
BSI FRANCE	●	●	●	●	●	●	●											◆▮
BSSI CONSEIL ET AUDIT	●	●	●	●	●	●	●	●	●	◆		◆	◆▮✖	◆▮	◆▮	◆	◆▮	◆▮
BUG BOUNTY ZONE	●	●	●		●		●											
BY THE WAY	●	●	●	●		●			●			◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲
CALYPT CYBERSÉCURITÉ	●	●	●		●			●		◆		◆	◆✖		◆	◆	◆	◆
CAPGEMINI - SOGETI	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
CAPGEMINI TECHNOLOGY SERVICES	●	●	●	●	●	●	●		●	◆	◆▮	◆	◆▮	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮
CEGEDIM OUTSOURCING		●	●	●					●	◆▮▲	◆▮▲		◆▮▲				◆▮▲	◆▮▲
CEIS	●	●	●							◆	◆▮	◆▮	◆	◆▲		◆		
CGI FRANCE	●	●			●	●	●			◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲			◆▮
CLARANET	●	●					●		●			◆	▲	▲	▲	▲		▲
CNPP CYBERSECURITY	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆	◆	◆	◆	◆
CO-C	●	●	●	●	●	●	●	●	●				◆▮		◆▮			◆▮
COESSI	●	●	●	●	●		●			◆	◆	◆	◆		◆			◆
COGITAL	●	●		●	●				●	▮					◆▮	▮	▮	▮
CONIX	●	●	●	●	●		●		●	◆		◆	◆	◆	◆	◆		
CONSORT	●	●	●	●		●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
COREYE	●	●	●			●				◆▲		◆▮▲	◆▮▲	◆▮▲		◆▲	◆▲	◆▲
CORTEXERA	●	●	●	●	●	●	●	●	●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		◆▮	◆▮
CS -NOVIDY'S	●	●	●		●	●	●		●	◆▮▲	◆▮▲✖	◆▮	◆▮	◆▮✖	◆	◆▮✖	◆▮✖	◆▮▲✖
CYBER-EGIDE	●		●			●							◆					
CYBERENS	●				●		●			◆	◆	◆						◆✖
CYBERGLOBAL	●	●	●	●		●	●		●	◆▮	◆▮	◆▮	◆▮				◆▮	◆▮
CYBERSEC&YOU	●	●	●	●	●	●	●		●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
CYBERZEN	●									◆	◆	◆						◆
DATA PRIVACY PROFESSIONALS	●	●	●	●	●	●	●	●	●	◆	◆	◆					◆	◆

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			Labels		Adhésion		
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT (Computer Emergency Response Team)	Organisme de Formation **	Adhérent NUMEUM	Adhérent Hexatrust	Label ExpertCyber
	◆▮▲	◆▮▲			◆			▮▲				◆▮▲			◆▮▲						●
◆▮	◆▮	◆▮	◆▮		◆													●			
◆▮▲	◆▮▲	◆▮▲	◆	◆▮▲	◆	◆▮▲	◆▮	◆	◆	◆▮▲	◆	◆	◆	◆	◆	◆			●		●
◆▮	◆▮	◆▮	◆▮																		
	◆								◆		◆			◆							
◆▮	◆▮▲	◆▮▲			◆▮▲						◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
◆	◆	◆	◆	◆	◆▮	◆	◆▮	◆	◆			◆	◆▮		◆	◆▮					
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆					
	▲	▲	▲					▲													●
					◆							◆			◆						
					▮						◆			◆			●	●			
◆	◆▮	◆▮	◆▮	◆▮▲	◆	◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮	◆▮	◆▮▲	◆▮	◆▮	●	●			
◆		◆									◆			◆							
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲		◆▮▲	◆▮▲					●
◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆		●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●		
◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮	◆	◆▮▲	◆▮▲	◆	◆	◆	◆	◆	◆	◆	◆	◆			●		●
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		●	●		
					◆	◆▮▲	◆▲✖	◆▮			◆▲		◆	◆▲		◆		●		●	
◆	◆			◆	◆▮▲	◆▮▲	◆▮	◆▲	◆	◆▮▲	◆	◆	◆	◆	◆	◆			●		
▲	◆▲			▲	◆▲	▲	▲	▲	◆▲	◆▲	◆▲	◆	◆	◆▲	◆	◆			●		
◆	◆	◆	◆	◆	◆		◆	◆	◆		◆	◆	◆	◆	◆	◆					
◆▮		◆▮							◆▮		◆▮			◆▮				●			
◆	◆	◆	◆	◆	◆		◆		◆		◆	◆	◆	◆	◆	◆			●		
▮	◆▮	◆▮	◆▮		◆▮	▮		▮	▮		◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●		
				◆	◆	▮▲	◆	◆	◆		◆	◆	◆	◆	◆	◆	●				
◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲				●		
◆▮▲		◆▮▲		◆	◆▲	◆▮▲		◆▲	◆▲			◆	◆		◆	◆			●		
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮					●
◆▮▲✖	◆▮▲	◆▮▲✖	◆▮▲	◆	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲	◆▲	◆	◆	◆	◆	◆	◆			●		
			✖		◆							◆	◆		◆	◆					
					◆							◆	◆		◆	◆					
◆▮	◆▮	◆▮	◆▮					◆▮		◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮					
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮				●	
		◆					◆						◆			◆		●			
◆	◆	◆			◆			◆				◆	◆		◆	◆		●	●		

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
DAVID INFORMATIQUE	●		●	●					●		◆▮▲		◆▮▲	◆▮▲		◆▮▲	◆▮▲	
DBM PARTNERS		●	●	●		●	●		●	◆	◆	◆	◆				◆	◆
DELOITTE	●		●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆		◆
DEVELOPPEMENT CONSEIL COMMUNICATION	●		●	●	●	●	●		●	◆	◆▮▲	◆▮	◆▮▲✖	◆▮▲		◆▮▲✖	◆▮	◆▮
DEVOTEAM	●	●	●	●	●	●	●	●	●	◆	◆▮	◆	◆		◆▮	◆▮	◆▮	◆
DIGITAL SECURITY	●	●	●		●	●	●	●	●	◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
DIGITEMIS (CYBERSECURITY & PRIVACY)	●	●	●	●	●		●		●	◆	◆	◆✖	◆		◆		◆	◆
DIGORA	●	●									◆▮▲	◆▮▲						
DILITRUST	●	●		●						✖								✖
DPO CONSULTING	●									◆✖	◆✖	◆✖	◆✖					
EBRC	●	●	●	●		●			●	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲
E-CATALYST	●		●	●		●	●		●	◆▮▲	◆▮▲	◆	◆▮▲			◆▮▲		
ECO HARDWARE SAS	●	●	●	●	●	●	●	●	●									
EIFFAGE ENERGIE SYSTÈMES - CLEMESSY	●	●	●	●	●	●	●		●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		◆▮	◆▮
EIGHT TECH	●	●	●						●	◆▮▲	◆	◆	◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲
EITA CONSULTING	●	●	●				●			◆				◆	◆▮			◆
EXAPROBE - GROUPE ECONOCOM	●	●	●	●		●	●		●		▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
EXCELLIUM SERVICES	●	●	●	●		●		●				◆▮	◆▮	◆▮	◆▮	◆▮		◆▮
EXPONENS	●					●				◆		◆			◆		◆	
EXTERN IT	●	●	●	●					●		◆▮▲	◆	◆	◆▮▲			◆▮▲	◆▮▲
EXTREMIT	●	●	●						●	◆▮▲	◆▮▲	◆▮▲	◆▮▲					▮▲
FIDENS	●	●	●	●	●	●	●		●	◆	◆	◆						◆
FORMIND	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆			◆	◆
G-ECHO	●	●	●	●		●	●		●	◆▮	◆	◆▮	◆▮			◆	◆▮	◆▮
GFI INFORMATIQUE	●		●		●					◆	◆	◆	◆	◆▮▲✖	◆	◆▮▲✖	◆	◆
GPLEXPERT	●	●	●						●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲
GRAND E NOV	●	●	●	●	●	●	●	●										◆
GROUPE SII	●	●	●	●			●				◆		◆	◆	◆		◆▮	◆▮
HACKNOWLEDGE SA	●	●			●	●	●		●									
HARMONIE TECHNOLOGIE	●	●	●	●		●	●			◆▮	◆▮	◆▲	◆				◆▮	◆▮
HELIX SECURITY SAS	●		●									◆▮	◆▮	◆▮▲		◆▮	◆	◆▮
HEXANET	●	●	●	●		●			●	◆	◆	◆	◆	◆▮		◆	◆▮▲	◆▮▲
HIRMES	●		●				●		●		◆▮	◆▮	◆▮▲					
HOLISEUM	●	●	●	●	●	●	●	●	●	◆	◆▮▲	◆	◆▮▲	◆▮▲		◆	◆▮	◆▮
HUB ONE	●	●	●	●	●	●			●	◆▲		◆	◆▮▲	◆▮▲	◆	◆▮	◆▮	◆▮
I.S. MANAGEMENT	●	●	●	●	●				●									◆▮▲✖
IBC DIALOG	●	●	●	●					●		◆▲	◆▮▲	◆▮▲	◆▲			◆▮▲	◆▮▲
IDAXIO	●																	◆▮

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			Labels		Adhésion		
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT (Computer Emergency Response Team)	Organisme de Formation **	Adhérent NUMEUM	Adhérent Hexatrust	Label ExpertCyber
	◆▮▲	◆▮▲					◆▮▲	◆▮▲		◆▮▲									●		
	◆	◆	◆	◆	◆		◆				◆	◆	◆	◆	◆	◆					
◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆		●			
◆▮▲✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲✖	◆▮▲	◆▮	◆▮▲	◆▮	◆		◆▮	◆				●		●
◆	◆	◆		◆▮	◆		◆▮	◆	◆	◆	◆	◆	◆	◆	◆	◆	●		●		
◆▮	◆	◆▲	◆	◆▮	◆▮	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●	●	●		
◆	◆	◆	◆		◆		◆✖	◆			◆	◆	◆	◆	◆	◆			●	●	
																			●		
																			●		
					◆								◆✖			◆✖			●		
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●			●	
	◆▮▲✖		◆▮▲		◆▮▲						◆▮▲			◆▮▲					●		
◆▮	◆▮	◆▮	◆▮		◆▮	◆	◆▮				◆	◆		◆	◆						
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
◆▮✖		◆▮		◆▮	◆		◆▮		◆▮										●		
◆▮▲	◆▮▲✖	◆▮▲	◆▮▲	▮▲	◆▮	◆▮▲	▮▲	◆▮▲	▮▲	◆▮▲	▮▲	▮▲	▮▲	▮▲	▮▲	▮▲			●		
◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮	◆▮▲✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲✖	◆▮	◆▮		◆▮	◆▮		●	●			
					◆	◆	◆		◆			◆	◆		◆	◆					
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆	◆▮▲	◆			◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲			●		●
▮▲	▮▲	▮▲	▮▲					▮▲				▮▲	▮▲		▮▲	▮▲					●
◆	◆		◆		◆							◆	◆		◆	◆		●			
◆	◆	◆	◆	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆		●		●	
		◆▮		◆▮	◆▮		◆▮				◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		●	●		
◆	◆	◆	◆	◆	◆✖	◆▮▲✖	◆▮▲	◆▲		◆▮▲	◆	◆	◆	◆	◆	◆			●		
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
◆	◆	◆		◆▮	◆				◆		◆	◆	◆	◆	◆	◆		●	●		
◆▮				◆▮	◆▮		◆▮	◆▮	◆▮		◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●		
◆▮	◆▮	◆▮		◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮					
◆▮▲	◆▮▲	◆▮▲	◆▮▲			▲	▲	▲				◆	◆		◆	◆					●
	◆	◆▮	◆		◆▮			◆		◆	◆▮	◆▮		◆▮	◆▮						
◆▮▲	◆▮▲	◆▮▲		◆	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆		●		●	
◆▮	◆▮	◆▮	◆▮	◆	◆▮	◆▮▲	◆▮▲	◆	◆▮	◆▮▲	◆	◆	◆	◆	◆	◆			●		
	◆▮▲✖				◆▮▲																
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮		◆▮▲	◆▮		◆▮▲	◆▮					●

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
IDENTO	●	●		●		●	●										◆▮▲	
ID-LOGISM	●	●	●	●		●	●		●	◆▮		◆▮				◆	◆▮	◆▮
IDNA	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
IMS NETWORKS	●	●	●	●	●	●			●	◆	◆	◆	◆▮▲	◆▮▲	◆	✖	◆▮▲	◆▮▲
INDATABLE	●	●	●	●					●	◆	◆	◆	◆		◆			
INET SYSTEM	●		●						●		◆▮▲		◆▮▲				◆▮▲	
INFORSUD TECHNOLOGIES		●	●	●					●	◆▮		◆▮	◆▮▲				▮▲	▮
INFOSYS	●	●	●	●	●	●	●	●	●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
INOPS	●	●	●	●	●		●	●		◆▮		◆▮	◆▮				▮	◆
INQUEST	●	●	●		●	●	●		●	◆	◆	◆	◆			◆	◆	◆
INTEGRALE IP			●								◆▮							
INTERDATA		●	●	●		●	●		●				▮▲	▮▲		▮▲	▮▲	
INTRINSEC	●	●	●		●		●		●	◆	◆▲	◆	◆▮▲	◆▮▲	◆▲	◆▲		◆▲
IRON MOUNTAIN	●						●		●									
ISATECH	●	●	●	●						◆▮	◆▮	◆▮						◆▮▲
ISE SYSTEMS	●	●	●		●					◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
IT&M REGIONS	●	●	●	●					●		◆▲						◆▮▲	◆▮▲
IT3 INFORMATIQUE	●	●	●	●		●			●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
I-TRACING	●	●	●	●	●	●			●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
ITS GROUP	●	●	●	●		●	●		●	◆▮		◆▲	◆▲	▮		◆	◆▮	◆▮▲
IVISION	●	●	●						●	◆	◆	◆	◆		◆		◆▮▲	◆▮▲
JANUA		●	●	●		●	●											
JLLNET	●		●						●	◆▮	◆▮▲			◆▮			◆▮▲	◆▮▲
K SECURITY	●		●									◆						◆
KATANA DIGITAL SA	●			●			●		●									◆▲
KPMG	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
KUDELSKI SECURITY	●	●	●	●	●		●	●	●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮▲		
KYRON SI	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲
LECPAC CONSULTING	●	●	●			●			●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲
LEXFO	●	●	●	●	●	●	●	●	●		◆		◆	◆▲	◆	◆		
LISIS CONSEIL	●	●	●	●	●		●		●	◆▮	◆▮	◆▮	◆▮			◆▮	◆	◆
LOGIFORM CONSEIL	●	●	●	●					●		▲						◆▮	◆▮
LOGIN SECURITE	●	●	●	●	●	●	●	●	●	◆	◆	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲
MANIKA	●	●	●	●	●		●		●	◆	◆	◆	◆		◆			◆
MASTER SECURITY CONSEIL	●	●	●			●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
MATILAN	●	●	●	●					●			◆				◆▮▲	◆▮▲	◆▮▲
MEDIANE SYSTEME					●		●								◆			
METANEXT	●		●			●						◆▮	◆▮				◆▮	

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

	Protection							Exploitation							Contrôles			Labels		Adhésion		
	Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT (Computer Emergency Response Team)	Organisme de Formation **	Adhérent NUMEUM	Adhérent Hexatrust	Label ExpertCyber
																					●	
	◆	◆	◆	◆	◆▮	◆▮	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆			●		
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲	◆▮▲✖	◆▮▲	◆	◆▮▲	◆	◆	◆	◆	◆	◆			●		
						◆						◆	◆	◆	◆	◆	◆			●		
		◆▮▲		◆▮▲																●		
	◆▮	◆▮	◆▮▲	▮		◆▮▲					▲	◆▮	◆▮		◆▮	◆▮				●		
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●		
	◆				◆▮	◆▮	◆			◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●		
	◆	◆	◆	◆		◆			◆	◆			◆	◆		◆	◆					●
			◆▮▲										◆▮			◆▮						
	▮▲	▮▲	▮▲				▲	▲	▲	▲	▲	▲			▲							●
	◆▲	◆▲	◆▲	◆▲	◆▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▲	◆	◆	◆▲	◆	◆			●		●
	◆▮▲		◆▮▲	◆▮▲		◆▮			◆▮		◆▮▲		◆▮	◆▮		◆▮	◆▮		●	●		
	◆▮	◆▮	◆▮		◆▮	◆▮	◆▮	◆	▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮				●	
	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲		◆▮▲	◆▮▲				◆	◆		◆	◆			●		
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▲			◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●	●			
	▮▲	▮	◆▮▲	◆▮	◆▲	◆	▲			◆	◆▮▲	◆	◆		◆	◆						
	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲						◆▲	◆▲	◆▲	◆▲	◆▲	◆▲					
																				●		
	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆			◆▮▲	◆▮	◆▮▲		◆▮	◆▮		◆▮	◆▮					●
			◆▲										◆			◆						
						◆																
	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆					
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮		◆▮	◆▮						
	◆▮▲	◆▮▲	◆▮▲	◆		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆	◆		◆	◆					
							◆▲	◆	◆	◆	◆	◆	◆		◆	◆						
	◆	◆	◆	◆	◆	◆▮	◆	◆▮	◆▮		◆▮	◆		◆▮	◆		◆▮					
		◆▮	◆▮						◆▮▲				◆▮▲			◆▮▲			●	●		
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●	●	
	◆	◆	◆	◆		◆			◆	◆		◆	◆	◆	◆	◆	◆			●		
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		●			
	◆					◆														●		
			◆▮		◆▮	◆	◆▮						◆▮	◆		◆▮	◆			●		

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
METSYS	●	●		●		●	●		●	◆▮▲	◆▮	◆	◆	◆▮▲		◆▮	◆▮	◆▮
MHCONSEIL	●	●	●						●		◆▮▲	◆	◆					◆▮▲
MICROPOLE	●	●	●			●	●			◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
MIXCOM	●	●	●						●			◆						
MODIS		●	●	●	●		●		●			◆	◆	◆▮	◆▮			◆
MPTCONSEIL	●		●	●	●	●			●	◆	◆	◆▮					◆	◆
NAXIOS	●	●	●						●				◆▮▲					◆▮▲
NBS SYSTEM	●	●	●			●						◆	◆	▮▲	◆			▮▲
NDA-SECURITY	●	●	●	●	●	●	●	●	●	◆✖	◆	◆	◆✖	◆✖	◆✖	◆▮✖	◆	◆▮▲✖
NET FREED	●	●	●	●		●		●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
NETFORMATIC			●						●	◆	◆	◆					◆▮▲	◆▮▲
NEWLODE	●	●	●		●	●			●		◆▮		◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲
NOMIOS	●	●	●								◆▮▲		◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲
NOVENCI			●	●		●			●		◆▲	◆▮▲	◆▮▲	◆▲		◆▲	◆▮▲	◆▮▲
NOVIDY'S	●	●	●		●	●			●	◆	◆	◆	◆	◆▮▲✖	◆	◆		◆
NTT FRANCE	●	●	●	●	●	●	●	●	●	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮	◆▮	◆▮	◆▮
NXO FRANCE	●		●			●			●		◆▮	▮		▮			◆▮	◆▮
OFISS							●				◆	◆	◆				◆	◆
OÏKIALOG		●	●	●	●				●				◆▮▲	◆▮▲			◆▮▲	◆▮▲
ON-X GROUPE	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆▮▲	◆	◆
OPEN GROUPE		●																
OPENMINDED PART OF ACCENTURE	●	●	●		●	●				◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
OPENSPHERE	●	●	●		●		●			◆▮	◆	◆	◆	◆▮		◆	◆▮	◆▮
OPTRIUM	●					●				◆▮▲	◆▮▲		◆▮▲	◆▮▲			◆▮▲	◆▮▲
OPTYMA SARL	●	●		●		●			●	◆▮	◆	◆▮	◆					◆▮
ORANGE CYBERDEFENSE	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
OSINX - GROUPE ACTIMAC	●	●	●	●		●			●		◆▮▲	◆▮▲	◆▮▲				◆▮▲	◆▮▲
PCL ASSISTANCE INFORMATIQUE	●		●						●		◆▮▲	◆▲	◆▮▲					◆▮▲
PHOEBE					●							◆	◆					◆
PICTIME GROUPE	●	●	●			●				◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
PPP-CONSEIL			●		●		●				◆▮▲					◆▮		
PRIAMOS	●	●	●	●	●	●	●	●	●	◆	◆	◆					◆	◆
PRIVACY IMPACT	●	●	●	●		●	●	●	●	◆	◆	◆					◆	◆
PROBE I.T	●		●				●			◆▮	◆▮	◆▮▲	◆▮▲				◆	◆
PRODWARE	●	●	●	●		●	●		●									
QUIETIC			●	●					●		◆▲		◆▮			◆	◆	◆
QUODAGIS			●			●	●		●		◆▮▲		◆▮▲				▮▲	
QUODAGIS INTEGRATION		●	●	●		●			●									

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			Labels		Adhésion		
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT (Computer Emergency Response Team)	Organisme de Formation **	Adhérent NUMEUM	Adhérent Hexatrust	Label ExpertCyber
	◆▮▲	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮▲	▲	◆	◆▮▲	◆	◆	◆	◆	◆	◆			●	●	
	◆▮▲	◆▮▲			◆▮▲			◆▮▲			◆	◆▲	◆	◆	◆▲	◆					●
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					
◆																			●		
◆				◆	◆					◆▮▲		◆			◆			●	●		
◆	◆	◆	◆	◆	◆	◆▮	◆▮	◆▮		◆		◆	◆		◆	◆					
◆▮▲	◆▮▲	◆▮▲						◆▮▲	◆▮▲			◆			◆						
▮▲		▮▲		◆▮	▮▲	◆▲	▲	◆	◆	◆▲	◆	◆		◆	◆			●			
◆	◆▮▲✖	◆✖	◆▮▲✖	◆	◆▮	◆	◆✖	◆	◆	◆✖	◆✖	◆	◆	◆✖	◆	◆			●		
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			●		
	◆▮▲	◆▮▲	◆▮▲		◆▮▲			◆▮▲					◆			◆					●
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲		◆▮▲	◆▮▲			●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲			◆▮▲		◆▮▲			◆▮▲			●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▲	◆▲	◆▲	◆▲		◆▮▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲					●
◆	◆▮	◆▮			◆✖	◆▮▲	◆▲	◆▲	◆	◆	◆	◆	◆	◆	◆	◆		●			
◆▮	◆▮	◆▮	◆▮	◆	◆▮	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲					
◆▮	◆▮	◆▮	◆▮							▮	◆▮	◆▮		◆▮	◆▮				●		
◆	◆	◆									◆		◆	◆		◆	●	●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮	◆▮			◆	◆▮			◆▮							
◆	◆▮▲	◆▮▲	◆	◆	◆	◆▮▲	◆	◆▮▲	◆	◆▮▲	◆	◆	◆	◆	◆	◆			●	●	●
				◆▮▲✖															●		
◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●	●	
◆▮		◆▮▲	◆▮	◆	◆	◆▮▲	◆▲	◆▲	◆▲	◆▲	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●		
◆▮▲	◆▮▲		◆▮▲																		
	◆				◆▮	◆▮	◆▮	◆					◆			◆					
◆▮▲	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●	●	●		
	◆▮▲	◆▮▲	◆▮▲		◆▮▲			◆▮▲	◆▮		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
◆▮▲	◆▮▲	◆▮▲	◆▮									◆▮▲	◆▮▲		◆▮▲	◆▮▲					●
												◆	◆		◆	◆		●	●		
◆▮▲		◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●		
					◆▮							◆▮▲	◆▮▲		◆▮▲	◆▮▲			●		
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆					
◆	◆	◆	◆	◆	◆			◆	◆	◆	◆	◆	◆	◆	◆	◆					
◆	◆	◆			◆						◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					
					◆▮▲																
	◆▮▲	◆▮▲	◆		◆	◆	◆	◆		◆		◆▮▲	◆		◆▮▲	◆			●		●
	▮▲	▮▲			◆▮▲			▮▲		▮▲								●	●		
																			●		

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
QUONEX	●	●	●	●			●											
RAMPAR	●	●	●	●		●	●		●		◆		◆▮	◆▮▲	◆▮	◆▮▲	◆▮	◆▮
REALSOFT INFORMATIQUE	●	●	●															
RECOVEO										◆✖								
SAVANE CONSULTING	●	●	●			●						◆▮		◆▮		◆▮	◆▮	◆▮
SCASSI	●	●	●	●	●	●	●		●	◆	◆	◆▮	◆	◆▮▲	◆▲	◆	◆	◆▲
SCC FRANCE	●	●	●	●		●	●	●	●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
SCHNEIDER ELECTRIC			●		●		●											
SCIURUS CONSEIL	●	●	●	●					●		◆	◆	◆			◆	◆	◆
SEC-IT SOLUTIONS	●	●	●	●	●	●	●		●	◆	◆	◆	◆▮	◆▮			◆	◆▮
SECTOR					●							◆	◆		◆			
SECUREWARE	●	●	●	●					●				◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲
SECUREWORKS	●	●	●	●			●			◆	◆	◆	▲	▲		▲		◆▲
SECURIVIEW SAS			●						●	◆▮	◆▮	◆▮	◆▮▲✖	◆▮▲	◆			◆▮▲
SEKOIA										◆		◆	◆✖			◆▮▲✖	◆	◆
SERMA SAFETY & SECURITY	●	●	●	●	●	●	●		●			◆	◆▮▲		◆▮▲		◆▮▲	◆▮▲
SERVAL-CONCEPT	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆	◆			◆
SFR BUSINESS	●	●	●	●	●	●	●		●	◆▮▲	◆	◆	◆▮▲	◆▮▲	◆		▮▲	◆▮▲
SII					●													
SILICOM	●	●	●							◆	◆	◆	◆	◆	◆	◆	◆	◆
SMARTPOINT	●	●	●	●	●	●	●	●	●			◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲
SNS SECURITY		●	●						●			◆	◆▮▲	◆▮▲	◆	◆▮▲		
SOCOA										◆		◆					◆	
SODIFRANCE	●	●	●	●					●	◆	◆	◆	◆▮▲	◆▮▲	◆	◆▮▲	◆▮	◆▮
SO-IT			●						●	◆▮	◆▮	▮				◆▲		
SOLUCEO DGPF	●		●	●		●			●		◆▮▲	◆▮				◆▮▲	◆▮▲	◆▮▲
SOPRA STERIA	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	▮▲	◆▮▲
SOSATOUTPC	●	●	●				●		●	◆			◆					◆
SPIE ICS	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆▮▲		◆	◆▮▲	◆▮▲
SQUAD	●	●	●	●		●	●	●	●	◆▮	◆▮	◆	◆▮	◆▮▲	◆▮		◆▮▲	◆▮▲
STEEL PC	●	●	●	●					●	◆	◆	◆		◆▮▲			◆▮	
STRATEGY & GOVERNANCE	●	●	●	●							◆	◆	◆					◆
SYC CONSULTANTS	●	●						●										
SYNACKTIV	●	●	●	●	●		●		●				◆✖		◆			
SYNCHRONE	●	●	●	●	●	●	●	●	●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
SYNETIS	●	●	●	●		●			●	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
SYNEXIE	●	●	●		●	●	●		●								◆▮▲	◆▮▲

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

	Protection							Exploitation							Contrôles			Labels		Adhésion		
	Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT (Computer Emergency Response Team)	Organisme de Formation **	Adhérent NUMEUM	Adhérent Hexatrust	Label ExpertCyber
			▮																			
	◆▮▲	◆▮	◆▮▲	◆▮	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲		◆▮▲								●			
	◆▮▲✖	◆▮▲✖	◆▮▲✖																●			
	◆▮	◆▮	◆▮	◆▮			◆▮		◆▮	◆▮			◆▮	◆▮		◆▮	◆▮			●		
	◆▮	◆	◆	◆▮	◆	◆▮	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲✖	◆▲	◆▲	◆▮▲✖	◆▲	◆▲			●		
	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●		
																					●	
	◆	◆	◆	◆		◆			◆	◆		◆	◆	◆	◆	◆	◆		●			
	◆▮	◆▮	◆▮	◆▮		◆		◆▮▲	◆	◆	◆▮▲	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮					
						◆																
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●
	▲	◆▲	◆▲		▲	◆	◆▲	◆	◆▲	◆▲	▲	◆	◆	◆	◆	◆	◆		●			
	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆	◆	◆	◆	◆					
	◆	◆	◆	◆	◆	◆	◆▲✖	◆	◆	◆✖	◆	◆	◆	◆	◆	◆	◆	●	●			
	◆▮▲	◆▮▲	◆▮▲			◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					
	◆	◆		◆					◆	◆		◆▲	◆▲	◆	◆▲	◆▲	◆		●			
	▮▲	▮▲	▮▲	▮▲		◆▮	◆▲	◆	◆	◆	◆	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●		
																				●		
	◆	◆	◆		◆	◆	◆		◆	◆		◆	◆	◆	◆	◆	◆			●		
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●	●	●		
	◆▮▲	◆▮▲	◆▮▲		◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆	◆▮▲	◆▮	◆					
					◆	◆						◆	◆	◆	◆	◆	◆					
	◆▮	◆▮	◆▮	◆▮	◆▮	◆	◆▮▲	◆▲	◆	◆		◆	◆	◆	◆	◆	◆		●	●		
		◆	◆					◆						◆			◆		●			
		◆▮▲	◆▮▲	◆▮▲		◆	◆▮▲	◆▮▲	◆▮	◆▮		◆	◆	◆	◆	◆	◆		●	●		
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮	◆	◆	◆▮	◆	◆		●			
	◆▮	◆▮	◆▮		◆▮	◆			◆▮	◆▮	◆▲		◆▮	◆▮		◆▮	◆▮					●
								◆		◆	◆	◆	◆	◆	◆	◆	◆					
												◆✖	◆		◆✖	◆			●			
	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●		
	◆▮	◆▮▲	◆▮▲	◆▮▲		◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●	●	●
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲		◆▮▲	◆▮	◆▮		◆▮	◆▮						●

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
SYSDREAM	●	●	●	●	●	●	●		●	◆		◆	◆		◆	◆	◆	◆
SYSTEMIS		●	●	●		●	●		●	◆	◆	◆	◆	◆	◆	◆	◆	◆
TALC SI	●	●	●			●				◆▮▲		◆▮▲	◆▮▲	◆▮▲✖			◆▮▲	◆▮▲✖
TECODATA	●		●	●		●		●	●						◆		◆▲	◆▲
TEOS CYBERSECURITY	●	●	●		●		●		●			◆	◆		◆		◆	◆
TGS FRANCE INFORMATIQUE	●	●	●			●			●	◆▮	◆▮	◆	◆				◆▮▲	◆▮▲
TIBCO	●		●	●			●		●		◆▲	◆▲	◆▲	◆▲			◆▲	◆
TNP CONSULTANTS	●						●	●		◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		◆▮
TRAX	●	●	●	●	●	●	●	●	●									
TRÈFLE SOLUTION			●			●					◆	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
TRSB		●	●	●					●	◆▲	◆▲	◆▲	◆▲				◆▲	◆▲
T-SYSTEMS	●	●	●		●	●	●	●				◆▲	◆▲	◆▲		◆▲		◆▲
UBCOM SA	●		●		●		●			◆	◆	◆	◆		◆	◆		
UBG. CYBER	●	●	●	●	●	●	●		●			◆	◆			◆	◆	◆
UNUMKEY	●	●	●	●	●		●		●	◆	◆	◆	◆					◆
UPPER-LINK	●	●	●	●		●			●		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲
URAEUS CONSULT	●									◆	◆	◆	◆				◆	◆
UTIKXO	●			●		●			●	◆	◆	◆						
VAADATA	●	●		●			●											
VEYAN	●	●	●	●	●	●	●		●	◆	◆	◆	◆▮	◆		◆	◆	◆
VFLIT OMR INFOGÉRANCE	●		●			●			●	◆▲	◆▲	◆▲	◆▲	◆▮▲			◆▮▲	◆▮▲
VNEXT	●	●	●	●	●	●	●	●	●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
WALLACK	●	●	●	●	●	●			●		◆▮	◆▮		◆▮			◆	◆
WANCORE			●			●				◆		◆	◆▮▲	◆▮▲	◆	◆▮▲	◆	
WANNATH	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
WAPLI INFORMATIQUE	●	●	●	●					●		◆▮		◆▮▲	◆▮				
WAPSI	●	●		●		●			●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		◆▮	◆▮
WAVESTONE	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆▮	◆
WEODEO	●	●	●	●			●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲				◆▮▲
WISE PARTNERS	●	●	●			●	●	●		◆	◆	◆	◆	◆	◆		◆	◆
XMCO	●	●	●						●		◆		◆		◆			
XPERIZ													◆					
YEC'HED MAT CONSEIL	●																	
YOGOSHA SAS	●	●	●	●	●	●	●	●					◆		◆			
YOURAX	●		●	●					●	◆▮		◆▮	◆▮▲	◆▮			◆▮	◆▮▲
ZENIKA	●	●				●	●	●					◆	◆	◆		◆	◆
ZERO TRUST SAS	●	●	●	●			●		●	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲✖		◆▮▲		◆▮▲

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			Labels		Adhésion		
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT (Computer Emergency Response Team)	Organisme de Formation **	Adhérent NUMEUM	Adhérent Hexatrust	Label ExpertCyber
◆	◆	◆	◆	◆	◆	◆		◆	◆		◆	◆	◆	◆	◆	◆			●		
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			●		
	◆▮	◆▮▲	◆▮		✖	◆▮▲✖	◆▮▲			◆▮▲		◆▮			◆▮						●
◆▲	◆▲	◆▲		◆					◆		◆	◆		◆	◆						
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆					
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲			◆			◆	◆	◆	◆	◆	◆					●
	◆▮▲	◆▮▲	◆▮▲		◆▲	▲	▲	▲	▲	▲		◆▲	◆		◆▲	◆			●		
				◆▮	◆▮	◆▮		◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●		
																			●		
◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮	◆		◆▮	◆					
◆▲	◆▲	◆▲	◆▲	◆▲		◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲			●		
◆▲	◆▲	◆▲	◆▲			◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲		◆▲	◆▲				●		
				◆	◆	◆	◆▮	◆	◆	◆									●		
◆	◆	◆		◆	◆			◆	◆		◆		◆	◆		◆		●			
◆	◆			◆			◆✖				◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●	●			
◆	◆	◆	◆		◆					◆▲	◆		◆	◆		◆			●		
					◆																
											◆			◆							
◆	◆	◆	◆		◆		◆	◆		◆	◆	◆	◆▮	◆	◆	◆▮			●		
◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					
◆▮	◆▮	◆▮	◆▮	◆▮	◆	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		●	●		
◆▮	◆	◆▮	◆	◆	◆▮					◆▮		◆▮	◆▮✖		◆▮	◆▮✖					●
		◆▮▲				◆▮▲	◆▮▲	◆▮▲	◆▮		◆	◆▮▲		◆	◆▮▲						
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆		◆	◆		◆	◆					
	◆▮▲	◆▮▲									◆	◆		◆	◆						●
◆▮	◆▮		◆▮	◆▮	◆▮		◆▮						◆▮			◆▮					
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			●		
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					
◆	◆	◆		◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆					
								◆	◆	◆	◆	◆	◆	◆	◆	◆	●	●			
				◆	◆														●		
					◆													●			
				◆			✖			◆	◆✖			◆✖				●	●		
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮			◆▮▲		◆▮▲	◆▮	◆▮▲		◆▮	◆▮▲						●
◆				◆							◆	◆		◆	◆			●	●		
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆▮	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖		◆	◆		◆	◆					

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Comprendre

La technologie et les méthodes

Par Jérôme Saiz et Alain Clapaud

- Définitions : Buzzword
- IAM : La gestion des identités et des accès au cœur de l'approche « Zero Trust »
- Threat Intelligence
- DevSecOps, la transformation digitale des DSI
- La réponse à incident
- Protection du poste de travail
- Protection des terminaux mobiles
- Protection de la donnée
- Protection applicative
- Audit d'architecture
- SOC
- Tableaux de bord de sécurité
- SIEM

Buzzword

Ransomware

Un « ransomware » ou rançongiciel est un malware dont le mode de fonctionnement passe par le chiffrement des données de l'utilisateur afin de lui extorquer une somme d'argent contre la clé de déchiffrement. L'attaquant réclame la rançon sous forme de cryptomonnaies afin de ne pas être identifié par les autorités. La rançon varie de quelques centaines voire quelques milliers de dollars à plusieurs millions de dollars, en fonction de la taille de la cible. Une entreprise peut voir une large partie de son parc de postes utilisateurs infectés, voire des serveurs critiques, certains ransomware peuvent réaliser ce que l'on appelle des déplacements latéraux d'un poste à un autre. Certains cherchent notamment à rendre inutilisables les serveurs de backup afin de ne laisser aucune autre alternative à la victime que de payer pour récupérer ses données. Cependant, verser la rançon ne constitue en rien une garantie que la clé qui sera fournie soit efficace et permettra de déchiffrer le contenu des disques durs. De même, une entreprise attaquée, qu'elle paye ou non la rançon, doit immédiatement renforcer sa sécurité car rien ne lui garantit de ne pas être attaquée une seconde fois.

S'il est communément admis que le ransomware est apparu pour la première fois en 1989 avec le cheval de Troie baptisé AIDS, « Aids Info Disk » ou encore PC Cyborg Trojan qui s'installait dans le fichier AUTOEXE.BAT de MS/DOS, ce mode d'attaque s'est très largement développé à partir de 2012 comme le notait alors le bureau d'enregistrement des plaintes du FBI (Internet Crime Complaint Center / IC3). Depuis, l'industrie du ransomware s'est structurée et on a vu émerger des offres de type « Ransomware as a Service », où un utilisateur lambda sans connaissances techniques spécifiques peut commander en ligne une attaque s'appuyant sur des ransomware prêts à l'emploi.

Outre une protection renforcée des postes clients et des serveurs notamment au moyen de solutions de protection endpoint Next-Gen ou de solution de type EDR, la parade contre une attaque de ransomware consiste à mettre en place des solutions de sauvegarde des données efficaces et surtout à l'abri des attaquants. C'est le seul moyen de reconstituer un système d'information après une attaque en limitant au maximum les pertes de données. ■

A.C.

« Zero Trust »

L'architecture « Zero Trust », appelée aussi ZTNA (Zero Trust Network Architecture) correspond à un modèle de sécurité post-périmétrique. Celui-ci est basé sur la notion qu'il ne faut pas accorder de confiance par défaut à un terminal se connectant au réseau de l'entreprise quelle qu'en soit sa nature. Même si un terminal est connecté sur le réseau interne de l'entreprise, celui-ci doit faire l'objet de contrôle de sécurité pour s'assurer que le poste ne va pas être utilisé à des fins malveillantes. Le niveau de contrôle et les droits d'accès qui vont être accordés au poste qui se connecte vont varier en fonction de la situation dynamique de celui-ci. Les contrôles vont être particulièrement renforcés lorsque l'utilisateur souhaite se connecter au système d'information depuis une chambre d'hôtel à l'étranger, depuis un accès Wi-Fi public d'un aéroport ou son domicile.

On associe l'essor de ce modèle de sécurité au développement des utilisateurs nomades et au télétravail généralisé qui voit de plus en plus de collaborateurs vouloir accéder à des ressources IT de l'entreprise hors des locaux. La paternité du terme est attribuée à John Kindervag, analyste chez Forrester en 2009 mais ses concepts de base remontent au début des années 2000.

Le niveau de sécurité apporté par le modèle « Zero Trust » s'appuie sur 3 grands principes : D'une part, il ne faut systématiquement accorder aux utilisateurs et aux machines que des droits minimums, ne jamais faire confiance par défaut et toujours vérifier et monitorer systématiquement. Cette vérification s'appuie sur des données techniques telles que la nature du poste de travail, ses logiciels installés, son hardware, le réseau mis en œuvre, mais aussi sa géolocalisation et, bien évidemment, les moyens d'authentification qui vont être utilisés par l'utilisateur afin de lui accorder ou refuser des droits d'accès aux ressources IT de l'entreprise. La montée en puissance des services de sécurité dans le Cloud et des technologies d'Intelligence Artificielle a permis d'étendre les contrôles réalisés dynamiquement sur les accès, notamment afin d'analyser en temps réel le comportement des utilisateurs. ■

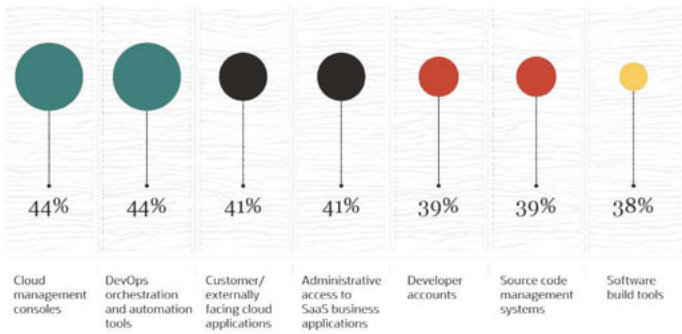
A.C.

IAM : La gestion des identités et des accès au cœur de l'approche « Zero Trust »

Migrer une infrastructure de sécurité vers le concept « Zero Trust » implique une gestion performante des identités et des accès. L'efficacité du système d'information tout entier repose sur l'IAM, une brique d'infrastructure dont les frontières ne cessent de s'étendre.

Parmi les grandes briques fonctionnelles de l'IAM figure la gestion des comptes utilisateurs et la notion d'annuaire universel qui regroupe les utilisateurs de l'ensemble des ressources informatiques de l'entreprise. Cette centralisation de l'ensemble des comptes permet notamment d'offrir aux utilisateurs une fonction de SSO (Single Sign-On) qui apporte un réel confort d'utilisation de leurs applications au quotidien, notamment pour accéder aux diverses applications SaaS auxquelles l'entreprise a souscrit. Une solution IAM doit supporter l'authentification forte de type MFA (Multi-Factor Authentication) quel que soit le moyen d'authentification choisi par l'entreprise. Les éditeurs de solutions IAM ont étendu le périmètre fonctionnel de leurs plateformes, notamment pour aller vers la gestion des API, la gestion des accès multicloud.

Les plateformes IAM trainaient la réputation de projets longs à mener et complexes à cause du fastidieux travail que représente la vérification des comptes actifs/inactifs dans toute l'entreprise, mais aussi des multiples intégrations à mettre en place avec les applications utilisées par les collaborateurs. Sur le plan technique, le modèle Cloud est venu apporter un élément de réponse. Le marché de l'IDaaS (Identity as a Service) grimpe en flèche avec un taux de croissance supérieur à 21% par an selon Markets&Markets. Ces offres Cloud simplifient aussi la connexion aux autres applications SaaS puisque les connecteurs pour les principales solutions du marché sont prêts à l'emploi et activables en quelques clics. La solution IAM peut alors jouer le rôle de plateforme de fédération d'identité à l'image de ce que Google, Facebook réalisent pour donner à de multiples sites B2C via leur identifiant unique.



Une étude KPMG montre que 51% des entreprises ont mis en place l'authentification multi facteurs mais celle-ci reste encore souvent cantonnée à quelques cas d'usage, quelques applications.

Source : KPMG, 2020

Un cadre pour la gouvernance des identités

Outre l'aspect purement fonctionnel de l'IAM pour les administrateurs et les utilisateurs, la mise en place d'une telle plateforme et un moyen d'élever le niveau de sécurité du système d'information par la mise en place de règles de gouvernance des identités et des accès que personne ne peut contourner. Accorder un accès à une ressource est contrôlé en temps réel au niveau de la plateforme et l'outil permet d'appliquer systématiquement une stratégie de moindre privilège (Least Privilege), un des grands principes de base de l'approche « Zero Trust ».

L'IAM se destine initialement à la gestion des identités des collaborateurs, mais l'approche a été déclinée en CIAM (pour Customer IAM) afin de gérer les identités des clients amenés à se connecter aux différents dispositifs digitaux de l'entreprise. Les fonctionnalités sont adaptées à la gestion de ce type de profils, de même que les

frais de licences, sachant qu'en B2C, le nombre de profils clients peut être extrêmement élevé. Dans le même ordre d'idée, IAM of Things (IAMoT) transpose l'approche au monde des objets connectés et de l'IoT. On sait que bon nombre d'objets connectés ont un niveau de sécurité très faible, beaucoup restant configurés toute leur durée de vie avec le login/mot de passe mis par défaut par leur fabricant. Pour ces derniers, l'enjeu est de disposer de solutions IAM spécialisées capables de gérer de manière industrielle les milliers voire les centaines de milliers d'identités des objets connectés qu'ils commercialisent en intégrant les spécificités de l'IoT en matière de connectivité, des faibles capacités de traitement de ces objets. Ce sera sans nul doute la prochaine évolution des plateformes IAM attendues pour ces prochaines années.

Les fonctions clés d'une plateforme IAM

- Gestion des comptes utilisateurs,
- Annuaire universel des comptes utilisateurs et terminaux,
- Gestion du cycle de vie des accès en temps réel,
- Gestion des ressources Cloud (IaaS, PaaS, SaaS),
- Fonction SSO (Single Sign-On),
- Authentification forte type MFA,
- Passerelle vers les applications tierces Cloud et on-premise,
- Gestion des accès aux API,
- Gestion de la conformité et reporting.

Pourquoi il faut renforcer les moyens d'authentification des utilisateurs

En parallèle à ce besoin de renforcer les procédures de gestion des identités, le besoin de sécuriser les moyens d'authentification est de plus en plus critique. Un simple mot de passe ne suffit plus à protéger l'accès d'un compte : Que ce soit par force brute, par ingénierie sociale ou vol de fichiers, les mots de passe de vos utilisateurs sont vulnérables et vendus par millions sur le Darknet.
Une récente étude Ponemon montre que dans 59% des entreprises, les collaborateurs doivent mémoriser de multiples mots de passe et il n'y a rien d'étonnant que « 123456 » ou « Azerty » restent des mots de passe encore très populaires ou que celui-ci soit inscrit sur un post-it collé à côté de l'écran. Mettre en place des procédures rigides au moyen d'une brique IAM afin de lutter contre les mots de passe triviaux et contraindre les collaborateurs à les renouveler fréquemment. Néanmoins, il ne s'agit que d'un pis-aller et il fait désormais consensus chez les experts qu'une authentification double ou multi-facteur est désormais nécessaire pour assurer un niveau de sécurité acceptable.

Le MFA devient la règle

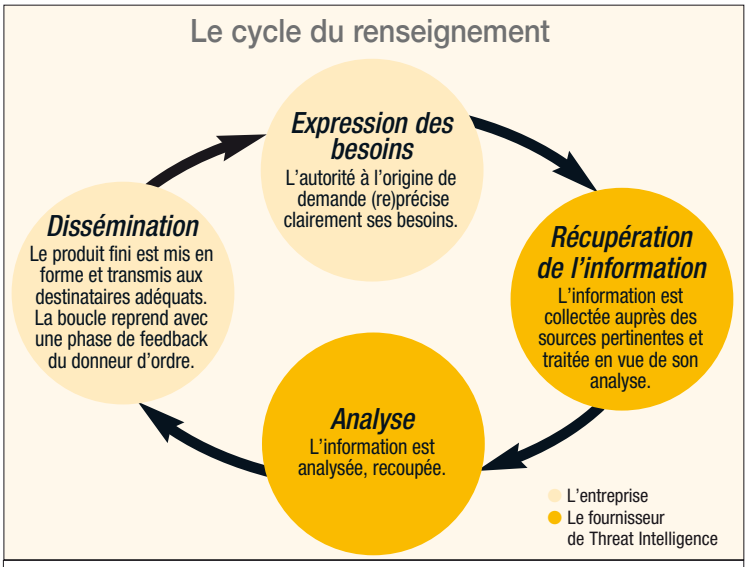
L'authentification à double facteur (2FA / 2 Factors Authentication) et l'authentification multi facteurs (MFA / Multi-Factor Authentication) consiste à mettre en œuvre un second facteur d'identification pour s'assurer que l'utilisateur qui saisit son mot de passe est bien la personne qu'il prétend être. Ce second facteur peut être une clé USB portant un jeton d'identification, une carte à puce, un certificat numérique. Depuis plusieurs années le standard FIDO2 a simplifié la connexion double facteur aux sites Web. C'est néanmoins l'essor du smartphone et des tablettes numériques qui a totalement révolutionné l'approche. Ces terminaux numériques offrent de multiples moyens d'authentification de l'utilisateur, notamment des dispositifs biométriques intégrés qui peuvent être exploités par le processus d'authentification sur les applications d'entreprise. Le moyen le plus simple consiste en l'envoi d'un SMS de confirmation à l'utilisateur au moment de sa demande de connexion. L'envoi d'un code permet de débloquer l'accès. Le dispositif est simple à mettre en œuvre et rapide mais les chercheurs ont montré sa vulnérabilité face aux attaques de spoofing et à la capacité des pirates à intercepter ces SMS et se connecter à la place des utilisateurs légitimes.
Néanmoins, le smartphone présente l'avantage de pouvoir faire tourner une application MFA mobile qui va pouvoir interagir avec la solution IAM pour accorder les accès. Le contrôle d'accès peut être réalisé par un code PIN, mais aussi la lecture d'empreinte qui équipe aujourd'hui tous les smartphones ou encore la reconnaissance du visage. Alors que la mise en œuvre de moyens biométriques était considérée comme extrêmement coûteuse et réservée à quelques cas d'usage bien définis, les smartphones ont participé à la démocratisation de l'accès à ces technologies par toutes les entreprises.
Le MFA est l'avenir de l'authentification forte et il est désormais une obligation pour les entreprises soumises à diverses réglementations, notamment la directive NIS ou la loi de programmation militaire. ■

A.C.

Threat Intelligence

La Threat Intelligence promet une veille et une analyse des menaces émergentes afin d'aider les entreprises à mieux anticiper.

Les prestataires de renseignement sur la menace (« Threat Intelligence ») collectent de l'information brute sur les cyber-menaces, les associent, les analysent et livrent à leurs clients des informations enrichies qui les aident à orienter leur stratégie de sécurité.
La matière première de ce type de service n'est pas nouvelle : à l'image de Monsieur Jourdain les (bons) éditeurs d'antivirus font de la Threat Intelligence pour leur propre compte depuis toujours ! Leurs chercheurs suivent l'activité des groupes de pirates de premier plan et documentent l'évolution de leurs capacités techniques, l'émergence de nouvelles techniques et de nouvelles menaces. Cela fait partie de leur coeur de métier.
Ce qui est nouveau, en revanche, c'est l'émergence d'un marché pour ce type d'information (voir encadré).



Dans le monde du renseignement, la collecte, l'analyse et l'exploitation du renseignement suit un cycle formel. L'entreprise devra le comprendre si elle souhaite tirer tous les bénéfices d'une solution de Threat Intelligence digne de ce nom.

Une exigence de maturité

Mais aussi séduisante soit-elle sur le papier, la Threat Intelligence exige de l'entreprise une véritable implication afin d'en tirer tous les bénéfices. Le cycle du renseignement (voir illustration) donne une bonne idée des responsabilités partagées entre le client et son fournisseur de Threat Intelligence.
Si l'on s'en tient à ce modèle, le fournisseur est responsable de la collecte et de l'analyse (étape 2 et 3) tandis que l'entreprise doit être capable de déterminer précisément ce qu'elle attend du service (étape 1) et de disséminer la bonne information aux bons destinataires (étape 4). Bien que ce modèle n'ait pas été conçu spécifiquement pour le marché de la Threat Intelligence il a le mérite de montrer que le client demeure en contrôle de ses besoins et de la dissémination de l'information. Ces deux phases exigent de l'entreprise une excellente compréhension de ses besoins et un bon niveau de maturité. Car autant les flux de données techniques pourront être livrés directement au

Un service de Threat Intelligence ?

Un bon fournisseur de Threat Intelligence sera en mesure d'associer divers flux d'informations concernant l'activité d'acteurs malveillants. Il s'agira par exemple de :

- Adresses IP ou domaines utilisés dans le cadre d'attaques présentes ou passées (notamment des serveurs de Command & Control)
- Informations sur les vulnérabilités zero-days mises en vente sur les marchés clandestins et leurs indicateurs de compromission (IoC) associés
- Statistiques sur les attaques en cours (quelles industries ? Quelles régions ?)
- Visibilité sur les groupes d'attaquants les plus actifs et leurs motivations, ou encore sur les systèmes les plus ciblés actuellement (quelle vulnérabilité a la cote ?)

Ces informations seront ensuite validées, dédoublées - automatiquement et par des experts humains - et des informations de réputation leur seront associées. Le tout sera alors livré aux clients sous forme de flux, parfois directement dans des équipements de sécurité (mise en place de listes de blocage) ou sous forme d'API, et même de fichiers Excel ! Charge alors à l'entreprise d'en faire bon usage.

LA RÉFÉRENCE POUR VOS ÉQUIPES DEVOPS

FAITES VOTRE VEILLE TECHNOLOGIQUE AVEC PROGRAMMEZ!

Abonnement numérique
(format PDF)
directement sur www.programmez.com

Kiosque / Abonnement - Version papier / Version PDF

SIEM ou aux équipements de sécurité sous forme de listes de blocages et seront alors immédiatement utiles, autant des informations plus prospectives ou plus "métier" exigeront un action manuelle.

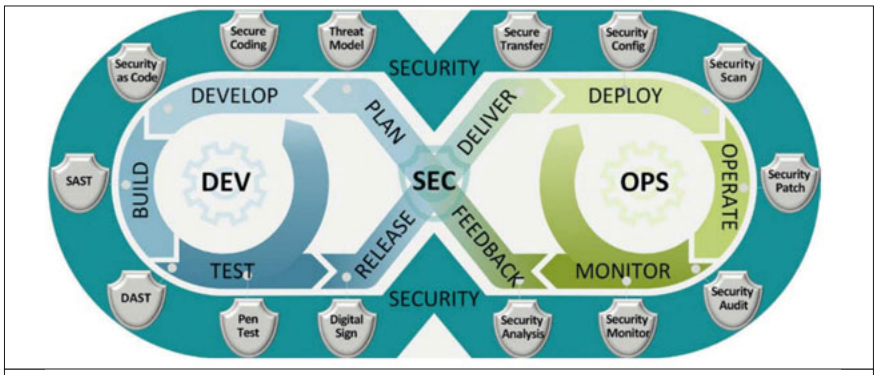
Au delà des flux techniques

Ainsi, que faire des rapports sur les menaces émergentes ou les nouvelles pratiques en cours ? Quel responsable sera le plus à même d'exploiter correctement cette information ? Quelles actions concrètes exige-t-elle ?
Ces actions seront avant tout managériales : il faudra comprendre ce qu'implique pour l'activité la recrudescence de telle ou telle pratique émergente chez les pirates, la recrudescence de telle attaque chez nos concurrents, ou encore faire le lien entre la motivation de tel groupe d'attaquants et son propre contexte : sommes-nous une cible ?
Il faudra alors valider que l'on dispose d'équipements vulnérables, ou peut-être comprendre qu'il s'agit seulement d'un problème de configuration. Et enfin déterminer la meilleure manière d'y faire face (corriger ? Isoler ?).
Et il ne s'agit encore là que d'une vision technique. Si les attaques en question intègrent une composante d'ingénierie sociale, par exemple, il faudra en outre être en mesure d'en comprendre les ressorts, déterminer si et comment ces derniers s'appliquent à l'entreprise, et enfin décider d'un plan de sensibilisation adapté. Et rien de tout cela ne s'automatise !
Tout ceci est un autre pan du marché de la Threat Intelligence, servi essentiellement par des consultants spécialisés, mais aussi par certains fournisseurs de solutions de Threat Intelligence de type « premium ». ■

J.S.

DevSecOps, la transformation digitale des DSI

Alors que le développement agile s'est désormais imposé dans de nombreuses entreprises, la cybersécurité doit désormais trouver sa place et pousser les développeurs vers le "Secure by design".



La cybersécurité doit être présente à chaque étape du SDLC (cycle de vie de l'application): Cela passe par des outils et des processus, mais aussi par une remise en cause de l'équipe de sécurité qui doit sortir du silo où elle a longtemps été enfermée. Crédit : DoD Enterprise DevSecOps Reference Design, 2019

Le besoin d'agilité a poussé les grandes entreprises à se convertir à DevOps. Ces grands groupes internationaux se sont dotés de structures de type "Agile at Scale" afin de mener à bien leur transformation digitale. Néanmoins, la sécurité a eu bien du mal à trouver sa place dans cette nouvelle organisation : administrateurs et développeurs considéraient les experts en sécurité comme un frein dans une organisation entièrement tournée vers l'efficacité. Le pari des DSI est d'intégrer pleinement les bonnes pratiques de sécurité au sein des processus de création des applications. Les équipes sécurité ne doivent plus opérer comme un silo qui intervient en dernier lieu, au moment de la mise en production de l'application. Il est temps de basculer dans l'ère du DevSecOps.

Les RSSI doivent se rapprocher des équipes agiles

Les membres de l'équipe cybersécurité doivent être intégrés au moins de façon partielle aux équipes DevOps de manière à s'assurer que les bonnes pratiques de sécurité sont effectivement bien appliquées tout au long du cycle de vie de l'application. C'est sans doute le plus grand défi à relever dans cette transformation qui doit mener aux préceptes DevSecOps. La cybersécurité doit être prise en compte à chaque étape de ce cycle de vie, depuis les phases très amont de conception de l'architecture logicielle et technique jusqu'à l'exploitation, en passant par les étapes itératives de Build. Le code source doit être écrit dans le respect des bonnes pratiques de sécurité éditées par les RSSI, testé avec des outils automatiques de test de sécurité, puis faire l'objet de PenTest (tests de pénétration) et ce souci de créer un code à la fois "Secure by design" mais qui intègre aussi la notion de "Privacy by Design" afin de s'assurer de la conformité de l'application aux diverses réglementations liées à la protection des données personnelles. ■

A.C.

La réponse à incident

Alors que les brèches semblent inévitables, la capacité à bien répondre aux incidents devient essentielle. Les entreprises, pourtant, n'y consacrent pas encore suffisamment d'effort et de budget.

Cette petite phrase s'est imposée en quelques années dans les cercles de la cybersécurité. Vraie ou non, elle illustre surtout un changement dans l'approche du problème : on ne se contente plus de tenter d'empêcher les attaques, mais l'on accepte l'éventualité d'une crise majeure. Et l'on veut donc pouvoir la gérer au mieux. Cela implique de bouter l'attaquant hors du réseau et de reprendre le contrôle de ses actifs, mais aussi de limiter l'impact de l'incident sur l'activité et d'en tirer tous les enseignements (notamment en analysant a posteriori les données techniques de l'attaque)

De telles ambitions exigent des équipes extrêmement bien formées, aguerries et mobilisables rapidement 24h/24. Pourtant, un tel dispositif ne sera que rarement activé. Il est alors non seulement difficile de justifier son coût, mais aussi de maintenir son efficacité! C'est là qu'interviennent les prestataires de réponse à incident.

Ces derniers mutualisent l'expérience, l'expertise et les ressources humaines qui font défaut à leurs clients. Outre leur capacité de mobilisation plus importante, ces intervenants apportent également des connaissances et une pratique que les équipes internes ont parfois du mal à maintenir.

Les équipes internes essentielles au succès du projet

Pour autant, le rôle des équipes internes est crucial : elles connaissent parfaitement le terrain et l'activité et seront donc en mesure de guider efficacement les équipes externes.

La clé du succès d'un tel projet est ainsi une parfaite communication entre le prestataire et son client. En outre ce dernier doit faire l'effort d'anticiper l'intervention, notamment en documentant son réseau et ses procédures. Ainsi la signature d'un contrat de réponse à incident est presque un projet en soi !

Comment choisir un prestataire ?

Un bon prestataire de réponse aux incidents pourra prouver la qualité de ses intervenants (par leurs certifications notamment), leur disponibilité (qui sera encadrée contractuellement) et sa bonne connaissance des méthodes d'attaques du moment.

Les points de vigilance

Personnes	Assigner les bons contacts, être au clair sur les responsabilités de chacun, disposer des bonnes certifications.
Processus	Documenter les actions qui doivent être menées par chaque entité, prendre en compte les obligations légales (préservation de la preuve), tracer chaque action.
Technologie	Connaître son « terrain » technologique, les équipements et les solutions mises en oeuvre, leur état (correctifs, vulnérabilités…)
Information	Collecter des informations sur l'état du système d'information avant et pendant l'attaque, le contexte de l'incident, son origine, ses leviers, ses impacts, les intervenants extérieurs.

L'incident : pas seulement une affaire IT !

La réponse à incident est un processus pluridisciplinaire. La gestion de la crise doit également impliquer des juristes, des représentants des ressources humaines et de la communication. Ils doivent être en mesure de travailler de concert avec les équipes IT et sécurité, afin d'assurer que l'entreprise traverse la crise en subissant le moins d'impact possible, globalement, et chacun dans leur domaine respectif. Un bon prestataire de réponse à incident sera en mesure de s'intégrer dans un tel dispositif.

Le référentiel PRIS

Afin d'aider les entreprises à choisir le bon prestataire, l'ANSSI a créé un référentiel des prestataires de réponse à incident. À ce jour cela n'est toutefois qu'à titre indicatif, car aucun prestataire n'est encore qualifié, et seulement dix fournisseurs en cours de qualification ont accepté d'apparaître publiquement. ■

J.S.

Protection du poste de travail

Le bon vieil antivirus a évolué : La génération EDR (Endpoint Detection and Response) et maintenant les solutions XDR vont de plus en plus loin pour protéger les parcs de PC et les serveurs. Cette montée en puissance a été rendue nécessaire pour contrer à la fois les vagues successives de malwares qui continuent à déferler sur les entreprises, mais aussi réduire autant que faire se peut le délai de détection des redoutables APT.

Le marché des outils de protection du poste de travail est probablement le mieux connu, le plus ancien et l'un des plus vastes en matière de cybersécurité.

Parti des seuls antivirus dans les années 1980 il a évolué au fil des décennies pour aboutir à un ensemble de fonctions de sécurité intégrées au sein d'un client unique.

Sa fonction centrale demeure bien entendu la lutte contre les codes malveillants. L'antivirus s'est fait « anti-malware », un terme désormais fourre-tout qui englobe les capacités offertes par feu les anti-spywares, anti-rootkits, anti-adwares et autres « anti-tout » !
Ces outils ont donc su évoluer avec les menaces. Ils intègrent ainsi désormais aussi des protections plus génériques telles que la détection de vulnérabilités locales, la détection comportementale et le contrôle applicatif (sandboxing), la protection de la mémoire, l'analyse de réputation, et parfois même des fonctions légères de prévention des fuites de données ou de chiffrement du disque. Mais quelles que soient ses technologies l'outil de protection du poste aura toujours comme objectif d'empêcher l'exécution de code malveillant sur le poste de travail, quelle que soit la technique d'infection ou de persistance exploitée par ce dernier.

Les fonctions essentielles à exiger

ANTI-MALWARE	C'est la base et il faut le faire bien ! On inclut ici à minima les fonctions auparavant fournies par les antivirus, anti-adwares, anti-spywares, anti-rootkits, etc.
PARE-FEU PERSONNEL	Que ce soit au moment de l'infection ou pour contacter ensuite un serveur de Command & Control, les malwares exigent un accès à Internet. Et donc un pare-feu personnel est essentiel à l'anti-malware.
CONTRÔLE DES PÉRIPHÉRIQUES ET DES PORTS	Seconde voie d'infection après la navigation Internet ou l'email, les périphériques (USB notamment) doivent être contrôlés. Et cela permet en prime d'appliquer des politiques de chiffrement efficaces sur les supports externes.
TABLEAUX DE BORD & ADMINISTRATION CENTRALISÉE	L'outil doit pouvoir se déployer et s'administrer de manière centralisée, et fournir des rapports clairs sur l'état de protection du parc.
SUPPORT NON-WINDOWS	Autant aller jusqu'au bout du concept de la simplification du déploiement et de l'administration avec une solution unique disponible aussi pour Mac et Linux, voire spécifique à Microsoft Exchange et Sharepoint, par exemple.

Best of breed ou simplicité d'administration ?

Vaut-il mieux sélectionner un produit expert dans chaque fonction souhaitée, et ainsi devoir gérer une multitude de clients sur le poste de travail, ou opter pour un client unique qui ne saurait certes être excellent en tout mais dont l'administration sera largement simplifiée ? La question s'est posée dès les premières acquisitions par les grands éditeurs d'antivirus de plus petits éditeurs de technologies alors innovantes (anti-spam, détection d'intrusion locale, anti-rootkit, etc.).

Elle semble désormais réglée tant les entreprises optent majoritairement pour un client intégré et, selon l'analyste Gartner, consolident ce qui ne l'est pas encore.

Certes, des spécialistes de niche se créent encore mais ils ne manqueront pas d'être rachetés à leur tour par les poids lourds du domaine dès lors qu'ils auront fait la preuve de leur pertinence.

En définitive sur ce marché, les petits spécialistes innovent et les grands éditeurs rachètent !

SANDBOXING	L'isolation des applications est la seule approche générique susceptible de garantir pleinement la protection du poste de travail. Si elle n'est pas toujours applicable et doit être secondée, elle n'en demeure pas moins un atout important.
RÉPUTATION	L'analyse en temps réel de la réputation des sources (domaines, adresses IP) et des documents joue le rôle d'un système d'alerte collaboratif avancé. Cette approche est très efficace en complément des autres méthodes de détection.
PRÉVENTION DES FUITES DE DONNÉES (DLP)	La capacité du client antimalware à assurer un contrôle local pour le compte d'une solution de prévention des fuites de données (DLP) permettra de simplifier la mise en oeuvre de ce type de solution.
ENDPOINT DETECTION AND RESPONSE (EDR)	L'EDR apporte le volet « réponse » à des solutions jusqu'à présent plus axées « prévention ». Catégorie encore souvent à part aujourd'hui, elle sera certainement la prochaine à être intégrée aux outils de protection du poste de travail. Autant anticiper !

L'avenir est à la réponse

Si le marché de la protection du poste de travail est essentiellement tourné vers la prévention (on tente d'empêcher l'exécution du code malveillant), il a désormais tendance à évoluer vers la réponse. On voit ainsi émerger le marché du Endpoint Detection and Response, ou EDR. Ces outils surveillent en temps réel divers appels systèmes à la recherche des signes traditionnels d'exploitation d'une vulnérabilité. Ils offrent ainsi une vision temps-réel de l'activité des postes de travail, et permettent - en théorie - de bloquer l'exploitation d'une vulnérabilité inconnue.

Mais l'autre apport innovant de ces solutions - le « R » de « Response » - est leur capacité à collecter de nombreux paramètres liés à l'activité des postes de travail et ainsi permettre l'investigation poussée des brèches. Ces outils permettent notamment de récupérer immédiatement et à distance des éléments de n'importe quel poste (clé de registres, processus, dump de la mémoire vive, etc.). Les informations qu'ils collectent peuvent également être archivées et servir ultérieurement à enquêter sur une brèche ou définir plus aisément de nouveaux indicateurs de compromission (IoC) à diffuser. ■

J.S.

Protection des terminaux mobiles

Les terminaux mobiles sont encore une catégorie à part, mais pour combien de temps encore ? La tendance est à la protection de l'information quel que soit son support. Alors anticipons !

A l'heure où les ultra-portables dernier cri se font tactiles, plus légers et moins encombrants que les nouvelles tablettes professionnelles extra-larges, où se situe la frontière entre un poste de travail et un terminal mobile ? Et qu'est-ce qui distingue donc encore une solution de protection mobile de celle destinée aux postes de travail traditionnels ? Pas grand chose, à vrai dire. Mais encore suffisamment pour que la protection des terminaux mobiles fasse l'objet d'une catégorie à part dans cette édition du guide de la cybersécurité.

La sécurité tournée vers la donnée

Cela ne sera peut-être pas toujours le cas : la tendance est en effet de placer l'information - et non plus le terminal - au cœur de la stratégie de protection de l'entreprise.
Les notions de protection de l'information (le chiffrement, la classification, une gestion granulaire des droits) et du terminal (anti-malware, supervision, contrôles continus) convergent alors et doivent s'exercer à l'identique quel que soit le terminal.
C'est pourquoi il est important de rechercher dès aujourd'hui une solution de protection mobile capable de s'inscrire à terme dans cette stratégie globale : en choisissant par exemple un éditeur offrant une large couverture et ayant dès aujourd'hui une politique de convergence, ou un acteur de niche disposant d'accords (et d'API !) permettant à ses produits d'être supervisés et de s'intégrer sans heurt dans une infrastructure plus large. ■

J.S.

Le chiffrement, fonctionnalité reine de la mobilité

Le chiffrement intégral demeure la fonctionnalité incontournable des équipements mobiles, dont le risque de perte ou de vol est accru. Préférez pour cela une solution présentant des certifications internationales telles FIPS 140-2 ou Critères Communs (EAL).

Protection de la donnée

Et si l'on cherchait à protéger aussi la donnée elle-même, plutôt que seulement les systèmes qui la traitent ?

La montée en puissance des aspects réglementaires -notamment en ce qui concerne les données à caractère personnel- a rendu incontournable une nouvelle approche de protection dite "data centric", basée sur la donnée elle-même. Son objectif est de protéger le contenu plutôt que le contenant.
Pour cela le marché offre trois approches : le chiffrement, la gestion des droits numériques (EDRM) et la prévention des fuites de données (DLP).

J.S.

Gestion des droits numériques : pour garder le contrôle.

Les solutions de gestion des droits numériques (EDRM) permettent aux documents d'embarquer leurs propres règles d'accès et ainsi de garder le contrôle de la donnée lorsque celle-ci a quitté l'entreprise. Il sera ainsi possible de décider qu'un document PDF ne pourra être lu que sur une période donnée, ou encore de le mettre à jour une fois diffusé. Ces solutions permettent également de décider ce qui pourra être fait avec le document : copie, édition, impression, ouverture depuis quel type de terminal, etc.

EDRM : les questions à se poser

- Quels formats sont supportés ? (Adobe, Word, Excel, images, AutoCAD…)
- Disponibilité de connecteurs ? (CASB, DLP, ERM, partage de fichiers…)
- Simplicité de l'interface de création des politiques de sécurité ?
- Capacité à interpréter les politiques de sécurité existantes (règles SharePoint, etc.)

Le DLP, contre les fuites accidentelles

Mal comprises, jugées trop simples à contourner, les solutions de DLP n'ont pas toujours bénéficié d'une bonne réputation. Mais il s'agit assurément d'un malentendu : le marché de la prévention des fuites de données protège avant tout de l'erreur humaine et non du vol de donnée !

Associés à une solution de classification des données, les outils de DLP s'assurent, par exemple, que le document Excel signalé comme « Interne » envoyé par email n'est effectivement adressé qu'à des correspondants internes (qui n'a jamais commis d'erreurs liées à la saisie semi-automatique des adresses ?).

Sachant que l'erreur humaine est l'une des principales causes de pertes de données en entreprise, c'est un bon investissement !

Comme pour beaucoup de solutions de sécurité, les modèles d'intelligence artificielle sont en train d'étendre la vision des solutions de prévention des fuites de données. Des prestataires Cloud proposent ainsi de rechercher les données de l'entreprise qui ont déjà franchi ses protections et qui circulent sur Internet ou sur le Dark Web. Les algorithmes recherchent inlassablement les fichiers sensibles de l'entreprise afin de générer une alerte si un fichier sensible est repéré sur un forum de hackers ou tout simplement sur un disque dur portable ou la box Internet d'un salarié qu'il n'aurait pas sécurisé. Des spécialistes se chargent alors de neutraliser la fuite.

DLP : les questions à se poser

- Positionnement de la solution : sur les postes de travail, sur le réseau ou les deux ?
- Peut-on appliquer une politique unique entre réseau et postes de travail ?
- Support des applications métiers en mode SaaS ?
- Disponible sous forme d'appliance virtuelle ?
- Est-ce une solution dédiée au DLP ou s'agit-il d'une fonctionnalité complémentaire (présente sur certains pare-feux nouvelle génération, outils de classification, systèmes de détection d'intrusion, cloud access security brokers, etc.)

Le chiffrement, l'approche historique

Le chiffrement protège la donnée au repos (stockée) ou en mouvement (sur le réseau). Il intervient au niveau du matériel (équipements réseaux par exemple), du stockage ou de l'application (chiffrement des bases de données, par exemple). L'action de chiffrer peut être transparente (la donnée est alors protégée automatiquement sans intervention de l'utilisateur) ou déclenchée par ce dernier.

Le chiffrement de la donnée au repos couvrira le risque de vol des supports (ordinateur portable, supports externes tels que disques durs ou clés USB) tandis que le chiffrement de la donnée en mouvement couvrira l'interception de cette dernière (présence de l'attaquant sur le réseau).

Chiffrement : quelques questions à se poser

- Souhaite-t-on protéger des données stockées ou en transit ?
- Chiffrement du stockage, de l'applicatif, ou des bases de données ?
- Chiffrement transparent (« Full disk encryption ») ou volontaire ? (« file encryption »)
- Comment seront gérées (et générées) les clés ?
- Existe-t-il une clé maître ?
- Chiffrement individuel ou multi-utilisateurs ?
- Comment gérera-t-on les sauvegardes et l'archivage des données chiffrées vis-à-vis des changement de clés ?

Protection applicative

Avec 90 % des attaques ciblant la couche applicative, la protection des applications doit être une priorité. En particulier sur le Web.

Selon des chiffres du département américain de la sécurité intérieure, 90 % des attaques ciblent la couche applicative (en particulier sur le web). Heureusement, le marché propose deux approches complémentaires pour se protéger : l'une placée devant l'application à protéger, et l'autre en son cœur !

Le WAF en frontal des applications web

Le pare-feu applicatif web (WAF, pour Web Application Firewall) se place devant l'application et filtre le trafic qui lui est destiné. Fonctionnant à base de signatures le WAF va rechercher les signes d'attaques connues.
Le WAF ne demande pas de toucher à l'application, et il sera donc idéal pour protéger une application vieillissante impossible à améliorer (lorsqu'un règlement tel PCI-DSS lui impose un certain nombre de fonctionnalités de sécurité !).

La protection automatique du runtime (RASP)

Alors que le WAF est externe à l'application, l'approche du Runtime Application Self-Protection (RASP) est résolument interne : il s'agit de s'intercaler entre le code de l'application et les bibliothèques qui lui sont nécessaires, afin d'intercepter les appels jugés dangereux.
Si le RASP présente de nombreux avantages par rapport au WAF, il souffre de la nécessité d'accéder dans certains cas au code source de l'application et de déployer un outil spécifique sur le serveur. En outre ces outils ne supportent à l'heure actuelle que les technologies Java et .NET !

Exigez l'OWASP Top 10 !

La meilleure façon de protéger une application est de bien la concevoir dès le départ !
Pour cela l'association américaine Open Web Application Security Project (OWASP) œuvre depuis 18 ans à sensibiliser les développeurs web aux bonnes pratiques du développement sécurisé. Elle diffuse un outil contractuel d'une redoutable efficacité : une annexe prérédigée que tout donneur d'ordre pourra inclure au contrat de développement web qu'il s'apprête à signer. Celle-ci liste les 10 points-clés de sécurité que l'application devra respecter pour être recevable. C'est simple, c'est très efficace et c'est gratuit ! ■

J.S.

https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Audit d'architecture

L'audit d'architecture s'intéresse au SI dans son ensemble et cherche à valider la pertinence des choix technologiques et le respect des bonnes pratiques de sécurité

De tous les audits techniques, l'audit d'architecture est peut-être celui au périmètre le plus large. Il s'agit en fait d'un audit macroscopique ! Selon le périmètre, ce type d'audit exigera plus de temps et de ressources que les autres. Son objectif est de s'assurer que le Système d'Information (sa topologie, son organisation, ses priorités) est conforme aux exigences métiers, aux divers règlements qui s'y appliquent et aux bonnes pratiques de sécurité. L'audit d'architecture évaluera également les choix technologiques opérés par l'IT et la SSI, leur pertinence ainsi que la qualité de leur implémentation (et accessoirement leur bonne configuration, voir encadré)

Le choix du prestataire

Si dans le cadre du test d'intrusion l'entreprise suit souvent un auditeur individuel, l'audit d'architecture est une affaire d'équipe et de compétences multiples : un seul auditeur sera difficilement expert de l'ensemble des bonnes pratiques et des solutions déployées au sein de l'entreprise. En outre le prestataire devra disposer d'un volet de certifications éditeurs étendu. Ces contraintes font qu'à compétences égales, plutôt qu'un pure player du conseil il sera possible d'envisager un intégrateur spécialiste de la sécurité capable d'offrir du conseil. ■

J.S.

L'audit de configuration

L'audit de configuration est une prestation parfois distincte mais complémentaire à l'audit d'architecture. Plus ciblé, celui-ci porte sur la pertinence des configurations matérielles et logicielles du SI. Celles-ci seront étudiées sur la base des guides d'installation officiels, parfois des codes sources et surtout des meilleures pratiques de l'industrie. Là aussi, l'objectif est d'identifier les mauvaises pratiques (les configurations par défaut notamment) et de proposer un plan de correction.

SOC

Un Security Operations Center est le centre névralgique de la sécurité : il centralise, analyse et répond 24h/24, sept jours sur sept.

Le SOC est la pierre de voûte de l'édifice sécurité. Son rôle est d'unifier la fonction sécurité autour d'une organisation resserrée afin de détecter et de répondre aux menaces de manière coordonnée.
Élément central d'une stratégie sécurité, le SOC vient finaliser une démarche probablement entamée de longue date. Car pour en tirer tous les bénéfices l'entreprise devra avoir déjà atteint une maturité sécurité importante : elle devra notamment pouvoir compter sur des équipes expérimentées, des processus bien rodés et une bonne maîtrise des solutions qu'elle exploite déjà.
Ceci est particulièrement vrai, bien entendu, pour le SOC interne qu'elle animera seule. Mais c'est également le cas, dans une certaine mesure, du SOC exploité par un prestataire externe.
L'approche interne ne concernant que peu d'acteurs, nous nous intéresserons dans ce guide au choix d'un prestataire externe capable d'animer un SOC pour le compte de ses clients.

Les fonctions offertes par un SOC externe

- Intégration et supervision des flux de trafic de l'entreprise
- Surveillance continue des équipements et des solutions de sécurité (souvent à l'aide d'un SIEM exploité par le prestataire)
- Gestion des vulnérabilités remontées par un outil d'analyse automatisée
- Pré triage des alertes (nombreuses à ce stade !)
- Priorisation des alertes
- Gestion de la réponse selon les consignes de l'entreprise
- Analyse de la cause de l'incident
- Actions correctives (mises à jour, changement de configuration, etc.).

Ce que vous fournirez à votre prestataire de SOC externe

- Rapports d'analyses de vulnérabilités automatisées
- Liste des commandes sensibles passées aux bases de données
- Liste des commandes sensibles passées par les administrateurs systèmes
- Requêtes émises vers et renvoyées par les serveurs web
- Journaux des systèmes de filtrage de contenu web
- Journaux des équipements de sécurité (WAF, IDS, antivirus, etc.)
- Journaux du système d'authentification
- Journaux de la plateforme d'emails
- Autres journaux applicatifs (souvent centralisés au sein d'un SIEM)
- Requêtes DNS internes et vers l'externe
- Autres sources d'événements applicatifs (notamment issus d'applications hébergées en mode SaaS)

À noter : l'ANSSI propose un programme de qualification des « ***Prestataires de détection d'incidents de sécurité*** » (PDIS) qui pourra aider à présélectionner les prestataires. La liste des sociétés qualifiées est disponible ici : **https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/**

Multi-tenant or dédié ?

L'essentiel des offres de SOC externalisées est « multi-tenant » : les ressources techniques et humaines sont partagées entre tous les clients et les informations sur les menaces issues des flux d'un client bénéficient à tous les autres. Considérant que le coût de ressources dédiées serait largement plus élevé et que la mutualisation de l'analyse des flux bénéficie à l'ensemble des clients, ce n'est pas une mauvaise chose, à condition d'obtenir des garanties sur la confidentialité et l'isolation des informations clients.

La question de la confidentialité

Le prestataire devra notamment être en mesure de prouver qu'il prend les mesures nécessaires pour garantir l'isolation des informations confidentielles fournies par chaque client. En outre, le SOC étant par définition un point névralgique, il doit bénéficier lui-même d'un niveau de protection logique et physique adapté à la sensibilité des informations qu'il traite.

Les ressources internes

La mise en place d'un SOC externe n'est pas un projet mineur. Cela exigera des ressources et des efforts de la part de l'entreprise, tant avant que pendant la durée du contrat.
Avant, il sera notamment nécessaire de fournir des procédures précises de réaction aux incidents : qu'est-ce qui est normal dans le cadre de l'activité ? À partir de quel seuil tel ou tel événement devient-il une alerte ? Depuis quels pays des connexions de nos collaborateurs sont-elles légitimes ?
Enfin, durant la phase d'exploitation, il faudra être en mesure de répondre aux alertes et sollicitations du prestataire en temps et en heure, avec des procédures bien établies. Ce qui est déjà tout un projet en soi ! ■

J.S.

Tableaux de bord de sécurité

Meilleure visibilité et aide à la prise de décision : les tableaux de bord de sécurité sont un outil indispensable dans le pilotage de la sécurité.

Selon l'institut SANS, la difficulté à fixer les bonnes priorités et à mesurer la sécurité sont parmi les principales causes de défaillance de la cybersécurité. Les tableaux de bord de sécurité apportent une solution à ces deux freins. Et pourtant, si les entreprises ont souvent de bons tableaux de bord commerciaux, elles peinent à mettre en place l'équivalent en cybersécurité. Et quand ils existent ceux-ci sont souvent dédiés à la seule conformité. Mais la conformité n'a jamais garanti la sécurité !

Point de départ et référentiel quotidien

De bons tableaux de bord de sécurité présentent un double avantage : ils sont d'abord un excellent point de départ pour initier une démarche de cybersécurité. Ils aident à couvrir l'essentiel des éléments de base d'une stratégie de protection.
Mais ils sont surtout au quotidien le meilleur moyen de détecter les écarts dans la posture de sécurité de l'entreprise. Ils offrent une vision globale du niveau de risque à un instant T et sa tendance (sommes-nous en progrès ou nos capacités de remédiation baissent-elles ?)

SIEM, SOC et conseil !

Parce que les indicateurs nécessaires au tableau de bord sont issus des équipements de sécurité et autres sources techniques, ils peuvent être un produit dérivé d'une solution de SIEM, voire même être fournis par le prestataire du SOC externalisé.
Mais le tableau de bord sécurité peut aussi être un projet d'entreprise à part entière.
Il pourra alors être mené en interne ou avec l'aide d'un consultant. L'essentiel de la mission consistera à identifier les indicateurs pertinents et leurs sources, à déterminer les valeurs de seuil (qu'est-ce qui est anormal ?), à mettre en place les connecteurs nécessaires pour récupérer les données et enfin à trouver une solution de présentation adaptée. ■

J.S.

SIEM

Alimenté par l'ensemble des événements du SI, le SIEM voit, analyse et identifie les attaques. Mais il vaut peut-être mieux le faire exploiter par un spécialiste externe.

Un Security Information & Event Manager agrège des informations en provenance de sources diverses (applications, systèmes, équipements d'infrastructure...) afin d'identifier des attaques potentielles.
La force du SIEM réside dans sa capacité à corréler des signes qui, pris individuellement, seraient restés ignorés. Et donc à produire des alertes que l'on espère plus pertinentes.
Les SIEM sont utiles en temps réel pour donner l'alerte, mais aussi a posteriori pour aider l'analyse forensique. Ils contribuent également au respect des obligations réglementaires en alertant sur des situations non conformes.
Mais comme toute solution complexe, leur mise en oeuvre et surtout leur exploitation peut s'avérer trop coûteuse en interne. C'est pourquoi ces outils sont souvent exploités par un prestataire qui fournit en retour un flux d'alertes et, en option, pourra y répondre (voir SOC). ■

J.S.

4 questions à poser avant l'achat

1 ***Ai-je vraiment besoin d'un SIEM ?***
Le SIEM est un outil puissant capable de détecter des attaques sophistiquées. Il ne sera utile que si l'entreprise est déjà en mesure de détecter et de répondre aux attaques plus communes. Avez-vous vous déjà, par exemple, une solution de log management bien exploitée ?

2 ***Interne ou externe ?***
Exploiter correctement un SIEM exigera très probablement des ressources supplémentaires. C'est pourquoi il est courant de déléguer l'exploitation d'un SIEM à un prestataire (voir notamment le référentiel des « Prestataires de détection d'incidents de sécurité » (PDIS) qualifiés par l'ANSSI)

3 ***Support des sources existantes ?***
Les principaux SIEM proposent un grand nombre de connecteurs vers les équipements et applications communes, mais il sera nécessaire de faire un pointage précis.

4 ***Et les sources externes ?***
Le SIEM choisi est-il en mesure d'accepter des sources d'information externes ?

AFCDP

(Association Française des Correspondants à la protection des Données à caractère Personnel)

L'AFCDP, créée dès 2004, regroupe plus de 6000 professionnels de la conformité à la Loi Informatique & Libertés et au RGPD – dont les Délégués à la Protection des Données (ou DPO, pour Data Protection Officer).

Association représentative des DPD, l'AFCDP rassemble non seulement les professionnels de la protection des données et des DPD désignés auprès de la CNIL, mais aussi toutes personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside notamment dans la diversité des profils des adhérents : DPD, délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualiticiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Dès sa création, l'association s'est attachée à deux missions :

- Mutualiser, entre professionnels concernés, les expertises et les réussites, les interrogations, les bonnes pratiques.
- Promouvoir et défendre le nouveau métier de DPO (Data Protection Officer), tant auprès des décideurs publics et relais d'opinion que des entreprises, institutions et organisations, afin de leur faire prendre conscience des nouveaux enjeux de la protection des données personnelles et des modifications juridiques.

L'AFCDP fait le lien entre les professionnels de la protection des données à caractère personnel, les institutions et décideurs publics (CNIL, Parlementaires…), et les entreprises. Par son expertise et l'expérience de ses membres, elle formule régulièrement des recommandations et/ou des avis aux autorités publiques et aux acteurs de la protection des données personnelles et de la conformité. En 2021, à l'occasion de l'Université AFCDP des DPO plus de 850 DPO se sont réunis pour ce grand rendez-vous annuel désormais incontournable, et pensé en 100% distanciel en raison du contexte. Il s'est décliné ensuite en plusieurs ateliers mensuels réunissant entre 200 et 300 personnes connectées. La prochaine édition, début 2022, sera en version hybride.

"L'AFCDP entend défendre une conception de la protection des données qui met en son cœur une approche active, qui concilie les droits fondamentaux de chacun avec la possibilité pour les organismes que nous représentons de continuer à créer et innover. Cette approche se fonde sur certains principes que nous sommes heureux de voir repris dans le règlement européen : la souveraineté des individus sur l'usage de leurs données et la responsabilisation des entreprises. Ensemble, ces deux principes permettent de créer la confiance nécessaire à l'épanouissement de l'usage du numérique en France."

Souligne Paul-Olivier Gibert, Président de l'AFCDP.

ANSSI

(Agence nationale de la sécurité des systèmes d'information)

Créée en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité. Placée sous l'autorité du Premier ministre et rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), elle bénéficie d'un positionnement lui permettant de déployer une politique globale de cybersécurité et d'en assurer la coordination à l'échelle interministérielle.

La mission première de l'ANSSI est d'assurer par différents moyens la sécurité des infrastructures numériques publiques et privées les plus critiques et de les défendre en cas d'attaque informatique.

Au-delà de ces organisations les plus sensibles, elle s'adresse également à l'ensemble des acteurs de la transformation numérique du pays pour élever le niveau de cybersécurité global de la nation et favorise les conditions d'un dialogue de confiance avec ses partenaires français, européens et internationaux.

L'ANSSI en chiffres (2020)

- **114 certifications délivrées**
- **132 qualifications délivrées**
- **15 centres d'évaluation agréés au 31 décembre 2020**
- **64 formations labellisées SecNumedu au 31 décembre 2020**
- **20 opérations de cyberdéfense en 2020**

Les Visas de sécurité (voir pages 8-9)

En 2017, l'ANSSI s'est engagée dans une démarche de valorisation de ses activités de qualification et de certification : le Visa de sécurité ANSSI. Délivré par l'agence, il permet d'identifier facilement des solutions de sécurité numérique fiables et reconnues comme telles à l'issue d'une évaluation réalisée par des laboratoires agréés selon une méthodologie rigoureuse et éprouvée.

Cette évaluation prend notamment la forme de tests de pénétration poussés et d'une analyse approfondie pour vérifier la conformité de ces solutions aux référentiels correspondants.

Ce Visa se matérialise, selon le contexte et le besoin, par une certification ou une qualification. Il est un gage de sécurité pour les utilisateurs et un gage de compétitivité pour les fournisseurs et prestataires de services.

Contact

Agence nationale de la sécurité des systèmes d'information

51, boulevard de La Tour-Maubourg
75700 Paris 07 SP

Email : **communication@ssi.gouv.fr**
Site web : **www.ssi.gouv.fr/**
Twitter : **@ANSSI_FR**
Dailymotion : **DAILYMOTION.COM/ANSSI_FR/**
LinkedIn : **LINKEDIN.COM/COMPANY/ANSSI-FR**

Campus Cyber

Conçu, mis en place et dirigé par Michel Vandenberghe, (précédemment à la tête d'Orange Cyberdéfense), avec le soutien de l'ANSSI cet ambitieux projet a été initié par le président de République Emmanuel Macron.

Ce « Lieu totem de la cybersécurité » rassemblera les principaux acteurs nationaux et internationaux du domaine : des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des acteurs de la recherche et des associations.

Le Campus Cyber prévoit de mettre en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs.

Des partenariats entre le Campus national et des Campus territoriaux de cybersécurité seront développés dans les prochains mois.

Fin septembre, plus de 100 acteurs, issus d'une pluralité de secteurs d'activité, ont confirmé leur engagement.

Lieu vivant et ouvert, son immeuble de 26 000 m2 ,situé à la Défense, offrira à ses résidents et à ses partenaires des bureaux et des services communs (showroom, amphithéâtre, espace événementiel , espaces de formation etc).

Le Campus Cyber permettra, en rassemblant les experts de l'analyse cyber de :

- renforcer les capacités de veille, de détection et de réponse à la menace.
- créer un observatoire de la cybermenace et une base commune de « Threat Intelligence » composée des indices de compromission assemblés par les différents partenaires publics et privés.

L'accent est également mis sur la formation, avec notamment des programmes communs d'entraînement et de formation dispensés par des écoles ou des centres de formation.

Ouverture prévue pour fin 2021 / début 2022

Contact : **Campuscyber.fr**
https://campuscyber.fr/

CESIN

Le Club des Experts de la Sécurité de l'Information et du Numérique est une association regroupant des professionnels de la sécurité des systèmes d'information. Ses membres actifs doivent obligatoirement exercer une responsabilité dans la SSI au sein de leur organisation.

Au-delà du partage de connaissances et de l'enrichissement du réseau professionnel de ses membres, la vocation du CESIN est de porter la voix du RSSI en tant que profession. Le club participe à de nombreux événements, édite un baromètre annuel sur l'état de la cybersécurité des grandes entreprises françaises, aide à faire reconnaître et évoluer le métier de RSSI, ainsi qu'à alimenter la réflexion autour de son positionnement dans l'entreprise. Le club se donne également pour mission de sensibiliser les dirigeants d'entreprises face au risque cyber.

Par ailleurs, au travers des partenariats avec les pouvoirs publics, le CESIN ambitionne d'accompagner les évolutions réglementaires concernant la sécurité numérique.

Les membres du CESIN se retrouvent tout au long de l'année à l'occasion de groupes de travail dont les thématiques couvrent tous les domaines de la SSI, de la gouvernance ou l'analyse de risque, en passant par des thématiques plus opérationnelles, industrielles ou juridiques…

Le CESIN organise enfin un Congrès annuel en décembre, durant lequel ses membres, réunis en groupes de travail, se livrent à des analyses prospectives, des débats thématiques, et partagent leurs retours d'expérience.

Le Club est présidé par Mylène Jarossay, CISO du groupe LVMH.

Comment le CESIN aide les entreprises françaises

• ***Echange :*** le CESIN offre aux RSSI des entreprises françaises un environnement au sein duquel ils peuvent se rencontrer et échanger entre pairs.

• ***Information :*** A travers les travaux de ses membres, le CESIN publie des analyses et des études statistiques utiles, dont le baromètre annuel de la cybersécurité.

• ***Influence :*** En se donnant comme objectif d'accompagner les évolutions réglementaires et de porter la voix des RSSI, le CESIN œuvre à favoriser l'émergence de réglementations plus pragmatiques qui tiendront compte des contraintes des entreprises.

Contact

CESIN
115 rue Saint Dominique
756007 PARIS
Tél : 06 09 56 63 17
Site web : **https://cesin.fr/**
Ecrire : **https://cesin.fr/contact**

Cigref

Le Cigref est une association représentative des grandes entreprises et administrations publiques françaises, exclusivement utilisatrices de solutions et services numériques. Il accompagne ses membres dans leurs réflexions collectives sur les enjeux numériques contemporains. Le Cigref s'est donné pour mission de « développer la capacité de ses membres à intégrer et maîtriser le numérique ». Pour réussir cette mission, le Cigref s'appuie sur trois métiers qui font sa singularité : intelligence collective, appartenance, influence.

Au cours d'une année encore fortement marquée par les cyberattaques, le Cigref a intensifié ses travaux sur le sujet dans le cadre de son cercle Cybersécurité, piloté par Jean-Claude Laroche, Directeur des Systèmes d'Information chez Enedis, et Vice-Président du Cigref. Le Cigref appelle à un changement de paradigme de la sécurité numérique, autour de quatre piliers : cybersécurité, lutte contre la cybercriminalité et adaptation à celle-ci des moyens de police et de justice, cyberdéfense en profondeur, régulation, a minima à l'échelle européenne, de la sécurité par conception et la sécurité d'exploitation, des produits et services numériques, sur tout leur cycle de vie.

Le Cigref échange avec l'écosystème numérique et les pouvoirs publics pour avancer collectivement sur ce changement de paradigme. À ce titre, le Cigref a organisé en 2021 plusieurs événements dont une journée avec le Forum International de la Cybersécurité (FIC) virtuel, le 3 juin 2021, sur le thème « Régulation de l'espace numérique : la défiance va-t-elle l'emporter ? » et un webinaire intitulé « Sécurité numérique : changer de paradigme », en collaboration avec numeum, et disponible en replay. Par ailleurs, dans le cadre de l'Appel de Paris, le Cigref co-pilote un groupe de travail international sur les enjeux de sécurisation de la chaîne d'approvisionnement de l'industrie du numérique.

Contact

Cigref
21 avenue de Messine
75008 PARIS
Tel : +33 1 56 59 70 00
Email : **cigref@cigref.fr**
Site web : **https://www.cigref.fr**

Clusif

Créé en 1992, mais déjà association de fait depuis 1982, le Clusif est l'une des plus anciennes associations françaises consacrées à la sécurité des systèmes d'information. Son objectif est de favoriser les échanges d'idées et de retours d'expérience au travers de groupes et d'espaces de travail, de publications et de conférences thématiques, sur des sujets liés au risque et à la sécurité des systèmes d'information.

Basé à Paris, le Clusif est également présent en région à travers des clubs locaux (les CLUSIR) et à l'international à travers les CLUSI (Belgique, Italie, Luxembourg, Suisse, Canada, etc.).

Le Clusif accueille en parfaite équité offreurs de solutions et utilisateurs et favorise, par ses travaux, la mise en commun des expériences, les échanges d'idées et le transfert de compétences. Les travaux du Clusif donnent régulièrement lieu à des publications de type recommandations, méthodologies ou état de l'art. L'association est d'ailleurs bien connue pour sa méthode d'analyse des risques MEHARI, conçue en 1989 et régulièrement mise à jour depuis.

Comment le Clusif aide les entreprises françaises et les administrations.

• **Information :** Le Clusif publie régulièrement, sur son site, des analyses, des recommandations et des méthodologies utiles, qui pourront servir l'entreprise dans l'élaboration et le suivi de sa stratégie de sécurité numérique. Le panorama annuel de la cybercriminalité ou l'étude statistique MIPS (Menaces Informatiques et Pratiques de sécurité) sont deux exemples de publications particulièrement utiles.

• **Rencontres :** Le Clusif permet le brassage des expériences et les rencontres entre offreurs et utilisateurs, au sein de groupes de travail dédiés (pour les membres) ou à l'occasion d'événements publics. Espace RSSI, espace de travail dédié uniquement aux RSSI, sans sponsors et commerciaux, favorise quant à lui l'échange de savoir-faire et de retours d'expériences en toute confidentialité.

• **Influence :** Le Clusif est membre à l'AFNOR du Comité Stratégique Information et communication numérique et de la CN 27 SSI qui s'occupe des travaux de normalisation dans le domaine de la sécurité informatique, membre Utilisateurs du GIP ACYMA (cybermalveillance.gouv.fr). De par sa large représentativité dans le secteur SSI, il est régulièrement consulté par les organismes institutionnels pour recueillir l'avis de la profession que ce soit du côté prestataire ou RSSI.

Contact

Clusif
11 rue de Mogador
75009 Paris
Tél : 01 53 25 08 80
Site web : **https://clusif.fr/**
Ecrire : **clusif@clusif.fr**

CNIL

La Commission Nationale de l'Informatique et des Libertés est l'autorité nationale en charge de la protection des données personnelles. Elle a été créée en 1978 par la loi Informatique et Libertés avec le statut d'autorité administrative indépendante.

Si son périmètre ne se limite pas aux technologies de l'information, le numérique occupe bien entendu une place prépondérante dans son activité.

Son action est double : elle accompagne d'une part les entreprises afin de les aider à se mettre en conformité avec la législation sur la protection des données personnelles, et elle aide d'autre part les particuliers à maîtriser leurs données personnelles et exercer leurs droits.

Enfin, en tant que régulateur, elle est amenée à enquêter et sanctionner les entreprises qui ne respecteraient pas la réglementation sur la protection des données personnelles.

Dans le domaine du numérique, la CNIL s'attache notamment aux listes et fichiers nominatifs (clients, prospects) et la nature des informations qu'ils contiennent (coordonnées, commentaires, préférences religieuses, politiques ou sexuelles, notamment). Elle s'assure du bon respect de la réglementation concernant la collecte de ces informations (consentement du sujet), de la finalité du traitement et de la conservation (ou destruction...) des fichiers.

Après l'entrée en vigueur du règlement européen sur la protection des données personnelles (RGPD), la CNIL, outre le contrôle, aide les entreprises à mettre en application les nouvelles obligations introduites par le règlement.

Comment la CNIL aide les entreprises françaises

• ***Information et conseil :*** La CNIL offre de très nombreuses publications destinées aux entreprises, afin de les aider à se mettre en conformité avec la législation sur la protection des données personnelles. Enfin, la CNIL dispose d'une ligne de support téléphonique dédiée aux entreprises.

• ***Outils :*** La CNIL propose des outils, des packs de sensibilisation ou des formulaires d'autoévaluation destinés à aider l'entreprise à structurer sa fonction de protection des données à caractère personnel (fiche de poste du Data Protection Officer, formulaires divers...)

• ***Certification :*** La CNIL peut attribuer une certification à des produits ou des services (des "procédures") et à des organismes. Elle peut attribuer également une certification de compétences aux DPO (non obligatoire pour exercer sa fonction).

Contact

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS
3 Place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
Tél : 01 53 73 22 22

CNIL.

Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace sur le territoire français. Ses publics sont les particuliers, les entreprises (hors OIV et OSE) et les collectivités territoriales. Le dispositif est piloté par une instance de coordination, le Groupement d'intérêt public (GIP) ACYMA, composé d'une cinquantaine de membres issus du secteur public, du privé et du domaine associatif, et qui contribuent chacun à sa mission d'intérêt général. Cybermalveillance.gouv.fr référence sur sa plateforme des professionnels en sécurité numérique, répartis sur tout le territoire français, pour venir en aide aux victimes.

Cybermalveillance.gouv.fr en quelques chiffres :

- **plus de 300 000 victimes assistées depuis la création du dispositif (fin 2017)**
- **46 principaux types de menaces traités**
- **1150 prestataires de services référencés sur l'ensemble du territoire**
- **53 entités publics et privés membres du dispositif, unis pour lutter contre la cybermalveillance**

Le label ExpertCyber :

Depuis février 2021, le dispositif propose aux professionnels un accompagnement adapté par des prestataires de confiance assurant des prestations d'installation, de maintenance et d'assistance en cas d'incident. Au travers d'un parcours de sécurisation en ligne directement accessible sur la plateforme Cybermalveillance.gouv.fr, les entreprises, collectivités et associations peuvent être mises en relation avec un prestataire labellisé dans le cadre d'une demande d'installation ou de maintenance, bénéficiant ainsi d'une expertise vérifiée par l'AFNOR couvrant les domaines suivants :

- les systèmes d'informations professionnels (informatique, logiciels bureautiques, messageries, serveurs…) ;
- la téléphonie (serveurs téléphoniques professionnels) ;
- les sites Internet (administration et protection).

Plus d'informations : **www.expertcyber.fr**

Contact

Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Email : **communication@cybermalveillance.gouv.fr**
Site web : **www.cybermalveillance.gouv.fr**
Twitter et Facebook : **@cybervictimes**
Youtube : **Cybermalveillance-gouv-fr**
LinkedIn : **LINKEDIN.COM/COMPANY/CYBERMALVEILLANCEGOUVFR**
Dailymotion : **DAILYMOTION.COM/CYBERMALVEILLANCE**

Hexatrust

HEXATRUST, le groupement des champions français et européens de la cybersécurité et du cloud de confiance.

Les sociétés membres HEXATRUST, sont des startup, PME & ETI, éditeurs de logiciels, fournisseurs de solutions, sociétés de services, à la pointe de la technologie et de l'innovation, pépites françaises de la cybersécurité et du cloud de confiance.

Les sociétés HEXATRUST répondent toutes à des exigences techniques de maturité, sont reconnues en Europe et à l'international par les plus grandes organisations et s'inscrivent dans des logiques de certifications, de labellisations et de souveraineté.

Le catalogue HEXATRUST offre un panorama complet des produits innovants et développés par plus de 65 entreprises du groupement.

Le catalogue de solutions HEXATRUST est « one-stop-shop » pour les clients, il couvre l'ensemble des domaines de la cybersécurité et du cloud de confiance pour répondre aux grands enjeux de conformité réglementaire, de protection contre les cybermenaces et d'accompagnement dans les grands projets de transformation numérique.

Engagées, les entreprises d'HEXATRUST œuvrent ensemble pour promouvoir et construire la filière française de cybersécurité et Cloud de Confiance au sein du Comité Stratégique de Filière « Industrie de Sécurité ».

Dynamiques, elles contribuent au rayonnement numérique français, s'exportent et ambitionnent de devenir des leadeurs Européens.

Chaque année, retrouvez les sociétés d'HEXATRUST sur le pavillon du FIC, sur l'espace HEXATRUST aux ASSISES de Monaco et lors de l'Université d'Eté d'HEXATRUST, qui est l'évènement de la rentrée pour les professionnels de la cybersécurité et du cloud de confiance, la première semaine de septembre.

Contact

HEXATRUST Chez WALLIX
250 bis rue du faubourg Saint Honoré, 75008 Paris

Email : **contact@hexatrust.com**
Twitter : **@hexatrust**
#UEHT #LesExpertsMonaco
Site web : **http://www.hexatrust.com/**

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Numeum

Numeum est le premier syndicat professionnel des entreprises du numérique en France. Il regroupe les entreprises de services du numérique (ESN), les éditeurs de logiciels, les plateformes et les sociétés de conseil en technologies en France. Numeum représente plus de 2 300 entreprises qui réalisent 85 % du chiffre d'affaires total du secteur en France (soit plus de 56 Md€ de chiffre d'affaires, 510 000 employés). Numeum, né de la fusion entre Syntec Numérique et TECH IN France, est présidé par Godefroy de Bentzmann et Pierre-Marie Lehucher depuis sa création en juin 2021. Notre ambition fondatrice est d'agir au service d'un numérique responsable pour les entreprises, la société, l'humain et la planète. L'engagement de numeum repose sur quatre axes : la défense des intérêts de ses membres, l'incarnation de la France numérique en Europe, l'animation de l'écosystème numérique pour favoriser les synergies et l'innovation, et le renforcement du service à toutes les entreprises du numérique. La généralisation et la démocratisation de la formation au numérique pour les organisations privées et publiques comme pour les citoyens demeurent les leviers principaux du syndicat pour parvenir à ses objectifs.

La cybersécurité est au cœur des préoccupations de Numeum qui a créé en 2015 une Commission Cybersécurité réunissant une centaine d'entreprises autour d'objectifs communs.

Les axes principaux d'actions de cette Commission sont :

- Favoriser les échanges et renforcer la place de Numeum au sein de l'écosystème en tant qu'acteur de la cybersécurité,
- Rendre attractive la filière cybersécurité pour attirer les talents,
- Informer et sensibiliser les utilisateurs
- Faire connaître les solutions de cybersécurité.

Contact

Numeum
148 Boulevard Haussmann,
75008 Paris
Tel : +33 (0)1 44 30 49 70
Email : **contact@numeum.fr**
Site web : **www.numeum.fr**

Cybersécurité :
RESTEZ INFORMÉ

L'actualité quotidienne
News, avis d'experts, témoignages, livres blancs, etc.
https://www.solutions-numeriques.com/securite/

La newsletter
Chaque lundi, comme 40 000 professionnels et décideurs, recevez la synthèse des informations.
C'est gratuit, inscrivez vous :
https://www.solutions-numeriques.com/securite/inscription/

L'annuaire : Guide papier et en ligne
Trouvez l'éditeur de solution, le prestataire de services qu'il vous faut.
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

033CRI

Prenez le contrôle des cyber-incidents complexes

Renforcez la puissance de votre équipe cybersécurité avec des technologies de pointe enrichies par des renseignements de haut niveau sur les menaces, des connaissances et les conseils des meilleurs experts.

kaspersky.fr/enterprise-security

kaspersky BRING ON THE FUTURE

© 2021 AO Kaspersky Lab. Bring on the future : Bienvenue dans le futur.