HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Catalogue de solutions et services de confiance

Édition 2024/2025

pour l'application de la directive NIS 2

L'association en quelques mots

Hexatrust est une association loi 1901 qui regroupe et fédère les champions français et européens de la **cybersécurité**, du **cloud de confiance** & du **digital workplace**.

Les sociétés membres d'Hexatrust sont reconnues pour leur **complémentarité** et la **qualité** de leurs produits et services : éditeurs de solutions de cybersécurité, éditeurs et fournisseurs de Cloud de confiance (SaaS, PaaS, IaaS), utilisateurs, sociétés privées, établissement publics, intégrateurs, hébergeurs, avocats, courtiers d'assurance, établissements de financement...

Hexatrust en chiffres

123
sociétés adhérentes
au 1er janvier 2024

2,3
milliards d'€ de CA cumulés

1000+
inscrits aux Universités d'été 2023

+30%
de croissance en 2023

L'union fait la force

Unis pour construire ensemble une filière engagée pour un monde numérique plus sûr, résilient et protecteur des données.

L'association en quelques dates

2013
Naissance d'Hexatrust

Douze entreprises s'unissent pour fonder le Groupement HEXATRUST afin de proposer une gamme de produits et de services cohérente, complète et souveraine de cybersécurité et de confiance numérique.

2015
1ère Université d'été

L'occasion de débattre sur les enjeux et perspectives de la cybersécurité en Europe. Tous les acteurs clefs du domaine sont réunis pour des témoignages exclusifs et des débats organisés en tables rondes thématiques.

2017
Fusion x Cloud Confidence

Le 18 décembre 2017, les membres adhérents d'Hexatrust et de Cloud Confidence ont voté la fusion entre les deux associations dans le but de valoriser l'expertise et l'excellence des entreprises membres et de promouvoir une relation transparente et de confiance entre professionnels, utilisateurs, citoyens et pouvoirs publics.

2018
Partenaire principal du FIC

Hexatrust a été choisi comme partenaire principal du Forum International de la Cybersécurité (FIC). Cette collaboration inédite renforce les relations entre les entreprises du groupement et l'un des événements phares de la scène européenne en matière de cybersécurité.

2021
Accélérateur Hexatrust

ACCÉLÉRATEUR

Hexatrust lance son programme Accélérateur. Depuis, trois pépites dans le domaine de la cybersécurité sont accompagnées chaque année par l'association.

Sommaire

Éditos

Marina Ferrari

Secrétaire d'État chargée du Numérique

En 2016, la directive NIS faisait entrer les grands acteurs de secteurs dits stratégiques dans l'ère de la cyberrésilience. En 2024, avec la directive NIS2, ce sont plusieurs milliers d'entités qui basculent à leur tour dans l'ère de la cybersécurité pour tous.

Face à des cyberattaques qui s'intensifient et touchent un nombre toujours plus grand d'acteurs, la directive NIS2 élargit ses objectifs et son périmètre d'application, marquant ainsi un véritable passage à l'échelle. Au niveau national, plusieurs milliers d'entreprises, d'administrations centrales et de collectivités territoriales, appartenant à plus de 18 secteurs, seront mobilisées dans ce nouvel effort d'adaptation et de modernisation dont l'objectif reste inchangé : élever le niveau global de sécurité numérique en France en permettant aux entités concernées de mieux se protéger face à la menace, sur tous les maillons de la chaîne de valeur.

Pour ce faire, ces dernières pourront compter sur l'accompagnement de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui est d'ores-et-déjà mobilisée pour préparer la transposition française de la directive, dans une démarche de co-construction avec les futures entités régulées. Leurs contraintes financières, techniques et humaines seront également prises en compte pour garantir la pertinence et la soutenabilité des nouvelles exigences réglementaires. La mise en œuvre opérationnelle de NIS2 sera ainsi simplifiée au maximum et un délai de mise en conformité sera consenti à compter de l'entrée en vigueur du texte.

In fine, l'effort collectif sans précédent occasionné par NIS2 doit provoquer un changement de paradigme face à la menace cyber. La France et les autres États membres de l'Union européenne s'engagent aujourd'hui dans une plus intense coopération pour mettre au ban les groupes cybercriminels, qui ne connaissent pas de frontières, et renforcer notre souveraineté numérique européenne.

Dans le même temps, nous comptons sur l'écosystème cyber français pour répondre présent. NIS2 est l'occasion d'adapter les offres, afin qu'elles correspondent aux besoins des entités concernées par la réglementation, et de favoriser l'interopérabilité des solutions déjà présentes sur le marché. Nos collectivités et nos entreprises, en particulier les plus petites, ont besoin de pouvoir s'appuyer sur des offres clés-en-main et facilement intégrables. Le travail réalisé par Hexatrust, qui réunit les champions français et européens de la cybersécurité, est une première étape importante sur cette voie collective, que je tiens à saluer. Ne relâchons pas nos efforts et continuons à unir nos forces pour répondre, ensemble, aux défis qui nous concernent tous.

Jean-Noël de Galzain

Président d'Hexatrust,
Vice Président du CSF
« Industries de sécurité »

Alors que la directive NIS, première du nom, avait permis depuis 2016 d'initier un changement d'état d'esprit chez les acteurs institutionnels et les organisations des secteurs sensibles dans leur approche et leur compréhension des enjeux de cybersécurité, l'entrée en vigueur à l'automne 2024 de NIS2 représente lui un tournant majeur pour le monde économique dans son intégralité.

Cette nouvelle législation obligatoire, qui pose à l'échelle européenne des normes plus rigoureuses en matière de cybersécurité, va en effet amener un large panel des secteurs d'activités et de services à renforcer leur cyber-résilience face aux menaces croissantes. Actant ainsi le passage à une approche systémique de la cybersécurité dans tout le continent.

Mais au-delà de cette norme qui pèse sur les organisations, la NIS2 est une véritable opportunité pour notre économie. En poussant à un renforcement global de la sécurité numérique, la directive répond à un risque fort directement lié à la transformation numérique rapide de notre société : celui de la progression encore plus fulgurante du risque cyber auquel notre économie est confrontée.

Les chiffres le montrent : le nombre de cyberattaques augmente de manière exponentielle ces dernières années, touchant particulièrement les ETI et les PME, ainsi que les services essentiels de notre société, mettant en danger le fonctionnement des organisations visées, et la survie des entreprises touchées. Dans ce contexte, la mise en place d'une approche globalisée et coordonnée de la cybersécurité est nécessaire pour assurer une protection efficace de l'ensemble de notre tissu économique.

Réunis au sein du groupement Hexatrust, les acteurs français de la cyber souhaitent être des partenaires incontournables et de confiance au service de l'économie nationale, et du renforcement de sa sécurité numérique. Forts de leur vitalité, leur expertise et leur capacité d'innovation, ils sont mobilisés pour accompagner nos entreprises, nos organisations, en leur offrant des solutions adaptées à leur besoin, de manière coordonnée, tout en leur permettant de répondre facilement aux nouvelles obligations mises en place par la NIS2.

C'est dans cet objectif qu'Hexatrust a construit le présent guide pour faciliter la prise de décision et l'acquisition de solutions cyber innovantes, souveraines et alignées sur les 9 objectifs fixés par la directive. Ceux qui souhaitent améliorer leur résilience et répondre aux défis posés par NIS2 y trouveront les outils pour les satisfaire.

Plus que jamais, la sécurité numérique de la France doit être une priorité. Elle nous permettra de rester maître de notre destin numérique, de contrôler nos données et nos infrastructures critiques, devenus des maillons essentiels pour le bon fonctionnement du pays et de nos organisations. La NIS2 est un pas crucial dans cette direction. Hexatrust et ses membres sont résolument engagés à soutenir cette démarche aux côtés des utilisateurs de manière durable et responsable.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Avec NIS2, la résilience est plus cyber que jamais

Huit ans après la première directive NIS (Network and Information Security), l'Union européenne adapte son arsenal réglementaire à l'augmentation des cybermenaces. Adoptée en décembre 2022, la directive NIS2 est ambitieuse. Elle vient harmoniser les exigences en matière de cybersécurité à l'échelle européenne, élargir considérablement le périmètre des secteurs concernés et introduire de nouvelles obligations et sanctions. Évolution majeure de la législation en matière de cybersécurité, NIS2 renforcera la résilience de toutes les organisations et de l'Europe dans son ensemble. Ce dossier synthétique est à mettre entre toutes les mains, aussi bien des membres du Comex que des RSSI, des responsables « métiers », que des directeurs des services informatiques.

En 2016, la directive NIS posait les premières pierres d'une réglementation européenne commune en matière de cybersécurité. À l'époque, ces mesures s'imposaient face à la transformation numérique de notre société. Dans un contexte de marché unique où les frontières physiques sont abolies, les pays membres de l'Union européenne étaient plus que jamais exposés aux cybermenaces.

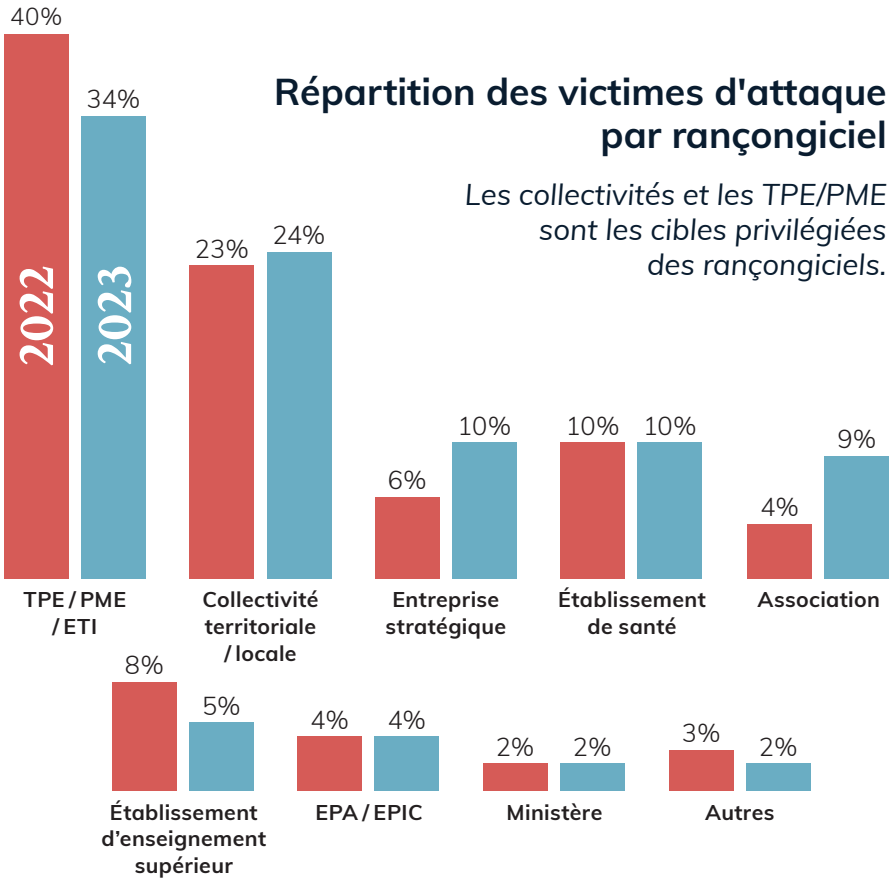
Pour autant, cette première dynamique de réglementation a rapidement trouvé ses limites :

- Un champ d'application circonscrit aux Opérateurs d'Importance Vitale, sans harmonisation des secteurs ;
- Un manque de détails dans les mesures techniques et organisationnelles ;
- Une exigence faible et inégale du niveau de résilience selon les secteurs ;
- Un pouvoir de sanction limité.

Dans le même temps, le niveau de menace augmente. Dans son Panorama de la cybermenace 2023, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) souligne que « *le niveau de la menace informatique continue d'augmenter, dans un contexte marqué par de nouvelles tensions géopolitiques et la tenue d'événements internationaux sur le sol français* ». Elle précise que « *la cybercriminalité représente toujours une menace importante pour le secteur public et les entités particulièrement sensibles aux interruptions de service, notamment dans les secteurs de la santé et de l'énergie* », sans compter les multiples PME et ETI, cibles d'attaques par rançongiciels.

Répartition des victimes d'attaque par rançongiciel

Les collectivités et les TPE/PME sont les cibles privilégiées des rançongiciels.



David Lisnard

Président

AMF
ASSOCIATION DES MAIRES DE FRANCE ET DES PRÉSIDENTS D'INTERCOMMUNALITÉ

La menace cyber est devenue, année après année, une inquiétante réalité qui pèse sur les communes et intercommunalités de France et dont les conséquences sont particulièrement lourdes pour les administrations et les administrés. La directive européenne NIS2, qui sera transposée en droit français en fin d'année 2024, doit nous conduire à atteindre une immunité cybernationale. Celle-ci ne sera atteinte que si les collectivités y sont pleinement associées, en considérant les moyens dont elles disposent. C'est pourquoi l'AMF est engagée, avec le gouvernement et les industriels, à trouver un juste équilibre entre l'ambition nécessaire d'une meilleure cybersécurité des communes, un investissement financier raisonnable et une offre industrielle souveraine. C'est un défi que nous devons relever rapidement et l'AMF y participe activement.

Jean-Paul Bonnet

Président de la commission « Cybersécurité et Protection de l'information »

CDSE
CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

La directive NIS2 témoigne de la volonté de l'Union européenne de passer d'une logique de protection à une logique de résilience qui implique de recourir à une pensée systémique des risques et des acteurs impliqués (partenaires, fournisseurs et prestataires). Dans ce cadre, le maintien de relations public-privé de haut niveau malgré le nombre d'entités concernées est un enjeu essentiel. Ces nouvelles exigences, couplées à celles de la directive REC dans le domaine physique, vont nécessiter des efforts en matière de réalisation des cartographies des risques et des programmes de mitigation, le renforcement des procédures de due diligence des partenaires et l'organisation de phases de test de la capacité des systèmes d'information à tenir face à des attaques. Chacune de ces exigences emporte des logiques capacitaires nouvelles qui vont nécessiter le recours à de nouvelles solutions, idéalement souveraines.

Les secteurs concernés

SECTEURS HAUTEMENT CRITIQUES

- Énergie
- Transports
- Secteur bancaire
- Infrastructures des marchés financiers
- Santé
- Eau potable
- Eaux usées
- Infrastructure numérique
- Gestion des services TIC (interentreprises)
- Administration publique
- Espace

AUTRES SECTEURS CRITIQUES

- Services postaux et d'expédition
- Gestion des déchets
- Fabrication, production et distribution de produits chimiques
- Production, transformation et distribution des denrées alimentaires
- Fabrication, industrie
- Fournisseurs numériques
- Recherche

Chaîne logistique, tous concernés ?

NIS2, dans son article 21.2.d, adresse « *la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs* ». En d'autres termes, les EE et les EI auront à sécuriser leurs chaînes de sous-traitance, chaînes couvrant d'ailleurs potentiellement des outils SaaS. Ces mesures pourraient bien se traduire sous forme contractuelle. Un sous-traitant qui fournit des services ou des composants à une entité essentielle ou importante devra sans doute adapter ses mesures de sécurité aux exigences de son client soumis à NIS2. Tout prestataire ou sous-traitant est donc virtuellement concerné par NIS2, quoique indirectement.

LES ENTITÉS ESSENTIELLES ET IMPORTANTES

SCHÉMATISATION SIMPLIFIÉE DE LA RÈGLE DE BASE

TAILLE ENTITE	NOMBRE D'EMPLOYÉS	CHIFFRE D'AFFAIRES (MILLIONS D'EUROS)	BILAN ANNUEL (MILLIONS D'EUROS)	SECTEURS HAUTEMENT CRITIQUES	AUTRES SECTEURS CRITIQUES
Intermédiaire et grande	X ≥ 250	Y ≥ 50	Z ≥ 43	Entites essentielles	Entites importantes
Moyenne	50 ≥ X ≥ 250	10 ≥ Y > 50	10 ≥ Z > 43	Entites importantes	Entites importantes
Micro et petite	X<50	Y <10	Z<10	Non concernées	Non concernées

Mylène Jarossay
Présidente
CESIN

L'ANSSI a mené une consultation sur NIS2 à laquelle le CESIN a participé et apporté ses commentaires. Le Club a mené des enquêtes et débats internes qui ont suscité une forte participation de ses membres, montrant la mobilisation de la communauté sur ce sujet. Avec plus de 40 % de potentiels EE ou EI, et 33 % d'indécis, NIS2 obtient un score élevé de prétendants. Les membres du CESIN ont exprimé leur souhait d'une clarification des critères d'éligibilité et des interactions avec l'opérateur qui soient fondées sur le pragmatisme et l'efficacité opérationnelle, avec des services qui prennent en compte les nouvelles architectures des SI. Les mesures proposées sont jugées au bon niveau d'exigence, parfois insuffisantes dans le domaine de la détection, et certaines mesures mériteraient des éclaircissements. La majorité des membres pressentent que la mise en œuvre sera plutôt difficile, mais comprennent l'intérêt de ces objectifs et le cap fixé pour une montée générale en maturité des entreprises.

Henri d'Agrain
Délégué Général
Cigref
RÉUSSIR
LE NUMÉRIQUE

La directive NIS2 est une vraie révolution dans les affaires de sécurité numérique en Europe, et une opportunité pour renforcer la résilience de la société française et de son économie. Sans trop de doute, tous les adhérents du Cigref seront concernés. Nous sommes donc attentifs à la façon dont elle sera transposée en droit français, et notamment au principe de proportionnalité, c'est-à-dire à la cohérence des exigences de sécurité avec la taille des entités concernées et la nature de leur activité. Il convient en effet d'éviter que des obligations excessives ne deviennent un fardeau qui engage leur compétitivité et leur performance. C'est dans cet esprit que nous collaborons avec l'ANSSI. Nous appelons par ailleurs la Commission à être attentive au risque de concurrence législative entre les États membres de l'UE, afin de prévenir l'apparition de « pavillons de complaisance » cyber, comme ce fut le cas, par exemple, avec le RGPD.

C'est ici qu'intervient la directive EU 2022/2555, ou NIS2, publiée le 27 décembre 2022 au Journal Officiel de l'Union européenne, que chaque État membre doit transposer en droit national d'ici au 18 octobre 2024.

NIS2 est un texte ambitieux. La directive entend renforcer la résilience des États-membres, de leurs collectivités, de leurs administrations, de leurs infrastructures critiques et de leur tissu économique face aux cybermenaces. Pour ce faire, elle étend le périmètre de NIS à un plus large éventail d'entités et harmonise les pratiques de cybersécurité à l'échelle de l'Union européenne. Par sa transposition au niveau national, NIS2 impose des exigences en matière de gestion des risques, de gouvernance de la cybersécurité et de préparation contre les cyberattaques. C'est grâce à ces exigences, et à leur respect, que les entités concernées pourront gagner en maturité sur le plan de la sécurité de leurs systèmes d'information et être prêtes à faire face aux défis cyber du numérique.

Quels sont les principales nouveautés de NIS2 ?

- **Étendre le champ des entités concernées :** NIS2 étend ainsi le champ des entités concernées. Désormais les secteurs adressés passeront de 10 à 18 et les entités régulées seront divisées entre « entités essentielles » et « entités importantes » selon leur taille et/ou leur chiffre d'affaires.

- **Adopter une approche plus unifiée de la cybersécurité :** le niveau des obligations imposées aux différentes entités concernées est relevé et les objectifs à atteindre sont plus détaillés à l'échelle européenne afin d'assurer un plus grand niveau d'harmonisation sur le marché unique, ainsi qu'une plus grande coopération sur le risque cyber.

Un régime de sanctions sévère

Responsabilité du dirigeant engagée en cas de manquement :

Pénale ou civile*

**en fonction de la transposition de la directive en droit national*

Entité essentielle :

Amende administrative

10 000 000 € ou égale à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent

Entité importante :

Amende administrative

7 000 000 € ou égale à 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent

- **Une obligation de notification et d'information :** à l'instar du RGPD et de la notification des violations de données à la Cnil, les entités concernées par NIS2 devront signaler tout incident de cybersécurité majeur à l'autorité nationale compétente.

- **Responsabiliser les directions faces aux enjeux cyber :** le régime de sanction administrative sera largement renforcé et pourra se fonder sur un pourcentage du chiffre d'affaires mondial de l'entité concernée, à l'image de ce qui est prévu dans le RGPD. Surtout, NIS2 introduit la possibilité pour les États membres d'instaurer un régime de responsabilité pénale pour les dirigeants des entités.

Quelles mesures nécessaires ?

Si l'ANSSI a annoncé le 27 février 2024 avoir une première ébauche du texte de transposition de la directive européenne en droit français, il est encore trop tôt pour fournir une liste d'exigences applicables.

Néanmoins, on peut d'ores et déjà déduire de la teneur des articles les mesures de cybersécurité qu'il sera nécessaire de mettre en œuvre. Celles-ci sont détaillées dans les articles 20 à 21.2.j de la directive EU 2022/2555. NIS2 aborde des mesures aussi bien organisationnelles que techniques, couvrant un champ très large allant de la gouvernance de la gestion du risque cyber au chiffrement en passant par la continuité d'activité.

Vous trouverez ***p. 16 à 19*** une description plus complète de ces articles et des prestations et solutions de cybersécurité correspondantes.

Loïc Guézo
Vice-Président
CLUSIF

La transposition imminente de NIS2 va exiger une adaptation rapide des législations nationales. Pour la France, cela appelle une collaboration étroite entre l'État, les entreprises et les organisations comme le Clusif. C'est une condition nécessaire pour garantir une transition effective et une amélioration durable de la posture de cybersécurité du pays. Cette nouvelle étape induit une responsabilisation des comex, car elle peut impliquer des ajustements dans les opérations, des investissements conséquents dans les infrastructures et les compétences. Cela peut être intimidant pour certains, surtout s'ils sont déjà confrontés à des contraintes budgétaires ou à des ressources limitées. Pour d'autres déjà très réglementés, cela sera plutôt une poursuite de la feuille de route existante.

Antoine Trillard
Président
coTer numérique

Au moment où j'écris cette citation fin février, la directive européenne NIS2 n'est toujours pas transposée par l'ANSSI pour la France. L'ANSSI a annoncé intégrer les associations à la réflexion de cette transposition ; à ce jour, le coTer numérique n'a pas été saisi. Si le périmètre des collectivités n'est pas connu, il semble que les collectivités de plus de 50 000 habitants seront concernées en tant qu'entités importantes et non essentielles et feront l'objet d'un mécanisme de proportionnalité prévu par la directive. Certaines exigences seront d'application directe et d'autres devraient être soumises à un délai de mise en conformité. Je compte sur le pragmatisme de l'ANSSI, à l'instar de leur très réussi plan de relance, pour définir des exigences adaptées et proportionnées aux enjeux des collectivités et au regard de leurs ressources. Une certitude, les DSI, RSSI et élus de nos collectivités n'ont pas attendu cette directive ; ils sont déjà très impliqués et sensibilisés à ces menaces.

Par où commencer ?

La directive NIS2 peut sembler un défi parce qu'elle mobilise des investissements, des ressources et des compétences, le tout dans un délai contraint. Cependant, NIS2 représente l'opportunité, pour les EE et EI mais aussi pour toute organisation dont l'activité opère sa transformation numérique, de rehausser son niveau de sécurité informatique et de gagner en résilience face aux cybermenaces.

La tâche n'est d'ailleurs pas aussi insurmontable qu'il n'y paraît et il est possible dès aujourd'hui de s'y préparer. Tout d'abord en déterminant si vous êtes concernés par NIS2, sur la base des critères mentionnés plus haut, ou si l'un de vos clients risque d'exiger de vous que vous vous mettiez à niveau. Cette première étape effectuée, nous ne pouvons que vous conseiller de cartographier l'ensemble des « métiers » de votre organisation, d'évaluer leur criticité et l'impact en cas de paralysie et d'identifier leurs besoins particuliers en matière de cybersécurité. Cette cartographie est une démarche nécessaire puisqu'elle vous permettra d'identifier les composants de vos systèmes d'information et de prioriser les actions à mener. Une cartographie des risques s'avèrera également utile. Non seulement NIS2 l'impose, mais détecter les principales menaces en les corrélant avec les activités de votre entité facilitera la démarche de priorisation des besoins.

Il ne s'agit finalement que de faire l'inventaire de l'existant. Ce faisant, vous serez en mesure de développer une connaissance approfondie de votre système d'information et de sa gouvernance, de sorte à mieux comprendre les dépendances, les risques voire les interconnexions non maîtrisées avec d'autres systèmes d'informations ou outils, autrement appelées « Shadow IT ». Profitez-en pour évaluer vos

Combien ça coûte ?

Une question ne manquera pas d'émerger quand les travaux de mise en conformité commenceront : combien ça va nous coûter ? Pour citer la FAQ de l'ANSSI sur le sujet, « *cette question est complexe car il y a autant de réponses possibles que d'entités* ». Il ne sera possible d'évaluer l'impact financier de NIS2 pour une organisation qu'après la réalisation des cartographies des systèmes d'information et des risques, l'évaluation de la maturité cyber de l'entité et l'établissement d'une feuille de route. Notons néanmoins que l'ANSSI n'exclut pas un mécanisme de présomption de conformité lorsque l'entité a recours à des prestations qualifiées par l'ANSSI (Prestataires d'Audit de la Sécurité des Systèmes d'Information, Prestataires de Détection d'Incidents de Sécurité, Prestataires de Réponse aux Incidents de Sécurité, etc.).

capacités de détection des anomalies et de traitement des alertes. Votre résilience, à travers l'existence ou non de plan de continuité/reprise d'activité, de sauvegardes hors site et de mesures de réponses aux incidents, doit également faire l'objet d'une attention particulière. Vous pourrez ainsi évaluer le niveau de maturité en cybersécurité de votre organisation et, sur cette base, établir une feuille de route. En fonction de ce niveau de maturité, il vous sera aisé de trouver les ressources correspondant à vos besoins, notamment auprès de l'ANSSI et de Cybermalveillance.gouv, qui ont mis au point différents guides de bonnes pratiques adaptés à votre situation.

Une recommandation indispensable : la première action concrète à mettre en place consiste à sensibiliser la direction générale et les directions « métiers » aux enjeux de la cybersécurité et de NIS2 en particulier, notamment les sanctions prévues par la directive en cas de manquements. C'est à travers cette démarche que vous pourrez changer les comportements et amener une prise de conscience sur les risques, simplifiant vos futures tâches de mise en conformité à la directive.

Claire Laurent

Pilote de la commission numérique

Gifen

Le GIFEN (Groupement des industriels français de l'énergie nucléaire) a été consulté par l'ANSSI dans le cadre de la transposition de la directive NIS2 en droit français. Cette directive doit permettre de renforcer la résilience des entreprises industrielles face au risque cyber, et notamment celles de la filière nucléaire qui sont de plus en plus interconnectées avec l'utilisation des nouvelles technologies. La directive NIS1 ne concernaient que quelques opérateurs de services essentiels. La directive NIS2 embarque plus largement la filière avec notamment l'ensemble de fabricants d'équipements. Selon une première estimation, 40 fois plus d'acteurs de la filière seront concernés par NIS2 par rapport à NIS1. Au sein d'une filière nucléaire constituée majoritairement de PME, répondre aux attentes de NIS2 est donc un enjeu majeur pour gagner en maturité et être armés faces aux menaces potentielles.

Eric Freyssinet

Président

OSSIR

La directive européenne NIS2 va accélérer le déploiement des bonnes pratiques de sécurité numérique. Elle se traduit ainsi par des engagements plus forts des organisations, y compris de leurs dirigeants. Aussi, la communauté de l'OSSIR, composée de nombreux experts, compte bien appuyer sa mise en œuvre. Nos attentes portent notamment sur :
. des guides et formations pour se préparer de manière autonome ;
. des outils permettant de suivre simplement le déploiement des exigences ;
. la mise en place de nouvelles certifications, y compris des sous-traitants ;
. et en particulier pour les organisations entrant dans un périmètre d'exigences renforcé par NIS2, le recrutement de personnes dédiées à cette mission
La solidarité et le partage au sein de la communauté seront des éléments clés de la réussite face à ce nouveau défi.

Comment comprendre ce document ?

Dans les pages qui suivent, vous découvrirez un tableau référençant les adhérents d'Hexatrust en fonction des solutions et prestations qu'ils fournissent en lien avec les mesures de sécurité prévues par la directive NIS2.

Ce référentiel a été conçu pour faciliter l'identification des éditeurs, intégrateurs, ESN et hébergeurs les plus à même de répondre aux besoins de votre organisation en matière de cybersécurité et de conformité à NIS2.

Pour bien comprendre les pages suivantes, il est nécessaire de revenir sur les dispositions des articles 20 et 21 de la directive et ce qu'ils comprennent.

- **L'article 20** de la directive couvre principalement la gouvernance de la sécurité informatique et la responsabilité des Comex et autres organes de direction. Ceci comprend à la fois les prestations de conseil en Politique de Sécurité des Systèmes d'Information (PSSI) et les outils de Systèmes de management de la sécurité informatique (SMSI).

NIS2
Article 20 : Gouvernance

1. Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 21, supervisent sa mise en œuvre et puissent être tenus responsables de la violation dudit article par ces entités.

L'application du présent paragraphe est sans préjudice du droit national en ce qui concerne les règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

2. Les États membres veillent à ce que les membres des organes de direction des entités essentielles et importantes soient tenus de suivre une formation et ils encouragent les entités essentielles et importantes à offrir régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

NIS2
Article 21 : Mesures de gestion des risques en matière de cybersécurité

1. Les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

Les mesures visées au premier alinéa garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

2. Les mesures visées au paragraphe 1 sont fondées sur une approche « tous risques » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles comprennent au moins:

a) les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;

b) la gestion des incidents;

c) la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;

d la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;

e) la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités;

f) des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;

g) les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité;

h)des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;

i) la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;

j) l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

• **L'article 21.2** intègre la maîtrise des accès physiques aux locaux, serveurs et autres matériels informatiques.

• **L'article 21.2.a** traite, à l'instar de l'article 20, de sujets de gouvernance et de mise en œuvre d'une politique de sécurité des systèmes d'information (PSSI), comprenant notamment des mesures de gestion et d'analyse des risques.

• **L'article 21.2.b** est dédié à la gestion des incidents. Il regroupe toutes les solutions de détection et de réponse aux incidents de sécurité, les systèmes automatisant le traitement des données de sécurité et les mesures de remédiation, mais aussi les sujets de préparation, de simulation et de gestion de crise ainsi que le forensic.

• **L'article 21.2.c** traite de continuité/reprise des activités. On y trouve sans surprise les solutions de sauvegarde et de récupération, de stockage sécurisé ainsi que les conseils en PRA/PCA (plan de reprise/continuité d'activités).

• **L'article 21.2.d** porte sur « *la sécurité de la chaîne d'approvisionnement* ». Il comprend aussi bien des mesures techniques, telles que la cartographie des interconnexions du système d'information à des services et applications tierces ou encore la sécurité de la chaîne logicielle, qu'un aspect juridique relatif aux relations contractuelles entre l'entité et ses partenaires.

• **L'article 21.2.e** regroupe toutes les mesures techniques nécessaires à garantir la sécurité du SI. Le périmètre est donc extrêmement large : des solutions de détection et de réponse sur les endpoints (EDR) à la gestion des vulnérabilités, en passant par les tests de configuration, la sécurisation des accès distants, la mise en place d'une architecture Zero Trust, les SIEM, et SOAR, pare-feu et gateway, le filtrage IP, la sécurité de l'Active Directory, la gestion des identités et des accès, le durcissement des postes de travail, les WAF et WAAP ou encore les analyses de surface d'exposition. La liste est loin d'être exhaustive.

• **L'article 21.2.f** vient vérifier la solidité et l'efficacité de la démarche de gestion des risques, au travers d'audits si nécessaires.

• **L'article 21.2.g** traite de la formation et de la sensibilisation de la direction de la sécurité numérique dans la gestion des ressources humaines, notamment dans l'onboarding et l'offboarding des salariés.

• **L'article 21.2.h** concerne l'utilisation de la cryptographie et du chiffrement. Il s'agit de sécuriser l'architecture de ses systèmes d'information, notamment eu égard aux accès distants. Mais cette disposition peut être également mise en lien avec les sujets de PSSI pour intégrer dans ces politiques et procédures la microsegmentation du système d'information et le recours à une architecture Zero Trust.

• **L'article 21.2.i** couvre « *la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs* », un champ particulièrement étendu couvrant aussi bien l'IAM et le PAM que de la cartographie du système d'information, la data discovery avec une forte dimension gouvernance. En résumé, ce sont toutes les mesures permettant de connaître son système d'information, ce qui s'y trouve, qui s'y trouve, qui a accès à quoi, etc.

• **L'article 21.2.j** comprend « *l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité* ».

Les 12 entrées du référentiel NIS2

Article 20 :
Gouvernance de la gestion des risques en matière de cybersécurité

Article 21.2 :
Protection de l'environnement physique des réseaux et systèmes d'information

Article 21.2.a :
Politiques d'analyse des risques et de la sécurité des systèmes d'information

Article 21.2.b :
Gestion des incidents

Article 21.2.c :
Continuité des activités

Article 21.2.d :
Sécurité de la chaîne d'approvisionnement

Article 21.2.e :
Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Article 21.2.f :
Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Article 21.2.g :
Cyberhygiène et formation à la cybersécurité

Article 21.2.h :
Cryptographie et chiffrement

Article 21.2.i :
Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Article 21.2.j :
Authentification, communications sécurisées et communication d'urgence

Comment les adhérents d'Hexatrust peuvent répondre à vos besoins de mise en conformité à NIS2

Le tableau qui suit comporte :
- selon les colonnes verticales, les dispositions des articles 20 et 21 de NIS2 sur lesquelles nous nous sommes appuyé pour créer ce référentiel ;
- selon les lignes horizontales, les sociétés offrant des solutions et/ou services en réponse aux dispositions associées.

	Art. 20	Art. 21.2	Art. 21.2.a	Art. 21.2.b	Art. 21.2.c	Art. 21.2.d	Art. 21.2.e	Art. 21.2.f	Art. 21.2.g	Art. 21.2.h	Art. 21.2.i	Art. 21.2.j
6CURE				x			x	x		x		
AISI	x		x	x	x	x	x	x	x		x	
ALGOSECURE	x		x	x	x	x	x	x	x	x	x	x
ALTOSPAM					x		x		x	x	x	
ANTEMETA					x		x					
ARCAD SOFTWARE							x	x				
ASTRAN					x					x		
ATEMPO		x			x			x				x
AUCAE				x	x				x			
AVANT DE CLIQUER									x			
AXIANS	x		x	x	x	x	x	x	x	x	x	
BELLEDONNE COMMUNICATION							x					x
BLUEMIND					x							x
BOARD OF CYBER			x			x	x				x	
BONJOURCYBER	x		x	x	x	x	x	x	x		x	
BRAIN NETWORKS	x		x	x			x	x	x		x	
BRAIN SECURITY									x			
CONSCIO TECHNOLOGIES									x			
CONTINUS.IO						x	x	x				
CROWDSEC				x			x				x	
CRYPTONEXT SECURITY							x			x		x
CUSTOCY				x			x					
CYBER-DETECT			x	x		x						
CYBERIUM							x			x		
CYBERVADIS						x						
CYBERWATCH			x				x					
CYBERXPERT	x		x	x	x		x	x	x	x		
DASTRA												
DEFANTS				x				x				

	Art. 20	Art. 21.2	Art. 21.2.a	Art. 21.2.b	Art. 21.2.c	Art. 21.2.d	Art. 21.2.e	Art. 21.2.f	Art. 21.2.g	Art. 21.2.h	Art. 21.2.i	Art. 21.2.j
DELETEC	x		x	x	x		x	x	x	x	x	
DEVENSYS CYBERSECURITY	x		x	x			x	x	x			
DIGITALBERRY	x		x	x	x	x	x	x		x	x	x
DOCAPOSTE	x		x	x	x		x	x		x	x	x
EBRC	x	x	x	x	x	x	x	x	x		x	
EGERIE	x		x					x	x			
EQUISIGN					x					x	x	x
ERCOM					x							x
EVERTRUST SAS			x				x				x	x
EXCELSIOR SAFETY			x		x		x		x		x	
EXIPTEL SAS			x	x	x		x					
EXO PLATFORM												x
EY FRANCE	x		x	x	x	x	x	x	x	x	x	x
FAIRTRUST	x						x				x	x
FILIGRAN	x		x	x				x				
GATEWATCHER			x	x	x	x	x				x	
GLIMPS				x			x				x	
HARFANGLAB				x			x				x	
HIASECURE	x		x				x				x	x
HOLISEUM			x					x		x		
ILEX INTERNATIONAL							x				x	x
INQUEST	x		x	x	x			x	x			
INSPEERE					x							
ISE SYSTEMS	x		x	x		x	x	x	x		x	
ITRUST - GROUPE ILIAD				x	x		x				x	
JALIOS			x			x			x		x	x
JAMESPOT												x
LAGERTHA										x		x
LEVIIA					x							
LOGIN SECURITE	x	x	x	x	x	x	x	x	x	x	x	x
MAILINBLACK							x		x	x	x	
MAKE IT SAFE	x		x	x		x	x	x				
MATHIAS AVOCATS									x			
MEROX	x		x				x		x			
METSYS	x		x	x	x	x	x	x	x		x	x
MINDFLOW					x		x				x	
MOABI SOLUTIONS						x		x		x		
N-CYP				x	x	x	x					
NAMESHIELD	x		x				x	x			x	
NEOTECH ASSURANCES	x								x			
NEOTRUST	x		x	x	x	x	x	x	x		x	
NEOWAVE		x									x	x
NETEXPLORER			x	x	x						x	
NUMSPOT					x		x			x	x	x

	Art. 20	Art. 21.2	Art. 21.2.a	Art. 21.2.b	Art. 21.2.c	Art. 21.2.d	Art. 21.2.e	Art. 21.2.f	Art. 21.2.g	Art. 21.2.h	Art. 21.2.i	Art. 21.2.j
OLFEO							x		x		x	
OLIVIER WEBER AVOCAT												
OLVID					x					x		x
OODRIVE	x		x	x	x		x	x	x	x	x	x
OUTSCALE - DASSAULT SYSTEMS					x				x	x	x	
OVERSOC			x			x	x	x				
P4S										x	x	
PARSEC							x			x		x
PATROWL			x			x	x	x			x	
PRIM'X							x			x		
PRIVATE DISCUSS												x
PRIZM	x		x				x				x	
PROVENRUN						x	x					
QONTROL	x		x		x		x	x			x	
RESCO COURTAGE	x		x	x								
RETARUS							x					
REVERSENSE							x				x	
RYDER & DAVIS												
SCALAIR	x		x	x	x	x	x	x		x	x	
SCALITY					x							
SECLAB					x		x				x	x
SEELA									x			
SEKOIA.IO				x			x				x	
SMART GLOBAL GOVERNANCE	x		x	x	x	x		x	x			
SNOWPACK							x			x	x	
SOSAFE	x		x						x			
SURICATE							x				x	
SYNETIS	x	x	x	x	x	x	x	x	x		x	x
TENACY	x		x			x	x	x				
TERSEDIA	x		x	x	x	x	x	x	x	x	x	
THEGREENBOW						x	x			x		
TIXEO					x							x
TRANQUIL IT							x				x	
TRUSTBUILDER (INWEBO)											x	x
TRUSTINSOFT							x					
TYREX (EX. KUB)							x		x			
UBIKA							x		x			
UGLOO					x							
UNCOVERY											x	
VADE				x	x		x		x		x	
WALLIX							x				x	x
WHALLER					x							x
YESWEHACK							x	x				
YOGOSHA								x				

Fiches Entreprises

Informations contact

CLERC Françoise | contact@6cure.com
09 71 16 21 50 | www.6cure.com
701, rue Léon Foucault — Hérouville Saint Clair

Description et produits

6cure, éditeur, développe des solutions de protection contre différentes catégories d'attaques, notamment DDoS, visant la disponibilité des réseaux et des infrastructures DNS. Ces offres permettent aux organisations sensibles d'accroitre leur réactivité face aux attaques multiformes.

6cure propose aussi une offre de service de tests de résistance aux attaques DDoS.

- **Protection DDoS** 6cure DDoS Threat Protection : Identifie et filtre en temps réel les attaques DDoS complexes, en préservant les flux légitimes
  Protection sur site, cloud ou hybride
- **Sécurité DNS** 6cure DNS Protection : solution « tout-en-un », transparente et agnostique, qui garantit la disponibilité et la qualité de service et offre une visibilité complète de la menace
  Réaction rapide face aux infections, exfiltrations de données, fraudes
- **Audit DDoS** DDoS Assessment évalue la résilience des infrastructures face aux DDoS.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Informations contact

Miguel De Oliveira | laura.bleuse@aisi.fr
06 59 58 69 50 | www.aisi.fr
1 avenue Alphand 94160 Saint-Mandé

Description et produits

Expert Cybersécurité depuis plus de 7 ans et auprès de 400 clients !

Notre stratégie à destination des PME, ETI et services publics, est issue du savoir-faire d'une équipe d'experts (issue du CAC40 / SBF120).

Sécurité stratégique / RSSI as a service

- Conformité, Gouvernance, Diagnostic, Mise en place et optimisation des processus SSI, Préparation à la gestion de crise cyber

Sécurité opérationnelle

- SOC et CSIRT
- Test d'intrusion

Sécurité des Infrastructures

- Audits d'architectures et de configuration (on premise / cloud / hybrides)
- Design, déploiement et gestion des solutions réseau et sécurité, EDR, NDR, XDR, etc.
- Services managés associés (MCO, MCS)

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

---

Informations contact

LY NANCY | Nancy.ly@algosecure.fr | contact@algosecure.fr
04 26 78 24 86 | www.algosecure.fr

Description et produits

AlgoSecure est un cabinet conseil français spécialisé en cybersécurité. Depuis 2008, il accompagne les entreprises et les organismes publics dans la sécurisation de leurs systèmes d'information.

Qualifié PASSI sur toutes les portées de tests d'intrusion et certifié ISO27001,

AlgoSecurebénéficie d'une forte expertise technique et propose :

- Des audits techniques/gouvernance (test intrusion externe, web, Red team, analyse de risque, audit de configuration...) ;
- Des conseils et de la sécurisation : accompagnement SSI et à la certification ISO 27001, RSSI externalisé, ... ;
- De la surveillance : gestion de surface externe (EASM) ;
- De l'assistance en cas d'incidents : réponse à incidents, analyse forensic,...

Les engagements d'AlgoSecure :

- Bénéficier de conseils impartiaux de la part d'un partenaire indépendant.
- Générer de la valeur ajoutée grâce à une approche pragmatique.

PASSI

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité
Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information
Art. 21.2.b : Gestion des incidents
Art. 21.2.c : Continuité des activités
Art. 21.2.d : Sécurité de la chaîne d'approvisionnement
Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité
Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Informations contact

MANHES Stéphane | smanhes@altospam.com
0825.950.038 | www.altospam.com
31 rue Belle Étoile 33000 BORDEAUX

Description et produits

ALTOSPAM est un éditeur français, depuis plus de 20 ans, dans la protection des messageries professionnelles. Nos solutions souveraines, rapides à installer, faciles à gérer et transparentes pour les utilisateurs, sont reconnues pour leur performance.

ALTOSPAM s'engage sur un SLA et intègre un PRA gratuit.

- MailSafe, solution de filtrage des emails entrants, combine 16 technologies antispam, 6 antivirus et des systèmes anti-zerodays.
  MailSafe protège votre entreprise des spams, virus, malwares, phishing, spear-phishing, fovi, ransomwares.
- MailOut, solution de filtrage du flux sortant, améliore la délivrabilité des emails. Elle assure la transmission fluide des emails tout en prévenant la diffusion de spams et virus.

Notre politique tarifaire permet aux TPE et PME soucieuses de la sécurité de leurs emails de se protéger efficacement.
ALTOSPAM sécurise aujourd'hui plus de 8000 clients.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

DACQUAY Ronan | info@antemeta.fr
0130623322 | www.antemeta.fr
5 rue Jacqueline Auriol 78280 GUYANCOURT

Description et produits

AntemetA est l'un des leaders du cloud hybride et de la protection des données. L'entreprise accompagne plus de 1000 clients dans l'évolution de leurs systèmes d'information, par la mise en œuvre de solutions d'infrastructure (VAR), la fourniture de services Cloud et de cybersécurité (CSP) et une expertise des services managés (MSP). Entreprise à taille humaine avec près de 300 collaborateurs, le groupe compte 6 agences implantées en France ainsi qu'une filiale au Maroc. **L'ensemble des offres cloud et du service clients AntemetA sont certifiés ISO 27001, garantissant la sécurité et la confidentialité des informations hébergées.** En 2022, l'entreprise obtient la certification Hébergeur de Données de Santé et l'attestation ISAE 3402.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Informations contact

Miki Laurent | marcom@arcadsoftware.com
+33 450 578 396 | www.dot-anonymizer.fr
55 rue Adrastée 74650 Chavanod

Description et produits

Avec plus de 30 ans d'expérience en DevSecOps dans tous les secteurs d'activité et technologiques, ARCAD Software est un acteur français majeur de gestion des données de test.

ARCAD Software répond aux défis actuels du respect des données personnelles et de l'intégrité des systèmes d'informations avec ses solutions de détection, d'extraction, de masquage, de pseudonymisation et d'anonymisation des données : **DOT Anonymizer** et **DOT Extract**.

DOT Anonymizer masque les données personnelles et identifiantes tout en conservant leur cohérence, dans toutes les sources de données et SGBD. Il permet de s'affranchir des contraintes liées au RGPD et d'éliminer le risque lié aux fuites de données hors production.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Informations contact

Yosra Jarraya | yosra.jarraya@astran.io | 06 59 38 72 63
www.astran.io | 19 bd Poissonnière, 75002 Paris

Description et produits

Astran, spécialiste français en résilience et sécurité des données, agit comme le dernier rempart contre les cyberattaques en mettant continuellement à disposition des entreprises leurs kits de survie numérique cyber et business (procédures et contacts d'urgence, données critiques, clefs, active directory). Astran permet ainsi de renforcer les dispositifs de continuité d'activité, en mettant à disposition un lieu de stockage hautement disponible et sécurisé.

La résilience apportée par la solution Astran est assurée par **l'association d'algorithmes de fragmentation de données à un RAID5 en multi-cloud (Secret Sharing)**. Astran est en cours de certification CSPN auprès de l'ANSSI et a été sélectionnée par les services du Premier Ministre pour le dispositif d'accélération SecNumCloud (programme France 2030).

Les clients d'Astran incluent Eiffage, BNP et Sanofi, ainsi que des ETI et PME.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Informations contact

Luc D'Urso | luc.durso@atempo.com | 0603023024
23 avenue Carnot, 91300 Massy

Description et produits

Atempo, éditeur français de logiciels de protection et de gestion des données, offre des solutions de sauvegarde et de reprise d'activité (Continuity, Lina, Tina) pour serveurs physiques, virtuels et postes de travail. Sa solution Miria assure l'archivage, l'analyse, la sauvegarde, la synchronisation et la migration entre différents stockages de grands volumes de données non structurées.

Membre de Cybermalveillance.gouv.fr, Atempo renforce la cyber résilience en préservant les entreprises de tout sinistre.
Labellisées **« *Utilisé par les Armées Françaises* »** et **« *France Cybersecurity* »**, ses solutions sont référencées aux Centrales d'Achat RESAH, CAIH, UGAP.

- Continuity : appliance de sauvegarde tout-en-un
- Lina : solution de protection continue des données des postes de travail
- Tina : solution de sauvegarde pour serveurs virtuels ou physiques
- Miria : plateforme de gestion de données non structurées

Référentiel NIS 2

Art. 21.2 : Protection de l'environnement physique des réseaux et systèmes d'information

Art. 21.2.c : Continuité des activités

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Informations contact

PEREZ Pascale | pascale.perez@aucae.com
05 82 95 13 36 | https://aucae.com
12 Rue Courtois de Viçose
Bat Pyrenea — Portes Sud
31100 TOULOUSE

Description et produits

AUCAE est éditeur d'une solution SaaS souveraine de pilotage de crise cyber simple, intuitive et résiliente. Cette solution possède des atouts qui répondent aux besoins de s'entrainer avant crise et de réagir en équipe quand une crise survient.

L'ergonomie et simplicité de l'interface permet son appropriation par des « opérationnels, non-experts ».

Elle possède des atouts qui répondent aux besoins de résilience des organisations face aux menaces numériques : intégration de plusieurs types de cellules, plusieurs types de crise, procédures et annuaires de crise, infrastructure de communication de secours souveraine intégrée et administrable directement dans la solution.

AUCAE compte parmi ses clients des établissements publics et des entreprises privées en France et à l'International.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

AvantdeCliquer
L'humain au cœur de la cybersécurité .com

Informations contact

Hauguel Anaïs | 02 79 49 12 59 | https://avantdecliquer.com
129 rue E. Delamare Deboutteville, 76160 Saint Martin du Vivier

Description et produits

Avant de Cliquer est une entreprise spécialisée dans la sensibilisation à la cybersécurité, qui a été créée en 2017 avec l'objectif de **sensibiliser les collaborateurs** des entreprises aux risques de la cybercriminalité et aux bonnes pratiques de sécurité en ligne.

Avec une équipe de 40 professionnels passionnés et expérimentés, « Avant de Cliquer » est devenue un acteur de référence dans son domaine d'activité en France et à l'international.

Cette jeune entreprise permet aux DSI, RSSI, DPO et dirigeants de réduire le **risque de cyberattaques de manière drastique**.

FRANCE CYBER SECURITY

Référentiel NIS 2

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

axians

Informations contact

DJEBAR Karim | karim.djebar@axians.com | 0781334092 | www.axians.fr
2169 boulevard de la Défense — CS90274 — 92741 Nanterre Cedex

Description et produits

Audit & Conseil : cybersécurité IT & OT, gouvernance, gestion des risques, accompagnement aux normes et certifications, assistance RSSI/DPO, sensibilisations et formations.

Solutions de Sécurité : audit d'architectures et de configurations, conseil et intégration de solutions de sécurité des infrastructures, des données, des accès ainsi que la sécurité du contenu et du Cloud.

Services Opérationnels : Red Teaming, Vulnerability Management, détection & analyse, Threat Intelligence et réponse aux incidents.

Nous disposons de plusieurs offres cybersécurité souveraines en mode XaaS hébergées dans nos propres Datacenters en France :

- Crystal by CERT Axians : Service de veille en vulnérabilités IT & OT.
- WaaSA (Wallix as a Service by Axians) : Plateforme de Bastion as a Service.
- SOLAR SOC : Solution de MDR en mode Cloud Axians.

EXPERT CYBER

PASSI

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité
Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information
Art. 21.2.b : Gestion des incidents
Art. 21.2.c : Continuité des activités
Art. 21.2.d : Sécurité de la chaîne d'approvisionnement
Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité
Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

NECTOUX Elisa | elisa.nectoux@belledonne-communications.com
09 52 63 65 05 | www.linphone.org
3 avenue Marie Reynoard, 38100 GRENOBLE

Description et produits

Suite logicielle pour les communications unifiées sécurisées : appels par internet (VoIP, visio), messagerie instantanée, groupes et vidéoconférence.
Notre softphone Linphone et notre suite serveur Flexisip sont basés sur le protocole de télécommunication SIP. Ils répondent à vos besoins de communication collaborative, dans votre réseau ou en télétravail.

Linphone chiffre de-bout-en-bout tous les médias échangés (voix, vidéo, tchat) et est déjà robuste aux attaques des futurs ordinateurs quantiques. Protégez les communications à tous les niveaux de votre organisation, grâce à une application facile à utiliser tout en étant à la pointe de la sécurisation des communications.

Solution 100 % open source et souveraine depuis 2010, disponible on premise ou en services managés.

Services proposés : installation serveurs, support, personnalisation à vos couleurs, développements à la demande.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Informations contact

Pierre Baudracco | pierre.baudracco@bluemind.net | 06 82 84 63 67
www.bluemind.net | 40 rue du village d'entreprises, 31670 Labège

Description et produits

Éditeur de 2 solutions : une de messagerie collaborative et une de communication de secours en cas de cyberattaque ou crise

- **BlueMind,** la messagerie collaborative, alternative de référence à MS Exchange / 365, offrant la souveraineté sans compromis au niveau des usages. En étant la seule solution à supporter nativement Outlook, à proposer la collaboration avec Thunderbird, le web et les mobiles, BlueMind permet aux organisations de concrétiser, sur l'application la plus utilisée et exposée, les volontés de souveraineté et de maîtrise de son système d'information !
- **BlueMind Digital Crisis :** Solution de communication de secours, décorrélée du SI, pour préserver les capacités de communication (email, agenda, visio, mobiles) même quand le SI est paralysé pour gérer une crise ou cyberattaque.

S'interface avec la **solution d'AUCAE** pour fournir une solution globale de gestion de crise

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

board of cyber

Informations contact

Luc Declerck | ldeclerck@boardofcyber.io | 06 60 72 39 23
www.boardofcyber.io/fr | 7 avenue de la Cristallerie 92310 Sèvres

Description et produits

Board of Cyber est une startup française fondée en 2022, spécialisée dans la gestion du risque cyber. Ses **solutions SaaS automatisées** permettent à ses clients d'évaluer, piloter et améliorer en continu la performance cyber de leur organisation et de leur écosystème. Board of Cyber, avec ses 40 collaborateurs, accompagne plus de 350 clients.

Sa mission est de créer un écosystème de confiance.
Le premier produit développé par Board of Cyber est le **Security Rating®** qui délivre une notation de la performance et de la maturité cyber des entreprises sur leur empreinte Internet à partir de données publiques.

Vient s'ajouter un tout nouveau produit, l'**AD Rating®**, un outil de pilotage du risque cyber qui délivre une évaluation du niveau de sécurité de vos domaines Active Directory.

Board of Cyber commercialise également le produit **TrustHQ®**, une solution de pilotage de la conformité et des risques SSI qui assiste les RSSI dans leur démarche d'amélioration en continue.

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Bonjour Cyber ®

Informations contact

Lahlou Farid | bonjour@bonjourcyber.com | 01 76 35 03 04
www.bonjourcyber.com | 34 Boulevard DES ITALIENS 75009 Paris

Description et produits

Chez BonjourCyber®, notre mission est claire : démocratiser la cybersécurité pour la rendre accessible à tous. Experts en protection des PME et ETI, nous adaptons nos services pour chaque entreprise, des novices à la cybersécurité aux plus expérimentés.

Notre but ? Transformer la cybersécurité en un avantage concurrentiel. Chez BonjourCyber®, nous sommes fiers de nos équipes, chacune dédiée à un aspect crucial de la cybersécurité dans les PME et ETI.

- L'équipe **BonjourPhishing®** se concentre sur la sensibilisation et la formation au risque de phishing,
- L'équipe **HackMelfYouCan®** est experte en tests d'intrusion et audits de sécurité, offrant une évaluation réaliste de la robustesse de vos systèmes face aux menaces extérieures,
- L'équipe **BonjourBackup®** assure la sécurité de vos données grâce à des solutions de sauvegarde fiables et innovantes.

FRANCE CYBER SECURITY — EXPERT CYBER

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

JOSSET Anselme | aj@brain-networks.fr
06 50 69 97 05 | www.brain-networks.fr
294 avenue Georges Clémenceau, 92000 Nanterre

Description et produits

Brain Networks est une société indépendante fondée en 2007 par des spécialistes de la sécurité réseau et de l'optimisation WAN.

Véritable bras droit des DSI et RSSI, elle a consolidé sa double expertise au fil des ans autour d'un leitmotiv : l'engagement de résultat.

C'est ainsi qu'elle apporte aujourd'hui un accompagnement sur-mesure à chaque étape de la transformation numérique des entreprises, en assurant la performance, la sécurité, et la conformité de leur système d'information.

Brain Networks a développé des compétences très pointues sur toutes les dimensions de la cybersécurité :

- Préventive : audit, sensibilisation
- Défensive : solutions technologiques (intégration et services managés) ;
- Offensive : pentests, campagnes de phishing ;
- Visibilité : EDR/XDR, SIEM (mini-SOC) ;
- Gouvernance : architecture, stratégie cyber, PSSI.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

Martin Sacha | sacha@brainsecurity.io | +33 6 31 73 23 79
229 rue Saint-Honoré, 75001, Paris — France | https://brainsecurity.io/fr

Description et produits

Brain transforme la sensibilisation à la cybersécurité avec une plateforme SaaS complète, alliant expérience utilisateur, gamification, et neurosciences pour un apprentissage captivant et efficace. Notre approche cible le comportement humain, renforçant la culture de sécurité au sein des organisations.

- **Apprentissage Gamifié :** plongez dans des modules tels que Cyberbook, Cyberreflexes, et Cyber Cup pour un apprentissage interactif et divertissant.
- **Brian, l'Assistant Cyber :** guide virtuel intelligent, Brian répond aux questions des utilisateurs, enrichissant leur parcours d'apprentissage.
- **Simulateur de Phishing :** évaluez et renforcez la vigilance des employés avec des simulations de phishing réalistes.
- **Dashboard Analytique :** un tableau de bord intuitif offre rapports détaillés et permettant de personnaliser la sensibilisation.

Référentiel NIS 2

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

conscio technologies

Informations contact

Vanina DEROUBAIX | vanina.deroubaix@conscio-technologies.com
01 84 80 03 93 | www.conscio-technologies.com
3 rue Camille Claudel, 56890 Plescop — Bâtiment M

Description et produits

Conscio Technologies est un éditeur de logiciel SaaS, notamment de la plateforme **« Sensiwave »**, la solution française la plus complète en matière de **sensibilisation cybersécurité et de contenus de sensibilisation**. Nous accompagnons les RSSI, DSI et DPO depuis 17 ans, dans la mise en œuvre de leur stratégie de sensibilisation cyber en ligne. Grâce à notre approche sectorielle : santé, collectivités territoriales, industrie et retail, nous développons des contenus dédiés à chacun, coconstruits avec les équipes cyber du secteur, pour **coller au mieux à leur réalité**. Nous disposons d'un catalogue riche, de 160 modules traitant des différentes thématiques sous de multiples formats, plus de 150 scénarios de test phishing... Un catalogue mis à jour en continu par notre équipe contenus.

Nous proposons un accompagnement personnalisé unique en France de notre équipe Customer Success.

Référentiel NIS 2

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

---

continus

Informations contact

EL AOUADI Tarik | tarik.elaouadi@continus.io | +33 6 64 13 43 43
https://continus.io/ | 34 Avenue des Champs-Élysées 75008 Paris

Description et produits

Continus.io est une Startup de cybersécurité basée à Paris et fondée par deux experts en Sécurité Applicative.

Nous développons des produits et solutions pour sécuriser les cycles de développement logiciel. Nous éditons la plateforme All-In-One **« Continus DevSecOps »** qui unifie, dans une seule solution, les outils indispensables aux équipes de développement pour adresser les besoins de sécurité et de conformité tout au long du cycle de vie logiciel.

Nos solutions sont conçues avec **flexibilité** pour s'adapter à nos clients et pouvoir les accompagner quel que soit leur niveau de maturité au départ.

Continus.io permet d'intégrer la **sécurité by-design dans les cycles de développement logiciel** en alliant sécurité, simplicité, budget et Time-to-Market.

Référentiel NIS 2

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Informations contact

Jean Devaux | jean@crowdsec.net
06 30 26 32 19 | www.crowdsec.net
20 rue Maurice Arnoux 92120 Montrouge — France

Description et produits

CrowdSec redéfinit la cybersécurité grâce à sa stratégie de défense proactive et à son approche collaborative unique. Leader dans le domaine des listes de blocage de sécurité, **l'entreprise exploite le plus grand réseau mondial de renseignements sur les cybermenaces**, fondé sur des données recueillies auprès de sa communauté, offrant ainsi une protection et une efficacité inégalées. L**es listes de blocage de CrowdSec renforcent non seulement la sécurité de manière proactive, mais permettent également d'améliorer considérablement l'efficacité des opérations de sécurité et de réduire les coûts**.

Conçues pour une intégration sans effort, les solutions de CrowdSec s'adaptent en douceur à toute infrastructure existante. Les **Blocklists CrowdSec** sont créées sur la base de la plus grande source de réputation IP au monde. Avec plus de 70 000 utilisateurs actifs dans plus de 190 pays à travers le monde, partageant en moyenne 10 millions de signaux sur des IP agressives chaque jour, les CrowdSec Blocklists offrent une approche infaillible de la veille sur les menaces.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

Christian d'Orival | christian.d-orival@cryptonext-security.com
06 03 00 26 31 | www.cryptonext-security.com
16 Boulevard Saint-Germain 75005 Paris

Description et produits

CryptoNext Security, éditeur de logiciels Français spécialisé en **cryptographie résistante au quantique**, a été fondée en 2019 après 20+ années de recherche académique. Elle a reçu le Prix Innovation Assises 2022, citée dans le Top 5 du rapport Gartner et est membre actif du NIST/NCCoE et de l'IETF.

CryptoNext Quantum Safe Remediation Suite (C-QSR) est une suite logicielle nativement crypto-agile et hybride **dotée d'implémentations performantes et souveraines des algorithmes PQC** (NIST, agences de sécurité), d'**une protection contre les attaques physiques**, des principaux protocoles, certificats, outils d'intégration et plugins applicatifs. Elle permet la mise en œuvre efficace et évolutive des capacités de protection contre la menace quantique des systèmes, infrastructures et applications IT/OT des entreprises et des produits des constructeurs et éditeurs.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

CUSTOCY®

Informations contact

SIVIGNON Sébastien | ssivignon@custocy.com | 06 23 02 82 30
www.custocy.ai | 1244 L'Occitane 31670 Labège

Description et produits

Créé en 2018, Custocy est un éditeur spécialisé en cybersécurité, basé à Toulouse, en région Occitanie. Forte d'une équipe de 15 personnes dont 30 % de docteurs et doctorants en intelligence artificielle et d'experts en cybersécurité, Custocy a développé sa solution **NDR** (Network Detection & Response).

La pépite toulousaine ambitionne de devenir le leader européen de la détection d'intrusion réseau à base d'IA. La solution NDR de Custocy repose sur **une technologie unique d'IA collaboratives, conçue en interne** au sein de son laboratoire de recherche. En dépassant les limites des outils traditionnels, son approche innovante assure une **identification proactive des attaques sophistiquées (APT) et inconnues (ZERO-DAY) en cours sur le réseau des entreprises**, avec une précision sans précédent.

Pensée pour apporter 4 principales capacités — surveillance continue du réseau, détection en temps réel, réponse ciblée et reporting automatique pour preuve de conformité NIS2 —, cette solution SaaS est le fruit de 5mEUR d'investissements depuis sa création et d'efforts continus pour offrir une solution de pointe en matière de sécurité numérique.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

CYBER-DETECT© MORPHOLOGICAL ANALYSIS

Informations contact

Régis LHOSTE | r.lhoste@cyber-detect.com | 06 89 30 73 75
www.cyber-detect.com | 82 rue du Sergent Blandan 54000 Nancy

Description et produits

CYBER-DETECT propose une **méthode d'analyse unique** pour la détection et caractérisation de malwares 0 day.

Baptisée Gorille, **cette solution identifie rapidement le comportement d'un fichier exécutable inconnu, polymorphe ou packé**.
Elle s'intègre dans les CERT ou SOC et s'interface avec les EDR, SIEM ou SOAR.

Cette méthode d'analyse apporte également des pistes concrètes de remédiation telles que MITRE ATT&CK et MITRE D3FEND ainsi qu'une précision singulière sans phase d'apprentissage.

Gorille se décline en 3 offres :

- **Gorille Expert :** solution de caractérisation de logiciels malveillants complexes (obfusqués, dormants...)
- **Gorille Cloud :** outil de caractérisation instantané en SAAS ou on-premise
- **Gorille Patrouille :** la cyber analyse qui protège le parc informatique des menaces dormantes »

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Cyberium

Informations contact

VERLEY Stanislas | stan@cyberium.solutions | 06 07 89 14 04
www.cyberium.solutions | 450 rue Baden Powell 34000 Montpellier

Description et produits

Cyberium, StartUp française résolument orientée vers l'international, excelle dans la **segmentation des réseaux pour les entités critiques**, avec une expertise marquée **dans les domaines des réseaux industriels / OT, des agences gouvernementales et des infrastructures Cloud**.

Grâce à notre technologie brevetée de proxy/guichet logiciel, nous étendons les capacités des fournisseurs de solutions hardware ou software de cybersécurité en flexibilité, fiabilité, bande passante et niveau de sécurité.

Notre innovation permet aux industriels d'adopter des solutions avancées comme les Data Diodes unidirectionnelles, conformes aux normes strictes du marché (certification ANSSI en France, standard international Common Criteria EAL 7+) : tout en préservant leurs flux de données et protocoles habituels, ils peuvent tirer parti de l'ensemble des données de leurs infrastructures, même hautement sensibles. **Les clients répondent ainsi aux directives de sécurité telle que NIS2, tout en poursuivant leur transformation numérique**.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

cybervadis

Informations contact

Estelle Joly | ejoly@cybervadis.com | 01 86 26 94 66
www.cybervadis.com | 43 Av. de la Grande Armée 75116 Paris

Description et produits

CyberVadis offre à ses clients une solution complète et intégrée pour **piloter le risque cyber lié aux tiers**. Nous évaluons pour nos clients la cybersécurité de leurs tiers, qu'ils soient fournisseurs, partenaires ou filiales. Toutes les évaluations sont basées sur la revue de preuves afin d'assurer la fiabilité des ratings qui en résultent. Notre méthodologie s'appuie sur **les principaux référentiels de sécurité**, notamment le NIST Cybersecurity, l'ISO 27001 et le RGPD. Ces évaluations sont délivrées sur une plateforme SaaS qui propose, au-delà des évaluations, une offre complète pour gérer l'ensemble des fournisseurs à risque (risque spécifique, plan de remédiation, détection de certification, monitoring, gestion de la compliance...).

Avec la solution CyberVadis :

- gérez tous vos tiers sur une seule plateforme,
- collectez des indicateurs, centralisez vos données et priorisez les évaluations,
- obtenez des résultats détaillés, validés par nos analystes sur la base de preuves,
- collaborez avec vos tiers sur leur plan d'amélioration et partagez vos recommandations avec votre organisation.

Référentiel NIS 2

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

cyberwatch

Informations contact

Maxime ALAY-EDDINE | maxime@cyberwatch.fr | 06 25 23 64 81
https://cyberwatch.fr | 10 rue Penthièvre 75008 Paris

Description et produits

Cyberwatch est un éditeur français de logiciels de sécurité informatique, spécialisé dans **la gestion des vulnérabilités et le contrôle des conformités**.

Membre du groupement Hexatrust, de l'Alliance pour la Confiance Numérique et du CLUSIF, référencé à l'UGAP, Cyberwatch propose **des logiciels simples et flexibles, avec des outils pertinents d'aide à la décision**. Cyberwatch est une filiale de Framatome, groupe EDF.

Cyberwatch Vulnerability Manager est une solution de gestion des vulnérabilités, avec cartographie du système d'information, détection des vulnérabilités, priorisation basée sur le risque et sur les contraintes métiers, aide à la décision, et module de correction.

Cyberwatch Compliance Manager est une solution de contrôle des conformités, avec analyse du niveau de durcissement et personnalisation complète possible des règles et des référentiels testés.

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

CyberXpert

Informations contact

Fabrice Hecquet | fabrice.hecquet@cyberxpert.be
+32 4 78 82 03 03 | www.cyberxpert.be
heidebadlaan 34 — 2900 Schoten — Belgique

Description et produits

Chez CyberXpert, nous comprenons que définir une cyber stratégie et faire les bons choix en termes de gouvernances et solutions n'est pas toujours facile. Cela reste un domaine d'Experts.

Depuis plus de 10 ans, nous accompagnons nos clients issus de tous secteurs pour répondre à leurs besoins en Belgique et au Luxembourg.
Nos services vont **de l'audit de sécurité, à des tests de vulnérabilités, la définition d'une stratégie cyber, les mises en conformités ou le déploiement de solutions**. Nous nous positionnons en tant que votre partenaire SECURITÉ pour mener à bien vos projets.

Consultance en cybersécurité, Pen testing, audit, Conformité NIS2, Services SOC as a service intégration de solutions cyber européennes :

Partenaires : VADE, Gatewatcher, Wallix, Cyberwatch, ESET, Pradeo, Oodrive, Board of Cyber, Atempo, Patrowl, 6cure, Primx, Arcad Software, Sekoia, Cyberium, Tranquil IT, P4S, Snowpack, 6cure, Ilex, Trustbuiler, Dastra, Avant de Cliquer...

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

dastra

Informations contact

Bidault Paul-Emmanuel | paulemmanuel.bildault@dastra.eu
01 76 46 12 30 | www.dastra.eu | 25 Rue de Tolbiac 75013 Paris

Description et produits

Dastra est **une plateforme privacy** permettant aux délégués à la protection des données (DPO) de mettre en œuvre la gouvernance de la conformité RGPD. Grâce à des fonctionnalités avancées utilisant notamment l'IA, Dastra facilite la collaboration entre les DPO et les métiers, **en structurant les processus et en assurant un pilotage efficace de la conformité**.

Notre offre consiste en **un logiciel SaaS collaboratif** qui répond à tous les cas d'usage du RGPD, comme le registre des traitements, la cartographie, les analyses d'impact, la gestion de risques sous-traitant, les audits, les demandes d'exercices de droit, les violations de données et le consentement cookies. **Disponible en plug & play** sous forme d'un guichet unique, Dastra peut être testé gratuitement.

defants
COLLABORATIVE & AUTOMATED SOLUTIONS

Informations contact

François KHOURBIGA | f.khourbiga@defants.com
06 50 37 59 12 | www.defants.com/fr
1137 A Avenue des Champs Blancs, Digital Square 35510 Cesson Sévigné

Description et produits

Defants est une entreprise éditrice de logiciel basée à Rennes qui existe depuis août 2021. Elle a été fondée par trois cofondateurs François Khourbiga, Thomas Maréchal et Maxime Lebreton. Elle compte aujourd'hui une vingtaine de collaborateurs et propose de **redéfinir l'investigation numérique** grâce à sa plateforme de Threat Investigation, no-code, Defants vSIRT.

Grâce à elle, vous allez pouvoir redéfinir l'investigation numérique de manière drastique, avec de l'**automatisation**, de la **collaboration**, **l'utilisation de graph sémantique** et **en obtenant un rapport** qui se rédige seul dès que l'investigation débute.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Informations contact

Jonathan AMAR | jonathan.amar@deletec.fr | 06 75 73 21 68
www.deletec.fr | 35 rue de Prony 75017 Paris

Description et produits

DELETEC est une **ESN de confiance**, spécialisée en transformation digitale depuis 25 ans. Notre offre de services couvre l'ensemble des besoins IT des entreprises et des organisations, avec un accent particulier accordé à la sécurité : consulting, optimisation des infrastructures et du workspace, pérennisation des données, cloud, cybersécurité, infogérance, télécoms.

Nous vous accompagnons tout au long de votre parcours cyber, de la prévention et sécurisation de vos systèmes d'information à l'intervention d'urgence en cas d'incidents : • **Consulting et gouvernance** • **Protection des identités** • **Audits de sécurité et tests d'intrusion** • **Surveillance, détection et réaction — SOC** • **Sécurisation des endpoints** • **Sécurisation des infrastructures et accès sécurisé** • **CERT**

Solutions : EDR, hardening AD, MFA, PAM, SIEM, VM HDS hybride, sauvegarde M365, sauvegarde externalisée, PRA, RGPD, RSSI externalisé...

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

Gonzales Léo | leo.gonzales@devensys.com | +33 4 67 71 77 49
www.devensys.com | 836 rue du Mas de Verchant, 34000 Montpellier

Description et produits

Devensys Cybersecurity, Pure Player cybersécurité français est une société fondée à Montpellier il y a 11 ans par des ingénieurs. Les valeurs de l'entreprise sont : **Expertise, Qualité, Ethique**.

L'activité est structurée autour de 5 pôles :

- **Red Team & Pentest** (web, logiciel, mobile, attaques complexes, social engineering, intrusion physique...)
- **SOC 24/7** (MXDR, SLA avec GTI 30 min., pénalités, équipes 100 % France, habilitations...)
- **VOC & CERT** (suivi de vulnérabilités, surveillance fuite de données, alertes proactives, préparation et réponses aux incidents avec GTI 2h...)
- **Sécurité Cloud & Infrastructure** (analyse de risque, intégration, projets complexes, réseau, firewall, PKI/HSM, PAM, SSO, EDR, sécurité Microsoft...)
- **Formation & Certification** (sensibilisations, formations, centre officiel des 3 plus grands noms : EC-Council CEH / OffSec OSCP / ISC2 CISSP...)

digitalberry

Informations contact

Iguenane Matthieu | matthieu.iguenane@digitalberry.fr
06 72 89 69 09 | www.digitalberry.fr
10 Place de la Joliette 13002 Marseille

Description et produits

Fondé en 2014, Digitalberry est un éditeur français de cybersécurité, spécialisé dans la gestion des certificats numériques et des clés de sécurité.

Sa solution CLM, **BerryCert** permet de **simplifier et d'automatiser la gestion du cycle de vie des certificats** au moyen d'un inventaire exhaustif et d'un processus de renouvellement ou de révocation automatique, en passant par l'audit de leur conformité en ligne avec la politique de sécurité définie par les entreprises et les recommandations de l'ANSSI. Le volume des certificats numériques ne cesse de croitre tandis que leur durée de vie diminue. BerryCert garantit que les certificats soient convenablement cartographiés, émis, révoqués, renouvelés ou remplacés et ce, en temps voulu.

Sa solution **BerryTMS** permet de **gérer le cycle de vie des clés de sécurité** : inventaire, protection des secrets d'administration, initialisation et déploiement des clés, ou encore restriction et révocation des droits d'accès à distance.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

DOCAPOSTE

Informations contact

Picard Gaëlle | gaelle.picard@docaposte.fr
www.docaposte.com | 06 87 22 22 16
45/47 boulevard Paul Vaillant Couturier
94220 Ivry-sur-Seine

Description et produits

Docaposte, acteur référent pour un **numérique de confiance, souverain et éthique**, vous propose de vous accompagner sur tous vos besoins en cybersécurité, **du diagnostic à l'audit en passant par l'analyse de risque, le conseil et jusqu'au déploiement de solutions de protection, d'analyse et de détection** au sein de vos réseaux et systèmes.

Avec un engagement unique, celui de couvrir l'intégralité de votre besoin en cybersécurité. L'offre cyber de Docaposte est constituée de deux volets complémentaires :

- **Une solution de sécurisation technique**, au travers d'un package cyber regroupant les meilleures technologies du marché. Avec un unique contrat, tous les aspects de la cybersécurité sont pris en compte pour une sécurisation simple et efficace.
- **Un volet conseil**, porté par la filiale Softeam, pour vous accompagner lors de :
  - la mise en œuvre d'une gouvernance cyber performante
  - la réalisation d'audits techniques ou organisationnels,
  - la préparation à la gestion de crise ou de continuité d'activité
  - la mise à disposition de ressource d'accompagnement.

eIDAS
PVID

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Informations contact

Philippe Dann | philippe.dann@ebrc.com | +33 6 08 10 78 60
www.ebrc.com | 85 rue Edouard Vaillant 92300 Levallois-Perret

Description et produits

Experts en résilience et cybersécurité, EBRC et sa filiale Digora conseillent, conçoivent, opèrent, protègent et maintiennent l'activité digitale des organisations les plus sensibles, en adéquation avec les réglementations européennes (NIS2, DORA). Nous sommes présents en France, au Luxembourg et au Maroc. Nous délivrons **une gamme de services intégrés et certifiés ISO 27001, ISO 22301, ISO 20000**, à travers nos Data Centres certifiés Tier IV, un Cloud européen et des solutions pour le multicloud.

EBRC et Digora sont partenaires d'Egerie (Cyber Risk Management intégré) et Conscio (sensibilisation et e-learning Cyber, RGPD, RSE).

Cyber Resilience Portal, notre logiciel de pilotage de la continuité des opérations, permet de convertir la méthodologie SMCA en métriques 360° pour la cyber-résilience et la mise à disposition de rapports consolidés pour une présentation au management.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité
Art. 21.2 : Protection de l'environnement physique des réseaux et systèmes d'information
Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information
Art. 21.2.b : Gestion des incidents
Art. 21.2.c : Continuité des activités
Art. 21.2.d : Sécurité de la chaîne d'approvisionnement
Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité
Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

Jean Larroumets | contact@egerie.eu | +33 (0)4 94 63 81 09
https://www.egerie.eu

Description et produits

EGERIE est une plateforme collaborative qui **cartographie et quantifie financièrement les risques d'origine cyber et aide les organisations à industrialiser leurs programmes de cybersécurité** pilotés par les risques. Reconnue par les plus hautes autorités gouvernementales et réglementaires françaises et européennes, la technologie d'EGERIE permet ainsi aux entreprises **d'identifier, de manière dynamique, les risques et menaces élevés**, en mesurant les résultats des efforts de réduction des risques tout en emportant l'adhésion de tous les niveaux de l'organisation pour faire de la cybersécurité un actif dont la valeur dépend de l'implication de chacun.

La plateforme logicielle collaborative, « EGERIE Risk Manager », à travers son moteur multiméthodes d'analyse et ses bibliothèques métiers et normatives, propose à tous ses utilisateurs d'**élaborer une cartographie progressive des risques** leur permettant de maîtriser, dans la durée, leur niveau d'exposition et de prendre des décisions éclairées **tout en optimisant leurs budgets de sécurisation**.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité
Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information
Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

EQUISIGN

Informations contact

Loth Demay Guillaume | contact@equisign.fr | 0142919244
https://www.equisign.fr
Tour Opus 12, 77 Esplanade du Général de Gaulle 92081 Paris La Défense Cedex

Description et produits

Equisign est un éditeur de logiciels spécialisé dans la sécurité digitale. Ses produits sont MFT (solution de transfert de fichiers sécurisé) et Letreco (lettre recommandée électronique).

- **MFT** est la solution de transfert sécurisé de fichiers utilisée par plus de 2 millions d'utilisateurs (AMF, CNIL, Société Générale, Framatome, SNCF, Engie, Safran, Thales, Ministère de la justice, DGFIP, Ministère de l'Éducation Nationale, ADSN...). MFT a été certifiée par l'Anssi en obtenant une CSPN. MFT et est disponible à partir de 10 utilisateurs jusqu'à plus de 100 000 utilisateurs, en Saas ou On premise.
- **Letreco qualifiée** est une Lettre recommandée électronique qualifiée (art. 44 du Règlement eIDAS) inscrite par l'Anssi sur la liste de confiance française et sur la Trust List européenne. **Letreco simple** est un envoi recommandé électronique simple, selon les dispositions de l'article 43 du règlement eIDAS.

CSPN ; eIDAS

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

ERCOM

Informations contact

Romain Waller | romain.waller@ercom.fr
+33 6 07 52 33 58
https://cds.thalesgroup.com/fr/ercom
6 rue Dewoitine 78140 Vélizy-Villacoublay

Description et produits

ERCOM, filiale du groupe Thales, est une société française reconnue pour ses solutions de sécurisation des communications, données et terminaux en mobilité. Nos solutions sont déployées en France et à l'International auprès d'entreprises et d'institutions publiques qui ont besoin d'outils évolutifs, fiables et hautement sécurisés.
Découvrez nos solutions souveraines et certifiées :

- **CRYPTOSMART Mobile,** La solution ultime pour sécuriser les terminaux et les communications mobiles au niveau Diffusion Restreinte.
- **CRYPTOSMART PC,** La solution VPN pour PC clé en main avec un niveau de sécurité gouvernemental.
- **CRYPTOBOX,** La solution de partage et de stockage sécurisée, accessible partout.
- **CITADEL TEAM,** La solution d'audio & visioconférence et de messagerie sécurisée.
- **CYBELS HUB DR,** La plateforme collaborative sécurisée sur le Cloud DR pour collaborer au niveau Diffusion Restreinte.

CC EAL3+ & 4+
Qualification Standard
Agrément Diffusion Restreinte

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

EVERTRUST

Informations contact

Aufrere Alexandre | aau@evertrust.fr | +33663196303
https://evertrust.fr/ | 24 rue de Londres 75009 Paris

Description et produits

EVERTRUST est un éditeur de logiciels spécialisé dans un secteur clé de la cybersécurité : la gestion de la confiance numérique.

Notre mission est de fournir **des solutions opérationnelles, sécurisées et performantes** qui articulent la sécurité informatique et le contrôle du cycle de vie des certificats électroniques dont l'expiration est vecteur d'incidents majeurs qui impactent les organisations, les entreprises et les accès.

Notre connaissance des rouages des différentes infrastructures nous permet d'**identifier les chaînons manquants aux solutions disponibles** et de répondre aux défis des systèmes d'information (DevOps, Cloud).

Nos logiciels **Stream** et **Horizon** sont créés pour satisfaire les besoins sur la délivrance, l'automatisation et les besoins de continuité des services de confiance. Ils s'intègrent de manière non-intrusive, simple et efficace.

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

eXcelsior Safety

Informations contact

| Bodinier Hervé | hbodinier@excelsiorsafety.fr | +33762961634
16 allée Claude Monet 78160 Marly Le Roi | www.excelsiorsafety.fr

Description et produits

eXcelsior Safety, expert indépendant pour la **sécurité fonctionnelle, cybersécurité et gestion des DATA de vos procédés et machines industrielles**.

Notre expérience métier de plus de 35 ans et notre réseau d'experts ISEAClub, nous permettent d'apporter des produits & services aux ETI/PME voire grands groupes tout en fédérant nos ressources et investissements.

- **Gestion des risques industriels et cyber OT/IACS**
- **Diagnostics Cyber, cartographie/inventaire gestion des flux zones & conduits, organisationnel.**
- **Analyse de risques sécurité industrielle et cybersécurité (IEC 61882 & IEC 61508/61511/62061 & IEC 62443/27001).**
- **Vérification et Validation performances SIL/SL.**
- **Audit cybersécurité IEC62443/ANSSI.**
- **Solution sauvegarde & redémarrage production 30 s (PRA/PCA).**
- **Solution CDMaaS (Cyber-Data-Management-as-a-Service) Automatisation de la collecte, traitement et transport des données OT/IT avec DMZ intégré**

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

CAILLARD Jean-François | contact@exiptel.fr
0612200089 | https://exiptel.fr/
Campus Cyber, 5-7 rue Bellini 92800 Puteaux

Description et produits

Fondée en 2006 par des passionnés de réseaux et de sécurité informatique, Exiptel est une **entreprise de services du numérique** qui s'est spécialisée sur ces technologies, au service de grands clients, qui nous font confiance sur la durée. Société à taille humaine, nous attachons une grande importance aux recrutements et entretenons **une forte proximité** avec nos consultants, tout au long de leurs missions, de leurs formations et de leurs certifications sur les solutions les plus pointues.

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Informations contact

Rémy FABÉ | rfabe@exoplatform.com | 06 19 38 20 97
10 place Vendôme 75001 Paris | www.exoplatform.com

Description et produits

Éditeur français de logiciels open-source depuis 20 ans, eXo Platform est un **spécialiste des solutions intranet et digital workplace**. Son approche agile et son accompagnement sur mesure favorisent une adoption de la solution dans la durée.

Disponible **on-premise ou dans le cloud** (cloud privé & SecNumCloud), eXo est **une plateforme complète, sécurisée et paramétrable sans développement** selon les différents cas d'usages des administrations, collectivités territoriales et entreprises : intranet moderne, plateforme collaborative, gestion de communautés et gestion des connaissances.

La solution offre une expérience ergonomique, fluide, intégrée et unifiée, centrée sur le collaborateur. **eXo Platform respecte les normes de sécurité les plus élevées et propose des fonctionnalités avancées**, telles que la protection contre la fuite de données (DLP), l'authentification multi-facteurs ou la gestion des collaborateurs externes.

eXo se positionne comme une alternative open-source et souveraine à Microsoft 365.

Informations contact

AYADI Marc | marc.ayadi@fr.ey.com
06 07 70 71 59
Tour First, 1 Place des Saisons
TSA 14444 92037 Paris La Défense cedex
www.ey.com/fr_fr/consulting
www.ey.com/fr_fr/cybersecurity

Description et produits

EY Consulting est le **cabinet leader de la transformation en France** avec une équipe de 2.300 consultants spécialisés en innovation, technologie, conseil en management, conseil en ressources humaines et gestion des risques.

Présent sur le marché de la cybersécurité depuis 25 ans, EY Consulting dispose d'une équipe de **plus de 150 consultants et auditeurs spécialisés**, accompagnant au quotidien les organisations publiques et privées dans la définition de leur stratégie et leur conformité en matière de sécurité, la protection de leurs données, la gestion des identités, la définition et l'évaluation des architectures, l'ingénierie cyber, les cyber opérations intégrants tests techniques et services managés.

Les expériences, qualifications et certifications (PASSI, VISA de sécurité, TF-CSIRT, FIRST et CREST) permettant de **répondre aux besoins de ses clients suivants leurs enjeux, leurs priorités et leurs contraintes**.

PASSI RGS ;
FIRST ;
TCSIRT

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité
Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information
Art. 21.2.b : Gestion des incidents
Art. 21.2.c : Continuité des activités
Art. 21.2.d : Sécurité de la chaîne d'approvisionnement
Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques n matière de cybersécurité
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité
Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Informations contact

Arnaud Sraka | arnaud.sraka@f24.com
06 83 42 15 48 | https://f24.com/fr
Campus Cyber, 5-7 rue Bellini 92800 Puteaux

Description et produits

Fondé en 2000, F24 est le 1er fournisseur européen de **logiciels SaaS pour la gestion des incidents et des crises et des notifications d'urgence**. F24 équipe à la fois des OIV français, des sites SEVESO, des hôpitaux, et des institutions comme les ARS, l'AFD, de nombreux clients du CAC40, mais également la Belgique pour son alerte à la population. F24 s'appuie sur **une équipe dédiée et des outils de gestion de crise 360° résilients** pour mettre en place et suivre de les plans PCA, PRA.

FACT24 ENS+ est une solution permettant de prévenir ou de réunir des collaborateurs en quelques secondes. FACT24 CIM offre en plus de l'alerte, un tableau de bord complet pour gérer les incidents avec une description de l'incident, la gestion de tâches, où tout est tracé et horodaté via un tchat sécurisé et indépendant du SI client, un outil de création de rapports et une main courante dynamique.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Informations contact

Frédéric PIERRE | fpierre@fairtrust.com
06 62 70 12 34 | www.fairtrust.com
9 allée du bois Louët 35235 Thorigné-Fouillard

Description et produits

FairTrust conçoit des solutions de cybersécurité performantes, modernes et rapidement opérationnelles, conformes aux exigences gouvernementales, afin de **renforcer la sécurité des accès au SI** pour les entreprises de tous secteurs et de toutes tailles et les établissements de santé.

Nos produits Cloud ou On-Premises sont disponibles rapidement **sans avoir besoin d'infrastructures complexes ou de ressources importantes** et apportent une réponse basée sur des technologies à la pointe de l'état de l'art :

- **FairTrust SSO & FairTrust Vault :** solution complète de coffre-fort, d'authentification forte et d'authentification unique (SSO).
- **FairTrust IAM :** Gestion des identités et des habilitations contribuant à une approche « Zero Trust » basée sur le principe de moindre privilège en attribuant automatiquement aux utilisateurs uniquement les droits nécessaires pour remplir leurs rôle ou fonction, au bon moment.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Filigran

Informations contact

Samuel Hassine | samuel.hassine@filigran.io | https://filigran.io

Description et produits

Filigran, cybertech créée en 2022, propose des solutions de cybersécurité open source couvrant **la gestion du renseignement sur les menaces** (Threat Intelligence), **la simulation d'attaques** (Breach & Attack Simulation) et **le management des risques cyber**. Elle propose une suite de solutions appelée « Filigran eXtended Threat Management (XTM) », composée actuellement de deux solutions :

- **OpenCTI :** plateforme conçue pour organiser, stocker et opérationnaliser les informations de renseignement sur les menaces à un niveau technique technique et stratégique ;
- **OpenBAS :** plateforme de simulation d'attaques permettant d'identifier les éventuelles lacunes dans la posture de cybersécurité d'une entreprise.

Plus de 4 200 organisations à travers le monde utilisent les solutions, et deux autres produits sont en cours de développement pour compléter la vision et la stratégie de Filigran.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

GATEWATCHER

Informations contact

contact@gatewatcher.com | www.gatewatcher.com

Description et produits

Leader dans la **détection des cybermenaces**, Gatewatcher protège depuis 2015 les réseaux critiques des grandes entreprises et des institutions publiques à travers le monde.

Nos solutions de Network Detection and Response (NDR) et de Cyber Threat Intelligence (CTI) vous permettent d'**identifier et de caractériser au plus tôt toutes types de menaces**, afin d'engager des actions de remédiation globale et d'en minimiser immédiatement l'impact.

Par **l'association de l'IA à des techniques d'analyses dynamiques**, Gatewatcher vous offre une vision à 360° et en temps réel des cybermenaces sur l'ensemble du réseau, dans le cloud et on premise.

« Secured by design », notre NDR qualifié permet de répondre efficacement aux enjeux réglementaires majeurs (PDIS, NIS 2, DORA, CRA, etc.) et garantit une détection renforcée sur l'ensemble de vos infrastructures, notamment sensibles et déployées hors-ligne.

CSPN ; Qualification élémentaire

Référentiel NIS 2

Art.21.2.a : Politique relative à l'analyse des risques et de la sécurité des systèmes d'information.

Art. 21.2.b : Gestion des incidents

Art.21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

GLIMPS

Informations contact

Aurélie BELTRAMINO | aurelie.beltramino@glimps.re
06 38 56 45 46 | www.glimps.fr
1137A Av. des Champs Blancs 35510 Cesson-Sévigné

Description et produits

GLIMPS est le spécialiste français de l'analyse de fichiers en vue de détecter et de caractériser les menaces avancées en quelques secondes. GLIMPS a développé un moteur unique d'IA basé sur le Deep Learning qui détecte toute forme de Malware au sein des fichiers par comparaison de code.

- **GLIMPS Malware Kiosk** est un portail simple à travers lequel chaque collaborateur peut tester ses fichiers et obtenir rapidement un verdict compréhensible.
- **GLIMPS Malware Detect** permet la détection avancée des fichiers malveillants. Après analyse inférieure à 3 s, GLIMPS Malware Detect renvoie un verdict immédiat aux applications.
- **GLIMPS Malware Expert** est l'outil d'expertise pour des travaux de qualification des alertes et de la menace, d'investigation et de réponse à incident. Il permet l'automatisation de la totalité des tâches de malware forensics et threat hunting et une diminution du MTTR de 70 %.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'informations

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

Stanislas de Truchis | stanislas.detruchis@harfanglab.fr
06 61 84 73 80 | https://harfanglab.io/
Campus Cyber, 5-7 rue Bellini 92800 Puteaux

Description et produits

Conscient qu'offrir une excellente capacité de détection est le strict minimum pour un EDR. HarfangLab est devenu le leader de sa catégorie en travaillant sur deux axes :

- améliorer l'environnement de travail des analystes et des équipes de réponses à incident
- favoriser la mise en application de la roadmap cyber identifiée par les RSSI

HarfangLab s'attache à proposer **la meilleure technologie de protection au niveau des terminaux**.

Depuis 2018, l'EDR HarfangLab se distingue par :

- ses hautes capacités de **détection et de réponse à incident**, notamment via son IA et ses nombreuses automatisations ;
- sa **transparence**, l'ensemble des règles de détection sont visibles par les équipes SOC pour leur permettre d'appréhender au mieux les évènements de sécurité ;
- son ouverture et ses nombreux connecteurs pour favoriser une intégration et une **interopérabilité** efficace avec vos autres solutions.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

Marc OLIVIER | marc.olivier@hiasecure.com
06 85 54 13 56 | https://hiasecure.com
14 rue Beffroy 92200 Neuilly-sur-Seine

Description et produits

HIAsecure propose des services d'authentification sur une base cognitive (user friendly), pour prévenir les usurpations et attaques automatisées contre les comptes de ses clients. Cette technologie est plug & play, s'adapte facilement à tous les systèmes modernes d'authentification en étant pris en compte comme un facteur additionnel (MFA).

Produit d'authentification cognitive 'plug&play', disponible pour une installation immédiate.

Produit adapté à tout type de support, d'activité et d'environnement. Le service s'adapte aux équipements, services et Applications déjà opérationnels.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Informations contact

contact@holiseum.com | www.holiseum.com
Tour Légende — 20 place de la Défense 92800 Puteaux

PASSI

Description et produits

HOLISEUM est spécialiste en **cybersécurité des infrastructures critiques et industrielles** avec une vision globale, dite holistique, de la sécurité. Société française indépendante à rayonnement en France et à l'international, HOLISEUM est qualifié PASSI par l'ANSSI sur l'ensemble des portées d'audit.

HOLISEUM est reconnu pour ses innovations telles que le 1er **« Tir à Blanc de Ransomware® »** du marché. Solution inédite permettant connaître le niveau d'exposition de son organisation face aux ransomwares, le Tir à Blanc de Ransomware® est désormais référencé à l'UGAP (Réf. 6008784).

HOLISEUM propose de nombreux services clé en main :

- **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.
- **SÉCURISER :** Accompagnement, cadrage et intégration de solutions cybersécurité.
- **FORMER :** Sensibilisation et formation aux problématiques de la cybersécurité.
- **INVESTIGUER :** Faire la lumière sur les compromissions avérées ou supposées.

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Informations contact

Joffrey Rigaudie | sales-ilex@inetum.fr | 04 42 72 10 50
www.ilex-international.com
7 Rue Touzet Gaillard 93400 Saint-Ouen

Description et produits

Découvrez la puissance de la plateforme Ilex IAM : avec une base solide de plus de 300 clients, notre solution incarne l'excellence en matière de sécurité, de flexibilité avec une expérience utilisateur fluide.

Nos produits répondent aux exigences les plus strictes en matière de réglementation (LPM, NIS2, DORA, RGS & eIDAS) et offrent une gamme complète et **un déploiement flexible on premise ou SaaS** :

- **Ilex Identity Management :** Gestion efficace du cycle de vie des utilisateurs, du provisioning des comptes et des droits.
- **Ilex Access Management :** Authentification forte et adaptative, un SSO robuste, et une fédération d'identité sans faille.
- **Ilex CMS :** Gestion du cycle de vie des tokens et des cartes, pour le contrôle d'accès physique (MIFARE DESFIRE) et logique (PKI & FIDO).
- **Ilex CIAM :** Gestion optimale des identités et des accès des clients, des patients, des citoyens, et bien plus encore.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

INQUEST

Informations contact

PAILLET Gaël | gael.paillet@inquest-risk.com
01 81 93 52 00 | www.inquest-risk.com
15 rue Jean Jaurès, Campus Aviso,
Bâtiment B 92800 Puteaux

Description et produits

Inquest propose des services de conseil, d'audit et de formation pour aider les entreprises à identifier et à réduire leurs risques cyber.

Inquest dispose d'un centre d'intervention en cybersécurité (CSIRT) qui est disponible 24h/24 et 7j/7 pour répondre aux incidents cyber.
Ces services comprennent :

- **le diagnostic, l'établissement du plan d'action et son pilotage** pour se mettre en conformité avec les réglementations ou normes (RGPD, DORA, NIS2, ISO 27001, CIS CSC, etc)
- **l'audit organisationnel** de la sécurité des systèmes d'information
- la mise en place de **politiques de sécurité informatique**
- **la sensibilisation** des collaborateurs aux risques cyber
- **l'accompagnement MOA en cybersécurité**

Le CSIRT est disponible 24x7 pour répondre aux incidents cyber : mesures conservatoires, investigation, communication de crise, accélération de la reconstruction et renforcement des SI et de leur sécurité, RETEX.

FRANCE CYBER SECURITY — EXPERT CYBER

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

INSPEERE

Informations contact

Michaël Ferrec | michael@inspeere.com | 06 88 89 94 70
www.inspeere.com | 24 boulevard du Grand Cerf 86000 Poitiers

Description et produits

Inspeere propose **DATIS**, une solution de sauvegarde exclusive et brevetée par le CNRS et l'UCA.

DATIS chiffre, fragmente et distribue les données sur un réseau sécurisé, garantissant leur intégrité et confidentialité. Elle offre **une souveraineté totale** aux utilisateurs, répondant ainsi aux exigences de NIS2. En favorisant **une approche écoresponsable**, DATIS réduit l'empreinte carbone en évitant les data centers. Une solution complète et éthique pour protéger les données critiques des entreprises..

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Informations contact

Mickaël ATTIAS | mickael.attias@ise-systems.fr
01 85 78 59 76 | https://ise-systems.fr
259 rue Saint-Honoré 75001 Paris

Description et produits

ISE SYSTEMS est un cabinet Cyber Data Cloud Hybride qui allie une forte expertise opérationnelle, consolidée par le développement de solutions innovantes telles que Cyber Résilience 360°, plateforme gamifiée immersive d'entraînement et de sensibilisation à la gestion de crise Cyber, ainsi qu'un centre de service managé avancé de réponse à incidents et de Red Timing.

L'offre **Cyber Résilience 360°** s'appuie sur des plateformes de simulation d'attaques hyperréalistes. La maîtrise de la plateforme permet aux experts cyber ISE SYSTEMS d'organiser des sessions d'entraînements et formations proches de la réalité comme dans un SOC, et adaptées aux besoins des équipes chargées de cyber défense et des risques.

Un parcours de cyberformations individuelles gamifiées, full cloud permet aux participants de remplir des missions de cyberdéfense ou d'Ethical hacking. Les participants acquièrent des compétences, améliorent et évaluent leurs performances en se formant dans des infrastructures simulées du monde réel.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

---

Informations contact

Bounakhla Faouzi | fbounakhla@itrust.fr
M : +33 (0)7 86 00 51 54 | B : +33 (0)1 80 87 83 62
www.itrust.fr | Siège : 1253 L'Occitane, 31670 Labège
Agence Paris : 6 rue du 4 Septembre, 92130 Issy-les-Moulineaux

PASSI

Description et produits

Plus de 1 300 entreprises et collectivités françaises nous font déjà confiance pour les **protéger quotidiennement contre les cybermenaces**.

Editeur de solutions souveraines et prestataire de services cyber depuis 2007, notre expertise est reconnue au travers d'un catalogue unique de solutions :

- La prévention grâce à **IKare**, notre scanner de vulnérabilités ;
- La détection grâce à **Reveelium**, notre plateforme SIEM UEBA dopée à l'IA ;
- La surveillance est assurée par **nos SOC** et **notre offre EDR Managé** offrant interventions rapides et remédiations automatisées en 24x7.

Conformes aux réglementations (NIS, RGPD, ISO27XXX), nous sommes certifiés PASSI, ISO 9001, garantissant excellence en cybersécurité.

Enfin, l'entrée du Groupe iliad au capital de ITrust affirme notre volonté de démocratiser la cybersécurité et la rendre accessible à tous les budgets. Rejoignez-nous !

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

JALIOS

Informations contact

Jean-François Pellier | jean-francois.pellier@jalios.com
01 39 23 92 80 | www.jalios.com
58 rue Pottier 78150 Le Chesnay-Rocquencourt

CSPN

Description et produits

Jalios fournit **une plateforme digitale souveraine et sécurisée** pour rendre durablement l'organisation plus efficace et le travail de chacun plus épanouissant.

Disponible en SaaS hébergé en France, en région SecNumCloud et en cloud privé, sa solution JPlatform détient le visa de sécurité CSPN de l'ANSSI.

À la fois puissant CMS et plateforme d'expérience collaborateur, elle est utilisée en tant qu'Intranet, Digital Workplace, suite bureautique collaborative, GED, plateforme collaborative de gestion de crise, de gestion de données sensibles, extranet, bases de connaissances ou digital learning.

Labellisé Numérique Responsable, Jalios compte près de 500 clients : des administrations centrales (DINUM, DGFIP, AMF...), des collectivités territoriales (Pas-de-Calais, Nantes Métropole, Région Grand-Est...) et des entreprises privées de toute taille (Système U, La Redoute, Indigo, MAIF, MGEN...).

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Jamespot.

Informations contact

Alain GARNIER | alain.garnier@jamespot.com | 01 48 58 18 01
www.jamespot.com
66 rue Marceau — Bât. C' — 93100 Montreuil

Description et produits

Créé en 2005, Jamespot est le 1er éditeur de solutions collaboratives dans le Cloud français. Jamespot conçoit des solutions numériques personnalisables qui améliorent l'expérience collective des équipes et des organisations, tout en garantissant un déploiement rapide et sans développement à travers 3 offres.

- **Fast Intranet** | L'intranet collaboratif pour un système d'information unique axé sur une communication fluide.
- **Open Agora** | Le réseau social d'entreprise, centré autour de la collaboration et l'optimisation des échanges transverses.
- **Smart Place** | La Digital Workplace qui réunit le meilleur de Fast intranet et d'Open Agora pour un outil dédié aussi bien à la collaboration que la communication.

Jamespot propose également 3 offres dédiées à la sécurité :

- L'offre **Vault** dédiée aux grandes entreprises
- L'offre **HDS** dédiée aux données de santé
- L'offre **SecNumCloud** pour répondre aux enjeux de souveraineté

La solution Jamespot est aujourd'hui utilisée par plus 350 organisations et plus de 400 000 professionnels à travers le monde.

Référentiel NIS 2

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

LAGERTHA

Informations contact

Marie-Gabrielle CORONA | marie-gabrielle@lagertha.tech
06 71 82 60 61 | https://lagertha.tech
Cité de l'Entreprise, 200 bd de la Résistance 71000 Mâcon

Description et produits

Lagertha étend votre cyberprotection en rendant confidentielles vos données. S'appuyant sur **les plus hauts standards cryptographiques**, Lagertha rend caduc le risque de fuite des données en créant rapidement une architecture Zéro Trust.
Créez votre environnement Zéro Trust, grâce à plusieurs SDK et produits :

- **Lagertha-API :** permet aux équipe IT, d'intégrer rapidement du chiffrement de bout-en-bout dans vos Software pour protéger vos données en transit et en stockage. Zero Trust by design. Le système est déployable sur tous type d'infrastructure, même legacy.
- **Lagertha-Transfert :** permet aux collaborateurs d'échanger des documents confidentiels par mail sans changer leurs outils bureautiques et de sécuriser le maillon faible de l'organisation : sa boite mail.
- **Lagertha-Storage :** assure la sauvegarder vos projets les plus précieux (moteur d'IA, plans de prototypes, documents sensibles...) afin que seuls les personnes authentifiées y ait accès. Permet la traçabilité des accès et garantit également l'intégrité du projet.

Référentiel NIS 2

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

leviia

Informations contact

Quentin Maury | quentin.maury@leviia.com | 07 45 89 16 66
www.leviia.com | 14 Av. de l'Europe 77144 Montévrain

Description et produits

Leviia est une entreprise française qui fournit des solutions de stockage de données souveraines, sécurisées et économiques. Géo-répliqués et certifiés ISO27001 & HDS, nos services — adaptés aux entreprises, aux administrations et aux revendeurs / intégrateurs de toutes tailles — comptent aujourd'hui plus 300 000 utilisateurs uniques.

- **Leviia Stockage Objet :** au minimum 80 % moins cher qu'Amazon S3, structure tarifaire transparente et prévisible. Idéal pour vos sauvegardes externalisées. Compatible API S3 et tout logiciel supportant ce protocole (Veeam, Rubrik, Commvault, MSP360, Atempo, Synology, QNAP, etc.)
- **Leviia Drive Pro :** stockage, partage, édition, collaboration, agenda... pour protéger les données de votre organisation et collaborer avec vos équipes sur un cloud professionnel 100 % français.
- **Leviia Next :** déploiement sur-mesure de Nextcloud dans votre organisation à haute volumétrie de stockage et d'utilisateurs. Leviia est certifiée Nextcloud Platinium.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

LOGIN SÉCURITÉ

Informations contact

Antoine PATOIS | antoine.patois@login-securite.com
06 88 25 11 43 | www.login-securite.com
199 bureaux de la colline 92210 Saint-Cloud

Description et produits

Login Sécurité accompagne ses clients dans l'**évaluation de leur sécurité** et la **mise en œuvre de solutions opérationnelles** de protection et de réaction.

Login Sécurité accompagne les DSI dans la définition et la mise en œuvre de leur stratégie de Confiance Numérique en s'appuyant sur **des offres couvrant l'ensemble du cycle de vie de la sécurité**, de l'identification des risques aux services opérationnels de surveillance et d'action.

Nos équipes délivrent des prestations de conseil, d'intégration, de services managés et de formation, adaptées aux contraintes de nos clients, sur site ou depuis notre centre de Cybersécurité.

L'offre de Cybersécurité de Login Sécurité couvre l'ensemble du cycle de vie de la sécurité, de l'identification des risques aux services opérationnels de surveillance et d'action.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité
Art. 21.2 : Protection de l'environnement physique des réseaux et systèmes d'information
Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information
Art. 21.2.b : Gestion des incidents
Art. 21.2.c : Continuité des activités
Art. 21.2.d : Sécurité de la chaîne d'approvisionnement
Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité
Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

MAILINBLACK

Informations contact

MARET Laura | lmaret@mailinblack.com | www.mailinblack.com
4 Place Sadi-Carnot, 13002 Marseille

Description et produits

Mailinblack est le leader européen de la protection cyber de l'utilisateur. Entreprise française forte de 20 ans d'expertise en sécurité, R&D et intelligence artificielle, Mailinblack propose l'offre de cybersécurité la plus complète du marché. Ses **solutions de protection mail, web, gestion et sécurisation des mots de passe, et de sensibilisation et formation** des collaborateurs permettent aux entreprises et organisations publiques **une protection à 360°**. Ses 22 000 clients font confiance à Mailinblack pour son expertise, la performance de ses solutions et leur facilité de prise en main.

- **Protect :** sécurisation de messagerie
- **Cyber Coach :** sensibilisation aux cyber menaces
- **Cyber Academy :** plateforme e-learning de formation à la cybersécurité
- **Sikker :** gestionnaire de mots de passe

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité
Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

MAKE IT SAFE

Informations contact

Longepe Clément | clement.longepe@makeitsafe.fr | 09 72 11 71 86
www.makeitsafe.fr | 1 bd Jean Monnet 44400 Rezé

Description et produits

Make IT Safe est le logiciel métier français, commun aux RSSI, DPO et consultants, pour **maîtriser le risque** et r**éussir sa conformité cybersécurité & RGPD**.

Créé en 2018, c'est aujourd'hui plus de 150 clients équipés et satisfaits car c'est la solution la plus simple, complète et collaborative.

Make IT Safe, c'est aussi **une équipe d'experts et passionnés**, basée en France. Notre solution logicielle est également développée et hébergée en France.

Make IT Safe, c'est le tableau de bord RSSI & DPO avec une plateforme unique pour évaluer et piloter efficacement votre gouvernance et conformité cybersécurité & RGPD.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Mathias Avocats

Informations contact

MATHIAS Garance | gmathias@avocats-mathias.com
06 15 91 44 07 | www.avocats-mathias.com
19 rue de Vernier, 75017 Paris

Description et produits

Par leur complémentarité et pluridisciplinarité, les équipes de Mathias Avocats accompagnent leurs clients sur tous sujets liés au **droit du numérique, technologies & innovations, cybersécurité, conformité** (RGPD, loi Sapin 2, etc.) **et affaires publiques**.

- Enjeux de **contrats** IT, Cloud, ERP, SOC, etc. ;
- **Faisabilité juridique** d'un projet et sa mise en œuvre (en tenant compte de tous les aspects : IA, OSINT, compliance...) ;
- **Veille et préconisations opérationnelles** sur les législations impactant l'activité de nos clients (le développement et l'anticipation de leur business) et sur les textes européens (NIS 2, DORA, Data Governance Act, etc.) ;
- **Formation** (Qualiopi).

Le cabinet intervient plus spécifiquement au Canada (Québec) aux côtés d'un cabinet dédié à la protection des données (notamment sécurisation des transferts) et intervient en cas de litiges (gestion de risques, contentieux).

« *A chaque client, un accompagnement sur-mesure, pour transformer les évolutions réglementaires en opportunités business* ».

Référentiel NIS 2

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

merox
DNS SECURITY & DMARC

Informations contact

Murielle BOCHATON | murielle.bochaton@merox.io | 06 67 29 78 25
www.merox.io | 836 rue du mas de Verchant 34000 Montpellier

Description et produits

Merox est un éditeur français spécialisé en cybersécurité, salué par Gartner, offrant une surveillance des noms de domaine, messageries et emails via sa plateforme SaaS :

- **Cartographie, Maîtrise DNS Complète :** permet aux entreprises de visualiser, de contrôler l'intégralité de leur environnement DNS, offrant une visibilité sur les configurations et les vulnérabilités.
- **Surveillance, Vérification des Entrées DNS :** Merox aide les organisations à identifier, à résoudre les anomalies, renforçant la résilience de leur infrastructure.
- **Surveillance Emails :** Merox facilite l'adoption des protocoles de sécurité tels que SPF, DKIM, DMARC et BIMI pour garantir la conformité des emails, réduire les risques de phishing, protéger la réputation de la marque.
- **Alertes Sécurités :** veille constante, alertant les équipes en cas d'attaques, de modifications non autorisées sur leurs domaines.
- **Surveillance des Domaines Proches :** garantissant que les domaines similaires ne sont pas exploités pour des activités malveillantes (typosquatting).

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

METSYS

Informations contact

THIBAULT Hervé | contact@metsys.fr | 01 81 89 19 70
www.metsys.fr | 121 rue d'Aguesseau 92100 Boulogne Billancourt

Description et produits

Metsys, **acteur de proximité et acteur clé de votre cyber-résilience** — 500 personnes en IDF + 11 agences en région — Conseil, Intégration (architecture, expertise), 2 centres de service Cloud (Microsoft 365, Azure) et Cybersécurité (SOC/MSSP)

Metsys associe l'expertise pointue de ses consultants associée à son réseau de partenaires de confiance, pour anticiper vos risques, mettre en place une gouvernance solide et sécuriser les 6 piliers de votre SI (Identité, EndPoint, Infrastructure & Réseau, Data, Applications et Outils Collaboratifs) avec ARMI360 by Metsys :

- **Anticipate — Prévenir & détecter** : CTI, VOC, SOC, GRC
- **Resist — Sécuriser vos SI** : Expertise AD, Entra, Microsoft 365, Azure
- **Mitigate — Réagir, intervenir & réparer** : SOC, CERT
- **Improve — Superviser & gouverner** : SOC, GRC

EXPERT CYBER

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

mindflow

Informations contact

Paul-Arthur Jonville | https://mindflow.io
128 rue la Boétie 75008 Paris — France

Description et produits

Mindflow est **une plateforme d'automatisation et d'orchestration no-code révolutionnaire** pour les équipes de Sécurité, IT et Cloud.

Simplifiant la suppression des tâches répétitives, elle connecte aisément tous vos outils sans nécessiter de compétences en codage. Sa technologie unique propose **un catalogue d'intégrations sans égal**, enrichissant l'automatisation avec des fonctionnalités d'IA avancées pour la cybersécurité : suggestions, génération automatique d'automatisations, et agents AI autonomes.

Mindflow booste ainsi la performance opérationnelle, renforce la sécurité et la gouvernance des entreprises.

Reconnue pour son innovation, Mindflow a été honorée par **des prix prestigieux** comme la Meilleure Start-Up Cyber Européenne par l'ECSO, Most Promising Tech Startup par Rothschild, et le Prix du FIC.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

MOABI

Informations contact

Nicolas GAUME | nicolas.gaume@moabi.com
06 45 26 64 22 | https://moabi.com
535 Route des lucioles 06560 Valbonnes

Description et produits

MOABI est une entreprise de cybersécurité spécialisée dans la sécurité produit et logicielle. Nous travaillons sur **des technologies de ruptures, totalement innovantes**. Notre but est d'accompagner nos clients afin de sécuriser leur processus de développement ainsi que leur supply chain.

Pour ceci nous avons développé des solutions techniques permettant de réaliser des **audits de logiciels de façon automatique** afin de gagner en temps, en efficacité et de se concentrer sur la remédiation. Du fait que nous n'ayons pas besoin du code source, nous travaillons également avec certains clients à la formulation d'exigences cyber à destination de leur fournisseur. Grâce à cela ils peuvent évaluer la posture sécurité des livrables fournisseurs et les renvoyer en développement si ceux-là ne matchent pas les exigences cyber.

Référentiel NIS 2

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Informations contact

contact@n-cyp.com | 02 50 85 87 36
www.n-cyp.fr
82 Avenue de Thiès 14000 Caen

Description et produits

N-CyP s'est créée avec la volonté d'apporter un haut niveau de protection cyber aux acteurs Mid-Market et collectivités de tailles petites à moyennes. Notre SOC s'appuie sur des technologies Françaises ou Européennes les plus avancées du marché afin de garantir la qualité de nos prestations. Nous avons une capacité reconnue à nous interconnecter à des environnements complexes pour garantir la qualité de supervision de la cybersécurité Nos équipes de réponses à incident interviennent pour stopper les attaquants et rétablir un environnement fiable.

- **SOC Managé :** Le SOC agrège les sondes de sécurité à disposition (Firewall, EPP, EDR, NDR, DLP,..) pour détecter les attaques potentielles le plus tôt possible et adopter les postures de lutte nécessaires
- **CSIRT :** le CSIRT N-CyP agit lors de cyber attaques afin d'appliquer les procédures d'urgence, d'analyse et de remédiation adaptées à la situation de crise.
- **MicroSOC EDR :** Sécurisation basique des postes & serveurs via un EDR managé par nos équipes de surveillance — Maintien en condition opérationnelle.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Informations contact

Murielle Bochaton | murielle.bochaton@nameshield.net
+33 6 67 29 78 25 | www.nameshield.com
39 boulevard des Capucines 75002 Paris

Description et produits

Depuis 30 ans, Nameshield protège les noms de domaine stratégiques de ses clients contre les cybermenaces.

Certifiée ISO 27001 et disposant d'un CERT, Nameshield évolue au cœur de l'écosystème cybersécurité et anticipe les défis actuels et futurs des entreprises et administrations.

Nameshield apporte **une réponse unique pour couvrir la surface d'attaque des actifs numériques**, en proposant des solutions de gestion et de sécurisation :

- **Risques administratifs :** service et plateforme avancés de gestion des noms de domaine.
- **Risques techniques :** accès renforcés, infrastructures DNS Premium anycast, DNSSEC, certificats, DMARC...
- **Risques d'usurpation :** surveillance du territoire numérique (cybersquatting, Fake Shops, logos...), actions de lutte et remédiation.

Référentiel NIS 2

Art. 20 Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

LEMAIRE BENOIT | blemaire@lsngroupe.com
01 53 25 46 27 | www.neotech-assurances.fr
39, rue Mstislav Rostropovitch 75017 Paris

Description et produits

Neotech Assurances est un courtier en assurance spécialisé dans **la gestion des risques et des assurances** des sociétés des Hautes Technologies (Informatique, Télécom, Média et Internet). Ils offrent **des produits d'assurance adaptés** aux professionnels de l'informatique, des éditeurs de logiciels, des spécialistes des télécommunications et d'Internet 2.

Leur expertise comprend l'analyse des risques, les audits réguliers des contrats d'assurance, la veille juridique et technologique, les interventions lors de conférences, la participation aux commissions de Syntec Numérique Assurances et de l'Association du Droit des Robots, la cartographie des risques des métiers du numérique et la cartographie des cyber-risques 2.
Ils proposent également des offres sur mesure pour les entreprises issues des nouvelles technologies.

Référentiel NIS 2

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Informations contact

Kim-Thibault DANG-HEUDEBERT | kim@neotrust.io
+33 6 15 77 92 23 | www.neotrust.io
5 rue Bellini, 92800 Puteaux

Description et produits

NEOTRUST, **spécialiste en transformation sécurité**, vous accompagne dans la définition et l'exécution de votre stratégie cyber tenant compte de votre contexte business.

Avec notre gamme de services, nous aidons nos clients à renforcer leur posture sécurité pour lutter contre la cybercriminalité et protéger leurs données.

Domaines d'intervention :

- RSSI à temps partagé : intervention de CISO expérimentés pour définir, piloter l'exécution de stratégies sécurité innovantes.
- Audit et Conseil : évaluations des risques pour renforcer la sécurité des processus et des infrastructures.
- Gouvernance, Risques et Conformité : mise en conformité NIS2, RGPD, DORA, NIST CSF, et certifications ISO/IEC 27001, 22301, 9001 et 14001.
- CERT as a Service : renforcement de vos défenses avec la surveillance du Dark Web, Purple Team, évaluation du SOC, Réponse à incident...
- Expertises en cybersécurité : délégation d'experts
- Formation et Sensibilisation
- Cabinet de recrutement : chasse de profils en CDI jusqu'au C-level (CISO, Head of SOC, Manager Cyber, etc.).

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

NEOWAVE

Informations contact

Corinne JOACHIN | corinne.joachin@neowave.fr
04 42 50 70 05 | www.neowave.fr
Pôle d'Activités Yvon Morandat, 1480 rue d'Arménie 13120 Gardanne

CSPN

Description et produits

NEOWAVE est une entreprise française spécialisée dans **l'authentification forte et les transactions sécurisées**. Sa 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.

Ses solutions adressent les marchés de la cybersécurité, de la confiance numérique et de la gestion des identités.

Ses produits comprennent **des clés de sécurité**, **des cartes à puce** et **des lecteurs de badge**, tous fabriqués en France. Ils portent le label « Cybersecurity Made in Europe » et respectent les normes de sécurité européennes (RGS, eIDAS, NIS, DSP2...). Ses clés de sécurité FIDO2 (compatibles avec les standards FIDO U2F et FIDO2) sont par ailleurs certifiées par l'ANSSI. En outre, NEOWAVE est partenaire de Microsoft pour ses **solutions d'authentification « passwordless »** (FIDO2).

Référentiel NIS 2

Art. 21.2 : Protection de l'environnement physique des réseaux et systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

NetExplorer

Informations contact

Charles-Étienne GARIEL | charly@netexplorer.fr
06 73 32 81 44 | www.netexplorer.fr
Bâtiment Gamma, 11 Bd Deodat de Sévérac 31770 Colomiers

Description et produits

Le spécialiste français du partage de fichiers, du travail collaboratif et du stockage en ligne depuis 15 ans.

Depuis 2007, NetExplorer propose **une solution Cloud de gestion de fichiers** qui vous accompagne dans toutes les étapes du cycle de vie de vos documents, accessible de n'importe où et qui offre des exigences fortes en matière de sécurité.

Nous disposons d'un contrôle et d'une maîtrise totale de la solution, du **développement logiciel réalisé en interne** par nos équipes jusqu'à **l'infrastructure d'hébergement 100 % souveraine** et française.

NetExplorer c'est aussi plus de 30 de collaborateurs qui œuvrent chaque jour à délivrer un service performant et sécurisé à tous les utilisateurs de la solution pour faciliter la gestion de leurs données et les protéger en toutes circonstances.

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

Jocelyne Kauffmann | contact@numspot.com
06 15 21 44 93 | www.numspot.com
La Défense. 110, Esplanade du Général de Gaulle
Cœur Défense — Tour A, 11ème étage CS 80 371
92931 Paris

Description et produits

NumSpot est un acteur du cloud souverain et de confiance.
Issu de la volonté de quatre entreprises de premier plan du public et du privé, (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom,) NumSpot propose une offre de cloud indépendante, souveraine et robuste adossée sur le IaaS de OUTSCALE qualifié SecNumCloud. NumSpot est un cloud robuste, réversible et transparent basé principalement sur l'open source et des solutions européennes.

L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, banque/finance/assurance, OIV/OSE) en France et en Europe qui recherchent une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot propose **des sevices de cloud public** (Iaas, Paas, Saas). L'utilisation de son infrastructure qualifiée SecNumCloud facilitera votre mise en conformité NIS2

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Art.21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Informations contact

Gadrat Emeric | egadrat@olfeo.com | 07 85 16 53 65
www.olfeo.com | 4 rue de Vantadour 75 001 Paris

Description et produits

Olfeo est le leader européen de la sécurité web. Ses solutions de passerelle de sécurité web protègent les entreprises des contenus malveillants ou illicites et sécurisent le trafic web des utilisateurs. Son **approche unique du filtrage par liste blanche (le Trust-Centric)** permet d'offrir le plus haut niveau de sécurité pour les entreprises en n'autorisant l'accès qu'à des contenus préalablement vérifiés. L'offre de sécurité est complétée par une solution de formation aux risques et enjeux de cybersécurité

Les solutions allient

- Sécurisation intégrale du trafic web grâce au filtrage avancé des contenus, un antivirus de flux pour neutraliser les malwares, le déchiffrement TLS pour sécuriser les flux https, le filtrage DNS, etc. ;
- Flexibilité des déploiements, en SaaS pour la simplicité et la rapidité, en on-premise pour la flexibilité et personnalisation ;
- Protection juridique adaptée.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

AVOCAT
Olivier Weber

Informations contact

Weber Olivier | o.weber@ow-avocat.com
06.60.91.33.07 | https://weber-avocat.com
14 rue Perchepinte 31000 Toulouse

Description et produits

DPO et gouvernance des données

« À la création du cabinet, l'empreinte était encore fraîche de mes vingt ans passés à la direction générale d'une entreprise française de taille intermédiaire et de dimension internationale, de mon expérience de la mise en œuvre des processus normatifs et du rôle clé joué par les DSI dans tout projet stratégique. »

Les éléments étaient réunis pour que le Cabinet se tourne vers **la mise en œuvre du RGPD en Entreprise** dont la réussite est conditionnée à la capacité à fédérer les équipes et à définir un projet intégrable au fonctionnement de la structure.

Olvid

Informations contact

Cédric Sylvestre | cedric.sylvestre@olvid.io | 06 77 58 23 41
www.olvid.io/fr | 26 rue Vignon 75009 Paris

CSPN

Description et produits

Olvid est une société experte en **cryptographie**. Elle propose **la seule messagerie instantanée certifiée par l'ANSSI**. Nos protocoles cryptographiques permettent de prouver mathématiquement l'impossibilité pour un tiers de prendre connaissance des communications.

L'utilisation d'Olvid est stratégique dans un contexte croissant de cyberattaques et de la nécessité d'avoir recours à des solutions souveraines, sans jamais céder la moindre donnée à l'éditeur. Olvid permet en effet de **poursuivre les communications pendant une crise informatique**, respecte le RGPD, et s'affranchit des solutions étrangères soumises à des lois extra-territoriales.

Dans le cadre de l'offre Olvid Entreprise, vous avez accès à une console d'administration qui vous permet de déployer et de piloter Olvid très facilement et vos utilisateurs entrent en contact les uns avec les autres en un seul clic.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Informations contact

Pfender Delubac Elisée
elisee.pfenderdelubac@on-x.com
+33 (0) 6 46 91 92 15 | www.on-x.com
15, quai de Dion Bouton 92816 Puteaux cedex

PASSI

Référentiel NIS 2

Art. 21.2 : Protection de l'environnement physique des réseaux et systèmes d'information

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Description et produits

ON-X, cabinet français indépendant de conseil et d'expertise, est spécialisé dans **l'intégration du numérique** dans les entreprises, les administrations et les collectivités.

Bénéficiant de plus de 30 ans d'expérience, **ON-X est organisé autour de 5 expertises et 5 bureaux** (Paris, Toulouse, Montbéliard, Lyon, Laval) qui accompagnent nos clients successivement à définir la stratégie de transition, à passer les grandes étapes d'aide à la décision, à architecturer puis à conduire leurs projets de mise en œuvre et enfin à piloter les services délivrés.

Labellisé French Tech au titre de son affiliation avec Laval Virtual University, ON-X est l'une des 12 entreprises innovantes en réalité virtuelle et augmentée, qui obtient ainsi ce prestigieux label sur le réseau thématique #EdTech #Entertainment, valorisant les technologies du numérique pour l'éducation.

Les compétences du groupe **couvrent l'ensemble du cycle de vie des systèmes** : audit, conception, déploiement et conduite du changement et enfin exploitation. Elles sont organisées autour d'offres globales portées par des équipes constituées de consultants-managers, consultants seniors et consultants. Nous sommes certifiés ISO 9001.

Informations contact

Geffray Maxime | m.geffray@oodrive.com
06 59 00 90 47 | www.oodrive.com
26 rue du Faubourg Poissonnière 75010 Paris

SecNumCloud

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité
Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information
Art. 21.2.b : Gestion des incidents
Art. 21.2.c : Continuité des activités
Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité
Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Description et produits

Oodrive est leader européen de la suite collaborative de confiance. Fort de plus de 3 500 clients dans 45 pays, Oodrive garantit la confiance numérique à un million d'utilisateurs avec des **solutions collaboratives françaises qui assurent sécurité, souveraineté et conformité réglementaire** (partage de fichier, meeting, e-signature, sauvegarde, remote browser isolation).

Oodrive **garantit aux Entités Essentielles ou Importantes un niveau inégalé de protection et de confidentialité des données sensibles**. Ses offres sont qualifiées SecNumCloud depuis 2019 et répondent à plus de 400 points d'exigences définis par l'ANSSI. Ses clients et partenaires bénéficient des meilleures pratiques de sécurité, conformes à la directive européenne NIS2 : sécurité SI, RH, analyse de risques, gestion d'incidents, continuité d'activité, accès et authentification, cryptographie, etc.

OUTSCALE

SecNumCloud 3.2

Informations contact

Sales-eu@outscale.com | +33 1 53 27 52 70 | https://fr.outscale.com
1 rue Royale — 319 Bureaux de la Colline 92210 Saint-Cloud

Description et produits

OUTSCALE, marque de Dassault Systèmes, est **le premier opérateur Cloud souverain et durable d'Experience** en tant que service. Métamorphosant la manière dont les organisations fonctionnent, par notre approche du jumeau virtuel, nous donnons aux institutions et entreprises la possibilité d'exploiter pleinement leurs données, optimisant ainsi leurs opérations et favorisant la collaboration dans tous les secteurs. **Nous mettons la souveraineté au cœur de nos solutions**, permettant à nos clients de contrôler intégralement leurs données. En tant qu'acteur responsable, **nous optimisons l'efficacité énergétique de nos infrastructures** et encourageons nos clients à adopter des pratiques soutenables.

OUTSCALE propose 3 modèles de Cloud :

- Cloud Souverain : Cloud public qualifié SecNumCloud 3.2 en France favorisant une collaboration de confiance dans un cadre juridique et fiscal commun. Il dispose aussi des certifications HDS, ISO 27001 et CISPE.
- Cloud Dédié : Cloud clé en main, sur mesure et sur site avec des certifications internationalement reconnues.
- Cloud International : Cloud pour une collaboration sécurisée mondiale, certifié ISO 27001, HDS, CISPE pour un hébergement sécurisé et une protection des données.

Autre :

- OUTSCALE Marketplace : un guichet unique de solutions technologiques.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

OVERSOC
Cybersecurity, loud & clear

Informations contact

Dayez Nicolas | ndayez@gmail.com
0633105044 | www.oversoc.com
47 rue du faubourg de Roubaix 59800 Lille

Description et produits

OverSOC propose **une solution CAASM** (Cyber Asset Attack Surface Management) qui **agrège, corrèle et unifie vos données cyber dans une cartographie 3D** de votre système d'information en temps réel.

Notre interface visuelle innovante, compréhensible et ergonomique, permet aux responsables sécurité et IT de gagner un temps précieux dans le suivi opérationnel : asset management, priorisation des vulnérabilités, suivi de la conformité, réponse à incident.

OverSOC est un cockpit de gestion central pour les DSI / RSSI qui cherchent à maximiser leurs ressources opérationnelles en ciblant les actions de cybersécurité à prioriser en fonction de leur contexte métier.

La solution OverSOC répond à 3 enjeux importants : l'expansion et la complexité croissante de la surface d'attaque cyber à protéger (utilisateurs, machines, applications), l'explosion du nombre d'outils et consoles de cybersécurité pour la maîtriser, le manque de ressources humaines cyber.

FRANCE CYBER SECURITY

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Informations contact

Yves DUFAYET | yves.dufayet@p4 s-archi.com
0684191277 | www.p4 s-archi.com
(Siège) 27 bis rue des Plantes 91230 Montgeron

Description et produits

P4S propose **des équipements réseau** (routeurs, passerelles, chiffreurs) basés sur **une technologie de rupture nommée SOFTLESS**.
Cette solution ne laisse aucune faille logicielle potentiellement exploitable car elle est basée sur une architecture exclusivement matérielle mais reste très souple car reconfigurable à volonté.

En outre cette technologie, permet de disposer de performances inégalées avec **des temps de latences jusqu'à 1000 fois plus faibles que des solutions logicielles classiques** et **une consommation énergétique drastiquement réduite**.

Cette technologie issue de plus de 10 années de recherche est 100 % française, les équipements sont entièrement conçus et fabriqués en France.

Référentiel NIS 2

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Informations contact

Thierry LEBLOND | thierry.leblond@scille.fr
0782078507 | http://parsec.cloud
Campus Cyber de Nouvelle Aquitaine
6 rue Adrienne Bolland 33600 Pessac

CSPN

Description et produits

PARSEC apporte **la garantie cryptographique** que le partage de données sensibles ne peut être ni lu ni modifié par des tiers non autorisés.

Les différenciateurs sont : end-to-end encryption, intégration d'une PKI (Infrastructure de Gestion de Clés), pas d'annuaire central, certification ANSSI, asynchronicité (mode dé/disconnecté natif), open source, Data Zero Trust, pas de limite de volumétrie, et utilisation intuitive.

Les cibles de PARSEC sont les organisations de la finance, de la santé, de technologie, recherche & développement, du juridique ou de la défense et de la sécurité. Il leur apporte une réponse ergonomique aux risques de violation de la confidentialité, à la conformité réglementaire, aux menaces de cybersécurité, à l'intégrité des données, à la complexité des solutions classiques de chiffrement et à la sécurité de la collaboration distante pour un prix abordable.

PARSEC, certifiée CSPN par l'Agence Nationale de Sécurité des Systèmes (https://cyber.gouv.frproduits-certifies/parsec-version-200), est disponible en version SaaS ou « on premise ».

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Patrowl

Informations contact

Gattin Romaric | romaric.gattin@patrowl.io
0768784634 | https://patrowl.io
6 rue du General de Larminat 75015 Paris

Description et produits

Patrowl offre une couverture étendue des risques, incluant les incidents accidentels tels que les certificats périmés, les mauvaises réputations d'adresses IP et les problèmes de configuration d'infrastructures mail. Il adresse également les attaques opportunistes ainsi que les attaques ciblées, assurant une protection complète contre divers scénarios de menace.

Pour remédier à ces risques, l'offre de Patrowl repose sur 4 étapes clés :

- **Cartographie :** surveillez en continu vos actifs.
- **Identification :** détectez en temps réel vos faiblesses et vulnérabilités.
- **Remédiation :** automatisez la correction en un clic.
- **Contrôle :** supervisez les remédiations ou corrections en un clic.

Référentiel NIS 2

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

PRIMX
MAKE ENCRYPTION HAPPEN

Informations contact

Vanessa de CHAMBRUN | business@primx.fr
01 40 95 24 80 | www.primx.eu/fr
21 rue Camille Desmoulins 92130 Issy-les-Moulineaux

Qualification Standard

Description et produits

PRIM'X propose **des solutions de confidentialité** des données stockées, échangées et partagées dans les environnements de travail, locaux, réseaux et Cloud (MS 365).

Ses solutions permettent de protéger les données de l'entreprise contre la perte, le vol, la publication et l'espionnage.

Afin de garantir un haut niveau de confiance à ses clients, PRIM'X a mis **les certifications au cœur de sa Politique Stratégique**. Certifications CC EAL3+, Visa de sécurité ANSSI (Qualification), EU et OTAN Restreint sont renouvelés régulièrement.

Les solutions de chiffrement de PRIM'X équipent + de 2 millions d'utilisateurs en Europe : organisations publiques et privées, tous secteurs, toutes tailles.

- **ZONECENTRAL**, chiffrement des environnements utilisateurs
- **ORIZON,** chiffrement des espaces MS 365 et du cloud
- **. ZED,** échanges de conteneurs ou d'emails chiffrés
- **CRYHOD,** chiffrement des disques des ordinateurs portables

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

PRIVATE DISCUSS

Informations contact

Olivier LACH | o.lach@private-discuss.com | 07 69 24 91 28
https://private-discuss.com | 304 Route Nationale 6 — 69760 Limonest

Description et produits

Private Discuss, **plateforme de visioconférence, messagerie et collaboration**, ON PREMISE (SAAS OVH) **garantit l'absolue protection de vos échanges et communications**.

Private Discuss est 100 % propriétaire de son code, propose 100 % des fonctionnalités et 100 % des performances des leaders américains.

Private Discuss s'adresse, **en priorité, aux secteurs sensibles** (Défense, Recherche, Spatial, Santé, Droit...) et répond aux cas d'usages suivants : communications de crise, secret des affaires, PCA, communication COMEX et Conseil d'Administration, compliance, M&A.

Private Discuss permet des visioconférences jusqu'à 200p et les webinaires jusqu'à 10000p, des appels audio/video et intègre une GED sécurisée avec co-édition, du collaboratif avec un fil d'actualité, un compresseur de PDF, un transfert de fichiers volumineux (jusqu'à 20 Go) et un bridge SIP pour connecter vos salles de visio...

Référentiel NIS 2

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

PRIZM

Informations contact

LETELLIER Guillaume | contact@prizm-security.com
06 59 96 72 89 | www.prizm-security.com
9, rue des bouleaux, Coloft, Société PRIZM, 59810 Lesquin

Description et produits

PRIZM, basée à Lille, est une société de conseil en gestion des identités et des accès (IAM). Nous positionnons **la gestion des identités** au premier plan de votre transformation digitale par une approche sur-mesure et stratégique de l'IAM. Ainsi, nous sommes votre partenaire clé pour sécuriser vos accès, consolidant ainsi la confiance numérique et renforçant la résilience des organisations face à un écosystème connecté constamment exposé à de nouvelles menaces.

Notre expertise couvre les domaines de : • Gestion du cycle de vie des identités (IM) • Access Management (AM) • Identity Governance and Administration (IGA) • Authentification Multi-Facteurs (MFA) • Gestion des accès aux ressources cloud (CIEM) • Privileged Access Management (PAM)

Chaque projet est unique, nous offrons plusieurs services d'accompagnement adaptés à vos exigences :
• Conseils & cadrage en phase d'avant-projet • Accompagnement projet • Déploiement & support post-projet • Services transverses : stratégie, diagnostic de maturité

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

PROVENRUN

Informations contact

Benjamin Mouchard | benjamin.mouchard@provenrun.com
06 43 24 33 25 | 77 avenue de Niel 75017 Paris | www.pronvenrun.com

Description et produits

Chez ProvenRun, nous nous consacrons à l'établissement d'une confiance absolue dans l'Internet des objets (IoT). Nous croyons en **une approche proactive de la sécurité**. En nous appuyant sur des méthodes formelles, nous employons une approche unique pour créer des composants sécurisés dès leur conception. Notre objectif est de parvenir à **l'état sans bogue tant convoité pour les systèmes embarqués complexes**, en garantissant le plus haut niveau de sécurité.

Nos produits inclus :

- **ProvenCore :** Un système d'exploitation ultra-sécurisé développé à l'aide de méthodes déductives formelles pour fournir une sécurité inégalée et des services critiques de sécurité de l'hôte.
- **ProvenVisor :** un hyperviseur de nouvelle génération spécialement conçu pour les dispositifs embarqués présentant une grande flexibilité et des exigences élevées en matière de sécurité.

Et des services de conseil en sécurité.

Référentiel NIS 2

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Qontrol

Informations contact

Trancart Pierre-Henri | ph@qontrol.io
06 08 77 83 60 | www.qontrol.io

Description et produits

Qontrol est une plateforme SaaS pour PME, startups, organisations publiques. Elle propose **un diagnostic et un plan d'action cybersécurité** assisté par l'IA, pour protéger l'entreprise et **prouver sa posture de sécurité**, rassurant ainsi ses partenaires business.

• Diagnostic cyber — évalue rapidement votre posture • Choix de référentiels (SOC 2, NIS 2, ISO27001, ANSSI, SECNUMCLOUD...), ou personnalisé • Feuille de route sur-mesure pour atteindre vos objectifs • Assistance à la mise en place des mesures • Création de documents et politiques de cyber par l'IA • Recueil des preuves de l'application et de conformité • Passeport Cybersécurité Qontrol : gage de confiance partageable, mettant en valeur vos engagements • Assistant virtuel IA — pour répondre à toute question cyber • Accompagnement par expert Cyber • Réponse aux incidents • Automatisation de la réponse aux questionnaires de sécurité

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

RESCO COURTAGE

Informations contact

GRESSEL Arnaud | arnaud.gressel@resco-courtage.com
07 67 10 16 13 | https://resco-courtage.com
1 rue Guglielmo Marconi 44800 Saint-Herblain

Description et produits

RESCO Courtage est courtier conseil en assurance, spécialisé dans les risques Sûreté et Cyber.

RESCO Courtage adresse TPE, PME et ETI ainsi que les collectivités locales.

Nos missions :

- **Conseil en souscription :** guider et accompagner les organisations dans l'évaluation du risque et l'analyse des critères d'éligibilité en vue de souscrire une assurance cyber
- **Recherche des conditions optimales :** identifier les meilleures conditions d'assurance et conseiller sur le choix de l'offre la plus adaptée au profil du risque
- **Négociation des renouvellements :** représenter nos clients dans la négociation pour des conditions de renouvellement optimales
- **Gestion de Crise :** accompagner nos clients dans la gestion de crises cyber pour une reprise rapide des activités

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

retarus:

Informations contact

Herbet Matthieu | matthieu.herbet@retarus.fr | 06 17 29 85 88
www.retarus.com | Tour Montparnasse 75014 Paris

Description et produits

Plébiscité en France par plus de la moitié des entreprises du CAC40 et par des OIV et OSE, Retarus permet à ses clients de protéger leurs flux d'e-mails (messagerie et mails applicatifs) et de se doter de services innovants grâce à une solution cloud européenne 100 % conforme au RGPD.

En plus de sécuriser les flux d'emails, les offres Retarus sont complétées par nombreux services additionnels tels que l'E-mail continuity par exemple.

Retarus propose enfin une approche "à la carte" unique qui permet de sélectionner les briques fonctionnelles réellement nécessaires, en complément des solutions déjà opérationnelles.

- **Secure Email Gateway** — Solution de prise en charge de l'ensemble des flux SMTP applicatifs (in/out)
- **Email Security** — Solution complète de protection de messagerie
- **Email Continuity** — Solution de maintien des échanges d'email utilisateur en cas de crise cyber

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

</ReverseSense>

Informations contact

Georges-Bastien MICHEL | georges.michel@reversense.com
05 61 90 57 63 | www.reversense.com
11 avenue de toulouse, 31220 Cazeres — France

Description et produits

Reversense s'est positionnée dès sa création dans **le domaine de l'industrialisation de la rétro-ingénierie** afin d'offrir des solutions aussi bien clé-en-main que sur-mesure à destination des professionnels de la cybersécurité et les éditeurs d'applications. L'objectif ? Accompagner les entreprises et les aider à bâtir des offres basées sur la rétroconception d'applications mobiles et embarquées.

Reversense est une entreprise française proposant **une technologie capable d'évaluer automatiquement et sans accès au code source** la présence de certaines caractéristiques ou algorithmes au sein d'applications mobiles ou embarquées.

Nos solutions permettent de **répondre aux besoins d'audit** des équipes sécurité produits, des laboratoires d'évaluation, et des RSSI, mais également à ceux des DPO par **l'identification en boîte noire des données personnelles manipulées**, et bien d'autres.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Ryder & Davis

Informations contact

Alexis DELB | alexis.delb@ryder-and-davis.com | 06 89 98 99 71
www.ryder-and-davis.com | 223 rue Saint Honoré 75001 Paris

Description et produits

Conseils financiers pour les opérations de haut de bilan :

- **Levée Venture**
- **LBO / MBO**
- **Cession**
- **Acquisition**

Aide au développement de la filière par accompagnement au financement et à la consolidation. Grâce à notre forte implication dans la cybersécurité française, nous échangeons chaque jour avec les principaux acteurs mais également avec les leaders de demain. Cette expertise nous permet de conseiller au mieux les entrepreneurs spécialisés dans le domaine de la cybersécurité pour choisir la voie de développement la plus adaptée à leur entreprise mais aussi à leur vision future. Nous sommes conseillers financiers, stratégiques, mais avant tout humains.

Scalair

Informations contact

Vignault Damien | dvignault@scalair.fr | 07 62 58 64 86
2 bis Avenue Antoine Pinay, 59510 Hem | www.scalair.fr

Description et produits

Scalair est une société de services experte en matière de cybersécurité et de protection des données (MSSP), Membre de la French Tech & de l'Alliance HEXATRUST. L'entreprise propose **des technologies innovantes** pour protéger les données des entreprises. **Scalair design**, implémente et exploite des solutions de qualité supérieure, tout en offrant une protection efficace contre les menaces informatiques.

Notre entreprise propose **des solutions clés en main** visant à assurer un niveau élevé de disponibilité du système d'information. De la consultation à la gouvernance, nous élaborons des offres flexibles et sécurisées. Notre approche intègre **Cloud souverain** hébergé en France, **solution réseau de nouvelle génération (SASE)**, et sécurisation des utilisateurs via des **services managés de cybersécurité**. Nos offres sont sans engagement de durée.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

SCALITY

Informations contact

Nguyen-Phuoc Anh | anh.nguyen-phuoc@scality.com
+33 06 74 14 71 95 | www.scality.comfr
11 rue Tronchet, 75008, PARIS

Description et produits

Scality résout les plus grands défis liés au stockage de données auxquels les entreprises doivent faire face : croissance, sécurité et coût. En offrant **100 % de disponibilité**, une protection anti ransomware infaillible et une résilience maximale, **les solutions de stockage Scality RING et ARTESCA** permettent de rendre les infrastructures de stockage évolutives, scalables et sans limite.

Scality RING est le socle de votre stockage sur une architecture, flexible, agile, en mode cloud. Compatible avec tout type de serveur, application ou cloud public, il fournit une solution unique qui stocke et protège toutes vos données et sans coût caché.

Scality ARTESCA est la solution S3 simple, fiable et évolutive de stockage objet pour le backup immuable des applications. Elle se déploit facilement et rapidement en compatibilité de la règle 3-2-1-1.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

seclāb
-cybersecurity-

Informations contact

Xavier Facélina | contact@seclab-security.com | 0762517525
www.seclab-security.com | 40 avenue Theroigne de Mericourt

Description et produits

Leader français de la cyberprotection des systèmes cyberphysiques, SECLAB **sécurise les échanges entre les domaines OT et IT** en simplifiant les architectures d'interconnexion et en supprimant les risques liés aux failles logicielles des équipements de cybersécurité.

La **technologie brevetée de rupture électronique de tous les protocoles de communication réseau et USB** permet de déployer des architectures de télémaintenance sécurisée, de mise à jour de parc industriel, de pilotage distant de systèmes cyberphysiques ou encore d'échange de fichiers.

Certifiés par l'ANSSI nos produits sont nés pour sécuriser les infrastructures les plus critiques du pays. Aussi, nos clients adressent la cybersécurité industrielle avec **des solutions plus simples à mettre** en œuvre et à maintenir que les approches traditionnelles, tout en bénéficiant du plus haut niveau de sécurité existant.

CSPN

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Seela

Informations contact

information@seela.io | www. Seela.io

Description et produits

La plateforme de formation SEELA du groupe NEVERHACK permet **la gestion des cycles de formation** et **la création de contenus de formation personnalisés** pour les équipes client. La plateforme inclut également **deux solutions CyberRange d'entraînement en ligne** afin d'assurer une formation pratique adaptée aux utilisateurs.

Notre solution de formation cyber comprend plus de **700 heures de formation** basée sur les descriptions des métiers selon l'ANSSI. La plateforme propose des travaux pratiques sur des environnements techniques simulés grâce à des CyberRange. Le client peut bénéficier des formations existantes qui couvrent la majeure partie de domaines techniques autour des problématiques de la Cyber sécurité (leçons et TD pratiques associés).

EXPERT CYBER

Référentiel NIS 2

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

sekoia

Informations contact

Freddy Milesi | contact@sekoia.io | https://sekoia.io
54, rue des Petites écuries 75010 Paris

Description et produits

Sekoia.io est la cybertech européenne leader des solutions de détection et de réponse étendues s'appuyant sur le renseignement d'intérêt cyber (Cyber Threat Intelligence).

- **Sekoia Defend (SIEM Next-Gen)** est une plateforme SOC de détection et réponse étendue (XDR) disponible en mode SaaS, et alimentée par du renseignement cyber exclusif. Anticipation des attaques, automatisation, nombreuses intégrations et règles de détection vérifiées simplifient la protection des environnements hybrides.
- **Sekoia Intelligence (CTI)** offre une connaissance approfondie des menaces. La normalisation des flux de renseignements facilite la compréhension des attaques, intrusions et actes malveillants. Le renseignement exclusif produit est contextualisé et actionable, bénéficiant aux équipes stratégiques et opérationnelles.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Smart Global Governance

Informations contact

Pascal Petitjean | pascal.petitjean@smartglobal.com
04 12 39 25 20 | www.smartglobalgovernance.com
300 rue du Vallon, "Les Vaisseaux" 06560 Valbonne

Description et produits

Smart Global Governance est l'éditeur de la plateforme Smart GRC, solution de gestion des risques et conformité utilisée par plus de 300 utilisateurs dans 100 pays.

Disponible en SaaS ou on premise, Smart GRC offre aux CISO et à leurs équipes **une solution spécialisée de gestion des risques et conformité**.

• Cartographie des risques cyber • Identification et priorisation des risques • Gestion des risques cyber • Evaluation et suivi des risques • Gestion des Incidents de sécurité • Gestion des conformités • Plus de 45 standards interconnectés (AI ACT, DORA, NIS 2, ISO 27001, GDPR) • Gestion des risques Tiers • Audit et contrôle • Plan de continuité d'activité • Data Discovery

Smart GRC est ainsi une suite de solutions spécialisées formant une plateforme globale et centralisée de gouvernance, risque et conformité pour les entreprises.

• Data & Privacy • Ethics et transparency • Legal • ESG • Health and Safety • Quality • IA Intégrée « Smart Colleague »

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

snowpack

Informations contact

MOREL Olivier | olivier.morel@snowpack.eu | +33 6 99 09 13 21
https://snowpack.eu/fr/ | Centre d'intégration NANO-INNOV,
2 Boulevard Thomas Gobert, 91120 Palaiseau

Description et produits

Snowpack est un spin-off du CEA, créée en 2021, lauréate I-lab 2022 et DeepNum20, soutenue par la stratégie d'accélération cyber.
Snowpack fournit **la technologie VIPN (Virtual & Invisible Private Network)** — très innovante et brevetée — qui permet de protéger les utilisateurs, données, composants du système d'information et services web exposés sur Internet en les rendant INVISIBLES des hackers.
Avec Snowpack les attaquants NE VOUS VOIENT PAS, ainsi ILS NE VOUS ATTAQUENT PAS !
VIPN prémunit contre de nombreuses attaques réseaux, telles que la surveillance et l'interception des communications, le scan externe du système d'information, et l'exploitation des vulnérabilités des composants et services exposés sur Internet. **Elle réduit considérablement la surface d'attaque externe des organisations**, en la rendant invisible, et élimine tout besoin de confiance dans l'infrastructure.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

sosafe

Informations contact

Yan Richard | yan.richard@sosafe.de | www.sosafe.fr
23-25 avenue MacMahon, 75017, Paris — France

Description et produits

SoSafe est **la plateforme de sensibilisation à la cybersécurité et à la gestion des risques cyber axées sur l'humain**. Notre plateforme automatisée et sans effort, modifie les comportements de vos collaborateurs pour vous sécuriser via des modules d'e-learning et des simulations de cyberattaques.
Alimentée par **les sciences du comportement** et **des algorithmes intelligents**, SoSafe permet aux sociétés de développer une culture de la cybersécurité et de transformer leurs employés en alliés contre les menaces de sécurité.

- Formation personnalisée SoSafe pour changer rapidement les comportements.
- Modules de micro-apprentissage interactifs et ludiques sur la cybersécurité.
- Simulations de phishing personnalisées.
- Tableau de bord pour mesurer votre niveau de sécurité.
- Un chatbot interactif pour alerter en cas d'urgence.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Suricate

Informations contact

SENAUX Rémi | remi.senaux@suricate.pm
06 38 08 40 04 | www.suricate.pm
2 rue du 19 mars 1962, 92110 Clichy

Description et produits

Suricate est le spécialiste français du **Patch Management IT/OT en service managé**, certifié ISO 27001, en gestion intégrale et fonctionnant en 24/7. Suricate assure **la gestion des OS, de plus de 500 logiciels et applications intégrées nativement ainsi que l'infrastructure et réseau**.

Suricate c'est : • Une équipe dédiée en 24/7 avec une méthodologie et des process éprouvés • Des Outils IT uniques pour un pilotage performant et un reporting engageant • La gestion des alertes CVE / CERT-FR, gestion de crise et process accéléré de validation • La garantie des meilleures pratiques via la certification « ISO 27001 » • L'assurance de conformité avec, chaque mois, la délivrance d'un rapport détaillé de l'état du parc • La souveraineté : implanté à Caen et Paris, Suricate ne fait aucune externalisation. • La gestion du air-gap (infrastructures et machines non connectées au réseau). • Une couverture applicative de plus de 500 applications sous distributions Microsoft et Linux. • L'intégration possible des applicatifs métiers via process spécifique.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

synetis

Informations contact

Fréderic Le Landais | frederic.lelandais@synetis.com
07 64 67 33 97 | 19 rue du Général Foy, 75008 Paris
www.synetis.com

Description et produits

Créé en 2010, Synetis est aujourd'hui le leader des cabinets — français et indépendants financièrement — de conseil et d'expertise technologique spécialisés en **sécurité des Systèmes d'Information** (SSI). Synetis se positionne comme pure-player français de la cybersécurité et propose une démarche complète à ses clients — PME et grandes entreprises de tous secteurs d'activité, de **l'accompagnement à la mise en œuvre et la gestion de nouvelles solutions au sein de leur SI**.

Synetis intervient aujourd'hui sur cinq domaines d'expertise : l'audit de sécurité, le CERT, la GRC (Gouvernance, Risques et Conformité), l'identité numérique et la sécurité opérationnelle. Certifié Qualiopi, Synetis propose également une large gamme de formations couvrant toutes les expertises cybersécurité — pour permettre à tous de s'adapter et rester performant face aux nouveaux enjeux cyber.

EXPERT CYBER

PASSI

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité
Art. 21.2 : Protection de l'environnement physique des réseaux et systèmes d'information
Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information
Art. 21.2.b : Gestion des incidents
Art. 21.2.c : Continuité des activités
Art. 21.2.d : Sécurité de la chaîne d'approvisionnement
Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité
Art. 21.2.g : Cyberhygiène et formation à la cybersécurité
Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Tenacy
EMPOWERING CYBERSECURITY

Informations contact

Baptiste DAVID | baptiste.david@tenacy.io | 06 61 10 52 12
55 avenue René Cassin - 69009 Lyon | www.tenacy.io

Description et produits

Notre mission : pérenniser les organisations via un usage plus efficace des ressources de cybersécurité. Grâce à notre plateforme SaaS tout-en-un à destination des équipes SSI, **nous consolidons et simplifions le pilotage de la cybersécurité et de la conformité**.

Leader en France, nous comptons plus de 150 clients de l'ETI au grand compte (Michelin, GL Events, groupe Henner, Gerflor, Sephora, groupe RATP, CHU de Lille).

Grâce à une modélisation intelligente des référentiels et des risques, **Tenacy interconnecte l'ensemble de vos processus cyber**. Vous pouvez ainsi mesurer en continu votre niveau de sécurité, suivre vos opérations efficacement, et fédérer les parties prenantes.

Avec 30+ connecteurs, Tenacy se branche à l'ensemble de l'écosystème IT et cyber. Cela permet de centraliser les KPIs de sécurité, consolider les anomalies et renforcer la collaboration des équipes.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Tersedia

Informations contact

Jessica Belingard | jessica.belingard@tersedia.fr | 06 95 65 01 23
18 rue Charles Despeaux 78400 Chatou | www.tersedia.fr

Description et produits

Spécialiste des infrastructures multicloud sécurisées depuis 1996, notre vision est simple : faire de l'infrastructure une commodité pour nos clients.
Pour cela, nous nous appuyons sur deux savoir-faire :

- La **conception d'architectures sur-mesure** avec notre approche unique « secured by design »
- La **gestion et la supervision cyber** d'infrastructures informatiques

En complément de notre centre d'opération du réseau (NOC), nous disposons de centres de supervision de la sécurité (SOC) et d'alerte/réaction aux attaques cyber (CERT), assurant **une surveillance constante et une réaction proactive** aux menaces.

Nos certifications ISO27001 et HDS, ainsi que notre labélisation Cybermalveillance, garantissent la qualité de nos services, conformes aux normes strictes telles que DORA.

Avec Tersedia, nos clients peuvent se concentrer pleinement sur le développement de leur business, sans se soucier de la capacité de leur système d'information désormais performant et cyber résilient.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

THEGREENBOW

Informations contact

Louise BAUTISTA | louise@thegreenbow.com | 0635338207
28 rue de Caumartin 75009 Paris | www.thegreenbow.com

Description et produits

Créé en 1998, TheGreenBow est un éditeur français de logiciels de cybersécurité qui fournit des solutions VPN de confiance et dont l'expertise repose sur la sécurisation des communications. Premier opérateur à avoir été certifié CC EAL3+, qualifié standard et agréé DR OTAN et UE en 2013, pour son logiciel Client VPN Windows, TheGreenBow distribue ses logiciels dans plus de 70 pays.

Produits et services :

- **Endpoint Secure Connection** : gamme de Clients VPN d'entreprise la plus fiable et la plus polyvalente du marché :
- **Connection Management Center** : gamme de consoles web regroupant des services qui permettent de gérer des configurations VPN et le parc de licences, créer des règles ZTNA et enfin d'analyser les logs.
- **Services professionnels** : assistance technique sur-mesure, technical account management, formations

Certification Critères Communs EAL3+

Référentiel NIS 2

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

TIXEO
SECURE VIDEO CONFERENCING

Informations contact

AZAN Olivier | oazan@tixeo.com | +33 (0)7 86 14 42 27 | www.tixeo.com
Parc 2000 — 244 rue Claude François 34080 Montpellier — France

Description et produits

Depuis 20 ans, Tixeo, éditeur français de **solutions de collaboration et de visioconférence sécurisée**, accompagne les organisations pour garantir l'efficacité et la sécurité de leurs échanges en ligne.

Tixeo intègre la seule technologie de visioconférence certifiée/qualifiée ANSSI et vient compléter les solutions de collaboration standards avec **une technologie propriétaire basée sur des mécanismes de sécurité innovants**.
Tixeo permet aux organisations de limiter le risque cyber, renforcer leur cyber-résilience ou les aider à se conformer aux règlementations.

Tixeo est utilisé dans des secteurs stratégiques (défense, aérospatial, industrie, énergie, finance) ainsi que par certaines instances étatiques ou juridiques.

La visioconférence Tixeo s'adapte ainsi aux besoins de tout type d'organisation. Elle est disponible dans le cloud public et privé (qualifié SecNumCloud) ainsi qu'On-Premise.

CSPN Qualification élémentaire

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Tranquil IT

Informations contact

Vincent CARDON | commercial-tis@tranquil.it
+33 2 40 97 57 55 | www.tranquil.it
12 avenue Jules Verne, 44230 Saint Sébastien sur Loire — France

Description et produits

La mission de Tranquil IT est d'apporter de la tranquillité à ceux et à celles qui travaillent avec l'outil informatique.

Basée à Nantes, nous solutionnons le désir de nos clients pour **d'avantage de cyber-résilience et de protection contre les vulnérabilités logicielles et les défauts de configuration** avec 2 produits, **WAPT** et **Samba-AD**.

WAPT permet aux entreprises et aux administrations de déployer (1) des logiciels, (2) des configurations, (3) des mises à jour et (4) des systèmes d'exploitation sur un parc Windows, Linux et macOS, comme Microsoft SCCM, WSUS et MDT mais en plus simple.

Samba-AD, c'est **la technologie Active Directory sous Linux** et en open source pour gérer et sécuriser les identifiants, les méthodes d'authentification et les contrôles d'accès, comme Microsoft AD, là aussi en plus simple.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

TrustBuilder

CSPN

Informations contact

Jean-Dominique QUIEN | jean-dominique.quien@trustbuilder.com
06 21 09 28 43 | www.trustbuilder.com | 55 Rue de Châteaudun 75009 Paris

Description et produits

TrustBuilder, acteur européen avec une portée mondiale comptant plus de 500 clients, est votre partenaire de confiance en cybersécurité. Nous allons au-delà du rôle traditionnel d'un éditeur de logiciels en proposant **des solutions robustes qui garantissent la sécurité du parcours numérique de vos employés, partenaires et clients** avec la plateforme TrustBuilder.io.

L'authentification forte de TrustBuilder.io est une technologie MFA brevetée, certifiée par l'ANSSI et résistante aux tentatives de phishing. Elle adopte une approche d'**authentification adaptative, passwordless et smartphoneless** pour une expérience utilisateur fluide. Son intégration en mode SaaS facilite le travail des développeurs.

TrustBuilder.io propose une **offre CIAM sur-mesure**, offrant un service « haute couture » en matière de cybersécurité avec une gestion avancée des accès. Notre approche, basée sur les personas et notre moteur de workflow personnalisable, permet des ajustements de sécurité précis en fonction des besoins uniques de chaque client.

Référentiel NIS 2

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

TRUST IN SOFT

Informations contact

DEW Ashley | ashley.dew@trust-in-soft.com | +33 1 84 06 43 91
https://trust-in-soft.com | 222 cour avenue du Maine 75014 Paris

Description et produits

TrustInSoft commercialise des **outils et services d'analyse exhaustive de code source C et C++** permettant d'apporter des garanties mathématiques sur la qualité des logiciels de ses clients. Ces solutions d'analyses de logiciel permettent d'avoir des garanties sur la sécurité et la fiabilité du code source sans modifier le processus de développement. Ces offres sont déployées dans le monde entier chez les développeurs et intégrateurs de composants logiciels issus des industries aéronautique, automobile, ferroviaire, militaire, nucléaire, télécoms, ou l'IoT. La **technologie est reconnue** par l'agence fédérale américaine National Institute of Standards and Technology (NIST), et était la première au monde à répondre aux Critères d'Ockham de la **norme SATE V** du NIST pour les logiciels de haute qualité.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

TYREX

Informations contact

Ably Laurent | laurent.ably@tyrex-cyber.com
+33 1 74 903 900 | www.tyrex-cyber.com
2 rue du 19 Mars 1962 — 92110 Clichy

Description et produits

TYREX conçoit, fabrique et opère des **stations de décontamination de support USB**, capables de détecter les menaces connues et inconnues afin d'échanger des données de manière sécurisée.
Notre solution allie excellence technologique et simplicité de déploiement et d'utilisation afin de s'adapter à tous les usages, toutes les infrastructures IT ou OT et toutes les réglementations.

Avec plus de **3 700 bornes déployées dans le monde**, TYREX opère depuis 2017 dans des secteurs tels que la Défense, l'industrie, les transports, les organismes publics et gouvernements ainsi que les OIV (Opérateurs d'Importance Vitale) et protège ainsi leurs infrastructures critiques.

La solution TYREX se compose d'**une console de management** permettant une administration facilitée et centralisée, à laquelle viennent se rattacher **4 modèles de stations blanches** : CONSOLE / TOTEM / SATELLITE / MOBILE.

En option, TYREX propose également **un agent qui bloque l'accès des clés USB non certifiées** par une station TYREX au système d'information.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

UBIKA

Informations contact

Stéphane De Saint Albin | stephane.desaintalbin@ubikasec.com
01 46 20 96 00 | www.ubikasec.com
9 - 11 rue Jeanne Braconnier 92360 Meudon

CSPN

Description et produits

Fondé en 2001, UBIKA, **acteur souverain de la sécurité applicative**, est le leader européen de la protection des applications Web et des APIs. Connu précédemment sous les étendards de Bee Ware, DenyAll ou plus récemment Rohde & Schwarz Cybersecurity, la société fournit **des solutions innovantes de protection des applications Web & des APISs** contre les nouvelles menaces comme le DDOS volumétrique ou applicatif, les injections de code malveillant, les défacements et en général contre le Top 10 de l'OWASP. Agnostique des fournisseurs de cloud, les solutions peuvent être déployées en mode multi-cloud, On-Premise et en mode SaaS afin de prévenir les cyberattaques de manière proactive.

Plus de 600 entreprises et institutions publiques dans 35 pays nous confient la sécurité de leurs applications et de leurs APIs.

UBIKA est en cours de re-certification par l'ANSSI.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Ugloo

Informations contact

Gonzague Dupont | gonzague.dupont@ugloo.com
06 75 65 02 38 | www.ugloo.fr
9 rue du quatre septembre 75002 Paris

Description et produits

Ugloo propose une **solution de stockage S3 distribuée**, la solution récupère les données en sortie de solutions de sauvegardes, les fragmente, et les redonde sur des disques répartis sur des serveurs de commodité (Intel ou AMD). Les donnés sont en permanence vérifiées et reconstruites automatiquement en cas de problème. **Notre solution qui se veut très simple, tout en un, intègre un loadbalanceur est multi tenante et doublement immuable.** Notre logiciel est commercialisé en mode acquisition ou en mode souscription, et s'installe soit en « on prem » soit en mode cloud. Nous supportons entre autres le protocole DICOM pour archiver les PACS.

Solution souveraine, notre logiciel permet de conserver des données de façon immuable dans la durée sur une architecture résiliente basée sur des serveurs de commodité et à des couts raisonnés. Nous supportons entre autres le protocole DICOM.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

UNCOVERY

Informations contact

contact@uncovery.io | www.uncovery.io

Description et produits

Uncovery est spécialisée dans la **gestion de la surface d'attaque externe** (EASM, External Attack Surface Management).

Son innovation est issue de 6 ans de R&D et consiste à avoir automatisé et industrialisé toutes les étapes réalisées par un attaquant pendant sa phase de reconnaissance. Elle édite **une solution SaaS 100% automatisée** qui identifie, surveille les actifs exposés sur Internet, et évalue leur niveau de risque.

Elle permet d'obtenir une haute visibilité sur les actifs exposés sur Internet, via un inventaire précis, à jour et sans positif, mais également d'évaluer leur niveau de risque afin de se prémunir des cybermenaces.

Référencée UGAP, Uncovery aide les acteurs publics mais également une 40aine d'ETI et grandes entreprises du secteur privé à maîtriser leur surface d'exposition.

Référentiel NIS 2

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

vade

Informations contact

Dimitri Perret | insidesales@vadesecure.com | +33 3 59 61 66 50
2 bis, avenue Antoine Pinay - Parc d'Activités des 4 vents 59510 Hem
www.vadesecure.com

Description et produits

Entreprise internationale de Cybersécurité, spécialisée dans la protection des échanges collaboratifs basée sur l'IA améliorée par l'humain. Vade protège 1,4 milliard de messageries et analyse plus de 100 milliards d'emails par jour pour plus de 18 000 clients dans le monde.

Vade for M365 & pour Vade for GWS : sont des solutions de sécurité des emails en mode API basée sur l'IA, capable de bloquer les attaques de ransomwares/ malwares, phishing & spear phishing les plus sophistiquées et protégeant toutes entreprises des liens malveillants intégrés dans les emails (Remote Browser Isolation)

Vade Cloud : protège en mode relai cloud vos boîtes mails contre le phishing, les malwares & le spam. Solution simple, intuitive, évolutive qui s'adapte à votre activité en bénéficiant de toute la technologie Vade

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.b : Gestion des incidents (CSIRT depuis février 2024)

Art. 21.2.c : Continuité des activités

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

wallix

CSPN

Informations contact

Hervé PATRY | hpatry@wallix.com | 06 60 69 18 58 | www.wallix.com
250 bis, rue du Faubourg Saint Honoré 75008 Paris

Description et produits

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 usurpées et aux privilèges élevés accordés pour accéder aux actifs sensibles de l'entreprise.

- **WALLIX One :** plateforme SaaS de gestion et sécurisation des accès et identités
- **WALLIX PAM** : gestion des accès à privilège / Gestion du moindre privilège / Sécurisation des accès distants
- **WALLIX IdaaS** : solution de Fédération et sécurisation des identités, SSO et MFA
- **WALLIX IAG** : gouvernance des identités et des accès

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

Whaller

Informations contact

Luez Laetitia | contact@whaller.com | 01 47 92 82 18
https://whaller.com | 3 Rue Salomon de Rothschild 92150 Suresnes

Description et produits

Whaller est une plateforme sociale sécurisée et collaborative, idéale pour entreprises, écoles, associations et familles. Unique en son genre, elle supporte des milliers d'utilisateurs, facilitant **la création de réseaux collaboratifs variés**. Au cœur de son fonctionnement, les « sphères » permettent une gestion fine des communautés et communications. Respectueuse de la vie privée, Whaller s'engage à ne pas exploiter les données personnelles.
Lancée en 2013 par Thomas Fauré, elle compte aujourd'hui plus de 1 million d'utilisateurs et 50 000 réseaux. Pour les entités exigeant une sécurité renforcée, **Whaller DONJON**, en partenariat avec OVHcloud, offre une solution « cyber-renforcée » avec une suite collaborative sur le cloud privé qualifié SecNumCloud d'OVHcloud. Cette version spéciale assure une cybersécurité maximale et répond aux besoins de souveraineté numérique avec une protection des données de haut niveau.

Référentiel NIS 2

Art. 21.2.c : Continuité des activités

Art. 21.2.j : Solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence

YesWeHack

Informations contact

Lionel Pascaud | l.pascaud@yeswehack.com | 06 79 12 72 82
www.yeswehack.com | 14 rue Charles V, 75004 Paris

Description et produits

YesWeHack est une plateforme globale de Bug Bounty et de gestion des vulnérabilités. Fondée en 2015, **YesWeHack connecte les organisations du monde entier à des dizaines de milliers de hackers éthiques**, dont l'objectif est de découvrir les vulnérabilités potentielles au sein de sites web, applications mobiles, appareils connectés et infrastructures numériques.

YesWeHack offre une gamme de solutions intégrées, basées sur des API : le **Bug Bounty** (recherche de vulnérabilités via une approche crowdsourcée) ; la **Politique de Divulgation de Vulnérabilités**, **VDP** (création d'un canal sécurisé pour le signalement de vulnérabilités) ; le **Pentest Management** (gestion des rapports de pentest issus de différentes sources) ; l'**Attack Surface Management** (cartographie continue de l'exposition numérique et détection des vecteurs d'attaque) ; ainsi que **le «Dojo»** et **YesWeHackEDU** (formation au hacking éthique).

Référentiel NIS 2

Art. 21.2.e : La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités

Art. 21.2.f : Des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité

yogosha

Informations contact

Fabien Barrois | f.barrois@yogosha.com | 06 59 69 20 46
https://yogosha.comfr | 113 rue d'aboukir 75002 PARIS

Description et produits

Yogosha est une plateforme de Sécurité Offensive vous permettant d'identifier vos vulnérabilités les plus critiques et les plus difficiles à trouver en tirant parti de nos 4 piliers :

- **Nos opérations de Sécurité Offensive** : Pentest as a service et Bug Bounty.
- **Notre communauté de chercheurs en sécurité** : La Yogosha Strike Force.
- **Notre plateforme** : Le Vulnerability Operations Center.
- **Nos services professionnels.**

Référentiel NIS 2

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Création graphique : Franck Soulier
Crédits images : Freepiks, MEFSIN, Arnaud Février pour l'AMF.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

2024

HEXATRUST

CAMPUS CYBER

5-7 rue Bellini,
92800 Puteaux

contact@hexatrust.com
www.hexatrust.com

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY