CATALOGUE

DE SOLUTIONS ET DE SERVICES

de confiance pour les collectivités territoriales, les établissements de santé, et les organismes au service des citoyens

ÉDITION 2023/2024

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

SOMMAIRE

QUI SOMMES-NOUS ?

HEXATRUST, LE GROUPEMENT DES CHAMPIONS FRANÇAIS ET EUROPÉENS DE LA CYBERSÉCURITÉ ET DU CLOUD DE CONFIANCE

Les offres et solutions Hexatrust répondent toutes à des exigences techniques de maturité et d'excellence. Elles sont reconnues en Europe et à l'international par les plus grandes organisations et s'inscrivent dans des logiques de certification et de souveraineté. Les sociétés membres d'Hexatrust œuvrent ensemble pour promouvoir et construire la confiance dans le Cloud et l'excellence en matière de Cybersécurité, et contribuent ainsi au rayonnement numérique européen.

+95 MEMBRES

+6 500 SPÉCIALISTES

+1,5 Md€ CHIFFRE D'AFFAIRES RÉALISÉ PAR LES ADHÉRENTS D'HEXATRUST

Nos valeurs

EXCELLENCE ▸ CONFIANCE ▸ INNOVATION ▸ ACTION

Membre du Campus Cyber et membre suppléant du CA au titre du collège des associations

CAMPUS CYBER RÉSIDENT

ECS

6cure · AISI · algosecure · Antemeta · ARCAD · ATEMPO · Avant de Cliquer · board of cyber · Brain Networks · Brainwave GRC · conscio · continus · CrowdSec · Cryptonext Security · Cyber-Detect · cybervadis · CyberXpert · Cyberwatch · DASTRA · devensys Cybersecurity · DOCAPOSTE · ebrc · efficient IP · EGERIE · ERCOM · EQUISIGN · EVERTRUST · EXAMIN · eXo · F24 · FIC · formind · GATEWATCHER · HarfangLab · GLIMPS · HIA secure · HOLISEUM · HOSTEUR · identa · Ilex IAM Platform · inetum · ise Systems · Jalios · jscrambler · Jamespot · KDDI France · KUB · leviia · LOGIN · MAILINBLACK · MAKE IT SAFE · merox · MOABI · METSYS · nameshield · NeoTech · NEOWAVE · NetExplorer · Olfeo · Olvid · onx groupe · OUTSCALE · oodrive · OVERSOC · retarus · Patrowl · PRIMX · PRIZM · ProHacKtive · PROVENRUN · Qontrol · Ryder & Davis · satelliz · Scalair · Schneider Electric · seclab · Seela · sekoia · Smart Global Governance · Suncate · Snowpack · synetis · Tenacy · Tersedia · THEGREENBOW · TIXEO · Tranquil IT · TRUSTINSOFT · TrustHQ · TrustBuilder · UBIKA · vade · WALLIX · Whaller · YES WE HACK · yogosha

ÉDITO

Marc Loutrel
Directeur Expertise,
Innovation et International

AGENCE DU NUMERIQUE EN SANTÉ

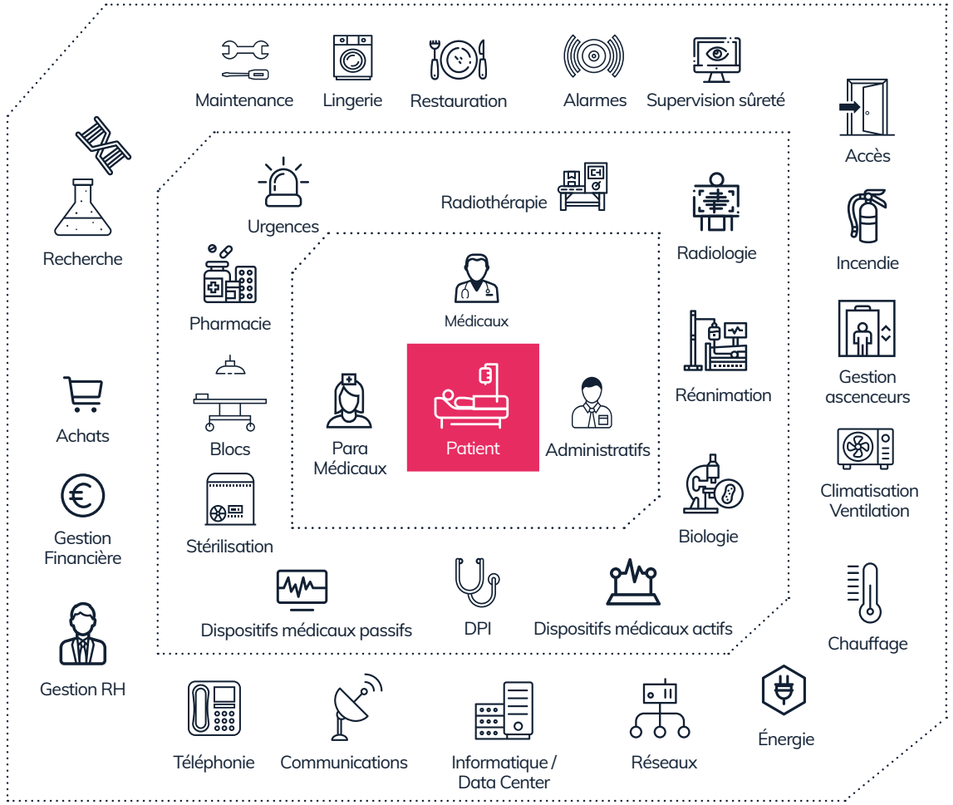
Après une période de pandémie qui a entrainé une ouverture massive des systèmes d'information hospitaliers et des attaques massives sur 2020 et sur 2021, la cybermenace ne diminue pas, et nous y sommes collectivement un peu mieux préparés. Après le premier plan de renforcement cyber décidé par le Président de la République, et malgré les disparités entre les différents secteurs d'activité, le niveau de maturité a augmenté pour la santé. Et surtout, il y a maintenant une réelle prise de conscience par les pouvoirs publics, de l'échelle nationale à l'échelle de l'établissement de santé, de la nécessité de progresser « collectivement » sur ce sujet.

Les incidents récents du CHSF (Centre Hospitalier Sud-Francilien) de Corbeil-Essonnes et du Centre Hospitalier de Versailles démontrent, si cela était nécessaire, que la menace est encore bien présente et qu'il est nécessaire d'encore plus se préparer.

Nous ne sommes jamais réellement prêts à ce type de crise et même à recevoir autant de sollicitations médiatiques et de reporting… et pourtant c'est précisément ce que les établissements de santé qui ont été victimes de cyberattaques doivent affronter : une communication massive et des demandes d'analyse et de comptes-rendus venant de toutes parts, notamment des institutions (Ministère de tutelle, ARS, Préfectures…).

En tant que CERT Santé, et pour se préparer à la gestion de crise au service des ES (Établissement de Santé), nous avons été très fiers de coconstruire avec nos pairs en région, des kits de cybercrise comprenant plusieurs niveaux, du débutant jusqu'au niveau avancé, qui nous l'espérons permettront aux structures sanitaires et médico-sociales de se préparer à une cybercrise.

Le cas du CHSF a été le point de départ d'annonces politiques : une nouvelle enveloppe de 20 millions d'Euros.



Une task force a été montée en octobre dernier pour élaborer avec les acteurs d'administration centrale, mais aussi régionale, le plan de renforcement cyber massif dont les ES ont besoin, notamment sur la partie infrastructure. Cela est parfaitement intégré au projet de la nouvelle feuille de route la e-santé 2023-2027 en cours de concertation. Il déterminera notamment pour la cyber les sujets de : gouvernance, sensibilisation, ressources, exercices, remédiation, financements et certifications, hébergement.

En parallèle, l'Agence du Numérique en Santé prépare également la vague 2 du Ségur du numérique qui introduira, à cet égard, des exigences en sécurité des systèmes d'information pour les solutions proposées aux professionnels de santé par les entreprises du numérique en santé.

Toutes ces initiatives pour se déployer sur le terrain ont besoin d'acteurs industriels bien au fait des problématiques de cyber et ayant une réelle connaissance du secteur de la santé. À cet égard, Hexatrust fédère un grand nombre d'acteurs proposant des solutions souveraines indispensables aux acteurs de la santé pour sécuriser leurs établissements.

ÉDITO

Jean-Noël de Galzain
Président d'Hexatrust
Pilote du projet Cybersécurité
au sein du Comité Stratégique de
Filière « Industries de sécurité »

Cette seconde brochure capacitaire Hexatrust est un guide pratique des solutions cyber françaises, destiné à faciliter la prise de décision et l'acquisition de solutions pour faire face aux risques numériques et aux cyberattaques.

Elle s'inscrit dans la continuité des travaux du projet de cybersécurité au cœur de la stratégie nationale française lancée en 2021 par le Président de la République. Son objectif, à travers le volet cybersécurité de France Relance, est de renforcer la résilience des collectivités territoriales, des établissements de santé et des organismes au service de tous, tout en dynamisant l'écosystème industriel français.

Ce dispositif confié à l'ANSSI depuis 2021 a insufflé une dynamique vertueuse de modernisation des protections cyber en agissant sur les compétences, l'audit et le financement d'équipements appropriés, essentiellement français et européens. La méthodologie retenue consiste à réaliser un audit, avant de suivre un parcours de cybersécurité adapté à l'état d'urgence des organisations publiques et privées pour faire face à la menace des cyberattaques.

Car il y a urgence !

L'état de la menace cyber est élevé comme jamais. Elle est devenue en 2022 le risque majeur selon les dirigeants des entreprises interrogés par le cabinet PWC dans le monde, en atteste la forte augmentation des attaques par malware ou ransomware (+400% en 2021), et des fuites de données (+78% en deux ans). Avec l'utilisation croissante du numérique dans les organisations, le besoin de se protéger et de protéger la chaîne de confiance est indissociable d'une démarche responsable en matière de gouvernance.

Les acteurs industriels réunis autour d'Hexatrust ont donc constitué ce catalogue de solutions cyber et numériques de confiance, innovantes, souveraines et alignées sur les recommandations des Parcours cyber de l'ANSSI. Il est dédié à tous ceux qui veulent réaliser une transformation numérique résiliente et durable de leur organisation, en résistant aux cyberattaques, avec une démarche responsable.

Comme dit le proverbe chinois, « *ce n'est pas le but qui compte mais le chemin* ». Alors faisons un bout de chemin ensemble, et suivez le guide...

COLLECTIVITÉS ET SECTEUR HOSPITALIER : DES SOLUTIONS SOUVERAINES EXISTENT POUR PARER LES RISQUES CYBER

Le numérique irrigue aujourd'hui l'ensemble des activités des établissements publics. Collectivités territoriales comme établissements de santé l'ont largement intégré dans leurs activités : relations dématérialisées avec les usagers, travail à distance des agents, utilisation du cloud, stockage des données patients, etc.

Cet usage accru du numérique améliore la qualité du service rendu au public, mais il amène également son lot de contraintes, dans un contexte où les risques cyber sont, chaque année, plus importants. Le principal danger est celui d'une perturbation voire une paralysie de l'activité en cas d'atteinte sur le système d'information.

Le secteur des collectivités locales et celui de la santé traitent des données personnelles (comme l'état civil) et/ou sensibles (comme les données de santé). D'éventuelles perturbations dans leur fonctionnement peuvent avoir des conséquences graves. Collectivités locales et établissements de santé sont donc exposés à des enjeux particulièrement forts en matière de sécurisation de leur système d'information et des données qu'il contient.

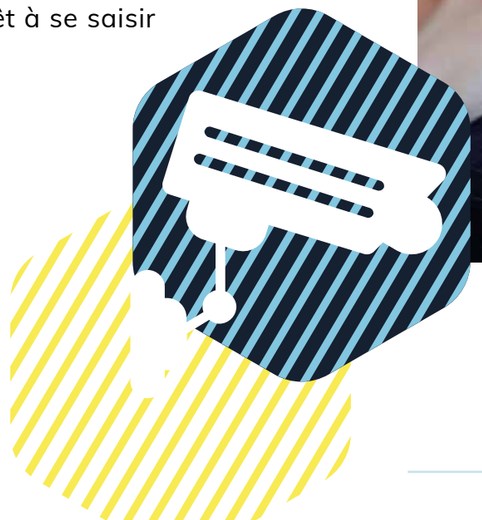
Ces acteurs ne peuvent se protéger seuls face à des acteurs cybercriminels qui se spécialisent, se professionnalisent et se structurent en véritables organisations. Des solutions souveraines existent pour les aider à sécuriser leur système d'information et accroître leur niveau global de sécurité.

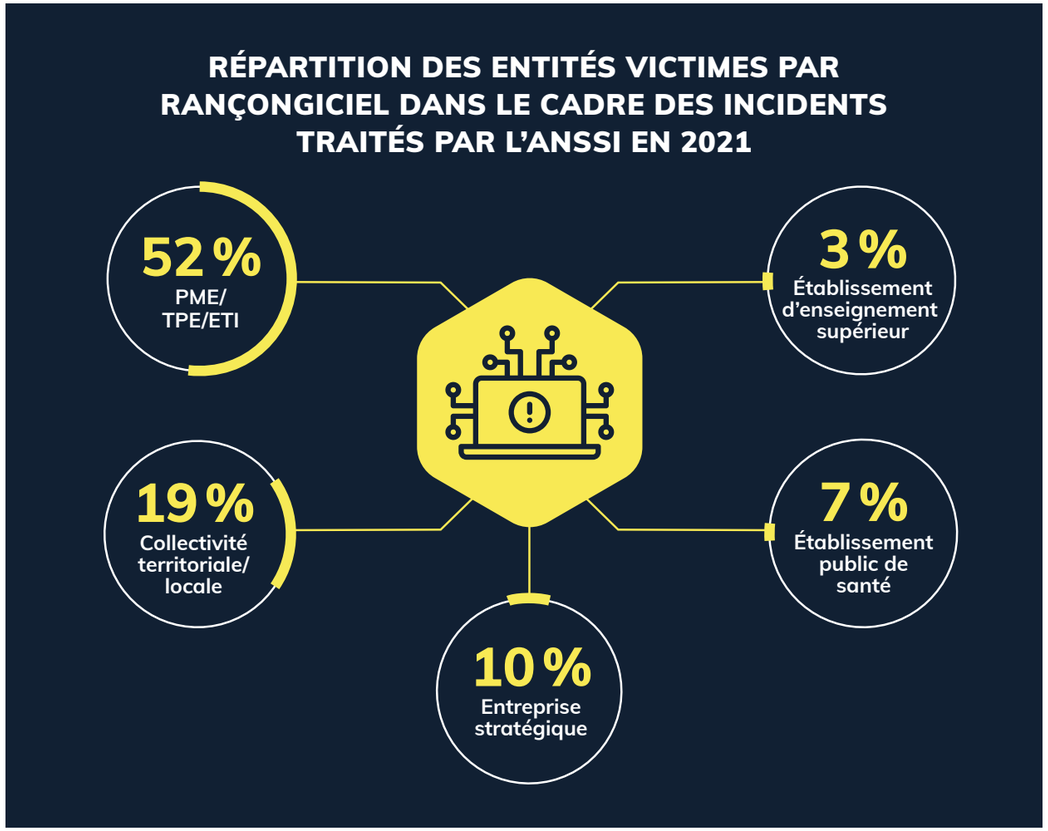
PAS DE RÉPIT POUR LES COLLECTIVITÉS

Les systèmes d'information de nos collectivités se sont complexifiés ces dernières années, avec l'apparition de nouveaux usages (e-services, vidéoprotection, télétravail, objets connectés, WiFi public). Les collectivités manipulent au quotidien de grandes quantités de données à caractère personnel en lien avec leurs activités, qui relèvent, pour certaines d'entre elles, du domaine juridique ou politique. Elles sont également tenues d'assurer la continuité du service public, et leur maturité en matière de sécurisation des systèmes d'information est très hétérogène. Autant d'éléments qui en font des cibles de choix, quelle que soit leur taille, pour les organisations cybercriminelles.

Pour les collectivités, l'inaccessibilité de tout ou partie des documents financiers et administratifs peut avoir des répercussions multiples, en particulier dans le domaine juridique. Elles ont donc tout intérêt à se saisir des enjeux cyber pour mieux protéger les données qu'elles manipulent et limiter (voire éviter) la perturbation de leurs activités en cas de cyberattaque.

Les principaux risques auxquels sont exposées les collectivités sont le rançongiciel, l'hameçonnage, le piratage de compte et la violation de données (en forte hausse)*.





QUELLES CONSÉQUENCES EN CAS DE CYBERATTAQUES VISANT DES COLLECTIVITÉS TERRITORIALES ?

D'une part, toutes les attaques visant un système d'information n'ont pas le même niveau de gravité. D'autre part, les collectivités n'ont pas toutes le même niveau de préparation, ni les mêmes capacités de réponse à incident. Voici quelques exemples de conséquences de cyberattaque sur le fonctionnement d'une collectivité :

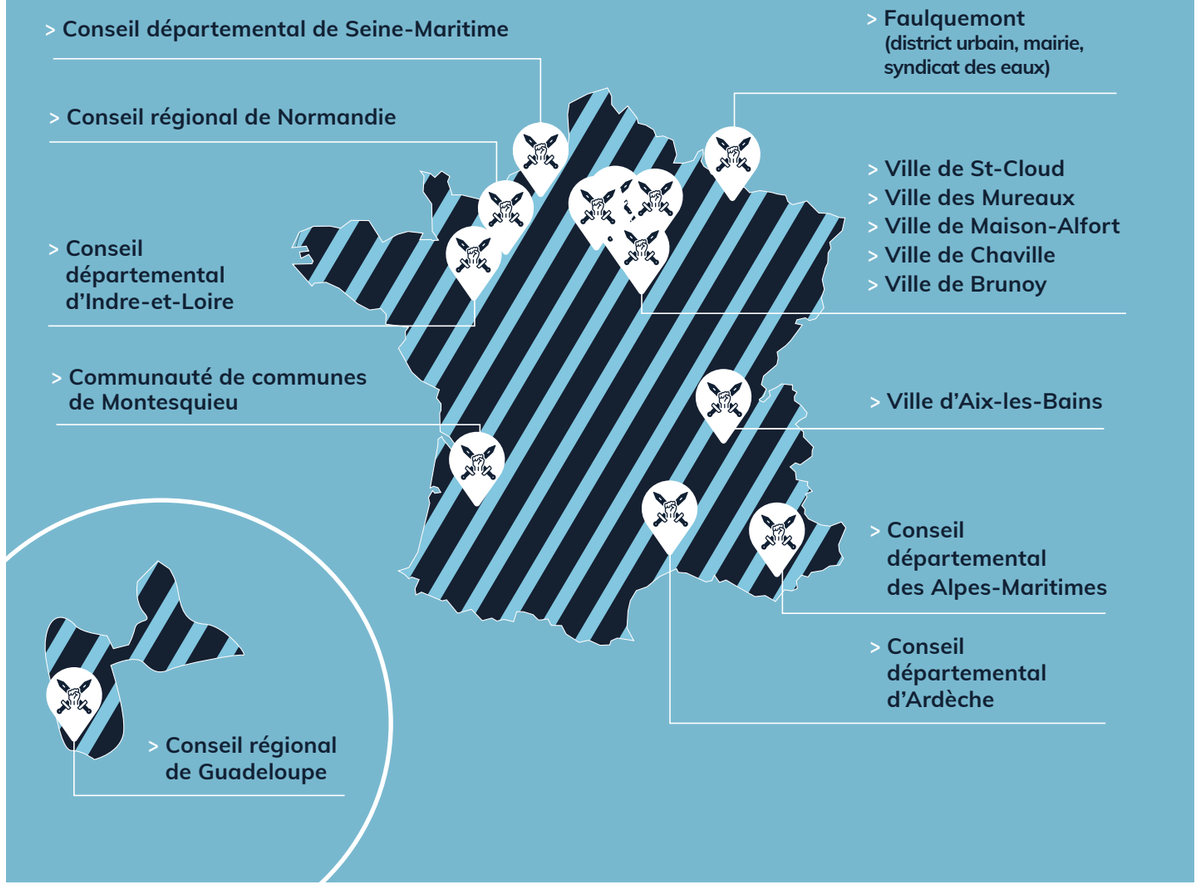
- Perturbation et dysfonctionnement des services publics locaux : restauration scolaire, gestion des finances publiques, état civil, versement d'allocations, gestion de l'eau, parkings, piscines, etc ;
- Fuite de données à caractère personnel (conséquences juridiques) ;
- Perte de données (parfois irrémédiable) ;
- Coût et délai de reconstruction du SI ;
- Atteinte à l'image et à la réputation, avec altération du lien de confiance avec les citoyens ;
- Impact psychologique sur les agents, sur l'équipe IT.

* Source ANSSI : https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf

UNE VAGUE DE CYBERATTAQUES DÉFERLE SUR LES COLLECTIVITÉS

PLUSIEURS COLLECTIVITÉS TERRITORIALES ONT ÉTÉ VICTIMES DE CYBERATTAQUES EN 2022*

JAN	FEV	MARS	AVRIL	MAI	JUIN	JUIL	AOÛT	SEPT	OCT	NOV	DÉC
1	0	2	1	0	1	1	0	2	3	3	1



*Liste non exhaustive en raison du trop grand nombre de collectivités touchées et de l'absence de communication de certaines d'entre elles.

QUEL PLAN D'ACTION POUR RENFORCER LA CYBERSÉCURITÉ DES COLLECTIVITÉS ET ADMINISTRATIONS ?

Des collectivités territoriales particulièrement affectées par les attaques par rançongiciel :

Les collectivités locales constituent la deuxième catégorie de victime la plus affectée par des attaques par rançongiciel derrière les TPE, PME et ETI. **Elles représentent ainsi 23 %** des incidents en lien avec des rançongiciels traités par ou rapportés à l'ANSSI en 2022. Les conséquences de ces attaques sont particulièrement importantes pour les collectivités concernées. Ces attaques parfois destructrices perturbent **notamment les services de paie, le versement des prestations sociales et la gestion de l'état civil**. Passé la découverte de l'attaque, le fonctionnement de ces entités continue d'être dégradé le temps de la reconstruction, affectant durablement les services à destination des administrés.

Accompagner les collectivités dans le renforcement de leur niveau de cybersécurité est aujourd'hui indispensable, mais surtout urgent. Les actions de sécurisation portent notamment sur la disponibilité du système d'information, l'intégrité des services fournis et des informations manipulées, ou encore la confidentialité des données gérées.
Les collectivités territoriales ont été les principales bénéficiaires (avec les établissements de santé) du volet cybersécurité du plan France Relance 2021-2022, intégré à la Stratégie Nationale de Cybersécurité dans le cadre du plan « France 2030 ». Ainsi, elles se sont vu attribuer 60 millions d'euros (sur la base du volontariat et d'une candidature), sur une enveloppe de 136 millions d'euros afin d'élever leur niveau de cybersécurité, en finançant concrètement :

- Des projets et des parcours de cybersécurité de systèmes d'information existants (avec un accompagnement de l'ANSSI adapté au niveau de maturité de chaque acteur),
- La création de centres régionaux de réponse à des incidents cyber (CSIRT).

Le déblocage d'une enveloppe supplémentaire de 30 millions d'euros à destination des collectivités, PME et ETI pour 2023 a été annoncé par Jean-Noël BARROT, Ministre délégué chargé de la Transition numérique et des Télécommunications. Concernant les collectivités, l'objectif est notamment de prolonger les parcours de sécurisation de 125 d'entre elles, et d'ouvrir l'accès à ces parcours à 50 collectivités supplémentaires. À la fin de l'année 2023, plus de 1 000 collectivités et administrations auront suivi ce parcours de sécurisation. Enfin, cette enveloppe financera également la création d'une plateforme de services mutualisés. L'objectif de cette plateforme clé en main est notamment de permettre aux collectivités et à toutes les communes, même les plus petites, de bénéficier d'un nom de domaine, d'une messagerie et de services en ligne sécurisés.

LES ÉTABLISSEMENTS DE SANTÉ SOUS TENSION

Avec de nombreux systèmes connectés et un matériel biomédical supporté par des systèmes informatiques hétérogènes, les établissements de santé constituent des cibles vulnérables pour les cyberattaquants. Ces établissements traitent de grande quantité de données de santé que les cybercriminels cherchent à se procurer.

Dans ce contexte de grande vulnérabilité, le risque cyber est désormais mieux pris en compte par les établissements de santé. Le niveau de maturité en sécurité informatique de ces établissements progresse, mais pas encore assez vite pour faire face à une menace cyber qui augmente (à la fois en volume et en sophistication) et à des groupes cybercriminels qui forment désormais une véritable industrie.

Il s'agit de se préparer à la survenue d'une cyberattaque, en particulier par rançongiciel, qui fait figure de risque numéro 1. Il y a aujourd'hui urgence à investir dans la protection cyber des établissements de santé pour leur permettre de continuer à assurer leurs missions quotidiennes et accueil et orientation des patients, fonctionnement des objets médicaux connectés, gestion de la restauration, organisation des services administratifs, protection des données médicales, etc. Il faut à la fois mieux équiper les établissements de santé, leur permettre de recruter davantage d'experts en sécurité informatique (en mutualisant les compétences) et sensibiliser leur personnel au risque cyber.

QUELLES CONSÉQUENCES EN CAS DE CYBERATTAQUES VISANT LES ÉTABLISSEMENTS DE SANTÉ ?

Les différentes activités du secteur de la santé reposent aujourd'hui presque en totalité sur le numérique. Résultat : tout incident de sécurité informatique peut avoir des conséquences directes ou indirectes sur la prise en charge des patients.

En fonction de la gravité de l'attaque et du niveau de préparation de l'établissement, le délai de remise à niveau peut varier de quelques jours à plusieurs mois, avec des conséquences parfois critiques :

- Mise en place d'un fonctionnement en mode dégradé du système de prise en charge des patients, arrêt temporaire de certaines activités de soins ;
- Dysfonctionnement de l'établissement : accueil des patients, matériel médical, accès, parking, restauration, énergie, biologie, etc ;
- Mise en danger potentielle des patients avec risque vital pour certains d'entre eux, dans le cas d'attaque de grande ampleur ;
- Risque de publication de données de santé à caractère personnel...

Si le nombre d'attaques par rançongiciel est en baisse sur l'année 2022, leurs conséquences demeurent très importantes, plus particulièrement dans des secteurs critiques comme la santé. Outre les conséquences financières, ce type d'évènement peut également avoir un impact sur le suivi des patients et la confidentialité de leurs données de santé. Dans la nuit du 20 au 21 août 2022, le Centre Hospitalier Sud Francilien a été victime d'une attaque par rançongiciel revendiquée par le groupe Lockbit. L'indisponibilité d'une partie des données et des applications portées par le système d'information a contraint les services hospitaliers à fonctionner en mode dégradé. En outre, le 23 septembre 2022, 11 gigaoctets de données exfiltrées lors de la compromission ont été publies sur le site web du groupe cybercriminel. Parmi les éléments divulgués figuraient notamment des données médicales et personnelles liées aux patients et au personnel hospitalier. Une situation similaire s'est répétée quelques mois plus tard au Centre Hospitalier de Versailles. (source panorama de la cybermenace 2022- ANSSI)

L'action des équipes techniques du Centre Hospitalier, assistées par l'ANSSI et par plusieurs prestataires, a permis un redémarrage des services critiques. La reconstruction sécurisée du système d'information ainsi que le retour à un fonctionnement normal nécessiteront un travail de long terme.

L'INTENSIFICATION DE LA MENACE CYBER PESANT SUR LES ÉTABLISSEMENTS DE SANTÉ

Les attaques par rançongiciel sont en recrudescence depuis cinq ans. Elles sont désormais menées par des groupes qui se professionnalisent. Les cybercriminels font même désormais pression sur leurs cibles en les menaçant de divulguer les données exfiltrées pour les amener à payer une rançon. Parce qu'ils assurent des activités particulièrement critiques et détiennent de grandes quantités de données de santé, les établissements de santé sont particulièrement exposés au risque cyber.

733
déclarations d'incident ont été gérées par le CERT Santé en 2021

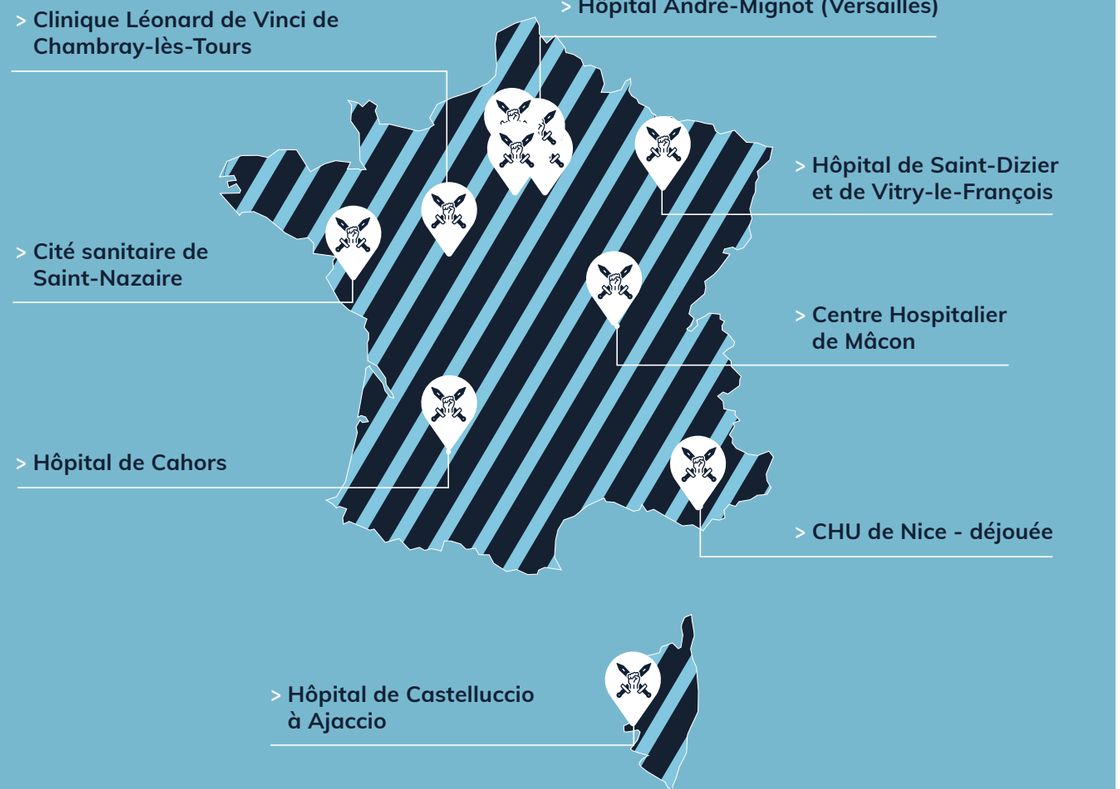
X2
soit le double par rapport à 2020*.

L'année 2022 a été marquée par deux cyberattaques d'envergure visant des établissements de soins : l'une sur le Centre Hospitalier Sud Francilien (CHSF) à Corbeil-Essonnes, le 21 août, et l'autre sur le Centre Hospitalier de Versailles (CHV), le 3 décembre. Dans les deux cas, les établissements ont déclenché leur plan blanc et réussi à maintenir la sécurité des soins. Des patients ont été transférés vers d'autres établissements. Tous les incidents de sécurité affectant des établissements de santé n'atteignent pas ce niveau de gravité, mais ils sont fréquents.

* Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf

ÉTABLISSEMENTS DE SANTÉ TOUCHÉS PAR UNE CYBERATTAQUE EN 2022

JAN	FEV	MARS	AVRIL	MAI	JUIN	JUI	AOÛT	SEPT	OCT	NOV	DÉC
2	0	1	1	1	0	0	1	1	1	0	3



RENFORCER LA CYBERSÉCURITÉ DES ÉTABLISSEMENTS DE SANTÉ : PLAN D'ACTION

Les établissements de santé ne peuvent relever seuls le défi de la cybersécurité. L'État s'engage à leurs côtés et les soutient pour leur permettre d'améliorer leur niveau de résilience en matière de cybersécurité.

Dans le cadre du plan France Relance 2021-2022, 25 millions d'euros ont été attribués au secteur de la santé pour la sécurisation des établissements de santé, du ministère et des organismes qui en dépendent. Concrètement, ce montant a permis aux acteurs de la santé de financer des prestations et des produits de cybersécurité.

20 millions d'euros supplémentaires ont été attribués à l'ANSSI pour la cybersécurité des établissements de santé suite à l'attaque du Centre Hospitalier sud francilien. Objectif : financer des actions de renforcement du niveau de cybersécurité des établissements de santé.

142
établissements de santé désignés « Opérateurs de services essentiels » (OSE)

13
CHU désignés « Opérateurs d'importance vitale » (OIV)

UN NOUVEAU GUIDE CYBERSÉCURITÉ À DESTINATION DU MÉDICO-SOCIAL

Ce guide d'information et de sensibilisation **répond à 13 questions** concrètes que se posent les établissements et services médico-sociaux, ressources et conseils à l'appui.

*Source : Agence du numérique en santé https://esante.gouv.fr/actualites/un-nouveau-guide-cybersecurite-destination-du-medico-social

DE NOUVEAUX ENGAGEMENTS POUR RENFORCER LA CYBERSÉCURITÉ DES ÉTABLISSEMENTS DE SANTÉ ONT ÉTÉ PRIS PAR LE GOUVERNEMENT EN DÉCEMBRE 2022* :

- Lancement d'un programme de préparation aux incidents cyber, avec pour objectif que « 100 % des établissements de santé les plus prioritaires aient réalisé de nouveaux exercices d'ici mai 2023 »,
- Élaboration d'un plan blanc numérique au premier trimestre 2023 « pour doter les établissements des réflexes et pratiques à adopter si un incident cyber survient »,
- Mutualisation des ressources compétentes au niveau de chaque région en lien avec les agences régionales de santé (ARS),
- Création d'une task force pour bâtir d'ici mars 2023 un nouveau projet de plan cyber pluriannuel, dans le cadre de la nouvelle feuille de route 2023-2027 du numérique en santé.

PRIVILÉGIER ET SOUTENIR LES SOLUTIONS DE CONFIANCE NATIONALES

CHOISIR DES SOLUTIONS SOUVERAINES

Ces menaces font désormais peser de grands risques sur la poursuite d'activité des collectivités ainsi que sur des secteurs stratégiques de notre pays. Ces enjeux, par nature géopolitique, appellent une réponse réfléchie qui pose la question et l'opportunité de choix techniques et technologiques forts.

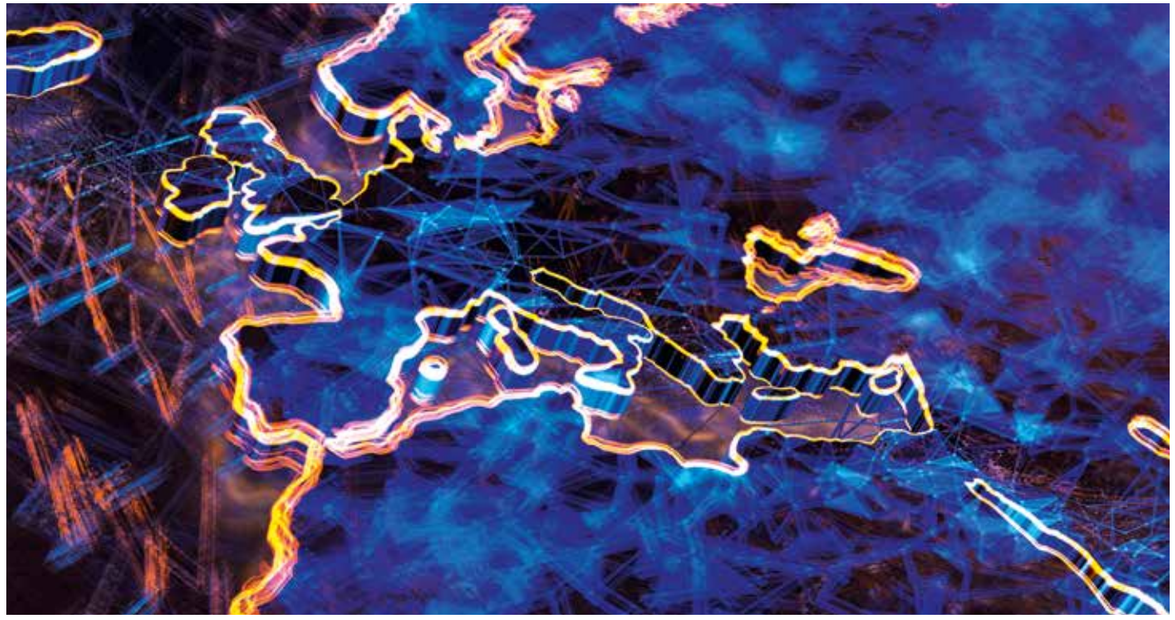
Placer la souveraineté au cœur de nos décisions d'achat devient un enjeu de cyber résilience. Maintenir nos données sur le sol européen, préserver notre R&D ainsi qu'une partie des emplois de demain deviennent le corollaire nécessaire pour rendre la chaîne de valeur cohérente et impliquée. La cybersécurité est une compétence stratégique. Il est essentiel de la développer et de la maintenir sur notre sol et d'accompagner les synergies entre les territoires et les entreprises made in France de cybersécurité et du cloud. L'industrie cyber française est dynamique et son offre est diversifiée.

RÉPONDRE À L'URGENCE NUMÉRIQUE

Les établissements publics doivent rapidement se doter de solutions et services pour répondre à l'urgence numérique et devenir davantage résistants, à court terme, face aux cyberattaques.

Dans ce domaine, l'offre française s'est grandement enrichie et diversifiée, à tel point qu'il est désormais possible de choisir des solutions françaises ou européennes répondant aux standards de qualité nécessaires, tout en respectant les règles de la commande publique. Nous pouvons nous appuyer sur un tissu industriel français très actif. Ce catalogue de solutions et de services le prouve. Celui-ci permet aux collectivités, établissements de santé, structures sanitaires, sociales et médico-sociales de trouver des solutions concrètes, souveraines et adaptées aux besoins de sécurisation de leur système d'information.

Choisir ces solutions innovantes et souveraines permet de répondre aux exigences des recommandations cyber de l'ANSSI et d'atteindre les objectifs opérationnels de ses différents parcours.



SOUTENIR L'ÉCOSYSTÈME FRANÇAIS DE LA CYBERSÉCURITÉ

À plus long terme, investir dans des solutions souveraines est une démarche responsable. La transformation et la sécurisation de nos établissements publics passent par le choix de solutions de confiance nationales. Opter pour des solutions françaises permet d'être certain que nos données soient bien protégées conformément aux réglementations en vigueur.

Soutenir l'écosystème national de la cybersécurité contribue à valider la proposition de valeur d'entreprises françaises, lesquelles contribuent aux finances publiques via le paiement des charges sociales et de l'impôt sur les sociétés. Cela permet également de reconnaître la qualité des formations et d'accompagner le développement de l'emploi dans les territoires. Pouvoir s'appuyer au quotidien sur une équipe formée et disponible est un atout certain pour lutter contre les menaces cyber pesant actuellement sur les établissements publics.

CESIN

coTer numérique

CDSE CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

CLUSIF

Alain **BOUILLÉ**

Délégué Général du CESIN

Le CESIN est fier d'apporter son soutien à la deuxième édition de cette brochure capacitaire mettant en avant les solutions de cybersécurité « made in France ».
La transformation numérique des entreprises et des administrations entraine de facto une augmentation de leur surface d'attaque et se protéger correctement devient un véritable challenge voire un casse-tête pour leurs dirigeants. Toutes les entreprises n'ont pas les moyens d'être soutenues par un spécialiste de la sécurité numérique et cette brochure doit permettre au dirigeant d'y voir plus clair en matière de protection contre les cyberattaques.
La menace est toujours très présente, mais l'anticipation lorsqu'elle est mise en œuvre porte ses fruits et des mesures bien orchestrées de prévention, protection et détection sont à la portée de toutes les organisations pour peu que la prise de conscience par le dirigeant n'arrive pas post-crise.

Antoine **TRILLARD**

Président de Coter-Numérique

La complexité des SI de nos collectivités par l'apparition de nouveaux usages depuis plusieurs années (e-services, vidéoprotection, télétravail, IoT, WiFi Public) et la montée en charge de la cybercriminalité ces dernières années, font de la sécurité informatique un axe prioritaire de nos collectivités.

La sécurité des SI reste une problématique de tous les instants.

C'est pourquoi il est nécessaire d'être extrêmement vigilant sur les incontournables de la sécurité (sauvegarde immuable, AD durci, MàJ, EDR, sécurisation (mail,web,vpn).

Enfin dans le cadre du plan de relance pour les collectivités, le parcours cyber de l'ANSSI permet d'établir pour chacune d'elles une feuille de route claire avec des priorités réalisables et la mise en place d'outils français financés par ce plan répondant à des besoins réels.

Jean-Paul **BONNET**

Président de la commission
« Cybersécurité et Protection de l'information »
du Club des directeurs de sécurité des entreprises

L'actualité le démontre jour après jour : aucune organisation ou collectivité, quelle que soit sa taille ou sa mission, n'est à l'abri d'actes de cybermalveillance aux conséquences parfois désastreuses.

Ainsi, dans un monde toujours plus connecté, la protection des systèmes d'information et des données de toute organisation, salariés, agents, usagers ou clients devient une préoccupation constante. Afin de limiter le risque d'ingérence malveillante et de mieux protéger ses données, il devient crucial de renforcer sa posture de cybersécurité en se tournant vers des solutions souveraines, de confiance. Ce catalogue offre un bon aperçu d'une offre tricolore efficace et innovante, en capacité de répondre aux besoins de tout un chacun, quelle que soit l'organisation.

Luména **DULUC**

Directrice du Clusif

Prendre en compte le risque cyber doit désormais être considéré comme une priorité absolue par les organisations. Il est impératif de prendre des mesures pour le gérer efficacement. L'actualité en fait écho, les menaces en ligne peuvent causer des dommages considérables à la vie privée, à l'économie et menace jusqu'à l'intégrité physique des personnes. Les organisations doivent donc mettre en place des mesures de sécurité solides pour protéger à la fois leur capital informationnel et leurs données sensibles. Il est également important de former les employés à la cybersécurité.

Au-delà du partage de connaissance et d'expériences issu de ses publications et de ses conférences, le Clusif soutient toute action qui vise à renforcer la sécurité informatique de nos organisations.

COMMENT UTILISER CE DOCUMENT

Ce document a été conçu pour répondre aux besoins de toute organisation, **publique ou privée**, cherchant à améliorer son niveau de cybersécurité et recherchant des solutions, produits et offres de confiance disponibles dans ce domaine.

Pour faciliter l'utilisation de ce document, nous avons gardé la démarche appliquée par l'ANSSI, permettant ainsi d'accompagner le volet investissement du pack relais. Cette démarche s'appuie sur 4 Parcours de cybersécurité, chaque parcours s'articulant autour de 8 thèmes adaptés, déclinés en fonction des enjeux et des menaces de chaque organisation.

* https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/

1 PARCOURS FONDATION

- Ce parcours est adapté aux organisations disposant de ressources limitées (humaines, financières et techniques)

2 PARCOURS INTERMÉDIAIRE

- Ce parcours est destiné aux organisations souhaitant recruter un référent en cybersécurité ou disposant en interne d'un référent junior à faire monter en compétence

3 PARCOURS AVANCÉ

- Ce parcours est prévu pour les organisations qui disposent, en interne et à temps plein, d'un spécialiste en cybersécurité ou d'un RSSI

4 PARCOURS RENFORCÉ

- Ce parcours vise à obtenir un niveau comparable à celui des organisations d'un opérateur essentiel ou vital

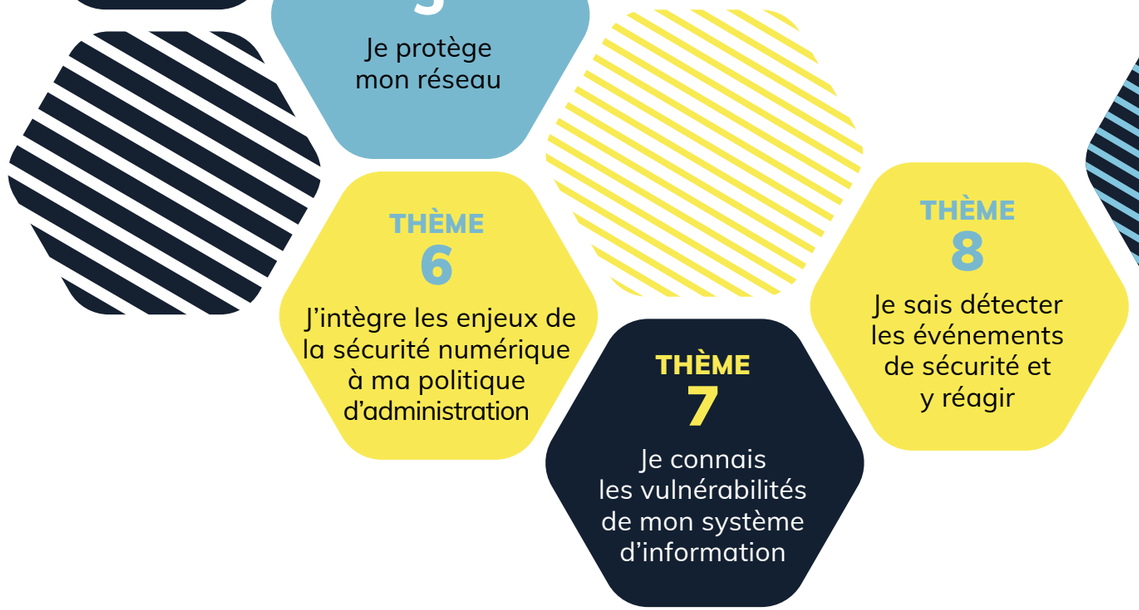
Nous avons donc réparti les solutions de ce guide selon ces parcours et ces thèmes. Toutefois certaines remarques doivent être prises en compte :

- Pour une meilleure lisibilité du document, nous avons simplifié et regroupé certains sous-thèmes détaillés par l'ANSSI dans les parcours de cybersécurité. Ainsi par exemple le thème 1 du parcours fondation « Je m'organise et je sensibilise face au risque numérique » a été divisé en deux sous-thèmes : « Identification des partenaires » et « Sensibilisation ».
- Certains sous-thèmes apparaissent dans plusieurs parcours et plusieurs thèmes. Les parcours étant disjoints, nous avons répété les sous-thèmes dans chaque parcours. Par exemple, le sous-thème « Gestion des logs » apparaît ainsi dans les parcours « Intermédiaire » et « Avancé ».

Les tableaux qui suivent (un par parcours) comportent donc chacun :

Selon les lignes horizontales, les différents thèmes et sous-thèmes du parcours considéré.

Selon les colonnes verticales, les sociétés offrant des solutions et/ou services en réponse aux thèmes et sous-thèmes associés.



1

PARCOURS
FONDATION

1 PARCOURS FONDATION

	OUTSCALE	6CURE	AISI	ALGOSECURE	ANTEMETA	ATEMPO	AVANT DE CLIQUER	BOARD OF CYBER	BRAIN NETWORKS	BRAINWAVE GRC	CONSCIO TECHNOLOGIES	CONTINUS.IO
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires												
Sensibilisation						✓	✓			✓		
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion centralisée des identités									✓			
Gestion des mots de passe				✓								
Protection des accès distants				✓								
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Analyse des vulnérabilités			✓			✓			✓		✓	
Protection de la messagerie					✓	✓						
Protection des services exposés sur Internet		✓		✓				✓				
Thème 4 : Je sécurise mes équipements de travail												
Inventaire des équipements												
Antivirus					✓							
Firewall					✓							
Gestion des mises à jour des postes de travail												
Thème 5 : Je protège mon réseau												
Cartographie du réseau												
Protection des accès réseau Wi-Fi								✓				
Filtrage Réseau		✓										
Proxy												
VPN	✓											
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Gestion des comptes à privilèges								✓	✓			
Authentification et contrôle d'accès	✓								✓			
Sécurité des flux d'administration												
Gestion des mises à jour des serveurs et applications												
Dispositif de sauvegarde					✓	✓						
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité du SI exposé sur Internet			✓				✓	✓				
Audit organisationnel de sécurité			✓	✓			✓					
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion d'incidents de sécurité		✓	✓		✓							

	CROWDSEC	CRYPTONEXT SECURITY	CYBER-DETECT	CYBERVADIS	CYBERWATCH	DEVENSYS CYBERSECURITY	DIGITALBERRY	EBRC	EGERIE	EQUISIGN	ERCOM	EVERTRUST SAS
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires												
Sensibilisation								✓	✓			
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion centralisée des identités					✓							
Gestion des mots de passe												
Protection des accès distants	✓	✓								✓	✓	
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Analyse des vulnérabilités				✓					✓			
Protection de la messagerie		✓								✓	✓	
Protection des services exposés sur Internet	✓					✓				✓		✓
Thème 4 : Je sécurise mes équipements de travail												
Inventaire des équipements									✓			
Antivirus			✓									
Firewall												
Gestion des mises à jour des postes de travail				✓								
Thème 5 : Je protège mon réseau												
Cartographie du réseau						✓						
Protection des accès réseau Wi-Fi												✓
Filtrage Réseau	✓											
Proxy												
VPN		✓								✓		
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Gestion des comptes à privilèges					✓							
Authentification et contrôle d'accès		✓			✓	✓						✓
Sécurité des flux d'administration						✓						
Gestion des mises à jour des serveurs et applications				✓								
Dispositif de sauvegarde							✓			✓		
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité du SI exposé sur Internet			✓	✓								
Audit organisationnel de sécurité			✓				✓					
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion d'incidents de sécurité			✓		✓		✓					

1 PARCOURS FONDATION

	EXAMIN	EXO PLATEFORM	F24 FRANCE SAS	FORMIND	GATEWATCHER	GLIMPS	HARFANGLAB	HIASECURE	HOLISEUM	IDENTO I-TRACING GROUP	ILEX - INETUM GROUP	ISE SYSTEMS
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires	✓											
Sensibilisation				✓					✓			✓
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion centralisée des identités		✓					✓			✓	✓	
Gestion des mots de passe								✓		✓	✓	
Protection des accès distants								✓			✓	
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Analyse des vulnérabilités									✓			✓
Protection de la messagerie						✓						
Protection des services exposés sur Internet		✓				✓		✓				
Thème 4 : Je sécurise mes équipements de travail												
Inventaire des équipements					✓							
Antivirus					✓	✓						
Firewall												
Gestion des mises à jour des postes de travail												
Thème 5 : Je protège mon réseau												
Cartographie du réseau					✓							
Protection des accès réseau Wi-Fi												
Filtrage Réseau												
Proxy												
VPN												
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Gestion des comptes à privilèges									✓			
Authentification et contrôle d'accès							✓		✓	✓		
Sécurité des flux d'administration												
Gestion des mises à jour des serveurs et applications												
Dispositif de sauvegarde		✓										
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité du SI exposé sur Internet				✓				✓				✓
Audit organisationnel de sécurité				✓				✓				
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion d'incidents de sécurité			✓	✓	✓	✓						✓

	JALIOS	JAMESPOT	JSCRAMBLER	KDDI FRANCE	KUB CLEANER	LEVIIA	LOGIN SÉCURITÉ	MAILINBLACK	MAKE IT SAFE	MEROX	METSYS	MOABI
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires			✓					✓				
Sensibilisation		✓					✓	✓				
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion centralisée des identités	✓			✓	✓					✓		
Gestion des mots de passe												
Protection des accès distants	✓	✓		✓	✓							
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Analyse des vulnérabilités			✓	✓		✓						
Protection de la messagerie							✓		✓			
Protection des services exposés sur Internet			✓						✓			
Thème 4 : Je sécurise mes équipements de travail												
Inventaire des équipements												
Antivirus				✓			✓					
Firewall												
Gestion des mises à jour des postes de travail												
Thème 5 : Je protège mon réseau												
Cartographie du réseau												
Protection des accès réseau Wi-Fi												
Filtrage Réseau			✓									
Proxy												
VPN												
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Gestion des comptes à privilèges										✓		
Authentification et contrôle d'accès	✓				✓					✓		
Sécurité des flux d'administration												
Gestion des mises à jour des serveurs et applications										✓		
Dispositif de sauvegarde		✓	✓									
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité du SI exposé sur Internet		✓				✓						✓
Audit organisationnel de sécurité						✓		✓				✓
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion d'incidents de sécurité			✓		✓	✓		✓	✓			

1 PARCOURS FONDATION

	NAMESHIELD	NEOWAVE	NETEXPLORER	OLFEO	OLVID	ON-X GROUPE	OODRIVE	OVERSOC	PATROWL	PRIM'X	PRIZM	PROHACKTIVE
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires												
Sensibilisation	✓			✓		✓	✓					
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion centralisée des identités		✓								✓		
Gestion des mots de passe										✓		
Protection des accès distants								✓				
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Analyse des vulnérabilités						✓		✓	✓			✓
Protection de la messagerie	✓	✓			✓					✓	✓	
Protection des services exposés sur Internet	✓		✓									
Thème 4 : Je sécurise mes équipements de travail												
Inventaire des équipements							✓					✓
Antivirus												
Firewall												
Gestion des mises à jour des postes de travail							✓					
Thème 5 : Je protège mon réseau												
Cartographie du réseau							✓					✓
Protection des accès réseau Wi-Fi				✓								
Filtrage Réseau												
Proxy				✓								
VPN												
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Gestion des comptes à privilèges			✓							✓		
Authentification et contrôle d'accès		✓	✓		✓				✓	✓		
Sécurité des flux d'administration			✓									
Gestion des mises à jour des serveurs et applications												✓
Dispositif de sauvegarde												
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité du SI exposé sur Internet	✓							✓				
Audit organisationnel de sécurité						✓						
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion d'incidents de sécurité						✓						

	QONTROL	RETARUS	SATELLIZ	SCALAIR	SECLAB	SEELA	SEKOIA.IO	SMART GLOBAL GOVERNANCE	SNOWPACK	SURICATE	SYNETIS	TENACY
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires												✓
Sensibilisation	✓					✓						
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion centralisée des identités										✓		
Gestion des mots de passe	✓				✓							
Protection des accès distants										✓		
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Analyse des vulnérabilités						✓				✓		
Protection de la messagerie		✓		✓								
Protection des services exposés sur Internet		✓				✓		✓				
Thème 4 : Je sécurise mes équipements de travail												
Inventaire des équipements	✓											
Antivirus												
Firewall				✓		✓						
Gestion des mises à jour des postes de travail									✓			
Thème 5 : Je protège mon réseau												
Cartographie du réseau												
Protection des accès réseau Wi-Fi												
Filtrage Réseau				✓	✓			✓				
Proxy												
VPN								✓				
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Gestion des comptes à privilèges			✓									
Authentification et contrôle d'accès											✓	
Sécurité des flux d'administration		✓		✓		✓		✓				
Gestion des mises à jour des serveurs et applications		✓		✓					✓			
Dispositif de sauvegarde	✓	✓	✓									
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité du SI exposé sur Internet	✓						✓					
Audit organisationnel de sécurité					✓		✓					
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion d'incidents de sécurité		✓				✓	✓					

1 PARCOURS FONDATION

	TERSEDIA	THEGREENBOW	TIXEO	TRANQUIL IT	TRUSTBUILDER	TRUST HQ	TRUSTINSOFT	UBIKA	VADE	WALLIX	WHALLER	YESWEHACK	YOGOSHA
Thème 1 : Je m'organise et je sensibilise face au risque numérique													
Identification des partenaires					✓								
Sensibilisation									✓				
Thème 2 : Je maîtrise les accès à mon système d'information													
Gestion centralisée des identités				✓	✓								
Gestion des mots de passe										✓			
Protection des accès distants	✓	✓			✓					✓	✓		
Thème 3 : Je sécurise mes données, mes applications et services numériques													
Analyse des vulnérabilités	✓					✓					✓	✓	✓
Protection de la messagerie	✓		✓				✓	✓					
Protection des services exposés sur Internet						✓	✓					✓	✓
Thème 4 : Je sécurise mes équipements de travail													
Inventaire des équipements				✓									
Antivirus													
Firewall											✓		
Gestion des mises à jour des postes de travail				✓									
Thème 5 : Je protège mon réseau													
Cartographie du réseau												✓	
Protection des accès réseau Wi-Fi													
Filtrage Réseau						✓	✓						
Proxy													
VPN		✓											
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration													
Gestion des comptes à privilèges										✓			
Authentification et contrôle d'accès		✓			✓					✓			
Sécurité des flux d'administration													
Gestion des mises à jour des serveurs et applications				✓									
Dispositif de sauvegarde	✓												
Thème 7 : Je connais les vulnérabilités de mon système d'information													
Scans de vulnérabilité du SI exposé sur Internet												✓	
Audit organisationnel de sécurité						✓							
Thème 8 : Je sais détecter les événements de sécurité et y réagir													
Gestion d'incidents de sécurité									✓		✓		

2 PARCOURS INTERMÉDIAIRE

2 PARCOURS INTERMÉDIAIRE

	OUTSCALE	6CURE	AISI	ALGOSECURE	ANTEMETA	ARCAD SOFTWARE	ATEMPO	AVANT DE CLIQUER	BOARD OF CYBER	BRAIN NETWORKS	BRAINWAVE GRC	CONSCIO TECHNOLOGIES
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires												
Politique SSI			✓	✓								
Sensibilisation							✓	✓			✓	
Analyse de risques		✓										
Test de phishing							✓					
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion du cycle de vie des utilisateurs et des habilitations										✓		
Coffres-forts de mots de passe												
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Approche Security-by-design			✓									
Chiffrement des données						✓						
Gestion des mises à jour de sécurité												
Sécurisation du réseau	✓	✓	✓							✓		
Sécurité applicative												
Thème 4 : Je sécurise mes équipements de travail												
End point security			✓				✓			✓		
Gestion centralisée des appareils mobiles												
Thème 5 : Je protège mon réseau												
Filtrage Réseau		✓		✓								
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Cartographie de l'infrastructure du SI											✓	
Gestion des comptes de service											✓	
Sécurisation des services Cloud (IaaS/PaaS)	✓											
Contrôle d'accès physique												
Restauration de l'activité / PRA					✓		✓					
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité sur tout le SI					✓					✓		
Gouvernance des Identités et des Accès				✓								
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs					✓					✓		
Gestion d'incidents de sécurité	✓	✓		✓	✓							
Arrêt d'urgence												

	CONTINUS.IO	CROWDSEC	CRYPTONEXT SECURITY	CYBER-DETECT	CYBERVADIS	CYBERWATCH	DASTRA	DEVENSYS CYBERSECURITY	DIGITALBERRY	EBRC	EGERIE	EQUISIGN
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires												
Politique SSI				✓					✓	✓		
Sensibilisation									✓			
Analyse de risques				✓		✓			✓	✓		
Test de phishing							✓					
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion du cycle de vie des utilisateurs et des habilitations												
Coffres-forts de mots de passe												
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Approche Security-by-design	✓									✓	✓	
Chiffrement des données		✓						✓			✓	
Gestion des mises à jour de sécurité				✓								
Sécurisation du réseau		✓										
Sécurité applicative	✓	✓	✓					✓				
Thème 4 : Je sécurise mes équipements de travail												
End point security		✓		✓								
Gestion centralisée des appareils mobiles												
Thème 5 : Je protège mon réseau												
Filtrage Réseau							✓					
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Cartographie de l'infrastructure du SI				✓	✓			✓		✓		
Gestion des comptes de service												
Sécurisation des services Cloud (IaaS/PaaS)		✓	✓									
Contrôle d'accès physique												
Restauration de l'activité / PRA									✓			
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité sur tout le SI				✓								
Gouvernance des Identités et des Accès							✓	✓				
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs		✓					✓					
Gestion d'incidents de sécurité												
Arrêt d'urgence												

2 PARCOURS INTERMÉDIAIRE

	ERCOM	EVERTRUST SAS	EXAMIN	EXO PLATEFORM	F24 FRANCE SAS	FORMIND	GATEWATCHER	GLIMPS	HARFANGLAB	HIASECURE	HOLISEUM	IDENTO I-TRACING GROUP
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires												
Politique SSI			✓	✓		✓					✓	
Sensibilisation												
Analyse de risques			✓			✓					✓	
Test de phishing						✓						
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion du cycle de vie des utilisateurs et des habilitations												✓
Coffres-forts de mots de passe										✓		✓
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Approche Security-by-design	✓			✓							✓	
Chiffrement des données	✓	✓										
Gestion des mises à jour de sécurité												
Sécurisation du réseau	✓	✓					✓	✓				
Sécurité applicative				✓								
Thème 4 : Je sécurise mes équipements de travail												
End point security	✓							✓	✓	✓		
Gestion centralisée des appareils mobiles												
Thème 5 : Je protège mon réseau												
Filtrage Réseau												
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Cartographie de l'infrastructure du SI							✓					
Gestion des comptes de service				✓						✓		
Sécurisation des services Cloud (IaaS/PaaS)		✓					✓	✓				
Contrôle d'accès physique												
Restauration de l'activité / PRA												
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité sur tout le SI											✓	
Gouvernance des Identités et des Accès		✓				✓				✓		✓
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs									✓			
Gestion d'incidents de sécurité					✓		✓	✓	✓			
Arrêt d'urgence												

	ILEX INETUM GROUP	ISE SYSTEMS	JALIOS	JAMESPOT	JSCRAMBLER	KDDI FRANCE	KUB CLEANER	LEVIIA	LOGIN SÉCURITÉ	MAILINBLACK	MAKE IT SAFE	MEROX
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires				✓						✓		
Politique SSI			✓					✓		✓	✓	
Sensibilisation		✓		✓			✓		✓			
Analyse de risques												
Test de phishing		✓						✓	✓			
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion du cycle de vie des utilisateurs et des habilitations	✓		✓									
Coffres-forts de mots de passe	✓											
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Approche Security-by-design							✓			✓		
Chiffrement des données							✓					
Gestion des mises à jour de sécurité					✓							
Sécurisation du réseau					✓		✓					
Sécurité applicative				✓	✓							
Thème 4 : Je sécurise mes équipements de travail												
End point security					✓		✓					
Gestion centralisée des appareils mobiles							✓					
Thème 5 : Je protège mon réseau												
Filtrage Réseau												
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Cartographie de l'infrastructure du SI												✓
Gestion des comptes de service												
Sécurisation des services Cloud (IaaS/PaaS)					✓							
Contrôle d'accès physique					✓							
Restauration de l'activité / PRA				✓								
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité sur tout le SI					✓			✓	✓			
Gouvernance des Identités et des Accès	✓											✓
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs		✓						✓				
Gestion d'incidents de sécurité		✓		✓						✓	✓	
Arrêt d'urgence												

2 PARCOURS INTERMÉDIAIRE

	METSYS	MOABI	NAMESHIELD	NEOWAVE	NETEXPLORER	OLFEO	OLVID	ON-X GROUPE	OODRIVE	OVERSOC	PATROWL	PRIM'X
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires								✓				
Politique SSI			✓			✓						
Sensibilisation							✓	✓				
Analyse de risques								✓	✓			
Test de phishing												
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion du cycle de vie des utilisateurs et des habilitations	✓											
Coffres-forts de mots de passe												
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Approche Security-by-design		✓			✓		✓					
Chiffrement des données			✓	✓	✓		✓					✓
Gestion des mises à jour de sécurité	✓							✓		✓		
Sécurisation du réseau				✓		✓				✓		
Sécurité applicative		✓					✓			✓		
Thème 4 : Je sécurise mes équipements de travail												
End point security	✓											✓
Gestion centralisée des appareils mobiles								✓				
Thème 5 : Je protège mon réseau												
Filtrage Réseau			✓			✓						
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Cartographie de l'infrastructure du SI										✓	✓	
Gestion des comptes de service					✓							
Sécurisation des services Cloud (IaaS/PaaS)	✓			✓						✓	✓	
Contrôle d'accès physique				✓								
Restauration de l'activité / PRA					✓							
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité sur tout le SI										✓		
Gouvernance des Identités et des Accès												
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs												
Gestion d'incidents de sécurité								✓				
Arrêt d'urgence												

	PRIZM	PROHACKTIVE	QONTROL	RETARUS	SATELLIZ	SCALAIR	SECLAB	SEKOIA.IO	SNOWPACK	SURICATE	SYNETIS	TENACY
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Identification des partenaires											✓	
Politique SSI	✓		✓							✓	✓	
Sensibilisation												
Analyse de risques											✓	
Test de phishing												
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion du cycle de vie des utilisateurs et des habilitations	✓											
Coffres-forts de mots de passe						✓						
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Approche Security-by-design		✓	✓					✓		✓		
Chiffrement des données												
Gestion des mises à jour de sécurité						✓			✓			
Sécurisation du réseau		✓					✓	✓	✓			
Sécurité applicative		✓										
Thème 4 : Je sécurise mes équipements de travail												
End point security			✓		✓	✓		✓	✓	✓		
Gestion centralisée des appareils mobiles												
Thème 5 : Je protège mon réseau												
Filtrage Réseau			✓			✓						
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Cartographie de l'infrastructure du SI		✓										
Gestion des comptes de service	✓											
Sécurisation des services Cloud (IaaS/PaaS)			✓	✓	✓		✓					
Contrôle d'accès physique												
Restauration de l'activité / PRA				✓	✓							
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Scans de vulnérabilité sur tout le SI		✓										
Gouvernance des Identités et des Accès	✓		✓									
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs				✓			✓					
Gestion d'incidents de sécurité			✓	✓			✓				✓	
Arrêt d'urgence												

2 PARCOURS INTERMÉDIAIRE

	TERSEDIA	THEGREENBOW	TIXEO	TRANQUIL IT	TRUSTBUILDER	TRUST HQ	TRUSTINSOFT	UBIKA	VADE	WALLIX	WHALLER	YESWEHACK	YOGOSHA
Thème 1 : Je m'organise et je sensibilise face au risque numérique													
Identification des partenaires						✓							
Politique SSI													
Sensibilisation								✓					
Analyse de risques													
Test de phishing								✓					
Thème 2 : Je maîtrise les accès à mon système d'information													
Gestion du cycle de vie des utilisateurs et des habilitations					✓								
Coffres-forts de mots de passe									✓				
Thème 3 : Je sécurise mes données, mes applications et services numériques													
Approche Security-by-design	✓		✓	✓			✓	✓		✓	✓	✓	✓
Chiffrement des données		✓	✓								✓	✓	
Gestion des mises à jour de sécurité			✓	✓									
Sécurisation du réseau	✓												
Sécurité applicative							✓	✓					
Thème 4 : Je sécurise mes équipements de travail													
End point security	✓	✓		✓					✓				
Gestion centralisée des appareils mobiles				✓									
Thème 5 : Je protège mon réseau													
Filtrage Réseau													
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration													
Cartographie de l'infrastructure du SI												✓	
Gestion des comptes de service									✓				
Sécurisation des services Cloud (IaaS/PaaS)	✓				✓					✓			
Contrôle d'accès physique													
Restauration de l'activité / PRA													
Thème 7 : Je connais les vulnérabilités de mon système d'information													
Scans de vulnérabilité sur tout le SI												✓	
Gouvernance des Identités et des Accès					✓								
Thème 8 : Je sais détecter les événements de sécurité et y réagir													
Gestion des logs								✓		✓			
Gestion d'incidents de sécurité								✓					
Arrêt d'urgence													

3 PARCOURS AVANCÉ

3 PARCOURS AVANCÉ

	OUTSCALE	6CURE	AISI	ALGOSECURE	ANTEMETA	ARCAD SOFTWARE	ATEMPO	AVANT DE CLIQUER	BRAIN NETWORKS	BRAINWAVE GRC	CONSCIO TECHNOLOGIES	CONTINUS.IO
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Organisation et pilotage de la SSI				✓								
Sensibilisation et formation										✓		
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion des droits d'accès									✓			
Revues d'habilitations									✓			
Authentification forte					✓			✓				
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Homologation des SI sensibles				✓		✓						
Audit, scan, revue de code									✓			
Web application firewall												
Effacement des données						✓						
Thème 4 : Je sécurise mes équipements de travail												
Gestion des comptes à privilèges				✓								
Chiffrement des postes de travail												
Détection d'intrusion, EDR, IPS			✓					✓				
Thème 5 : Je protège mon réseau												
Filtrage de flux réseau		✓	✓		✓							
Protection DDOS		✓										
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Principe du moindre privilège pour les administrateurs									✓			
Plan de sauvegarde					✓		✓					
Plan de reprise d'activité	✓				✓		✓					
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Tests d'intrusion		✓	✓	✓				✓				
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs			✓					✓				
Gestion de crise cyber	✓	✓										

	CROWDSEC	CRYPTONEXT SECURITY	CYBER-DETECT	CYBERVADIS	CYBERWATCH	DASTRA	DEVENSYS CYBERSECURITY	DIGITALBERRY	EBRC	EGERIE	EQUISIGN	ERCOM
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Organisation et pilotage de la SSI			✓		✓				✓	✓		
Sensibilisation et formation												
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion des droits d'accès								✓				
Revues d'habilitations												
Authentification forte		✓				✓	✓					
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Homologation des SI sensibles												
Audit, scan, revue de code			✓	✓			✓					
Web application firewall												
Effacement des données											✓	
Thème 4 : Je sécurise mes équipements de travail												
Gestion des comptes à privilèges						✓	✓					
Chiffrement des postes de travail												✓
Détection d'intrusion, EDR, IPS	✓		✓									
Thème 5 : Je protège mon réseau												
Filtrage de flux réseau	✓											
Protection DDOS	✓											
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Principe du moindre privilège pour les administrateurs												
Plan de sauvegarde								✓				
Plan de reprise d'activité								✓	✓			
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Tests d'intrusion				✓		✓						
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs	✓					✓						
Gestion de crise cyber		✓						✓				

3 PARCOURS AVANCÉ

	EVERTRUST SAS	EXAMIN	F24 FRANCE SAS	FORMIND	GATEWATCHER	GLIMPS	HARFANGLAB	HIASECURE	HOLISEUM	IDENTO I-TRACING GROUP	ILEX INETUM GROUP	ISE SYSTEMS
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Organisation et pilotage de la SSI	✓	✓							✓			
Sensibilisation et formation				✓					✓			✓
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion des droits d'accès								✓		✓	✓	
Revues d'habilitations										✓	✓	
Authentification forte	✓							✓		✓	✓	
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Homologation des SI sensibles		✓			✓				✓			
Audit, scan, revue de code												
Web application firewall								✓				
Effacement des données												
Thème 4 : Je sécurise mes équipements de travail												
Gestion des comptes à privilèges								✓				
Chiffrement des postes de travail												
Détection d'intrusion, EDR, IPS					✓	✓	✓					✓
Thème 5 : Je protège mon réseau												
Filtrage de flux réseau					✓	✓						
Protection DDOS					✓							
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Principe du moindre privilège pour les administrateurs												
Plan de sauvegarde												
Plan de reprise d'activité		✓		✓								
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Tests d'intrusion				✓					✓			✓
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs							✓					
Gestion de crise cyber			✓	✓		✓	✓					✓

	JALIOS	KDDI FRANCE	KUB CLEANER	LEVIIA	LOGIN SÉCURITÉ	MAILINBLACK	MAKE IT SAFE	MEROX	MOABI	NAMESHIELD	NEOWAVE	NETEXPLORER
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Organisation et pilotage de la SSI	✓			✓			✓	✓				
Sensibilisation et formation	✓					✓	✓			✓		
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion des droits d'accès	✓											✓
Revues d'habilitations												
Authentification forte	✓											
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Homologation des SI sensibles		✓					✓					
Audit, scan, revue de code				✓	✓			✓				
Web application firewall			✓									
Effacement des données												
Thème 4 : Je sécurise mes équipements de travail												
Gestion des comptes à privilèges										✓		
Chiffrement des postes de travail		✓								✓		
Détection d'intrusion, EDR, IPS		✓										
Thème 5 : Je protège mon réseau												
Filtrage de flux réseau		✓		✓								
Protection DDOS		✓		✓					✓			
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Principe du moindre privilège pour les administrateurs												
Plan de sauvegarde		✓										✓
Plan de reprise d'activité		✓										✓
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Tests d'intrusion				✓								
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs				✓								✓
Gestion de crise cyber			✓	✓								

3 PARCOURS AVANCÉ

	OLFEO	OLVID	ON-X GROUPE	OODRIVE	OVERSOC	PATROWL	PRIM'X	PRIZM	PROHACKTIVE	QONTROL	RETARUS
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI			✓	✓	✓			✓			
Sensibilisation et formation	✓										
Thème 2 : Je maîtrise les accès à mon système d'information											
Gestion des droits d'accès							✓				
Revues d'habilitations							✓				
Authentification forte						✓	✓				
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Homologation des SI sensibles			✓		✓						
Audit, scan, revue de code						✓					
Web application firewall											
Effacement des données		✓				✓					
Thème 4 : Je sécurise mes équipements de travail											
Gestion des comptes à privilèges							✓				
Chiffrement des postes de travail						✓			✓		
Détection d'intrusion, EDR, IPS			✓								
Thème 5 : Je protège mon réseau											
Filtrage de flux réseau	✓										✓
Protection DDOS											✓
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
Principe du moindre privilège pour les administrateurs											
Plan de sauvegarde									✓		✓
Plan de reprise d'activité		✓									✓
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Tests d'intrusion			✓			✓			✓	✓	
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Gestion des logs				✓							
Gestion de crise cyber		✓			✓					✓	

	SATELLIZ	SCALAIR	SECLAB	SEELA	SEKOIA.IO	SMART GLOBAL GOVERNANCE	SNOWPACK	SURICATE	SYNETIS	TENACY	TERSEDIA
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI									✓	✓	
Sensibilisation et formation			✓								
Thème 2 : Je maîtrise les accès à mon système d'information											
Gestion des droits d'accès											
Revues d'habilitations											
Authentification forte											
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Homologation des SI sensibles							✓				
Audit, scan, revue de code											
Web application firewall											
Effacement des données											
Thème 4 : Je sécurise mes équipements de travail											
Gestion des comptes à privilèges								✓			
Chiffrement des postes de travail											
Détection d'intrusion, EDR, IPS		✓		✓				✓			✓
Thème 5 : Je protège mon réseau											
Filtrage de flux réseau			✓				✓				
Protection DDOS											
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
Principe du moindre privilège pour les administrateurs	✓										
Plan de sauvegarde	✓	✓									
Plan de reprise d'activité	✓	✓				✓					✓
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Tests d'intrusion						✓		✓			
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Gestion des logs	✓	✓			✓	✓		✓			✓
Gestion de crise cyber						✓					

3
PARCOURS
AVANCÉ

	THEGREENBOW	TIXEO	TRANQUIL IT	TRUSTBUILDER	TRUST HQ	TRUSTINSOFT	UBIKA	VADE	WALLIX	WHALLER	YESWEHACK	YOGOSHA
Thème 1 : Je m'organise et je sensibilise face au risque numérique												
Organisation et pilotage de la SSI				✓								
Sensibilisation et formation			✓					✓		✓		
Thème 2 : Je maîtrise les accès à mon système d'information												
Gestion des droits d'accès	✓		✓	✓					✓			
Revues d'habilitations												
Authentification forte	✓			✓					✓			
Thème 3 : Je sécurise mes données, mes applications et services numériques												
Homologation des SI sensibles	✓											
Audit, scan, revue de code						✓				✓	✓	✓
Web application firewall							✓				✓	
Effacement des données											✓	
Thème 4 : Je sécurise mes équipements de travail												
Gestion des comptes à privilèges									✓			
Chiffrement des postes de travail	✓	✓										
Détection d'intrusion, EDR, IPS												
Thème 5 : Je protège mon réseau												
Filtrage de flux réseau										✓		
Protection DDOS							✓					
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration												
Principe du moindre privilège pour les administrateurs			✓						✓			
Plan de sauvegarde												
Plan de reprise d'activité			✓									
Thème 7 : Je connais les vulnérabilités de mon système d'information												
Tests d'intrusion										✓	✓	✓
Thème 8 : Je sais détecter les événements de sécurité et y réagir												
Gestion des logs							✓					
Gestion de crise cyber												

4
PARCOURS
RENFORCÉ

4 PARCOURS RENFORCÉ

	OUTSCALE	6CURE	AISI	ALGOSECURE	ANTEMETA	ARCAD SOFTWARE	ATEMPO	BOARD OF CYBER	BRAIN NETWORKS	BRAINWAVE GRC	CONTINUS.IO
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI			✓								
Politique SSI											
Indicateurs SSI											
Thème 2 : Je maîtrise les accès à mon système d'information											
Revue d'habilitations									✓		
SSO											
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Cartographie des données du SI						✓			✓		
Homologation des SI sensibles											
Audit, scan, revue de code				✓						✓	✓
Data loss prevention		✓					✓				
DRM – Gestion des droits numériques											
Thème 4 : Je sécurise mes équipements de travail											
Sécurité des équipements mobiles							✓				
Thème 5 : Je protège mon réseau											
Sondes de détection d'intrusion								✓			
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
IPS ; EDR								✓			
Plan de reprise d'activité					✓		✓				
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Audit red team				✓							
Scans de vulnérabilité en continu				✓				✓	✓		
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Forensic et analyse des logs			✓	✓	✓						
SIEM			✓		✓				✓		
SOC	✓		✓		✓						

	CROWDSEC	CYBER-DETECT	CYBERVADIS	CYBERWATCH	DASTRA	DEVENSYS CYBERSECURITY	DIGITALBERRY	EBRC	EGERIE	EQUISIGN	ERCOM
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI		✓		✓				✓	✓		
Politique SSI								✓			
Indicateurs SSI								✓	✓		
Thème 2 : Je maîtrise les accès à mon système d'information											
Revue d'habilitations											
SSO					✓						
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Cartographie des données du SI				✓		✓			✓		
Homologation des SI sensibles				✓							
Audit, scan, revue de code		✓	✓	✓		✓					
Data loss prevention										✓	✓
DRM – Gestion des droits numériques						✓					
Thème 4 : Je sécurise mes équipements de travail											
Sécurité des équipements mobiles						✓					✓
Thème 5 : Je protège mon réseau											
Sondes de détection d'intrusion	✓										
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
IPS ; EDR	✓	✓			✓						
Plan de reprise d'activité							✓				
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Audit red team					✓						
Scans de vulnérabilité en continu		✓	✓								
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Forensic et analyse des logs	✓	✓									
SIEM											
SOC					✓						

4 PARCOURS RENFORCÉ

	EVERTRUST SAS	EXAMIN	F24 FRANCE SAS	FORMIND	GATEWATCHER	GLIMPS	HARFANGLAB	HIASECURE	HOLISEUM	IDENTO I-TRACING GROUP	ILEX INETUM GROUP
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI	✓	✓		✓				✓			
Politique SSI	✓	✓						✓			
Indicateurs SSI	✓	✓									
Thème 2 : Je maîtrise les accès à mon système d'information											
Revue d'habilitations										✓	✓
SSO							✓			✓	✓
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Cartographie des données du SI											
Homologation des SI sensibles					✓			✓			
Audit, scan, revue de code		✓									
Data loss prevention											
DRM – Gestion des droits numériques											
Thème 4 : Je sécurise mes équipements de travail											
Sécurité des équipements mobiles											
Thème 5 : Je protège mon réseau											
Sondes de détection d'intrusion					✓	✓					
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
IPS ; EDR						✓	✓				
Plan de reprise d'activité											
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Audit red team				✓				✓			
Scans de vulnérabilité en continu											
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Forensic et analyse des logs				✓	✓		✓				
SIEM			✓			✓					
SOC				✓	✓	✓					

	ISE SYSTEMS	JALIOS	JSCRAMBLER	KDDI FRANCE	KUB CLEANER	LEVIIA	LOGIN SÉCURITÉ	MAKE IT SAFE	MEROX	METSYS	MOABI
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI	✓	✓					✓	✓			
Politique SSI							✓	✓			
Indicateurs SSI							✓				
Thème 2 : Je maîtrise les accès à mon système d'information											
Revue d'habilitations									✓		
SSO						✓					
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Cartographie des données du SI		✓					✓	✓			
Homologation des SI sensibles											
Audit, scan, revue de code						✓					✓
Data loss prevention		✓					✓				
DRM – Gestion des droits numériques											
Thème 4 : Je sécurise mes équipements de travail											
Sécurité des équipements mobiles		✓			✓				✓		
Thème 5 : Je protège mon réseau											
Sondes de détection d'intrusion											
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
IPS ; EDR											
Plan de reprise d'activité				✓		✓					
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Audit red team	✓						✓				
Scans de vulnérabilité en continu	✓	✓									✓
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Forensic et analyse des logs					✓		✓				
SIEM		✓			✓				✓		
SOC	✓				✓	✓	✓	✓	✓		

4 PARCOURS RENFORCÉ

	NEOWAVE	NETEXPLORER	OLFEO	OLVID	ON-X GROUPE	OODRIVE	OVERSOC	PATROWL	PRIM'X	PRIZM	PROHACKTIVE
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI						✓					
Politique SSI					✓						
Indicateurs SSI						✓				✓	
Thème 2 : Je maîtrise les accès à mon système d'information											
Revue d'habilitations									✓		
SSO	✓										
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Cartographie des données du SI		✓				✓				✓	
Homologation des SI sensibles											
Audit, scan, revue de code							✓				
Data loss prevention		✓						✓			
DRM – Gestion des droits numériques											
Thème 4 : Je sécurise mes équipements de travail											
Sécurité des équipements mobiles	✓		✓	✓	✓						
Thème 5 : Je protège mon réseau											
Sondes de détection d'intrusion											
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
IPS ; EDR											
Plan de reprise d'activité		✓		✓							
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Audit red team					✓		✓			✓	
Scans de vulnérabilité en continu							✓			✓	
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Forensic et analyse des logs		✓									
SIEM					✓						
SOC					✓	✓			✓		

	QONTROL	RETARUS	SCALAIR	SECLAB	SEKOIA.IO	SNOWPACK	SURICATE	SYNETIS	TENACY	TERSEDIA	THEGREENBOW
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI	✓							✓			
Politique SSI								✓			
Indicateurs SSI	✓							✓			
Thème 2 : Je maîtrise les accès à mon système d'information											
Revue d'habilitations									✓		
SSO											
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Cartographie des données du SI	✓							✓			
Homologation des SI sensibles						✓					
Audit, scan, revue de code											
Data loss prevention		✓		✓					✓		
DRM – Gestion des droits numériques											
Thème 4 : Je sécurise mes équipements de travail											
Sécurité des équipements mobiles					✓						✓
Thème 5 : Je protège mon réseau											
Sondes de détection d'intrusion											
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
IPS ; EDR			✓		✓						
Plan de reprise d'activité	✓	✓	✓								
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Audit red team							✓				
Scans de vulnérabilité en continu											
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Forensic et analyse des logs				✓			✓				
SIEM			✓	✓			✓		✓		
SOC			✓	✓			✓				

4
PARCOURS
RENFORCÉ

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

FICHES ENTREPRISES

	TIXEO	TRANQUIL IT	TRUSTBUILDER	TRUST HQ	TRUSTINSOFT	UBIKA	VADE	WALLIX	WHALLER	YESWEHACK	YOGOSHA
Thème 1 : Je m'organise et je sensibilise face au risque numérique											
Organisation et pilotage de la SSI		✓		✓							
Politique SSI				✓					✓		
Indicateurs SSI				✓			✓				
Thème 2 : Je maîtrise les accès à mon système d'information											
Revue d'habilitations											
SSO			✓			✓		✓	✓		
Thème 3 : Je sécurise mes données, mes applications et services numériques											
Cartographie des données du SI										✓	
Homologation des SI sensibles				✓							
Audit, scan, revue de code					✓					✓	
Data loss prevention											
DRM – Gestion des droits numériques											
Thème 4 : Je sécurise mes équipements de travail											
Sécurité des équipements mobiles	✓	✓								✓	
Thème 5 : Je protège mon réseau											
Sondes de détection d'intrusion											
Thème 6 : J'intègre les enjeux de la sécurité numérique à ma politique d'administration											
IPS ; EDR											
Plan de reprise d'activité		✓							✓		
Thème 7 : Je connais les vulnérabilités de mon système d'information											
Audit red team					✓						
Scans de vulnérabilité en continu										✓	✓
Thème 8 : Je sais détecter les événements de sécurité et y réagir											
Forensic et analyse des logs						✓	✓				
SIEM											
SOC											

OUTSCALE
https://outscale.com/
+33 (0)1 53 27 52 70
sales-eu@outscale.com

1 PARCOURS FONDATION
- VPN
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Sécurisation du réseau
- Sécurisation des services Cloud (IaaS/PaaS)
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Plan de reprise d'activité
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- SOC

OUTSCALE, marque de Dassault Systèmes, est un opérateur souverain et durable de business experience de confiance en mode service. Sa mission est de proposer une architecture unique de services, qui comprend un large éventail d'offres adaptées pour la création d'expériences de jumeaux virtuels. OUTSCALE offre aux organisations publiques et privées des expériences métiers accessibles en continu, de manière simple, sécurisée et durable.

PRODUITS & SERVICES

OUTSCALE propose 3 modèles de Cloud :

- **Cloud souverain :** Cloud public détenant les plus hautes certifications de sécurité internationales par pays, pour une collaboration de confiance dans un espace juridique et fiscal commun. De plus, il comprend la qualification SecNumCloud pour la France et l'Europe, ainsi que ITAR pour les États-Unis.
- **Cloud dédié :** Cloud clé en main, sur mesure et sur site avec des certifications internationalement reconnues telles que l'ISO 27001.
- **Cloud International :** Cloud public pour la collaboration sécurisée.

Ce modèle fournit des certifications reconnues au niveau international, telles que la norme ISO 27001, relatives au management de la sécurité de l'information, l'hébergement des données de santé de manière sécurisée avec la certification HDS et la certification TISAX qui, elle, démontre la conformité aux exigences de sécurité et de protection des données de l'industrie automobile.

6cure
https://www.6cure.com
+33 (0)9 71 16 21 50
contact@6cure.com

1 PARCOURS FONDATION
- Protection des services exposés sur Internet
- Filtrage Réseau
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Analyse de risques
- Sécurisation du réseau
- Filtrage réseau
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Filtrage de flux réseau
- Protection DDOS
- Tests d'intrusion
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Data loss prevention

6cure, PME spécialisée dans la sécurité des systèmes d'information, développe des solutions de protection contre différentes catégories d'attaques visant la disponibilité des réseaux et des infrastructures DNS jusqu'aux services applicatifs, et en particulier les menaces de type DDoS. Ces solutions permettent aux entreprises et aux organisations publiques d'accroître leur réactivité face aux multiples attaques qui ciblent notamment le monde de la santé et des collectivités.

PRODUITS & SERVICES

1 - Protection DDoS :
6cure Threat Protection® garantit la disponibilité de vos services face aux attaques les plus avancées avec une protection adaptée sur site, cloud ou hybride. Identifie et filtre en temps réel les attaques DDoS complexes, jusqu'au niveau applicatif (L2-L7) en préservant l'intégrité et la performance des flux légitimes.

2 - Sécurité DNS :
6cure DNS Protection® est une solution européenne de sécurité DNS « tout-en-un » permettant de garantir la disponibilité et la qualité de service, de manière transparente et agnostique, d'offrir une visibilité précoce et complète de la menace à vos équipes opérationnelles. Elle constitue le moyen de réaction le plus rapide face à des menaces d'infection, d'exfiltration de données par des canaux cachés, ou de fuite d'informations indésirables.

3 - Test de résistance aux DDoS :
DDoS Assessment évalue la résilience de vos infrastructures réseau et services face à la menace DDoS dans un contexte maîtrisé, grâce à notre expertise DDoS et à notre plate-forme unique.

AISI
https://www.aisi.fr/
+33 (0)1 85 09 18 45
contact@aisi.fr

1 PARCOURS FONDATION
- Analyse des vulnérabilités
- Scans de vulnérabilité du SI exposé sur Internet
- Audit organisationnel de sécurité
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Approche Security-by-design
- Sécurisation du réseau
- End point security

3 PARCOURS AVANCÉ
- Détection d'intrusion, EDR, IPS
- Filtrage de flux réseau
- Tests d'intrusion
- Gestion des logs

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Forensic et analyse des logs
- SIEM
- SOC

Expert Cybersécurité depuis 2016, AISI se consacre exclusivement à la sécurité stratégique et opérationnelle des organisations françaises de taille intermédiaire.

Notre vocation est de connecter et protéger sans transiger les systèmes d'information qui accélèrent la croissance des PME, ETI et services publics de proximité.

PRODUITS & SERVICES

Face aux cybercriminels et à leurs attaques, **DSI et dirigeants** doivent trouver une **solution pragmatique** sous contrainte forte de ressources leur permettant de :
- S'appuyer sur les **technologies** de cybersécurité nécessaires,
- Mettre réellement des **experts** derrière les machines,
- Organiser les **processus.**

Avec l'offre de **sécurité stratégique et opérationnelle d'AISI**, complète et modulable, vous élaborez votre propre programme cybersécurité, en bénéficiant des conseils, des solutions et de l'amélioration continue :
- LA SÉCURITÉ STRATÉGIQUE pour renforcer la protection et la capacité de réaction de l'organisation : diagnostics, analyse de risques, gouvernance, conformité, PSSI, RSSI as a service.
- LA SÉCURITÉ DES INFRASTRUCTURES pour minorer les vulnérabilités techniques et réduire l'exposition aux risques : audit, design et intégration d'infrastructure et de solutions de sécurité, MCO, MCS.
- LA CYBERSÉCURITÉ OPÉRATIONNELLE pour agir au cœur de votre système de défense pour surveiller, confiner, investiguer et remédier : pentest, détection (SOC) threat intelligence intégrée, réponse (CSIRT, forensic), reconstruction.

AlgoSecure
https://www.algosecure.fr
+33 (0)4 26 78 24 86
contact@algosecure.fr

1 PARCOURS FONDATION
- Gestion des mots de passe
- Protection des accès distants
- Protection des services exposés sur Internet
- Audit organisationnel de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Filtrage réseau
- Gouvernance des Identités et des Accès
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Homologation des SI sensibles
- Gestion des comptes à privilèges
- Tests d'intrusion

4 PARCOURS RENFORCÉ
- Audit, scan, revue de code
- Audit red team
- Scans de vulnérabilité en continu
- Forensic et analyse des logs

AlgoSecure est un cabinet de conseil français indépendant spécialiste de la cybersécurité, créé en 2008. Son métier : accompagner les entreprises et les organismes publics dans la sécurisation de leurs systèmes d'information.

Qualifié PASSI, AlgoSecure a développé une expertise dans l'accompagnement des organisations les plus sensibles. L'entreprise est certifiée ISO 27001 et labellisée Expert Cyber.

PRODUITS & SERVICES

AlgoSecure propose un accompagnement complet SSI :

- AUDITER : évaluer la sécurité de votre SI, identifier vos actifs critiques (pentest web, audit LAN,...).
- CONSEILLER/SÉCURISER : élever le niveau de sécurité (accompagnement certification ISO 27001, sécurisation Active Directory...).
- SENSIBILISER ET FORMER : insuffler la culture cyber et/ou former vos collaborateurs.
- RÉAGIR EN CAS D'INCIDENTS DE SÉCURITÉ : détecter les fuites de données, prévenir, analyser et traiter les incidents de sécurité.

Focus sur nos services :
- AlgoCert, une offre pour gagner en sérénité face aux incidents de sécurité.
- RSSI externalisé et accès à notre Centre de compétences Cyber.
- Accompagnement RGPD et DPO externalisé.

Les engagements d'AlgoSecure :
- Bénéficier d'une forte expertise technique.
- Être accompagné par une équipe de consultants hautement qualifiés et passionnés.
- Être conseillé en toute impartialité (vis-à-vis des constructeurs et éditeurs).

ANTEMETA

ANTEMETA
https://www.antemeta.fr
+33 (0)1 85 40 02 80
contact@antemeta.fr

1 PARCOURS FONDATION
- Antivirus
- Firewall
- Dispositif de sauvegarde
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Restauration de l'activité/ PRA
- Scans de vulnérabilité sur tout le SI
- Gestion des logs
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Authentification forte
- Filtrage de flux réseau
- Plan de sauvegarde
- Plan de reprise d'activité

4 PARCOURS RENFORCÉ
- Plan de reprise d'activité
- Forensic et analyse des logs
- SIEM
- SOC

ETI française créée en 1995, AntemetA est aujourd'hui l'un des leaders du cloud hybride et de la protection des données. Entreprise à taille humaine avec plus de 300 collaborateurs, le groupe compte 7 agences implantées en France ainsi qu'une filiale au Maroc. Engagée dans une démarche globale de responsabilité sociétale et environnementale, l'entreprise a lancé notamment un projet de reforestation labellisé « Bas carbone » destiné à réduire son empreinte énergétique.

PRODUITS & SERVICES

Partenaire de la DSI et garant de la souveraineté des données, AntemetA accompagne ses clients dans l'évolution de leurs systèmes d'information, par la mise en œuvre de solution d'infrastructure (VAR), la fourniture de services Cloud (CSP) et une expertise des services managés (MSP).

L'ensemble des offres cloud et du service client 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 ISAE 3402 type1.
AntemetA accompagne plus de 1000 clients de tailles et de secteurs différents et la relation client d'Antemeta est travaillée sur 3 angles : un portail dédié, une relation de proximité avec des gouverneurs (SDM) et un support téléphonique 24/7. La communauté des clients AntemetA se réunit plusieurs fois par an. Ces échanges permettent de nourrir les convictions du groupe sur l'importance d'avoir des équipes de R&D.

ARCAD SOFTWARE

Arcad Software
https://www.dot-anonymizer.fr
+33 (0)4 50 57 83 96
contact-fr@arcadsoftware.com

1 PARCOURS FONDATION

2 PARCOURS INTERMÉDIAIRE
- Chiffrement des données

3 PARCOURS AVANCÉ
- Homologation des SI sensibles
- Effacement des données

4 PARCOURS RENFORCÉ
- Cartographie des données du SI

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 la gestion des données de test.
Les solutions DOT permettent à ARCAD Software de répondre aux défis actuels du respect des données personnelles et de l'intégrité des systèmes d'information en automatisant le masquage et l'extraction des données.

PRODUITS & SERVICES

DOT Anonymizer est une solution permettant d'anonymiser les données personnelles et identifiantes tout en préservant leur format et leur type. DOT Anonymizer fournit un moteur central unique pour protéger les données de toutes les bases de données d'une entreprise. Il peut être mis en place dans n'importe quel type de configuration :
- Après copie d'une base de données de production dans un environnement hors production.
- En liaison avec un ETL (Extract, Transfert, Load).
- En combinaison avec un outil de réplication de données.
- En sortie de l'outil d'extraction des données DOT Extract.

Les données anonymisées peuvent être utilisées comme ressources de test dans des conditions d'utilisation réelles tout en respectant les contraintes légales en matière de transfert de données. DOT Anonymizer est entièrement agnostique, quelle que soit la plate-forme, et prend en charge tous les systèmes d'exploitation et tous les SGBD et les fichiers plats type texte.
DOT Extract permet l'échantillonnage d'un jeu de données et fonctionne en synergie avec DOT Anonymizer.

ATEMPO
https://www.atempo.com
+33 (0)1 64 86 83 00
info@atempo.com

1 PARCOURS FONDATION
- Protection de la messagerie
- Dispositif de sauvegarde

2 PARCOURS INTERMÉDIAIRE
- End point security
- Restauration de l'activité / PRA

3 PARCOURS AVANCÉ
- Plan de sauvegarde
- Plan de reprise d'activité

4 PARCOURS RENFORCÉ
- Data loss prevention
- Sécurité des équipements mobiles
- Plan de reprise d'activité

Membre actif du groupement Cybermalveillance.gouv.fr et du GINUM (Groupement des Intervenants du Numérique), nos solutions sont labellisées 'Utilisé par les Armées Françaises', répertoriées au catalogue GouvTech de la DINUM et référencées aux marchés des centrales d'achat RESAH, CAIH, UGAP. Disponibilité, écoute, réactivité et qualité de service irréprochable... sont régulièrement cités par nos clients et partenaires qui peuvent compter sur des équipes support disponibles 24/7.

PRODUITS & SERVICES

Atempo, éditeur français de logiciels de Data Protection et Data Management, propose des solutions de sauvegarde des données sensibles, que ces données soient stockées directement sur les postes de travail, des serveurs applicatifs virtualisés, des serveurs de fichiers Scale-Out NAS, des systèmes de fichiers parallèles, sur vos infrastructures ou dans le cloud. Trente années d'expertise dans la sauvegarde nous permettent de protéger les organisations de tout risque de perte de données et interruption d'activité consécutive à un sinistre (vol, panne, catastrophe naturelle, attaque cybercriminelle). Nos solutions Tina, Lina et Miria permettent une restauration rapide des données et une reprise d'activité simplifiée.
« Lorsque nous avons subi une attaque informatique de grande ampleur en novembre 2019, nous avons pu remonter l'intégralité des données à la suite de la remédiation des serveurs. Les équipes Atempo sont d'un grand soutien au quotidien, et leur disponibilité s'est particulièrement vérifiée au moment où nous en avions le plus besoin. » Sylvain François, DSI du CHU de Rouen.

Avant de Cliquer
https://avantdecliquer.com
+33 (0)2 79 49 05 90
carl@avantdecliquer.com

1 PARCOURS FONDATION
- Sensibilisation
- Analyse des vulnérabilités
- Protection de la messagerie
- Audit organisationnel de sécurité

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation
- Test de phishing

3 PARCOURS AVANCÉ
- Sensibilisation et formation

4 PARCOURS RENFORCÉ

AdC a développé un programme automatique de sensibilisation sur 12 mois. L'objectif est de faire monter en compétence les utilisateurs afin qu'ils apprennent à se protéger des attaques par phishing et également de développer, au sein de leur organisation, une véritable culture de la cybersécurité.

PRODUITS & SERVICES

Notre mission est de protéger les organisations des cyberattaques en sensibilisant le personnel aux techniques du phishing et à la cybersécurité. Chaque utilisateur intègre un programme complet de montée en compétences leur permettant de les acculturer à la cybersécurité et de les rendre autonomes face aux cyberattaques par phishing.

Pour ce faire, Avant de Cliquer a développé une plateforme permettant aux utilisateurs d'acquérir les connaissances nécessaires au développement de réflexes de vigilance grâce à son algorithme intelligent et innovant de mise en situation. Des e-mails sont envoyés régulièrement et non de manière ponctuelle, en proposant un programme de formation évolutif sur un an.

Sur une période de 12 mois, nous divisons par 10 le risque de cliquer sur un e-mail malveillant.

Board of Cyber
https://www.boardofcyber.io/
contact@boardofcyber.io

1 PARCOURS FONDATION
- Sensibilisation
- Scans de vulnérabilité du SI exposé sur Internet

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation

3 PARCOURS AVANCÉ

4 PARCOURS RENFORCÉ
- Scans de vulnérabilité en continu

Découvrez la notation en continu de votre performance cyber.
Board of Cyber est une startup française avec une mission : créer un écosystème de confiance. La cybersécurité commence par une connaissance fine et objective de ses propres performances mais également celle de ses partenaires. Notre produit phare est Security Rating®, une solution SaaS de notation cyber non intrusive, 100 % automatisée qui a convaincu déjà plus de 150 clients.

PRODUITS & SERVICES

Évaluez et améliorez la performance cyber de votre organisation et celle de votre écosystème avec Security Rating®. Une solution SaaS non-intrusive qui évalue la maturité cyber sécurité d'une société à travers ses actifs publics. La notation peut être enrichie par des questionnaires en ligne directement accessibles sur la plateforme.

Au-delà de la notation, Security Rating® indique les observables, leur sévérité et permet aux entreprises de disposer de constats et de recommandations pour une amélioration continue de leur cybersécurité et celle de leur écosystème. Security Rating® permet d'adresser de nombreux cas d'usage : les RSSI qui souhaitent piloter leur propre posture cyber ainsi qu'évaluer la maturité de leurs filiales et de leurs fournisseurs, les courtiers pour aider leurs clients à souscrire une assurance cyber dans les meilleures conditions, les dirigeants de PME pour rassurer leurs clients clés, les collectivités territoriales pour se protéger et assurer la continuité du service public, les fonds de Private Equity pour accompagner leurs participations, les experts en M&A pour réaliser une Due Diligence cyber...

Brain Networks
https://www.brain-networks.fr/
+33 (0)9 72 50 51 19
contact@brain-neworks.fr

1 PARCOURS FONDATION
- Protection des services exposés sur Internet
- Protection des accès réseau Wi-Fi
- Gestion des comptes à privilèges
- Scans de vulnérabilité du SI exposé sur Internet

2 PARCOURS INTERMÉDIAIRE
- Sécurisation du réseau
- End point security
- Scans de vulnérabilité sur tout le SI
- Gestion des logs

3 PARCOURS AVANCÉ
- Authentification forte
- Détection d'intrusion, EDR, IPS
- Tests d'intrusion
- Gestion des logs

4 PARCOURS RENFORCÉ
- Sondes de détection d'intrusion
- IPS ; EDR
- Scans de vulnérabilité en continu
- SIEM

Notre mission est d'aider les organisations à relever les défis posés par leur transformation digitale en termes de sécurité (IT, IoT, OT), performance, évolutivité et gestion des risques.
À cette fin, nous avons développé des pôles d'excellence pour lesquels nous disposons de compétences techniques pointues :
- Audit sécurité et Pentest
- Conseil
- Intégration de solutions de sécurité
- Sensibilisation
- Cybersécurité managée
- Maintien en Conditions de Sécurité

PRODUITS & SERVICES

Nos services à forte valeur ajoutée :
- **Audit sécurité :** pentest, audit d'architecture, audit CyberIoT, identification des vulnérabilités, évaluation Shadow IT, sécurité du Cloud.
- **Conseil en cybersécurité :** stratégie, architecture, bonnes pratiques.
- **Intégration de solutions de sécurité :** Secure SD-WAN et SASE, Zero Trust, NGFW, NAC, VPN, MFA, SIEM, PAM, CASB, DLP, sécurité 360° (endpoint/web/mail/réseau).
- **Sensibilisation :** accompagnement global de sensibilisation à la cybersécurité (Directions Métier, Utilisateurs finaux).
- **Cybersécurité managée :** offres clefs en main conseil, exploitation, supervision et pilotage.
- **Maintien en Conditions de Sécurité :** détection des menaces, remédiation, gestion des vulnérabilités, mise à l'épreuve du SI de façon récurrente.

BRAINWAVE GRC

Brainwave GRC
https://www.brainwavegrc.com/fr/
+33 (0)1 84 19 04 10
info@brainwavegrc.com

C.A.I.H. UGAP

1 PARCOURS FONDATION

- Gestion centralisée des identités
- Analyse des vulnérabilités
- Gestion des comptes à privilèges
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE

- Gestion du cycle de vie des utilisateurs et des habilitations
- Cartographie de l'infrastructure du SI
- Gestion des comptes de service

3 PARCOURS AVANCÉ

- Gestion des droits d'accès
- Revues d'habilitations
- Audit, scan, revue de code
- Principe du moindre privilège pour les administrateurs

4 PARCOURS RENFORCÉ

- Revue d'habilitations
- Cartographie des données du SI
- Audit, scan, revue de code

Brainwave GRC est une solution clé en main d'analyse des identités et des accès aux données et applications, pour les entreprises et organismes publics qui cherchent à maîtriser leurs droits d'accès logiques afin de démontrer leur conformité, réduire les risques tout en responsabilisant les premières lignes de défense. Avec Brainwave GRC, répondez aux recommandations d'audit IT, automatisez vos revues, maîtrisez vos comptes à privilèges, et accélérez votre système IAM.

PRODUITS & SERVICES

Brainwave Identity Analytics vous aide à reprendre le contrôle des droits d'accès : qui travaille ou collabore avec l'entreprise, qui a accès à quoi, quels sont les risques associés. Brainwave Identity Analytics automatise les revues de droits d'accès à tous les niveaux : comptes utilisateurs, comptes techniques, droits d'accès aux infrastructures, aux applications, aux données. La solution vous permet ainsi de répondre facilement aux différentes contraintes réglementaires. PAM Booster as a Service est une nouvelle solution compagnon de CyberArk PAM pour améliorer les fonctionnalités du Privileged Account Manager et offrir une visibilité plus claire et plus précise sur les personnes ayant accès aux informations d'identification à l'intérieur des coffres de CyberArk. Il surveille en permanence la chaîne d'accès de CyberArk, y compris les comptes et groupes AD, afin de détecter les changements qui exposent l'organisation à des risques inutiles. Les résultats sont présentés dans des tableaux de bord exploitables pour les administrateurs PAM.

conscio technologies

Conscio Technologies
https://www.conscio-technologies.com
+33 (0)1 84 80 82 01
contact@conscio-technologies.com

C.A.I.H. UGAP

1 PARCOURS FONDATION

- Sensibilisation

2 PARCOURS INTERMÉDIAIRE

- Sensibilisation

3 PARCOURS AVANCÉ

- Sensibilisation et formation

4 PARCOURS RENFORCÉ

Conscio Technologies est le spécialiste de la sensibilisation cybersécurité. Nous travaillons avec les RSSI, DSI et DPO afin de les aider à franchir le dernier kilomètre de la cybersécurité qui est celui du changement de comportements des utilisateurs.

Conscio Technologies accompagne déjà nombre d'agglomérations et de Conseils départementaux dans la mise en oeuvre de leur sensibilisation cyber et a développé une offre spécialement pour les acteurs de la santé.

PRODUITS & SERVICES

L'offre est constituée tout d'abord, d'un catalogue de plus de 90 modules dont des modules sectoriels (santé, collectivités territoriales et industrie).
Ces modules présentent différents formats (vidéos interactives, quiz, interface chat, livres interactifs...)
Elle est constituée ensuite d'une solution logicielle, **Sensiwave**, conçue spécialement pour la mise en œuvre des campagnes de sensibilisation et de tests phishings (nombreux scénarios disponibles).
Sensiwave associe une puissante gestion des campagnes et la possibilité de personnaliser vraiment les contenus, de créer des campagnes incluant et agençant les modules que vous sélectionnez de la façon dont vous le voulez.
Sensiwave intègre également toute une bibliothèque d'outils de gestion des contenus vous permettant de bénéficier d'une richesse d'outils avec notamment la possibilité de créer et personnaliser des vidéos interactives.
Points forts :
- Totalement personnalisable.
- Gestion des statistiques Big Data.
- Création de vos propres contenus.
- Colle avec votre organisation (décentralisée, internationale).
- Nombreuses langues disponibles.

Continus.io
https://www.continus.io
contact@continus.io

1 PARCOURS FONDATION
- Analyse des vulnérabilités

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Sécurité applicative

3 PARCOURS AVANCÉ
- Audit, scan, revue de code

4 PARCOURS RENFORCÉ
- Audit, scan, revue de code

Continus.io est un éditeur de logiciels de cybersécurité expert en sécurité applicative.

Il édite la solution Continus DevSecOps qui unifie dans une seule plateforme les outils indispensables aux équipes agiles/DevOps afin d'automatiser les vérifications de sécurité et la gestion des vulnérabilités de l'ensemble des couches applicatives, du code source à l'infrastructure-as-code en passant par les dépendances externes.

PRODUITS & SERVICES

Continus.io développe des solutions innovantes pour sécuriser le développement moderne des applications tout au long de leur cycle de vie :

- **Continus DevSecOps :** Plateforme All-In-One englobant plusieurs sous-produits, c'est le compagnon idéal des équipes Agiles/DevOps pour automatiser les vérifications de sécurité, simplifier l'intégration de la sécurité au sein des chaines CI/CD et évaluer la sécurité de l'ensemble des couches applicatives, du code source à l'infrastructure-as-code, en passant par la dépendance externe et/ou open-source.
- **Continus SAST :** Pour analyser le code et identifier les sources des vulnérabilités.
- **Continus SCA :** Pour analyser les dépendances externes et identifier les librairies open-source vulnérables.
- **Continus DAST :** Pour simuler des attaques contre les applications web et API.
- **Continus IACS :** Pour analyser la sécurité des images dockers et autres infra-as-code.
- **Continus SBOM :** Pour générer le SBOM (Software Bill Of Material) lors de la construction logicielle (processus de build).

Crowdsec
https://crowdsec.net
+33 (0)6 24 91 10 09
philippe@crowdsec.net

1 PARCOURS FONDATION
- Protection des accès distants
- Protection des services exposés sur Internet
- Filtrage Réseau

2 PARCOURS INTERMÉDIAIRE
- Sécurité applicative
- End point security
- Sécurisation des services Cloud (IaaS/PaaS)
- Gestion des logs

3 PARCOURS AVANCÉ
- Détection d'intrusion, EDR, IPS
- Filtrage de flux réseau
- Protection DDOS
- Gestion des logs

4 PARCOURS RENFORCÉ
- Sondes de détection d'intrusion
- IPS ; EDR
- Forensic et analyse des logs

CrowdSec est un IPS participatif et open-source IPS. Il détecte les comportements anormaux dans les logs et propose une remédiation contextualisée (firewall, Rproxy, application, etc.), du type que l'on veut (MFA, Captcha, Drop, Report, etc.).

L'unicité de la solution vient de sa partie collaborative. Toute IP repérée puis bloquée chez un membre est vérifiée puis redistribuée à tous, fournissant ainsi un Waze des firewalls, qui combine analyse comportementale et réputationnelle.

PRODUITS & SERVICES

La solution est composée de deux éléments locaux et deux en ligne. Le premier élément est l'agent (en Go), qui est un IDS basé sur l'assimilation de logs. Le second est un IPS, à choisir parmi un vingtaine à ce jour, qui forcera la remédiation choisit si l'IDS détecte un comportement anormal ou si une IP aggressive tente de se connecter. Il peut agir à très bas niveau (firewall, LB, etc.), niveau intermédiaire (RP) ou très haut niveau (applicatif) selon le besoin.

Ces composants sont open source et gratuits.

En SaaS, deux éléments sont fournis, une console qui fait à la fois office de tableau central de pilotage et reporting et de CTI pour se renseigner sur une IP. Un second élément est accessible, une API, qui permet d'automatiser les requêtes à notre CTI pour les utiliser dans n'importe quel contexte (IoT, On demand, Soc, CTI, etc.).

CryptoNext Security
https://www.cryptonext-security.com
+33 (0)1 84 60 84 29
contact@cryptonext-security.com

1 PARCOURS FONDATION
- Protection des accès distants
- Protection de la messagerie
- VPN
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Chiffrement des données
- Sécurisation du réseau
- Sécurité applicative
- Sécurisation des services Cloud (IaaS/PaaS)

3 PARCOURS AVANCÉ
- Authentification forte

4 PARCOURS RENFORCÉ

CryptoNext Security, fondée en 2019, est une startup française, basée à Paris, spin-off de INRIA, du CNRS et de Sorbonne Université après plus de 20 ans de recherches académiques. Éditeur spécialisé dans la cryptographie post-quantique (PQC) et les solutions de remédiation aux attaques de l'ordinateur quantique, ses solutions permettent aux entreprises, intégrateurs, éditeurs et constructeurs de migrer aisément et de façon pérenne leurs infrastructures IT/OT vers l'ère de la cybersécurité post quantique. CryptoNext Security est citée parmi les 5 leaders référence du rapport Gartner sur la cryptographie post-quantique et a reçu le Prix de l'Innovation des Assises 2022.

PRODUITS & SERVICES

La menace induite par l'arrivée de l'ordinateur quantique vis-à-vis de la cryptographie à clés publiques est maintenant là. CryptoNext Security propose une suite complète d'outils et d'applications pour remédier à cette menace pour les données et infrastructures matérielles et logicielles IT/OT.

CryptoNext Quantum Safe Remediation Suite (C-QSR) est articulée autour de sa bibliothèque logicielle Quantum Safe Library (QSL). QSL est complète, performante, nativement crypto-agile et permettant l'hybridation avec la cryptographie classique ou en pure cryptographie post-quantique. Elle inclut également un ensemble d'outils d'intégration « plug & play » ainsi que des plugins applicatifs (HSM, VPN, Signatures, Authentification, IoT, Bockchain, Messagerie...).

CryptoNext propose enfin un ensemble de services visant à accompagner ses clients et partenaires dans cette remédiation perenne.

CYBER-DETECT
https://cyber-detect.com
+33 (0)3 72 74 49 72
contact@cyber-detect.eu

1 PARCOURS FONDATION
- Antivirus
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Scans de vulnérabilité sur tout le SI
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Détection d'intrusion, EDR, IPS
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- IPS; EDR
- Forensic et analyse des logs

CYBER-DETECT a mis au point une technologie unique pour la détection et caractérisation de malwares.
Son savoir-faire, appelé analyse morphologique, permet d'identifier rapidement les attaques les plus sophistiquées telles que les variants de malware 0 day ou les fichiers packés, réussissant à tromper les systèmes de défense classiques.

Cette solution, baptisée GORILLE, s'intègre dans la chaine de protection des CERT ou SOC et s'interface avec les solutions d'EDR, SIEM ou SOAR.

PRODUITS & SERVICES

CYBER-DETECT a développé 3 produits, articulés autour des problématiques de ses clients :

- **Gorille Expert :** une solution de caractérisation de logiciels malveillants complexes, dédiées aux experts en reverse engeenering,

- **Gorille Cloud:** un outil de détection et caractérisation instantané de fichiers exécutables en SAAS, on-premise, ou intégré dans les solutions packagées de nos partenaires,

- **Gorille Patrouille :** la cyber-analyse permettant la levée de doute en cas de menaces dormantes au sein du parc informatique.

cybervadis

CyberVadis
https://cybervadis.com/
+33 (0)1 82 28 88 88
info@cybervadis.com

1 PARCOURS FONDATION

- Scans de vulnérabilité du SI exposé sur Internet
- Audit organisationnel de sécurité

2 PARCOURS INTERMÉDIAIRE

- Politique SSI
- Analyse de risques

3 PARCOURS AVANCÉ

- Organisation et pilotage de la SSI
- Audit, scan, revue de code

4 PARCOURS RENFORCÉ

- Organisation et pilotage de la SSI
- Audit, scan, revue de code
- Scans de vulnérabilité en continu

CyberVadis offre une solution d'évaluation de la maturité cybersécurité des tiers. Toutes nos 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.

PRODUITS & SERVICES

Nous proposons 2 cas d'usage :
Vous faire évaluer et partager avec vos tiers (Parcours 1 et 2) :
- Évaluation basée sur la revue de preuves par des analystes cybersécurité.
- Livrables : Scorecard détaillée, benchmark et plan de remédiation priorisé.
- Accès à un service de support qui vous accompagne lors de votre évaluation puis pour vous guider sur la mise en place d'actions d'améliorations de vos pratiques cybersécurité.
- Partage illimité de vos résultats depuis votre espace en ligne.
- Rapport de scans de vulnérabilités.

Évaluer vos tiers et suivre l'amélioration de leurs pratiques cybersécurité (Parcours 3 et 4) :
- Évaluer la posture cybersécurité de vos tiers grâce à une évaluation basée sur la revue de preuves.
- Chaque tiers évalué reçoit une Scorecard détaillée et un plan de remédiation priorisé.
- Collaborer avec eux sur l'amélioration de leurs pratiques cybersécurité directement sur la plateforme CyberVadis.

Cyberwatch

Cyberwatch
https://cyberwatch.fr
+33 (0)1 85 08 69 79
contact@cyberwatch.fr

1 PARCOURS FONDATION

- Analyse des vulnérabilités
- Gestion des mises à jour des postes de travail
- Gestion des mises à jour des serveurs et applications
- Scans de vulnérabilité du SI exposé sur Internet

2 PARCOURS INTERMÉDIAIRE

- Gestion des mises à jour de sécurité
- End point security
- Cartographie de l'infrastructure du SI
- Scans de vulnérabilité sur tout le SI

3 PARCOURS AVANCÉ

- Audit, scan, revue de code
- Tests d'intrusion

4 PARCOURS RENFORCÉ

- Homologation des SI sensibles
- Audit, scan, revue de code
- Scans de vulnérabilité en continu

Cyberwatch est un éditeur français de logiciels de sécurité informatique, spécialisé dans la gestion des vulnérabilités et le contrôle des conformités. Cyberwatch aide les entreprises et administrations, les Opérateurs d'Importance Vitale (OIV) et les Opérateurs de Services Essentiels (OSE), à réduire leur risque informatique, à l'aide d'analyses continues et de rapports pertinents adaptés à leur environnement métier. Membre d'Hexatrust, du CLUSIF, et de l'ACN.

PRODUITS & SERVICES

Cyberwatch Vulnerability Manager est une solution de gestion des vulnérabilités, qui vous aide à identifier les vulnérabilités de votre système d'information, à repérer et prioriser les vulnérabilités les plus simples à utiliser pour les pirates et les plus graves pour vos actifs. Le logiciel Cyberwatch Vulnerability Manager vous indique les actions à réaliser pour traiter vos vulnérabilités, et dispose d'un module de Patch Management embarqué qui permet de planifier et déployer, si vous le souhaitez, des correctifs de sécurité.

Cyberwatch Compliance Manager est une solution de contrôle des conformités, avec analyse du niveau de durcissement lié au respect de règles issues des principaux guides du marché. Le logiciel Cyberwatch Compliance Manager vous permet également de personnaliser les règles disponibles et de créer vos propres référentiels, vous donne de la visibilité sur votre niveau de conformité au regard de vos objectifs, et vous indique les actions nécessaires pour traiter vos non-conformités. Cyberwatch se déploie facilement dans votre réseau, avec ou sans agent.

DASTRA

DASTRA
https://www.dastra.eu/fr
+33 (0)6 59 3681 88
paulemmanuel.bidault@dastra.eu

1 PARCOURS FONDATION

2 PARCOURS INTERMÉDIAIRE
- Analyse de risques
- Cartographie de l'infrastructure du SI

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Cartographie des données du SI
- Audit, scan, revue de code

Créé en 2020, Dastra, à mi-chemin entre la LegalTech et la Data (Dastra est l'abréviation de Data-Stratégie), est une startup française dans un domaine d'actualité : la protection des données personnelles.

Dastra est un logiciel qui aide les entreprises à simplifier et automatiser la mise en œuvre et le suivi de la conformité RGPD à travers une plateforme SaaS simple, ergonomique et collaborative et orientée-données.

PRODUITS & SERVICES

En tant que Délégué à la Protection des Données, vous avez besoin de conseiller et contrôler les responsables de traitements de votre société dans leur conformité RGPD. 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 et pouvant être testé avec une offre gratuite, mais également des services comme des audits cookies, coach DPO, formation ou simulation de contrôle, délivrés par nos experts, anciens de la CNIL.

Devensys Cybersecurity

Devensys Cybersecurity
https://www.devensys.com/
+33 (0)4 67 71 77 49
contact@devensys.com

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Gestion des comptes à privilèges
- Authentification et contrôle d'accès
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Test de phishing
- Filtrage réseau
- Gouvernance des Identités et des Accès
- Gestion des logs

3 PARCOURS AVANCÉ
- Authentification forte
- Gestion des comptes à privilèges
- Tests d'intrusion
- Gestion des logs

4 PARCOURS RENFORCÉ
- SSO
- IPS ; EDR
- Audit red team
- SOC

Devensys Cybersecurity, entreprise française spécialisée en sécurité des systèmes d'information. Une équipe d'experts certifiés basée en France, garantie zéro sous-traitance. Nos valeurs : Expertise, Qualité, Ethique. Nous accompagnons nos clients privés et institutionnels autour des grandes thématiques suivantes :
- RedTeam & Pentest,
- Sécurité Managée & SOC 24/7,
- Sécurité Cloud & Infrastructure,
- Centre Formation & Certification.

PRODUITS & SERVICES

Pure player en cybersécurité 100 % français, garanti sans sous-traitance, nous intervenons sur de nombreux volets des différents parcours « Prestataire terrain France Relance ».
Nos équipes certifiées (CISSP, CEH, CHFI, OSCP…) peuvent vous accompagner sur tout ou partie du périmètre : de l'audit à l'intégration, en passant par la formation et la sensibilisation, jusqu'au service managé (SOC 24/7 - 30 minutes).

Digitalberry
https://www.digitalberry.fr/
+33 (0)1 84 19 95 57
contact@digitalberry.fr

1 PARCOURS FONDATION
- Protection des services exposés sur Internet
- Cartographie du réseau
- Authentification et contrôle d'accès
- Sécurité des flux d'administration

2 PARCOURS INTERMÉDIAIRE
- Chiffrement des données
- Sécurité applicative
- Cartographie de l'infrastructure du SI
- Gouvernance des Identités et des Accès

3 PARCOURS AVANCÉ
- Gestion des droits d'accès
- Authentification forte
- Audit, scan, revue de code
- Gestion des comptes à privilèges

4 PARCOURS RENFORCÉ
- Cartographie des données du SI
- Audit, scan, revue de code
- DRM – Gestion des droits numériques
- Sécurité des équipements mobiles

Digitalberry a pour mission de lutter contre les cyberattaques et d'en finir avec la gestion manuelle et les tâches répétitives.
Fondé en 2014, Digitalberry est un éditeur français de solutions de cybersécurité, spécialisé dans la gestion des certificats numériques et des clés de sécurité. Avec nos solutions complètes et simples, gagnez en temps, sérénité et sécurité !

PRODUITS & SERVICES

BerryCert est une solution CLM (Certificate Lifecycle Management). Elle vous permet de simplifier et automatiser la gestion du cycle de vie de vos certificats numériques :
- Cartographiez l'ensemble de votre parc de certificats,
- Renouvelez en 1 clic,
- Auditez en continu,
- Programmez vos alertes,
- Automatisez le déploiement.

Avec BerryCert, c'est 50 % de charges opérationnelles gagnées et 90 % d'arrêts de service évités.

BerryTMS est une solution qui vous permet de gérer en toute sécurité un parc important de clés de sécurité. Une seule interface d'application à distance où vous pouvez auditer, générer, sécuriser, restreindre ou révoquer vos clés.
- Déployez facilement et en toute sécurité,
- Gérez via une seule interface et à distance le cycle de vie de vos clés,
- Appliquez votre politique de sécurité,
- Générez intuitivement et de façon sûre les secrets dans vos clés,
- Bénéficiez des audits et reportings complets.

EBRC (European Business Reliance Centre)
https://ebrc.com
(+352) 26 06-1
marketing.support@ebrc.com

1 PARCOURS FONDATION
- Sensibilisation
- Dispositif de sauvegarde
- Audit organisationnel de sécurité
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Sensibilisation
- Analyse de risques
- Restauration de l'activité / PRA

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Plan de sauvegarde
- Plan de reprise d'activité
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Politique SSI
- Indicateurs SSI
- Plan de reprise d'activité

Expert en résilience et sécurité des systèmes d'information, EBRC conseille, conçoit, opère, protège et maintient l'activité digitale des organisations les plus sensibles. EBRC propose une gamme de services intégrés et certifiés ISO 27001, ISO 22301 et ISO 20000, et dispose de ses propres infrastructures de Data Centres certifiés Tier IV et d'un Cloud souverain européen. Par ailleurs, EBRC a rejoint l'initiative GAIA-X en tant que « day one member ». Pilotez votre Cyber-Résilience avec EBRC.

PRODUITS & SERVICES

Le Cyber Resilience Portal (CRP) est un logiciel de gestion de la continuité des opérations qui permet de convertir la méthodologie SMCA (Système de Management de la Continuité d'Activité) et de consolider tous les résultats et livrables nécessaires à assurer la conformité avec la norme ISO 22301 (Système de Gestion de la Continuité des Activités) au travers de 4 modules :
1 - Structure CRP : base du portail, il permet de centraliser les documents nécessaires au SMCA et d'administrer les comptes et les droits d'accès des différents utilisateurs du Cyber Resilience Portal.

2 - BIA : définition des métiers de l'organisation et appréciation des métriques de continuité d'activité tels qu'Objectif de Temps de Reprise (OTR), Objectif de Point de Reprise (OPR), Indisponibilité Maximale Admissible (IMA), visualisation des informations saisies sous forme de rapports consolidés et éditables en vue d'une présentation au management. Le module BIA (Business Impact Analysis) est à la base de l'élaboration des documents nécessaires au SMCA.
3 - Risk : évaluation des risques des métiers de votre organisation.

4 -BCP : génération automatique des Plans de Continuité des Affaires (PCA).

efficient iP®

EfficientIP SAS
https://www.efficientip.com
+33 (0)1 75 84 88 98
info@efficientip.com

1 PARCOURS FONDATION

2 PARCOURS INTERMÉDIAIRE

3 PARCOURS AVANCÉ

4 PARCOURS RENFORCÉ

EfficientIP, société spécialisée dans les solutions DDI (DNS-DHCP-IPAM), avec une croissance parmi les plus fortes au monde, aide les organisations à améliorer leur efficacité opérationnelle en leur permettant de s'appuyer sur des infrastructures réseau à la fois fiables, évolutives et sécurisées. Notre approche unifiée de la gestion DDI et des configurations réseau garantit une visibilité totale, le contrôle de la cohérence et une automatisation poussée.

PRODUITS & SERVICES

La solution EfficientIP SOLIDserver™ offre une technologie DDI intégrée unique, basée sur une gamme de serveurs virtuels et physiques évolutifs, sécurisés et robustes. Les différents modules peuvent être activés à la demande pour s'adapter aux architectures et aux besoins fonctionnels.

SOLIDserver™ DDI : Gestion unifiée et automatisée des services DNS/DHCP multifournisseurs et du plan d'adressage depuis une plate-forme centrale d'administration.

SOLIDserver™ DNS Security : Protection active des utilisateurs, des données et des applications contre les cybermenaces (Phishing, DGA, APT, DoS, etc.).
SOLIDserver™ Network Automation : Découverte automatique des réseaux physiques et virtuelles sur site et dans le Cloud pour optimiser l'utilisation des ressources, diminuer les coûts et améliorer le contrôle de conformité.
SOLIDserver™ DNS GSLB : Routage DNS intelligent du trafic réseau pour optimiser les performances de livraison des applications et renforcer la résilience des services informatiques.

EGERIE
INTEGRATED CYBERRISK MANAGEMENT

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

1 PARCOURS FONDATION
- Sensibilisation
- Analyse des vulnérabilités
- Inventaire des équipements

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Analyse de risques
- Approche Security-by-Design
- Cartographie de l'infrastructure du SI

3 PARCOURS AVANCÉ
- Organisation et Pilotage de la SSI
- Plan de reprise d'activité

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Indicateurs SSI
- Cartographie des données du SI

EGERIE est l'éditeur leader de l'analyse et du pilotage des risques cyber en Europe.
EGERIE propose une plateforme collaborative qui aide les organisations à orchestrer, automatiser et centraliser leurs stratégies d'analyses des risques en cybersécurité et à industrialiser leurs programmes cyber pilotés par les risques.

PRODUITS & SERVICES

Avec sa plateforme logicielle collaborative, son moteur multi méthodes d'analyse et ses bibliothèques métiers et normatives, EGERIE 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.

EGERIE accompagne au quotidien, clients et partenaires, pour répondre à leurs besoins et enjeux métiers que ce soit pour :
- Réaliser des analyses de risques,
- Intégrer la cybersécurité dans les projets,
- Maîtriser la démarche de mise en conformité RGPD,
- Mesurer le niveau d'application des mesures de l'entreprise,
- ...

EQUISIGN

Equisign
https://www.equisign.fr
+33 (0)1 42 91 92 44
contact@equisign.fr

1 PARCOURS FONDATION
- Protection des services exposés sur Internet
- Protection de la messagerie

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Chiffrement des données

3 PARCOURS AVANCÉ
- Effacement des données

4 PARCOURS RENFORCÉ
- Data loss prevention

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). Ces produits sont déployés dans plus de 200 comptes dont une quinzaine issus du CAC 40.

PRODUITS & SERVICES

MFT est la solution de transfert sécurisé de fichiers utilisée par 150 groupes et par plus d'un million 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** est disponible par abonnement 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 et de l'article 48 du Décret n° 2020-834 du 2 juillet 2020.

ERCOM
Cyber Solutions by Thales

ERCOM
https://www.ercom.fr
+33 (0)1 39 46 50 50
marcom@ercom.fr

1 PARCOURS FONDATION
- Protection des accès distants
- Protection de la messagerie
- VPN
- Dispositif de sauvegarde

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Chiffrement des données
- Sécurisation du réseau
- End point security

3 PARCOURS AVANCÉ
- Chiffrement des postes de travail

4 PARCOURS RENFORCÉ
- Data loss prevention
- Sécurité des équipements mobiles

Depuis plus de 30 ans, Ercom a développé une position de leader sur les marchés de la sécurité des communications, des données et des terminaux. Cette position repose sur des expertises en infrastructure télécom, cloud, en cryptographie et sur des valeurs partagées : innovation, expertise, engagement et confidentialité. Cela permet à Ercom de proposer des solutions avec le meilleur niveau de sécurité avec une expérience utilisateur digne des meilleurs produits grand public.

PRODUITS & SERVICES

Ercom a pour vocation de protéger les données et les communications de ses clients, au bureau, en mobilité ou en situation de télétravail. **Cryptosmart** fournit aux terminaux Android Samsung une triple protection au niveau « Diffusion Restreinte ». La version mobile offre par le chiffrement de bout en bout, la protection du terminal et de ses données, des communications voix et SMS et des flux internet (VPN). La version PC offre la protection des flux internet (VPN). **Cryptobox** est une solution de partage de fichiers et de travail collaboratif avec un niveau de sécurité « Diffusion Restreinte ».

Cryptobox a été développée pour le Cloud avec la sécurité au cœur de chaque fonctionnalité. Le chiffrement de bout en bout et toutes les fonctions de sécurité sont quasi invisibles grâce à une expérience utilisateur grand public. Citadel est un service de messagerie, d'audio et visio conférence idéal pour collaborer en toute sécurité et confidentialité.
Cybels Hub DR est une plateforme collaborative sécurisée dans le Cloud sécurisé Thales pour collaborer au niveau « Diffusion Restreinte ». Ce service réunit les solutions Citadel et Cryptobox sur une seule plateforme afin de faciliter et booster la collaboration entre clients et partenaires sur des données sensibles ou confidentielles.

EVERTRUST

EverTrust SAS
https://evertrust.fr
+33 (0)1 88 32 74 02
contact@evertrust.fr

1 PARCOURS FONDATION

- Protection des accès distants
- Protection des services exposés sur Internet
- Protection des accès réseau Wi-Fi
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE

- Chiffrement des données
- Sécurisation du réseau
- Sécurisation des services Cloud (IaaS/PaaS)
- Gouvernance des Identités et des Accès

3 PARCOURS AVANCÉ

- Organisation et pilotage de la SSI
- Authentification forte

4 PARCOURS RENFORCÉ

- Organisation et pilotage de la SSI
- Politique SSI
- Indicateurs SSI

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).

PRODUITS & SERVICES

Nos logiciels Stream, Horizon et OCSP 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.
Notre offre SaaS est facile à déployer - facile à utiliser - performante - ergonomique - sans captivité : vous gardez le contrôle.
EverTrust Horizon est une solution de gouvernance et de gestion du cycle de vie des certificats X.509 qui permet de :

- Réaliser un inventaire des certificats X.509 déployés au sein du SI de l'organisation.
- Analyser le parc de certificats afin d'en examiner la conformité afin de définir les actions à mener pour remédier aux écarts constatés.
- Déployer les certificats depuis une interface unifiée ou via divers scénarios d'automatisation.

Ces fonctionnalités permettent de systématiser le déploiement des certificats émis par la ou les IGCs de l'organisation.
Puis de gérer la bonne conformité initialement et sur la durée.
Le cas échéant, EverTrust peut fournir sa propre IGC.
Les offres sont commercialisées pour être déployées au sein du SI de l'organisation en environnement Cloud ou SaaS.

EXAMIN

Examin
https://examin.eu
+33 (0)6 64 69 84 94
f.duflot@examin.eu

1 PARCOURS FONDATION

- Identification des partenaires

2 PARCOURS INTERMÉDIAIRE

- Politique SSI
- Analyse de risques

3 PARCOURS AVANCÉ

- Organisation et pilotage de la SSI
- Homologation des SI sensibles
- Plan de reprise d'activité

4 PARCOURS RENFORCÉ

- Organisation et pilotage de la SSI
- Politique SSI
- Indicateurs SSI
- Audit, scan, revue de code

Examin est un éditeur de logiciel de conformité dans le domaine de la cybersécurité et de la protection des données.
Nous fournissons une plateforme pour gérer la conformité à la réglementation (LPM, NIS, PSSIE, Guide d'hygiène...) et aux normes techniques (ISO 27k, PCI-DSS..) y compris sectorielles (MaturiN-H, HOP'EN...).
Nous assistons nos clients pour qu'ils puissent mettre en place des dispositifs de conformité performants et pérennes (audit, pilotage, etc.).

PRODUITS & SERVICES

Examin permet d'assurer un pilotage précis et rapide de la conformité sur l'ensemble de notre catalogue de normes (plus de 50 à ce jour !) avec la possibilité d'importer des référentiels de toute nature (réglementaire, technique, interne, etc.).

Elle agit comme un véritable tiers de confiance qui va proposer un ensemble de fonctionnalité complet (tableau de bord, rapport, plan d'action, suivi des recommandations, gestion des utilisateurs, suivi des risques, etc.) destiné à faciliter vos audits, le suivi de vos certifications, etc. Elle va également enregistrer les preuves de conformité au fil de l'eau afin que l'utilisateur puisse prouver à tout moment la situation ainsi que les actions réalisées.

Enfin, elle permet d'assurer un suivi et d'avoir une vision globale de la conformité de l'ensemble de son écosystème particulièrement utile aux groupements de communes, agglomérations, groupement hospitaliers, etc. tout en limitant la charge associée à ces audits.
Elle est disponible gratuitement sur quelques référentiels et guides de l'ANSSI.

eXo

eXo Platform
https://www.exoplatform.com/fr/
+33 (0)1 82 83 77 31
contact@exoplatform.com

C.A.I.H. UGAP

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Protection des services exposés sur Internet
- Dispositif de sauvegarde

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Approche Security-by-design
- Sécurité applicative
- Gestion des comptes de service

3 PARCOURS AVANCÉ

4 PARCOURS RENFORCÉ

Éditeur français de logiciels open-source depuis 20 ans, eXo Platform est un spécialiste des solutions collaboratives, intranet et digital workplace. eXo accompagne ses clients dans leur transformation digitale en leur offrant une plateforme ergonomique, complète, sécurisée et souveraine au service de l'expérience collaborateur. Avec son approche agile et son accompagnement sur mesure à la conduite de changement, eXo favorise une adoption de la solution dans la durée.

PRODUITS & SERVICES

Plateforme flexible disponible dans le cloud (hébergement SecNumCloud) ou on-premise, eXo permet de construire des solutions adaptées aux différents cas d'usages des administrations, collectivités territoriales et entreprises : intranet, plateforme collaborative, digital workplace, base de connaissances, portail partenaires et gestion de communautés.
La solution eXo offre une expérience centrée utilisateur, fluide, intégrée et unifiée autour de 4 piliers – communication, collaboration, connaissance et productivité.

Solution open-source, eXo Platform propose des fonctionnalités renforçant la sécurité applicative, telles que la protection contre la fuite de données (DLP), l'authentification multi-facteur ou la gestion des collaborateurs externes.

eXo se positionne comme une alternative souveraine à Office 365.

F24

F24 France SAS
https://f24.com/fr/
+33(0)1 45 93 90 93
Sales_france@f24.com

C.A.I.H. UGAP

1 PARCOURS FONDATION
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- SIEM

Fondé en 2000, F24 est le 1er fournisseur européen de logiciels SaaS pour la gestion des incidents et des crises, les notifications d'urgence.
F24 équipe des OIV français, des sites SEVESO, des hôpitaux, et des institutions comme les ARS, l'AFD ainsi que de nombreux clients du CAC40.
F24 équipe également la Belgique pour son alerte à la population.
F24 s'appuie sur une équipe dédiée pour accompagner ses clients dans la mise en place et le suivi de leurs plans, PCA, PRA.

PRODUITS & SERVICES

F24 propose des solutions complètes, permettant de rapidement s'équiper pour faire face à une menace cyber via une solution résiliente pour les PCA, PRA et DRP. FACT24 ENS+ est une solution d'alerte et de mobilisation de cellule de crise permettant de prévenir ou de réunir des collaborateurs en quelques secondes ou de mobiliser une cellule de crise. Largement utilisée en France pour alerter, mobiliser, organiser des cellules de crise en urgence, des téléconférences. **FACT24 CIM** offre en plus de l'alerte, un tableau de bord complet pour gérer les incidents cyber.

Description de l'incident, affichage du PRA ou du PCA, gestion de tâches. Tout est tracé, horodaté. **FACT24 CIM** intègre une gestion documentaire, un tchat sécurisé et indépendant du SI client, un outil de création de rapports (Points de situation, Rapport d'intervention), une main courante dynamique. Disponible sur tablette, Android ou IOS.

FACT24 CIM est un outil complet résilient pour gérer toutes vos situations de crise. ISO 27001 et 22301- Disponibilité garantie de 99,99 % sur l'alerte et 99,5 % en gestion de crise.

formind

Formind
https://www.formind.fr
contact@formind.fr

1 PARCOURS FONDATION
- Sensibilisation
- Scans de vulnérabilité du SI exposé sur Internet
- Audit organisationnel de sécurité
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Analyse de risques
- Test de phishing
- Gouvernance des Identités et des Accès

3 PARCOURS AVANCÉ
- Sensibilisation et formation
- Plan de reprise d'activité
- Tests d'intrusion
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Audit red team
- Forensic et analyse des logs
- SOC

Formind est un leader Français indépendant expert en cybersécurité. Créé en 2010 et pure player de plus de 260 consultants, Formind connaît une forte croissance en développant de nombreuses expertises/savoir-faire en cybersécurité.

Créé initialement à Paris, Formind s'est déployé à Rennes, Nantes, Lyon, Toulouse, Bordeaux ainsi qu'au Maroc, en Espagne et au Canada. Formind accompagne ainsi ses clients sur toute problématique avec une vision risque.

PRODUITS & SERVICES

Formind accompagne ses clients sur de nombreux sujets cyber :
- Gouvernance cyber : Stratégie, gestion des risques, pilotage et contrôle.
- Continuité, crise et résilience.
- Conformité légale, réglementaire et normative.
- Expertise technique, architecture, Cloud, IAM, OT
- Intégration de solutions.
- Audits techniques, sûreté, redteam,
- Services managés (CERT, SOC, vulnérabilités) et gestion d'incident (FIR).
- Formation.

Notre objectif reste le même : accompagner nos clients sur des problématiques de gestion de risques et être à leurs côtés avec une véritable volonté d'engagement et de proactivité sur les solutions que nous pouvons leur apporter.

Nous intervenons aussi bien en engagement de moyens que de résultats et veillons à adapter notre approche à chaque contexte.

GATEWATCHER

GATEWATCHER
https://www.gatewatcher.com/
+33 (0)1 44 51 03 93
contact@gatewatcher.com

1 PARCOURS FONDATION
- Inventaire des équipements
- Antivirus
- Cartographie du réseau
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Sécurisation du réseau
- Cartographie de l'infrastructure du SI
- Sécurisation des services Cloud (IaaS / PasS)
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Homologation des SI Sensibles
- Détection d'intrusion, EDR, IPS
- Filtrage de flux réseau
- Protection DDOS

4 PARCOURS RENFORCÉ
- Homologation des SI sensibles
- Sondes de détection d'intrusion
- Forensic et analyse des logs
- SOC

Leader technologique dans la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux critiques des grandes entreprises et des institutions publiques, en France et à l'international.

Notre offre associe l'IA à des techniques d'analyse dynamique pour offrir une vision à 360° et en temps réel des cybermenaces sur l'ensemble du réseau, dans le cloud et on premise.

PRODUITS & SERVICES

Nos solutions apportent une amélioration immédiate aux enjeux actuels et futurs de cybersécurité par une réponse adaptée aux nouveaux besoins de détection des organisations. Elles sont conçues pour être évolutives et immédiatement opérationnelles pour une intégration et un usage simplifié chez nos clients et partenaires.

Gatewatcher NDR : plateforme de détection et de réponse réseau pour identifier avec certitude les actions malveillantes, comportements suspects par une cartographie de l'intégralité des assets présents sur le SI.

Qualifiée ANSSI depuis 2019, **Gatewatcher Sensors** répond aux enjeux des organisations qui doivent se conformer aux recommandations et exigences réglementaires de détection réseau en temps réel.
Gatewatcher CTI : offre de Cyber Threat Intelligence offrant une amélioration immédiate de votre niveau de protection en enrichissant vos outils de cybersécurité par des renseignements contextuels sur les cybermenaces internes et externes visant spécifiquement votre activité.
Gatewatcher Analyser : solution pour opérer une levée de doute en analysant les fichiers et URL potentiellement malveillants dans un environnement contrôlé afin d'effectuer une première estimation des capacités de nuisance d'un malware.

GLIMPS

GLIMPS
https://www.glimps.fr/
+33 (0)2 44 84 78 44
contact@glimps.re

1 PARCOURS FONDATION
- Protection de la messagerie
- Protection des services exposés sur Internet
- Antivirus
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Sécurisation du réseau
- End point security
- Sécurisation des services Cloud (IaaS/PaaS)
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Détection d'intrusion, EDR, IPS
- Filtrage de flux réseau
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Sondes de détection d'intrusion
- IPS; EDR
- SIEM
- SOC

Créée en 2019 par 4 experts en reverse-engineering, GLIMPS propose des solutions de cybersécurité basées sur une technologie révolutionnaire capable de lire et de comprendre le code informatique de manière automatique.

Cette technologie a permis de développer des solutions de cybersécurité à des fins d'analyse d'applications et de détection de malwares avancés : GLIMPS Audit et GLIMPS Malware.

PRODUITS & SERVICES

Basée sur le Deep Learning, la technologie GLIMPS permet d'extraire d'un binaire les concepts associés à un code informatique, nommés les « concepts-code ». La confrontation de ces derniers entraîne une comparaison efficace des logiciels à notre base de données afin d'en isoler les points communs. Nos deux produits incluent cette technologie de manière unique : **GLIMPS Malware**, notre eXtended **Malware Analysis Platform** permet de faire face aux groupes d'attaquants les plus armés avec l'analyse, la détection et la caractérisation de tous vos fichiers.

GLIMPS Audit est un outil de reconnaissance et reverse-engineering automatique de software. Il est destiné aux auditeurs de logiciels souhaitant un gain de temps dans l'analyse d'un binaire.

HarfangLab

HarfangLab
https://www.harfanglab.io
marketing@harfanglab.fr

1 PARCOURS FONDATION
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- End point security
- Gestion des logs
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Web application firewall
- Détection d'intrusion, EDR, IPS
- Gestion des logs
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- IPS; EDR
- Forensic et analyse des logs

HarfangLab, éditeur français, propose aujourd'hui le seul EDR certifié par l'ANSSI. L'entreprise s'attache à proposer la meilleure technologie de protection au niveau des terminaux. Grâce à elle, les RSSI n'ont plus à choisir entre la protection de leur SI et la maitrise de leurs données. Ce positionnement fait d'HarfangLab le principal éditeur des collectivités territoriales et les établissements de santé.

PRODUITS & SERVICES

HarfangLab EDR est une solution de sécurité composée d'agents logiciels sur les terminaux (postes de travail ou serveurs) et d'un manager qui pilote les capacités de cyberdéfense.
Notre technologie se distingue par ses 5 moteurs de détection complémentaires qui lui permettent de proposer une capacité de détection efficace contre tout type de menace.

La solution permet de qualifier au plus vite les alertes de sécurité grâce à ses fonctions d'investigations avancées et offre des capacités de remédiation simultanée sur tous les postes infectés.

Les choix technologiques décidés dès 2018 permettent de bénéficier de toutes les fonctionnalités d'**HarfangLab EDR** par un déploiement simple, tant en Cloud qu'en On-Premise.

Les agents logiciels sont développés en RUST. Langage renommé comme étant l'un des plus fiables et des plus économiques tant en consommation énergétique qu'en RAM & CPU.

Ces agents s'installent et se mettent à jour sans redémarrage des terminaux. Notre EDR est reconnu pour s'intégrer facilement aux autres solutions de protection déjà présentes dans votre parc.

HIAsecure
https://hiasecure.com/
+33 (0)1 83 62 53 75
contact@hiasecure.com

1 PARCOURS FONDATION
- Gestion des mots de passe
- Protection des accès distants
- Protection des services exposés sur Internet
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Coffres-forts de mots de passe
- End point security
- Gestion des comptes de service
- Gouvernance des Identités et des Accès

3 PARCOURS AVANCÉ
- Gestion des droits d'accès
- Authentification forte
- Gestion des comptes à privilèges

4 PARCOURS RENFORCÉ
- SSO

HIAsecure est une société innovante spécialisée dans le domaine de l'authentification cognitive forte. Ses produits répondent aux normes bancaires européennes DSP2 et RGPD.

HIAsecure a été conçu pour sécuriser les opérations en ligne au travers de 2 types de solutions MFA :
1. L'authentification de l'usager
2. La certification de transaction

PRODUITS & SERVICES

HIAsecure garantie, à chaque transaction, l'intervention humaine de l'usager. HIAsecure propose un service d'authentification des usagers et de sécurisation des transactions en rupture avec les solutions du marché. Basé sur le constat que quel que soit la méthode utilisée (je possède, je connais, je suis), les fraudes et usurpations de privilèges (et rançongiciel) n'ont jamais été aussi importantes. HIAsecure propose une solution qui s'appuie sur une spécificité inhérente à l'être humain : sa capacité cognitive.
L'usager est pourvu d'une formule qui lui est propre, qu'il appliquera sur chaque challenge présenté pour s'authentifier ou certifier une opération (« je sais bâtir la réponse attendue»).

La technologie proposée est RGPD par conception (architecture Cloud hybride et distribuée sur base de containers, disponible en mode SaaS), compatible des schémas DSP2 et eiDAS et permet de viser les plus haut niveaux d'assurance pour les Clients et les utilisateurs. La plateforme de service intègre les derniers standards du marché (SAML, OpenID Connect, OAuth2 et bien entendu Keycloak) et peut aussi être utilisé en complément des systèmes Legacy existant.

HOLISEUM
https://www.holiseum.com
contact@holiseum.com

1 PARCOURS FONDATION
- Sensibilisation
- Analyse des vulnérabilités
- Scans de vulnérabilité du SI exposé sur Internet
- Audit organisationnel de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Analyse de risques
- Approche Security-by-design
- Scans de vulnérabilité sur tout le SI

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Sensibilisation et formation
- Homologation des SI sensibles
- Tests d'intrusion

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Politique SSI
- Homologation des SI sensibles
- Audit red team

- Spécialiste de la protection des infrastructures critiques et industrielles (IT/OT/SI Sûreté/IoT).
- Editeur du 1er tir à Blanc de Ransomware du marché.
- Qualifié PASSI sur l'ensemble des portées.
- Approche holistique de la cybersécurité.

PRODUITS & SERVICES

Nos consultants interviennent sur des missions à fortes valeurs ajoutées et sur des problématiques et contextes complexes au travers de nos 5 services :
- **CONSEILLER :** Aider votre organisation à établir ou développer une stratégie globale de sécurité.
- **AUDITER :** Proposer une gamme complète d'audits, du plus élémentaire au plus complexe.
- **SÉCURISER :** Accompagnement, cadrage et intégration de solutions cybersécurité.
- **FORMER :** Sensibiliser et former vos collaborateurs aux problématiques de la cybersécurité.
- **INVESTIGUER :** Faire la lumière sur les compromissions avérées ou supposées.

HOLISEUM s'investit également fortement dans les activités d'innovation et R&D en cybersécurité et disciplines adhérentes de pointe (ex. blockchain, quantique, etc.) et est un acteur reconnu pour ses innovations telles que :
- Le 1er « Tir à Blanc de Ransomware » du marché;
- La création de démonstrateurs de hacking réalistes sur des systèmes divers (industriels, maritime, sûreté);
- Une approche éducative unique : la web-série Cyber Vox®, le serious game Cyber Wargame® etc.

Idento - I-TRACING Group
https://idento.fr
+33 (0)1 47 99 55 49
contact@idento.fr

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Gestion des mots de passe
- Gestion des comptes à privilèges
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Gestion du cycle de vie des utilisateurs et des habilitations
- Coffres-forts de mots de passe
- Gouvernance des Identités et des Accès

3 PARCOURS AVANCÉ
- Gestion des droits d'accès
- Revues d'habilitations
- Authentification forte

4 PARCOURS RENFORCÉ
- Revue d'habilitations
- SSO

Idento, filiale d'I-TRACING, est le leader français dans la gouvernance des identités et des accès (IAM) avec 85 experts dédiés. I-TRACING, pure-player des services de cybersécurité, accompagne plus de 400 clients, dont 35 acteurs du CAC 40, dans la maîtrise de leurs risques cyber depuis l'anticipation des menaces pour maintenir le meilleur niveau de sécurité de leurs systèmes et actifs, à la capacité de réaction en cas d'attaques pour limiter les conséquences.

PRODUITS & SERVICES

Au travers d'une gamme complète de service de cybersécurité allant du conseil à l'intégration aux services managés, SOC et CERT, I-TRACING réunit toutes les expertises techniques et l'expérience d'ingénierie pour répondre aux demandes des clients les plus exigeants.

I-TRACING propose une offre de services de bout en bout allant du conseil à l'intégration, jusqu'aux services managés. Fort de ses retours d'expérience et de sa culture de la sécurité, I-TRACING accompagne ses clients dans de nombreux domaines d'expertises :
- Gestion des identités & des accès (IAM) au travers de sa filiale IDENTO.
- Gestion des menaces & des vulnérabilités.
- Sécurité du Cloud.
- Sécurité des infrastructures réseaux.
- Sécurité des applications (AppSec).
- Protection des données.
- Gestion des risques & Conformité.
- Sécurité du workplace.
- Sécurité industrielle & OT.

Ilex - Inetum Group
https://www.ilex.fr/
+33 (0)1 46 88 03 40
info@ilex.fr

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Gestion des mots de passe
- Protection des accès distants
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Gestion du cycle de vie des utilisateurs et des habilitations
- Coffres-forts de mots de passe
- Gouvernance des Identités et des Accès

3 PARCOURS AVANCÉ
- Gestion des droits d'accès
- Revues d'habilitations
- Authentification forte

4 PARCOURS RENFORCÉ
- Revue d'habilitations
- SSO

Dans le domaine de la cybersécurité, Inetum accompagne ses clients dans leur stratégie IAM grâce à la plateforme Ilex Identity & Access Management. Cette offre complète se décline en 3 gammes de solutions : Ilex Access Management, Ilex Identity Management et Ilex Customer IAM.

Forte de plus de 300 clients et 14 millions d'utilisateurs, l'offre Ilex IAM Platform est notamment déployée dans de très nombreux établissements de santé, collectivités, ministères ou organismes. #IAM #CIAM #SSO #MFA #Passwordless

PRODUITS & SERVICES

Notre plateforme IAM offre un large catalogue de solutions, rapides à déployer, capables de répondre à l'ensemble de vos besoins et de couvrir tous vos cas d'usages utilisateurs. Elle répond en particulier aux enjeux spécifiques des établissements de santé (CPS/e-CPS et Pro Santé Connect, ...) ou des collectivités (FranceConnect et portail citoyen, Carte de Vie Quotidienne, ...).
La gamme '**Ilex Access Management**' couvre tous les domaines de la gestion des accès : authentification multi-facteur et adaptative, single sign-on (SSO) et fédération d'identités, self-service password reset, card management system.
La gamme '**Ilex Identity Management**' adresse la gestion et gouvernance des identités et des habilitations : gestion automatisée du cycle de vie des utilisateurs du système d'information et de leurs droits sur le SI.
La gamme '**Ilex CIAM**' permet de maîtriser les identités et des accès de vos utilisateurs 'grand public' (citoyens, patients, ...) et de leur offrir ainsi une expérience utilisateur optimale au service d'une relation de confiance, conforme à la réglementation.

ISE SYSTEMS
https://www.ise-systems.fr
+33 (0)6 13 22 33 71
mickael.attias@ise-systems.fr

1 PARCOURS FONDATION
- Sensibilisation
- Analyse des vulnérabilités
- Scans de vulnérabilité du SI exposé sur Internet
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation
- Test de phishing
- Gestion des logs
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Sensibilisation et formation
- Détection d'intrusion, EDR, IPS
- Tests d'intrusion
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Audit red team
- Scans de vulnérabilité en continu
- SOC

ISE SYSTEMS conçoit et déploie pour ses clients des programmes de formations et d'entraînements permettant aux organisations d'améliorer efficacement leur niveau de cyber résilience. Grâce à son expertise de plus de 15 ans en cybersécurité et la maîtrise de technologies de simulations et de plateforme d'entraînements cyber, ISE SYSTEMS propose des parcours d'entraînements et d'exercices de crises uniques où la plus grande part de la pédagogie est laissée aux mises en situation Pro.

PRODUITS & SERVICES

L'offre **CyberGame** 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. Différents types de cyberattaques sont traités en temps réel, permettant d'expérimenter une gamme d'impacts sur l'ensemble des équipements du S.I complet (intégrité des données, disponibilité du service, perte de confidentialité) mis à disposition par la plateforme. L'architecture et la souplesse de la plateforme permettent de concevoir des exercices pour des équipes de nombreux joueurs agissant simultanément comme équipe de défenseurs sur plusieurs sites de manière native. 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.

JALIOS
https://www.jalios.com
+33 (0)1 39 23 92 80
info@jalios.com

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Protection des accès distants
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Gestion du cycle de vie des utilisateurs et des habilitations

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Sensibilisation et formation
- Gestion des droits d'accès
- Authentification forte

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- SSO
- Cartographie des données du SI

Leader français sur le marché Cloud et On-Premise d'Intranet et de Digital Workplace, Jalios a pour mission de rendre les organisations plus efficaces et le travail de chacun plus épanouissant. Jalios compte plus de 450 clients, dont de nombreuses collectivités territoriales (20 départements, 6 régions, 40 villes et intercommunalités, 17 SDIS) et organismes de santé (l'Agence de Biomédecine, la HAS, l'ANAP, le SNITEM, des ARS, des CPAM, le CHPF, la FHVI, l'ADMR, etc.).

PRODUITS & SERVICES

Jalios Workplace est un environnement de travail numérique complet, utilisé au quotidien en tant qu'Intranet, Digital Workplace, Extranet, Réseau social, Gestion documentaire (GED), Base de connaissances (KM), Plateforme collaborative, ou encore d'e-learning.

Répondant à la fois aux enjeux de communication interne, de collaboration et de gestion des connaissances, la solution fluidifie le parcours utilisateur. Elle s'adresse à tous les collaborateurs, au siège comme sur le terrain, pour créer du lien et permettre une collaboration transverse et tenable dans la durée, même avec les externes.

Interopérable, **Jalios Workplace** se décline en 3 éditions prêtes à l'emploi, personnalisables et extensibles. Les éditions dédiées à Microsoft 365 et à Google optimisent et complètent l'utilisation de ces suites. L'édition Liberty est une alternative souveraine.

Multicloud, la solution est disponible en SecNumCloud et en cloud privé. Son socle JPlatform a été homologué CSPN par l'ANSSI.

Jamespot

Jamespot
https://www.jamespot.com
+33 (0)1 48 58 18 01
info@jamespot.com

1 PARCOURS FONDATION
- Sensibilisation
- Protection des accès distants
- Dispositif de sauvegarde
- Scans de vulnérabilité du SI exposé sur Internet

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation
- Sécurité applicative
- Restauration de l'activité / PRA
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ

4 PARCOURS RENFORCÉ

Éditeur de solutions collaboratives dans le cloud, Jamespot réinvente la communication et la collaboration d'entreprise depuis plus de 15 ans en créant des outils collaboratifs sécurisés et facilement déployables et utilisables pour les organisations. La solution Jamespot est aujourd'hui utilisée par plus de 400.000 utilisateurs à travers le monde.

PRODUITS & SERVICES

Sous la forme d'un intranet, d'un réseau social d'entreprise, d'une Digital Workplace ou de bureaux virtuels, la solution Jamespot se distingue par sa modularité, son haut niveau de sécurité et sa facilité de déploiement et d'utilisation à travers son large panel de fonctionnalités no code.
2 offres sont spécifiquement dédiées à la sécurité :

- L'offre Vault dédiée aux grandes entreprises ;
- L'offre HDS dédiée aux données de santé.

jscrambler

jscrambler
https://jscrambler.com
hellojscrambler.com
+33 (0)6 47 61 84 37
herve.hulin@jscrambler.com

1 PARCOURS FONDATION
- Identification des partenaires
- Analyse des vulnérabilités
- Protection des services exposés sur Internet

2 PARCOURS INTERMÉDIAIRE
- Scans de vulnérabilité du SI exposé sur Internet
- Identification des partenaires
- Sécurité applicative
- End point security

3 PARCOURS AVANCÉ

4 PARCOURS RENFORCÉ

Jscrambler, leader de la sécurité côté client, protège les sites Web en rendant visibilité et contrôle du code exécuté dans le navigateur, permettant de détecter et bloquer les attaques Magecart et l'exfiltration de données.

Les applications JavaScript deviennent auto défensives, et résistantes à la falsification et à la rétro-ingénierie. Avec Code Integrity (Applications) et Web Page integrity (sites Web), les utilisateurs de vos services en ligne sont protégés.

PRODUITS & SERVICES

Code Integrity (CI) Solution de sécurité résiliente pour vos Applications Javascript avec technique d'obscurcissement « obfuscation » polymorphe combiné à des mécanismes de renforcement de la sécurisation (« Code-Locks, Countermeasures, Runtime Code Protection »).

Différents outils pour garantir les objectifs de performance et de taille de fichiers. Il est possible de sécuriser des applications hybrides Mobiles avec la complémentarité de nos partenaires protégeant les applications natives.

Web Page Integrity (WPI) est une solution permettant une meilleure visibilité et surveillance de la sécurité des sites WEB côté CLIENT/ Navigateur en contrôlant l'activité des « Third Party » scripts. L'utilisation de Jscrambler facilite la mise en conformité par exemples pour RGPD et PCI-DSSv4.
Reconnue par « Fortune 500 » et des grandes entreprises, aux cas d'usages liés aux données sensibles, Jscrambler est mentionnée régulièrement par Gartner.
Pour plus d'informations, jscrambler.com.

KDDI France

KDDI France
https://www.kddi.fr
+33 (0)1 58 01 29 80
telecloud-sales@fr.kddi.eu

1 PARCOURS FONDATION
- Filtrage Réseau
- Dispositif de sauvegarde
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Gestion des mises à jour de sécurité
- Sécurisation du réseau
- Sécurisation des services Cloud (IaaS/PaaS)
- Contrôle d'accès physique

3 PARCOURS AVANCÉ
- Filtrage de flux réseau
- Protection DDOS
- Plan de sauvegarde
- Plan de reprise d'activité

4 PARCOURS RENFORCÉ
- Plan de reprise d'activité

KDDI France, fournisseur de Cloud privé souverain :
- Héberge les applications de production sur ses plateformes Cloud.
- Protège les données contre les sinistres et les ransomwares.
- Assure une continuité de service pour les applications critiques.
- Dispose des certifications ISO 27001, 9001, 14001, 50001 et HDS.

PRODUITS & SERVICES

TELECLOUD AGILITY
VM à la demande avec services d'infrastructure :
- Firewall, supervision, snapshots, ...
- PRA intégré en option (différents RTO/RPO disponibles).

TELECLOUD DIRECTOR
Datacenter virtuel en self-provisionning basé sur VMware Cloud Director :
- Réplication synchrone possible sur site distant pour PCA.

TELECLOUD CYBER PROTECTION
Sauvegarde déportée pour vous protéger d'un sinistre ou d'une cyberattaque :
- Avec option coffre-fort numérique et PRA.

KUB

KUB Cleaner
https://www.kub-cleaner.com
+33 (0)1 74 90 39 00
contact@kub-cleaner.com

1 PARCOURS FONDATION
- Antivirus
- Protection des accès distants
- Gestion centralisée des identités
- Analyse des vulnérabilités

2 PARCOURS INTERMÉDIAIRE
- End point security
- Gestion centralisée des appareils mobiles

3 PARCOURS AVANCÉ
- Homologation des SI sensibles
- Chiffrement des postes de travail
- Détection d'intrusion, EDR, IPS
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Sécurité des équipements mobiles
- Forensic et analyse des logs
- SIEM
- SOC

KUB est née dans l'industrie française de la Défense. KUB est leader des solutions de stations blanches antivirus et antimalware pour tous les périphériques amovibles USB.

KUB Cleaner est une solution pour l'Industrie, l'IT, l'OT et la Défense, permettant d'analyser tous vos matériels USB, de détecter les menaces connues et inconnues (0Day, APT, ...), de les nettoyer et enfin de certifier le support USB. KUB adresse les contraintes réglementaires : ii901, IGI1300, ANSSI.

PRODUITS & SERVICES

La solution KUB Cleaner, c'est :
- La décontamination et la certification de vos supports USB.
- Le transfert de fichiers depuis le KUB vers l'entreprise en mode SaaS.
- L'effacement sécurisé des périphériques avec 12 méthodes différentes.
- L'analyse des supports chiffrés, l'authentification utilisateurs, la 4G, le fonctionnement complet en Airgap et Offline.

Les KUB existent en 4 formats :
- **KUB Mobile :** prévu pour la mobilité et les conditions extrêmes,
- **KUB Satellite** utilisé sur les navires, les plateformes offshores,
- **KUB Console** utilisé dans les bureaux et les salles de réunion,
- **KUB Totem** destiné aux zones d'accueil du public.

KUB est une solution durcie physiquement et logiciellement prévue pour répondre aux exigences réglementaires, opérer dans les conditions extrêmes : nos clients utilisent tous les jours plus de 3000 stations KUB, dans des bureaux, des navires, des plateformes offshore et bien plus !

LEVIIA
https://www.leviia.com
+33 (0)7 45 89 16 66
quentin.maury@leviia.com

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Protection des accès distants
- Authentification et contrôle d'accès
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation
- Approche Security-by-design
- Chiffrement des données
- Sécurisation du réseau

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Web application firewall
- Filtrage de flux réseau
- Protection DDOS

4 PARCOURS RENFORCÉ
- SSO
- Audit, scan, revue de code
- Plan de reprise d'activité
- SOC

Spécialistes du stockage de données en ligne, nous concevons des solutions françaises, performantes et accessibles au prix juste :
- une solution drive pour les particuliers et les professionnels avec suite collaborative intégrée.
- une solution stockage objet souveraine et jusqu'à 4 fois moins chère que nos concurrents, à performances égales voire meilleures.

Utilisée par plus de 250 000 utilisateurs, notre infrastructure est robuste et résiliante, répliquée (erasure coding) dans trois data-centers distants de plusieurs dizaines/centaines de kilomètres (Strasbourg, Roubaix et Gravelines).
Anti-DDOS, WAF, SSO, snapshots... secure by Design !

PRODUITS & SERVICES

Notre technologie permet de garantir une durabilité des données de 99,999999 % et une très haute disponibilité. Nous proposons des débits allant jusqu'à 10 Gbit/s sans mesure de consommations.
Nous nous positionnons comme un challenger des gros acteurs américains avec une technologie et un prix concurrent de ceux-ci.
Nous souhaitons prouver qu'il est possible de stocker ses données en France dans les mêmes conditions techniques et à des prix plus abordables que les acteurs américains et chinois.

Offres Drive :
- Particuliers à partir de 2 € HT par mois pour 100 Go de stockage.
- Pro à partir de 50 € HT/mois pour une instance dédiée en totale marque blanche (nom de domaine, logo, couleurs, base de données) comprenant 5 utilisateurs et 1 To de stockage.
- Leviia Next : déploiement d'instance Nextcloud massive avec milliers d'utilisateurs et Po de données sur une infrastructure dédiée.

Offre Stockage objet (comptabile S3) :
- 5,99€/To/mois (sans aucun autre frais). 80 % moins chers qu'Amazon S3 avec souveraineté de vos données garantie.

Société française et data-centers en France.

Login Sécurité
https://www.login-securite.com/
+33 (0)6 83 17 48 55
brice.bonnet@login-securite.com

1 PARCOURS FONDATION
- Analyse des vulnérabilités
- Scans de vulnérabilité du SI exposé sur Internet
- Audit organisationnel de sécurité
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Test de phishing
- Scans de vulnérabilité sur tout le SI
- Gestion des logs

3 PARCOURS AVANCÉ
- Audit, scan, revue de code
- Test d'intrusion
- Gestion des logs
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Audit red team
- Forensic et analyse des logs
- SOC
- Data loss prevention

Login Sécurité est une société de conseil et de services en Cybersécurité qui accompagne ses clients dans la gestion de leurs risques Cyber via des missions de conseil, d'audit et de tests d'intrusion, de formation et de sensibilisation, et de sécurité opérationnelle au travers de son SOC mutualisé et externalisé.

PRODUITS & SERVICES

La nature des menaces auxquelles sont confrontées les entreprises a profondément évolué ces dernières années. Les cyber criminels sont organisés et se comportent aujourd'hui comme des professionnels à la recherche de performances et de gains financiers, vendant leurs services à des commanditaires aux mobiles de tous ordres.

Login Sécurité accompagne ses clients dans la protection de leurs informations et leur permet de saisir de nouvelles opportunités et d'accélérer le développement de leur potentiel numérique en toute confiance.

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 :
- Identifier et prévenir les risques.
- Protéger les informations.
- Détecter et réagir.

MAILINBLACK

Mailinblack
https://www.mailinblack.com/
+33 (0)4 88 60 07 80
contact@mailinblack.com

C.A.I.H.

UGAP

1 PARCOURS FONDATION
- Sensibilisation
- Protection de la messagerie
- Antivirus

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation
- Test de phishing
- Scans de vulnérabilité sur tout le SI

3 PARCOURS AVANCÉ
- Sensibilisation et formation
- Audit, scan, revue de code

4 PARCOURS RENFORCÉ

Mailinblack, entreprise française experte en cybersécurité depuis 20 ans, protège plus d'1,5M d'européens face aux risques liés au numérique. Elle conçoit et développe des solutions innovantes et accessibles qui sécurisent les messageries contre les malwares, phishing, spearphishing et spams et sensibilisent et forment les collaborateurs face aux cyber risques avec des programmes de simulations automatisées.

PRODUITS & SERVICES

90 % des cyberattaques passent par l'email et dans 9 cas sur 10 elles aboutissent suite à une manipulation humaine. Mailinblack conçoit et développe deux solutions indépendantes, basées sur intelligence artificielle et sciences cognitives, qui protègent les organisations des risques d'attaque par email et sensibilisent et forment les collaborateurs avec une approche pédagogique innovante.
La solution Protect protège les messageries professionnelles contre toutes formes d'attaques (malware, phishing, spearphishing…) : elle trie les emails non désirés (newsletters, spams) et neutralise les emails malveillants grâce à ses technologies propriétaires couplées à de l'intelligence artificielle.
La solution Cyber Coach entraîne les collaborateurs à faire face aux cyberattaques.
Elle permet d'évaluer le niveau de vulnérabilité humaine au sein de son organisation via un audit, de sensibiliser ses équipes en les mettant en situation avec des simulations d'attaques de phishing et de ransomware. Et enfin de les former efficacement avec des contenus ludiques et adaptés, partagés au bon moment.

MAKE IT SAFE

Make IT Safe
https://www.makeitsafe.fr/
+33 (0)9 72 11 71 86
contact@makeitsafe.fr

C.A.I.H.

UGAP

1 PARCOURS FONDATION
- Identification des partenaires
- Sensibilisation
- Audit organisationnel de sécurité
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Identification des partenaires
- Politique SSI
- Approche Security-by-design
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Sensibilisation et formation

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Politique SSI
- Indicateurs SSI
- Cartographie des données du SI

Créé en 2018, Make IT Safe est le logiciel métier français, commun entre le RSSI et le DPO, souhaitant maîtriser le risque et garantir leur conformité Cyber & RGPD.
Make IT Safe, c'est une équipe d'experts et passionnés, tous basés en France.

Notre logiciel est 100% développée et hébergée en France.
C'est aujourd'hui + de 100 clients équipés et satisfaits. Ils ont fait le choix de Make IT Safe car c'est la solution la plus simple, complète et collaborative.

PRODUITS & SERVICES

Dans un outil unique, évaluez et pilotez la gouvernance et conformité Cyber & RGPD de votre écosystème (interne + externe) avec une approche multiréférentielle.
Ce que vous allez pouvoir faire, plus simplement :
- Suivre votre politique et vos indicateurs SSI dans un tableau de bord dynamique.
- Cartographier les données du SI.
- Piloter efficacement votre campagne d'évaluation et d'audit, simplifier la collecte d'informations, générer automatiquement vos rapports.
- Intégrer la Sécurité & Conformité dans vos Projets : impliquer les métiers, définir les phases clés et les critères à respecter.
- Gérez efficacement vos Risques et Incidents de Sécurité.
- Assurez votre conformité RGPD : Registre de traitement, gérer les demandes de droit, les violations.
- Consolidez et priorisez vos actions dans des projets collaboratifs.
- Sensibilisez et formez vos équipes en partageant les bonnes pratiques.
- Regrouper la documentations dans une GED sécurisée.

Enfin, automatisez les tâches chronophages, concentrez-vous sur votre métier et obtenez un gain de productivité en moyenne de 30 %.

Merox
https://merox.io/
+33 (0)9 80 80 26 26
contact@merox.io

1 PARCOURS FONDATION
- Protection de la messagerie
- Protection des services exposés sur Internet
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Cartographie de l'infrastructure du SI
- Gouvernance des Identités et des Accès
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Homologation des SI sensibles

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Politique SSI
- Cartographie des données du SI
- SOC

La société Merox est un éditeur de logiciel montpelliérain, spécialisé dans la sécurité des DNS et des technologies s'y rapportant, tels que les emails. Son objectif est d'améliorer la sécurité de l'identité des entreprises en proposant un outil complet, simple et clef en main à travers un réseau de partenaires de confiance, certifiés, garantissant un accompagnement de haut niveau et une proximité. Les logiciels sont développés en interne par une équipe experte en DevSecOps.

PRODUITS & SERVICES

Merox est une plateforme SaaS modulaire de surveillance et pilotage de la cybersécurité orienté protection des DNS, de la marque et de la messagerie. Les différents modules permettent de gérer et monitorer au quotidien plusieurs aspects techniques spécifiques :
- Cartographie et maîtrise de l'environnement DNS complet.
- Surveillance et vérification des entrées DNS.
- Surveillance des emails : contrôlez la conformité de vos emails par l'adoption des protocoles tels que SPF, DKIM, DMARC et BIMI.
- Toolbox complète : Testeur DNS & Blacklist, validateur de syntaxe, analyse d'en-tête de message, etc.
- Alertes sécurités : soyez informés des attaques potentielles ou des changements non désirés sur vos domaines.
- Surveillance des domaines proches : générez des listes de surveillances pour vous protéger du typosquatting.

L'accompagnement par nos partenaires vous apportera les bénéfices suivants :
- Maîtriser l'ensemble de votre environnement DNS
- Empêcher l'usurpation d'identité.
- Réduire le phishing.
- Protéger votre marque.
- Augmenter votre délivrabilité email…

METSYS
https://www.metsys.fr/
+33 (0)1 81 89 19 70
contact@metsys.fr

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Gestion des comptes à privilèges
- Authentification et contrôle d'accès
- Gestion des mises à jour des serveurs et applications

2 PARCOURS INTERMÉDIAIRE
- Gestion du cycle de vie des utilisateurs et des habilitations
- Gestion des mises à jour de sécurité
- Endpoint security
- Sécurisation des services Cloud (IaaS/PaaS)

3 PARCOURS AVANCÉ

4 PARCOURS RENFORCÉ
- Revue d'habilitations
- Sécurité des équipements mobiles
- SIEM
- SOC

Intégrateur de solutions de Cybersécurité, d'infrastructure et de Cloud, Metsys délivre une offre globale de services : Conseil & Gouvernance, Analyse, Intégration, Services Managés SOC/ Micro SOC/CERT/GRC as a Service, Formation. Metsys compte environ 500 collaborateurs répartis sur 10 agences en France et a réalisé en 2022 un chiffre d'affaires de 67,2M€.

PRODUITS & SERVICES

Metsys propose des services et solutions afin d'anticiper les risques et de mettre en place une gouvernance solide sur les différents points d'entrées des cyberattaques : Identité – Endpoint – Data – Réseau – Applications – Outils collaboratifs.

Nos missions :
1/ **Prévention & Détection :** Identification des risques potentiels (Analyse de risques et d'architecture, de configuration, d'investigation et Forensic - Test d'intrusion - Sensibilisation utilisateurs) et Collecte, analyse via le Centre Opérationnel de Sécurité (SOC).
2/ **Sécurisation du SI** (Conseil, implémentation et accompagnement).
3/ **Intervention & Remédiation** (Fourniture et déploiement des solutions, mise en place des processus de gestion de réponse aux incidents et gestion de crise avec un réseau d'experts mobilisables ainsi qu'un centre de services en extension pour les opérations récurrentes).
4/ **Supervision & Gouvernance** (Définition et pilotage de la stratégie de sécurité – Déploiement de la gouvernance sécurité – Suivi de l'activité en temps réel via un accompagnement récurrent (services managés)).

MOABI

MOABI Solutions
https://moabi.com/
nicolas.gaume@moabi.com

1 PARCOURS FONDATION
- Scans de vulnérabilité du SI exposé sur Internet
- Audit organisationnel de sécurité

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Sécurité applicative

3 PARCOURS AVANCÉ
- Audit, scan, revue de code

4 PARCOURS RENFORCÉ
- Audit, scan, revue de code
- Scans de vulnérabilité en continu

Sécuriser le système d'information d'une entreprise suppose de fiabiliser les différents dispositifs qui le constituent, de manière à permettre la meilleure disponibilité, intégrité, confidentialité et traçabilité des données.

Pour autant, le nombre de cyberattaques ne cesse d'augmenter. Un nombre important de ces dernières utilisent les faiblesses des programmes. Ainsi, il est primordial de s'assurer en continu de la sécurité des applications et des logiciels.

PRODUITS & SERVICES

MOABI développe et commercialise de nouvelles solutions et méthodes pour la gouvernance de la sécurité produit pour tout type de logiciel et pour les objets connectés (IoT).

La plateforme MOABI fournit des outils et des méthodes pour évaluer et améliorer la sécurité des logiciels. MOABI propose ainsi des audits sécurisés et automatisés. À partir d'un moteur d'analyses et de tests à la pointe de la recherche en cybersécurité, 7 métriques sont étudiées pour déterminer les faiblesses des binaires des logiciels. MOABI indique également les actions de remédiation à effectuer. Le gestion et le suivi de ces actions peut se faire au sein même de MOABI, ou au sein d'une application tierce (comme Jira).

Moabi automatise l'analyse et le test rapide de milliers de binaires qui composent un logiciel : MOABI n'effectue pas qu'un simple échantillonnage, il analyse le code dans son intégralité. MOABI s'appuie sur une technologie de rétroconception (reverse engineering) afin d'effectuer des analyses sans avoir besoin du code source.

nameshield Online Assets Security

NAMESHIELD
https://www.nameshield.com/
+33 (0)2 41 18 28 28
commercial@nameshield.net

1 PARCOURS FONDATION
- Sensibilisation
- Protection de la messagerie
- Protection des services exposés sur Internet
- Scans de vulnérabilité du SI exposé sur Internet

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation
- Chiffrement des données
- Filtrage réseau

3 PARCOURS AVANCÉ
- Sensibilisation et formation
- Protection DDOS

4 PARCOURS RENFORCÉ

Avec 30 ans d'expérience au service de ses clients, Nameshield garantit la haute disponibilité des services en ligne (site web, messagerie, etc.) d'une collectivité/administration et assure la défense contre les attaques sur le périmètre Internet.

Registrar français de référence en gestion et sécurisation de portefeuille de noms de domaine et services associés (SSL/registry lock/monitoring/audit/remédiation/DMARC etc.). Nameshield est certifiée ISO 27001 et intègre un CERT.

PRODUITS & SERVICES

Pour une collectivité ou un établissement de santé, une interruption de service est impensable. Devant l'augmentation des menaces, il est vital de se protéger des attaques et d'utiliser une solution DNS résiliente et fiable.

Avec la solution **DNS Premium**, labellisée France Cybersecurity, protégez vos services en ligne des attaques, évitez toute indisponibilité grâce à l'infrastructure DNS anycast et le filtre anti-DDoS. Bénéficiez également de potentialités d'optimisation avec le déploiement d'options pertinentes : DNSSEC /Failover /GeoIP.

Le **DNS Premium** répond à vos exigences et obligations de présence digitale et de sécurisation de vos données grâce à son cœur de réseau européen. Grâce à la solution **DNS Premium**, vous pouvez :
- Simplifier la gestion de vos configurations techniques et réduire vos coûts.
- Éviter les interruptions et garantir une continuité de service.
- Bénéficier d'un accompagnement et d'un service de proximité.
- Améliorer le temps de réponse de vos pages.
- Être en conformité avec les exigences normatives.
- Protéger contre le hijacking de données (spoofing).

NEOWAVE

NEOWAVE
https://neowave.fr
+33 (0)4 42 50 70 05
contact@neowave.fr

1 PARCOURS FONDATION

- Gestion centralisée des identités
- Protection de la messagerie
- Protection des services exposés sur Internet
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE

- Chiffrement des données
- Sécurisation du réseau
- Sécurisation des services Cloud (IaaS/PaaS)
- Contrôle d'accès physique

3 PARCOURS AVANCÉ

- Authentification forte
- Gestion des comptes à privilèges
- Chiffrement des postes de travail

4 PARCOURS RENFORCÉ

- SSO
- Sécurité des équipements mobiles

NEOWAVE est une entreprise innovante 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.

PRODUITS & SERVICES

NEOWAVE est une société française spécialisée dans l'authentification forte et les transactions sécurisées. Elle propose trois familles de produits :

- **Les solutions ID 2.0** (cartes à puce et tokens USB avec leur middleware) pour une protection maximale des accès aux données informatiques et en mobilité.
- **Les produits FIDO** (cartes à puce et tokens USB compatibles avec les standards FIDO U2F et FIDO2) pour une authentification forte sur le web et sur le Cloud.
- **Les lecteurs de cartes à puce** à contact et sans contact pour une intégration simple de multiples applications sécurisées dans un environnement bureautique.

Les produits de NEOWAVE combinent le haut niveau de sécurité offert par la carte à puce avec des technologies de stockage et de connectivités : USB, technologies sans contact RFID/NFC, Bluetooth Low Energy (BLE). Conçus et fabriqués en France, ils répondent aux exigences de sécurité des agences européennes.

NetExplorer

NetExplorer
https://www.netexplorer.fr/
+33 (0)5 61 61 20 10
contact@netexplorer.Fr

1 PARCOURS FONDATION

- Protection des services exposés sur Internet
- Gestion des comptes à privilèges
- Authentification et contrôle d'accès
- Sécurité des flux d'administration

2 PARCOURS INTERMÉDIAIRE

- Approche Security-by-design
- Chiffrement des données
- Gestion des comptes de service
- Restauration de l'activité / PRA

3 PARCOURS AVANCÉ

- Gestion des droits d'accès
- Plan de sauvegarde
- Plan de reprise d'activité
- Gestion des logs

4 PARCOURS RENFORCÉ

- Cartographie des données du SI
- Data loss prevention
- Plan de reprise d'activité
- Forensic et analyse des logs

NetExplorer est une société Toulousaine qui sécurise les données numériques de 1500 organisations Françaises dans un cloud souverain & certifié (ISO27001, ISO9001 et HDS) tout en leur donnant les moyens de les exploiter facilement et durablement.

Et par «exploiter» il s'agit de partager des fichiers de toute taille en toute sécurité, de collaborer efficacement où que l'on soit, d'éditer ou coéditer en ligne ou en local et de pouvoir valider & signer ses documents.

PRODUITS & SERVICES

La mission qui anime l'équipe de NetExplorer est de sécuriser les données numériques des organisations tout en leur donnant les moyens de les exploiter facilement et durablement.

En pratique, NetExplorer est la solution cloud souveraine qui protège les documents de plus de 1500 organisations publiques ou privées. Au-delà de leur stockage, la solution permet :

- D'éditer ou co-éditer ses documents en ligne ou en local,
- De collaborer efficacement avec tous les intervenants d'un projet, où que l'on soit,
- De partager simplement et de façon totalement sécurisée ses fichiers,
- De valider et/ou signer électroniquement des documents avec ses partenaires internes comme externes.

Conçue pour garantir le respect de la vie privée & protéger tout type de données, la solution NetExplorer est certifiée ISO 27001, ISO 9001 et HDS (Hébergeur de Données de Santé) et est conforme RGPD. NetExplorer est une alternative française à Microsoft Sharepoint / OneDrive, Dropbox, Wetransfer, Google, etc.

Olfeo

Olfeo
https://www.olfeo.com/fr/
+33 (0)1 78 09 68 07
contact@olfeo.com

1 PARCOURS FONDATION
- Sensibilisation
- Protection des accès réseau Wi-Fi
- Proxy

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation
- Filtrage réseau
- Sécurisation du réseau

3 PARCOURS AVANCÉ
- Sensibilisation et formation
- Filtrage de flux réseau

4 PARCOURS RENFORCÉ
- Sécurité des équipements mobiles

Olfeo est la plateforme de sécurité web qui protège votre SI des cyber-menaces. En utilisant sa technologie innovante «trust-centric», Olfeo s'assure que vos collaborateurs n'accèdent qu'à des sites dont la confiance est garantie. La technologie «trust-centric» est possible grâce à l'exhaustivité et la qualité de la base de donnée des domaines Olfeo contenant plus de 20 millions d'URLs et couvrant 99,5% des sites visités en France et Europe. Disponible dans le cloud souverain ou en on-premise, la solution Olfeo est facile et rapide à mettre en oeuvre. Elle s'accompagne d'un module d'apprentissage et de sensibilisation aux enjeux de la cyber-securité pour associer vos collaborateurs à votre stratégie de cyber-défense.

PRODUITS & SERVICES

Olfeo propose 2 solutions :
- Une solution on-premise qui s'installe dans l'infrastructure des clients.
- Une nouvelle plateforme de sécurité web 100 % en SaaS.

Elles sont une barrière de protection indispensable contre les attaques par ransomwares. Olfeo protège l'intégralité de ses clients avec 100 % de succès.
Ces solutions innovantes et disruptives allient :
- La sécurisation intégrale des accès web grâce à des innovations technologiques comme le «trust-centric» rendu possible grâce à une base de données d'URLs d'une qualité inégalée.
- La confidentialité des données garantie par un éditeur souverain.
- La formation des collaborateurs en les rendant acteurs de la politique de sécurité de l'entreprise.
- La protection juridique totale grâce à l'intégration des lois françaises & européennes (droit pénal, RGPD, etc.).

Nos solutions couvrent les fonctions de proxy, déchiffrement SSL, filtrage web, antivirus, nomadisme, portail public, e-learning à la cybersécurité, etc.

Olvid

Olvid
https://olvid.io
+33 (0)6 77 58 23 41
contact@olvid.io

1 PARCOURS FONDATION
- Protection de la messagerie
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Chiffrement des données
- Sécurité applicative

3 PARCOURS AVANCÉ
- Effacement des données
- Plan de reprise d'activité
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Sécurité des équipements mobiles
- Plan de reprise d'activité

Seule messagerie instantanée certifiée ANSSI, Olvid prouve mathématiquement l'impossibilité pour un tiers de prendre connaissance des informations. Un niveau de sécurité sans précédent, sans céder la moindre donnée à l'éditeur, en poursuivant vos communications même en cas d'attaque informatique.

PRODUITS & SERVICES

Les moyens de communication usuels (mails, messageries grand public et professionnelles...) font reposer leur sécurité sur des serveurs centralisés imposés auxquels vous êtes obligés de faire confiance.
Les risques sont multiples : possibilité de déchiffrer/modifier les échanges, manipulation des identités, exploitation des données personnelles, risque d'attaques informatiques et d'espionnage par les États. Avec Olvid, l'excellence des protocoles cryptographiques permet de prouver mathématiquement l'impossibilité pour un tiers de prendre connaissance des communications.

Olvid répond ainsi à l'ensemble des problématiques suivantes : maîtriser les identités numériques, protéger les données en respectant le RGPD, sécuriser les communications internes et avec l'extérieur, lutter contre le shadow IT, s'affranchir de solutions étrangères soumises à des lois extra territoriales, poursuivre les communications pendant une crise informatique, et proposer des outils simples à utiliser.

Plus besoin de se déplacer pour retrouver le niveau de sécurité d'une conversation physique à huis-clos.

on-x Groupe
https://www.on-x.com
+33 (0)1 40 99 14 14
contact.sec@on-x.com

1 PARCOURS FONDATION
- Sensibilisation
- Analyse des vulnérabilités
- Audit organisationnel de sécurité
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Analyse de risques
- Gestion des mises à jour de sécurité
- Gestion centralisées des appareils mobiles

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Homologation des SI sensibles
- Détection d'intrusion, EDR, IPS
- Tests d'intrusion

4 PARCOURS RENFORCÉ
- Sécurité des équipements mobiles
- Audit red team
- SIEM
- SOC

Pionnier de la cybersécurité, **on-x** Groupe est un cabinet de conseil français indépendant spécialisé depuis plus de 30 ans dans la transformation numérique. Nos équipes pluridisciplinaires en sécurité numérique, composées d'experts organisationnels, techniques et juridiques, vous accompagnent pour sécuriser vos systèmes et protéger vos données.

Le cabinet, de près de 200 consultants, est membre de la French Tech, certifié ISO 9001, qualifié PASSI et labellisé ExpertCyber.

PRODUITS & SERVICES

Nos offres phares du moment :
- Diagnostic cybersécurité 360° (collectivités, startups, PME, ETI, grands groupes).
- Parcours de cybersécurité ANSSI.
- Analyses de risque et accompagnement à l'homologation (RGS, PPST, NIS ...).
- Accompagnement à la certification ISO 27001.
- Diagnostic et mise en conformité RGPD, DPO externalisé.
- Audits de sécurité PASSI.
- Services managés de détection et de réponse aux menaces (MDR) avec le pilotage de solution d'EDR / XDR.

Oodrive
https://www.oodrive.com
+33 (0)1 46 22 07 00
accueil@oodrive.com

1 PARCOURS FONDATION
- Sensibilisation

2 PARCOURS INTERMÉDIAIRE
- Analyse de risques
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Gestion des logs

4 PARCOURS RENFORCÉ
- Politique SSI
- SOC

Oodrive est leader européen de la gestion des contenus sensibles. Chez Oodrive, nous donnons aux organisations qui possèdent des contenus sensibles les outils dont elles ont besoin pour collaborer rapidement. Notre suite d'applications fournit les meilleurs outils de collaboration tout en assurant les plus hauts niveaux de sécurité des données, afin que les équipes puissent sécuriser leurs contenus sensibles sans être ralenties dans leur travail.

PRODUITS & SERVICES

Oodrive offre une suite de collaboration intuitive, souveraine et sécurisée. Parmi ses solutions :
Oodrive Work est l'environnement de confiance pour tous les contenus sensibles. Il permet de créer, partager des documents et collaborer efficacement tout en garantissant les plus hauts niveaux de sécurité.
- Sécurité des données et du contenu : Oodrive Work facilite la gestion et la surveillance de l'utilisation des contenus.
- Simplification du partage de documents : les utilisateurs peuvent facilement stocker, trouver et partager leurs fichiers en toute sécurité.
- Travail d'équipes et la collaboration fluide : les équipes peuvent visualiser, co-éditer, annoter et partager des fichiers.

Oodrive Meet permet d'organiser des réunions de direction efficaces grâce à des outils de planification et de visioconférence dans un environnement totalement sécurisé.
- Gestion facilitée de tous les aspects des réunions à distance : de la recherche de l'horaire jusqu'à la communication des comptes-rendus.
- Partage efficace des informations : Oodrive Meet rassemble les calendriers de travail.

OVERSOC

OverSOC
https://oversoc.com/
+33 (0)6 64 82 18 01
sales@oversoc.com

C.A.I.H. UGAP

1 PARCOURS FONDATION
- Analyse des vulnérabilités
- Inventaire des équipements
- Gestion des mises à jour des postes de travail
- Cartographie du réseau

2 PARCOURS INTERMÉDIAIRE
- Gestion des mises à jour de sécurité
- Sécurisation du réseau
- Sécurité applicative
- Cartographie de l'infrastructure du SI

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Indicateurs SSI
- Cartographie des données du SI

OverSOC propose une solution de gestion de la surface d'attaque des cyber-actifs à l'aide d'une cartographie 3D du système d'information. Sur la base d'un inventaire du parc informatique interne et/ou externe, OverSOC permet une visualisation intuitive des vulnérabilités et de la conformité technique des éléments du SI pour optimiser la prise de décision et les actions de protection des systèmes d'information.

PRODUITS & SERVICES

OverSOC propose une solution SaaS de cartographie de l'inventaire et des risques de cybersécurité du système d'information, représentés en 3D. Dans le cyber espace, la cartographie du SI a longtemps été perçue comme irréaliste. OverSOC la rend possible en proposant un medium commun de collaboration compréhensible, interactif, et mis à jour automatiquement. Dans un contexte cyber dans lequel :
- Il est difficile de recruter ;
- Le nombre d'attaques explose et ;
- Les entreprises sont fortement dépendantes des prestataires de services onéreux.

OverSOC est construit sur les travaux de l'ANSSI, d'EBIOS Risk Manager, et du NIST pour rassembler les parties prenantes de la cyber défense autour d'une vision commune et partagée pour :
- Construire une cartographie la plus exhaustive et à jour possible du SI (« on ne peut protéger que ce que l'on connait ») ;
- Comprendre en un instant la robustesse du SI et pouvoir en justifier ;
- Optimiser la défense en priorisant sereinement les actions des différentes équipes IT ;
- Gagner un temps précieux dans la gestion de crise.

Patrowl

Patrowl
https://patrowl.io
+33 (0)7 68 55 68 71
sales@patrowl.io

C.A.I.H. UGAP

1 PARCOURS FONDATION
- Protection des accès distants
- Analyse des vulnérabilités
- Scans de vulnérabilité du SI exposé sur Internet

2 PARCOURS INTERMÉDIAIRE
- Cartographie de l'infrastructure du SI
- Sécurisation des services Cloud (IaaS/PaaS)
- Scans de vulnérabilité sur tout le SI

3 PARCOURS AVANCÉ
- Audit, scan, revue de code
- Tests d'intrusion

4 PARCOURS RENFORCÉ
- Audit, scan, revue de code
- Audit red team
- Scans de vulnérabilité en continu

Patrowl est une solution de sécurité Offensive as a Service permettant de protéger votre Surface Exposée sur Internet.
Anticipez les menaces cyber en rendant vos organisations plus efficaces contre les attaquants.

Grâce à l'hyper-automatisation des contrôles de sécurité et des tests d'intrusions, Patrowl permet d'identifier, de connaître et de suivre la correction des risques cyber de manière simple et en permanence.

PRODUITS & SERVICES

La moitié des piratages provient d'un manque de maîtrise d'actifs informatiques exposés sur Internet. À l'instar des audits, Patrowl intervient très tôt dans la chaîne de sécurité, en découvrant problèmes (souvent nombreux), avant la concrétisation des incidents. Contrairement aux audits de sécurité, ponctuels, Patrowl assure une surveillance active, alerte et assiste en continu l'entreprise dans la remédiation. Patrowl est un portail simple d'utilisation mais ultra-performant, prêt à l'emploi, sans intégration longue ou complexe :
- (Re)découverte permanente des actifs exposés à Internet dont le Shadow IT (EASM).
- Identification continue de toutes vos faiblesses et vulnérabilités avec notre Pentest as-a-Service (PTaaS) et notre surveillance continue des cybermenaces.
- Remédiation facile avec priorisation et contextualisation.
- Contrôle de la remédiation avec retest en un clic.

Patrowl signe la fin du shadowIT dans l'entreprise, affranchit les équipes des tâches de sécurité les plus rébarbatives et contribue à une meilleure gouvernance de la donnée.

PRIMX
MAKE ENCRYPTION HAPPEN

PRIM'X
https://www.primx.eu/
+33 (0)1 40 95 24 80
business@primx.fr

C.A.I.H.

UGAP

1 PARCOURS FONDATION
- Protection de la messagerie
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Chiffrement des données
- End point security
- Sécurisation des services Cloud (IaaS/PaaS)

3 PARCOURS AVANCÉ
- Authentification forte
- Effacement des données
- Chiffrement des postes de travail

4 PARCOURS RENFORCÉ
- Data loss prevention

PRIM'X met son expertise du chiffrement au service de la protection des données des organisations. La confidentialité doit être dirigée par l'entreprise à 360° : une protection souveraine et de bout-en-bout. Pour protéger les données sensibles contre la perte, le vol, la publication et l'espionnage, PRIM'X introduit une nouvelle manière d'appliquer le chiffrement qui doit être GLOBAL, AUTOMATIQUE et TRANSPARENT et dirigé par une POLITIQUE DE SÉCURITÉ.

PRODUITS & SERVICES

ORIZON
ORIZON garantit la confidentialité des fichiers déposés dans le Cloud. Le chiffrement apporte cette protection à la source, depuis le terminal de l'utilisateur. Les données sont préservées des accès indésirés du fournisseur Cloud, de collaborateurs ou de personnes externes. Désormais compatible avec MS 365(Teams, OneDrive, Exchange...).

ZONECENTRAL
ZONECENTRAL utilise le chiffrement pour apporter un service de confidentialité applicable sur l'ensemble des fichiers d'une organisation. Il permet de gérer le droit d'en connaître et protège les données sensibles contre les accès externes et internes en cloisonnant les informations entre utilisateurs et services ainsi que vis-à-vis des opérateurs IT.

ZONEPOINT
Chiffrement de fichiers dans les bibliothèques SharePoint®.

ZED! and ZEDMAIL
Conteneurs chiffrés pour les échanges, l'archivage et les emails.

CRYHOD
CRYHOD, solution Certifiée de Full Disk Encryption (FDE), permet le chiffrement intégral des dispositifs de stockages physiques et virtuels pour protéger la mobilité, le télétravail et sécuriser le recyclage.

PRIZM

PRIZM
https://prizm-security.com/
contact@prizm-security.com

C.A.I.H.

UGAP

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Gestion des mots de passe
- Gestion des comptes à privilèges
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Gestion du cycle de vie des utilisateurs et des habilitations
- Gestion des comptes de service
- Gouvernance des Identités et des Accès

3 PARCOURS AVANCÉ
- Gestion des droits d'accès
- Revues d'habilitations
- Authentification forte
- Gestion des comptes à privilèges

4 PARCOURS RENFORCÉ
- Revue d'habilitations
- SSO

PRIZM est une société de conseil pure player de la gestion des identités et des accès. À travers une démarche d'accompagnement à la fois transverse et de proximité, PRIZM vous propose une offre de conseil qui ne se contente pas de renforcer l'excellence opérationnelle de vos projets, mais qui repositionne également la gestion des identités comme enjeu stratégique de votre transformation digitale.

PRODUITS & SERVICES

CONSULTING IAM / DIRECTION DE PROJETS
- Cadrage d'avant-projet, Conseil en stratégie IAM.
- Communication, Lobbying Managérial.
- Prise de poste régie : Direction de projet, Chefferie de projet, Architecture fonctionnelle ou technique, Product Owner.
- Animation projets, Appels d'offre.
- Conduite du changement et industrialisation.
- Expertise technique solutions.

Assessment maturité
- Revue globale de la stratégie de gestion des identités.
- Revue d'infrastructure, pratiques d'authentification, gestion des rôles et du cycle de vie des identités, gouvernance des accès.

INTÉGRATION SOLUTIONS
- Réponse à un appel d'offre avec un partenaire éditeur.
- Expertise et intégration de solutions de gestion des accès, gestion des identités, gouvernance des accès, ou solutions d'identité clients.

CONDUITE DE CHANGEMENT ET DÉVELOPPEMENT DE LA STRATÉGIE IAM
- Aide à la décision et sensibilisation des organisations à l'IAM pour faciliter et accélérer le déploiement de la stratégie IGA.
- Conférence, présentations et relations fortes avec les équipes RH et Cybersécurité.

ProHacKtive
CYBER SERENITY

ProHacKtive
https://prohacktive.io
+33 (0)7 83 88 18 61
bmz@prohacktive.io

1 PARCOURS FONDATION
- Analyse des vulnérabilités
- Inventaire des équipements
- Gestion des mises à jour des serveurs et applications
- Cartographie du réseau

2 PARCOURS INTERMÉDIAIRE
- Scans de vulnérabilité sur tout le SI
- Sécurisation du réseau
- Sécurité applicative
- Cartographie de l'infrastructure du SI

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Tests d'intrusion

4 PARCOURS RENFORCÉ
- Indicateurs SSI
- Cartographie des données du SI
- Audit red team
- Scans de vulnérabilité en continu

ProHacktive a pour mission de rendre la cybersécurité accessible à toutes les entreprises, et leur permettre de maîtriser leur risque cyber en permanence. Aujourd'hui les outils de protection (antivirus, firewalls) ne suffisent plus. Et les audits en cybersécurité sont ponctuels, destinés aux entreprises qui peuvent se le permettre techniquement et financièrement.

Notre promesse est de proposer un outil d'audit automatisé en cybersécurité préventive, installé en moins d'1 minute.

PRODUITS & SERVICES

ProHacktive permet de réaliser un audit permanent de vos risques cyber grâce à sa solution automatisée de détection et d'évaluation des vulnérabilités :
- **Sherlock**, Offre d'audit de cybersécurité permanent, automatique 24h24 7j7 ;
- **Sherlock Flash**, Offre d'audit ponctuel instantané et sans engagement ;
- **KB**, accès libre à la base de connaissance des CVE, multilingue ;
- **uPKI**, solution logicielle Open Source de gestion de certificats serveurs et clients.

Qontrol

QONTROL
https://www.qontrol.io/
+33 (0)6 08 77 83 60
ph@qontrol.io

1 PARCOURS FONDATION
- Sensibilisation
- Gestion des mots de passe
- Inventaire des équipements
- Audit organisationnel de sécurité

2 PARCOURS INTERMÉDIAIRE
- Politique SSI
- Approche Security-by-design
- Gouvernance des Identités et des Accès
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Chiffrement des postes de travail
- Plan de sauvegarde
- Tests d'intrusion
- Gestion de crise cyber

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Indicateurs SSI
- Cartographie des données du SI
- Plan de reprise d'activité

Qontrol est une plateforme de pilotage de la fonction cybersécurité pour petites structures (PME, Startups, organisations publiques) à destination des dirigeants et de leurs équipes. Nous permettons de définir, déployer et suivre une politique de cybersécurité adaptée, en recommandant des outils, des configurations et des process facilités par la plateforme. Notre passeport cyber permettra d'exposer votre posture de sécurité numérique à vos partenaires.

PRODUITS & SERVICES

Qontrol est une plateforme SaaS de pilotage de la fonction cybersécurité pour petites structures (PME, Startups, organisations publiques) à destination des dirigeants et de leurs équipes. Nous permettons de définir, déployer et suivre une politique de cybersécurité adaptée, en recommandant des outils, des configurations et des process facilités par la plateforme.
Nous engageons l'ensemble des collaborateurs sur la plateforme afin de comprendre leurs enjeux et de les accompagner dans le suivi de leur sécurité numérique.

À la suite d'un diagnostic initial interne, la plateforme organise un plan d'actions. Il est composé de différents chantiers cadencés sur plusieurs mois pour atteindre une maturité adaptée à son environnement.

Qontrol joue le rôle de responsable cybersécurité en organisant cette nouvelle fonction support.

L'objectif est d'accroitre la maturité numérique des organisations suivies et d'être capable de prouver sa bonne posture de sécurité à son environnement.

retarus:

Retarus
https://www.retarus.com/fr/
+33 (0)6 17 29 85 88
info@retarus.fr

C.A.I.H. UGAP

1 PARCOURS FONDATION
- Protection de la messagerie
- Protection des services exposés sur Internet
- Dispositif de sauvegarde

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- End point security
- Filtrage réseau
- Sécurisation des services Cloud (IaaS/PaaS)

3 PARCOURS AVANCÉ
- Plan de sauvegarde
- Plan de reprise d'activité
- Filtrage de flux réseau
- Protection DDOS

4 PARCOURS RENFORCÉ
- Data loss prevention
- Plan de reprise d'activité

Retarus est un éditeur de solutions cloud européen, créé en 1992.
Nos solutions sont opérées en cloud privé régionalisé et nos processus certifiés conformes au RGPD.

Notre but: cloudifier, sécuriser et industrialiser toutes les communications et échanges d'informations de nos clients (Messagerie utilisateurs et flux applicatifs).

PRODUITS & SERVICES

Retarus propose des services cloud de sécurisation et d'industrialisation des communications et échanges d'informations, hébergés en Cloud Privé européen et 100 % conformes au RGPD.
Communications Transactionnelles : Prise en charge des échanges de données transactionnels entrants/sortants et multi canal : Mail/SMS/Fax/EDI.
Envois transactionnels et marketing
- **Email :** Protéger la réputation des domaines émetteurs, éviter les blacklistages, assurer la haute délivrabilité, sécuriser les envois et réceptions, retours d'informations intégrés aux applicatifs.
- **SMS :** Haute délivrabilité, routes premium, 2ways SMS.
- **Fax :** Cloud fax applicatif.

Echanges machine to machine
- **Cloud EDI :** Connexion API unique pour conversion aux formats partenaires.
- **Webconnect :** EDI basé sur le protocole Email pour vos petits partenaires.
- **E-Invoicing :** Routage des flux de facturation et déclarations aux autorités fiscales européennes.
- **ICS :** Reconnaissance de caractères, extraction et intégration de données.

Emails Bureautiques
- **Protection de la Messagerie** pour tous types d'infrastructures.
- **Continuité et résilience de la Messagerie** en cas de crise cyber ou IT.

Ryder&Davis

Ryder & Davis
https://www.ryder-and-davis.com/
+33 (0)9 75 86 20 71
contact@ryder-and-davis.com

C.A.I.H. UGAP

1 PARCOURS FONDATION

2 PARCOURS INTERMÉDIAIRE

3 PARCOURS AVANCÉ

4 PARCOURS RENFORCÉ

Ryder & Davis est une banque d'affaires indépendante fondée par des entrepreneurs pour les entrepreneurs. Depuis 2013, nous avons réalisé plus de 60 opérations de M&A pour un volume d'affaires de 700 millions d'euros.

La société se différencie par son ADN entrepreneurial et ses expertises verticales, en particulier en cybersécurité, où nous avons gagné la confiance de clients référents du secteur tels que CEIS, Yogosha et Egerie.

PRODUITS & SERVICES

Nous proposons des services de conseil en fusions, cessions, acquisitions et levées de fonds :
M&A Sell-side, M&A Buy-Side, Leverage buy-out, levées de fonds Seed, Series A, Series B, Growth.

M&A sell-side:
Nous concevons et mettons en œuvre les meilleures stratégies pour votre sortie. En tant qu'anciens entrepreneurs, nous savons comment trouver le partenaire idéal pour construire le meilleur projet aux meilleures conditions.

M&A buy-side:
Nous sommes constamment à la recherche d'opportunités de croissance externe innovantes et structurantes pour nos clients.
Levées de fonds et Leverage buy-out :
Nous aidons les entrepreneurs à lever des fonds auprès des investisseurs les plus pertinents selon leur profil et leur industrie. Travaillant exclusivement pour les entrepreneurs, nous bénéficions d'une indépendance parfaite vis à vis des fonds, mise au service de nos clients.

SATELLIZ
https://www.satelliz.com
+33 (0)1 30 15 78 24
contact@satelliz.com

1 PARCOURS FONDATION
- Sécurité des flux d'administration
- Gestion des mises à jour des serveurs et applications
- Dispositif de sauvegarde
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Sécurisation des services Cloud (IaaS/PaaS)
- Restauration de l'activité / PRA
- Gestion des logs
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Principe du moindre privilège pour les administrateurs
- Plan de sauvegarde
- Plan de reprise d'activité
- Gestion des logs

4 PARCOURS RENFORCÉ

Depuis 2010, SATELLIZ propose des services managés 24/7 afin d'accompagner les entreprises dans le maintien en condition opérationnelle de leur plate-forme Cloud & Kubernetes. Les solutions de SATELLIZ - compatibles SecNumCloud, HDS, ... - font face aux enjeux de disponibilité, de sécurité et de souveraineté. SATELLIZ est une société française indépendante, agnostique, partenaire notamment des acteurs français 3DS Outscale, OVHcloud, Scaleway.

PRODUITS & SERVICES

En s'appuyant sur l'expertise et les services managés 24/7 de SATELLIZ, les équipes informatiques et devops n'ont plus à se soucier des imprévus en 24/7 et de la gestion au quotidien de leur plate-forme Cloud & Kubernetes, où qu'elle soit hébergée.

Les solutions de SATELLIZ sont clef en main et incluent des services 24/7 de gestion d'incidents et d'administration d'une part, et tous les outils logiciels d'exploitation nécessaires d'autre part : suite logicielle de supervision développée par SATELLIZ, PaaS GitOps, PaaS ELK, ...

Les solutions de SATELLIZ sont proposées sous forme d'abonnement forfaitaire (sans variable) et s'installent en quelques semaines.

Parmi nos solutions de maintien en condition opérationnelle pour plates-formes Cloud & Kubernetes :
– Supervision & Gestion d'incidents 24/7
– Co-Administration en mode GitOps de plates-formes Kubernetes
– Administration Multi-Cloud
– Administration en environnement qualifié SecNumCloud, HDS, ...
– ...

SCALAIR
https://scalair.fr/
+33 (0)3 20 68 21 21
dvignault@scalair.fr

1 PARCOURS FONDATION
- Protection de la messagerie
- Firewall
- Gestion des comptes à privilèges
- Dispositif de sauvegarde

2 PARCOURS INTERMÉDIAIRE
- Gestion des mises à jour de sécurité
- End point security
- Sécurisation des services Cloud (IaaS/PaaS)
- Restauration de l'activité / PRA

3 PARCOURS AVANCÉ
- Détection d'intrusion, EDR, IPS
- Plan de sauvegarde
- Plan de reprise d'activité
- Gestion des logs

4 PARCOURS RENFORCÉ
- IPS ; EDR
- Plan de reprise d'activité
- SIEM
- SOC

Scalair est une entreprise 100 % Française, spécialisée dans le déploiement et le management d'infrastructures Cloud Sécurisées.
Scalair propose une offre de Cloud souverain hébergé en France et des services managés de Cyber Sécurité (E.DR, P.A.M, Etc). Du conseil en architecture jusqu'à la gouvernance complète de leurs plateformes, Scalair conçoit des offres sur-mesure et sans engagement de durée pour ses clients.

PRODUITS & SERVICES

SCALAIR propose une offre de Cloud souverain hébergé en France et des services managés de Cyber Sécurité.
NOS SERVICES
- Protection des infrastructures via le Cloud SCALAIR 100 % Souverain.
- Protection des infrastructures Cloud HyperScaler comme Microsoft Azure via la surveillance des configurations par les experts SCALAIR.
- Protection des environnements Microsoft 365 via des services managés d'anti-phishing et de sauvegarde.
- Protection des postes de travail via un service managé E.D.R (EndPoint Detection & Response) certifié par l'ANSSI.
- Protection des administrateurs via une plateforme P.A.M (Privileged Access Management) pour vos partenaires applicatifs.
- Protection réseau via la mise à disposition et la gestion de firewall certifiés par l'ANSSI.
- Surveillance et management de vos sauvegardes et de votre plan de reprise d'activité (P.R.A). Via l'équipe des Customer Success Manager SCALAIR, nos clients bénéficient d'un accompagnement très fort et personnalisé.

Toutes nos offres sont sans engagement de durée !

SECLAB
https://www.seclab-security.com
contact@seclab-security.com

1 PARCOURS FONDATION
- Gestion des mots de passe
- Filtrage Réseau
- Sécurité des flux d'administration
- Gestion des mises à jour des serveurs et applications

2 PARCOURS INTERMÉDIAIRE
- Coffres-forts de mots de passe
- Sécurisation du réseau
- End point security
- Filtrage réseau

3 PARCOURS AVANCÉ
- Filtrage de flux réseau

4 PARCOURS RENFORCÉ
- Data loss prevention

SECLAB développe des solutions renforcées par des technologies électroniques brevetées et cerfifiées par l'ANSSI permettant de :
- sécuriser les échanges de données (fichiers, flux applicatifs) entre deux réseaux
- sécuriser l'usage des clés USB en environnements sensibles
- sécuriser la gestion des mots de passe en mode déconnecté

Basée à Montpellier, Seclab possède des références significatives dans les secteurs du Transport, de l'Énergie, de la Défense.

PRODUITS & SERVICES

Secure Xchange Network :
La passerelle réseau « Secure Xchange Network », se positionne en coupure entre deux réseaux de sensibilité différente et permet de transférer des données entre des deux réseaux de façon sécurisée et maîtrisée grâce :
- à la rupture protocolaire par l'électronique (technologie brevetée Seclab),
- au filtrage configuré selon vos règles de sécurité.

Cette passerelle est complémentaire des firewalls existants pour renforcer la sécurité des échanges.

Secure Xchange USB :
Le produit « Secure Xchange USB » permet de connecter une clé USB à un poste sensible tout en l'isolant strictement de la clé USB : seuls les fichiers conformes à la politique de filtrage apparaissent sur le poste. Il peut être complémentaire des stations d'analyses antimalware de clés USB pour garantir un usage sécurisé de bout en bout des clés USB

Pocket Pass :
Le Produit Pocket Pass permet la gestion hors ligne de codes et de mots de passe ainsi que leur changement régulier sans risque de perte d'exploitation.

SEELA
https://www.seela.io/
hello@seela.io

1 PARCOURS FONDATION
- Sensibilisation
- Analyse des vulnérabilités
- Firewall
- Audit organisationnel de sécurité

2 PARCOURS INTERMÉDIAIRE

3 PARCOURS AVANCÉ
- Sensibilisation et formation

4 PARCOURS RENFORCÉ

Accréditée organisme de formation, Seela est une société spécialisée dans le cyber entraînement. Plateforme d'e-learning en CyberSécurité basant ses parcours de formation sur l'accompagnement et la simulation grâce à la CyberRange d'Airbus Cybersecurity. Notre mission est de faire passer les compétences de vos collaborateurs au niveau supérieur en leur donnant accès au seul environnement pratique représentatif de vos applications et de votre SI.

PRODUITS & SERVICES

Seela est une plateforme proposant une solution d'E-learning et de Cyber Entrainement.
Dans un environnement professionnel (et personnel) hyperconnecté, la cybersécurité est au cœur de la stratégie des entreprises ou des organismes publics qui se doivent de définir des objectifs de sécurité, des règles d'optimisation des risques d'attaques et des méthodes de protection de leur SI, en s'appuyant sur des personnes spécialement formées sur ce domaine.
L'offre Seela répond à plusieurs besoins du marché, en effet :
- elle répond à cette nécessité croissante d'expertise en Cybersécurité face au développement constant des nouvelles menaces,
- face à la difficulté à recruter des experts en Cyber, la meilleure solution pour les organismes, reste la formation régulière et l'Upskill de leurs équipes IT.

Seela, basée sur la dualité « Théorie/Pratique » apporte les compétences, les connaissances nécessaires pour identifier les sources et les raisons des attaques, pour mettre en place des mesures de prévention et pour analyser et gérer rapidement les menaces.
Seela et l'enjeu de la simulation.

SEKOIA.IO
https://www.sekoia.io/
contact@sekoia.io

1 PARCOURS FONDATION
- Protection des accès distants
- Protection des services exposés sur Internet
- Sécurité des flux d'administration
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Sécurisation du réseau
- Sécurisation des services Cloud (IaaS/PaaS)
- Gestion des logs
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Détection d'intrusion, EDR, IPS
- Gestion des logs

4 PARCOURS RENFORCÉ
- IPS; EDR
- Forensic et analyse des logs
- SIEM
- SOC

SEKOIA.IO est la plateforme de cybersécurité opérationnelle qui neutralise les menaces cyber avant impact. Pour fédérer les systèmes de sécurité et optimiser leurs ressources, SEKOIA.IO assure la détection et réponse étendues pilotées par le renseignement et propose une cybersécurité plus simple, plus intelligente, et plus collaborative.

PRODUITS & SERVICES

La plateforme SOC SEKOIA.IO XDR allie l'anticipation, via la connaissance des attaquants, aux capacités d'automatisation pour la détection et la réaction face aux attaques.

SEKOIA.IO XDR permet de détecter et de répondre aux incidents de sécurité en tirant profit des solutions de sécurité existantes. La réponse aux menaces détectées est possible grâce aux fonctionnalités d'orchestration (ou SOAR) nativement intégrées.

SEKOIA.IO CTI permet d'avoir une maîtrise et une connaissance détaillée des groupes d'attaquants. Sa base de données structurée et contextualisée est continuellement mise à jour et enrichie au quotidien par les travaux menés par l'équipe de recherche de SEKOIA.IO afin de rendre le renseignement produit exploitable.

SEKOIA.IO TIP est une plateforme de renseignement sur les menaces qui permet une gestion centralisée, structurée et automatisée des données de CTI. Cette solution s'adresse aux équipes opérationnelles qui souhaitent collecter du renseignement cyber, le capitaliser de façon structurée et le disséminer finement de façon automatique.

Smart Global Governance
https://www.smartglovernance.com
+33 (0)4 22 13 57 55
hello@smartglobal.com

1 PARCOURS FONDATION
- Scans de vulnérabilité du SI exposé sur Internet
- Audit organisationnel de sécurité
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE

3 PARCOURS AVANCÉ
- Plan de reprise d'activité
- Tests d'intrusion
- Gestion des logs
- Gestion de crise cyber

4 PARCOURS RENFORCÉ

Smart Global Governance offre une solution SaaS primée pour gérer efficacement vos obligations de conformité et de gestion des risques. Plus de 170 normes et réglementations activables et 10 modules pour prendre des décisions en temps réel. Conçue pour PME et entreprises internationales, notre solution automatise les processus pour vous offrir la confiance nécessaire. Bénéficiez d'une interface ergonomique, d'un support client réactif et d'un réseau mondial d'intégrateurs.

PRODUITS & SERVICES

Smart Global Governance est une solution SaaS qui vous aide à gérer toutes vos conformités et vos risques en toute simplicité.

Avec plus de 170 normes et règlementations activables progressivement, cette solution est préconfigurée pour cibler votre secteur d'activité, la taille de votre organisation et vos objectifs. Elle comporte 10 modules qui couvrent des domaines tels que la Privacy & Data, la Sécurité IT, RSE, Qualité, Risque Tiers, l'Ethique, etc. Vous pourrez gérer vos obligations en temps réel grâce aux tableaux de bord actualisés et aux outils de mise en œuvre accessibles aux employés et aux tiers.

Avec Smart Global Governance, vous pourrez automatiser facilement les processus et prendre des décisions en toute confiance grâce à l'intégration de toutes vos parties prenantes et au partage des informations en temps réel.
Plus de 300 000 utilisateurs font déjà confiance à cette solution facile d'accès et ergonomique. Le support client est également réactif et facile à contacter.

Snowpack

Snowpack
https://snowpack.eu
+33(0)1 69 08 05 47
contact@snowpack.eu

1 PARCOURS FONDATION
- Protection des services exposés sur Internet
- Filtrage Réseau
- VPN
- Sécurité des flux d'administration

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Sécurisation du réseau
- End point security

3 PARCOURS AVANCÉ
- Filtrage de flux réseau

4 PARCOURS RENFORCÉ
- Sécurité des équipements mobiles

Snowpack, jeune spin-off du CEA créée en 2021, développe et opère SNO, premier réseau overlay d'invisibilité. Mariant anonymat et sécurité, SNO transforme la cybersécurité réseau : anonymat sans tiers de confiance, garanties de qualité de sécurité, obfuscation de la surface d'attaque, impossibilité des attaques man in-the-middle. Véritable couche d'indépendance entre l'infrastructure et les données, SNO protège les utilisateurs des vulnérabilités sur la chaîne de confiance.

PRODUITS & SERVICES

Sur la base de son réseau overlay d'invisibilité SNO, Snowpack propose deux produits :
- **VIPN (Virtual & Invisible Private Network) :** une suite complète de connecteurs à SNO permettant de bénéficier directement des propriétés d'anonymat et/ou d'invisibilité réseau pour des usages variés : sécurisation de la navigation, tests de pénétration, investigations et recueils de renseignements sur les réseaux (clearnet, deepweb et darknet), complément de sécurisation de l'infrastructure contre les menaces non-couvertes par les VPN classiques (flux non identifiable, redondance intrinsèque, split-tunneling facilité, obfuscation du serveur) ;
- **« Secured by Snowpack » :** une API permettant l'intégration simple des connecteurs SNO dans des applications et services afin qu'elles bénéficient de ses propriétés d'invisibilité. Cette API permet l'invisibilité de communications point-à-point (pour de la navigation sécurisée, la sécurisation de l'accès cloud, un serveur VPN caché) et point-à-multipoints (pour les visioconférences, le partage d'informations sensibles, le stockage cloud).

Suricate

Suricate
https://www.suricate.pm/
+33 (0)1 74 903 900
contact@suricate.pm

1 PARCOURS FONDATION
- Gestion des mises à jour des postes de travail
- Gestion des mises à jour des serveurs et applications

2 PARCOURS INTERMÉDIAIRE
- Gestion des mises à jour de sécurité
- End point security

3 PARCOURS AVANCÉ
- Homologation des SI sensibles

4 PARCOURS RENFORCÉ
- Homologation des SI sensibles

Suricate est le spécialiste français du Patch Management en service managé. Créé en 2017 au sein du groupe informatique RAS, le service de Patch Management est devenu Suricate en 2020. Installé à Caen et Paris, Suricate a une approche intégrale du Patch Management, géré en globalité, en toute transparence et avec engagement sur les métriques. Nos clients vont de l'industrie aux sociétés de services, en passant par le secteur public.

PRODUITS & SERVICES

Le Patch Management avec Suricate, c'est :
- Equipe dédiée en 24/7 avec une méthodologie et des process éprouvés.
- Outils IT uniques pour un pilotage performant et un reporting engageant.
- Alertes CVE / CERT-FR, gestion de crise et process accéléré de validation.
- Garantie des meilleures pratiques via la certification « ISO 27001:2013 ».
- Conformité avec, chaque mois, délivrance d'un rapport détaillé de l'état du parc.
- Souveraineté, implanté à Caen et Paris, Suricate ne fait aucune externalisation.
- Gestion du air-gap, Suricate intègre la gestion des machines non connectées.
- Plus de 500 applications sous distributions Microsoft et Linux.
- Intégration possible des applicatifs métiers via process spécifique.

Suricate est la garantie d'une infrastructure IT à jour.

synetis

SYNETIS
https://www.synetis.com
+33 (0)1 47 64 48 66
contact@synetis.com

1 PARCOURS FONDATION
- Analyse des vulnérabilités
- Authentification et contrôle d'accès
- Gestion centralisée des identités
- Protection des accès distant

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- End point security
- Gestion des incidents sécurité
- Politique SSI

3 PARCOURS AVANCÉ
- Détection d'intrusion EDR, IPS
- Gestion des comptes à privilèges
- Gestion des logs
- Tests d'intrusion

4 PARCOURS RENFORCÉ
- Audit red team
- Forensic et analyse des logs
- SIEM
- SOC

Créé en 2010, Synetis est, aujourd'hui, leader des cabinets de conseil 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.

PRODUITS & SERVICES

Synetis a développé une approche globale répondant aux nouvelles problématiques, proposant donc une large gamme de services et solutions, compétences organisationnelles et expertises techniques – et intervenant aujourd'hui sur :

- **L'AUDIT DE SÉCURITÉ :** connaître son niveau de risque face aux cybermenaces ;
- **LE CERT – RÉPONSE À INCIDENT :** prévenir, anticiper les menaces et réagir en cas d'incident ;
- **LA GRC (GOUVERNANCE, RISQUES, CONFORMITÉ) :** organiser et piloter sa cybersécurité (définition des exigences, identification des axes d'amélioration, analyse de la valeur des actifs et des données, etc.) ;
- **L'IDENTITÉ NUMÉRIQUE :** maîtriser ses identités et ses accès ;
- **LA SÉCURITÉ OPÉRATIONNELLE :** déployer des solutions technologiques de protection des SI.

Synetis, organisme de formation agréé - certifié Qualiopi, propose également une large gamme de formations couvrant les différentes expertises cybersécurité – pour permettre à tous de s'adapter et rester performant face aux nouveaux enjeux cyber.

Tenacy

Tenacy
https://www.tenacy.io/
contact@tenacy.io

1 PARCOURS FONDATION
- Identification des partenaires

2 PARCOURS INTERMÉDIAIRE
- Identification des partenaires
- Politique SSI
- Analyse de risques

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Politique SSI
- Indicateurs SSI
- Cartographie des données du SI

Créee en 2019 à Lyon, Tenacy est le partenaire quotidien des équipes cybersécurité au service de la performance de l'entreprise. Notre mission est de simplifier et automatiser le management de la cybersécurité pour toutes les équipes cyber.

Pour cela nous développons et commercialisons une plateforme SaaS tout-en-un simple et structurante. Labellisée France Cybersecurity, Tenacy compte 30 collaborateurs, +de 100 clients et 2000 utilisateurs répartis dans 35 pays.

PRODUITS & SERVICES

Tenacy est la plateforme leader de gestion de la cybersécurité. Elle aligne en permanence la stratégie Cyber, les opérations et les performances tout en rassemblant les personnes, les processus et les données au même endroit pour atteindre les objectifs de sécurité. Avec Tenacy, vous bénéficiez d'une vision globale & consolidée pour piloter et agir avec réactivité et efficacité. La plateforme est «structurante» puisqu'elle propose également un framework en 3 étapes :

1) Définissez votre stratégie :
- Modélisez l'organisation et vos périmètres à sécuriser.
- Définissez vos risques.
- Sélectionnez vos référentiels applicables (ISO 27001, PSSI-E, HDS).
- Evaluez votre position.
- Lancez et maintenez votre programme de certification.

2) Pilotez vos opérations :
- Construisez vos plans d'action.
- Maintenez vos dispositifs opérationnels.
- Définissez vos plans de contrôle.
- Gérez vos incidents, dérogations & écarts.

3) Mesurez et partagez votre performance :
- Choisissez vos indicateurs.
- Créez vos tableaux de bord.
- Benchmarkez vos datas.
- Bénéficiez d'aide à la décision.

Tersedia

TERSEDIA
https://www.tersedia.fr/
+33 (0)1 34 80 72 92
marketing@tersedia.fr

1 PARCOURS FONDATION
- Protection des accès distants
- Analyse des vulnérabilités
- Protection de la messagerie
- Dispositif de sauvegarde

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- End point security
- Sécurisation des services Cloud (IaaS/PaaS)
- Sécurisation du réseau

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Détection d'intrusion, EDR, IPS
- Plan de reprise d'activité
- Gestion des logs

4 PARCOURS RENFORCÉ
- Revue d'habilitations
- SIEM
- Data loss prévention

PRODUITS & SERVICES

It-as-a-service :
Que vous choisissiez une infrastructure "on premise", dans notre cloud privé, dans un cloud public ou encore une solution hybride, toutes nos solutions informatiques sont sur mesure, supervisées et toujours sécurisées. Nous vous garantissons ainsi une flexibilité et une modularité totale pour toutes vos applications et tous vos types de déploiements, même en cas de panne, d'incident ou de piratage.
Infra Secured by design :
Nous anticipons les vulnérabilités de sécurité dès la conception des infrastructures : authentification, autorisation, confidentialité, intégrité des données, confidentialité, responsabilité, disponibilité, sécurité et non-répudiation, même lorsque le système est attaqué. Le tout, à un coût accessible au plus grand nombre d'entreprises.

SOC next gén :
Notre Security Operations Center de dernière génération assure la supervision de la sécurité opérationnelle de vos infrastructures informatiques du endpoint aux datacenters pour gérer les risques cyber et améliorer la sécurité de vos actifs en continu.

THEGREENBOW

THEGREENBOW
https://www.thegreenbow.com/fr/
+33 (0)1 43 12 39 37
sales@thegreenbow.com

1 PARCOURS FONDATION
- Protection des accès distants
- VPN
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Chiffrement des données
- End point security

3 PARCOURS AVANCÉ
- Gestion des droits d'accès
- Authentification forte
- Homologation des SI sensibles
- Chiffrement des postes de travail

4 PARCOURS RENFORCÉ
- Sécurité des équipements mobiles

TheGreenBow est un éditeur de logiciels VPN de confiance. Nous aidons les organisations et les individus à devenir cyber-responsables. Pour cela, nous concevons et développons des solutions fiables et faciles d'utilisation.

Nous protégeons les accès et les connexions à votre SI et assurons l'intégrité et la confidentialité des données échangées en toutes circonstances : entre des organisations, des collaborateurs nomades, des télétravailleurs ou des objets connectés.

PRODUITS & SERVICES

Pour garantir la sécurité des échanges de données, un VPN assure trois fonctions :
- Authentification par clé pour vérifier que les équipements sont bien autorisés à communiquer ensemble.
- Chiffrement des données pour assurer la confidentialité des échanges.
- Intégrité des données pour garantir que les données ne subissent aucune altération.

Pour des besoins aussi variés que la protection de connexions en télétravail ou avec des objets connectés, ou encore la sécurisation de communications critiques, nous proposons la gamme de Clients VPN la plus fiable et la plus polyvalente du marché : interopérables avec toute passerelle VPN IPsec ou OpenVPN, fonctionnant sur tout type de réseau (WiFi, 4G/5G, Satellite, ...), conçus pour s'intégrer dans toute Infrastructure de Gestion de Clé (IGC / PKI) et pour être déployés à large échelle.

Nos clients VPN sont disponibles pour Windows, Linux, Android, iOS et macOS.

Tixeo
https://www.tixeo.com/
+33 (0)4 67 75 04 31
contact@tixeo.com

1 PARCOURS FONDATION
- Protection de la messagerie

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Chiffrement des données
- Gestion des mises à jour de sécurité

3 PARCOURS AVANCÉ
- Chiffrement des postes de travail

4 PARCOURS RENFORCÉ
- Sécurité des équipements mobiles

Tixeo conçoit des solutions innovantes de vidéocollaboration sécurisée permettant de se réunir depuis n'importe quel équipement et offrant des fonctions avancées de collaboration. Tixeo est disponible dans le Cloud ou On-Premise. La sécurité est prise en compte à tous les niveaux dès la conception (Secure by design). Tixeo possède de nombreuses références: Orange, AMF, Naval Group, Dassault Aviation, Nexter, MBDA... La technologie 100 % française Tixeo est certifiée qualifiée par l'ANSSI.

PRODUITS & SERVICES

Avec Tixeo les entreprises bénéficient d'un haut niveau de sécurité pour leur visioconférence. Toutes les offres Tixeo intègrent une large gamme de fonctionnalités de collaboration et garantissent la confidentialité des communications (vidéo, audio, data) quel que soit le nombre de participants (Certifiée/Qualifiée ANSSI).

TixeoCloud
La visioconférence Tixeo est disponible en mode cloud pour un déploiement ultra-rapide et sécurisé. L'hébergement des serveurs Tixeo se répartit en France métropolitaine selon une stratégie multi-cloud.

TixeoPrivateCloud
Avec l'offre de Cloud dédié, infogérée par Tixeo, les organisations disposent de leur propre serveur de visioconférence dans le cloud sans passer par de lourdes étapes de déploiement et les désagréments de maintenance.

TixeoServer
L'approche On-Premise de Tixeo permet de répondre aux exigences les plus strictes en matière d'intégration. En installant TixeoServer au cœur de leurs infrastructures, les organisations gardent une totale maîtrise de leur installation et bénéficient d'une sécurité optimale pour leurs visioconférences.

Tranquil IT
https://tranquil.it
+33 (0) 240 975 755
commercial-tis@tranquil.it

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Inventaire des équipements
- Gestion des mises à jour des postes de travail
- Gestion des mises à jour des serveurs et applications

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Gestion des mises à jour de sécurité
- End point security
- Gestion centralisée des appareils mobiles

3 PARCOURS AVANCÉ
- Sensibilisation et formation
- Gestion des droits d'accès
- Principe du moindre privilège pour les administrateurs
- Plan de reprise d'activité

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Sécurité des équipements mobiles
- Plan de reprise d'activité

Tranquil IT se spécialise dans 2 domaines :
- Éditeur du logiciel WAPT pour déployer et maintenir des systèmes d'exploitation, des logiciels et des configurations (équivalent à Microsoft SCCM, MDT, WSUS ou Intune).
- Principal intégrateur de Samba Active Directory en France et en Europe.

Notre vision chez Tranquil IT est d'assembler astucieusement ces deux technologies pour proposer un socle sur lequel (re)construire un SI sûr et sécurisé, on-premise ou dans le cloud.

PRODUITS & SERVICES

PRINCIPAUX AVANTAGES DE WAPT
Pour les administrateurs système :
- Installer des logiciels et des configurations en mode silencieux.
- Maintenir à jour une base installée de logiciels et de configurations.
- Configurer des logiciels en contexte système et utilisateur.
- Supprimer silencieusement des logiciels et des configurations en fin de vie.

Pour les responsables de la sécurité informatique :
- Piloter la base installée de logiciels pour converger vers un standard de sécurité.
- Ne plus tolérer que des machines fonctionnent en mode administrateur.
- Ne plus tolérer que les utilisateurs téléchargent et exécutent des logiciels depuis leur répertoire personnel.
- Implémenter les SRP (Applocker).
- Réduire son exposition aux vulnérabilités logicielles et aux attaques par mouvement latéral.
- Obtenir des indicateurs de conformité pour mieux connaître l'état de sécurité global du parc.
- Être prompt à réagir à des failles 0 day.

Pour les utilisateurs finaux :
- Avoir des logiciels configurés pour bien fonctionner.
- Avoir de l'autonomie pour installer des logiciels.

TrustBuilder

TrustBuilder
https://www.trustbuilder.com/
01 46 94 68 38
sales+hxt@trustbuilder.com

1 PARCOURS FONDATION
- Gestion centralisée des identités
- Protection des accès distants
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Gestion du cycle de vie des utilisateurs et des habilitations
- Sécurisation des services Cloud (IaaS/PaaS)
- Gouvernance des Identités et des Accès

3 PARCOURS AVANCÉ
- Gestion des droits d'accès
- Authentification forte

4 PARCOURS RENFORCÉ
- SSO

Acteur européen de l'IAM (Identity and Access Management), TrustBuilder offre une expérience client fluide et un haut niveau de sécurité tout au long du parcours numérique des consommateurs, employés, partenaires et machines. Notre solution SaaS de cybersécurité permet aux entreprises de conquérir de nouveaux marchés tout en réduisant leurs coûts.

PRODUITS & SERVICES

TrustBuilder propose un ensemble complet de briques pour sécuriser les environnements numériques.
Notre plateforme de gestion des identités et des accès (IAM) assure des interactions sécurisées pour les clients, les employés et les machines.
Les modules de notre framework IAM répondent à divers cas d'utilisation : Single Sign-on, Multi-Factor Authentication, Passwordless Authentication, Federated Identity, Identity Verification, Identity Provisioning, Know Your Customer, Persona Selection and Management, Delegated Administration, Progressive Profiling...
Nous facilitons la vie des administrateurs système en proposant un environnement low-code/no-code.

TrustHQ

Trust HQ
https://trusthq.com/
+33 (0)6 62 49 03 04
contact@trusthq.com

1 PARCOURS FONDATION
- Identification des partenaires
- Audit organisationnel de sécurité

2 PARCOURS INTERMÉDIAIRE
- Identification des partenaires

3 PARCOURS AVANCÉ
- Organisation et pilotage de la SSI
- Homologation des SI sensibles

4 PARCOURS RENFORCÉ
- Organisation et pilotage de la SSI
- Politique SSI
- Indicateurs SSI
- Homologation des SI sensibles

TrustHQ est une startup française, éditrice d'une solution SaaS de pilotage de la gouvernance cybersécurité.

TrustHQ est fondée en 2020 par un ancien RSSI, sur la base de 3 constats :

1/ Complexité des organisations face à la digitalisation.
2/ Croissance exponentielle des normes et référentiels de sécurité.
3/ Nécessité d'outiller la fonction RSSI face à la quantité d'information à traiter

PRODUITS & SERVICES

RSSI - Automatisez - Gouvernance 2.0
Les gains passent par la simplification et l'automatisation des missions du RSSI.

TrustHQ couvre tous les services :
- Audit des fournisseurs (TPRM).
- Audit internes (Questionnaires).
- Suivi des risques.
- Sécurité dans les projets (ISP).
- Indicateurs SSI (KPI).
- Conformité aux référentiels.
- Certification et Homologation SSI.

TrustHQ vous accompagne dans le maintien en Conditions de Sécurité (MCS) de votre organisation.

TrustHQ vous accompagne quel que soit votre référentiel de sécurité : ISO / HDS / NIS / NIST...

Dîtes "adieu" au travail manuel et aux Excels. Entrez dans une Gouvernance 2.0.

TRUST IN SOFT

TrustInSoft
https://trust-in-soft.com/
+33 (0)1 84 06 43 91
contact@trust-in-soft.com

1 PARCOURS FONDATION
- Analyse des vulnérabilités
- Protection des services exposés sur Internet

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Sécurité applicative

3 PARCOURS AVANCÉ
- Audit, scan, revue de code

4 PARCOURS RENFORCÉ
- Audit, scan, revue de code
- Audit red team

TrustInSoft commercialise des outils et services d'analyse exhaustive de code source C et C++ et bientôt Java 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.

PRODUITS & SERVICES

TrustInSoft Analyzer est un analyseur avancé de code source C et C++ qui garantit mathématiquement l'absence de défauts, l'immunité des composants logiciels aux failles de sécurité, et la conformité avec une spécification.

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.

L'élément différentiateur de **TrustInSoft Analyzer** est son appui sur des approches mathématiques, dites « méthodes formelles », qui permettent une analyse exhaustive pour trouver toutes les vulnérabilités ou erreurs de runtime et ne relever que des vraies alarmes.

Les experts de TrustInSoft peuvent également accompagner les clients pour des audits de code, et les assister en matière de formation, de support et de services supplémentaires.

UBIKA

Ubika
https: //www.ubikasec.com
+33 (0)1 46 20 96 00
info@ubikasec.com

1 PARCOURS FONDATION
- Protection de la messagerie
- Protection des services exposés sur Internet
- Filtrage Réseau

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Sécurité applicative

3 PARCOURS AVANCÉ
- Web application firewall
- Protection DDOS

4 PARCOURS RENFORCÉ
- SSO

Fondée en 2001 avec son siège social à Meudon en France et un centre de recherche à Montpellier, Ubika, le nouveau DenyAll, est un fournisseur européen en matière de cybersécurité. Sa mission est d'aider les organisations à sécuriser leur transformation digitale en protégeant les applications contre les cyberattaques.

Notre technologie Web Application & API Protection (WAAP) peut être déployée sur site, dans le Cloud, en mode SaaS ou comme conteneur, pour sécuriser à la fois les applications existantes et les applications cloud-native. Plus de 600 entreprises et institutions publiques dans 35 pays nous confient la sécurité de leurs applications.

PRODUITS & SERVICES

Ubika WAAP Gateway protège vos applications critiques et vos API contre les cybermenaces avancées grâce à de puissants workflows personnalisables.

Ubika WAAP Cloud est un complément d'Ubika WAAP Gateway qui se déploie en cloud privé, clouds publics AWS, Azure, Google, et en mode hybride.

Ubika Cloud Protector : WAAP en mode SaaS avec ou sans services managés.
Coût total de possession (TCO) compétitif.
Waf avec anti-DDoS intégré. 14 jours d'essai gratuit.

Ubika WAAP Container:
Proposez des applications cloud native dignes de confiance en intégrant une protection avancée à vos pratiques DevOps.

Ubika Web Acces Manager:
Le Web Access Manager (WAM) est un module optionnel de Ubika WAAP Gateway et Ubika WAAP Cloud, qui contrôle l'accès aux applications web en fournissant divers services dont l'authentification unique sur le web (WebSSO).

Vade
https://www.vadesecure.com
+33 (0) 359 616 650
contact@vadesecure.com

1 PARCOURS FONDATION
- Sensibilisation
- Protection de la messagerie
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Sensibilisation
- Test de phishing
- Gestion des logs
- Gestion d'incidents de sécurité

3 PARCOURS AVANCÉ
- Sensibilisation et formation
- Gestion des logs

4 PARCOURS RENFORCÉ
- Indicateurs SSI
- Forensic et analyse des logs

Vade aide les entreprises, les FAI et les autres éditeurs de sécurité à protéger leurs utilisateurs contre les cybermenaces sophistiquées comme le phishing, le spear phishing, les malwares et les ransomwares.

La solution prédictive de protection de l'e-mail de Vade utilise l'intelligence artificielle et les données de 1,4 milliard de messageries afin de bloquer les attaques ciblées et novatrices dès le premier e-mail.

PRODUITS & SERVICES

Les solutions de protection de la messagerie de Vade protègent les utilisateurs des cybermenaces les plus sophistiquées, comme le phishing, le spear phishing et les malwares. Proactives, nos solutions s'appuient sur les données de plus de 1,4 milliard de boîtes aux lettres, l'intelligence artificielle et l'apprentissage automatique pour offrir une protection contre les attaques inconnues et ciblées. Grâce à plus de 10 ans de collaboration avec les plus grands FAI du monde entier, Vade a accès à des volumes de données colossaux et sait mettre au point des solutions de grande envergure pensées pour la vitesse et la performance.

2 solutions sont proposées :

Vade for M365 est une solution de sécurité de l'e-mail intégrée nativement à Microsoft 365 par l'intermédiaire de l'API Microsoft.

Vade for Cloud est une solution positionnée en coupure du flux SMTP pour toutes les messageries Exchange on premise, Zimbra, Bluemind ou Gsuite.

WALLIX
https://www.wallix.com/fr
+33 (0)1 53 42 12 81
info@wallix.com

1 PARCOURS FONDATION
- Gestion des mots de passe
- Protection des accès distants
- Gestion des comptes à privilèges
- Authentification et contrôle d'accès

2 PARCOURS INTERMÉDIAIRE
- Coffres-forts de mots de passe
- Approche Security-by-design
- End point security
- Gestion des comptes de service

3 PARCOURS AVANCÉ
- Gestion des droits d'accès
- Authentification forte
- Gestion des comptes à privilèges
- Principe du moindre privilège pour les administrateurs

4 PARCOURS RENFORCÉ
- SSO
- Forensic et analyse des logs

Éditeur de logiciels de cybersécurité, WALLIX est le spécialiste européen de la sécurisation des accès et des identités. Cotée sur Euronext, WALLIX accompagne plus de 2000 organisations dans la sécurisation de leur transformation numérique.

PAM4ALL, sa solution de gestion unifiée des privilèges et des accès, permet de répondre aux enjeux actuels de protection des données. Elle est distribuée par un réseau de plus de 300 revendeurs et intégrateurs à travers le monde.

PRODUITS & SERVICES

WALLIX PAM4ALL, la solution unifiée de gestion des privilèges et des accès.

PAM4ALL réduit les risques liés aux accès et aux privilèges associés, permet une gestion granulaire de vos accès distants et offre des accès uniquement pour des usages et des durées spécifiques, réduisant ainsi considérablement les surfaces d'attaques, sans affecter la productivité et en respectant les directives réglementaires.

PAM4ALL sécurise, contrôle et administre les accès de tous les utilisateurs, pour toutes les sessions sur tous vos actifs, et pour tous vos terminaux, au bon moment et de n'importe où.

- Traçabilité des sessions : maintenez la conformité.
- Protection des mots de passe : prévenez l'exposition.
- Sécurisation des accès à distance : protégez le système d'information.
- Gestion du moindre privilège : supprimez les droits locaux.
- Authentification forte : diminuez les risques.

Whaller

Whaller
https://whaller.com
+33 (0)1 47 92 82 18
contact@whaller.com

1 PARCOURS FONDATION
- Protection des accès distants
- Analyse des vulnérabilités
- Firewall
- Gestion d'incidents de sécurité

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Chiffrement des données
- Sécurisation des services Cloud (IaaS/PaaS)
- Gestion des logs

3 PARCOURS AVANCÉ
- Sensibilisation et formation
- Audit, scan, revue de code
- Filtrage de flux réseau
- Tests d'intrusion

4 PARCOURS RENFORCÉ
- Politique SSI
- SSO
- Plan de reprise d'activité

Whaller est une plateforme sociale et collaborative complète. De l'intranet collaboratif au réseau social d'entreprise, elle s'adresse aux organisations qui veulent accélérer leur transformation numérique, sans délaisser leur cybersécurité. Whaller convient aussi bien aux petites équipes qu'aux très grands réseaux.

PRODUITS & SERVICES

Whaller est une solution collaborative complète, facile à prendre en main, qui permet de créer des réseaux sociaux et collaboratifs sécurisés. Respectueuse des données de ses utilisateurs et garante de leur confidentialité, la plateforme s'adresse aux entreprises, institutions, administrations, établissements éducatifs, associations etc.
La solution répond à l'ensemble de leurs besoins de communication et de collaboration. Elle propose de multiples fonctionnalités telles que les messages cryptés, une gestion électronique des documents, un système de Drive, les événements, les sondages, la gestion de tâches, la conversation en temps réel, la visio-conférence, etc. La plateforme permet ainsi de répondre à de nombreux usages : réseau social d'entreprise, intranet, plateforme collaborative ou encore digital workplace complète.

La confidentialité et la cybersécurité constituent des aspects majeurs de la plateforme. Vos données sont stockées sur des serveurs français et ne sont soumises à aucune loi extraterritoriale. Whaller est engagé dans la qualification SecNumCloud et tire une grande fierté d'être utilisé par les armées françaises.

YES WE HACK

YesWeHack
https://www.yeswehack.com/
+33 (0)1 86 95 84 18
contact@yeswehack.com

1 PARCOURS FONDATION
- Analyse des vulnérabilités
- Protection des services exposés sur Internet
- Cartographie du réseau
- Scans de vulnérabilité du SI exposé sur Internet

2 PARCOURS INTERMÉDIAIRE
- Approche Security-by-design
- Chiffrement des données
- Cartographie de l'infrastructure du SI
- Scans de vulnérabilité sur tout le SI

3 PARCOURS AVANCÉ
- Audit, scan, revue de code
- Web application firewall
- Effacement des données
- Tests d'intrusion

4 PARCOURS RENFORCÉ
- Cartographie des données du SI
- Audit, scan, revue de code
- Sécurité des équipements mobiles
- Scans de vulnérabilité en continu

Fondée en 2015, YesWeHack est la première plateforme européenne de Bug Bounty et de Vulnerability Disclosure Policy (VDP). Le Bug Bounty est un modèle qui récompense les chercheurs à la vulnérabilité. La plateforme connecte plus de 45 000 experts en cybersécurité dans 170 pays avec des centaines d'organisations à travers le monde. YesWeHack gère plus de 500 programmes de Bug Bounty en Europe et en Asie, en conformité avec les réglementations européennes les plus strictes.

PRODUITS & SERVICES

Le principe du Bug Bounty est de rémunérer les testeurs au résultat (lorsqu'ils découvrent une vulnérabilité valide) en fonction de paramètres prédéfinis par les organisations (périmètres, méthodes d'audits, grilles de primes, etc.).

- **Programmes de Bug Bounty privés :** Sélectionnez les chercheurs que vous souhaitez selon vos critères d'expertise, de compétences et de nationalité.
- **Programmes de Bug Bounty publics :** Mobilisez l'intégralité de la communauté et communiquez sur votre stratégie de sécurité.
- **Vulnerability Disclosure Policy (VDP) :** Offrez aux chercheurs un canal sécurisé et structuré pour remonter les vulnérabilités de vos systèmes d'information, avant qu'elles ne soient exploitées par des personnes malveillantes.
- **Pentest Management Solution :** pilotez et orchestrez l'ensemble de vos tests d'intrusion à travers une plateforme unique.

La plateforme YesWeHack intègre un support client avancé, gérant vos programmes de bout en bout : définition et mise à jour des règles, sélection et rotation des chercheurs, triage des rapports de vulnérabilités, suivi des budgets et indicateurs des programmes en ligne avec les objectifs du client, etc.

yogosha

Yogosha
https://yogosha.com/
+33 (0)6 98 36 51 07
contact@yogosha.com

1 PARCOURS FONDATION

- Analyse des vulnérabilités
- Protection des services exposés sur Internet

2 PARCOURS INTERMÉDIAIRE

- Approche Security-by-design

3 PARCOURS AVANCÉ

- Audit, scan, revue de code
- Tests d'intrusion

4 PARCOURS RENFORCÉ

- Scans de vulnérabilités en continu

Yogosha est un VOC – Vulnerability Operations Center :
- Un hub pour identifier, gérer et corriger les vulnérabilités.
- Une plateforme pour réunir les communautés
- RSSI, hackers éthiques, équipes sec & dev...
- Une arène où mener des opérations de sécurité
- VDP, pentest et bug bounty.
- Un centre de commandement pour superviser toutes les stratégies de gestion des vulnérabilités.

PRODUITS & SERVICES

- **Bug Bounty :** Traquez les vulnérabilités avec des hunters d'élite. Récompensez uniquement les résultats exploitables.

- **Pentest as a Service :** Un audit rapide, économique et efficace pour évaluer la sécurité numérique d'un actif et répondre aux obligations de conformité.

- **Vulnerability Disclosure Program :** Un canal sécurisé et continu pour agréger toutes les divulgations spontanées de vulnérabilités.

izidée Création graphique - Crédit photo : Istock, stock.adobe - Hexatrust

HEXATRUST

CAMPUS CYBER

5-7 rue Bellini,
92800 Puteaux

contact@hexatrust.com
www.hexatrust.com

H E X A T R U S T

CLOUD CONFIDENCE & CYBERSECURITY