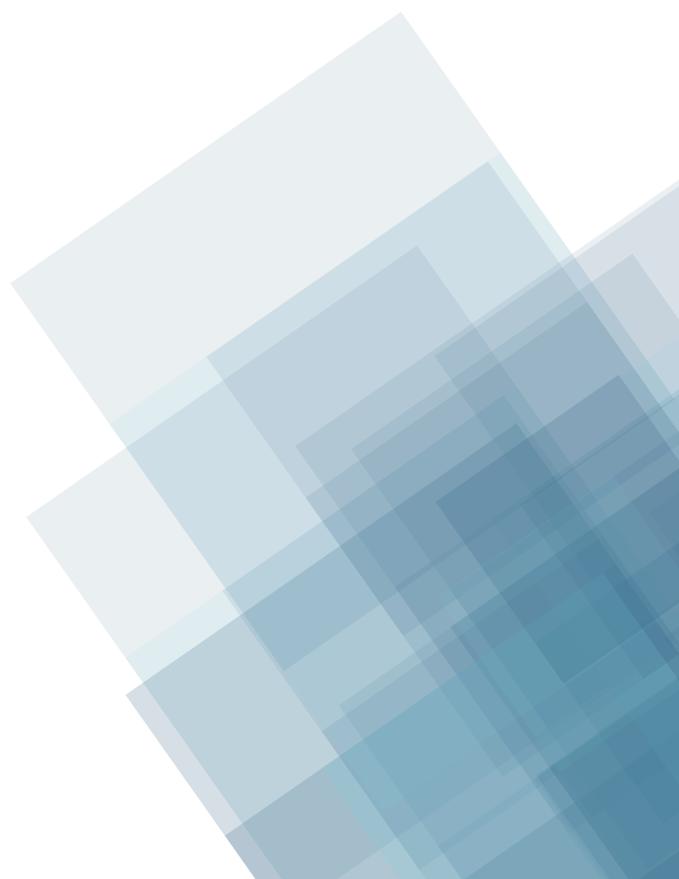


SOLUTIONS POUR SÉCURISER LE TÉLÉTRAVAIL

Confiance numérique

ACN

Alliance pour la confiance numérique ■■■





AGNÈS PANNIER-RUNACHER,

MINISTRE DÉLÉGUÉE AUPRÈS
DU MINISTRE DE L'ÉCONOMIE,
DES FINANCES ET DE LA RELANCE,
CHARGÉE DE L'INDUSTRIE



La crise sanitaire a accéléré certaines transformations du monde du travail, sans que nous ne sachions toujours en mesurer les conséquences. Le télétravail est un exemple de ces transformations à marche forcée. Il a impliqué la dématérialisation de nombreuses procédures, avec un risque accru de cyberattaques qui impose de développer des solutions de protection. Ainsi, l'ANSSI a révélé une augmentation de 255 % du nombre de rançongiciels entre 2019 et 2020. Face à cela, il existe des solutions françaises, à même de garantir notre souveraineté.

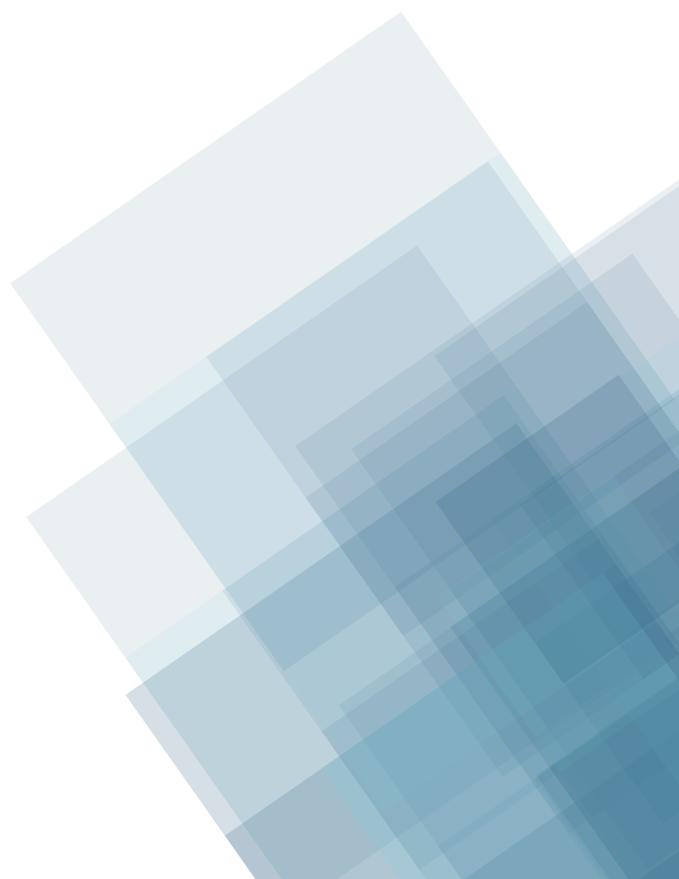
Ces solutions françaises sont développées par la filière de la confiance numérique qui représente 13,4 milliards d'euros de chiffre d'affaires, réalisés en France en 2020 par plus de 2000 entreprises et près de 70.000 salariés.

L'alliance pour la confiance numérique (ACN), qui participe activement aux travaux du Comité stratégique de Filière Industries de Sécurité, présente dans ce document les solutions développées par la filière dans sa grande diversité. Nous avons une responsabilité conjointe pour éclairer les utilisateurs sur les outils à leur disposition afin qu'ils puissent pleinement bénéficier de la transition numérique, tout en réduisant les risques liés à une numérisation non maîtrisée.

Je salue ce travail de recensement indispensable pour faire connaître l'offre française auprès des entreprises et collectivités qui souhaiteraient entreprendre une démarche de cybersécurisation de leurs activités en télétravail. Entreprise, réseau ou domicile : une offre est disponible pour sécuriser l'intégralité de la chaîne du télétravail et accompagner notamment les trois millions de nouveaux télétravailleurs depuis le début de la crise sanitaire.

La démarche de l'ACN s'inscrit pleinement dans le cadre de la stratégie nationale de cybersécurité annoncée par le président de la République.

En rendant visibles et lisibles les offres sécurisées dédiées au télétravail, ce guide fait œuvre utile et constitue un soutien très précieux pour tous ceux qui souhaitent continuer de bénéficier des apports du télétravail en toute sécurité et dans le respect de notre souveraineté.



INTRODUCTION

Comme l'a rappelé notre Premier Ministre Jean Castex lors de sa conférence de presse le 4 février 2021 « télétravailler partout où c'est possible devient un impératif ». En un an, le télétravail est devenu incontournable pour permettre à notre pays de continuer à lutter contre la crise de la Covid 19 tout en maintenant une activité économique et sociale.



230 milliards €

Le recours au télétravail a permis de sauvegarder entre 216 et 230 milliards d'euros de PIB en 2021.

Lors du premier confinement, les entreprises ont dû s'adapter extrêmement rapidement à cette nouvelle norme et un peu plus de trois millions de travailleurs sont devenus télétravailleurs pour la première fois.

Selon une étude du Ministère du Travail, de l'emploi et de l'insertion (DARES), en janvier 2021 30% des actifs télétravaillaient à temps complet (64% partiellement), contre 45% à temps complet début novembre 2020 (70% partiellement)².

Bien que depuis le début de l'année 2021 le nombre d'actifs pratiquant le télétravail a légèrement décroché, ce mode de d'activité est devenu une nouvelle norme.

De nombreuses études indiquent que les adeptes du télétravail souhaitent poursuivre cette pratique bien au-delà de la crise que nous traversons.



84% des salariés souhaitent demander à maintenir le télétravail³.

L'objectif pour le télétravailleur est de pouvoir exercer son activité de la manière la plus proche possible de celle qu'il a au sein de son entreprise. Cela nécessite d'avoir un accès à ses données et à ses applications professionnelles, de pouvoir partager, communiquer et échanger grâce à des outils de visioconférence ou bien encore de pouvoir dématérialiser tout ce qui nécessitait une présence physique par exemple une signature ou la consultation d'archives.



Pour 69% des cadres, dont 76% des moins de 30 ans, la possibilité de télétravailler constitue un critère important dans la recherche d'emploi⁴.

¹ 167 et 173 milliards d'euros de PIB lors du premier confinement, et entre 49 et 57 milliards d'euros lors du second confinement. <https://www.institutsapiens.fr/wp-content/uploads/2021/03/Quel-avenir-pour-le-te%CC%81le%CC%81travail.pdf>

² <https://dares.travail-emploi.gouv.fr/publications/activite-et-conditions-d-emploi-de-la-main-d-oeuvre-pendant-la-crise-sanitaire-119594>

³ <https://newsroom.malakoffhumanis.com/actualites/barometre-annuel-teletravail-2021-de-malakoff-humanis-db57-63a59.html>

⁴ Etude réalisée par APEC – décembre 2020 : Le télétravail des cadres en temps de crise. <https://corporate.apec.fr/files/live/sites/corporate/files/Nos%20%3%a9tudes/pdf/le-teletravail-des-cadres-en-tem>

Dans le cadre de ce document, l'approche du télétravail retenue se fonde sur la définition proposée par le Ministère du Travail de l'emploi et de l'insertion comme méthode consistant pour le salarié à travailler volontairement hors des murs de l'entreprise, à son domicile ou dans un espace de cotravail en utilisant les technologies de l'information et de la communication⁵.

La notion de « nomadisme numérique » défini par l'ANSSI comme « toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, de lieux distants, ces lieux n'étant pas maîtrisés par l'entité »⁶ n'entre que partiellement dans le cadre de cette étude.

Un potentiel de **6 millions**
de télétravailleurs effectifs.



Pour répondre à tous ces besoins et permettre une véritable confiance dans le télétravail, les entreprises doivent de leur côté s'adapter à ce nouveau paradigme pour offrir aux salariés la possibilité de travailler à distance tout en maintenant un niveau de sécurité aussi élevé dans ce nouveau contexte. La généralisation du télétravail et les différents accès aux systèmes d'informations hors de l'entreprise entraînent de nouveaux risques qu'il s'agit de réduire au maximum.

Cela implique de repenser et d'adapter les logiques et les processus de sécurisation établis et de porter une attention particulière aux spécificités et aux nouveaux risques induits par l'aspect distanciel notamment sur la sécurisation de l'accès au système d'information, la sécurisation du télétravailleur et celle des réseaux et des flux de données qui les traversent.

+ 630 % d'attaques contre les Clouds



Entre janvier et avril 2020, on recense une augmentation de 630% du nombre d'attaques externes contre les Clouds des entreprises suite à la migration des employés des locaux de l'entreprise vers leurs lieux de télétravail⁷.

L'actualité illustre chaque jour un peu plus ces nouveaux risques à travers les différentes cyberattaques subies par les entreprises⁸ et organisations de toutes tailles, publiques ou privées. L'enseignement majeur de ces dernières années est que tous types d'infrastructures peuvent être désormais ciblés : des hôpitaux⁹, des fournisseurs de services numériques, des hébergeurs de données, des grandes entreprises¹⁰, les services de messagerie¹¹...

Ces attaques ne s'arrêtent pas uniquement aux services, serveurs ou fournisseurs, elles descendent en cascade sur toutes les infrastructures utilisatrices de ces services. La généralisation du télétravail a mis en avant une vulnérabilité forte aux attaques par périphérie : les attaquants ciblent désormais plus volontiers les télétravailleurs plutôt que le SI de l'entreprise.

+ 93% du nombre de fuites de données en 2020
= 1,7 Million de fuites

Source : Etude réalisée sur l'année 2020 par la société Imperva¹².



⁵Code du Travail Partie 1, Livre II, Titre II, Chapitre II, Section 4 : Télétravail, Article L1222-9.

⁶<https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/>

⁷Constat réalisé par McAfee : <https://cyberhedge.com/insights/daily/2020/05/27/mcafee-reports-630-percent-increase-in-external-attacks-on-cloud-based-services/#:~:text=Data%20from%2030m%20McAfee%20MVISION,over%20the%20same%20time%20period>

⁸Selon une enquête d'OpinionWay pour Cesin, 19% des entreprises déclarent avoir été victime d'un ransomware.

⁹L'hôpital de Dax (09/02/21), l'hôpital de Villefranche-sur-Saône (15/02/21) et l'hôpital des Pyrénées-Atlantiques (10/03/21).

¹⁰Selon une enquête d'OpinionWay pour Cesin, 57% des grandes entreprises déclarent avoir été victime d'au moins une cyberattaque au cours de l'année 2020.

¹¹Cyberattaque de Microsoft Exchange.

¹²<https://www.itproportal.com/news/data-leakage-attacks-saw-huge-rise-in-2020/>

Un des enjeux prioritaires des prochaines années sera notre capacité à apporter des réponses pour augmenter le niveau de sécurité de l'ensemble de la chaîne de valeur numérique comme l'a rappelé le 18 février 2021 le Président de la République à travers l'annonce de la Stratégie Nationale pour la cybersécurité¹³.

Le recours à des solutions, produits ou services présentant un haut niveau de confiance permettrait aux entreprises de toutes tailles de sécuriser les différents éléments nécessaires à un télétravail de confiance. Pour répondre à ces problématiques, notre pays dispose, grâce à un tissu d'entreprises de la confiance numérique, d'une expertise

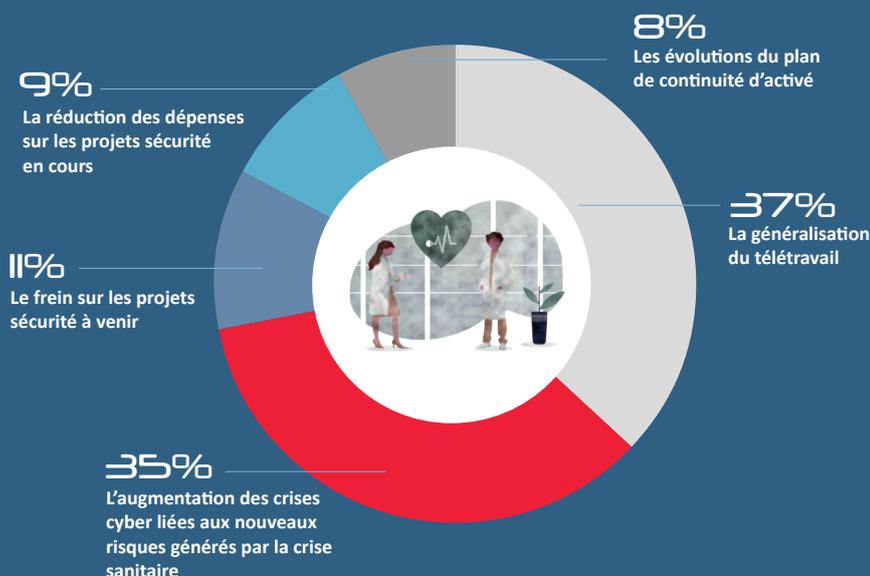
souveraine en la matière. Le télétravail et l'augmentation des crises cyber sont les changements impactant le plus fortement les entreprises pendant la crise sanitaire.

La numérisation à marche forcée due à la crise sanitaire a mis en exergue une très forte dépendance de toutes nos activités aux solutions étrangères posant une véritable problématique de souveraineté. Il est donc urgent de concilier la sécurisation de notre espace numérique et la protection de notre souveraineté nationale et/ou de notre autonomie stratégique européenne.

C'est dans ce contexte que l'Alliance pour la Confiance Numérique (ACN) souhaite proposer une réflexion sur les diverses solutions à disposition de toutes les entreprises souhaitant s'engager dans une démarche de sécurisation du télétravail.

Cette offre capacitaire se veut pédagogique et ambitieuse d'aider les entreprises à mieux visualiser les différents risques inhérents à la pratique du télétravail et à y apporter un catalogue de réponses concrètes et adaptées.

Avec la crise sanitaire en cours, quel phénomène impacte le plus l'activité de cybersécurité de votre entreprise ?



Source : Baromètre de la cyber-sécurité des entreprises réalisé par Opinion Way pour le CESIN.

¹³ <https://www.gouvernement.fr/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite>



ASSEMBLEE NATIONALE



POINT DE VUE PARLEMENTAIRE



JEAN-MICHEL MIS

DÉPUTÉ DE LA LOIRE

Pendant cette si singulière crise sanitaire, l'utilité des outils numériques s'est imposée dans notre société. Notre quotidien a été bouleversé par la nécessaire utilisation des nouvelles technologies de l'information et des communications tant dans nos modes de production, de consommation, de communication, de partage que de collaboration.

Au sein même de l'Assemblée nationale, nous avons dû adapter notre mode de fonctionnement afin de concilier la continuité de nos missions au sein de notre Institution et la mise en place de règles sanitaires strictes. C'est en ce sens que j'ai participé aux travaux du groupe de travail chargé d'anticiper le mode de fonctionnement des travaux parlementaires en période de crise¹.

Mais tous ces changements de paradigme dans notre organisation professionnelle et « sociétale » ne sont pas sans risque dans un univers totalement connecté, de plus en plus menacé, voire menaçant.

Par facilité, par urgence, par méconnaissance, nous nous sommes mis à utiliser les outils rendus célèbres par les réseaux sociaux, en dépit de toutes règles de sécurité².

L'exemple de l'explosion du télétravail (près de 40 % de la population active³) est riche d'enseignement. Deux tiers de la population active ignorent les bonnes pratiques, et pourtant nous utilisons tous des applications comme Zoom ou Partyhouse, qui n'avaient pas d'usage stratégique⁴ et n'étaient pas destinées à un usage de masse. Non sécurisées, elles n'ont pas été développées pour un échange de données sensibles, rendant les intrusions faciles et constituant donc un vrai facteur de risque !

Cette mise en œuvre non maîtrisée du télétravail a donc augmenté considérablement les risques de sécurité pour les entreprises et organisations.

¹ <https://www.jeanmichelmis.fr/lassemblee-nationale-adopte-une-modification-de-son-reglement-pragmatique-et-adaptée-a-levolution-de-ses-missions-en-période-de-crise/>

² L'Opinion, « Les outils sûrs existent, il faut les utiliser » Jean Michel Mis, interview Emmanuelle DUCROS, 2020-04-07.

³ Selon une étude réalisée par l'Association Nationale des DRH.

⁴ L'Opinion, « Les outils sûrs existent, il faut les utiliser » Jean Michel Mis, interview Emmanuelle DUCROS, 2020-04-07.

Il nous faut donc promouvoir et populariser les outils français et européens qui garantissent notre sécurité numérique ou, à tout le moins, veiller à utiliser des outils robustes pour nous prémunir des assaillants non étatiques. C'est un travail que nous devons mener ensemble et auprès de tous les publics.

Il nous faut aussi faire preuve de pédagogie auprès de nos concitoyens. La cybersécurité est, en effet, l'affaire de tous. Les moyens alloués à l'éducation et la formation continue dans le domaine de la cybersécurité doivent donc être au cœur de nos préoccupations.

Par ailleurs, il existe aujourd'hui un trop grand nombre de sites demandant au grand public de prouver son identité en ligne. Le mot de passe, moyen d'identification le plus répandu, n'est pas suffisamment protecteur des données identificatrices qu'il doit couvrir.

Le développement d'une solution régaliennne d'identité numérique est donc une nécessité pour permettre à chacun de garantir sa véritable identité. C'est en ce sens que j'ai été co-rapporteur, aux côtés de Christine Hennion, de la mission d'information commune sur l'identité numérique à l'Assemblée nationale, dont les conclusions ont été rendues en juin 2020⁵.

Il demeure enfin indispensable de développer des solutions de Cloud européennes et souveraines. Il nous faut donc penser à l'échelle européenne à la mise en place d'une économie innovante et compétitive avec des entreprises de premier plan. Ce marché numérique européen passera par une harmonisation des standards, un partage des avancées technologiques, une augmentation de l'offre, un renforcement de nos outils de certification, seul garant de nos valeurs.

La réglementation à elle seule ne peut être une barrière suffisamment solide pour se protéger de la concurrence étrangère. L'Europe et la France, en premier lieu, doivent donc se préoccuper de garder sur leur sol hormis leurs opérateurs vitaux, leurs industries stratégiques.

La maîtrise de la donnée numérique est un élément majeur pour garantir la protection des intérêts des Français et des Européens et donc celui de notre souveraineté. Nous ne pouvons pas nous laisser dicter nos choix par d'autres que ce soient des puissances étatiques ou bien des puissances privées.

⁵ <https://www.jeanmichelmis.fr/vers-une-identite-numerique-de-confiance/>

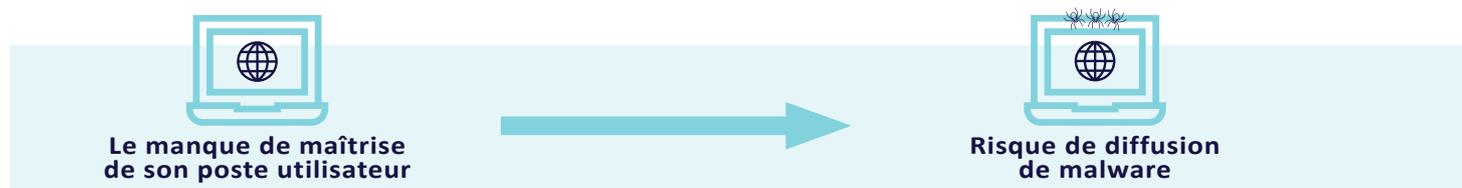
FACTEURS DE RISQUE/IMPACT

A travers cette partie, nous souhaitons mettre en exergue des couples généraux facteur de risque/ impacts qui doivent être considérés par les organisations qui recourent au télétravail.

Trois couples d'exemples sont proposés :

FACTEUR DE RISQUE 1

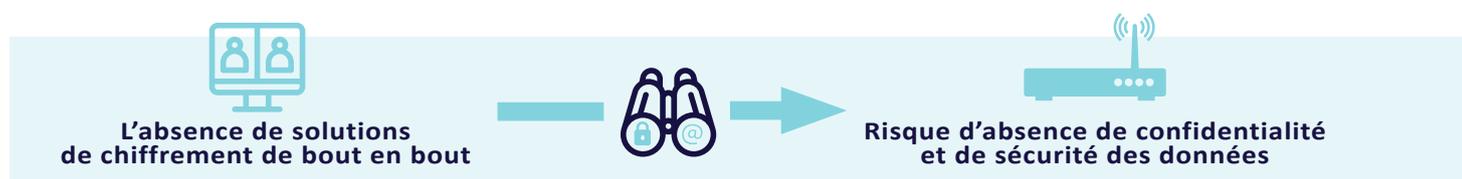
LE MANQUE DE MAÎTRISE DU POSTE UTILISATEUR ENTRAÎNE UN RISQUE DE DIFFUSION DE MALWARE.



Le manque de maîtrise de l'environnement, un Wifi non sécurisé, l'absence de mise à jour des systèmes d'exploitation ou des anti-virus, l'utilisation d'un même poste par plusieurs utilisateurs, rend le poste vulnérable en favorise, augmente le risque d'infection du poste et, s'il est connecté au réseau de l'organisation, favorise la diffusion de malware.

FACTEUR DE RISQUE 2

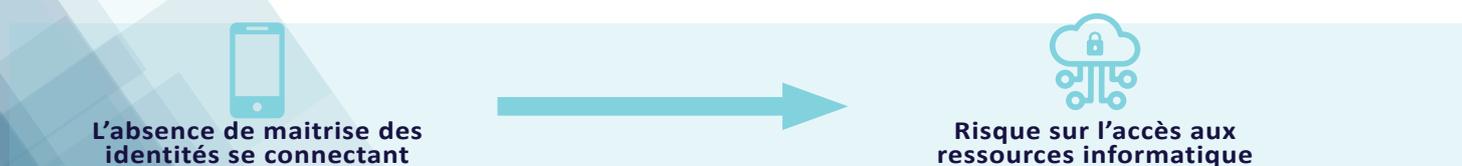
L'ABSENCE DE CHIFFREMENT DE BOUT EN BOUT IMPLIQUE UN RISQUE DE FUITE OU DE PERTE DE DONNÉES OU DE VIOLATION D'ACCÈS.



L'accès distant aux actifs de l'organisation ne doit se faire que grâce à des moyens de chiffrement adéquats : un VPN qui est une sécurité périmétrique permettant de connecter deux réseaux de confiance, un Accès Réseau Zero Trust (ZTNA) qui est une sécurité logique basée sur l'identité de l'utilisateur, le contexte d'utilisation et l'application qu'il utilise.

FACTEUR DE RISQUE 3

D'UN MANQUE DE MAÎTRISE DES IDENTITÉS SE CONNECTANT RÉSULTE UN RISQUE SUR LES ACCÈS AUX RESSOURCES INFORMATIQUES DE L'ORGANISATION.



Sur le site, le collaborateur ou le prestataire a souvent passé l'obstacle des accès physiques aux bureaux et des accès logiques aux applications depuis l'intérieur du réseau de l'entreprise. Une fois en dehors du site, la certitude de l'identité de l'utilisateur est plus difficile à garantir : même authentifié, quelqu'un peut prendre la place d'un utilisateur négligent qui a laissé la session ouverte, par exemple. Il faut réfléchir à un renforcement de l'authentification pour s'assurer de l'identité de la personne présente derrière son poste.

COMMENT LIRE CE GUIDE ?

Ce guide a été conçu pour pouvoir répondre aux besoins de toute entité s'interrogeant sur les questions de sécurisation du télétravail et recherchant les solutions, produits et offres disponibles dans ce domaine.

Pour une plus grande lisibilité, les solutions présentées dans le cadre de cette offre capacitaire ont été segmentées en fonction de trois critères alternatifs ou cumulatif.

Critère 1 : Nature de l'offre

Nous avons souhaité introduire la notion de la nature de l'offre afin d'indiquer au lecteur si l'offre proposée est un produit ou logiciel directement utilisable, une prestation de service (l'intégration d'un produit ou un logiciel), ou encore une prestation de conseil.



PRODUIT/LOGICIEL



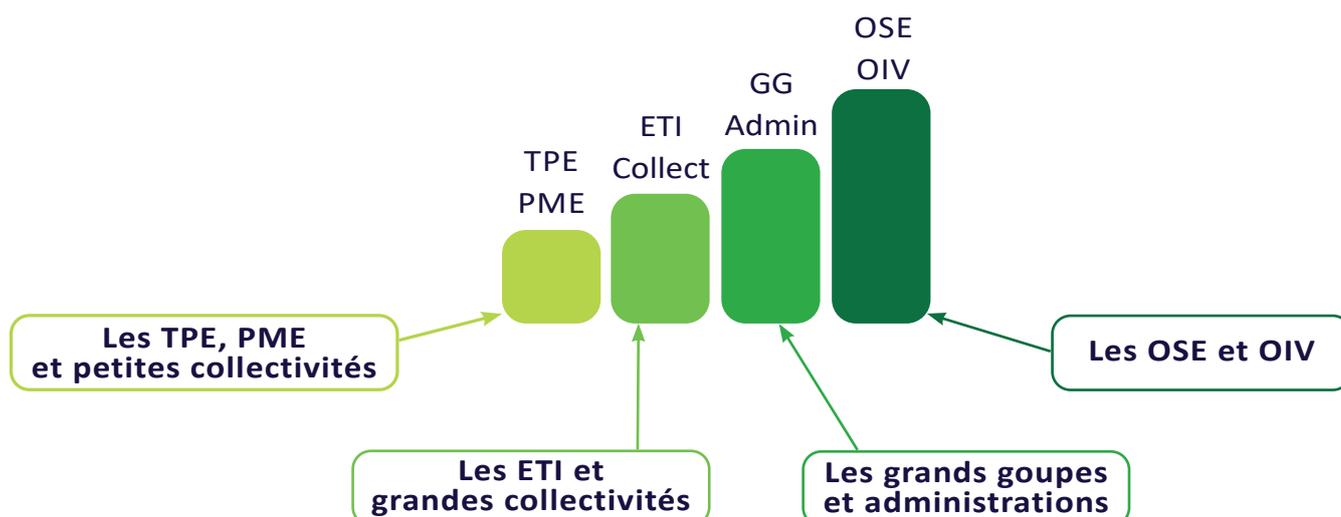
SERVICE



CONSEIL

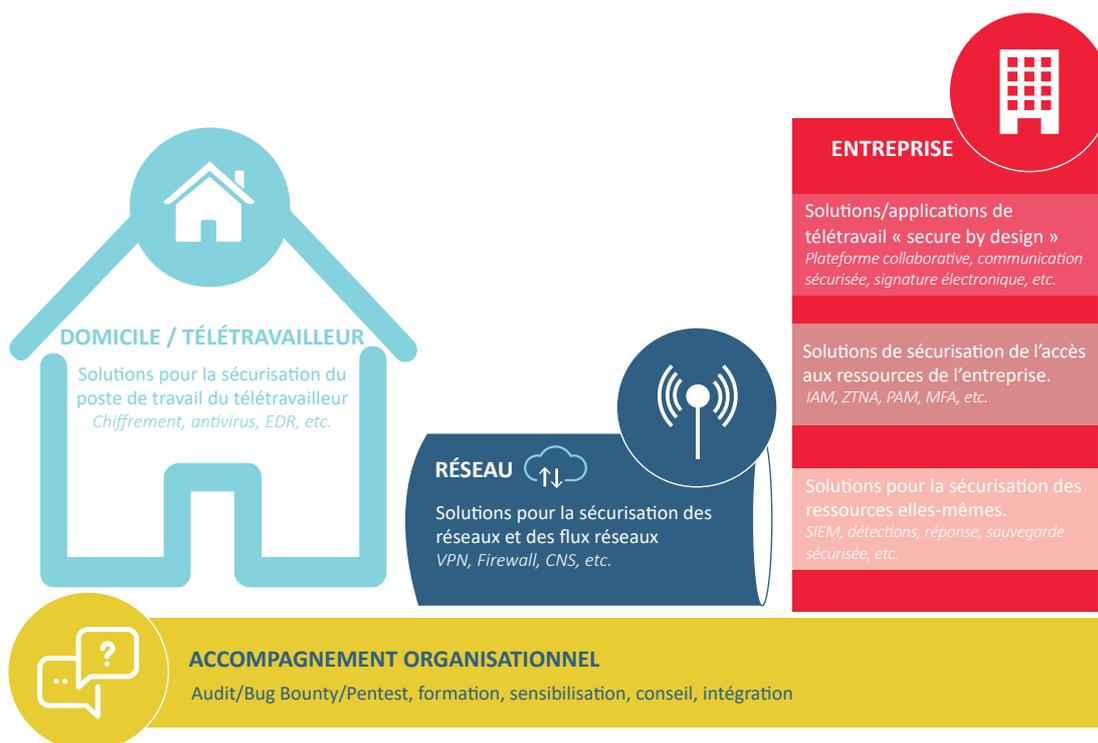
Critère 2 : Les cibles auxquelles s'adressent les offres présentées.

Pour compléter cette approche, nous avons souhaité introduire un deuxième critère qui est celui des cibles auxquelles s'adressent les offres répertoriées. Nous avons décidé de séparer ces cibles en quatre catégories :



Critère 3 : La place dans l'offre dans le schéma du télétravail

Enfin, nous avons également désiré introduire un troisième critère qui est celui du positionnement de l'offre au sein du schéma fonctionnel spécifique au télétravail, selon qu'elle se place au niveau de la sécurisation du télétravailleur, du réseau, ou de l'accès au système d'information de l'organisation.



Répartition des offres par entreprise

-  produit/logiciel
-  intégration/service
-  conseil

DOMICILE/
TÉLÉTRAVAILLEUR

RÉSEAUX

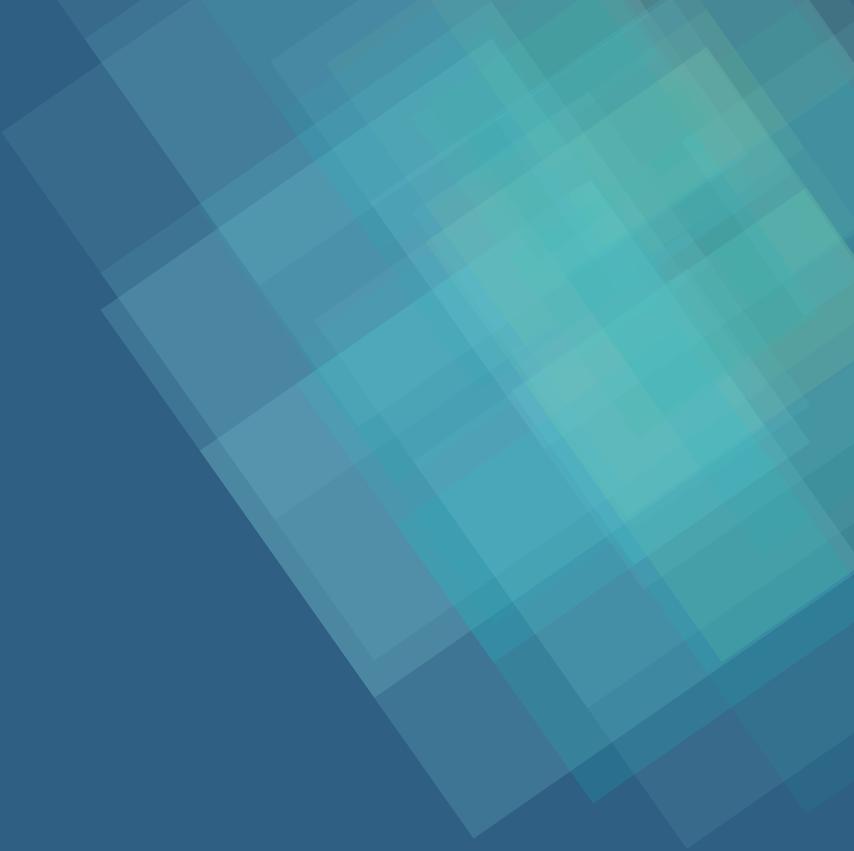
TÉLÉTRAVAIL
« SECURE BY DESIGN »

SÉCURISATION
DE L'ACCÈS AUX
RESSOURCES

SÉCURISATION DES
RESSOURCES
ELLES-MÊMES

ACCOMPAGNEMENT
ORGANISATIONNEL

AIRBUS					 p.34	 p.38
ATOS		 p.19	 p.24		  p.34	
ATOS EVIDIAN				 p.28		
AVANT DE CLIQUER	 p.16					 p.38
CHAMBERSIGN				 p.28		
CORALIUM						 p.38
DOCAPOSTE	 p.16	 p.19	 p.24	  p.29	 p.35	 p.39
ERCOM		 p.19 / 20	 p.24 / 25	 p. 29 / 30	 p.35	
HARFANG LAB	 p.16				 p.35	
HARMONIE TECHNOLOGIE				 p.30		 p.39
KEOPASS	 p.17			 p.31		
LEX PERSONA		 p.20	 p.25 / 26		 p.36	
NET EXPLORER			 p.26			
NEXUS				 p.31		
OXIBOX					 p.36	
PRIVATE DISCUSS	 p.17		 p.26			
RED ALERT LABS						 p.39
RUBYCAT		 p.20			 p.37	
SERMA SAFETY & SECURITY						 p.40
SOGETI					 p.37	 p.40
STORMSHIELD	 p.17 / 18	 p.21		 p.31		
SYSTANCIA		 p.21 / 22		 p.32 / 33		
THALES						 p.40  p.41
THEGREENBOW		 p.22 / 23			 p.37	 p.41
TIXEO			 p.27			
TRANQUIL IT	 p.18	 p.23				
YOGOSHA						 p.41



LES OFFRES DE LA FILIÈRE



DOMICILE/TÉLÉTRAVAILLEUR

Solutions pour la sécurisation du poste de travail du télétravailleur Chiffrement, antivirus, EDR, etc.



AVANT DE CLIQUER



SOLUTION DE SENSIBILISATION À LA CYBERSÉCURITÉ FACE AU PHISHING SUR POSTE DE TRAVAIL



Avant de Cliquer développe une culture de cybersécurité avec des outils autonomes, accessibles à tous, immédiatement opérationnels et inter-services. Après un audit de vulnérabilité, Avant de Cliquer déploie un programme de sensibilisation au phishing basé sur l'apprentissage par l'action, créé sur mesure pour chaque utilisateur et animé sur la durée sans intervention de votre part.

Ainsi, Avant de Cliquer installe une solution SaaS développant des algorithmes intelligents associant audit de vulnérabilité, plateforme de e-learning, envoi de mails d'apprentissage et process d'alerte cyber pour les SI pour automatiser une solution complète de sensibilisation à la cybersécurité phishing.



DOCAPOSTE



L'Identité Numérique

IDENTITÉ NUMÉRIQUE



L'identité numérique La Poste est une preuve d'identité en digital.

C'est une clé universelle permettant de s'identifier et de s'authentifier avec un identifiant, un mot de passe et un code secret unique. Déjà présente sur des centaines de sites via France Connect, L'Identité Numérique est la première et unique solution certifiée de niveau substantiel selon le règlement iIDAS par l'ANSSI. L'utilisation de l'application L'Identité Numérique La Poste est donc équivalente à un face à face physique.



HARFANG LAB



HARFANGLAB EDR



HarfangLab, éditeur d'un logiciel EDR (Endpoint Detection and Response), technologie qui permet d'anticiper et neutraliser les cyberattaques modernes et inconnues, sur ordinateurs et serveurs.

Certifié par ANSSI depuis 2020, HarfangLab compte parmi ses clients de grandes entreprises d'envergure internationale, évoluant dans des secteurs très sensibles. HarfangLab EDR se distingue par : l'ouverture de sa solution qui s'intègre nativement à toutes les autres briques de sécurité grâce à son API ; par sa transparence, car les données collectées par l'EDR restent accessibles et par l'indépendance numérique qu'il offre, car ses clients sont libres de choisir leur mode d'hébergement : cloud, public ou privé, ou dans leur propre infrastructure.

DOMICILE/TÉLÉTRAVAILLEUR

Solutions pour la sécurisation du poste de travail du télétravailleur Chiffrement, antivirus, EDR, etc.



KEOPASS

PMIE ETI GG OSE/OIV



CLÉ BIOMÉTRIQUE



La Clé KeoPass est un dispositif biométrique portable, autonome et décentralisé, pour le contrôle d'accès logique et physique, ne nécessitant pas d'intégration logicielle, ni de modification d'infrastructure matérielle.

La Clé KeoPass permet de sécuriser le poste de travail par les empreintes digitales de son utilisateur et de le verrouiller automatiquement en cas d'éloignement. Elle est le complément idéal d'un VPN, SSO et AD pour sécuriser les accès aux ressources de l'entreprise.

Doté d'un gestionnaire de mots de passe web avec vérification d'URL, la Clé KeoPass est un rempart contre le hameçonnage et les attaques par force brute ou ingénierie sociale; elle facilite et sécurise l'authentification des utilisateurs et réduit les appels hotline.



PRIVATE DISCUSS

PMIE ETI GG OSE/OIV



PRIVATE DISCUSS



Private Discuss est une plateforme de communication collaborative, utilisée pour les visioconférences, les webinaires ou encore le télétravail.

Véritable bureau hybride et ergonomique, Private Discuss est chiffrée de bout-en-bout et conforme RGPD, elle se démarque des solutions étrangères en proposant une plateforme complète grâce à ses fonctionnalités nombreuses et inédites, mais aussi en promouvant la souveraineté numérique et le savoir-faire technologique et cyber français.

Conçue à partir de technologies 100% propriétaires, sur les algorithmes les plus puissants du marché et hébergée sur des serveurs français, Private Discuss vous garantit la protection robuste de vos données et une entière satisfaction lors de son utilisation.



STORMSHIELD

PMIE ETI GG OSE/OIV



Chiffrement de bout en bout multi-devices et multi-applications



Le Stormshield : Une solution de chiffrement des données non-branchées On-Premise & Cloud. Chiffrement au plus près de la donnée assure une protection de bout en bout.

STORMSHIELD DATA SECURITY



Stormshield Data Security assure une confidentialité de bout en bout des données sensibles, quels que soient les supports (emails, clés USB et serveurs de fichiers), terminaux (poste de travail et mobile) et applications (« On-Premise » ou Cloud) sur lesquels ces données sont stockées ou partagées. Stormshield Data Security permet d'assurer la confidentialité de vos documents de travail, de vos répertoires locaux ou des données partagées entre collaborateurs internes et externes. Le chiffrement s'intègre en toute transparence aux outils de collaboration et de communication habituels.

DOMICILE/TÉLÉTRAVAILLEUR

Solutions pour la sécurisation du poste de travail du télétravailleur Chiffrement, antivirus, EDR, etc.



STORMSHIELD

ETI GG OSE/OIV

VISA DE SÉCURITÉ

Stormshield Endpoint Security
Protection avancée des postes Windows

LES Stormshield : Une protection proactive unique et non connectée

Stockage sécurisé des données investiguées et mise à disposition des éléments d'investigation détectés

STORMSHIELD ENDPOINT SECURITY



Stormshield Endpoint Security fournit une protection en profondeur et proactive face aux menaces, mêmes inconnues, dédiée aux environnements Windows. La solution combine les capacités d'une protection EPP (Endpoint Protection Platform) innovante et d'une solution EDR (Endpoint Detection & Response) dans une solution de sécurité unique. SES réagit dynamiquement en fonction de son environnement, cette capacité d'adaptation unique permet de durcir automatiquement le niveau de protection en cas de changement du contexte (sur site ou en situation de télétravail). L'architecture sécurisée en micro services de SES garantit la robustesse de la solution grâce à un mécanisme d'autoprotection et d'autoréparation.



TRANQUIL IT

PMIE ETI GG OSE/OIV

VISA DE SÉCURITÉ

FRANCE CYBER SECURITY

WAPT Enterprise

WAPT



WAPT installe, met à jour et supprime les logiciels et les configurations sur les appareils Windows, Linux et macOS. Le déploiement de logiciels (Firefox, MS Office, etc.) peut être effectué à partir d'un serveur central à l'aide d'une console graphique.

Des entreprises privées de toutes tailles, des écoles, des universités, des CNRS, des gouvernements locaux et nationaux, des hôpitaux, des mairies et des ministères d'État du monde entier utilisent avec succès WAPT.

WAPT est très efficace pour répondre aux besoins récurrents de mise à jour de Firefox ou Chrome et c'est souvent pour couvrir ce besoin de base que WAPT est initialement adopté ; il devient alors un outil de choix pour les tâches quotidiennes de l'administrateur système.



RÉSEAUX

Solutions pour la sécurisation des réseaux et des flux réseaux VPN, Firewall, CNS, etc.

ATOS

PME ETI GG OSE/OIV

VISA de sécurité

FRANCE CYBER SECURITY

SOLUTIONS DE CHIFFREMENT TRUSTWAY



La protection des données est l'une des principales préoccupations de l'entreprise.

Atos aide les organisations à mettre en place une protection des données complète en commençant par le déploiement des solutions nécessaires pour assurer la confidentialité des données critiques :

- Modules Matériel de sécurité Trustway Protecchio pour assurer l'intégrité et la sécurité des opérations cryptographiques
- Sécurité des réseaux IP avec Trustway IP Protect, gamme de chiffreur réseau
- Chiffrement de tous formats et types de données (machines virtuelles, bases de données, fichier système, application et tokenisation) avec Trustway DataProtect

DOCAPOSTE

PME

EUKLES
UNE MARQUE DE DOCAPOSTE

TITAN PAR EUKLES



Le Titan, appliance haute sécurité, protège le patrimoine documentaire de l'entreprise. Permettant de conserver la valeur probatoire des documents électroniques en interne, ce système de coffre fabriqué en France par Eukles est conçu dans un boîtier testé à toute épreuve.

Le Titan comprend les deux solutions GED et Backup éditées par Eukles, mettant à l'abri en cloud privé les données de l'entreprise.

ERCOM

PME ETI GG OSE/OIV

VISA de sécurité

FRANCE CYBER SECURITY

CRYPTOSMART
BY ERCOM

CRYPTOSMART MOBILE



CRYPTOSMART MOBILE est l'unique solution, développée en partenariat avec SAMSUNG, qui sécurise vos communications, données, terminaux mobiles, avec un niveau de sécurité élevé (agrément Diffusion Restreinte délivré par l'ANSSI*), sur des smartphones et tablettes grand public de dernière génération.

Grâce au chiffrement de bout en bout, vos données sont protégées contre les risques d'interception des communications, la perte ou de vol de votre smartphone.

RÉSEAUX

Solutions pour la sécurisation des réseaux et des flux réseaux VPN, Firewall, CNS, etc.

ERCOM

PMI ETI GG OSE/OIV

VISA DE SÉCURITÉ ANSSI

FRANCE CYBER SECURITY

CRYPTOSMART BY ERCOM

CRYPTOSMART PC



Pour faire face aux nouveaux enjeux de mobilité et de travail à distance, Ercom a développé Cryptosmart PC, une solution souveraine de VPN pour sécuriser les connexions de vos ordinateurs Windows distants.

Cryptosmart PC s'appuie sur les briques technologiques reconnues de Cryptosmart mobile, solution historique d'Ercom qui sécurise les communications, données et terminaux mobiles.

Cette solution VPN est d'ores et déjà utilisée sur le marché pour garantir l'intégrité et la sécurité des données échangées, à distance, par vos salariés.

LEX PERSONA

PMI ETI GG OSE/OIV

FAIRE SIGNER



Plateforme personnalisable pour faire signer tous vos cas d'usages.

Portail et API avec signature électronique sans transmission des documents. Intégration France Connect

Signature de tout type de document aux formats XAdES, CAAdES et PAdES.

Signature avancées à la volée ou qualifiées eIDAS (tokens, carte à puce).

API de signature électronique certifiée par l'ANSSI (CSPN).

Accompagnement individualisé lors du déploiement.

RUBYPAT

PMI ETI GG OSE/OIV

VISA DE SÉCURITÉ ANSSI

BASTION D'ADMINISTRATION PROVE IT



Renforcez la sécurité des accès sensibles au SI avec PROVEIT

PROVE IT est une solution logicielle de type « bastion-PAM » certifiée Visa de sécurité ANSSI. Elle contrôle, trace et enregistre les actions réalisées par les comptes à privilèges sur le SI (accès internes et externes).

Tracer les accès sensibles à vos équipements critiques est important cf RGPD, certification HDS, ISO 27001, guide de sécurisation du SI de l'ANSSI,...

PROVE IT est non invasive, simple à déployer et facile à administrer ;

comprend API REST et segmentation des droits - version Cluster

Licence uniquement dimensionnée au nombre de sessions concomitantes.

Licence POC gratuite – webinaires de démo sur le site RUBYPAT.

RÉSEAUX

Solutions pour la sécurisation des réseaux et des flux réseaux VPN, Firewall, CNS, etc.

STORMSHIELD

PME ETI GG OSE/OIV

VISA DE SÉCURITÉ ANSSI

Stormshield Network Security
Une gamme de pare-feux & VPN de nouvelle génération

Le Stormshield : Des performances inédites au meilleur coût

Protection de tous les environnements IT/OT et Cloud en une gamme complète et un seul logiciel d'administration

STORMSHIELD NETWORK SECURITY



La gamme de pare-feux Stormshield Network Security, qualifiée par l'ANSSI, est axée sur la sécurité des réseaux informatiques, et se compose de boîtiers physiques ou d'appliances virtuelles qui permettent de :

- Protéger vos infrastructures IT des menaces internes comme externes, grâce à une technologie de protection proactive unique.
- Assurer la continuité de votre activité : nos solutions intègrent tous les moteurs de protection pour répondre aux attaques les plus sophistiquées et des fonctions réseau pour la disponibilité des accès et la gestion SDWAN.
- Connecter vos collaborateurs qui disposent d'un accès sécurisé aux ressources de l'entreprise où qu'ils se trouvent et depuis n'importe quel terminal (accès distant pour télétravail).

SYSTANCIA

ETI GG OSE/OIV

FRANCE CYBER SECURITY

FRANCE CYBER SECURITY

Systancia Cleanroom
Anciennement IPdiva Cleanroom

SYSTANCIA CLEANROOM



Solution de surveillance des accès («Privileged Access Management», PAM) permettant aux organisations de contrôler les accès des utilisateurs à pouvoir ou des administrateurs à toutes les ressources de leur système d'information, en particulier les ressources les plus critiques. La solution offre la découverte des comptes, un accès protocolaire (Web, SSH, RDP) aux ressources informatiques, la traçabilité complète et l'enregistrement des sessions sans aucune infrastructure supplémentaire, le renforcement de l'authentification, l'injection des identifiants de connexion (évitant de les communiquer), une recherche avancée d'une action particulière dans l'ensemble des sessions enregistrées, etc.

SYSTANCIA

PME ETI GG OSE/OIV

FRANCE CYBER SECURITY

Systancia Cleanroom session

CLEANROOM SESSION SERVICE



Solution de surveillance des accès en service cloud («Privileged Access Management», PAM as a Service) permettant aux organisations de contrôler les accès des utilisateurs à pouvoir ou des administrateurs à toutes les ressources de leur SI, en particulier les plus critiques. La solution offre la découverte des comptes, un accès protocolaire (Web, SSH, RDP) aux ressources informatiques, l'enregistrement des sessions sans aucune infrastructure supplémentaire, etc. Disponible via le cloud public, dans un mode « self-service » permettant de démarrer l'usage en quelques minutes, cette solution permet aux organisations de gérer leurs besoins de surveillance des accès en toute autonomie.

RÉSEAUX

Solutions pour la sécurisation des réseaux et des flux réseaux VPN, Firewall, CNS, etc.



The image shows the Systancia logo at the top left. Below it are three green bars representing different categories: ETI, GG, and OSE/OIV. To the right are two circular logos: 'VISA DE SÉCURITÉ' and 'ANSSI'. At the bottom, there is a white box with the 'Systancia Gate' logo and the text 'Anciennement IPdiva Secure'.

SYSTANCIA GATE



Solution d'accès distant sécurisé («Zero Trust Network Access», ZTNA) des employés à tout leur environnement de travail (postes de travail, applications, données, infrastructures, etc.) en toute situation (télétravail, mobilité, astreinte, infogérance, prestation, etc.). La solution contrôle l'intégrité du terminal d'accès, contrôle l'accès aux applications de façon granulaire, et offre une fenêtre unique d'accès aux applications, même si elles sont déployées dans plusieurs datacenters/clouds. Elle assure aux entreprises une conformité à leur politique de sécurité, par une double barrière et un tunnel de confidentialité créé au moment de la connexion entre le terminal utilisateur et l'application, et potentiellement chiffré avec votre propre clé, par des flux uniquement sortant sans ouverture de ports réseaux, par une rupture protocolaire et un filtrage des interactions utilisateurs qui protègent des programmes malveillants.



The image shows the Systancia logo at the top left. Below it are four green bars representing different categories: PME, ETI, GG, and OSE/OIV. To the right are two circular logos: 'VISA DE SÉCURITÉ' and 'ANSSI', and a 'FRANCE CYBER SECURITY' logo. At the bottom, there is a white box with the 'Systancia Workroom session' logo and a green icon of a house with a Wi-Fi symbol and 'Ws'.

WORKROOM SESSION SERVICE



Solution d'accès distant sécurisé en service cloud («Zero Trust Network Access», ZTNA as a Service) des employés à tout leur environnement de travail (postes de travail, applications, données, infrastructures, etc.) en toute situation (télétravail, mobilité, astreinte, infogérance, prestation, etc.). La solution contrôle l'intégrité du terminal d'accès, contrôle l'accès aux applications de façon granulaire, et offre une fenêtre unique d'accès aux applications. Disponible via le cloud public, dans un mode « self-service » permettant de démarrer l'usage en quelques minutes, cette solution permet aux organisations de gérer leurs besoins d'accès distant sécurisé en toute autonomie.



The image shows 'THE GREENBOW' logo at the top left. Below it are four green bars representing different categories: PME, ETI, GG, and OSE/OIV. To the right are two circular logos: 'VISA DE SÉCURITÉ' and 'ANSSI', and a 'FRANCE CYBER SECURITY' logo. At the bottom, there is a large green shield icon with a white outline.

LE VPN FRANÇAIS



Référencé dans plusieurs marchés UGAP, le VPN Français est une offre destinée à tous les organismes publics français qui ont besoin de protéger les connexions à distance de leurs collaborateurs. Quel que soit le nombre de postes à équiper et quelle que soit la durée d'engagement, les clients VPN TheGreenBow sont proposés au prix unique de moins d'un euro par mois par poste utilisateur.

Faciles à installer et simples à utiliser, ils sont disponibles pour Windows, Linux, Android, iOS et macOS. Également disponibles en version certifiée pour Windows et Linux, ils sont interopérables avec d'autres équipements qui disposent aussi de visas de sécurité ANSSI pour répondre aux exigences d'organismes ayant le statut d'OIV/OSE.

RÉSEAUX

Solutions pour la sécurisation des réseaux et des flux réseaux VPN, Firewall, CNS, etc.



TheGreenBow logo featuring a green shield with a white mountain range. Below it are three green bars labeled ETI, GG, and OSE/OIV. To the right are logos for VISA DE SÉCURITÉ, ANSSI, and FRANCE CYBER SECURITY.

SÉCURISATION ET REMÉDIATION DES SOLUTIONS DE TÉLÉTRAVAIL



Afin d'aider les grandes entreprises et collectivités à évaluer le niveau de sécurité de leur SI, renforcer leur cybersécurité ou encore sécuriser l'accès aux ressources pour leurs collaborateurs nomades, TheGreenBow et Sogeti ont associé leurs expertises pour proposer une offre dédiée à la sécurisation et à la remédiation des solutions de télétravail.

Cette offre comprend :

- l'audit des infrastructures et équipements VPN réalisé par Sogeti ;
- la mise en œuvre technique de propositions d'amélioration ;
- le déploiement et l'intégration de Clients VPN TheGreenBow.

Nos clients VPN sont disponibles pour Windows, Linux, Android, iOS et macOS. Une version disposant d'un un Visa de l'ANSSI est proposée pour Windows et Linux.



Tranquil IT logo featuring a blue triangle with a white mountain range. Below it are four green bars labeled PME, ETI, GG, and OSE/OIV. To the right are logos for VISA DE SÉCURITÉ, ANSSI, and FRANCE CYBER SECURITY. At the bottom is the WAPT Enterprise logo.

WAPT



WAPT installe, met à jour et supprime les logiciels et les configurations sur les appareils Windows, Linux et macOS. Le déploiement de logiciels (Firefox, MS Office, etc.) peut être effectué à partir d'un serveur central à l'aide d'une console graphique.

Des entreprises privées de toutes tailles, des écoles, des universités, des CNRS, des gouvernements locaux et nationaux, des hôpitaux, des mairies et des ministères d'État du monde entier utilisent avec succès WAPT.

WAPT est très efficace pour répondre aux besoins récurrents de mise à jour de Firefox ou Chrome et c'est souvent pour couvrir ce besoin de base que WAPT est initialement adopté ; il devient alors un outil de choix pour les tâches quotidiennes de l'administrateur système.



ENTREPRISE

Solutions/applications de télétravail « secure by design »

Plateforme collaborative, communication sécurisée, signature électronique, etc.



ATOS



IDNOMIC DIGITAL SIGNATURE

Atos

Dans le contexte actuel, les organisations recherchent des solutions accélérant numériquement les processus papier traditionnels, qu'il s'agisse de contrats, de factures ou de dossiers RH. Les solutions de signature électronique peuvent aider à améliorer l'intégrité des documents numérisés et à garantir l'identité du signataire. Atos propose des solutions de :

- Signature électronique (IDnomic metasign) offrant aux employés le bon niveau de signature électronique (avancé et qualifié), conforme à la réglementation eIDAS,
- Horodatage (IDnomic metatime) permettant l'ajout d'une date et heure sûres associées à un document, apportant un élément de preuve,
- Identité numérique de confiance (IDnomic IDPKI) assurant l'intégrité de l'identité numérique liée à la signature, partie de l'offre labellisée France Cybersecurity.



DOCAPOSTE



SIGNATURE ÉLECTRONIQUE

DOCAPOSTE

La gamme signature de Docaposte permet de déployer des solutions de signature de niveau simple, avancé et qualifié. Accessibles en mode SaaS, API et sur projet sur-mesure, les solutions Docaposte s'adaptent à tous vos besoins et ce peu importe la taille et le secteur de votre organisation. Avec une chaîne de confiance 100% intégrée, bénéficiez de l'ensemble des certificats proposés par notre Autorité de Certification Certinomis, ainsi que de notre système d'archivage électronique à vocation probatoire permettant de garantir l'intégrité et l'opposabilité de vos documents signés dans le temps.



ERCOM



CITADEL TEAM

ERCOM
a Thales company

Basé sur des technologies robustes et sur le savoir-faire de Thales, le service Citadel Team est une alternative souveraine et de confiance aux outils grand public de messagerie, d'audio et visio-conférence pour les professionnels. L'application garantit un haut niveau de sécurité et est en cours de qualification élémentaire par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information). Aujourd'hui, la communauté Citadel Team représente des dizaines de milliers de membres parmi plus de 50 entreprises et organisations.

ENTREPRISE

Solutions/applications de télétravail « secure by design »

Plateforme collaborative, communication sécurisée, signature électronique, etc.



ERCOM



CRYPTOBOX



Cryptobox est la solution de travail collaboratif et de transfert de fichiers agréée Diffusion Restreinte par l'ANSSI qui chiffre vos données de bout en bout, disponible dans n'importe quel environnement, Cloud ou On Premise. Vos documents sont alors accessibles de manière totalement sécurisée depuis votre PC, smartphone et tablette.

Aucun risque de piratage de vos données puisqu'elles sont chiffrées depuis votre terminal jusqu'au stockage et que votre mot de passe n'est stocké sur aucun serveur.



LEX PERSONA



CACHETER



Permet aux personnes morales de cacheter des données émises tout en s'adaptant aux contraintes de sécurité et de souveraineté des données. idéal pour :

- Un grand volume de données.
- Des contraintes de sécurité et de souveraineté des données élevées.

Logiciel pour serveurs Windows ou Linux et déployable :
En mode Shell / En mode Web service / En mode API / En mode batch / Compatible avec un certificat hébergé ou local



LEX PERSONA



FAIRE SIGNER



Plateforme personnalisable pour faire signer tous vos cas d'usages.

Portail et API avec signature électronique sans transmission des documents.
Intégration France Connect
Signature de tout type de document aux formats XAdES, CAdES et PAdES.
Signature avancées à la volée ou qualifiées eIDAS (tokens, carte à puce).
API de signature électronique certifiée par l'ANSSI (CSPN).
Accompagnement individualisé lors du déploiement.

ENTREPRISE

Solutions/applications de télétravail « secure by design »

Plateforme collaborative, communication sécurisée, signature électronique, etc.



LEX
PERSONA



SIGNER



Un logiciel bureautique pour prendre l'initiative et apposer votre signature électronique en illimité sur tous vos documents.

Solution idéale pour les personnes physiques qui souhaitent disposer d'un contrôle total sur la signature électronique des documents sur lesquels elles s'engagent comme des réponses aux appels d'offres, les attestations, les PV de contrôle qualité... Cet outil permet également la dématérialisation fiscale des factures, la réalisation de copies fiables et de copies fiscales.

Logiciel disponible pour Mac & PC. Il est compatible avec des certificats de personnes physiques au format logiciel ou sur support cryptographique.



NET
EXPLORER



NET EXPLORER



NetExplorer est une solution Cloud clé en main de stockage et partage documentaire.

NetExplorer vous permet notamment de : Partager des fichiers, sans limite de taille / Collaborer en temps réel sur des documents avec vos équipes / Valider et signer des documents en ligne / Sécuriser et protéger vos données / Accéder à distance à l'ensemble de vos fichiers, en toute sécurité, même en télétravail

Acteur 100% français, la sécurité est au coeur de notre activité : Hébergement dans 2 datacenters en France / Solution certifiée ISO 27001 / SLA 99,9% garantie / Sauvegarde sur site distant incluse dans toutes nos offres / Solution conforme au RGPD



PRIVATE
DISCUSS



PRIVATE DISCUSS



Private Discuss est une plateforme de communication collaborative, utilisée pour les visioconférences, les webinaires ou encore le télétravail.

Véritable bureau hybride et ergonomique, Private Discuss est chiffrée de bout-en-bout et conforme RGPD, elle se démarque des solutions étrangères en proposant une plateforme complète grâce à ses fonctionnalités nombreuses et inédites, mais aussi en promouvant la souveraineté numérique et le savoir-faire technologique et cyber français.

Conçue à partir de technologies 100% propriétaires, sur les algorithmes les plus puissants du marché et hébergée sur des serveurs français, Private Discuss vous garantit la protection robuste de vos données et une entière satisfaction lors de son utilisation.

ENTREPRISE

Solutions/applications de télétravail « secure by design »

Plateforme collaborative, communication sécurisée, signature électronique, etc.



The image shows a red background with the TIXEO logo at the top left. Below it are four vertical bars of increasing height labeled 'PME', 'ETI', 'GG', and 'OSE/OIV'. To the right are two circular logos: 'VISA DE SECURITE' and 'FRANCE CYBER SECURITY'. At the bottom is a photograph of a person in a light blue shirt sitting at a desk, looking at a large monitor displaying a video conference with several participants. A small TIXEO FUSION logo is overlaid on the bottom right of the photo.

TIXEO FUSION



L'offre TixeoFusion accompagne les organisations dans leur stratégie de déploiement du télétravail généralisé. Ce mode de collaboration propose aux équipes un espace vidéo-collaboratif sécurisé permettant de conserver le lien social durant toute une journée de travail sans subir les désagréments d'une visioconférence intrusive.

Au sein d'un véritable open-space virtuel, vos équipes s'organisent en plusieurs groupes de discussion indépendants respectivement matérialisés par une couleur distincte.

TixeoFusion offre un véritable chiffrement de bout en bout des communications (vidéo, audio et data) assurant ainsi la confidentialité de vos échanges. Tixeo intègre l'unique technologie de visioconférence à être certifiée et qualifiée par l'ANSSI.



ENTREPRISE

Solutions de sécurisation de l'accès aux ressources de l'entreprise.

IAM, ZTNA, PAM, MFA, etc.



ATOS



Evidian

EVIDIAN WAM

Atos

Evidian Web Access Manager: Fournisseur d'identité (Identity Provider) pour les applications web supportant les protocoles SAMLv2, OpenId Connect, OAuth2.0. Egalement capable de protéger les applications Web traditionnelles (internes, externes ou dans le Cloud). Evidian WAM gère le contrôle d'accès de tous les utilisateurs quel que soit leur lieu de connexion et le terminal employé. Il embarque également un catalogue de méthodes d'authentification forte intégré, comprenant divers OTP, l'authentification Push, FIDO2, les certificats X509, les cartes PKI, France Connect et ProSanté Connect.

Grace à l'option mobile-eSSO, les comptes protégées en internes, le sont également pour un accès externe, en utilisant une authentification appropriée.



ATOS



Evidian

EVIDIAN IDAAS

Atos

Evidian IDaaS est une offre de contrôle d'accès aux applications web et mobile des entreprises. Elle est disponible entièrement « as a Service », opérée depuis la France par Evidian. Evidian IDaaS pré-intègre les plus grandes applications commerciales pour une mise à disposition immédiate aux utilisateurs.

Un catalogue de méthodes d'authentification fortes prêtes à l'usage est également inclus dans l'offre, qui comprend : FIDO2, X509 (cartes PKI), OTP, TOTP, Mobile Push...

La gestion des utilisateurs peut se faire au travers de l'interface web, de l'API SCIM ou encore par glisser-déposer de fichiers texte.

Evidian IDaaS protège les applications et les utilisateurs quelque soit leur contexte et le terminal utilisé lors de la connexion.



CHAMBERSIGN



CRYPTOSMART
BY ERCOM

SERVICE DE CERTIFICATION ÉLECTRONIQUE

ChamberSign
Autorité de certification

Identités numériques permettant l'authentification forte des personnes morales et physiques rattachées à une organisation ainsi que la signature électronique et le scellement des données.

- Avec un seul et même outil, le collaborateur peut s'authentifier de façon sécurisée à son poste de travail, sa session Windows et à ses différents services web. Il peut également signer électroniquement tous types de documents et certifier ses emails.

- Les certificats électroniques de la personne morale permettent d'authentifier de manière certaine l'organisation et ainsi instaurer la confiance dans les échanges électroniques puisqu'ils assurent l'entière confidentialité et l'intégrité des données transmises.

ENTREPRISE

Solutions de sécurisation de l'accès aux ressources de l'entreprise.

IAM, ZTNA, PAM, MFA, etc.



DOCAPOSTE



L'Identité Numérique

IDENTITÉ NUMÉRIQUE



L'Identité numérique La Poste est une preuve d'identité en digital.

C'est une clé universelle permettant de s'identifier et de s'authentifier avec un identifiant, un mot de passe et un code secret unique. Déjà présente sur des centaines de sites via France Connect, L'Identité Numérique est la première et unique solution certifiée de niveau substantiel selon le règlement iIDAS par l'ANSSI. L'utilisation de l'application L'Identité Numérique La Poste est donc équivalente à un face à face physique.



DOCAPOSTE



EUKLES

UNE MARQUE DE DOCAPOSTE

TITAN PAR EUKLES



Le Titan, appliance haute sécurité, protège le patrimoine documentaire de l'entreprise. Permettant de conserver la valeur probatoire des documents électroniques en interne, ce système de coffre fabriqué en France par Eukles est conçu dans un boîtier testé à toute épreuve.

Le Titan comprend les deux solutions GED et Backup éditées par Eukles, mettant à l'abri en cloud privé les données de l'entreprise.



ERCOM



CITADEL TEAM

CITADEL TEAM



Basé sur des technologies robustes et sur le savoir-faire de Thales, le service Citadel Team est une alternative souveraine et de confiance aux outils grand public de messagerie, d'audio et visio-conférence pour les professionnels. L'application garantit un haut niveau de sécurité et est en cours de qualification élémentaire par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information). Aujourd'hui, la communauté Citadel Team représente des dizaines de milliers de membres parmi plus de 50 entreprises et organisations.

ENTREPRISE

Solutions de sécurisation de l'accès aux ressources de l'entreprise.

IAM, ZTNA, PAM, MFA, etc.

ERCOM

VISA DE SÉCURITÉ

FRANCE CYBER SECURITY

PMI ETI GG OSE/OIV

CRYPTOSMART BY ERCOM

CRYPTOSMART MOBILE



CRYPTOSMART MOBILE est l'unique solution, développée en partenariat avec SAMSUNG, qui sécurise vos communications, données, terminaux mobiles, avec un niveau de sécurité élevé (agrément Diffusion Restreinte délivré par l'ANSSI*), sur des smartphones et tablettes grand public de dernière génération.

Grâce au chiffrement de bout en bout, vos données sont protégées contre les risques d'interception des communications, la perte ou de vol de votre smartphone.

ERCOM

VISA DE SÉCURITÉ

FRANCE CYBER SECURITY

PMI ETI GG OSE/OIV

CRYPTOSMART BY ERCOM

CRYPTOSMART PC



Pour faire face aux nouveaux enjeux de mobilité et de travail à distance, Ercom a développé Cryptosmart PC, une solution souveraine de VPN pour sécuriser les connexions de vos ordinateurs Windows distants.

Cryptosmart PC s'appuie sur les briques technologiques reconnues de Cryptosmart mobile, solution historique d'Ercom qui sécurise les communications, données et terminaux mobiles.

Cette solution VPN est d'ores et déjà utilisée sur le marché pour garantir l'intégrité et la sécurité des données échangées, à distance, par vos salariés.

HARMONIE TECHNOLOGIE

FRANCE CYBER SECURITY

PMI ETI GG OSE/OIV

Conseil Cyber pour sécuriser le télétravail

CONSEIL ET SERVICE CYBER



Spécialiste de la cybersécurité et de la gestion des risques nous accompagnons les plus grandes entreprises françaises dans leur programme de transformation SSI pour renforcer leur sécurité et la résilience tout en améliorant leur performance grâce à l'adoption des nouveaux usages : télétravail, Cloud, RPA, Open Data, ...

Avec la double compétence fonctionnelle et technique, nous intervenons auprès des filières Risque et Contrôle, Sécurité de l'Information et des Directions Informatiques pour :

- organiser la maîtrise des risques cyber ;
- cadrer les programmes de sécurité ;
- intégrer les solutions de gestion des identités, accès et des données ;
- auditer la sécurité organisationnelle, fonctionnelle et technique (scan, pentest, red team).

ENTREPRISE

Solutions de sécurisation de l'accès aux ressources de l'entreprise.

IAM, ZTNA, PAM, MFA, etc.

KEOPASS

PME ETI GG OSE/OIV

A hand holding a KeoPass biometric key in front of a laptop screen displaying a login form with fields for 'Enter Password' and 'LOG IN'.

CLÉ BIOMÉTRIQUE



La Clé KeoPass est un dispositif biométrique portable, autonome et décentralisé, pour le contrôle d'accès logique et physique, ne nécessitant pas d'intégration logicielle, ni de modification d'infrastructure matérielle.

La Clé KeoPass permet de sécuriser le poste de travail par les empreintes digitales de son utilisateur et de le verrouiller automatiquement en cas d'éloignement. Elle est le complément idéal d'un VPN, SSO et AD pour sécuriser les accès aux ressources de l'entreprise.

Doté d'un gestionnaire de mots de passe web avec vérification d'URL, la Clé KeoPass est un rempart contre le hameçonnage et les attaques par force brute ou ingénierie sociale; elle facilite et sécurise l'authentification des utilisateurs et réduit les appels hotline.

NEXUS

ETI GG OSE/OIV

A diagram showing a central shield icon with a checkmark, connected to various icons representing users, applications, and services like AD, HR, and SSO.

NEXUS DIGITAL ACCESS



Nexus Digital Access permet d'implémenter des moyens d'authentification forte multi-facteurs afin de garantir un accès distant sécurisé aux applications internes et/ou Cloud des entreprises pour l'ensemble de leurs collaborateurs. La solution Digital Access offre de multiples fonctionnalités qui incluent :

- des moyens d'authentification (personal mobile push notification, OTP SMS, SW token, Mobile virtual Smart Card , HW OTP token...)
- Un portail dédié à la présentation des applications autorisées
- La fédération et l'orchestration des identités (SAML, Open ID connect)
- L'identification unique via SSO

Tous ces services sont à disposition des entreprises afin de leur garantir en télétravail ou en accès distant le niveau de sécurité optimal.

STORMSHIELD

PME ETI GG OSE/OIV

VISA DE SÉCURITÉ

Stormshield Network Security
Une gamme de pare-feux & VPN de nouvelle génération

Le Stormshield : des performances inégalées au meilleur coût

Production de tous les environnements IT/OT et Cloud en une gamme complète et un seul logiciel d'administration

A product image of a Stormshield Network Security device.

STORMSHIELD NETWORK SECURITY



La gamme de pare-feux Stormshield Network Security, qualifiée par l'ANSSI, est axée sur la sécurité des réseaux informatiques, et se compose de boîtiers physiques ou d'appliances virtuelles qui permettent de :

- Protéger vos infrastructures IT des menaces internes comme externes, grâce à une technologie de protection proactive unique.
- Assurer la continuité de votre activité : nos solutions intègrent tous les moteurs de protection pour répondre aux attaques les plus sophistiquées et des fonctions réseau pour la disponibilité des accès et la gestion SDWAN.
- Connecter vos collaborateurs qui disposent d'un accès sécurisé aux ressources de l'entreprise où qu'ils se trouvent et depuis n'importe quel terminal (accès distant pour télétravail).

ENTREPRISE

Solutions de sécurisation de l'accès aux ressources de l'entreprise.

IAM, ZTNA, PAM, MFA, etc.



SYSTANCIA

ETI GG OSE/OIV

FRANCE CYBER SECURITY

Systancia Cleanroom
Anciennement IPdiva Cleanroom

SYSTANCIA CLEANROOM



Solution de surveillance des accès («Privileged Access Management», PAM) permettant aux organisations de contrôler les accès des utilisateurs à pouvoir ou des administrateurs à toutes les ressources de leur système d'information, en particulier les ressources les plus critiques. La solution offre la découverte des comptes, un accès protocolaire (Web, SSH, RDP) aux ressources informatiques, la traçabilité complète et l'enregistrement des sessions sans aucune infrastructure supplémentaire, le renforcement de l'authentification, l'injection des identifiants de connexion (évitant de les communiquer), une recherche avancée d'une action particulière dans l'ensemble des sessions enregistrées, etc.



SYSTANCIA

PME ETI GG OSE/OIV

FRANCE CYBER SECURITY

Systancia Cleanroom session

CLEANROOM SESSION SERVICE



Solution de surveillance des accès en service cloud («Privileged Access Management», PAM as a Service) permettant aux organisations de contrôler les accès des utilisateurs à pouvoir ou des administrateurs à toutes les ressources de leur SI, en particulier les plus critiques. La solution offre la découverte des comptes, un accès protocolaire (Web, SSH, RDP) aux ressources informatiques, l'enregistrement des sessions sans aucune infrastructure supplémentaire, etc. Disponible via le cloud public, dans un mode « self-service » permettant de démarrer l'usage en quelques minutes, cette solution permet aux organisations de gérer leurs besoins de surveillance des accès en toute autonomie.



SYSTANCIA

ETI GG OSE/OIV

VISA DE SÉCURITÉ

FRANCE CYBER SECURITY

Systancia Gate
Anciennement IPdiva Secure

SYSTANCIA GATE



Solution d'accès distant sécurisé («Zero Trust Network Access», ZTNA) des employés à tout leur environnement de travail (postes de travail, applications, données, infrastructures, etc.) en toute situation (télétravail, mobilité, astreinte, infogérance, prestation, etc.). La solution contrôle l'intégrité du terminal d'accès, contrôle l'accès aux applications de façon granulaire, et offre une fenêtre unique d'accès aux applications, même si elles sont déployées dans plusieurs datacenters/clouds. Elle assure aux entreprises une conformité à leur politique de sécurité, par une double barrière et un tunnel de confidentialité créé au moment de la connexion entre le terminal utilisateur et l'application, et potentiellement chiffré avec votre propre clé, par des flux uniquement sortant sans ouverture de ports réseaux, par une rupture protocolaire et un filtrage des interactions utilisateurs qui protègent des programmes malveillants.

ENTREPRISE

Solutions de sécurisation de l'accès aux ressources de l'entreprise.

IAM, ZTNA, PAM, MFA, etc.



The image shows a red background with the Systancia logo at the top left. Below it are four green bars representing different categories: PME, ETI, GG, and OSE/OIV. To the right of these bars are two circular logos: one for VISA DE SÉCURITÉ and another for FRANCE CYBER SECURITY. At the bottom, there is a white box containing the text 'Systancia Workroom session' and a green icon of a house with a Wi-Fi signal and the letters 'Ws'.

WORKROOM SESSION SERVICE



Solution d'accès distant sécurisé en service cloud («Zero Trust Network Access», ZTNA as a Service) des employés à tout leur environnement de travail (postes de travail, applications, données, infrastructures, etc.) en toute situation (télétravail, mobilité, astreinte, infogérance, prestation, etc.). La solution contrôle l'intégrité du terminal d'accès, contrôle l'accès aux applications de façon granulaire, et offre une fenêtre unique d'accès aux applications. Disponible via le cloud public, dans un mode « self-service » permettant de démarrer l'usage en quelques minutes, cette solution permet aux organisations de gérer leurs besoins d'accès distant sécurisé en toute autonomie.



ENTREPRISE

Solutions pour la sécurisation des ressources elles-mêmes.
SIEM, détections, réponse, sauvegarde sécurisée, etc.



AIRBUS



ORION MALWARE

AIRBUS

Orion Malware permet la détection et l'analyse des malwares qui circulent sur les systèmes d'information. Il permet de prévenir le risque et de répondre aux incidents grâce à ses moteurs de détection complémentaires et à ses rapports d'analyses actionnables. Votre chaîne de sécurité est renforcée via le partage des informations avec vos autres équipements de sécurité. Orion Malware est un soutien pour toutes vos équipes de cybersécurité et s'adapte à chaque cas d'usage métier SOC, CSIRT/CERT, TI.

Il intègre des antivirus et développe des moteurs d'analyse statique avec machine learning et de l'analyse dynamique dans le but de repérer les malwares les plus furtifs.

Orion Malware vous fait gagner un temps précieux dans la réponse à incident grâce aux rapports d'analyse. Les rapports fournissent un niveau global de risque, exposent les tactiques et techniques des malwares, permettent l'export des IOC pour prévenir les futures attaques ou les contenir en cas d'incident.

Ces rapports peuvent être exportés vers les centres de supervision type SIEM et les indices de compromission extraits peuvent être partagés à travers une Threat Intelligence Platform.



ATOS



ATOS ENDPOINT PROTECTION

Atos

Les solutions traditionnelles de protection de terminaux visent à répondre aux menaces connues et présentent donc des angles morts. Elles ne permettent pas de contrer les menaces avancées et de répondre aux alertes complexes, comme le peuvent les services de Endpoint Detection and Response (EDR).

Atos Endpoint Protection fournit une protection complète contre les menaces ciblant tout type de terminaux (poste de travail, serveur et mobile). Les services Atos s'appuient sur des capacités de détection étendues, des équipes SOC et des outils de réponse dédiés.

Le service comprend :

- Intégration Security Information and Event Management (SIEM) pour une efficacité accrue et une réduction du temps d'intervention.
- Threat Hunting permettant d'identifier les menaces inconnues.
- EDR offrant une visibilité, détection et réponse continue et complète des terminaux.



ATOS



SOLUTIONS DE CHIFFREMENT TRUSTWAY

Atos

La protection des données est l'une des principales préoccupations de l'entreprise.

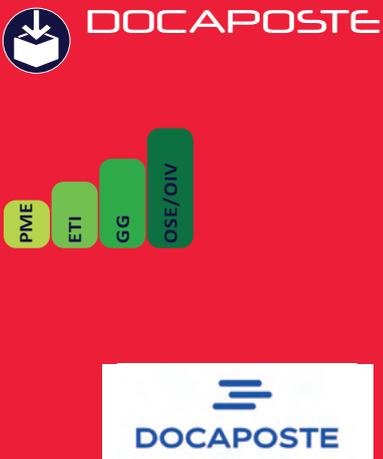
Atos aide les organisations à mettre en place une protection des données complète en commençant par le déploiement des solutions nécessaires pour assurer la confidentialité des données critiques :

- Modules Matériel de sécurité Trustway Proteccio pour assurer l'intégrité et la sécurité des opérations cryptographiques
- Sécurité des réseaux IP avec Trustway IP Protect, gamme de chiffreur réseau
- Chiffrement de tous formats et types de données (machines virtuelles, bases de données, fichier système, application et tokenisation) avec Trustway DataProtect

ENTREPRISE

Solutions pour la sécurisation des ressources elles-mêmes.

SIEM, détections, réponse, sauvegarde sécurisée, etc.



DOCAPOSTE

PMI
ETI
GG
OSE/OIV

DOCAPOSTE

SIGNATURE ÉLECTRONIQUE



La gamme signature de Docaposte permet de déployer des solutions de signature de niveau simple, avancé et qualifié. Accessibles en mode Saas, API et sur projet sur-mesure, les solutions Docaposte s'adaptent à tous vos besoins et ce peu importe la taille et le secteur de votre organisation. Avec une chaîne de confiance 100% intégrée, bénéficiez de l'ensemble des certificats proposés par notre Autorité de Certification Certinomis, ainsi que de notre système d'archivage électronique à vocation probatoire permettant de garantir l'intégrité et l'opposabilité de vos documents signés dans le temps.



ERCOM

PMI
ETI
GG
OSE/OIV

VISA DE SÉCURITÉ

ANSSI

FRANCE CYBER SECURITY

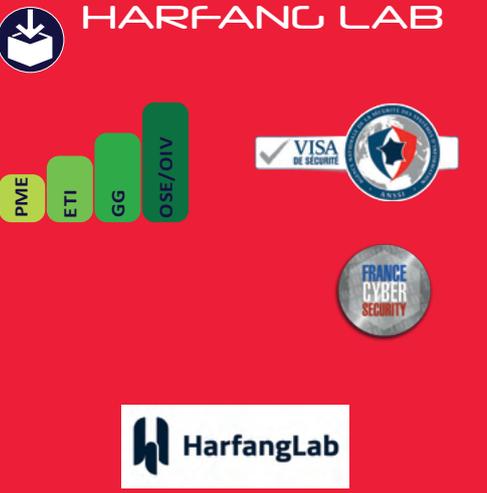
CRYPTOBOX
BY ERCOM

CRYPTOBOX



Cryptobox est la solution de travail collaboratif et de transfert de fichiers agréée Diffusion Restreinte par l'ANSSI qui chiffre vos données de bout en bout, disponible dans n'importe quel environnement, Cloud ou On Premise. Vos documents sont alors accessibles de manière totalement sécurisée depuis votre PC, smartphone et tablette.

Aucun risque de piratage de vos données puisqu'elles sont chiffrées depuis votre terminal jusqu'au stockage et que votre mot de passe n'est stocké sur aucun serveur.



HARFANG LAB

PMI
ETI
GG
OSE/OIV

VISA DE SÉCURITÉ

ANSSI

FRANCE CYBER SECURITY

HarfangLab

HARFANGLAB EDR



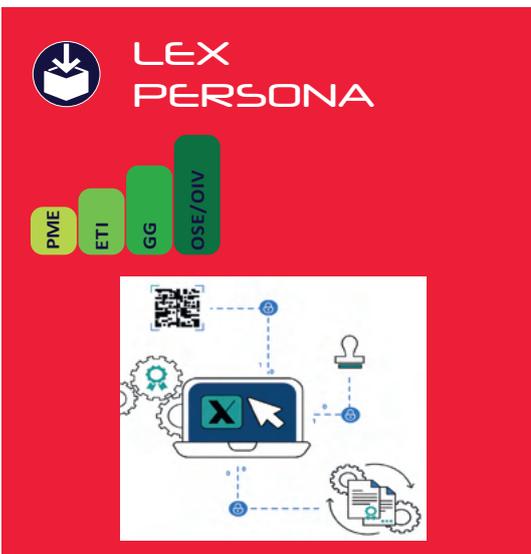
HarfangLab, éditeur d'un logiciel EDR (Endpoint Detection and Response), technologie qui permet d'anticiper et neutraliser les cyberattaques modernes et inconnues, sur ordinateurs et serveurs.

Certifié par ANSSI depuis 2020, HarfangLab compte parmi ses clients de grandes entreprises d'envergure internationale, évoluant dans des secteurs très sensibles. HarfangLab EDR se distingue par : l'ouverture de sa solution qui s'intègre nativement à toutes les autres briques de sécurité grâce à son API ; par sa transparence, car les données collectées par l'EDR restent accessibles et par l'indépendance numérique qu'il offre, car ses clients sont libres de choisir leur mode d'hébergement : cloud, public ou privé, ou dans leur propre infrastructure.

ENTREPRISE

Solutions pour la sécurisation des ressources elles-mêmes.

SIEM, détections, réponse, sauvegarde sécurisée, etc.



LEX PERSONA

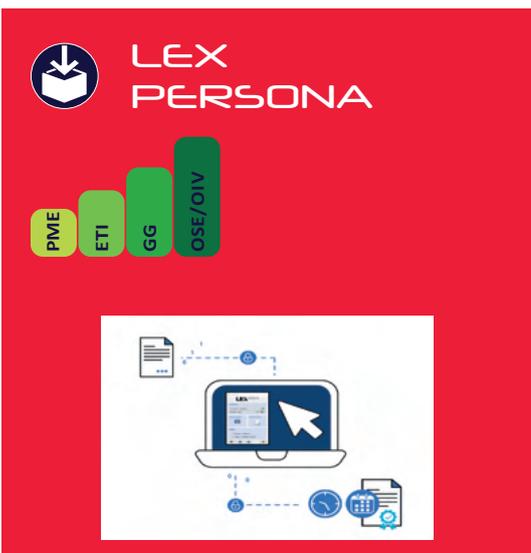
PME ETI GG OSE/DIV

CACHETER



Permet aux personnes morales de cacheter des données émises tout en s'adaptant aux contraintes de sécurité et de souveraineté des données.
idéal pour :
-Un grand volume de données.
-Des contraintes de sécurité et de souveraineté des données élevées.

Logiciel pour serveurs Windows ou Linux et déployable :
En mode Shell / En mode Web service / En mode API / En mode batch /
Compatible avec un certificat hébergé ou local



LEX PERSONA

PME ETI GG OSE/DIV

SIGNER



Un logiciel bureautique pour prendre l'initiative et apposer votre signature électronique en illimité sur tous vos documents.

Solution idéale pour les personnes physiques qui souhaitent disposer d'un contrôle total sur la signature électronique des documents sur lesquels elles s'engagent comme des comme les réponses aux appels d'offres, les attestations, les PV de contrôle qualité... Cet outil permet également la dématérialisation fiscale des factures, la réalisation de copies fiables et de copies fiscales.

Logiciel disponible pour Mac & PC. Il est compatible avec des certificats de personnes physiques au format logiciel ou sur support cryptographique.



OXIBOX

PME ETI GG

OXIBOX



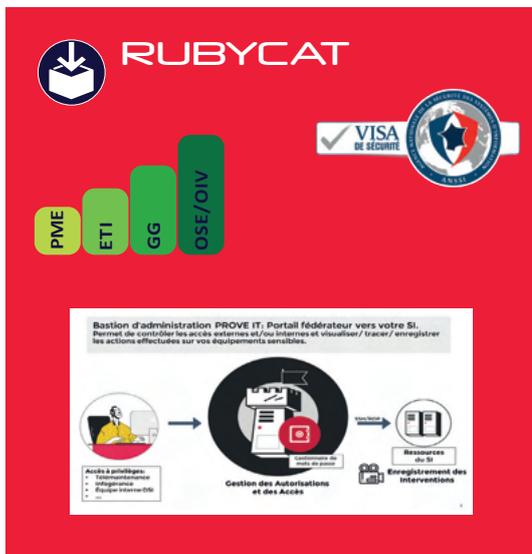
Oxibox permet aux entreprises de redémarrer leurs systèmes immédiatement après une cyberattaque ou un ransomware. Les solutions de sauvegarde et de protection des données ne suffisent plus à garantir la pérennité des systèmes face à l'explosion des menaces cyber. La technologie innovante d'Oxibox permet de répondre à cet enjeu par la création d'enclaves sécurisées qui garantissent l'immutabilité des données y étant déposées. Les sauvegardes sont ainsi rendues résistantes aux ransomwares.

Oxibox est multi-sources : la solution inclut la sauvegarde des données sur site, celle des postes nomades ainsi que les services cloud.
Plus de 1200 clients privés et publics nous font confiance pour la protection de leur SI.

ENTREPRISE

Solutions pour la sécurisation des ressources elles-mêmes.

SIEM, détections, réponse, sauvegarde sécurisée, etc.



RUBYCAT

VISA DE SÉCURITÉ

PMIE ETI GG OSE/OIV

Bastion d'administration PROVE IT. Portail fédérateur vers votre SI. Permet de contrôler les accès externes et/ou internes et visualiser/tracer/enregistrer les actions effectuées sur vos équipements sensibles.

Accès privilégiés, Intégration, Réponse d'Incidents

Gestion des Autorisations et des Accès

Ressources du SI

Enregistrement des Interventions

BASTION D'ADMINISTRATION PROVE IT



Renforcez la sécurité des accès sensibles au SI avec PROVEIT

PROVE IT est une solution logicielle de type « bastion-PAM » certifiée Visa de sécurité ANSSI. Elle contrôle, trace et enregistre les actions réalisées par les comptes à privilèges sur le SI (accès internes et externes). Tracer les accès sensibles à vos équipements critiques est important cf RGPD, certification HDS, ISO 27001, guide de sécurisation du SI de l'ANSSI,...

PROVE IT est non invasive, simple à déployer et facile à administrer ; comprend API REST et segmentation des droits - version Cluster Licence uniquement dimensionnée au nombre de sessions concomitantes.

Licence POC gratuite – webinaires de démo sur le site RUBYCAT.



SOGETI

VISA DE SÉCURITÉ

ETI GG OSE/OIV

FRANCE CYBER SECURITY

sogeti THEGREENBOW

Protégez les connexions de vos collaborateurs en accès distant

SÉCURISATION ET REMÉDIATION DES SOLUTIONS DE TÉLÉTRAVAIL

SÉCURISATION ET REMÉDIATION DES SOLUTIONS DE TÉLÉTRAVAIL



Vos enjeux

- Evaluer le niveau de sécurité de votre système d'information.
- Renforcer votre cybersécurité.
- Sécuriser l'accès à vos ressources pour vos collaborateurs nomades.

Une offre modulaire comprenant :

- L'audit par Sogeti des infrastructures de télétravail.
- L'accompagnement dans la mise en œuvre des propositions d'amélioration et des projets de sécurisation des solutions de télétravail.
- Le déploiement et l'intégration de clients VPN TheGreenBow (réputés pour leur niveau de sécurité, leur facilité d'installation et leur simplicité d'utilisation), technologie validée par des visas de sécurité de l'ANSSI.



THE GREENBOW

VISA DE SÉCURITÉ

PMIE ETI GG OSE/OIV

FRANCE CYBER SECURITY



CLIENT VPN THEGREENBOW



Pour des besoins aussi variés que la protection de connexions en télétravail ou avec des objets connectés, ou encore la sécurisation de communications critiques, TheGreenBow propose 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. Une version certifiée pour Windows et Linux permet de répondre aux exigences de sécurisation des communications des grandes organisations, OIV, OSE et administrations.



ACCOMPAGNEMENT ORGANISATIONNEL

Audit/Bug Bounty/Pentest, formation, sensibilisation, conseil, intégration

AIRBUS

ETI GG OSE/OIV

FRANCE CYBER SECURITY

CYBERRANGE

CYBERRANGE



La CyberRange est une plateforme d'intégration et de simulation de systèmes IT/OT. Elle permet de modéliser des systèmes complexes virtuels et physiques proches de votre environnement de production, de simuler des activités représentatives de vos opérations, d'effectuer des tests de pénétration en environnement isolé et de jouer des scénarios réalistes, sans délai (plug & play) et en mode collaboratif, comprenant de véritables cyberattaques.

Une interface WEB simplifie la modélisation, le déploiement d'infrastructures virtualisées

et l'exécution de scénarios d'attaques La CyberRange intègre également des bibliothèques prêtes à l'emploi et permet d'intégrer vos contenus déjà existants, ou ceux disponibles directement sur le « market place » internet.

CyberRange est disponible en SaaS, OnPremise, ou via caisson mobile. Airbus CyberSecurity peut apporter des services complémentaires sur la construction d'infrastructure, scénarios et offre de formation en CyberSécurité.

AVANT DE CLIQUER

PME ETI GG OSE/OIV

AUDIT DE VULNÉRABILITÉ

BOUCLIER ALERTE CYBER

PLATEFORME DE E-LEARNING

MAILS ET SMS D'APPRENTISSAGE

Une pédagogie innovante pour développer des réflexes de cybersécurité. La sensibilisation sur poste de travail créée sur mesure pour chaque utilisateur.

SOLUTION DE SENSIBILISATION À LA CYBERSÉCURITÉ FACE AU PHISHING SUR POSTE DE TRAVAIL



Avant de Cliquer développe une culture de cybersécurité avec des outils autonomes, accessibles à tous, immédiatement opérationnels et inter-services. Après un audit de vulnérabilité, Avant de Cliquer déploie un programme de sensibilisation au phishing basé sur l'apprentissage par l'action, créé sur mesure pour chaque utilisateur et animé sur la durée sans intervention de votre part.

Ainsi, Avant de Cliquer installe une solution SaaS développant des algorithmes intelligents associant audit de vulnérabilité, plateforme de e-learning, envoi de mails d'apprentissage et process d'alerte cyber pour les SI pour automatiser une solution complète de sensibilisation à la cybersécurité phishing.

CORALIUM

PME ETI GG

Coralium

PACK « TÉLÉTRAVAILLEZ EN TOUTE SÉCURITÉ »



Coralium est un cabinet de conseil en sécurité informatique. Notre volonté est de rendre la cybersécurité accessible à toutes les entreprises, quelle que soit la taille ou le système d'information.

Les usages évoluent, et le système d'information doit suivre ! Vos employés télétravaillent depuis peu, la multiplication des attaques vous inquiète ? Nous proposons un pack « Télétravaillez en toute sécurité » pour vous redonner confiance et accélérer votre transformation numérique.

Le pack comprend un audit de vos pratiques du nomadisme et du travail à distance, un livret de recommandations et bonnes pratiques, une formation à destination de vos employés sur les bonnes pratiques de sécurité en télétravail ainsi qu'une évaluation de leur niveau de sensibilisation aux risques engendrés par le travail à distance.

ACCOMPAGNEMENT ORGANISATIONNEL

Audit/Bug Bounty/Pentest, formation, sensibilisation, conseil, intégration



DOCAPOSTE



SOFTEAM
UNE MARQUE DE DOCAPOSTE

SOFTEAM



Softeam, la marque du conseil et du service de Docaposte, intervient auprès de ses clients sur des missions d'audit organisationnel, de mise en place de cadres normatifs visant à assurer une organisation efficace et une gestion de la sécurité numérique. Par la mise en place de ces organisations, Softeam aide, depuis plus de 30 ans, ses clients à mieux gérer l'ensemble de ses risques (cyber, de non-conformité, opérationnels,...).

Nous intervenons dès les phases de conseil, de mise en œuvre et de formation/acclimatation des équipes. Nous aidons de nombreux clients dans la gestion des données (RGPD, DPO,...) et de la maîtrise de leurs risques.



HARMONIE
TECHNOLOGIE



CONSEIL ET SERVICE CYBER



Spécialiste de la cybersécurité et de la gestion des risques nous accompagnons les plus grandes entreprises françaises dans leur programme de transformation SSI pour renforcer leur sécurité et la résilience tout en améliorant leur performance grâce à l'adoption des nouveaux usages : télétravail, Cloud, RPA, Open Data, ...

Avec la double compétence fonctionnelle et technique, nous intervenons auprès des filières Risque et Contrôle, Sécurité de l'Information et des Directions Informatiques pour :

- organiser la maîtrise des risques cyber ;
- cadrer les programmes de sécurité ;
- intégrer les solutions de gestion des identités, accès et des données ;
- auditer la sécurité organisationnelle, fonctionnelle et technique (scan, pentest, red team).



RED ALERT
LABS



«SECURITY BY DESIGN», FORMATION & ÉVALUATION



Le travail à distance entraîne des risques de cybersécurité liés à l'augmentation de la surface d'attaque et à des facteurs humains. Nous pouvons vous aider à assurer la sécurité des environnements de télétravail de vos équipes via les services suivants:

Définition de la gouvernance sécurité / Réalisation des analyses de risque / Réalisation des formations : « Introduction à la cybersécurité liée au télétravail », « Cybersécurité appliquée » / Mise en place des méthodologies de sensibilisation / Implémentation du « Security by Design » / «Sécurité du cycle de vie de développement (SDLC)» / Évaluation de la maturité de la sécurité / Réalisation de tests d'intrusion / Accompagnement dans la mise en conformité aux réglementations, standards et bonnes pratiques / Certification sécurité

ACCOMPAGNEMENT ORGANISATIONNEL

Audit/Bug Bounty/Pentest, formation, sensibilisation, conseil, intégration



SERMA SAFETY AND SECURITY

ETI GG OSE/OIV

VISA DE SECURITE

ANSSI

SERMA
SAFETY & SECURITY

CONSEIL EN SÉCURISATION DU TÉLÉTRAVAIL



SERMA accompagne ses clients dans la mise en conformité de leur SI (politiques de sécurité conformes aux bonnes pratiques), réalise des audits de sécurité informatique (identification du niveau de sécurité de leur SI + recommandations), intègre des solutions de cyber sécurité et propose un centre opérationnel de sécurité permettant de détecter en temps réel les menaces de cybersécurité et de s'en protéger.

Dans le cadre du télétravail, SERMA réalise des campagnes de phishing, met en place des solutions protégeant contre les ransomware, met en place des solutions d'accès à distance (ZTNA, IAM, VPN), sensibilise les équipes aux risques liés à la cybersécurité, propose du forensic et des actions de remédiation en cas d'attaque.



SOGETI

ETI GG OSE/OIV

VISA DE SECURITE

ANSSI

FRANCE CYBER SECURITY

sogeti THEGREENBOW

Protégez les connexions de vos collaborateurs en accès distant

SÉCURISATION ET REMÉDIATION DES SOLUTIONS DE TÉLÉTRAVAIL

SÉCURISATION ET REMÉDIATION DES SOLUTIONS DE TÉLÉTRAVAIL



Vos enjeux

- Evaluer le niveau de sécurité de votre système d'information.
- Renforcer votre cybersécurité.
- Sécuriser l'accès à vos ressources pour vos collaborateurs nomades.

Une offre modulaire comprenant :

- L'audit par Sogeti des infrastructures de télétravail.
- L'accompagnement dans la mise en œuvre des propositions d'amélioration et des projets de sécurisation des solutions de télétravail.
- Le déploiement et l'intégration de clients VPN TheGreenBow (réputés pour leur niveau de sécurité, leur facilité d'installation et leur simplicité d'utilisation), technologie validée par des visas de sécurité de l'ANSSI.



THALES

ETI GG OSE/OIV

THALES

CYBELS RISK & THREAT EVALUATION



Dans le cadre de la généralisation du télétravail, nous conseillons nos clients sur la façon de concevoir et protéger leurs systèmes d'information et les postes de leurs utilisateurs pour les préserver des cyberattaques même les plus sophistiquées, et ce dans le respect des réglementations nationales et internationales. Notre démarche inclut : *Audit fonctionnel* (identification des risques IT/OT, audit des points faibles sur les plans technique et organisationnel, contrôle de la conformité réglementaire de votre système d'information.) / *Tests de pénétration* (nos experts, en s'appuyant sur le logiciel CYBELS Scan, évaluent la robustesse de votre infrastructure informatique, afin d'évaluer sa conformité avec votre politique de sécurité, en particulier dans le cadre des pratiques de télétravail.) / *Architecture de votre infrastructure* (audit et redéfinition de l'architecture globale de vos systèmes d'information pour en améliorer la résilience.) / *Prévention des cybermenaces* (bénéficiez d'une veille de sécurité permanente via le CERT-IST (Computer Emergency Response Team – Industrie, Services and Tertiaire).) / *Gestion de crise* (définition de scénarios de réponse visant à élaborer un plan d'action réaliste à l'échelle de votre entreprise, tout en minimisant les impacts opérationnels, financiers et d'image.) / *Déploiement d'une équipe de réaction rapide* (en cas d'incident, mobilisation immédiate sur site de nos experts en cybersécurité.)

En choisissant Thales, vous bénéficiez de l'expérience de consultants qualifiés, disponibles 24/7.

ACCOMPAGNEMENT ORGANISATIONNEL

Audit/Bug Bounty/Pentest, formation, sensibilisation, conseil, intégration



THALES

THALES

CYBELS TRAIN & EXPERIMENT

THALES

Afin d'accompagner la mise en œuvre du télétravail, nous conseillons nos clients pour concevoir et protéger leurs systèmes d'informations et les préserver des cyberattaques. Notre démarche inclut :

Audit fonctionnel (identification des risques IT/OT, audit des points faibles techniques et organisationnels, contrôle de la réglementation) / *Tests de pénétration* (évaluation de la robustesse des infrastructures informatiques avec le logiciel CYBELS Scan en conformité avec la politique de sécurité de l'entreprise.) / *Architecture du SI* (audit et redéfinition de l'architecture des systèmes d'informations pour en améliorer la résilience.) / *Prévention des cyber menaces* (veille de sécurité permanente via le CERT-IST) / *Gestion de crise* (définition de plans d'actions en minimisant les impacts opérationnels, financiers et d'image.) / *Equipe de réaction rapide* : en cas d'incident, mobilisation sur site client de nos experts.

En choisissant Thales, vous bénéficiez de l'expérience de consultants spécialisés en Cybersécurité.



THE GREENBOW

THEGREENBOW

SÉCURISATION ET REMÉDIATION DES SOLUTIONS DE TÉLÉTRAVAIL

THEGREENBOW

Afin d'aider les grandes entreprises et collectivités à évaluer le niveau de sécurité de leur SI, renforcer leur cybersécurité ou encore sécuriser l'accès aux ressources pour leurs collaborateurs nomades, TheGreenBow et Sogeti ont associé leurs expertises pour proposer une offre dédiée à la sécurisation et à la remédiation des solutions de télétravail.

Cette offre comprend :

- l'audit des infrastructures et équipements VPN réalisé par Sogeti ;
- la mise en œuvre technique de propositions d'amélioration ;
- le déploiement et l'intégration de Clients VPN TheGreenBow.

Nos clients VPN sont disponibles pour Windows, Linux, Android, iOS et macOS. Une version disposant d'un un Visa de l'ANSSI est proposée pour Windows et Linux.



YOGOSHA

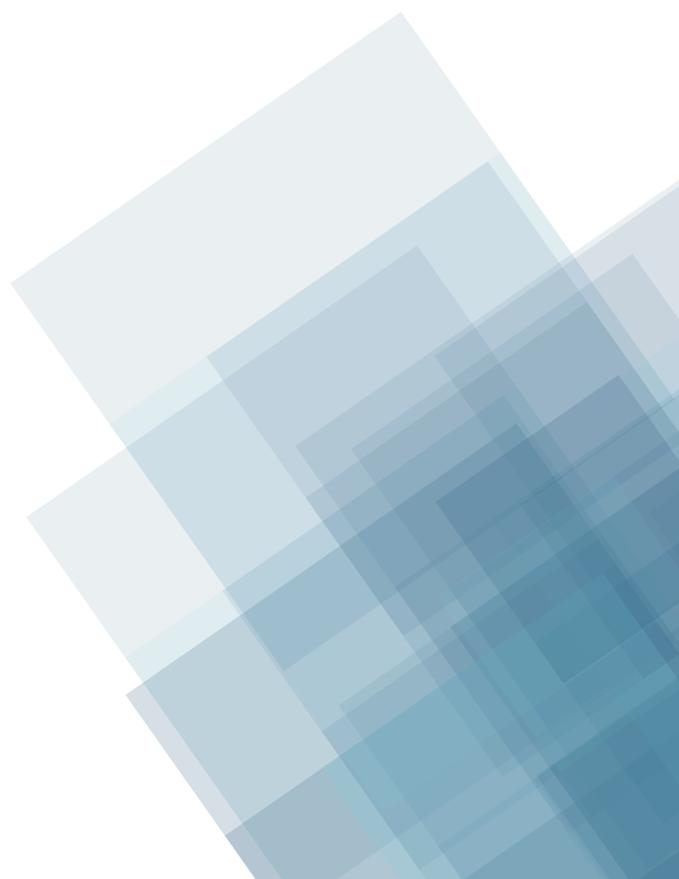
YogOsha

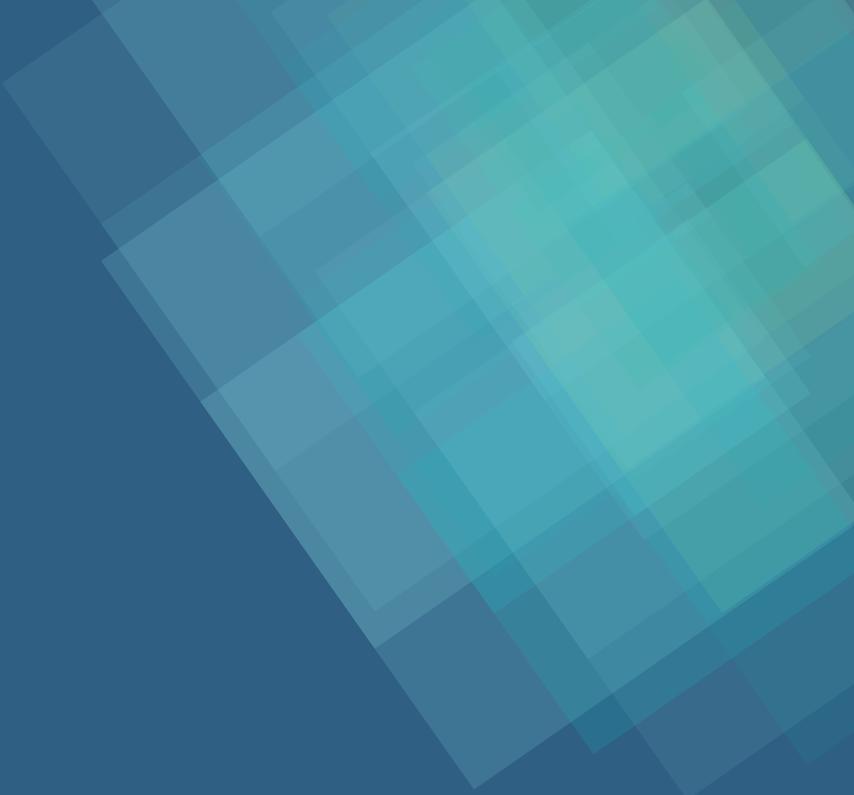
PLATEFORME MULTI-SERVICES DE PENTEST CROWDSOURCÉ ET DE BUG BOUNTY

YogOsha

Yogosha est une plateforme de cybersécurité multi-services permettant de collaborer avec une communauté de hackers d'élite certifiés pour détecter et gérer des vulnérabilités sur les systèmes les plus critiques. La plateforme permet de proposer des services de Bug Bounty, Pentests crowdsourcés et CVD. Yogosha ne sélectionne que les hackers les plus talentueux afin de s'assurer que les vulnérabilités les plus critiques sont identifiées rapidement et plus facilement corrigées. Yogosha permet à ses clients de développer des applications à l'épreuve des attaques, de réduire les risques, d'augmenter la conformité et d'accélérer le business.

La plateforme multi-services de Yogosha vous permet de définir rapidement vos besoins sécurité, d'analyser les rapports de vulnérabilités, la performance des campagnes et de faciliter les plans de remédiation.





INDEX DES SOCIÉTÉS

PRÉSENTATIONS



AIRBUS CYBERSECURITY

AIRBUS

Entité d'Airbus Defence and Space entièrement dédiée à la cybersécurité, Airbus CyberSecurity protège aussi bien des industries et des infrastructures critiques que des institutions publiques et des moyens militaires avec des solutions de cybersécurité à très haute fiabilité permettant de détecter, d'analyser et de contrer des cyberattaques de plus en plus sophistiquées.

CONTACT

Offre **ORION MALWARE**
M. Eric CHAMBAREAU
eric.chambareau@airbus.com
07 86 87 75 65

Offre **CYBERRANGE**
M. Yoann LE GUILLOU
yoann.le_guillou@airbus.com
06 09 55 70 97

Metapole
1 boulevard Jean Moulin
78996 Elancourt
01 61 38 50 00
contact.cybersecurity@airbus.com

www.airbus-cyber-security.com/fr

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





ATOS

Atos

Atos est un leader international de la transformation digitale avec 105 000 collaborateurs et un chiffre d'affaires annuel de 11 milliards d'euros.

Numéro un européen du cloud, de la cybersécurité et des supercalculateurs, le Groupe fournit des solutions intégrées pour tous les secteurs, dans 71 pays.

Pionnier des services et produits de décarbonation, Atos s'engage à fournir des solutions numériques sécurisées et décarbonées à ses clients. Atos est une SE (Société Européenne) cotée sur Euronext Paris et fait partie de l'indice CAC 40.

La raison d'être d'Atos est de contribuer à façonner l'espace informationnel. Avec ses compétences et ses services, le Groupe supporte le développement de la connaissance, de l'éducation et de la recherche dans une approche pluriculturelle et contribue au développement de l'excellence scientifique et technologique.

Partout dans le monde, Atos permet à ses clients et à ses collaborateurs, et plus généralement au plus grand nombre, de vivre, travailler et progresser durablement et en toute confiance dans l'espace informationnel.

CONTACT

Offre EVIDIAN WAM

Offre EVIDIAN IDAAS

M. Yann MORVAN

yann.morvan@evidian.com

06 72 75 57 28

Offre ATOS ENDPOINT PROTECTION

M. Mathieu VIGNERON

mathieu.vigneron@atos.net

01 73 26 29 51

Offre IDNOMIC DIGITAL SIGNATURE

Offre SOLUTIONS DE CHIFFREMENT

TRUSTWAY

M. Morgan FOLLIER

morgan.follier@atos.net

06 48 43 74 15

80 Quai Voltaire

95870 Bezons

01 73 26 00 00

www.atos.net

OFFRES



POSITIONNEMENT DANS LE
CYCLE DU TÉLÉTRAVAIL





AVANT DE CLIQUER



Société française, née en Normandie, Avant de Cliquer conçoit, héberge et développe ses outils en France grâce à des équipes pluridisciplinaires installées à Lille, Rouen et Caen.

Le phishing est source de plus de 90% des cyberattaques abouties. L'hameçonnage joue sur le manque de vigilance des utilisateurs, et les meilleures solutions techniques de sécurité sont impuissantes face aux actions d'utilisateurs non sensibilisés. La prévention est donc le meilleur moyen de lutte.

Avant de Cliquer installe une solution SaaS développant des algorithmes intelligents associant audit de vulnérabilité, sensibilisation par l'action sur poste de travail, e-learning, Bouton d'Alerte Cyber et process d'alerte cyber pour les SI pour automatiser une solution complète et autonome de sensibilisation à la cybersécurité phishing. L'objectif est de mettre en place une culture de cybersécurité basée sur l'acquisition de réflexes acquis grâce à la solution.

CONTACT

M. Carl HERNANDEZ
carl@avantdecliquer.com
06 31 37 41 50

9 rue Georges Braque
76 000 Rouen
02 78 77 53 86
contact@avantdecliquer.com

www.avantdecliquer.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





CHAMBERSIGN



Chambersign est une autorité de certification créée en 2000. Tiers de confiance, elle fournit un ensemble d'outils d'identités et de signatures numériques émis et délivrés dans le respect des normes les plus strictes de la profession garantissant ainsi un niveau de sécurité optimal dans les échanges électroniques.

ChamberSign délivre une gamme de certificats électroniques personnes physiques et morales conforme à la réglementation en vigueur (RGS et eIDAS). Multi-usages, ils permettent une authentification forte, la signature électronique, le scellement des données, la traçabilité des référentiels de données ou encore la sécurisation des accès et des échanges électroniques.

ChamberSign s'est vu décerner le visa de sécurité de l'ANSSI pour ses services de certification électronique et le Label France Cybersecurity. Elle est certifiée ISO 9001-2015 pour ses procédures internes.

CONTACT

commercial@chambersign.fr
08 92 23 02 52

10 cours de Verdun Rambaud
69002 Lyon
direction@chambersign.fr

www.chambersign.fr

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





CORALIUM



Coralium est un cabinet de conseil en sécurité informatique pour les petites et moyennes structures. Notre volonté est de rendre la cybersécurité accessible à toutes les entreprises, quelle que soit la taille ou le système d'information.

Notre cabinet bénéficie d'une expertise de pointe dans le domaine de la sécurité informatique grâce à son réseau de sachants, sélectionnés pour la diversité et la qualité de leurs compétences, experts techniques mais aussi gouvernance & process. Notre taille humaine et nos consultants issus du milieu des TPME nous permettent d'être à l'écoute des dirigeants et de leurs équipes, et de leur fournir des recommandations réalistes et immédiatement applicables.

Nous intervenons pour tout type de prestation de sécurité informatique : audits, test de pénétration (pentest), gestion des risques, formation, accompagnement ISO 27001, conseil, ...

Vous avez une question cyber ? Discutons-en !

CONTACT

M. Maxence DULONG
maxence.dulong@coralium.fr
06 43 04 53 48

10 rue de Penthièvre
75008 Paris
06 76 28 86 80
contact@coralium.fr

www.coralium.fr

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





DOCAPOSTE



DOCAPOSTE

Filiale numérique du Groupe La Poste, Docaposte a pour mission de rendre l'avenir plus simple pour nos clients, en confiance, en nous positionnant en partenaire de leur transformation, en leur offrant le meilleur de nous-même et de nos savoir-faire.

Nous accompagnons toutes les entreprises et administrations dans leur transformation digitale : nous proposons des solutions adaptées à l'ensemble de leurs besoins, nous les aidons à fluidifier et à sécuriser leurs échanges et transactions, nous les soutenons dans leur stratégie et leur rythme de transformation.

Notre conviction pour une transformation réussie : allier le meilleur de l'expertise métier, de la technologie et de l'humain.

Docaposte propose une des offres parmi les plus riches du marché en alliant conseils d'experts, solutions technologiques robustes et excellence de services.

- Avec plus de 140 solutions numériques et physiques, nous couvrons tous les besoins pour toutes les organisations et toutes les tailles d'entreprise en proposant des solutions sur mesure ou prêtes-à-l'emploi.
- Nous développons des plateformes combinant un savoir-faire éprouvé, un socle technologique robuste et ses solutions.
- Docaposte c'est aussi le meilleur du numérique et de l'humain, avec une expertise historique dans le Business Process Outsourcing pour accompagner nos clients dans l'externalisation de leurs activités.

La confiance est la pierre angulaire de notre promesse.

Nous sommes LE partenaire légitime de la confiance – universalité, pérennité, neutralité – car nous sommes Tiers de Confiance Numérique. Docaposte se porte garant des opérations : intégrité et non utilisation des données sans consentement, transparence à chacune des étapes d'une transaction et souveraineté. Nous créons des chaînes de confiance numérique qui reposent sur un service de qualité, des solutions numériques certifiées (L'Identité Numérique La Poste, Digiposte...) et des infrastructures numériques qui garantissent le respect des valeurs de confiance que nous partageons avec Le Groupe La Poste.

CONTACT

Mme. Gaëlle PICARD
gaelle.picard@docaposte.fr
01 56 29 79 30

45/47 boulevard Paul Vaillant Couturier
94220 Ivry-sur-seine

www.docaposte.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





ERCOM



Depuis plus de 30 ans, Ercom, filiale du groupe Thales, est une société française reconnue pour ses solutions de sécurisation de la mobilité, a développé une position de leadership sur les marchés de la sécurité des communications, données et terminaux.

Cette position repose sur des expertises technologiques complémentaires en infrastructure télécom/cloud, cryptographie et logiciel et sur des valeurs partagées : l'innovation, l'expertise, l'engagement et la confidentialité.

Ercom déploie ses solutions en France et à l'International auprès d'acteurs majeurs qui ont besoin d'outils évolutifs, fiables et hautement sécurisés.

CONTACT

M. Nicolas MOSTACCHI
sales_cybersec@ercom.fr
01 39 46 50 50

6 rue Dewoitine
78140 Velizy Villacoublay
01 49 36 50 50

www.ercom.fr

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL



HARFANGLAB



HarfangLab, éditeur d'un logiciel EDR (Endpoint Detection and Response), technologie qui permet d'anticiper et neutraliser les cyberattaques modernes et inconnues, sur ordinateurs et serveurs.

Certifié par ANSSI depuis 2020, HarfangLab compte parmi ses clients de grandes entreprises d'envergure internationale, évoluant dans des secteurs très sensibles. HarfangLab EDR se distingue par : l'ouverture de sa solution qui s'intègre nativement à toutes les autres briques de sécurité grâce à son API ; par sa transparence, car les données collectées par l'EDR restent accessibles et par l'indépendance numérique qu'il offre, car ses clients sont libres de choisir leur mode d'hébergement : cloud, public ou privé, ou dans leur propre infrastructure.

CONTACT

M. Bertrand JULIEN
bertrand@harfanglab.fr
06 98 65 53 47

55 rue La Boetie
75008 Paris
contact@harfanglab.io

www.harfanglab.io

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL



HARMONIE TECHNOLOGIE



Cabinet de conseil et d'expertise spécialiste de la cybersécurité, Harmonie Technologie accompagne ses clients de la définition de leur stratégie de cyber sécurité, à la protection de leur patrimoine informationnel, en passant par la prévention des risques.

Le cabinet accompagne les filières Risque et Contrôle, Sécurité de l'information et des Directions Informatiques pour aider ses clients à définir leurs schémas de transformation et les investissements nécessaires en matière de sécurité du SI. Dans la continuité des orientations stratégiques, les experts interviennent auprès des acteurs opérationnels en audit, conseil, formation et intégration de solutions.

Harmonie Technologie propose un accompagnement à 360° pour sécuriser la transformation digitale et notamment la mise en place du télétravail :

- Organiser la maîtrise des risques cyber
- Cadrer les programmes de sécurité
- Mettre en œuvre les nouvelles solutions
- Auditer la sécurité de l'organisation, des processus et des solutions

CONTACT

Mme. Gabrielle PAVIA
gabrielle.pavia@harmonie-technologie.com
01 73 54 30 00

47 rue Washington
75008 Paris
01 73 54 30 00
contact@harmonie-technologie.com

www.harmonie-technologie.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL



KEOPASS



KeoPass est une entreprise française spécialisée dans la conception, la fabrication et la commercialisation de dispositifs portables d'authentification multi-facteurs pour la sécurité logique et physique, basés sur la biométrie.

La Clé KeoPass est un dispositif portable et autonome d'authentification biométrique pour le contrôle d'accès physique (remplacement des badges) et logique (saisie de mots de passe) fonctionnant avec tout appareil fixe ou mobile et n'importe-quelle application ou service, sans installation ni modification logicielle ou d'infrastructure matérielle.

Conforme aux recommandations de l'ANSSI, La Clé KeoPass libère de la contrainte des mots de passe, facilite l'application de la RGPD, accélère et sécurise les processus d'authentification, permettant une réduction du hameçonnage et des appels à la hotline informatique.

Grâce à sa modularité, la Clé KeoPass est adaptable à tout contexte et pérenne via des mises à jour in-situ, en particulier vers l'OTP et le passwordless.

CONTACT

M. Hervé-François LE DEVEHAT
herve@keopass.com
02 97 58 00 95

18 rue du Gréo
56870 Baden
02 97 58 00 95
contact@keopass.com

www.keopass.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





LEX PERSONA

LEXpersona
You can trust each other

Lex Persona est un éditeur de logiciels français indépendant créé en 2005 certifié ISO 27001 et un prestataire de services de confiance qualifié eIDAS.

Notre raison d'être est de permettre à nos Clients de développer et renforcer la confiance qu'ils entretiennent avec leurs propres clients, fournisseurs, partenaires, collaborateurs, actionnaires, etc.

Grâce à nos solutions et à notre expertise, nos Clients peuvent véhiculer les valeurs de leur entreprise en personnalisant leurs propres applications de signature électronique.

Nous proposons des solutions qui permettent de signer, faire signer et cacheter électroniquement tout type de document, en conformité avec la réglementation.

CONTACT

Offre SIGNER

Mme. Julie-Anne MANGIN
julie-anne@lex-persona.com
03 25 43 90 78

Offre FAIRE SIGNER

Mme. Imane PASQUIER
commercial@lex-persona.com
03 52 59 00 98

Offre CACHERER

M. François DEVORET
fdevoret@lex-persona.com
06 72 74 35 53

2 rue Gustave Eiffel
10430 Rosieres-pres-troyes
03 25 43 90 78
info@lex-persona.com

www.lex-persona.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





NET EXPLORER



NetExplorer est le spécialiste français de la gestion des fichiers dans le Cloud pour les entreprises : partage de fichiers, travail collaboratif et stockage en ligne.

Véritable spécialiste de la gestion de fichiers en ligne, nous maîtrisons 100% de la chaîne du service SaaS fournis à nos clients : du développement de nos applications, réalisé en interne, à l'infrastructure d'hébergement.

Fervents défenseurs de la souveraineté et de la protection des données, nos centres d'hébergement sont localisés en France.

Présents sur le marché depuis 2007, NetExplorer équipe à ce jour plus de 1 500 entreprises et 200 000 utilisateurs quotidiens.

Afin d'attester de notre expertise et de renforcer notre engagement vis à vis de nos clients, NetExplorer est une entreprise certifiée ISO 27001 pour la sécurité de l'information et ISO 9001 pour la qualité. En complément, NetExplorer est certifiée HDS et accréditée par le gouvernement pour l'hébergement de données de santé.

CONTACT

Service commercial
contact@netexplorer.fr
05 61 61 20 10

24 boulevard des Frères Voisin
92130 Issy-les-moulineaux

www.netexplorer.fr

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





NEXUS



Nexus, filiale du groupe français IN Groupe, est un leader européen innovant de gestion d'identité et le partenaire de confiance offrant des identités professionnelles fiables pour les personnes et les objets.

Nexus développe une gamme de produits et services de sécurité.

Grâce à la solution SMART ID, nous permettons aux entreprises du monde entier de toutes tailles et de tous les secteurs d'émettre et de gérer le cycle de vie des identités certifiées de leurs employés et de leur lieu de travail ainsi que des objets connectés (IoT).

Nexus compte 300 employés dédiés à travers l'Europe et l'Inde et un vaste réseau mondial de partenaires. Nexus Suède, ainsi que tous ses services, sont certifiés conformes à la norme ISO 27001:2013 en matière de sécurité de l'information. Tous nos produits et services sont documentés en ligne.

CONTACT

M. Philippe FONTON
philippe.fonton@nexusgroup.com
06 08 81 59 25

104 avenue du Président Kennedy
75016 Paris
01 40 58 30 00

www.nexusgroup.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





OXIBOX

oxibox

Oxibox permet aux entreprises de redémarrer leurs systèmes immédiatement après une cyberattaque ou un ransomware.

Les solutions de sauvegarde et de protection des données ne suffisent plus à garantir la pérennité des systèmes face à l'explosion des menaces cyber.

La technologie innovante d'Oxibox permet de répondre à cet enjeu par la création d'enclaves sécurisées qui garantissent l'immutabilité des données y étant déposées. Les sauvegardes sont ainsi rendues résistantes aux ransomwares.

Cette technologie peut être déployée soit au sein d'une infrastructure de sauvegarde existante, soit sous un format tout-en-un intégrant notre propre technologie de sauvegarde et de restauration.

Nos solutions peuvent répondre aux besoins des grandes structures comme des TPE/PME et sont référencées par la DINUM et l'UGAP. Plus de 1200 clients privés et publics nous font confiance pour la protection de leur SI.

CONTACT

M. Jean-Baptiste D'ABOVILLE
06 58 97 67 48

15 boulevard des Chênes
78280 Guyancourt
01 30 54 45 79
contact@oxibox.fr

www.oxibox.com/fr

OFFRES



POSITIONNEMENT DANS LE
CYCLE DU TÉLÉTRAVAIL





PRIVATE DISCUSS



Private Discuss est une plateforme de communication collaborative, utilisée pour les visioconférences, les webinaires et le télétravail.

Véritable bureau hybride et ergonomique, Private Discuss est chiffrée de bout-en-bout et conforme RGPD, elle se démarque des solutions étrangères en proposant une plateforme complète grâce à ses fonctionnalités nombreuses et inédites (pause-café virtuelle, espaces méditation, exercices TMS, jauge bien-être...) mais aussi en promouvant la souveraineté numérique et le savoir-faire technologique et cyber français.

Conçue à partir de technologies 100% propriétaires, sur les algorithmes les plus puissants du marché et hébergée sur des serveurs français, Private Discuss vous garantit la protection robuste de vos données et une entière satisfaction lors de son utilisation.

CONTACT

M. Olivier LACH
o.lach@private-discuss.com
07 69 24 91 28

304 Route Nationale 6
69760 Limonest
04 82 62 62 10

www.private-discuss.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





RED ALERT LABS



RED ALERT LABS
IoT Security

Red Alert Labs est une entreprise française, spécialisée dans la cybersécurité, les objets connectés et la certification. Elle a pour objectif d'instaurer la confiance dans les objets connectés, en proposant une plateforme logicielle d'automatisation guidant l'utilisateur pour identifier les risques, mettre en place des exigences de sécurité et prouver le niveau de conformité et de robustesse des objets connectés à travers des processus de certifications simplifiés.

A côté des solutions logicielles développées pour répondre à ces enjeux, la société fournit des services de conseil et d'audits sécuritaires. Elle contribue de manière active à la définition de schémas de certification IoT, en collaboration avec des organismes de cybersécurité au niveau national, européen et international comme EUROSMT, ACN, ANSSI, ENISA... Elle fait également partie du Campus Cyber.

L'expertise de Red Alert Labs a été reconnue par de nombreuses distinctions, dont le « Label France Cybersecurity » et le prix de la communauté French IoT 2019.

CONTACT

Mme. Olga GHATTAS
olga.ghattas@redalertlabs.com
09 51 79 07 87

3 rue Parmentier
94140 Alforville
09 51 79 07 87
contact@redalertlabs.com

www.redalertlabs.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





RUBYCAT



Rubycat est un éditeur de logiciels français disposant d'une expertise en cybersécurité et plus particulièrement en traçabilité numérique.

Nous proposons la solution logicielle PROVE IT de type «Bastion/PAM», certifiée par l'ANSSI, permettant de contrôler, tracer et enregistrer les accès et actions effectuées sur les équipements sensibles du système d'information par les comptes à privilèges (administrateur, télé-mainteneur,...).

CONTACT

M. Thomas CRIBIER
thomas.cribier@rubycat.eu
07 85 93 47 70

1137 A avenue des Champs Blancs
33510 Cesson-Sevigne
02 99 30 21 11
sales@rubycat.eu

www.rubycat.eu

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





SERMA SAFETY AND SECURITY



SERMA Safety & Security est votre interlocuteur unique pour la sécurité et la sûreté de fonctionnement de vos produits et systèmes, qu'ils soient dans les domaines de l'IoT, de l'embarqué, de l'industrie ou des systèmes d'information. L'entreprise bénéficie d'une expertise unique développée depuis plus de 20 ans qui lui permet d'intervenir sur toute la chaîne de valeur de vos systèmes : depuis la conception jusqu'au maintien en conditions opérationnelles/supervision des équipements.

CONTACT

Mme. Nathalie MONEY
n.money@serma.com
06 20 52 04 87

14 rue Galilée
33600 Pessac
05 57 26 08 88
contact-s3@serma.com

www.serma-safety-security.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





SOGETI



Sogeti fait partie du groupe Capgemini, avec une présence dans plus de 100 sites à travers le monde. Travaillant en étroite collaboration avec ses clients et partenaires pour tirer pleinement parti des technologies, Sogeti allie agilité et rapidité de mise en œuvre pour concevoir des solutions sur mesure innovantes et tournées vers l'avenir dans les domaines de l'Assurance et du Testing, du Cloud et de la Cybersécurité, et intégrant les technologies d'intelligence artificielle et d'automatisation. Sogeti aide les entreprises à accélérer le rythme de déploiement des solutions digitales grâce à son approche pragmatique, « value in the making », et sa passion pour la technologie.

CONTACT

M. Yves LE FLOCH
yves.le-floch@sogeti.com
01 57 99 01 10

147 quai du Président Roosevelt
92130 Issy les Moulineaux
01 57 99 00 00
contact@sogeti.com

www.fr.sogeti.com

OFFRES



POSITIONNEMENT DANS LE
CYCLE DU TÉLÉTRAVAIL



STORMSHIELD



STORMSHIELD

Acteur européen de la sécurité des infrastructures numériques et filiale à 100% d'Airbus Cybersecurity, Stormshield propose des solutions de confiance, certifiées et qualifiées au plus haut niveau européen, pour anticiper les attaques et protéger les environnements informatiques et industriels.

Avec plus de 17 000 clients et une présence internationale dans 40 pays, Stormshield est le premier éditeur français pure-player en cybersécurité et le premier éditeur européen de solutions pare-feu. Son expertise se décline en trois gammes de produits, développées en France, assurant la protection des réseaux, des postes et serveurs ainsi que des données.

Fort de ses 400 collaborateurs passionnés, Stormshield a pour mission de cyber-séréniser les organisations exploitant des infrastructures critiques et opérationnelles pour qu'elles puissent se concentrer sur leur cœur de mission, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations.

Stormshield Endpoint Security
Protection avancée des postes Windows

Le Stormshield : une protection proactive unique et non connectée

Stockage sécurisé des attaques inconnues et mise à disposition des éléments d'investigation distants

Stormshield Network Security
Une gamme de pare-feux & VPN de nouvelle génération

Le Stormshield : des performances inégales au meilleur coût

Protection de tous les environnements IT, OT et Cloud en une gamme complète et un seul registre d'administration

Stormshield Data Security
Chiffrement de bout en bout multi-devices et multi-applications

Le Stormshield : une solution de chiffrement des données non-structurées On-Premise & Cloud

Chiffrement au plus près de la donnée assure une protection de bout en bout

CONTACT

M. Pierre Yves HENTZEN
pierre-yves.hentzen@stormshield.eu
06 13 51 67 23

Offre STORMSHIELD DATA SECURITY
Offre STORMSHIELD ENDPOINT SECURITY
Offre STORMSHIELD NETWORK SECURITY
Mme Claudia GUENOUN
claudia.guenoun@stormshield.eu
09 69 32 96 29

2-10 rue Marceau
92130 Issy-les-Moulineaux

www.stormshield.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





SYSTANCIA



Systancia est un éditeur global et indépendant de logiciels de cybersécurité qui offre aux employés une expérience d'accès à leur environnement de travail sécurisée et fluide.

Dans tout environnement de travail, il y a une personne qui mérite d'être en pleine maîtrise et en pleine confiance. C'est notre conviction et notre but. C'est pourquoi nous investissons toute l'ingéniosité de nos équipes pour relever le défi humain de l'expérience digitale : mettre des solutions technologiques intelligentes et conviviales au service des personnes.

Pour concrétiser cette vision, nous avons réuni un ensemble de technologies au sein d'une plateforme offrant une expérience unifiée et un guichet unique d'accès, permettant aux organisations de gérer la chaîne de confiance de bout en bout pour tous les employés de leur écosystème : de la gestion des identités et des habilitations des personnes (IAM) à l'accès distant sécurisé à leur environnement de travail (ZTNA et VDI), que ce soit en tant qu'opérateur métier ou en tant qu'administrateur informatique (PAM).

Systancia propose son offre sous forme de produits logiciels et/ou d'une plateforme de services cloud, souvent dans des modèles de déploiement hybrides. Elle s'appuie sur l'intelligence artificielle et la virtualisation d'environnement de travail pour renforcer la productivité et la sécurité des utilisateurs.

Nous sommes ravis que des centaines d'organisations publiques et privées fassent confiance à la plateforme d'expérience d'accès sécurisé de Systancia pour des projets tels que le télétravail sécurisé, l'accès sécurisé par des tiers, la surveillance des accès, l'embarquement des employés, l'accès unifié à des infrastructures multiclouds, la migration vers le cloud, la migration des applications vers le SaaS, l'atténuation des risques numériques, pour emmener l'organisation de l'agilité à la résilience, de la conformité à la responsabilité, de la technologie à la personne.

CONTACT

M. Xavier Hameroux
contact@systancia.com
03 89 33 58 20

3 rue Paul Henri Spaak
68390 Sausheim
03 89 33 58 20
info@systancia.com

www.systancia.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





THALES

THALES

Dans un monde en constante mutation, à la fois imprévisible et riche d'opportunités, nous sommes aux côtés de ceux qui ont de grandes ambitions : rendre le monde meilleur et plus sûr.

Riches de la diversité de leurs expertises, de leurs talents, de leurs cultures, nos équipes d'architectes conçoivent un éventail unique de solutions technologiques d'exception, qui rendent demain possible dès aujourd'hui.

Du fond des océans aux profondeurs du cosmos ou du cyberspace, nous aidons nos clients à maîtriser des environnements toujours plus complexes pour prendre des décisions rapides, efficaces, à chaque moment décisif.

Quel que soit l'enjeu.

Nous servons cinq grands secteurs essentiels pour le développement de nos sociétés :

- Aéronautique
- Espace
- Transport terrestre
- Identité et Sécurité numériques
- Défense et Sécurité

Des équipements et systèmes aidant nos clients à choisir la meilleure option et à agir en conséquence. L'expertise de ses 80 000 collaborateurs et sa présence opérationnelle dans 68 pays en font ainsi un acteur clé de la sécurité des citoyens, des infrastructures et des États.

CONTACT

Offre CYBELS TRAIN & EXPERIMENT

M. Eric WEBER

eric.weber@thalesgroup.com

01 46 13 21 59

Offre CYBELS RISK & THREAT EVALUATION

M. Laurent MARECHAL

laurent.marechal@thalesgroup.com

01 73 32 23 64

4 avenue des Louvresses

92230 Gennevilliers

01 41 30 30 00

www.thalesgroup.com

OFFRES



POSITIONNEMENT DANS LE
CYCLE DU TÉLÉTRAVAIL





THEGREENBOW



Créé en 1998, TheGreenBow est un éditeur français de logiciels de Cybersécurité qui fournit des solutions VPN de confiance et dont l'expertise repose sur la sécurisation des communications. Premier opérateur à avoir été certifié CC EAL3+, et agréé DR OTAN et UE en 2013, pour son logiciel Client VPN Windows, TheGreenBow, l'acteur de référence des Clients VPN, distribue ses logiciels dans plus de 70 pays. Depuis fin 2019, TheGreenBow détient le label « Utilisé par les armées françaises » pour le produit TheGreenBow VPN Client Windows Certifié CC EAL3+. Ce label atteste de la mise en œuvre du logiciel par les services du Ministère des Armées Françaises.

Réputés pour leur facilité d'installation et simplicité d'utilisation, les clients VPN TheGreenBow protègent les connexions au système d'information et assurent l'intégrité et la confidentialité des données échangées en toutes circonstances (nomadisme, diffusion restreinte, objets connectés, maintenance, sous-traitance ...).

CONTACT

Offre CLIENT VPN THEGREENBOW
Offre LE VPN FRANCAIS
M. Mathieu ISAIA
mathieu@thegreenbow.com
01 43 12 39 30

Offre SECURISATION ET REMEDIATION
DES SOLUTIONS DE TELETRAVAIL
M. François BONNET
francois.bonnet@thegreenbow.com
01 43 12 39 30

14 rue Auber
75009 Paris
01 43 12 39 30

marketing@thegreenbow.com

www.thegreenbow.fr

OFFRES



POSITIONNEMENT DANS LE
CYCLE DU TÉLÉTRAVAIL





TIXEO



Créée à Montpellier en 2004, Tixeo est leader européen de la visioconférence sécurisée.

Unique acteur français proposant des solutions de visioconférence et de vidéo-collaboration certifiées (CSPN)/qualifiée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et recommandées par la CNIL, Tixeo a conçu sa solution de visioconférence basée sur un ensemble de mécanismes innovants permettant d'assurer un niveau de sécurité encore jamais atteint pour des réunions en ligne.

La conception et le développement de ses logiciels sont exclusivement réalisés en France (100% Made in France) et sa technologie est non-soumise aux législations étrangères. La technologie française Tixeo est également labellisée « France Cybersecurity » et « Cybersecurity Made in Europe ».

Tixeo est membre de l'Alliance pour la Confiance Numérique (ACN), du CLUSIF, de la French Tech Méditerranée et d'HEXATRUST.

CONTACT

M. Laurent FLAVENOT
lflavenot@tixeo.com
06 16 24 61 23

Parc 2000
244 rue Claude François
34080 Montpellier
04 67 75 04 31
contact@tixeo.com

www.tixeo.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL



TRANQUIL IT



Tranquil IT est l'éditeur de WAPT, le seul outil certifié ANSSI pour déployer, patcher, auditer des logiciels et des configurations sur un parc Windows, Linux et macOS. Elle est aussi reconnue pour son savoir-faire Active Directory.

Nos solutions WAPT et Samba-AD se retrouvent chez des clients au profil diversifié : petites et grandes collectivités publiques (État, territorial, hospitalier), PME et grands comptes, et à l'international.

Nos valeurs s'articulent autour de l'excellence et de la maîtrise technique. Nous existons pour créer de bons produits qui assurent des fonctions utiles de cybersécurité, frugales en ressources, et qui agissent discrètement et efficacement.

Vous trouverez chez Tranquil IT des personnes performantes, aidantes et animés pour votre réussite.

CONTACT

Mme. Faustine BADIER
communication@tranquil.it
02 40 97 57 55

12 avenue Jules Verne
44230 Saint Sébastien sur Loire
communication@tranquil.it

www.tranquil.it

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL





TOGOSHA

YogOsha

Yogosha est une plateforme de cybersécurité pour les entreprises et les administrations souhaitant mieux sécuriser leurs applications, en allant au-delà des approches traditionnelles. Yogosha ne sélectionne que les hackers les plus talentueux afin de s'assurer que les vulnérabilités les plus critiques soient identifiées rapidement et plus facilement corrigées. Yogosha permet aux entreprises de développer des applications à l'épreuve des attaques, de réduire sensiblement les risques, d'augmenter la conformité et d'accélérer le business.

Basée à Paris et Berlin, Yogosha opère en France, en Europe et dans la région EMEA.

Références Clients Thales, Société Générale, Veolia, BNP Paribas, Cdiscount, Accor Hotels, Bouygues Telecom, Swiss Life, Mano Mano, Groupama, MACSF, Zadig & Voltaire, Stormshield, But...

CONTACT

M. Christophe MARNAT
c.marnat@yogosha.com

50 rue du Faubourg Saint Antoine
75012 Paris

contact@yogosha.com

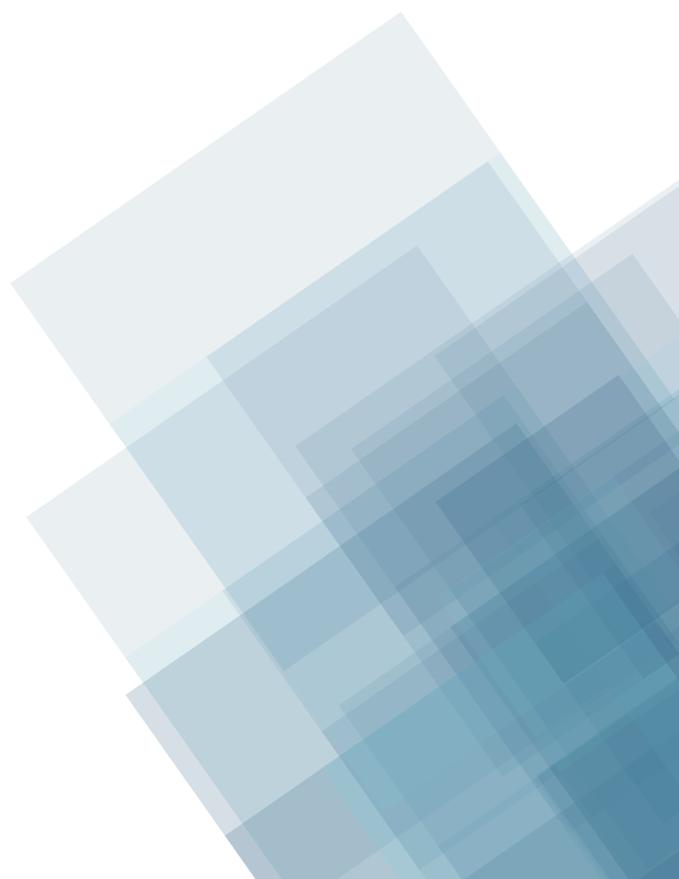
www.yogosha.com

OFFRES



POSITIONNEMENT DANS LE CYCLE DU TÉLÉTRAVAIL







Alliance pour la confiance numérique

www.confiance-numerique.fr

L'Alliance pour la Confiance Numérique (ACN) est l'organisation professionnelle qui représente les entreprises du secteur de la confiance numérique notamment celles de la cybersécurité, de l'identité numérique et de l'intelligence artificielle de confiance. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur.

On dénombre près de 2 100 entreprises réalisant en France 13,4 milliards d'euros de chiffre d'affaires dans ce secteur en croissance forte et durable (8,1% de croissance annuelle moyenne depuis 2015).
(Source : Observatoire ACN de la Confiance Numérique, éd. 2021.)

L'Alliance pour la Confiance Numérique (ACN) rassemble plus de 80 entreprises dont 9 des 10 leaders du secteur, mais aussi 85% de start-up, TPE-PME ou ETI, qui représentent plus des 2/3 du chiffre d'affaires des entreprises françaises de la Confiance Numérique dans le monde (fabricants de matériel, éditeurs de logiciels, intégrateurs, services, laboratoires d'évaluation de sécurité, recherche, ...).

L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) et participe activement aux travaux du CSF (Comité Stratégique de Filière) Industries de sécurité.

Par ailleurs, l'ACN est également membre fondateur de l'association représentant l'écosystème européen de la cybersécurité : ECSO (European CyberSecurity Organisation).

réalisé en lien avec le :

COMITÉ STRATÉGIQUE DE FILIÈRE INDUSTRIES DE SÉCURITÉ

Le Comité Stratégique de Filière « Industries de sécurité » a été créé le 22 novembre 2018 dans le cadre du Conseil National de l'Industrie (CNI). Il donne lieu à un contrat de filière bâti autour de cinq projets structurants proposés par l'industrie et comportant des engagements de l'industrie et de l'Etat, formalisés dans un contrat de filière, en cours d'élaboration. Les projets structurants identifiés par la filière sont : Identité numérique, Cybersécurité et Sécurité des IOT, Sécurité des grands événements et des JO Paris 2024, Territoires de confiance, Numérique de confiance.