MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE

Liberté
Égalité
Fraternité

Direction générale
des Entreprises

FICHE EVENEMENT

DGE

Accélérer l'économie
de demain !

Journée autonomie et souveraineté numérique

Rendez-vous le 6 mai 2025 !

JE CHOISIS LA FRENCH TECH

→ www.entreprises.gouv.fr

Rendez-vous sur le numérique et cybersécurité

Rendez-vous le 6 mai 2025 pour cet événement qui mettra en relation des acheteurs privés et publics avec des entreprises françaises du secteur de la cybersécurité.

Cet évènement, labellisé « Je choisis la French Tech », est organisé par la Direction Générale des Entreprises (DGE).

Cette Journée constitue ainsi une réponse à ce problème, avec l'objectif de mieux faire connaitre l'offre souveraine en cybersécurité auprès des grands donneurs d'ordres publics et privés. Elle répond à un des engagements pris par l'Etat dans le cadre du contrat de filière des industries de sécurité.

Promouvoir l'offre nationale en cybersécurité

La Journée « Autonomie et souveraineté numérique » organisée également en partenariat avec le Comité Stratégique de Filière (CSF) Industries de Sécurité, vise à faciliter la rencontre entre les acteurs de la filière et les grands donneurs d'ordres publics et privés en cybersécurité.

Des « speed meetings » au programme

L'événement sera ponctué de différents rendez-vous tout au long de la journée : des « speed meetings » seront organisés pour que les offreurs de solutions puissent rencontrer un ensemble d'acheteurs privés et publics potentiellement intéressés par leurs solutions.

Lors de ces moments d'échanges, les donneurs d'ordre seront répartis par thématique sur différents espaces du Centre de Conférence Pierre Mendès-France. Les « offreurs », sur ordre de roulement, pourront un à un présenter leur solution à un groupe de donneurs d'ordres.

Toutes les parties prenantes seront réunies : des représentants des acheteurs publics, des représentants des offreurs et des représentants et acheteurs privés, ainsi que la Direction générale des Entreprises.

Sommaire

Au programme

13h30 : Accueil des participants

14h00 – 15h15 : Séance plénière avec une table-ronde sur La construction de la souveraineté numérique dans le secteur de la cybersécurité

15h15- 15h30 : Pause

15h30 – 18h00 : Ateliers de « Rencontres Offreurs / Donneur d'ordre » avec une pause à 17h

18h00 : Fin de l'évènement

Liste des acheteurs

ACHETEUR	BESOINS CYBER EXPRIMES
Action Logement Services	• Gestion des tiers • Sécurité des applications • Sécurité des données • Sécurité des réseaux
AFD	• Gouvernance • Sensibilisation - formation
ALBINGIA	• Gestion des tiers • Sensibilisation - formation
BOUYGUES IMMOBILIER / GROUPE TF1	• Sécurité des endpoints • Gestion des identités et des accès • Détection et réponse à incidents
BUSINESS FRANCE	• Détection et réponse à des incidents • Gestion des identités et des accès • Gestion des tiers • Gouvernance • Sensibilisation – formation • Sécurité des applications • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux
CAISSE des DEPOTS	• Gestion des tiers • Gouvernance • Sensibilisation - formation
CARREFOUR	• Gestion des identités et des accès • IOT - SI industriels • Sensibilisation - formation
CESIN	• Gestion des identités et des accès • Gouvernance • IOT - SI industriels • Sécurité des données
DAUPHIN TELECOM INFRASTUCTURE	• Détection et réponse à des incidents • IOT - SI industriels • Sécurité des réseaux
ENGIE	• Détection et réponse à des incidents • Gestion des identités et des accès • Gestion des tiers • Gouvernance • IOT - SI industriels • Sécurité des applications • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux

Exact international	• IOT - SI industriels • Sensibilisation – formation • Sécurité des données
Fives Maintenance	• IOT - SI industriels • Sensibilisation – formation • Sécurité des réseaux
FORSEE POWER	• Détection et réponse à des incidents • Gouvernance • IOT - SI industriels • Sensibilisation – formation • Sécurité des données
France Télévisions	• Gouvernance • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux
FUJITSU	• Gestion des identités et des accès • Gestion des tiers • IOT - SI industriels • Sécurité des données
GHT YVELINES Nord	• Gestion des identités et des accès • Sécurité des applications • Sécurité des données|Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux
KNDS France	• Gestion des identités et des accès • Gestion des tiers • IOT - SI industriels • Sécurité des données • Sécurité des réseaux
LCH SA/LSEG	• Détection et réponse à des incidents • Gestion des identités et des accès • Gestion des tiers • Gouvernance • Sensibilisation – formation • Sécurité des applications • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux
MINISTERE DE L'AGRICULTURE ET DE LA SOUVERAINETE ALIMENTAIRE	• Détection et réponse à des incidents • Gestion des identités et des accès • Gestion des tiers • Gouvernance • Sécurité des applications • Sécurité des données
MINISTERE DE L'ECONOMIE ET DE LA SOUVERAINETE INDUSTRIELLE ET NUMERIQUE	• Gestion des identités et des accès • Gestion des tiers • Gouvernance • Sensibilisation – formation • Sécurité des applications • Sécurité des données • Sécurité des réseaux

MINISTERE DES ARMEES	• Détection et réponse à des incidents • Gestion des tiers • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • IOT - SI industriels|Sensibilisation - formation|Sécurité des réseaux • Gouvernance • Sécurité des applications • Sécurité des données
MINISTERE DE L'EDUCATION NATIONALE	• Détection et réponse à des incidents • Gestion des identités et des accès • Sécurité des applications • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux
NaTran	• Détection et réponse à des incidents • Gouvernance • IOT - SI industriels • Sensibilisation – formation • Sécurité des applications • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux
OMNES Education	• Détection et réponse à des incidents • Gestion des identités et des accès • Sécurité des applications
Orange	• Gouvernance • Sensibilisation - formation • Détection et réponse à des incidents • Sécurité des applications • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail)
ORANO	• Gestion des tiers • Gouvernance • Sensibilisation – formation • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail)
OVHCloud	• Sécurité des données • Sécurité des réseaux
THALES	• Gestion des identités et des accès • Gouvernance • IOT - SI industriels • Sécurité des applications • Sécurité des données • Sécurité des réseaux
Tikehau Capital	• Détection et réponse à des incidents • Gestion des identités et des accès • Gestion des tiers • Gouvernance • IOT - SI industriels • Sensibilisation – formation • Sécurité des applications • Sécurité des données

	• Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux
UGAP	• Détection et réponse à des incidents • Gestion des identités et des accès • Gestion des tiers • IOT - SI industriels • Sensibilisation – formation • Sécurité des applications • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux
Université Paris Cité	• Détection et réponse à des incidents • Gestion des identités et des accès|Gouvernance • Sensibilisation – formation • Sécurité des applications • Sécurité des données • Sécurité des endpoints (serveurs et postes de travail) • Sécurité des réseaux

Liste des offreurs de solutions sélectionnés

❖ Détection et réponse à des incidents

ALCYCONIE

EGIDIUM TECHNOLOGIES

ERIUM

ORANGE CYBER DEFENSE

❖ Gestion des identités et des accès

NEOWAVE

Rubycat-Labs

STid

SYSTANCIA

WHALLIX

❖ Gestion des tiers

Board of Cyber

Smart Global Governance

❖ Gouvernance

FORMIND (SAS)

❖ IOT - SI industriels

EQUANS DIGITAL CYBER

Red Alert Labs

EGIDIUM TECHNOLOGIES

❖ Sécurité des applications

OGO Security

YesWeHack

Yogosha

❖ Sécurité des données

CLESSE

ERCOM

Factory systèmes

Hackuity

NetExplorer

OODRIVE

OXIBOX

QUADRA SAS / ARCAD Software

RANDORISEC

Scille

Streamwide

TIXEO

TotalLinux

Whaller

WYSAM

YouSign

❖ Sécurité des endpoints (serveurs et postes de travail)

CS GROUP

DOCAPOSTE

HarfangLab

KERYS Software

Nucleon-Security

❖ Sécurité des réseaux

CYBERIUM

NUMERYX TECHNOLOGIES

Olfeo

SESAME IT

SNOWPACK

STORMSHIELD

Synacktiv

❖ Sensibilisation-formation

Avant de Cliquer

CONSCIO TECHNOLOGIES

ERIUM

ONLY ROCKS / CYBELUDIK

Fiche d'identité / description des offreurs de solutions

❖ Détection et réponse à des incidents

ALCYCONIE

Alcyconie est l'acteur de référence en matière de **gestion et communication de crise cyber**.

Fondée en 2018, l'entreprise **prépare les organisations à gérer une cyberattaque** et **accompagne les équipes décisionnelles, techniques et opérationnelles** tout au long du cycle de crise :

1. **Avant** : avec plus de **500 exercices et entraînements réalisés** sur sa plateforme d'entraînement PIA®
2. **Pendant** : grâce à une offre d'**astreinte & gestion de crise à chaud**
3. **Après** : pour structurer les retours d'expérience et renforcer la résilience.

Nos expertises s'articulent autour de six piliers : **dispositifs de gestion de crise**, mise en conformité NIS 2, **simulations & exercices**, **communication de crise cyber**, **astreinte & crise à chaud**, **accompagnement juridique** et **formations**.

Alcyconie accompagne les organisations les plus sensibles – secteurs public, privé et Défense – et s'appuie sur une **équipe de 25 collaborateurs** répartis entre la Bretagne, le Campus Cyber à Paris, et le Campus Méditerranée.

Lauréate **France 2030** pour son projet ALCY-CognIA, Alcyconie est en **cours de qualification PACS par l'ANSSI**.

EGIDIUM TECHNOLOGIES

Depuis plus de quinze ans, Egidium développe une suite logicielle d'Hypervision (Smart Shield ERP) combinant plus de 250 composants, internes (+180 h.a), certains issus du monde de l'open source ou d'autres provenant de tiers.

Au regard de la complexité et de la consommation de ressources R&D internes liés au suivi des vulnérabilités de tous nos composants, nous avons décidé d'investir il y a quelques années sur le développement d'une plateforme maison, que nous avons nommée CyberVeille.

Celle-ci vise à automatiser ce processus ce MCS et organiser cette traçabilité en permettant, à partir d'un référentiel système (COTS, composants logiciels, OS, librairies…) déclaré, de générer automatiquement les rapports de vulnérabilités, de leur donner un score, d'affecter aux

équipes, etc… Nous réduisons ainsi les risques de sécurité informatique de nos produits de façon significative tout en générant des économies. Lors des JOP, notre plateforme Smart Shield ERP déployée pour la Ville de Paris, dont nous assurions le suivi avec CyberVeille, a été testée avec succès par l'ANSSI, ce qui a permis sa mise en œuvre pendant les jeux.

En discutant avec des clients et d'autres acteurs industriels de toutes tailles, nous nous sommes aperçus que ce besoin était général. Nous sommes donc en phase de test et de commercialisation de ce nouveau service.

ERIUM

Erium est un groupe français spécialisé dans la cybersécurité opérationnelle. Implanté à Paris, à Rennes et en Italie, Erium répond aux besoins essentiels des organisations : d'une part, la gestion des compétences et la maîtrise des crises, d'autre part, l'évaluation technique de leurs défenses.

Pour faire face à la complexité grandissante des cyberattaques, Erium propose des approches concrètes et innovantes :

- Former individuellement et collectivement les collaborateurs via la plateforme Cyber Investigation,

- Valider les capacités de défense grâce à des scénarios d'attaques répétés et ciblés avec la technologie BlackNoise,

- Anticiper les crises, s'entraîner et gérer la continuité grâce à l'accompagnement de nos équipes d'experts.

Cyber Investigation est une plateforme de sensibilisation aux risques de cybersécurité immersive et engageant.
A travers de parcours d'enquête, du E-learning ludique, l'animation d'évènements cyber, de phishing et de modules de renforcement spécifiques, Cyber Investigation permet à tous les profils de collaborateurs d'adopter les meilleures pratiques en matière de cybersécurité.

Cette approche différenciante a un taux de satisfaction très élevé (97%) et permet une forte mémorisation des sujets traités (75%) BlackNoise est le leader européen de Breach & Attack Simulation (BAS) et de la validation de cyberdéfense. Plateforme SaaS éditée par le groupe ERIUM, elle permet aux entreprises de tous secteurs de tester, valider et renforcer en continu leur posture défensive cyber. Grâce à des technologies d'automatisation avancées, BlackNoise identifie les vulnérabilités et valide les défenses contre les menaces en constante évolution, garantissant ainsi des mesures proactives et durables de cybersécurité.

ORANGE CYBER DEFENSE

Orange Cyberdefense, filiale du groupe Orange spécialisée dans la cybersécurité, est un acteur de référence en Europe, affichant un chiffre d'affaires de 1,2 milliard d'euros en 2024, avec une croissance de 11,2 % par rapport à l'année précédente. L'entreprise accompagne plus de 9 000 clients à travers le monde, dans divers secteurs.

Chaque année, elle joue un rôle actif dans la sécurité numérique mondiale, en neutralisant plus de 40 000 sites web malveillants. Sa présence régulière dans les principaux rapports de marché témoigne de sa légitimité et de son influence dans le domaine. Orange Cyberdefense est reconnue internationalement pour l'excellence de ses services en Managed Detection and Response, Incident Response and Digital Forensics, Threat Intelligence, et Managed Security Services.

Ses principales activités incluent la surveillance et détection des menaces via ses centres opérationnels de sécurité (SOC), la réponse aux incidents pour une intervention efficace en cas de cyberattaque, et l'évaluation des vulnérabilités à travers des audits de sécurité et des tests d'intrusion. Elle propose également des services de conseil, de formation et de sensibilisation pour aider les organisations à développer des stratégies de cybersécurité adaptées, ainsi que l'intégration de solutions de sécurité pour protéger les réseaux, applications et données.

Forte de plus de 3 100 experts en cybersécurité, d'un CERT interne hautement qualifié, et d'un Datalake alimenté par plus de 500 sources de renseignement, l'entreprise garantit à ses clients un niveau de protection exceptionnel.

Ainsi, Orange Cyberdefense s'affirme comme un partenaire stratégique de confiance pour les entreprises de toutes tailles souhaitant renforcer leur résilience face aux menaces numériques.

❖ Gestion des identités et des accès

NEOWAVE

NEOWAVE est une entreprise française spécialisée dans la conception, la production et la commercialisation de dispositifs d'authentification forte à base de composants sécurisés. Elle propose quatre gammes de produits : PKI ID 2.0, FIDO2, FIDO2 + ID 2.0 et les lecteurs de cartes à puce. Ils adressent les marchés de la confiance numérique, de la cybersécurité et de la gestion des identités. 100% conçus et fabriqués en France, ils répondent aux exigences de sécurité européennes (eIDAS, NIS2, RGPD,...). Ils sont utilisés par 150 clients professionnels. NEOWAVE est membre de l'Alliance de la Confiance Numérique (ACN), du pôle de compétitivité mondial Aktantis et de l'alliance internationale FIDO. NEOWAVE finalise actuellement, en partenariat avec la Gendarmerie Nationale, le développement d'un nouveau lecteur de carte à puce dédié aux services de l'état.

Rubycat-Labs

Créé en 2014, Rubycat est un éditeur français de logiciels cybersécurité, basé à Rennes. Spécialisé en traçabilité et contrôle des accès sensibles, sa solution de PAM* – Bastion, PROVE IT, répond au manque de visibilité des actions réalisées en interne comme en externe sur le SI.

Reconnue et labellisée (Label France Cybersecurity), la maîtrise totale de nos développements en France apporte une garantie de qualité et d'adaptation de nos produits aux besoins de nos clients.

Certifiée Visa de sécurité – CSPN par l'ANSSI (depuis 2018 et renouvelée en 2023), PROVE IT contrôle, trace et enregistre les actions effectuées par les comptes à privilèges. Elle permet de

tracer les accès internes (administrateurs, ...) comme externes (télémainteneurs, infogérants) au système d'information.

Cette certification ANSSI procure à nos offres une assurance de robustesse.

Utilisée par plus de 250 entreprises, du secteur public comme privé, PROVE IT est plébiscité pour sa simplicité d'utilisation, sa souplesse et sa facilité d'administration au quotidien. PROVE IT est une solution non invasive (aucun agent à installer), évolutive et rapide à déployer (installation en 30 minutes).

STid

STid, la tech qui sécurise et connecte vos mondes

Depuis plus de 25 ans, STid conçoit des solutions d'identification sans contact (RFID, NFC, Bluetooth®, IoT) pour sécuriser les accès, tracer les opérations et protéger l'identité numérique, même dans les environnements les plus sensibles comme l'aéronautique, l'énergie ou la défense.

Engagé pour une cybersécurité souveraine, STid a fondé la SPAC Alliance, qui fédère les acteurs de la sécurité physique et logique autour d'une ambition commune : bâtir une souveraineté européenne forte.
Ses missions : informer, influencer et agir pour un cadre légal juste, et promouvoir des technologies de confiance comme le protocole SSCP.

SYSTANCIA

Editeur de logiciels de cybersécurité souverain, reconnu plusieurs fois par le Gartner comme le seul acteur européen détenant une vraie technologie Zero Trust, Systancia propose la seule plateforme IAM Zero Trust qui permet de donner aux collaborateurs ou aux prestataires, quel que soit leur contexte (au bureau, en télétravail, chez un prestataire, opérateur industriel ...) un accès transparent, immédiat, sécurisé et tracé (métier ou privilégié, local ou distant, ...) à toutes les ressources dont ils ont besoin pour travailler.
cyberelements, qui réunit gestion des identités et des accès (IAM), gestion des accès à privilèges (PAM), vérification de l'identité (analyse comportementale de l'utilisateur– UBA) et accès distant sécurisé (ZTNA), se distingue par :

- un time to value de 3 minutes puisqu'il suffit de remplir 3 champs pour instancier en moins de 3 minutes une plateforme IAM Zero Trust prête à être configurée,
- des fonctionnalités de sécurité intrinsèque au Zero Trust qui offrent la meilleure protection contre les malwares/ransomwares.

WALLIX

WALLIX est un éditeur européen de logiciels de cybersécurité et un leader mondial dans la gestion, la sécurisation des identités, des accès et de la gouvernance. Fondée en 2003 à Paris, WALLIX est cotée à la bourse Euronext compte plus de 250 collaborateurs. WALLIX offre une gamme complète conçue pour renforcer la sécurité et assurer la conformité, en atténuant les risques liés aux accès non autorisés et aux cybermenaces. Le portefeuille WALLIX est disponible en versions sur site, hybride et à travers la plateforme SaaS, offrant ainsi une adaptabilité aux divers besoins organisationnels.

WORKFORCE ACCESS - Sécurisation fluide de tous les accès de tous les utilisateurs

WALLIX One IDaaS et WALLIX One Enterprise Vault améliorent la sécurité et l'expérience utilisateur en rationalisant l'accès avec SSO et MFA et en centralisant et chiffrant les données d'identités sensibles pour un partage sécurisé.

PRIVILEGED ACCESS - Sécurise les comptes et contrôle les privilèges

WALLIX PAM et WALLIX One Remote Access protègent les actifs informatiques critiques en gérant respectivement les comptes à privilèges, souvent cibles de brèches majeures, et en contrôlant l'accès à distance pour maintenir la sécurité tout en permettant une interaction transparente avec des prestataires externes.

GOVERNANCE - Examine les accès et contrôle les droits

WALLIX IAG améliore la gouvernance des accès en fournissant une cartographie complète des identités et de leurs autorisations respectives, en agissant comme une tour de contrôle pour superviser les campagnes de certification d'accès et en suivant le cycle de vie des identités du personnel dans toutes les applications de l'entreprise

❖ Gestion des tiers

Board of Cyber

Board of Cyber est une startup française fondée en 2022, spécialisée dans la gestion du risque cyber. Ses solutions SaaS totalement automatisées permettent à ses clients d'évaluer, piloter et améliorer en continu la performance cyber de leur organisation et de leur écosystème. Board of Cyber, avec ses 50 collaborateurs, accompagne plus de 500 clients. Sa mission est de contribuer à créer autour des organisations un écosystème de confiance.

Notre solution de Security Rating, non intrusive et en continu permet de noter, d'évaluer et d'améliorer votre posture cyber et celle de votre écosystème.

Smart Global Governance

Smart Global Governance est une société spécialisée dans les solutions innovantes de cybersécurité, conformité réglementaire et gestion des risques, reconnue par plus de 200 organisations en Europe pour son efficacité opérationnelle et sa sécurité certifiée (ISO 27001/27018, accréditée Europrivacy pour la conformité RGPD). Sa force réside dans un écosystème modulaire, flexible et entièrement interconnectable, permettant aux entreprises de composer rapidement des solutions sur mesure, adaptées à leurs besoins précis.

Parmi ses **12 modules**, Answer Writer se distingue particulièrement en permettant de répondre 10 fois plus vite aux questionnaires de conformité, appels d'offres et audits grâce à ses quatre agents d'intelligence artificielle spécialisés, assurant fiabilité, traçabilité complète et sécurité des données. Les modules IT & Cybersecurity (+50 normes et réglementations automatisées), Data & Privacy '(+60 normes et réglementations automatisées), gestion des risques tiers (TPRM) et Enterprise Risk Management (ERM) viennent compléter efficacement cet écosystème, en **automatisant jusqu'à 90 % des tâches répétitives**. Ainsi, Smart Global Governance permet aux entreprises d'accélérer leur performance numérique tout en garantissant une parfaite conformité aux réglementations les plus exigeantes.

❖ Gouvernance

FORMIND (SAS)

Formind est un leader Français indépendant expert en cybersécurité.

Notre mission est simple et belle : protéger nos clients.

Nous sommes des passionnés, animés par des valeurs d'excellence, d'engagement et de bienveillance.

Formind s'appuie sur des convictions fortes pour aider les entreprises à se sécuriser :

- identifier et protéger vos données les plus sensibles,
- mettre en place des dispositifs adaptés à votre contexte et conforme aux règlementations en vigueur,
- être en mesure de détecter au plus vite des attaques et de réagir très rapidement.

Des grands groupes privés aux PME et aux ETI en passant par le secteur public, nous vous aidons à mettre en place un environnement de confiance et à faire de la cybersécurité un véritable levier de performance de vos activités.

Qualifié PASSI depuis 2019, en cours de qualification PRIS et PACS par l'ANSSI et certifié ISO 27001, nous aidons nos clients à être plus résilients et à poursuivre ainsi leur développement à travers nos trois métiers :

Conseil – Intégration – SOC&CERT.

❖ IOT - SI industriels

EQUANS DIGITAL CYBER

Equans Digital Cyber : votre allié en cybersécurité IT/OT
Face à la convergence croissante des technologies IT et OT, sécuriser les infrastructures critiques est essentiel.
EDC accompagne ses clients avec des solutions sur mesure grâce à une approche 360° :
Protection & Prévention : Services axés sur la sécurisation proactive des systèmes pour prévenir les cybermenaces
Audit qualifié PASSI sur les portées : Audit organisationnel et physique, Audit d'architecture et Audit de configuration
Pentest IT & OT, ainsi que du red teaming
Délégation d'expertise GRC / RSSI / DPO
Sensibilisation et Formation via l'Académie Cyber
Conformité / DPO / NIS2
Surveillance & Détection : Services de type MSSP centrés sur la surveillance continue et la détection rapide des menaces.
SIEM /EDR / Sondes
SOC IT & OT base en France et disponible en 24/7
VOC
Threat Intelligence / CTI

Réponse & Résilience : Services dédiés à la gestion des incidents et à la capacité à se remettre d'une attaque.
PRA / PCA
CSIRT / Forensic
Gestion de crise
Reconstruction du SI
Grâce à notre expertise en cyberdéfense, automatisation et robotique, nous intégrons des solutions adaptées aux grandes entreprises privés ou acteurs publics, garantissant protection, résilience et conformité (NIS2, RGPD, CRA). Transformez vos défis cyber en opportunités avec Equans Digital Cyber!

Red Alert Labs

Red Alert Labs est un laboratoire européen indépendant spécialisé dans la cybersécurité des objets connectés. Nous accompagnons les entreprises dans la sécurisation, l'évaluation et la certification de leurs produits numériques.

Grâce à notre plateforme SaaS **CyberPass**, nous simplifions le parcours de conformité en proposant une gestion centralisée des évaluations, des preuves et des exigences réglementaires telles que la **RED Directive**, l'**EUCC** et le **Cyber Resilience Act (CRA)**.
Notre approche associe expertise technique, innovation et connaissance approfondie des schémas de cybersécurité européens, au service de la souveraineté numérique.

EGIDIUM TECHNOLOGIES

Depuis plus de quinze ans, Egidium développe une suite logicielle d'Hypervision (Smart Shield ERP) combinant plus de 250 composants, internes (+180 h.a), certains issus du monde de l'open source ou d'autres provenant de tiers.

Au regard de la complexité et de la consommation de ressources R&D internes liés au suivi des vulnérabilités de tous nos composants, nous avons décidé d'investir il y a quelques années sur le développement d'une plateforme maison, que nous avons nommée CyberVeille.

Celle-ci vise à automatiser ce processus ce MCS et organiser cette traçabilité en permettant, à partir d'un référentiel système (COTS, composants logiciels, OS, librairies…) déclaré, de générer automatiquement les rapports de vulnérabilités, de leur donner un score, d'affecter aux équipes, etc… Nous réduisons ainsi les risques de sécurité informatique de nos produits de façon significative tout en générant des économies. Lors des JOP, notre plateforme Smart Shield ERP déployée pour la Ville de Paris, dont nous assurions le suivi avec CyberVeille, a été testée avec succès par l'ANSSI, ce qui a permis sa mise en œuvre pendant les jeux.

En discutant avec des clients et d'autres acteurs industriels de toutes tailles, nous nous sommes aperçus que ce besoin était général. Nous sommes donc en phase de test et de commercialisation de ce nouveau service.

❖ Sécurité des applications

OGO Security

OGO Security est une société française proposant un service de protections et d'accélérations des sites web, applications et API.

La solution d'OGO offre une protection à l'origine complète en combinant WAF/WAAP, IA, Anti DDOS, Bot Mitigation et CDN international (200 PoP), tout en garantissant la souveraineté de voss données.

La solution, disponible en mode SaaS, on-premise ou en cloud souverain est compliant RGPD.

YesWeHack

YesWeHack est une plateforme globale de Bug Bounty et de gestion des vulnérabilités. Fondée par des hackers éthiques en 2015, YesWeHack connecte les organisations du monde entier à des dizaines de milliers de hackers éthiques, dont l'objectif est de découvrir les vulnérabilités potentielles au sein de sites web, applications mobiles, appareils connectés et infrastructures numériques.
Nos clients bénéficient d'un système de triage réalisé en interne, d'un accompagnement sur mesure, d'un modèle agile et adaptable à chaque contexte, et d'un paiement basé sur les résultats. Au travers de sa plateforme certifiée ISO 27001 & ISO 27017 et hébergée sur un Cloud souverain, YesWeHack propose les solutions suivantes :
- Bug Bounty : Permet aux organisations de créer des programmes de Bug Bounty publics ou privés et d'accéder à plus de 90 000 experts techniques référencés selon un processus strict.
- Politique de divulgation de vulnérabilités (VDP) : Permet aux organisations de créer un canal sécurisé et structuré, de remontées de failles de sécurité.
- Gestion des tests d'intrusions (Pentest Management) : Permet aux organisations d'utiliser un outil unique pour gérer et centraliser l'ensemble de leurs audits et tests d'intrusions.
- Gestion de la surface d'attaque (Attack Surface Management) : Permet aux organisations de mettre sous surveillance leurs actifs numériques exposés sur Internet.

Yogosha

Yogosha est éditeur d'une plateforme de Sécurité Offensive vous permettant d'industrialiser et de piloter vos opérations de Pentests, Bug Bounty et audits en temps réel, avec un lancement en 48h à 72h. Une approche agile et continue, alignée avec les exigences de conformité (NIS2, DORA, CRA) pour sécuriser efficacement vos assets.

Accédez à la Yogosha Strike Force, une communauté de 1000+ chercheurs en sécurité hautement qualifiés, et recevez vos vulnérabilités critiques en quelques heures ou jours.

❖ Sécurité des données

CLESSE

CLESSE est fabricant de systèmes industriels électroniques depuis 40 ans.

Nous proposons des ordinateurs, des serveurs et des logiciels 100% conçus et fabriqués en France.
Nous avons conçu entièrement un système d'exploitation (OS) sans backdoor pour garantir sûreté et sécurité de fonctionnement aux entreprises et institutions françaises.
Un hardware, un OS, et des applications, maîtrisés à Lyon.
Nous avons la maîtrise de la confidentialité de l'information.
Nous avons la maîtrise de la production.
Nous avons la maîtrise de son avenir.
Osez acheter français pour ne plus subir.
Maintenant vous avez le choix.

ERCOM

ERCOM, filiale du groupe Thales, est une société française reconnue pour ses solutions collaboratives sécurisées et de sécurisation de la mobilité. Nous proposons des solutions de sécurisation certifiées, souveraines et en conformité avec les plus hautes exigences fonctionnelles.

- Cryptosmart Mobile est une solution, développée en collaboration avec SAMSUNG, qui sécurise vos communications, vos données et vos terminaux mobiles (téléphone et tablette), avec un niveau de sécurité gouvernemental et un agrément Diffusion Restreinte par l'ANSSI*.
- Cryptosmart PC est un VPN sécurisé souverain qui protège vos connexions depuis et vers vos PC, vous assurant un niveau de sécurité et de confidentialité gouvernemental.
- 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, SecNumCloud 3.2, On Premise ou Hybride.
- Citadel Team est la solution de communication professionnelle sécurisée qui chiffre vos messages, vos conversations audios et vos visioconférences de bout en bout, disponible en SaaS sur un environnement Cloud ou SecNumCloud 3.2.

*en cours de renouvellement

Factory systèmes

Fort de ce constat et s'appuyant sur 40 années d'expertise dans le domaine de l'informatique industrielle et de l'embarqué, Advantech offre à travers DeviceOn, une solution logicielle de gestion et de sécurisation des équipements informatiques industriels.

Hackuity

80% des cyberattaques exploitent une faille de sécurité publiée il y a cinq ans. Bien que la remédiation des vulnérabilités critiques soit bien entendu une priorité pour les directions de cybersécurité, des équipes fragmentées, la multiplication des outils et l'explosion des vulnérabilités brident aujourd'hui l'efficacité des équipes cyber.

Fondés par plusieurs leaders de la cybersécurité, Hackuity réinvente la gestion des vulnérabilités pour mieux protéger les plus grandes organisations mondiales :

• Agréger les données de 80+ outils leader du marché au sein d'une plateforme unique.

• Prioriser vos vulnérabilités grâce à notre algorithme propriétaire de scoring des risques.

• Automatiser votre remédiation en l'adaptant à votre surface d'attaque.

Hackuity s'intègre à votre écosystème pour aider les équipes cyber à se concentrer sur les risques réels, plutôt qu'à manipuler des tableaux Excel. Notre plateforme met un terme aux silos de sécurité et fournit une vue unifiée de votre exposition cyber spécifique à votre surface d'attaque. En résumé, Hackuity est le catalyseur de votre VOC.

NetExplorer

NetExplorer : L'alternative souveraine aux GAFAM pour gérer, partager et sécuriser vos fichiers

NetExplorer est une solution française qui permet aux organisations de partager, collaborer et protéger leurs fichiers sensibles en toute confiance. Pensée pour répondre aux enjeux de cybersécurité et de souveraineté, notre plateforme vous offre un contrôle total sur vos données, sans compromis entre sécurité et efficacité. Certifiée ISO 27001, HDS et en cours de qualification SecNumCloud, NetExplorer associe performance et conformité réglementaire (RGPD, NIS2, DORA…).

Adoptée par plus de 1 800 entreprises et institutions (OFII, Veolia, BPI France, AP-HP, Société Générale…), NetExplorer s'intègre à votre environnement IT (SSO, API, connecteurs messagerie et visio) et couvre tous vos usages documentaires : partage sécurisé, collaboration, signature électronique, et stockage souverain.

Découvrez :

- NetExplorer Share : L'alternative sécurisée à WeTransfer.
- NetExplorer Workspace : Le drive collaboratif souverain, remplaçant SharePoint ou Google Drive.
- NetExplorer DataRoom : La plateforme française pour vos échanges de données sensibles.

OODRIVE

Oodrive est la première suite collaborative de confiance en Europe. Qualifiée SecNumCloud par l'ANSSI dès 2019, notre plateforme SaaS garantit cybersécurité, conformité réglementaire et souveraineté numérique.
Plus de 2,5 millions de professionnels ont choisi de collaborer sur leurs projets sensibles au sein de la bulle de confiance Oodrive. Oodrive a développé une suite logicielle pour permettre aux organisations et à leurs parties prenantes de collaborer en toute confiance. Notre suite logicielle offre une **alternative souveraine aux solutions GAFAM**, capable de capter, protéger et faire circuler en toute sécurité les données stratégiques d'une entreprise ou d'un organisme public. Cet ensemble prend la forme d'une bulle de confiance où toutes les données stratégiques peuvent être partagées, éditées, discutées … sans compromis sur leur intégrité ni leur confidentialité, en interne comme à l'externe.
Voici des liens utiles vers nos solutions :
Suite collaborative : https://www.oodrive.com/fr/produits/oodrive-work/
Signature électronique : https://www.oodrive.com/fr/produits/oodrive-sign/
Instances digitalisées : https://www.oodrive.com/fr/produits/oodrive-meet/
SecNumCloud : https://www.oodrive.com/fr/secnumcloud/

OXIBOX

Editeur d'une solution de sauvegarde sécurisée, notre solution permet de garantir la déconnexion des sauvegardes par le biais de manière logicielle, sans contrainte matérielle et avec une sécurité démontrée pour garantir la conformité avec les préconisations de l'ANSSI.

QUADRA SAS / ARCAD Software

ARCAD Software est un éditeur de logiciels français implanté en Haute-Savoie. Depuis plus de 30 ans, nous accompagnons les organisations dans la gestion du cycle de vie de leurs applications, sur technologies ouvertes comme legacy, avec une attention particulière portée à la cybersécurité et au respect de la souveraineté numérique.

À travers sa branche DOT, ARCAD propose des solutions de gestion des données de test. DOT Anonymizer permet de générer des données fictives mais cohérentes pour les environnements hors production (test, formation, sous-traitance), réduisant ainsi les risques de fuite de données

personnelles et identifiantes, tout en garantissant la conformité au RGPD. DOT Extract permet l'extraction d'ensembles cohérents depuis la production, optimisant les environnements de test, accélérant les processus et réduisant l'empreinte environnementale.

RANDORISEC

Fondée en 2015 par des experts en sécurité des systèmes d'information, RandoriSec est une entreprise de services à taille humaine qui propose les services suivants :

- Tests d'intrusion et audits de sécurité

- Rétro ingénierie et recherche de vulnérabilités

- Audit et analyses inforensiques de plateformes mobiles

Elle s'appuie sur le savoir-faire de ses consultants qui accompagnent depuis 15 ans leurs clients dans la maîtrise des risques associés aux usages des technologies numériques.

SCILLE

PARSEC, solution certifiée ANSSI, sécurise le partage des grosses volumétries de données sensibles (vidéos, plans...). Nous visons des secteurs dans lesquels la sécurisation des données sensibles est règlementée. PARSEC assure chiffrement, garantie d'intégrité et résilience des données tout en sécurisant le partage entre personnes autorisées :
• Partage simple et rapide des informations sensibles de la supply chain grâce à une version web
• Confidentialité et intégrité des informations partagées, visibilité instantanée des partages et de leur gestion du « Droit-à-en-Connaître »
• Utilisation des réseaux civils pour se fondre dans la masse des utilisateurs
• Fonctionnement asynchrone sur des réseaux contraints permettant le transfert de documents volumineux sans interruption.
• Transfert de pièces jointes via un lien non confidentiel
• Diffusion restreinte : homologation engagée par la DINUM pour la version Resana Secure de PARSEC.

Streamwide

STREAMWIDE, est l'un des principaux fournisseurs des technologies françaises proposant des solutions de collaboration et de communication depuis plus de 20 ans pour les entreprises et pour les services publics.
Notre mission est d'offrir aux organisations et aux individus des solutions logicielles innovantes, sécurisées et souveraines pour les accompagner dans leur parcours de transformation numérique. Mettre la technologie au service de l'humain et favoriser une coordination efficace des équipes sous la promesse 'ACT AS ONE' constituent le fondement même de notre mission. La solution Team on the run présentée, accessible depuis un mobile ou une interface web, propose notamment une suite collaborative professionnelle (voix, video, données en temps réel) jusqu'aux services de géolocalisation, d'alerte et de transformation numérique des processus opérationnels sans compromettre la protection de vos données.

TIXEO

Depuis plus de 20 ans, Tixeo, éditeur français de solutions de collaboration sécurisée, accompagne de grandes organisations pour garantir l'efficacité et la sécurité de leurs échanges en ligne dans le cadre de leurs activités critiques. Disponible en mode Cloud ou On-Premise, Tixeo propose sa propre technologie de visioconférence, certifiée par l'ANSSI, qui vient compléter les solutions de collaboration standards pour encore plus de confidentialité. Conçue selon une approche Secure by Design, sa technologie intègre un véritable chiffrement de bout en bout des communications quel que soit le nombre de participants. Tixeo assure un niveau de confidentialité sans précédent aux communications de ses utilisateurs et permet aux organisations de limiter le risque cyber, renforcer leur cyber-résilience ou les aider à se conformer aux réglementations. Les solutions Tixeo sont particulièrement utilisées dans des secteurs clés tels que la défense, l'aérospatiale, l'industrie, l'énergie, la finance, et par diverses instances étatiques et juridiques.

TotaLinux

TotaLinuX est une Scale-Up DeepTech française fondée en 2004, spécialisée dans la mise en production de systèmes AI et HPC pour les entreprises du CAC40 et les acteurs mondiaux du numérique.
L'entreprise conçoit et exploite ses propres data centers souverains via son programme ITrium, combinant performance, sécurité et sobriété énergétique.

TotaLinuX propose aussi la construction de data centers labélisés Expert Cyber, hébergeant les solutions de Zenetys.
Notre offre Expert Cyber Zenetys accompagne les DSI publics et privés dans la conception, la sécurisation et l'exploitation d'infrastructures IT, avec une expertise Open Source forte.
L'équipe DevSecOps de Zenetys cumule plus de 25 ans d'expérience dans le développement de solutions sur-mesure et la gestion de services managés.
Cette expertise se traduit notamment par l'évolution de la solution SaaS LogVault, dédiée à l'archivage et à l'indexation des logs via des briques open source

Whaller

Whaller est une plateforme sociale et collaborative sécurisée pouvant accueillir plusieurs milliers de personnes. Whaller est le seul outil simple et complet pouvant répondre à un spectre aussi large d'usages. Whaller permet de construire des réseaux collaboratifs de toutes tailles et de toutes natures et ce, pour tous types de structures : entreprises, administrations, associations, écoles et universités, institutions, ministères, familles… L'incessibilité et la non-exploitation des données personnelles constituent deux principes fondamentaux de la plateforme. En se basant sur des communautés appelées des « sphères », indépendantes les unes des autres, Whaller permet à ses utilisateurs de maîtriser leurs communautés, leurs communications et leurs audiences. La plateforme Whaller DONJON, seule solution collaborative qualifiée SecNumCloud (SaaS), répond à toutes les exigences de la directive NIS2 mise en place au deuxième semestre 2024, offrant ainsi une solution fiable et conforme aux exigences de sécurité les plus strictes. Whaller a été créé en 2013 par Thomas Fauré, la plateforme regroupe aujourd'hui plus de 1 000 000 utilisateurs pour 50 000 réseaux créés. https ://whaller.com

WYSAM

Wysam est une solution conçue pour les TPE et PME qui souhaitent sécuriser leurs échanges de données numériques sans complexité. Ce n'est pas un secret, l'email est aussi vulnérable qu'une carte postale et les messageries instantanées ne sont pas en mesure de garantir une confidentialité absolue des échanges. Wysam propose une plateforme pour assurer la sécurité, la confidentialité et l'intégrité des échanges de données sensibles.

Notre plateforme c'est :

- Des envois et réceptions sécurisés de fichiers et de messages confidentiels
- Une interface simple et accessible pour tous
- Une intégration fluide dans les usages professionnels existants
- Une conformité RGPD et une infrastructure hébergée en France

Wysam est plus qu'un outil : c'est une approche responsable et sécurisée pour les échanges de données sensibles avec vos interlocuteurs.

Découvrez Wysam en 4 minutes sur www.wysam.fr

YOUSIGN

Fondée en 2013, Yousign est une plateforme européenne de signature électronique et de services de confiance. Elle simplifie la signature électronique, garantit l'intégrité et la traçabilité des transactions digitales et assure leur conformité aux normes européennes, notamment eIDAS.
Yousign accompagne plus de 25 000 organisations, des PMEs aux grandes entreprises, dans leur transformation et leur sécurisation digitales avec une solution complète leur permettant de signer, valider, certifier et authentifier leurs documents de manière 100 % électronique.
Enfin, grâce à son API flexible et facile à intégrer, Yousign s'intègre parfaitement aux outils métiers, offrant une expérience fluide et adaptée aux besoins des entreprises.

❖ Sécurité des endpoints (serveurs et postes de travail)

CS GROUP

a Sopra Steria company

CS GROUP assure la conception, la réalisation, le déploiement, la maintenance ainsi que l'exploitation de systèmes critiques, combinant sûreté et cybersécurité et intégrant de l'intelligence artificielle. Ces systèmes, basés sur des solutions souveraines, développées et maîtrisées par le groupe, garantissent l'efficacité de la conduite et de la sécurité des opérations et des missions critiques de nos clients, sur des marchés exigeants.

DOCAPOSTE

« Le Pack Cyber de Docaposte est une offre de service unique qui permet de couvrir l'ensemble des besoins de cybersécurité avec un seul point d'entrée, donc un interlocuteur unique. Cette offre exclusive permet de simplifier la couverture, le déploiement et la gestion au quotidien de tous les outils indispensables pour protéger les entreprises.

Avec un seul contrat et une seule facture, en fonction de leurs besoins, les TPE, PME et ETI peuvent protéger leur activité des risques cyber, en couvrant les trois piliers de la chaîne de sécurisation : se préparer, se protéger et réagir :

- Diagnostic initial et détection des vulnérabilités
- Sauvegarde sécurisée et automatique des données
- Détection et blocage des cyberattaques sur les équipements
- Analyse des flux applicatifs et messagerie (anti-spam, phishing, virus)
- Gestionnaire de mots de passe
- Supervision des événements et alertes
- Restauration en cas d'incident
- Partenariat avec un "assureur cyber »

Pour garantir la performance de son offre, le Pack Cyber réunit 14 acteurs français et européens de la cybersécurité respectant nos engagements et nos valeurs en matière de confiance numérique, et démontrés par leurs visas, certificats de sécurité, qualification ou attestation de conformité (ISO27001, certification HDS, datacenters qualifiés tier 3…). »

HarfangLab

HarfangLab est un éditeur français de solutions logicielles de cybersécurité spécialisé dans les technologies Endpoint Detection and Response (EDR) et Endpoint Protection Platform (EPP), permettant la détection et la réponse aux attaques sur les terminaux (postes de travail et serveurs). Les solutions HarfangLab sont certifiées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et peuvent être déployées en Cloud et On-premise.

Fondée en 2018, HarfangLab sert aujourd'hui plus de 600 clients privés et publics et collabore avec une trentaine de partenaires fournisseurs de services de cybersécurité (MSSP) en Italie et en Europe.

KERYS Software

KERYS Software est un éditeur de logiciels fournissant une solution de virtualisation sécurisée et performante visant divers cas d'utilisation aujourd'hui non couverts par les outils historiques : Postes de travail multiple, IA, Bases de données intensives...

Notre solution est :

- Sécurisée : nous visons un niveau de sécurité équivalent à celui des cartes de paiement
- Performante : tirez parti de la puissance réelle de la machine sans modification des environnements de travail

Pour tous ceux qui ont 2 PC ou plus pour des raisons réglementaires, d'outils de travail différents ou besoin de performance, notre solution permet d'embarquer dans un seul poste physique plusieurs environnements Windows / Linux sans modification des environnements de travail, avec une prise en main simple en 3 minutes et un accès sans connexion nécessaire. Les administrateurs configurent les politiques de sécurité de manière centralisée pour les différents profils. En mutualisant ainsi les postes de travail vous :

- Diminuez mécaniquement l'empreinte carbone de votre infrastructure IT de plus de 40%
- Simplifiez le quotidien de vos collaborateurs
- Diminuez votre facture informatique.

Nucleon-Security

Nucleon Security développe une plateforme de sécurité des endpoints (EDR) combinant Zero-Trust et IA pour détecter et bloquer les cybermenaces en temps réel. La solution automatise la génération de règles adaptatives, intègre une analyse comportementale avancée et s'interface facilement via API. Malprob, la solution d'analyse de fichiers par IA, détecte les fichiers malveillants et les menaces zero-day. Nucleon Security protège plus de 70 clients en Europe, Afrique et Amérique latine.

❖ Sécurité des réseaux

CYBERIUM

Cyberium est une PME française spécialisée dans la sécurisation des réseaux pour des secteurs critiques comme les réseaux industriels, les agences gouvernementales et les infrastructures Cloud. Grâce à une technologie brevetée de proxy logiciel, Cyberium améliore la flexibilité, la fiabilité, la bande passante et la sécurité des solutions de cybersécurité.

Notre innovation permet aux entreprises d'utiliser des solutions avancées comme les Data Diodes unidirectionnelles, conformes aux normes strictes (certification ANSSI en Italie, standard international Common Criteria EAL 7+). Cela permet aux entreprises de protéger leurs données sensibles tout en respectant les directives de sécurité comme NIS2, sans perturber leurs flux de données habituels.

NUMERYX TECHNOLOGIES

Numeryx est un acteur Européen de la transformation digitale, spécialisé dans la cybersécurité, les services IT managés et l'infogérance. Nous accompagnons les entreprises de toutes tailles — PME, ETI et grands comptes — dans la sécurisation, l'optimisation et la gestion de leur système d'information. Notre offre couvre l'ensemble du cycle de vie des infrastructures IT : conseil, intégration, exploitation, cybersécurité, ainsi que de la formation et le placement d'experts IT pour renforcer les équipes de nos clients.

Parmi nos solutions phares que nous pourrons présenter le 06 mai prochain, ASGUARD se distingue comme un firewall nouvelle génération (NGFW) intégrant des technologies avancées de Zero Trust Network Access (ZTNA). Décliné en plusieurs formats — matériel, virtuel ou As a Service — ASGUARD permet de protéger efficacement les environnements cloud et on-premise. Facile à déployer et à administrer, il offre une réponse agile aux nouvelles menaces, tout en s'adaptant aux enjeux de performance, de mobilité et de conformité des entreprises modernes.

Olfeo

Olfeo est l'éditeur français de référence en matière de filtrage web, proxy et contrôle d'accès Internet.
Notre solution garantit sécurité, conformité réglementaire et souveraineté numérique de la navigation internet, en s'appuyant sur une base de données d'URLs 100 % française.
Nous accompagnons plus de 1000 organisations dans la protection de leurs accès Internet tout en assurant productivité et conformité.

Le 6 mai, nous dévoilerons également nos dernières innovations en matière de Security Service Edge (SSE) et de CASB permettant de se protéger contre le Shadow IT.
Notre approche renforce la souveraineté numérique tout en répondant aux exigences de cybersécurité modernes.
Olfeo aide les entreprises à sécuriser l'usage d'Internet et du cloud, dans le respect des réglementations locales.
Nos solutions s'adaptent à chaque environnement SaaS ou On-Premise pour un contrôle efficace, simple et souverain.

SESAME IT / JIZO AI

Fondée en 2017, Jizô AI est une société française spécialisée dans la cybersécurité, qui accompagne les organisations françaises et européennes dans le déploiement de leur stratégie de cyberdéfense.

Sa plateforme d'observabilité des réseaux permet aux décideurs d'anticiper, d'identifier et de bloquer les cyberattaques, avec une efficacité prouvée sur de nombreux réseaux critiques de grandes entreprises et d'administrations. Jizô AI combine une architecture de détection multicouches à une intelligence artificielle avancée pour offrir une visibilité complète sur les réseaux IT, OT et Cloud, y compris les flux chiffrés.

Son système d'intelligence artificielle propriétaire apprend en continu des données réseau de l'organisation, permettant une détection proactive des anomalies et une réduction significative des faux positifs.

Conçue pour être entièrement sécurisée, sans partage de données et transparente dans les règles de détections, Jizô AI est utilisé par des organisations exigeantes pour sécuriser leurs infrastructures, offrant des alertes claires et exploitables qui accélèrent les réponses à incidents par les équipes sécurité.

SNOWPACK

« Si les hackers ne vous voient pas, ils ne peuvent pas vous hacker ! » Fondée sur ce principe, Snowpack, spin-off cybersécurité du CEA, lauréate 2024 du prix des Assises et du Forum InCyber, développe la technologie brevetée d'invisibilité VIPN qui garantit un niveau inédit d'autonomie et de souveraineté numérique. En supprimant toute dépendance à un tiers de confiance (y compris Snowpack), nous permettons aux organisations de protéger leurs utilisateurs, serveurs, objets connectés, services et données exposés sur Internet en les rendant totalement invisibles aux attaquants.
Seuls les acteurs explicitement autorisés pourront voir et accéder aux ressources numériques protégées par Snowpack. Et contrairement aux solutions traditionnelles de type ZTNA ou SASE, Snowpack ne voit, n'héberge ni n'intercepte les flux de données : les organisations regagnent ainsi la maîtrise complète de leurs infrastructures numériques (y compris au niveau applicatif) et de leurs données, sans dépendre d'un fournisseur tiers.
Les cas d'usage que nous adressons sont notamment :

- Réduire la surface d'attaque externe du SI
- Sécuriser les accès externes et distants au SI à des services web / systèmes / services d'administration / API sensibles
- Prévenir les risques d'exploitation de mauvaises configurations
- Simplifier la gestion de l'obsolescence et des opérations à distance sur les équipements industriels sans les exposer
- Protéger les opérations sensibles des équipes SOC et CTI
- Protéger les communications des utilisateurs sensibles

STORMSHIELD

Stormshield est un acteur européen majeur de la cybersécurité, reconnu pour ses solutions certifiées et qualifiées par l'ANSSI. Nous développons des technologies souveraines, de confiance, et répondant à la fois aux enjeux de l'IT et de l'OT.

Complémentaires, nos technologies permettent de sécuriser de bout en bout les réseaux, les postes de travail et les données, offrant ainsi une protection optimale aux entreprises et organisations exploitant des infrastructures critiques, des données sensibles et des environnements industriels.

Partenaire de confiance des ministères, des OIV, des OSE et des entreprises stratégiques, Stormshield s'engage pleinement pour renforcer la souveraineté numérique française et européenne.

Synacktiv

Synacktiv est une société spécialisée en cybersécurité offensive fondée en 2012 par des experts du domaine.
Son expertise s'articule autour de plusieurs activités :
- Tests d'intrusion et audit de sécurité
- Ingénierie inverse et recherche de vulnérabilités
- Développement d'outils en cybersécurité
- Réponse à Incidents

Synacktiv est qualifiée PASSI LPM (Prestataires d'audit de la sécurité des systèmes d'information) sur toutes les portées ainsi que CESTI (Centre d'Evaluation de la Sécurité des Technologies de l'Information).
Synacktiv emploie une équipe de plus de 150 experts sécurité depuis ses différents locaux à Paris, Toulouse, Lyon, Rennes, Lille et Bordeaux.

❖ Sensibilisation-formation

Avant de Cliquer

Avant de Cliquer réinvente la sensibilisation à la cybersécurité en mettant en place un programme SaaS de sensibilisation complet (PHISHING, Spear Phishing, SMS, Clés USB, Qrcode, VISHING…) et automatique, créé sur mesure pour chaque utilisateur et en l'animant sur la durée sans intervention du professionnel du système d'information (RSI, RSSI, DSI, DPO…). De plus, un chargé de compte dédié vous accompagne afin d'améliorer vos résultats.

CONSCIO TECHNOLOGIES

Conscio Technologies est un éditeur de logiciel SaaS et de contenus de sensibilisation. Nous accompagnons les RSSI, DSI depuis 17 ans dans la mise en œuvre de leur stratégie de sensibilisation cyber en ligne. Notre offre s'appuie sur une approche sectorielle, un catalogue riche (modules, scénarios test phishing), un accompagnement personnalisé…

ERIUM

Erium est un acteur reconnu de la cybersécurité opérationnelle qui accompagne les organisations face aux menaces cyber à travers trois offres complémentaires :

1. **Gestion des compétences et sensibilisation**
Plateforme cyberinvestigation.fr : apprentissage par la pratique, e-learning, mises en situation réelles et animation d'événements collectifs.

2. **Validation des capacités défensives**
Solution blacknoise.co : première solution européenne de simulation d'attaques pour mesurer l'efficacité en conditions réelles de la détection et de la réaction.

3. **Gestion de crise cyber**

Sous la direction d'Olivier Caleff (référent en France et à l'international) : programme de formation, de préparation et d'entraînement à la gestion de crise et à la continuité d'activité métier.

Erium compte parmi ses clients : 50% des entreprises du CAC 40, de nombreuses ETI et d'acteurs publics majeurs. Les capitaux du groupe sont 100% français.

CyberLudiK

CyberLudik innove en créant des formats ludiques et immersifs pour sensibiliser les publics à la cybersécurité et à protection des données. En s'appuyant sur des outils comme des bandes dessinées, une fresque ou encore une mallette pédagogique, ces outils made-in-france transforment des thématiques complexes en expériences accessibles, engageantes et impactantes. 100% personnalisables, ces supports peuvent être adaptés à chaque cadre normatif ou réglementaire, et au contexte de l'organisme ; il est également possible de transposer votre analyse de risques ou votre PCA/PRA en jeu !
Notre dernière innovation est le phishing USB : une clé USB qui permet de tester vos collaborateurs, et dont les indicateurs remontent même si les ports USB interdisent la connexion de stockage amovible.

Vigidomaine centralise dans une seule plateforme toutes les fonctions clés de surveillance cyber, auparavant dispersées entre de multiples outils complexes. Grâce à une automatisation intelligente, une approche souveraine et une architecture frugale, il rend la cybersécurité proactive. Il innove en combinant la surveillance des noms de domaine, des politiques email, de la disponibilité web et du DNS dans un outil simple et efficace

Conception : DGE
Réalisation : Sircom
Photos : @Adobe stock

→ www.entreprises.gouv.fr

@DGEntreprises

#DGEntreprises