CYBERSÉCURITÉ

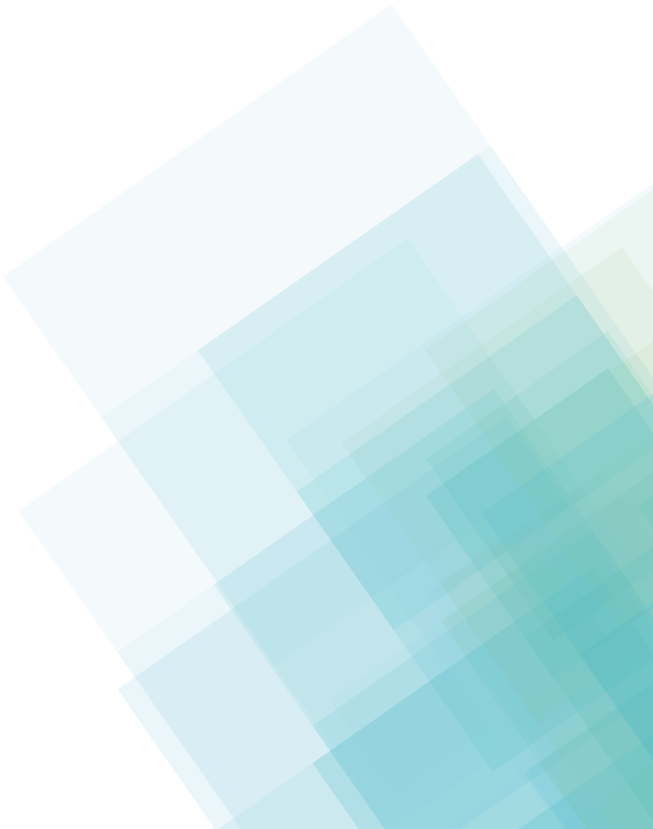
Approche capacitaire

ACN
Alliance pour la Confiance Numérique

FIEEC

GICAT

HEXATRUST
CYBERSECURITY & DIGITAL TRUST



EDITO

MOUNIR MAHJOUBI,

SECRÉTAIRE D'ÉTAT CHARGÉ DU NUMÉRIQUE

Le numérique est un facteur d'innovation majeur de nos sociétés qui a créé un nouvel espace au-delà des états et des frontières. Cet espace se développe tous les jours et des pans entiers de notre vie aussi bien physique que numérique s'y déroulent aujourd'hui. La sécurisation de cet espace est un des défis majeurs de la transformation numérique.

L'ambition du gouvernement est de faire de cet espace numérique, un espace de confiance pour l'ensemble des citoyens et des acteurs économiques. Cette confiance doit s'appuyer sur l'implication de tous et doit refléter nos valeurs de liberté, d'humanisme et d'égalité. La France et l'Europe portent cette vision singulière sur le numérique et construisent aujourd'hui un cadre adapté aux enjeux : il reflète l'attention de nos concitoyens pour le respect de la vie privée, pour la préservation d'un espace ouvert permettant l'innovation en défendant la neutralité d'internet et pour l'excellence technique, qui doit se traduire dans la certification de sécurité européenne.

Dans ce cadre, la structuration et le développement d'une filière française et européenne puissante en matière de sécurité numérique est indispensable pour relever ce défi. En se concentrant sur son excellence scientifique et sur son tissu d'entreprises innovantes allant des startups aux nombreuses PME reconnues pour la qualité de leurs produits et services, dont ce catalogue vous montrera les différentes facettes, la France se positionne pour devenir le leader européen de la sécurité numérique.

LA CYBERSÉCURITÉ

La cybersécurité peut se définir comme l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Dans un monde de plus en plus connecté, la cybersécurité est donc au cœur des enjeux et se positionne comme un préalable nécessaire à toute transition numérique.

Elle recouvre en effet un spectre très large, de la sécurité nationale de chaque Etat (défense, sécurité intérieure, administrations publiques), en passant par les infrastructures vitales (énergie, transport, santé, …), le secteur privé (industries, banques, mobilité, commerces, services, ….) jusqu'aux populations.

Qu'elles soient le reflet de motivations crapuleuses, idéologiques, stratégiques ou géopolitiques, les cyberattaques visent désormais tous les publics connectés aussi bien des citoyens, des entreprises, que des administrations avec des conséquences de plus en plus importantes.

Une prise de conscience collective s'impose : la confiance est un élément majeur pour le développement du numérique et la réalisation de toutes les promesses entrevues grâce à la connectivité. Cette confiance ne pourra s'obtenir que par l'intégration, dès la conception des produits et solutions, de la sécurité numérique (*security by design*) et de la protection des données personnelles (*privacy by design*).

Les savoir-faire et les outils existent et sont à disposition des utilisateurs pour les aider à relever ce défi. L'objectif de cette brochure capacitaire est de les guider dans cette démarche.

EN FRANCE : UNE INDUSTRIE PERFORMANTE AU SERVICE DE LA CONFIANCE NUMÉRIQUE

La France dispose, dans le domaine de la cybersécurité mais aussi de la confiance numérique, d'un tissu de laboratoires reconnus et d'un ensemble d'entreprises dotées de compétences larges. Cet ensemble, composé à la fois de grands groupes et de PME agiles et dynamiques offre tout un panel de compétences extrêmement précieux qui permet à notre pays de figurer parmi les leaders mondiaux dans ces domaines stratégiques.

Le cycle de cybersécurité

CONSEIL EN CYBERSÉCURITÉ

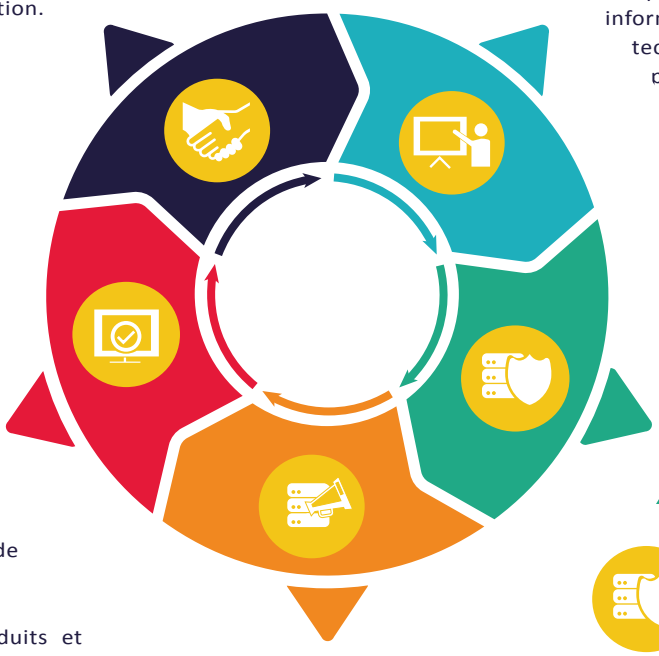
Le champ « Conseil en cybersécurité » permet de recourir à une expertise externe pointue pour mieux appréhender la sécurité de ses systèmes d'information.

La sécurisation et le maintien en condition de sécurité du système d'information est une action indispensable pour toute entité. Par la complexité et la diversité des systèmes et technologies interconnectés, cette sécurisation nécessite des experts à la fois en sécurité des systèmes d'information et dans chaque technique utilisée pour manipuler l'information. Ces spécialistes possèdent les qualifications nécessaires et sont à même de rendre des prestations de haut niveau en matière de gouvernance, contrôle, conception/intégration.

FORMATION-SENSIBILISATION

Le champ « Formation – sensibilisation » est un élément indispensable à la sécurisation d'un système d'informations.

Chaque maillon de la chaîne d'un système d'information participant à la sécurisation de celui-ci, les formations en cybersécurité sont indispensables pour garantir la sécurité de l'ensemble. Ces formations s'adressent à l'ensemble des salariés d'une entreprise (direction, management, techniciens, employés, etc.) et s'adaptent à leurs connaissances et à leur niveau de technicité. De la sensibilisation aux premières règles d'hygiène informatique, jusqu'à la formation technique la plus pointue, en passant par la formation des dirigeants aux enjeux et à la gestion des incidents cyber, tous les niveaux de l'entreprise doivent être formés pour obtenir une cybersécurité efficacité.



INVESTIGATION RÉSILIENCE-RENSEIGNEMENT

Le champ " Investigation et Résilience" fait suite à un incident.

Les objectifs de cette phase sont :
- d'analyser l'incident afin d'empêcher sa reproduction
- de réunir les preuves en cas de malveillance
- de permettre la continuité du service

Ce champ réunit l'ensemble des produits et solutions permettant de minimiser les préjudices des incidents et des sinistres, d'analyser les faits et de revenir à l'état initial le cas échéant.

PRÉVENTION PROTECTION

Le champ «Prévention et Protection» se situe en amont d'un incident et perdure tout au long de la durée de vie du système.

Il s'agit entre autres :
- d'anticiper et de prévoir les menaces et vulnérabilités et d'en déduire les risques
- de définir les architectures et procédures
- d'installer, configurer et maintenir en condition les ressources

Ce champ concerne l'ensemble des produits et solutions permettant d'éviter l'apparition des incidents et des sinistres sur une infrastructure et de s'y opposer.

DÉTECTION-RÉACTION

Le champ « Détection et Réaction » permet de détecter et contenir les attaques.

Le but est ici :
- de détecter les incidents et sinistres
- de collecter et d'analyser les flux et les comportements sur les systèmes afin de détecter un incident si celui-ci n'a pas été signalé auparavant
- de provoquer une réaction adéquate afin de circonscrire l'incident

Ce champ concerne l'ensemble des produits et solutions permettant la détection et le blocage des incidents et des sinistres sur une infrastructure.

Comment lire ce guide ?

Ce guide a été conçu pour pouvoir répondre aux besoins de toute entité s'interrogeant sur la cybersécurité et recherchant les offres disponibles dans ce domaine. Pour offrir la plus grande visibilité aux lecteurs trois critères différents ont été retenus classer les offres.

Le critère principal retenu pour la présentation de ce guide est celui de la catégorie de l'offre (voir les 11 catégories retenues ci-dessous).

Catégories d'offres de Cybersécurité

GOUVERNANCE, TRAÇABILITÉ ET AUDIT

Security Information and Event Management (SIEM), Systèmes de gestion, traçage et suivi

GESTION DES IDENTITÉS ET DES ACTES

Contrôle d'accès, identification, authentification, systèmes biométriques

SÉCURITÉ DES DONNÉES, CHIFFREMENT

Chiffrement de données, signature, Infrastructure de gestion de clés (IGC), archivage sécurisé, Digital Rights Management (DRM)

SÉCURISATION DE LA MESSAGERIE

Anti-spam, chiffrement de mails, messagerie sécurisée

SÉCURISATION DES APPLICATIONS

Sécurité des développements et des applications, test et modélisation

PROTECTION DES FLUX MOBILES ET WEB

Filtrage de contenu, filtrage applicatif, sécurité des communications

SÉCURITÉ DE L'INFRASTRUCTURE ET DES ÉQUIPEMENTS

Firewalls, antivirus, anti-dos, Intrusion Detection System (IPS/IDS), Web Application Firewall (WAF), matériel de chiffrement réseau, Hardware Security Module (HSM)

SÉCURITÉ DES RÉSEAUX INDUSTRIELS

Sécurité et supervision des réseaux industriels, cloisonnement des équipements

AUDIT, CONSEIL ET FORMATION

Audit, test de vulnérabilité et d'intrusion, gestion des risques et des menaces, forensics

INFOGÉRANCE ET EXPLOITATION

Support d'exploitation, Managed Security Service Provider (MSSP), gestion de continuité d'activité, tiers de confiance

RENSEIGNEMENT

Recueil, traitement et analyse de la masse de données présentes dans le cyberespace pour en déduire des informations pertinentes

Cycle de Cybersécurité

CONSEIL
EN CYBERSÉCURITÉ

FORMATION
SENSIBILISATION

PRÉVENTION
PROTECTION

DÉTECTION
RÉACTION

INVESTIGATION
RÉSILIENCE-RENSEIGNEMENT

Pour compléter cette approche, nous avons aussi souhaité introduire un deuxième critère qui est celui du positionnement de cette offre dans le cycle temporel de la cybersécurité, selon qu'elle se place avant, pendant ou après un incident potentiel (voir page 5).

Nature de l'offre

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

Deux tableaux synthétiques de présentation de l'ensemble des offres sont proposées au pages suivantes. Ces tableaux récapitulatifs permettent de croiser ces critères deux à deux et ainsi d'avoir une lecture dynamique selon les critères les plus pertinents en fonction de la recherche. Ces tableaux opèrent des renvois vers les pages suivantes de ce guide qui comportent à la fois les descriptions détaillées des offres proposées (partie 2), mais aussi des présentations générales des entreprises qui les proposent (partie 3).

PRODUIT/LOGICIEL

SERVICE

CONSEIL

Chiffres clés

Confiance numérique en France en 2016

9 Mds €

de chiffre d'affaires

60 000

emplois

50%
Cybersécurité

50%
Sécurité numérique

Un secteur en forte croissance

12,4%

Croissance du secteur par an en moyenne de 2014 à 2017

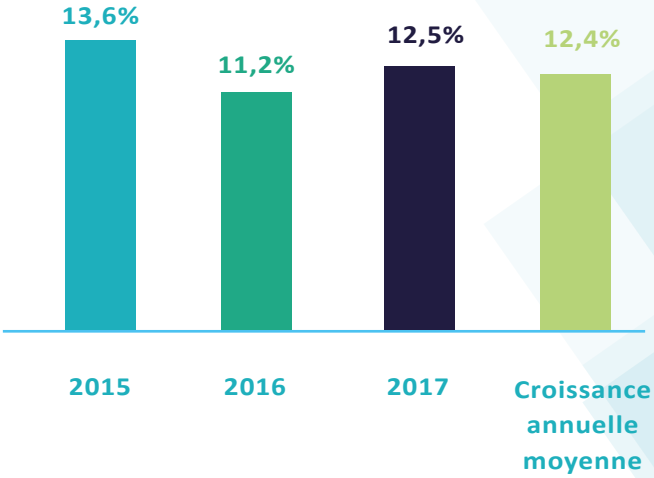
1,1%

Croissance du PIB par an en moyenne de 2014 à 2017

12,5%

de croissance prévue en 2017

Croissance moyenne pondérée du chiffre d'affaires des entreprises de la Confiance Numérique en France

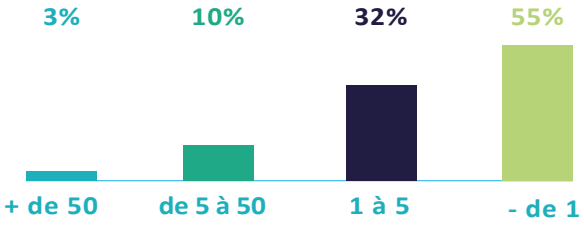


Un tissu vivant d'entreprises

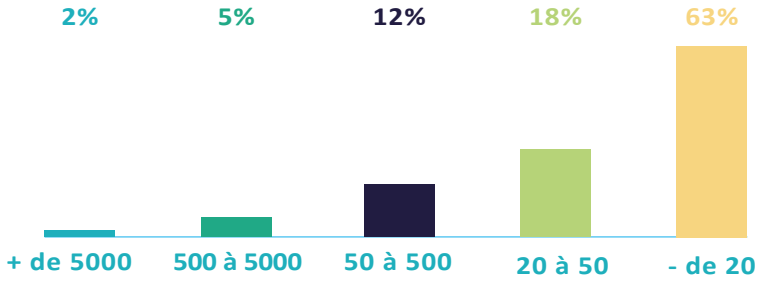
13% des entreprises du secteur ont un CA de **+5 Mds €**

81% des entreprises du secteur ont moins de **50 salariés**

Entreprises par chiffre d'affaires
en millions d'euros

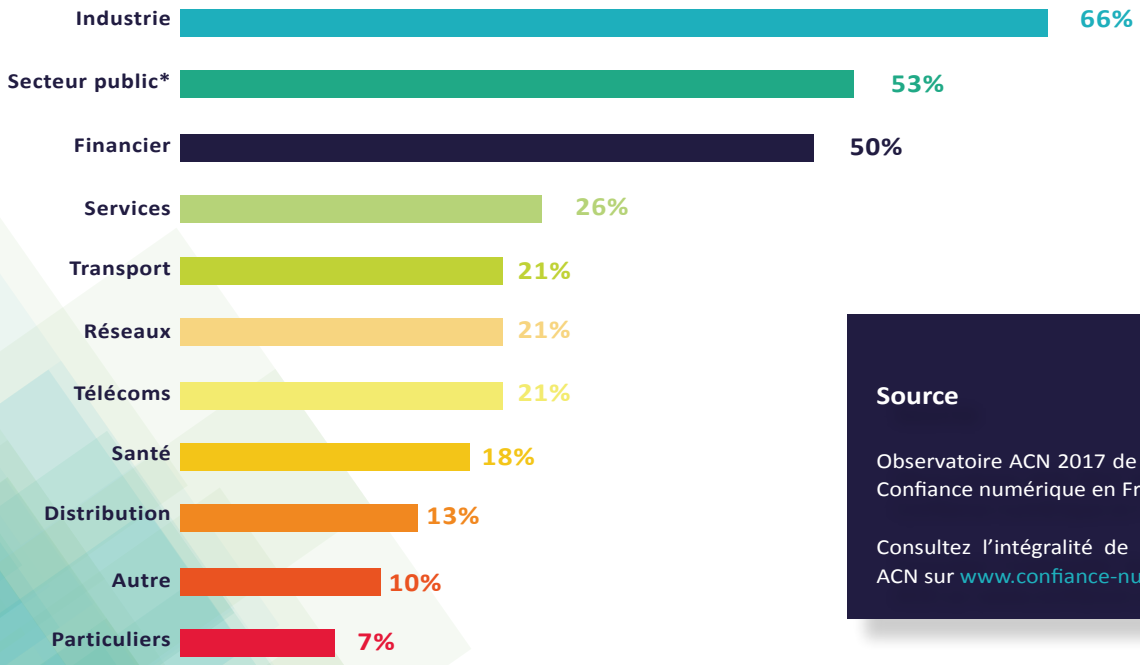


Entreprises par effectifs
nombre de personnes



Un positionnement marché dynamique

Présence des entreprises sur les secteurs clients
(% des entreprises)



Source

Observatoire ACN 2017 de la filière de la Confiance numérique en France

Consultez l'intégralité de l'Observatoire ACN sur www.confiance-numerique.fr

* administration, forces de sécurité, safe city, collectivités locales, hors santé et transports
Source : DECISION

produit/logiciel

intégration/service

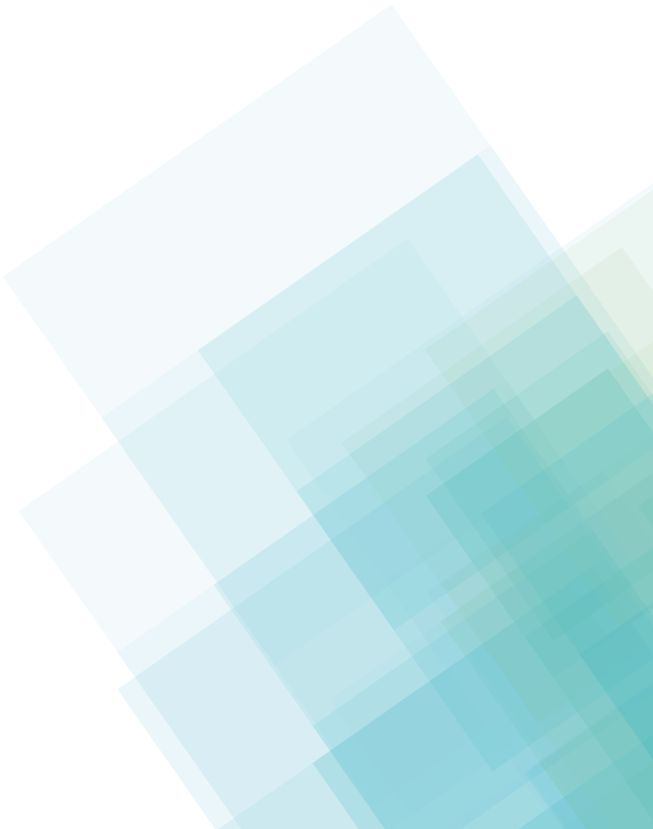
conseil

	GOUVERNANCE, TRAÇABILITÉ ET AUDIT	GESTION DES IDENTITÉS ET DES ACCÈS	SÉCURITÉ DES DONNÉES, CHIFFREMENT	SÉCURISATION DE LA MESSAGERIE	SÉCURISATION DES APPLICATIONS	PROTECTION DES FLUX MOBILES ET WEB	SÉCURITÉ DE L'INFRA ET DES ÉQUIPEMENTS	SÉCURITÉ DES RÉSEAUX INDUSTRIELS	AUDIT, CONSEIL ET FORMATION	INFOGÉRANCE ET EXPLOITATION	RENSEIGNEMENTS
6 CURE							p.33				
AIR-LYNX							p.33				
AIRBUS			p.23				p.33		p.39		
ALEPH NETWORKS									p.39		p.43
AMOSSYS									p.39		
ARTEM									p.40		
ATEMPO			p.23		p.30	p.32					
ATOS			p.24								
ATT		p.22									
BERTIN IT			p.25								p.43
BLUE-CYFORCE									p.40		
CEIS									p.40		p.44
CERTINOMIS	p.17					p.32					
CONSCIO									p.41		
CS								p.38			
DATASHUSH			p.23								
DENYALL			p.25		p.30						
ECRIN SYSTEMS						p.34					
EVIDIAN		p.18									
GEMALTO			p.25								
ICODIA				p.29		p.32					
IDNOMIC		p.19	p.26								

ILEX INTERNAT		p.19									
LINKURIOUS											p.44
MAXIM INTEGRATED			p.26								
OIKIALOG									p.41		
OVELIANE							p.34				
PRIM'X			p.26/27	p.29							
RISK&CO									p.41		
RUBYCAT	p.17										
SECLUDIT							p.34				
SEKOIA											p.44
SIEPEL							p.35				
SOPRA STERIA	p.17				p.31					p.42	
STMICRO							p.35				
STORMSHIELD			p.27				p.36	p.38			
SURYS		p.20	p.27								
SYSTANCIA		p.20/21									
TEHTRIS							p.36				
TEXPLAINED									p.42		
THALES							p.36/37				
THEGREEN-BOW			p.28								
TRACIP			p.28								
VOCAPIA											p.45
WALLIX		p.21/22									
WOOXO			p.28								

	CONSEILS EN CYBERSÉCURITÉ	FORMATION SENSIBILISATION	PRÉVENTION PROTECTION	DÉTECTION RÉACTION	INVESTIGATION RÉSILIENCE- RENSEIGNEMENT
6 CURE page 49					
AIR-LYNX page 50					
AIRBUS page 51					
ALEPH NETWORKS page 52					
AMOSSYS page 53					
ARTEM page 54					
ATEMPO page 55					
ATOS page 56					
ATT page 57					
BERTIN IT page 58					
BLUECYFORCE page 59					
CEIS page 60					
CERTINOMIS page 61					
CONSCIO page 62					
CS page 63					
DATASHUSH page 64					
DENYALL page 65					
ECRIN SYSTEMS page 66					
EVIDIAN page 67					
GEMALTO page 68					
ICODIA page 69					
IDNOMIC page 70					
ILEX INTERNAT page 71					

LINKURIOUS page 72					
MAXIM INTEGRATED page 73					
OIKIALOG page 74					
OVELIANE page 75					
PRIM'X page 76			 		
RISK&CO page 77					
RUBYCAT page 78					
SECLUDIT page 79					
SEKOIA page 80					
SIEPEL page 81					
SOPRA STERIA page 82					
STMICRO page 83					
STORMSHIELD page 84			  		
SURYS page 85					
SYSTANCIA page 86					
TEHTRIS page 87					
TEXPLAINED page 88					
THALES page 89					
THEGREENBOW page 90					
TRACIP page 91					
VOCAPIA page 92					
WALLIX page 93					
WOOXO page 94					



LES OFFRES CAPACITAIRES

SEGMENTATION FONCTIONNELLE

GOUVERNANCE, TRAÇABILITÉ ET AUDIT

CERTINOMIS

Certinomis
la confiance, ça se prouve

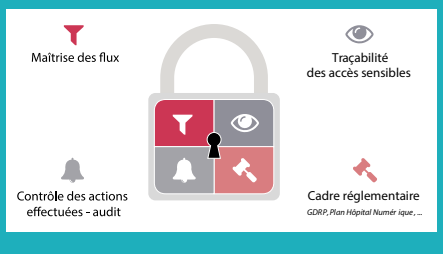
LA PKI OPÉRÉE

Certinomis Corporate est une Infrastructure de Gestion de Clés (IGC) en mode service.
Elle permet de déployer et gérer un parc de certificat électronique en s'appuyant sur des compétences et des ressources mutualisées, grâce à l'externalisation.

UN SERVICE SUR MESURE.
Cette solution est modulaire par conception : trois services distincts échangent de manière sécurisée pour réaliser les différentes étapes du cycle de vie des certificats. Ainsi, chaque client peut décider quelles fonctions sont assurées en interne, et quelles fonctions sont déléguées.
Certinomis Corporate offre un large éventail de possibilités depuis l'externalisation complète, avec des coûts uniquement variables en fonction des volumes, et l'internalisation complète, avec une possible intégration progressive de chacun des composants de la gamme.

RUBYCAT

RUBYCAT



PROVE IT

La solution logicielle française PROVE IT de RUBYCAT-Labs renforce la sécurité des **accès sensibles** à votre Système d'Information en y incluant **la traçabilité et le contrôle des utilisateurs à privilèges** (gestion des tiers, contrôle d'accès, …).

Vous savez qui s'est connecté à vos serveurs, quand, comment et vous pouvez de plus visualiser les actions effectuées en temps réel. Les sessions sont enregistrées pour une re-visualisation ultérieure.

PROVE IT contrôle, supervise, trace et enregistre le déroulement des connexions sensibles pour une visualisation immédiate ou différée (outil d'audit avancé).
La nouvelle version intègre de nouvelles fonctionnalités majeures dont un module natif de protection renforcée des identifiants des comptes d'accès sensibles.

SOPRA STERIA

sopra steria

GOUVERNANCE, AUDIT ET CONFORMITÉ

Maintien en condition de sécurité, Reprise & continuité d'activité

Avec plus de 700 experts en cyber-sécurité, Sopra Steria dispose d'une force humaine, technologique et industrielle de premier ordre.
Le Groupe fait bénéficier ses clients d'un savoir-faire de haut niveau et de capacités complètes en cyber-sécurité pour permettre la protection de leur patrimoine informationnel par la mise en œuvre de mesures techniques et l'adoption de dispositions organisationnelles adaptées au contexte.

Pour les audits de configuration, les audits organisationnels et physiques et les tests d'intrusion, Sopra Steria est un prestataire qualifié PASSI par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

GESTION DES IDENTITÉS ET DES ACCÈS

EVIDIAN

Bull Evidian

EVIDIAN WEB ACCESS MANAGER (WAM)

Web Access Manager (WAM) est un fournisseur d'identités, il fédère des accès aux apps web supportant les protocoles SAMLv2, OpenId Connect, WS-Fed. C'est aussi un Fournisseur de Services Web SSO pour les apps Web (internes, externes, Cloud).

Il sécurise l'accès des utilisateurs mobiles et remplace les mots de passe par un mode d'authentification unique et fort, utilisable à partir de PC, tablettes et autres non gérées par l'entreprise. L'authentification peut s'appuyer sur le fournisseur d'identité France Connect.

Evidian WAM supporte différentes méthodes allant du simple identifiants/mot de passe à l'authentification multi-facteurs et peut utiliser ses services d'authentification, celles d'un serveur d'un partenaire ou d'authentification SaaS. WAM gère l'accès des apps Web Office365.

EVIDIAN

Bull Evidian

EVIDIAN IDENTITY GOVERNANCE & ADMINISTRATION (IGA)

La solution Bull Evidian IGA, « Identity, Governance & Administration », permet d'identifier et gérer les utilisateurs autorisés à accéder au système d'information.

Elle définit et met à jour les droits des utilisateurs, et en gère l'évolution dans le temps selon une politique de sécurité basée sur les rôles, les organisations, les contextes et les règles métiers.

La solution s'appuie sur des processus de workflow métiers pour l'administration des droits, de provisionnement, pour mettre à jour les accès aux ressources dans l'entreprise ou dans le Cloud et pour la re-certification via des revues régulières de conformité.

EVIDIAN

Bull Evidian

EVIDIAN ENTREPRISE SINGLE-SIGN-ON (E-SSO)

Evidian Enterprise SSO gère l'accès aux applications d'entreprise et libère l'utilisateur de ses mots de passe et permet aussi de les changer automatiquement.

Le SSO peut être sécurisé avec une authentification forte, il propose le support du mode kiosque pour le partage sécurisé d'un poste de travail par plusieurs utilisateurs ainsi que l'authentification unique pour ouvrir ou verrouiller plusieurs postes par l'authentification d'un utilisateur. Ces mécanismes sont fréquemment utilisés pour des raisons de conformité réglementaire.

IDNOMIC

CORPORATE ID

Solution ouverte et modulaire qui crée, distribue et gère les identités numériques des utilisateurs et des terminaux au sein d'une PKI.
L'offre Corporate ID s'appuie sur les fonctions de :

- Credential Management System : Logiciel complet de gestion du cycle de vie des supports de certificats.
- Mobile Guard : Permet à l'entreprise d'étendre ses pratiques de sécurité aux mobiles et tablettes.
- Virtual Guard : Solution permettant de bénéficier des fonctions de gestion du cycle de vie des supports cryptographiques appliquées aux cartes à puces virtuelles en utilisant le module TPM (Trusted Platform Module).

IDNOMIC

CITIZEN ID

Solution de production et de gestion de titres d'identités électroniques pour la sphère citoyenne. En qualité de partenaire technologique, IDnomic propose ainsi aux gouvernements, ministères et intégrateurs systèmes en charge de programmes d'identité numérique à grande échelle d'assurer, à leurs usagers, un maximum de sécurité lors de leurs déplacements ou pour accéder à un e-service administratif sécurisé :

- Emission de titres d'identité électronique (passeport, titre de séjour, permis de conduire, etc.) non falsifiables.
- Accès aux données biométriques sensibles stockées dans les titres sécurisés et lecture contrôlée des informations.

ILEX INTERNATIONAL

ILEX IAM

L'offre logicielle d'Ilex International couvre la gestion du cycle de vie des identités et des habilitations, le provisioning des comptes et des droits sur le SI, la revue des habilitations, l'authentification forte et adaptative, le contrôle d'accès logique, le SSO et la fédération d'identités, et ce quels que soient les usages, les environnements utilisés, ou la nature des applications à protéger.

L'offre IAM d'Ilex s'articule autour de deux gammes de solutions :

- **Suite Ilex Identity** : solutions dédiées à la gestion des identités et des habilitations parfaitement adaptées aux besoins de toutes les organisations.
- **Suite Ilex Access** : offre complète et modulaire de gestion des accès vous permettant de gérer l'intégralité de vos problématiques en matière d'authentification renforcée, de WAM, de fédération d'identité, de eSSO et de Mobile SSO.).

SURYS

SURYS

PHOTOMETRIX™ VERS UNE IDENTITÉ DÉMATÉRIALISÉE

Photometrix™ est une solution de transition vers une identité totalement numérique ; une combinaison innovante alliant une image et un code barre 2D qui permet une authentification automatisée du portrait du porteur du document. Photometrix™ est réalisé grâce à un mécanisme de codage basé sur des caractéristiques particulières de la photo, certaines données relatives au porteur (nom, âge etc..) ainsi que des informations biométriques. Il agit ainsi comme une clé d'accès sécurisée qui ouvre les portes aux multiples opportunités du monde digital.

Le contrôle du Photometrix™ s'effectue par une App dédiée, pouvant indifféremment vérifier un code physique ou dématérialisé.

SYSTANCIA

Systancia

IPDIVA SECURE

IPdiva Secure est une solution française de cybersécurité qui permet de donner un accès sécurisé aux ressources choisies du SI pour tout type d'utilisateur (nomades / home-workers / tiers mainteneur, etc.). Avec un accès unique ne nécessitant pas l'ouverture de port du SI, IPdiva Secure offre des fonctionnalités avancées en matière de sécurité renforcée des terminaux mobiles, authentification forte, contrôle de conformité et intégrité et permet de vérifier en une seule vue que tout est en phase avec les bonnes pratiques et signale tout écart.

IPdiva Secure est la seule solution ayant obtenu la qualification Niveau-Elémentaire de l'ANSSI pour le domaine technique « Identification, authentification et contrôle d'accès ».

SYSTANCIA

Systancia

IPDIVA SAFE

IPdiva Safe, solution de surveillance des utilisateurs à pouvoirs (Privileged Access Management) permet l'enregistrement vidéo des sessions des utilisateurs et propose des fonctionnalités avancées en matière d'analyse temps réel permettant de détecter les comportements anormaux ou suspicieux ainsi que les cybermenaces dès la première tentative d'intrusion. Le moteur intelligent d'IPdiva Safe permet une analyse très fine des comportements et des événements sur les systèmes cibles et l'automatisation des actions conservatoires arrêtant l'utilisateur malveillant.

Solution packagée et très rapide à mettre en œuvre, IPdiva Safe s'appuie sur le moteur d'IPdiva Secure qui a obtenu la certification CSPN et la qualification élémentaire de l'ANSSI.

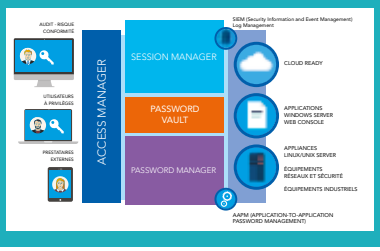
SYSTANCIA

AVENCIS SSOX

Avencis SSOX, labellisé France Cybersecurity, est une solution de contrôle des accès et authentification forte unifiée (SSO) garantissant la sécurité des connexions tout en simplifiant les accès des utilisateurs aux applications.

Elle permet de renforcer l'authentification primaire en proposant des fonctionnalités d'authentification multi-facteurs supportant de multiples moyens d'authentification (carte, biométrie, NFC…) ainsi qu'un module OTP. Avencis SSOX propose également des fonctionnalités avancées en matière d'authentification Out Of Band, coffre-fort de mot de passe, fédération d'identités et traçabilité de tous les accès garantissant d'être en conformité avec les réglementations et PSSI.

WALLIX



WALLIX BASTION

WALLIX Bastion est une plateforme logicielle de gestion des accès à privilèges (PAM) jouant un rôle significatif dans l'implémentation de mesures de prévention et de renforcement de la sécurité à travers :

• Bastion Session Manager : le contrôle des accès et le monitoring des sessions des utilisateurs à privilèges, la traçabilité des actions et la génération de rapport d'audit
• Bastion Password Manager : la sécurisation des mots de passe

En empêchant les connexions directes sur les infrastructures IT, WALLIX Bastion protège les actifs stratégiques des entreprises et répond aux enjeux de « privacy-by-design» de la transformation digitale, prévient des vols de données et assure une conformité rapide aux réglementations (RGPD, NIS, LPM,…).

WALLIX

BASTION SESSION MANAGER

Les comptes à privilèges sont des cibles pour les attaquants qui souhaitent atteindre les données et systèmes stratégiques des entreprises. Le Bastion Session Manager permet de monitorer les activités des comptes à privilèges :

• Etablissez votre défense : par la mise en place de règles de sécurité et conditions d'autorisations
• Organisez la supervision : avec une surveillance et analyse des sessions
• Coupez court aux tentatives malveillantes par la remontée d'alertes

Bastion Session Manager donne le niveau de visibilité indispensable des activités des comptes à privilèges (qui, quoi, quand). Un déploiement rapide et maitrisé, et à tout moment la possibilité d'évoluer vers la plateforme complète WALLIX Bastion.

WALLIX

BASTION PASSWORD MANAGER

Le Bastion Password Manager renforce la sécurité les mots de passe des comptes à privilèges. Que cela soit pour un utilisateur interne ou externe, il stocke et sécurise leurs identifiants et simplifie la gestion des niveaux d'accès aux informations :

- Stockez et sécurisez les mots de passe
- Gérez la rotation des mots de passe en fonction des configurations
- Supprimez les mots de passe des applications et scripts
- Renouvelez et redémarrez les comptes de services critiques

Bastion Password Manager vous permet de limiter les surfaces d'attaques en gérant les mots de passe partagés et les identifiants des utilisateurs à privilèges. Un déploiement rapide et maitrisé, et à tout moment la possibilité d'évoluer vers la plateforme complète WALLIX Bastion.

ATT

LE CODE SEALCRYPT®

SealCrypt est une gamme de codes 2D permettant le stockage d'importantes quantités de données vérifiables hors-ligne, et signées avec des clés asymétriques. SealCrypt garantit ainsi l'origine de son émission et l'intégrité de son contenu.

Sur tablette, smartphone ou document physique, SealCrypt peut contenir des informations sensibles, dont une photographie.

SealCrypt est aussi la première solution de stockage sécurisé biométrique vérifiable hors ligne sans utilisation d'une puce.

SÉCURITÉ DES DONNÉES, CHIFFREMENT

AIRBUS CYBERSECURITY

ORION MALWARE

Orion Malware est une plateforme de détection et d'analyse de codes malveillants capable de traiter des milliers de fichiers et de créer des règles de détection sur des nouvelles menaces.
Combinant des techniques de triage, d'analyse statique, d'analyse dynamique et de *machine learning,* Orion Malware est un outil collaboratif crucial dans la coordination des équipes SOC, de réponse sur incident et de *threat intelligence*, permettant de gagner du temps en investigation.

Orion Malware est proposé sous forme d'appliance avec une gamme complète ou en mode cloud via le portail *Check My File.*

Le produit embarque les dernières techniques d'analyse de codes malveillants et des jeux de règles de détection mis à jour régulièrement par les équipes de *Cyber Threat Intelligence* d'Airbus CyberSecurity.

ATEMPO

DIGITAL ARCHIVE

Solution de sauvegarde et d'archivage de gros volumes de données

Pour pallier la forte croissance des données et répondre aux exigences de rétention long-terme, les entreprises d'aujourd'hui ont besoin d'une solution de sauvegarde et d'archivage sécurisée et administrée de manière centralisée.

Atempo-Digital Archive est une plate-forme complète de sauvegarde et d'archivage de fichiers permettant aux utilisateurs de protéger, de transférer, manuellement ou automatiquement des données à contenu fixe vers des systèmes de stockage long-terme. Avec Atempo-Digital Archive, l'information est indexée et facile à trouver pour aussi longtemps que nécessaire.

DATASHUSH TECHNOLOGY

LOCKEMAIL

Un nouvel outil français pour protéger emails et données sensibles
Aujourd'hui la malveillance informatique et l'espionnage externe et interne ainsi que les nouvelles réglementations obligent les entreprises qui échangent par emails à se protéger de ces menaces. LockEmail.com offre une solution simple à utiliser, efficace et sécurisée sans changer de messagerie usuelle. Certes tous les emails ne sont pas à protéger cependant certains échanges doivent rester secrets. Nos produits sont disponibles pour LINUX, MAC, WINDOWS. Une version premium éditée conjointement avec «MDK solution» est disponible sur Clef USB chiffrée permettant une mobilité et une sécurité accentuée.
LockEmail.com est un service qui protège vos emails Confidentiels, Sensibles ou Privés par un moyen de chiffrement Bout En Bout avec des technologies Matures et ultra Sécurisés (GPG et clef de 4096 bits). Avec notre solution seul votre destinataire pourra lire le corps de l'email et ses pièces jointes.
Lockemail est disponible par abonnement.

ATOS

Bull Horus

HORUS IOT SECURITY

Bull Horus désigne la suite IoT Security d'Atos, une solution de tiers de confiance au service de l'IoE et de la sécurité de l'IoT. Avec Bull Horus, le business IoT est valorisé avec la mise en place de modèles de sécurité durables, adaptés à chaque secteur. Ses solutions et technologies de pointe couvrent toute l'infrastructure IoT, de la sécurité embarquée (solution matérielle d'ancre de confiance – CardOS) aux communications sécurisées et à la gestion des identités des objets (infrastructure de confiance et Module Matériel de Sécurité – HSM).

Bull Horus permet également d'établir une confiance décentralisée entre partenaires avec des consortiums Blockchain hautement sécurisés. Atos est membre de la LoRa Alliance et garantit l'intégrité des communications IoT avec le protocole LoRaWAN.

ATOS

Atos

SERVICES DE CYBERSÉCURITÉ

Avec ses 4500 experts en cybersécurité, Atos délivre des services de bout en bout allant du conseil à la fourniture de sécurité gérée à distance afin de définir puis d'appliquer une stratégie de prévention et de protection adéquate. Atos vous accompagne dans la mise en place de votre stratégie cybersécurité, la mesure et le suivi de vos cyber risques ainsi que la conformité aux règlementations en vigueur tel que RGPD/GDPR (Règlement General sur la Protection des Données), les directives NIS, PSD2 etc..

Atos a également développé la nouvelle génération de SOC (Security Operations Center) : Le Prescriptive SOC exploite le big data, machine learning et advanced threat intelligence pour anticiper et neutraliser les cyberattaques.

ATOS

Bull Trustway

TRUSTWAY PROTECTION DES DONNÉES

Protection des données : Bull Trustway est l'un des spécialistes européens du chiffrement de données, afin de garantir la protection des données et réseaux sensibles contre les cyberattaques.

Sa gamme de produits : Hardware Security Module (HSM), chiffrement réseaux IPsec et stockage sécurisé, possède de nombreux agréments et certifications en conformité avec les nouvelles réglementations, notamment le RGPD/GDPR, le Règlement Général sur la Protection des Données.

Sa solution Bull Trustway DataProtect fournit aux clients une solution de gestion de clés centralisé et de chiffrement pour tous les formats de données comme les machines virtuelles, les bases de données, les fichiers, les applications et la tokenisation, dans le cloud et on-premises.

BERTIN IT

CROSSING®

La passerelle d'interconnexion CrossinG® de Bertin IT est adaptée aux infrastructures sensibles. Elle sécurise et supervise les échanges d'informations entre des réseaux de domaines distincts ou de niveaux de confidentialité différents. Elle neutralise les attaques sur les systèmes sensibles ou distants par le contrôle des flux de données entrants et sortants. Enfin, elle lutte contre l'exfiltration d'informations d'un système d'information via le réseau.

DENYALL

CHIFFREUR RÉSEAUX

Protège les entreprises et les organisations contre l'espionnage et la manipulation des données qui sont transportées via Ethernet à travers les interconnexions fibre ou cuivre, les faisceaux hertziens et les liaisons par satellite.

- **Chiffrement des données** à la volée ou point à point.
- **Protège contre l'espionnage** et la manipulation des données.
- **Chiffreur Ethernet** pour les bandes passantes de 25 Mbit/s à 1 Gbit/s.
- **Approuvé par le BSI** (homologue allemand de l'ANSSI) et classifié « Diffusion restreinte » par **l'OTAN.**

GEMALTO

SAFENET KEYSECURE™

Gérez de façon centralisée vos clés de chiffrement et garantissez la possession de vos données avec SafeNet KeySecure, la plateforme de gestion des clés leader sur le marché.

Fonctionnant sous forme d'appliances matérielles validées FIPS 140-2 Niveau 3 ou 1, ou d'appliances virtuelles renforcées, SafeNet KeySecure propose une SafeNet Crypto Pack, une option de licence qui transforme votre appliance de gestion de clés en serveur incluant le support des connecteurs de chiffrement Gemalto tels que SafeNet ProtectApp, SafeNet ProtectFile, SafeNet ProtectDB, et SafeNet Tokenization.

Quel que soit leur emplacement, vos données sensibles sont protégées en cas d'acte malveillant.

IDNOMIC

OBJECT ID

Solution innovante de gestion des identités numériques pour protéger les objets connectés en leur attribuant une identité numérique sûre et en gardant l'information intègre et confidentielle. Pour cela, il est essentiel de mettre en place des systèmes d'authentification, de chiffrement et de signature des données (PKI) permettant d'assurer la gestion des identités numériques utilisées par les objets lors de leurs communications avec leur environnement. Les usages d'Object ID sont variés :

- Sécurisation de systèmes de transports intelligents
- Sécurisation d'appareils médicaux connectés
- Sécurisation de données de maintenance et de production
- Authentification de composants réseaux

MAXIM INTEGRATED

MICROCONTRÔLEURS SÉCURISÉS

Nous proposons une gamme complète basée sur le cœur Cortex M d'arm®. En combinant la protection de clef et la souplesse du cœur, cela permet d'associer les fonctions de stockage sécurisé et le support de nombreux algorithmes cryptographique (AES, RSA, ECDSA, SHA-x). Nous proposons également un microcontrôleur pré-programmé, le MAXQ1061. Son firmware développé par Maxim permet le stockage sécurisé de clefs et propose les fonctions les plus répandues pour la sécurité des systèmes embarqués comme la signature électronique ou le chiffrement.

Outre le domaine des terminaux de paiement, nos microcontrôleurs visent des applications comme les passerelles réseaux, les automates programmables, les décodeurs TV, etc. Ce sont donc les solutions complètes idéales pour sécuriser les réseaux, les applications, la gestion des identités, les accès, les flux, les infrastructures et les équipements industriels.

PRIM'X

ZONECENTRAL + ZONEPOINT + ORIZON

ZoneCentral, ZonePoint et Orizon sont basés sur des concepts de sécurité éprouvés : pas de passage des documents en clair sur les serveurs, aucune clé n'est stockée dans le système d'information, aucune clé ne transite sur le réseau, toutes les opérations de chiffrement sont réalisées sur le terminal (poste de travail, mobile…) avec la clé de l'utilisateur.

ZoneCentral permet le chiffrement de dossiers et fichiers : espaces de travail, serveurs de fichiers, partages, clés USB…

ZoneCentral coopère avec **ZonePoint,** chiffrement de documents dans les bibliothèques SharePoint® et avec **Orizon,** chiffrement des environnements utilisateurs et des espaces partagés dans le Cloud (OneDrive, Dropbox…), pour gérer le **DROIT D'EN CONNAÎTRE** sur l'ensemble des données « au repos » d'une organisation.

PRIM'X

CRYHOD

Chiffrement des disques des ordinateurs portables avec authentification pré-boot.

Pour une entreprise, le préjudice lié au vol ou à la perte d'un ordinateur portable va bien au-delà de la valeur du matériel. La perte des informations hébergées sur le disque dur de l'appareil ou leur simple communication à un tiers peuvent entraîner toutes sortes de graves désagréments : récupération d'informations sensibles par la concurrence, perte d'image, le tout pouvant être assorti d'infraction à la règlementation ou à la loi.

La solution de chiffrement de disque dur Cryhod de PRIM'X met votre entreprise à l'abri de ces risques.

STORMSHIELD

STORMSHIELD DATA SECURITY (SDS)

L'offre Stormshield Data Security (SDS) assure la confidentialité des données sensibles et prévient la fuite d'information sur tous types de supports : fichiers, courriels, disques virtuels, applications cloud comme Office365... Elle donne aux utilisateurs la possibilité de collaborer en toute sécurité, via du chiffrement, avec des interlocuteurs internes et externes.

L'option Cloud & Mobility permet de préserver la confidentialité des données stockées et partagées dans le cloud, notamment dans les plateformes de partage collaboratif comme Oodrive, Dropbox ou Office365, ... Les données confidentielles peuvent être téléchargées depuis un poste de travail sous Windows, Mac OSX ou depuis un terminal mobile (IOS ou Android).

SURYS

LE CODE PHOTOMETRIX™

Photometrix™ est une solution de transition vers une identité numérique, un mécanisme de codage basé sur des caractéristiques particulières du portrait. Le système extrait un certain nombre d'éléments de la photo qui sont ensuite compressés pour représenter seulement quelques octets d'informations, combinées avec certaines données relatives au porteur.

L'ensemble des données est ensuite signé en utilisant un algorithme de signature cryptographique asymétrique (Courbe elliptique DSA 512bits), afin de prouver que l'information a été émise par une source de confiance ; ce mécanisme garantit l'authenticité de l'information à un niveau de sécurité gouvernemental

THEGREENBOW

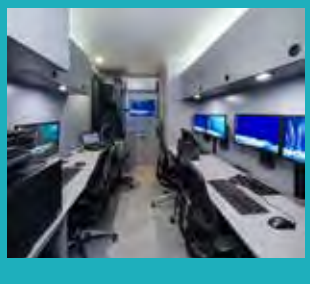
LOGICIEL CLIENT VPN THEGREENBOW *Connexion sécurisée de confiance*

Le Client VPN TheGreenBow est le premier logiciel de connexion sécurisée universel. Compatible avec toutes les gateways VPN, compatible avec toute PKI et déployable facilement sur toute infrastructure, le logiciel VPN TheGreenBow permet d'offrir rapidement et facilement à tous les collaborateurs de l'entreprise un accès sécurisé de confiance au Système d'Information.

Le Client VPN TheGreenBow est disponible pour toute plateforme : Windows, Android, macOS, iOS et Linux et permet d'établir des tunnels VPN sur tout type de réseau : 3G, 4G, Wi-Fi, Satellite, etc.

Le Client VPN TheGreenBow est l'unique solution de connexion sécurisée certifiée EAL3+ et qualifiée standard, habilitée à transmettre des flux diffusion restreint.

TRACIP



SPÉCIALISTE DU TRAITEMENT DE DONNÉES NUMÉRIQUES

Ordinateur, téléphone portable, clés USB… les supports d'investigation numérique sont multiples. Analyse d'images, de documents bureautiques, d'Emails ou de SMS, d'activité Internet mais également d'intrusion, de piratage, les types de données potentiellement sources de preuves sont multiples. TRACIP par son activité quotidienne auprès des services de police et gendarmerie, de l'armée, de la justice et des plus grandes entreprises a su développer des process pour répondre à chacun de ces cas de figure.

Partenaire privilégié des principaux éditeurs et fabricants de technologies d'investigation numérique à travers le monde, TRACIP vous accompagne dans vos besoins d'équipement et de formation aux outils et aux méthodes de l'investigation numérique.

WOOXO

PACKAGE BOX ALLROAD :

Les solutions Wooxo proposent un service complet de sauvegarde et de restauration du patrimoine numérique professionnel. En cas de sinistre majeur : cyberattaques, incendies, inondations, vols, vos données, vos applications et vos serveurs sont protégés et vous pouvez reprendre votre activité au plus vite en cas de besoin.

Notre offre clé-en-main 100% Made In France comprend le stockage local (Box ultra sécurisée et données cryptées) et cloud (datacenters français), le logiciel YooBackup, labellisé France Cybersecurity, l'installation et le paramétrage, le monitoring matériel et logiciel ainsi que le service après-vente.

SÉCURISATION DE LA MESSAGERIE

ICODIA

ICOCERBERUS.MEL

La solution hypercube DSS de sécurisation de la messagerie, capable de bloquer les menaces non-référencées.

Le pôle R&D d'Icodia a mis au point une plateforme de filtrage antivirus et antispam décisionnelle.
Elle utilise des technologies hypercube (OLAP), pour extraire et modéliser les menaces. Grâce à son intelligence artificielle, ses algorithmes décisionnels et au *machine-learning*, elle dispose de plusieurs niveaux d'intervention.

Elle apprend seule (*reverse-engineering,* stéganographie, *sandbox*), crée de nouvelles empreintes et signatures, identifie les comportements douteux. Votre organisation est protégée contre les cybermenaces.
Hébergé en Bretagne dans un datacenter sécurisé, elle fonctionne en SaaS.

IcoCerberus.Mel a reçu le label France Cybersecurity.

PRIM'X

ZED! ET ZEDMAIL

Chiffrement des emails et conteneurs chiffrés pour les échanges et les archives.

Zed! permet de créer des conteneurs chiffrés pour protéger les fichiers pendant leur transport indépendamment du canal utilisé (e-mail, support amovible, file-transfert, etc.). Un conteneur .zed est comparable à une « valise diplomatique » contenant des fichiers sensibles que seuls les destinataires identifiés ont le droit de lire.

ZedMail, intégré à Outlook®, permet de créer et de lire automatiquement des conteneurs .zed depuis la messagerie comme n'importe quel email. Les messages transitent chiffrés sur le réseau et au sein du serveur de messagerie de l'entreprise.

Une application gratuite et multiplateforme (Windows, Linux, macOS, iOS, Android) est disponible.

SÉCURISATION DES APPLICATIONS

ATEMPO

TIME NAVIGATOR

Solution de sauvegarde et de restauration pour les entreprises, en environnement virtuel et physique.
Time Navigator a une approche unique de la restauration avec son interface utilisateur basée sur la navigation temporelle qui permet de restaurer facilement vos données en 3 clicks.
La solution offre une évolutivité sans limite allant de la protection d'un simple groupe de travail jusqu'à des milliers de serveurs d'entreprise, avec plusieurs pétaoctets de données.
Avec Time Navigator, vous pouvez :

- protéger les plates-formes Windows, Mac OS X, Linux, les versions majeures d'Unix
- sauvegarder à chaud
- restaurer des grandes bases de données, systèmes de messagerie ainsi que les ERP
- supporter de nombreuses architectures de stockage (SAN, NAS, librairies de bande et VTL)

DENYALL

SCANNEURS DE VULNÉRABILITÉ

Détectez pro-activement les vulnérabilités de votre IT et réduisez votre surface d'attaque.

- **Vue complète des vulnérabilités** couvrant les couches réseau, système, applicative, base de données et flux Web.
- **Tableau de bord** pour rendre compte de la conformité de la politique de sécurité, de mesurer l'évolution dans le temps.
- **Reporting synthétique** pour le management, rapport détaillé pour les opérationnels, avec classification des vulnérabilités.
- **Choix du facteur de forme,** en interne avec une machine virtuelle, un scanner mobile pour contrôler les sites distants, ou en mode SaaS pour tester les défenses depuis l'extérieur.

DENYALL

WEB APPLICATION FIREWALL

Protégez votre site internet, applications et services web contre les vulnérabilités de l'OWASP top 10.

- **Sécurité éprouvée,** efficace contre les attaques connues et inconnues.
- **Modèles de sécurité négative et positive** combinés avec l'analyse du contexte utilisateur.
- **Interface graphique**, permettant aux administrateurs de gérer visuellement les politiques de sécurité et les flux de données.
- **Profilage et apprentissage** des applications Web.
- **Possibilité de rejouer les logs de trafic** pour affiner la politique ou analyser après coup.
- **APIs pour industrialiser le déploiement** sur appliances virtuelles ou matérielles.
- **Virtual patching** : patcher instantanément les vulnérabilités découvertes grâce au scanneur de vulnérabilités.

SOPRA STERIA

SECURITE DES DEVELOPPEMENTS ET DE L'EXPLOITATION

Disposant d'une expérience reconnue sur l'ensemble des domaines relevant de la sécurité Sopra Steria, est un partenaire de premier ordre des administrations et des grandes entreprises.

Le Groupe fait bénéficier ses clients d'un savoir-faire de haut niveau et de capacités complètes pour permettre la protection de leur patrimoine informationnel et faciliter en toute confiance leur transformation numérique.
Des garanties techniques de codage et des solutions de confiance alignées sur les processus métiers - classification des données, gestion des identités numériques (Identity and Access Management), Infrastructure à clés publiques (Public Key Infrastructure), protection contre les fuites de données (DLP), sécurité pour le Cloud et la mobilité - constituent un large éventail de dispositifs contribuant à la sécurité d'ensemble des applications.

PROTECTION DES FLUX MOBILES ET WEB

ATEMPO

Atempo
Data Protection Solutions

LIVE NAVIGATOR

Solution de sauvegarde en toute transparence et en temps réel les ordinateurs de bureau, les ordinateurs portables et les serveurs de fichiers.

- La **restauration en libre-service** permet à l'utilisateur d'accéder à l'historique des versions d'un fichier
- Grâce à une **déduplication efficace à la source et sur la cible**, Live Navigator n'envoie que les nouveaux blocs d'information vers le serveur de sauvegarde, économisant ainsi les ressources réseau et stockage
- A travers la **réplication hiérarchique multi-sites,** Live Navigator combine une restauration locale à haute vitesse avec une protection centralisée des données
- En cas de perte ou de panne de votre ordinateur, vos fichiers peuvent être restaurés à partir d'un navigateur web de n'importe quel endroit

CERTINOMIS

@ Certinomis
la confiance, ça se prouve

LES CERTIFICATS POUR SERVEUR

Les certificats serveur garantissent qu'une application informatique est mise en œuvre sous la responsabilité d'une organisation.

TROIS CATÉGORIES :

• Les certificats Serveur authentifient des services applicatifs jouant le rôle d'un serveur dans un échange, par exemple un site web.

• Les certificats Client authentifient des services applicatifs jouant le rôle d'un client dans un échange.

• Les certificats Cachet permettent à un service applicatif de sceller des données, pour en garantir l'origine et l'intégrité (par exemple pour émettre des factures, des bulletins de paye etc.).

UNE OFFRE MULTI-REFERENTIELS

Certinomis dispose de sa propre Autorité Racine référencée et qualifiée selon les différentes grilles d'exigence (RGS, ETSI, eIDAS, CA/B Forum) et peut ainsi répondre à l'ensemble des besoins de ses clients pour la sécurité de leurs échanges électroniques.

ICODIA

icodia.
Network Integrity

ICOCERBERUS.WEB

IcoCerberus.Web est une solution de filtrage applicatif (WAF) dotée d'un système d'analyse décisionnelle qui bloque les menaces en temps réel.

La sécurité des systèmes d'information est vitale. L'évolution des usages doit s'accompagner d'une protection maximale, afin de ne pas paralyser l'activité.

L'équipe R&D d'Icodia a développé une plateforme analytique qui filtre les requêtes HTTP et HTTPS afin de garantir l'accès aux visiteurs légitimes. L'analyse temps réelle permet d'appliquer dynamiquement des contre-mesures. Vos applicatifs sont protégés contre les cybermenaces.

L'interface d'administration responsive permet de visualiser les courbes de charge et de modifier l'ensemble de paramètres de sécurité.

IcoCerberus.Web a reçu le label France Cybersecurity.

SÉCURITÉ DE L'INFRASTRUCTURE ET DES ÉQUIPEMENTS

6CURE

6CURE THREAT PROTECTION®

Solution européenne de protection complète et efficace contre les attaques DDoS.

6cure Threat Protection® permet d'éliminer en temps réel les trafics malveillants à destination des services critiques avec une philosophie simple : préserver l'intégrité et la performance des flux légitimes. 6cure TP s'appuie sur une logique algorithmique éprouvée, permettant d'identifier et de filtrer les attaques DDoS les plus complexes, jusqu'au niveau applicatif, et ainsi d'assurer l'écoulement normal des requêtes autorisées vers les services protégés.
Les fonctions de sécurité avancées embarquées par 6cure TP apportent une protection des actifs critiques tels que des serveurs physiques ou virtuels, des applications informatiques installées sur ces serveurs, ou des composants réseau tels que des routeurs, des liaisons de données, ou des services d'infrastructure ou d'hébergement (ex. : DNS), contre les menaces DDoS.
La solution 6cure Threat Protection a reçu le label France Cybersecurity.

AIR-LYNX

RESEAU PRIVE 4G LTE AUTONOME

Créé en 2013, la société française AIR-LYNX est constructeur d'une solution innovante de réseau d'infrastructure 4G LTE Privé. Ce réseau tout-en-un, compact, souple en fréquences, sécurisé, haut débit, et rapide à déployer, peut être décliné en version nomade ou mobile. La solution intègre au travers d'une application maison, tous les services adaptés aux besoins des professionnels, comme le Push to Talk ou la vidéo. Elle peut être déployée dans de nombreux scénarios : bulle tactique de sécurité civile, protection de sites sensibles, sécurisation de lieux publics, transport routier ou ferroviaires, accès à internet rural, usine 4.0 ou Smart Cities. Air-Lynx a été maintes fois récompensée et a notamment reçu le prix de l'innovation MILIPOL 2017 dans la catégorie Smart and Safe Cities.

Pour en savoir plus : www.air-lynx.com

AIRBUS CYBERSECURITY

CYBER DEFENCE CENTRE (CDC)

Les 3 centres de cyber défense (CDC) d'Airbus CyberSecurity situés en France, Allemagne et Royaume-Uni sont des structures uniques rassemblant plus de 20 ans d'expertise en cybersécurité.

L'offre repose sur trois piliers : **Prévention - Détection - Réaction**

Actifs en 24/7, les CDC regroupent toute l'expertise Cyber d'Airbus CyberSecurity de l'opérateur à l'expert en réponse à incident et les services d'architecte, de *Threat Intelligence,* de veille, etc. afin d'assurer en temps réel la sécurité de votre environnement digital et superviser vos actifs.

Les CDC sont capables d'affronter toutes les cyber-menaces, des plus courantes (ransomwares) aux plus sophistiquées (APT), en vous alertant dès les premiers signaux de compromission.

ECRIN SYSTEMS

CALCULATEURS DURCIS POUR LA DÉFENSE ET L'INDUSTRIE

o Expert en électronique embarquée pour tous les marchés de l'industrie et de la défense
En 40 ans d'existence, ECRIN a construit son développement autour de trois activités pour devenir l'un des acteurs majeurs de l'électronique embarquée:
• l'ingénierie et les services ODM - Original Design Manufacturer- de calculateurs industriels et militaires sur spécifications ;
• la conception et la fabrication de systèmes COTS « Ready to your Application » qualifiés MIL-STD-810/461 et DO-160 facilement modifiables pour les besoins spécifiques du client
• l'intégration de calculateurs industriels pour la Cyber sécurité, le BigData, l'IIoT et les Communications
o Cette triple compétence fait d'ECRIN un partenaire unique dans le domaine de l'embarqué, qui se caractérise par sa forte capacité d'innovation et sa solide expertise.

OVELIANE

OSE : SOLUTION DE CONTRÔLE CONTINU DE LA CONFORMITÉ ET DE L'INTÉGRITÉ

La solution souveraine OSE contrôle le niveau de sécurité d'un parc de serveurs (physiques ou virtuels, locaux ou clouds) et des applications.
OSE mesure les écarts et les évolutions en continu par rapport à une politique de sécurité standard ou propre.
Un ensemble de points de contrôle est fourni, qu'il est possible d'adapter, de modifier ou de compléter.
Les informations générées sont remontées sous forme d'alertes (mail ou syslog) et de rapport de synthèse permettant de planifier les actions de remédiation.
Un module spécifique permet de vérifier que les bonnes pratiques préconisées par l'ANSSI sont respectées et donne les indications pour s'y conformer. OSE peut être couplé avec un SIEM et intégrables à un SOC.
OSE permet aussi de couvrir les demandes de contrôles d'intégrité et de capacité de résilience exigées dans l'article 32 de la RGPD.

SECLUDIT

ELASTIC WORKLOAD PROTECTOR

La seule solution française d'analyse de sécurité pour le Cloud intégrant un scanner de vulnérabilités.

Elle permet de surveiller en continu aussi bien les infrastructures IaaS, hybrides que multi-cloud. Sa technologie brevetée découvre automatiquement tous les actifs des SI et peut cloner les serveurs pour éviter d'affecter la production. Le risque de shadow IT est donc fortement diminué.
L'ajout du scanner de vulnérabilités et de sa base de 60 000 tests renforcent la surveillance des systèmes d'exploitation, réseaux, serveurs en plus des Cloud Workloads.
Les 200 tests automatiques de sécurité d'EWP sont basés sur les bonnes pratiques de sécurité IaaS, du CSA et du CIS. EWP permet de classer le niveau de risque par criticité grâce à des indicateurs de risque ANSSI, OWASP, PCI et RGPD.

SIEPEL

CYBERSÉCURITÉ DES INFRASTRUCTURES

La cybersécurité des infrastructures est notre cœur de métier. Notre expérience et notre savoir-faire nous permettent de nous positionner sur ce marché en tant que prestataire de qualité, avec une offre haut de gamme :

Produits

- Cages de Faraday hautes performances
- Salles de réunion sécurisées
- Faradisation architecturale à performances optimisées
- Pochettes faradisées
- Boitiers sécurisés
- Baies faradisées hautes performances.

SIEPEL

CYBERSÉCURITÉ DES INFRASTRUCTURES

Services

- Assistance à maîtrise d'ouvrage
- Plans de test pour mesures de réception
- Recettes techniques en usine & sur site
- Mesures d'affaiblissement électromagnétique selon EN50147-1(accréditation ISO/CEI 17025 :2005 du COFRAC), IEEE 499, MIL STD 285, ...,
- Mesures d'infrastructure Zonage-Tempest selon SDIP 27 et Directive 495
- Mesures de sécurisation de locaux et détection de menaces internes
- Maintien en Condition Opérationnelle (MCO) toutes marques
- Transfert, mise à jour, modification d'installations
- Formation à l'entretien préventif.

STMICROELECTRONICS

MICROCONTRÔLEURS SÉCURISÉS

STMicroelectronics, un leader mondial dans le domaine des technologies de sécurité, offre à ses clients une gamme de microcontrôleurs sécurisés et de solutions de sécurité « clé en main » qui garantissent votre tranquillité d'esprit dans un monde digital interconnecté : votre identité est vérifiée et vos données personnelles sont protégées et accessibles.

Au-delà des usages établis dans les cartes SIM, cartes de paiement ou passeports biométriques, ST permet le développement de transactions sécurisées sur des plateformes mobiles et contribue à protéger les appareils connectés à l'Internet des Objets.

Les microcontrôleurs sécurisés ST sont certifiés selon les standards les plus exigeants tels que EMVCo, Critères Communs ou FIPS et offrent un ensemble complet d'interfaces de communication contact et sans contact (ISO/IEC 7816, ISO/IEC 14443 Type A & B, NFC, USB, SPI, I^2C).

ST accompagne également certains clients, non experts en sécurité, lors de l'intégration de la sécurité dans leur business model et dans leur processus de production.

STORMSHIELD

STORMSHIELD NETWORK SECURITY / STORMSHIELD ENDPOINT SECURITY

Stormshield propose une offre complète et de bout-en-bout pour la protection des infrastructures et des équipements.
La gamme Stormshield Network Security (SNS) est conçue pour protéger les infrastructures les plus sensibles contre tous types de menaces, d'une manière transparente pour les utilisateurs et les administrateurs. Ces produits UTM et Next Generation Firewall combinent toutes les fonctions de sécurité réseau au sein d'un seul matériel ou appliance virtuelle.
En complément, la solution Stormshield Endpoint Security (SES) assure une protection de nouvelle génération des terminaux (serveurs, postes de travail…), grâce à sa technologie comportementale unique. Cette couche de défense, sans signatures, bloque les actions malveillantes les plus sophistiquées et celles capables de contourner les systèmes de protection traditionnels, comme les ransomwares les plus évolués.

TEHTRIS

E-GAMBIT

La solution logicielle française éditée par TEHTRIS, nommée eGambit assure une surveillance nominale face aux cyber menaces diverses et avancées de grandes infrastructures mondiales. eGambit est capable de surveiller et d'améliorer la sécurité des systèmes d'information face aux intrusions furtives et complexes. Tel un système d'alarme numérique, eGambit apporte son assistance à des entreprises en Chine, au Brésil, aux USA, au Moyen-Orient et en Europe contre des menaces internes et externes.

Son Intelligence Artificielle et tous les capteurs déployés à l'échelle d'une grande infrastructure, sont capables de repérer des virus, des outils d'espionnage, des bombes logiques inconnues, des événements à risque et des comportements anormaux.

THALES

CYBELS SENSOR

CYBELS Sensor, qui bénéficie des dernières innovations en matière d'intelligence artificielle, est une sonde de confiance pour la détection des cyberattaques et la protection des infrastructures critiques et des réseaux sensibles. La solution répond notamment aux exigences de la Loi de Programmation Militaire (LPM) avec laquelle les Opérateurs d'Importance Vitale (OIV) devront se mettre en conformité. Déployé sur les points critiques du réseau, CYBELS Sensor analyse les flux de données et les fichiers afin d'y détecter les attaques et les comportements anormaux.

Cybels Sensor peut être intégré au sein d'un SOC client ou géré par un service externalisé de supervision de sécurité.

THALES

ELIPS

La réglementation relative au traitement des informations de niveaux de sensibilité différentes exige un cloisonnement physique des réseaux (protection du secret médical, du secret industriel ou de défense).

La Diode ELIPS permet de créer une liaison monodirectionnelle évitant toute fuite d'informations confidentielles. Il est alors possible de relier un réseau critique industriel, classifié, ou stratégique à un réseau non protégé pour recevoir des données utiles sans qu'il soit possible d'émettre des informations dans l'autre sens.

ELIPS est agréé jusqu'au niveau secret défense pour le marché France et il est certifié NATO SECRET par le NATO Information Assurance Product Catalogue.

THALES

MISTRAL

MISTRAL est une solution de sécurité des réseaux IP (VPN) de niveau gouvernemental. Il permet la protection des applications confidentielles jusqu'au niveau Diffusion Restreinte sans dégradation de la qualité de service.

MISTRAL permet de lutter contre les menaces inhérentes à l'interconnexion des réseaux locaux via des infrastructures publiques comme internet ou les réseaux d'opérateurs grâce à un ensemble de services de sécurité de haut niveau (Authentification, Confidentialité, Intégrité).

La solution MISTRAL est certifiée au niveau Critères Communs EAL3+ et elle est agréée aux niveaux Diffusion Restreinte France, UE et OTAN.

SÉCURITÉ DES RÉSEAUX INDUSTRIELS

C-S

PRELUDE

Prelude est un SIEM, une solution de supervision de sécurité.

En centralisant la collecte et le traitement des informations issues de sources disparates, PRELUDE fournit une vision unifiée de l'état de sécurité pour une meilleure réactivité et protection en cas de cyberattaques. Basée sur des standards ouverts (IDMEF et IODEF), PRELUDE constitue une solution particulièrement performante et évolutive pour une sécurité intelligente notamment au cœur des opérations d'un SOC (Security Operation Center).

PRELUDE est la seule alternative européenne 100% SIEM (Security Information and Event Management) américaines pour répondre aux enjeux des Organismes d'Importance Vitale (OIV).

STORMSHIELD

STORMSHIELD NETWORK SECURITY / STORMSHIELD ENDPOINT SECURITY

Stormshield propose une offre complète et de bout-en-bout pour la protection des réseaux industriels. La solution SNi40 de la gamme Stormshield Network Security (SNS), disponible dans un format physique durci, permet de déployer une protection optimale au plus près des automates. Elle est l'unique produit du marché à être qualifié CSPN Pare-feu industriel (Certification de Sécurité de Premier Niveau) par l'ANSSI, permettant ainsi de répondre aux exigences de la réglementation française (LPM) pour la protection des Systèmes d'Information d'Importance Vitale (SIIV).

En complément, la solution SES (Stormshield Endpoint Security) assure une protection des terminaux industriels et postes opérateurs sous Windows. Cette couche de défense, sans signatures, bloque les actions malveillantes les plus sophistiquées et celles capables de contourner les systèmes de protection traditionnels.

AUDIT, CONSEIL, FORMATION

AIRBUS CYBERSECURITY

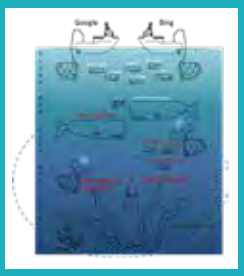
CYBERRANGE

CyberRange est une plateforme de cyber entrainement et de simulation permettant aux organisations de prendre en main la formation de leurs experts en Cyber sécurité.

Le service reproduit des environnements informatiques ou industriels réalistes au sein desquels peuvent être joués des scenarios incluant de véritables cyber attaques.

La CyberRange propose également de tester et éprouver des solutions techniques du marché dans le cadre de tests d'utilisation intensifs, et cela en toute sécurité dans un environnement isolé.

ALEPH NETWORKS



GAMME DE SERVICES

Le moteur GM Search Dark est complété par une gamme de Services : Émission de flux de données ciblées, reportings personnalisés, études cyber, formations… aleph-networks surveille et analyse en permanence et de façon industrialisée grâce à son moteur de recherche direct et discret, les zones les plus profondes du web, où se cache le cœur de la Cyber Criminalité.

AMOSSYS

EXPERTISE & INNOVATION EN CYBERSÉCURITÉ

Cabinet de conseil et d'expertise en cybersécurité reconnu, AMOSSYS accompagne ses clients dans la sécurisation de leur espace numérique à travers une offre globale de services à haute valeur ajoutée : audit, conseil, CERT, évaluation, R&D, logiciels innovants.

Gage de la fiabilité de ses interventions, AMOSSYS bénéficie de la reconnaissance des plus hautes instances étatiques : Centre d'Evaluation de la Sécurité des Technologies de l'Information (CESTI) agréé par l'ANSSI (agrément systèmes industriels), Prestataire d'Audit de la Sécurité des Systèmes d'Information qualifié pour les besoins de sécurité nationale (PASSI–LPM) et certificateur agréé par l'Agence de Régulation des Jeux En Ligne (ARJEL).

ARTEM

SENSIBILISATION, SIMULATION ET FORMATION À LA GESTION DES RISQUES ET DES CRISES

Notre équipe conçoit et anime des simulations de crise pour former dirigeants et managers aux principes et méthodologies de gestion de crise : organisation de cellules de crise, communication de crise, analyse des enjeux et attentes de parties prenantes critiques, prise de décision, etc.

Nous accompagnons nos clients pour actualiser et améliorer leurs procédures, sensibiliser leurs équipes et préparer/tester la résilience, la continuité ou la reprise de leurs activités.
Notre cabinet s'appuie sur un réseau d'experts et facilite le cas échéant la participation d'acteurs institutionnels.

BLUECYFORCE

FORMATION ET ENTRAÎNEMENT EN CYBERSÉCURITÉ « PAR LA PRATIQUE »

Formations et entraînements individuels sur tous les pans de la cybersécurité (pentest/hacking, detection/réaction, investigation numérique, sécurité des systèmes industriels), entraînements collectifs (principes de gestion de crise, logiques et processus d'équipe) et exercices complets de gestion de crise en équipe.

Tous nos entraînements se basent sur l'utilisation d'un environnement reproduisant des systèmes réels, avec des moyens de cybersécurité réels (nous avons plus de 25 partenaires technologiques, français et internationaux), et du trafic de vie basé sur des flux réels. Notre Red Team explore sans cesse de nouvelles attaques, de nouvelles failles, de nouvelles techniques, afin d'intégrer ces contenus aux entraînements. Chez bluecyforce, on s'entraîne à lutter contre les attaques d'aujourd'hui et de demain.

CEIS

CONSEIL & ETUDE STRATÉGIQUE

Parce que la réflexion doit précéder et nourrir la décision, nous accompagnons nos clients dans la compréhension de leur environnement et la définition de leur stratégie de transformation et de développement.

Nos consultants combinent une forte expertise sur les secteurs stratégiques (défense, sécurité, énergie, transport, numérique) et la maitrise d'une boite à outils méthodologique complète (animation de séminaires, élaboration de scénarios…). Particulièrement impliquée sur les questions de transformation numérique, CEIS est titulaire auprès du Ministère des armées du contrat-cadre de réalisation des études prospectives et stratégiques (EPS) en matière de sécurité du cyberespace et de cybersécurité. Nous abordons ainsi l'ensemble des enjeux liés à la sécurité et à la transformation numérique. Nos prestations : Etudes prospectives, Diagnostic stratégique, Analyse de marché, Accompagnement stratégique

CONSCIO TECHNOLOGIES

RAPIDAWARENESS

Conscio Technologies propose une offre couvrant l'ensemble des aspects de la sensibilisation en ligne sur la cybersécurité et le RGPD.
En matière de cybersécurité le contenu est très riche et comporte à ce jour près de 50 parcours.
Pour la mise en œuvre des campagnes deux solutions logicielles existent.
Sensiwave : Vous pilotez votre campagne dans les moindres détails et pouvez personnaliser le contenu pour l'adapter à votre environnement et votre message.

RapidAwareness : Cette solution offre l'avantage de la simplicité car avec RapidAwareness il est possible de mettre une campagne en œuvre en quelques minutes. Notre vidéo de présentation permet de comprendre la simplicité de RapidAwareness en 2 minutes : https://youtu.be/xWpv_yAtAYU

OÏKIALOG

AUDIT RISQUES ET MENACES

L'objectif général est d'étudier les besoins d'analyse et d'exploitation des logs pour la création d'indicateurs pertinents en fonction des risques et menaces à couvrir.
Plus précisément, cela permet de disposer :
- d'un état des lieux de l'existant en termes de sources de logs
- d'un état des besoins en termes de logs
- d'une liste des sources de logs permettant de générer les indicateurs
- d'une grille de choix de produit et d'une aide à la sélection d'un outil adapté

D'un point de vue opérationnel, l'étude présente :
- une grille de besoins
- une réflexion sur les menaces et les sources d'informations pour les couvrir
- une grille de choix de solutions

RISK&CO SOLUTIONS

SOLUTIONS

1. Identifier risques et vulnérabilités
- Analyse de risques pour l'identification des risques et des objectifs de sécurité d'un périmètre donné.
- Audits de sécurité, tests d'intrusion sur des périmètres organisationnels et techniques afin d'en identifier les vulnérabilités principales.

2. Réduire les risques
- Assistance à maîtrise d'ouvrage et maîtrise d'œuvre pour la conception d'architectures sécurisées, notamment sur les systèmes industriels et systèmes de sûreté/sécurité (contrôle d'accès, vidéosurveillance).
- Intégration et développement à façon de solutions à haute sécurité.

3. Accompagner les projets complexes
- Assistance à la planification de la sécurité dans les projets complexes.
- Homologation de systèmes sensibles, en accord avec les exigences réglementaires.

TEXPLAINED

LOGICIEL DE RECONSTITUTION DE PUCES ÉLECTRONIQUES

Forte de son expertise en sécurité des puces électroniques face au piratage et à la contrefaçon, Texplained a développé un logiciel permettant de reconstituer l'architecture de la puce étudiée sous différents formats : GDSII, Netlist, description VHDL.

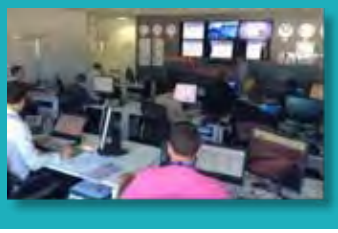
Ses atouts :

- Versatile : Utilisable pour tout type de puce (Smart Card, Microcontrôleur, Microprocesseur, FPGA,…)
- Facile d'utilisation : Guidage pas à pas
- Intelligent : Réutilisabilité des résultats des projets
- Optimisé : Installable sur ordinateur standard
- Performant : Traitement des données ultra rapide

Ses usages : Analyses de sécurité de puce / Recherche de portes dérobées Intelligence technologique / Étude pour remplacement de composants obsolètes ...

INFOGÉRANCE ET EXPLOITATION

SOPRA STERIA



MANAGEMENT DE LA SECURITE

Avec plus de 700 experts en cyber-sécurité et des centres de management de la sécurité en Europe et hors d'Europe opérant 24/7, Sopra Steria dispose d'une force humaine, technologique et industrielle de premier ordre.

Les services managés de sécurité offerts couvrent les prestations de type SOC (Security Operations Center) intégrant outils de SIEM (surveillance), détection des APT (Advanced Persistent Threats), forensic, jusqu'à la gestion de crise. Le centre de cyber-sécurité basé en France opère au profit d'organismes d'importance vitale (OIV) et de filières industrielles sensibles.

Sopra Steria est en cours d'agrément pour l'octroi de la qualification PDIS (Prestataire de détection d'incidents de sécurité) de l'Agence nationale de sécurité (ANSSI).

RENSEIGNEMENT

ALEPH NETWORKS

GM SEARCH DARK.

Aleph-networks a développé un moteur de recherche spécialisé et totalement indépendant de toute API pour explorer les Deep et Dark webs : GM Search Dark.

Le périmètre de surveillance et les fonctionnalités d'analyse sont uniques.
Sur le Dark Web, plus de 150 000 sites Tor et plus de 10 000 sites I2P sont surveillés ; Sur le Deep Web, plus de 1 200 sites 'Black Hat' sont surveillés ; Soit plus de 60 millions des pages indexées, avec un périmètre en constante évolution (+100% par an).
Le moteur indexe des sites, forums, places de marchés, ...
GM Search Dark est un outil unique, qui permet de mener des recherches et des analyses pointues dans les recoins les plus profonds et cachés du web.

BERTIN IT

MEDIACENTRIC®/ MEDIASPEECH®

Bertin IT sécurise les connexions et supervise les échanges d'informations entre réseaux sensibles et/ou distants via sa passerelle de confiance sécurisée CrossinG®. Sa solution MediaCentric® couvre pour sa part, l'anticipation des cyber menaces, la veille en vulnérabilités de système d'Information, la vigilance multicanal en situation de crise ainsi que la lutte antiterroriste et anticriminelle grâce à des capacités d'acquisition 24/7 multi-sources (web, tv, radio) et d'analyse en profondeur des contenus multimédias et multilingues. Expert en Technologies Vocales, Bertin IT conforte également son positionnement distinctif par sa solution logicielle MediaSpeech® dédiée à la valorisation des contenus parole multilingues dans les sources audio et vidéo et les interactions téléphoniques.

BERTIN IT

SERVICES DE CYBER THREAT INTELLIGENCE

Les services de cyber threat intelligence de Bertin IT garantissent l'anticipation et la veille sur les actifs de ses clients. Les experts Bertin IT sondent le web et ses profondeurs pour détecter tout type de menaces: indices de préparation de cyber-attaques, risques d'atteintes physiques, fuites de données sur Internet (intentionnelles ou non), contrefaçons et réseau de distribution.

CEIS

SECUINSIGHT

Connaître la menace, préparer ses défenses

Avec SecuInsight, CEIS propose à ses clients des services personnalisés de Cyber Threat Intelligence stratégique et opérationnelle. Préparer efficacement sa cybersécurité, c'est comprendre les chemins d'attaque potentiels, évaluer les risques IT externes (fuites de données, fraudes, réputation, vulnérabilités…) pour anticiper les menaces susceptibles de toucher son organisation.

Les données remontées sont rendues actionnables par l'analyse humaine réalisée par notre équipe de consultants et analystes aux compétences et profils complémentaires (analystes, linguistes, experts géopolitiques et business, juristes, hackers éthiques). Elles peuvent alimenter une plateforme MISP et être présentées dans un dashboard dédié, permettant à nos client un monitoring permanent du risque IT. Ceux-ci peuvent ainsi optimiser leur stratégie de cybersécurité, leurs choix de solutions et l'efficacité des équipes opérationnelles.

LINKURIOUS

LINKURIOUS ENTERPRISE

Linkurious conçoit et fournit une solution logicielle d'analyse de données permettant de détecter et d'investiguer des menaces telles que les fraudes informatiques, les cyberattaques, ou les failles de sécurité.

Grâce à une interface de visualisation simple de prise en main, Linkurious Enterprise vous permet d'investiguer vos données sous forme de graphes d'entités connectées entre elles. L'analyse de ces graphes offre une vision exhaustive des relations entre les entités composant réseaux informatiques et infrastructure d'information. Il est ainsi possible d'identifier les vulnérabilités des systèmes informatiques ou de visualiser les données relatives à une attaque pour en évaluer la nature afin de réagir en conséquence.

SEKOIA

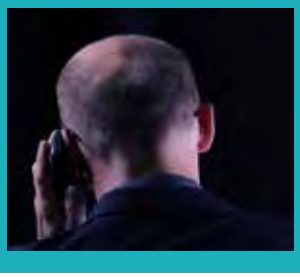
SOLUTION INTHREAT

SEKOIA, via sa solution inThreat, propose une offre de threat intelligence clé en main permettant de bénéficier de rapports de synthèse, de flux de données multiples, d'une plateforme d'échange dédiée et de services professionnels associés.

inThreat, c'est une application de Threat Intelligence tout en un et accessible via différents bundles pour permettre d'intégrer la threat intelligence qui correspond au mieux à l'entreprise selon son degré de maturité.

- Des rapports de synthèse sur les menaces permettent au client de comprendre très rapidement à quoi il est exposé et de prendre les bonnes décisions selon son secteur d'activité.
- Différents flux de données sont accessibles via inThreat pour les entreprises qui ont besoin de consommer des indicateurs de compromissions. Ces différents flux constituent l'une des plus grosses de threat intelligence sur Internet
- Une solution de partage privative basée sur MISP permet à chaque client d'avoir sa plateforme dédiée de threat intelligence sans avoir à se soucier de l'administration.

VOCAPIA RESEARCH



VOXSIGMA

Vocapia est une entreprise spécialisée dans le traitement automatique de la parole. Notre suite logicielle Voxsigma, dédiée à des utilisateurs professionnels traitant de grandes quantités de données audio, inclut les fonctionnalités suivantes :

- Transcription en temps réel de la parole
- Identification de la langue
- Segmentation parole/non-parole
- Détection de mots clés
- Segmentation en locuteurs
- Synchronisation audio-texte

INDEX DES SOCIÉTÉS

PRÉSENTATIONS

CONTACT

Justine BERNAGOU
justine.bernagou@6cure.com
0971162156

701, rue Léon Foucault - Z.I de la Sphère 14200 Hérouville Saint Clair

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

6CURE

6cure
secure your business

FRANCE CYBER SECURITY

6CURE – GARANTIR LA DISPONIBILITÉ DE VOS DONNÉES

6cure, éditeur français crée à la fin des années 2000, s'est spécialisé dans la lutte contre les attaques par déni de service distribué. Nous avons construit des offres efficaces de lutte intelligente contre les attaques, qui permettent à nos clients d'accroître leur réactivité et leur imperméabilité face aux atteintes malveillantes ciblant la disponibilité de leurs services critiques.

De nouvelles stratégies d'attaques voient le jour régulièrement et impliquent un développement permanent de nouvelles fonctionnalités, de nouvelles stratégies de détection et de neutralisation pour y répondre.

Nos domaines de compétences: détection et mitigation d'attaques informatiques multi-formes, lutte anti-DDoS, détection de botnet, analyse des sources d'attaque, traitement des incidents de sécurité informatique.

La famille de solutions développées par 6cure permet de protéger les systèmes d'information des attaques DDoS les plus complexes et intervient dans les domaines d'application suivants :

- Protection des infrastructures télécom et hébergement
- Sécurisation des infrastructures DNS
- Fourniture de services sécurisés contre les DDoS à tout type de client
- Protection spécifique pour le domaine e-commerce, banques, assurances, santé
- Solution souverainen particulièrement adaptée aux OIV
- Protection accessible et adaptée, des PME jusqu'aux grands groupes
- Test de résistance aux attaques DDoS

Nous mettons l'accent sur le développement de solutions de protection simples à déployer et à utiliser, offrant une grande visibilité aux utilisateurs, interopérables, collaboratives pour faire face à une cyber malveillance devenue multiforme.

Interopérabilité avec des solutions SIEM du marché

Pilotage et optimisation de solutions de sécurité (Firewall, IPS/IDS, etc.).

Complémentarité possible avec des solutions anti-DDoS déjà pré-positionnées.

CONTACT

Thierry BUFFENOIR
info@air-lynx.com
+33 (9) 81 43 46 46

1 avenue de l'Atlantique
91940 LES ULIS
www.air-lynx.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

AIR-LYNX

AIR-LYNX est un constructeur français de réseaux d'infrastructures 4G LTE privés et sécurisés. Ses solutions font partie des plus compactes et des plus rapides à déployer du marché. Autonomes, ces équipements permettent en effet la mise en oeuvre très simple d'un réseau 4G LTE n'importe où, en moins de 90 secondes. La gamme se décline en versions fixes ou nomades, avec notamment une bulle tactique (un réseau complet dans une valise de 30 kg), et un ManPack (réseau complet dans un sac à dos).

Les solutions AIR-LYNX présentent d'autres atouts, comme le fait d'être souples en fréquences, entièrement sécurisées et résilientes. Elles bénéficient de mécanismes de sécurité avancés, proposés en standard dans la norme LTE, et de mécanismes de chiffrement de type AES 128 bits.

Les réseaux privés AIR-LYNX permettent de répondre à des besoins de connectivité dans de nombreux cas d'usage : sécurité civile ou défense, protection de sites sensibles, sécurisation de lieux publics, transport routier ou ferroviaire, transport maritime, accès à internet rural, mines, plateformes pétrolières, usine 4.0, smart et safe cities…

AIR-LYNX développe également des services MCPTT adaptés aux besoins des professionnels, utilisateurs de la PMR, qui permettent par le haut débit induit par le LTE d'apporter la dimension de la transmission vidéo et en particulier le multicast (eMBMS) fonctionnant sur n'importe quel Smarphone Android. Pour en savoir plus : www.air-lynx.com

CONTACT

Laurence THOMAS
laurence.thomas@airbus.com
+33 (01) 61 38 62 00

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

AIRBUS

AIRBUS

Reposant sur l'expérience du groupe Airbus en matière de défense et de sécurité, et forte d'une équipe regroupant plus de 700 experts entièrement dédiés à la cyber sécurité, Airbus CyberSecurity met son expertise et ses solutions européennes de confiance au service de l'ensemble de ses clients.

Forte de son expertise humaine issue des cas majeurs de réponse à incident, l'offre d'Airbus CyberSecurity comprend une large gamme de produits (Keelback Net, Orion Malware, Cymerius, CyberRange, Stormshield, Ectocryp, SEG, etc.) et services (SOC, audits, consulting, Threat Intelligence, etc.) en cybersécurité, couvrant l'ensemble de la chaine de cyberdéfense et la protection de vos actifs.
En Europe comme au Moyen-Orient, organismes de défense et de sécurité, gouvernements, opérateurs d'infrastructures critiques ou industries sensibles ont accordé leur confiance aux produits et services développés par Airbus CyberSecurity.

S'appuyant plus particulièrement sur ses trois Cyber Defence Centres (CDC) établis en France, en Allemagne et au Royaume-Uni, Airbus CyberSecurity dispose de structures uniques associant de façon dynamique la veille, la détection précoce des attaques et leur investigation, réduisant ainsi drastiquement le temps de réponse et de traitement des incidents.

La mise en œuvre depuis plusieurs années d'une stratégie passant par un soutien à l'innovation, le recrutement d'experts et le développement de partenariats stratégiques (dans le domaine du transport aérien avec Sita par exemple) permet à Airbus CyberSecurity de fournir à ses clients les technologies et services appropriés à leur métier.

Avec 20% du chiffre d'affaires annuel investi dans l'innovation et la R&D, Airbus CyberSecurity reste à la pointe des dernières avancées technologiques en terme de connaissances de la menace, de moyens de détection et d'analyse et des techniques innovantes de *machine learning*.

CONTACT

Nicolas HERNANDEZ
nicolas.hernandez@aleph-networks.com
+336 15 68 51 32

333 montée de Buisante,
69480 Pommiers

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

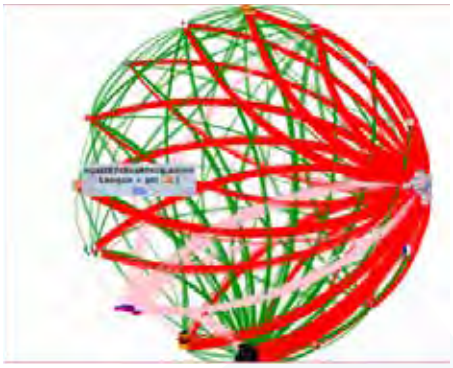
ALEPH-NETWORKS

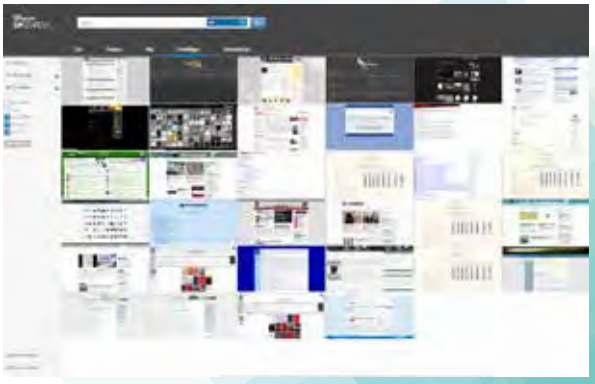
La société aleph-networks est éditrice de logiciels. Née d'un projet de R&D en 2010, elle commercialise depuis 2012 deux technologies innovantes en collecte, traitement, visualisation et anonymisation de données : GrayMatter et SafetyGate.

SafetyGate est une technologie de réseaux distribués (p2p) permettant de répondre aux risques induits par la transmission d'informations sensibles.
GrayMatter est une technologie d'indexation et structuration de données en très grands volumes, qui permet de traiter tout type de données, quels que soient leur format et leur provenance (Dark Web, Deep Web, OSINT, …), et de les structurer selon des critères de consultation métier :

- données publiques des réseaux sociaux professionnels,
- données de sites marchands,
- flux presse en très grands volumes pour de l'analyse orientée renseignement et veille,
- etc…

aleph-networks a développé une solide clientèle privée et publique, **ainsi qu'un réseau de forts partenariats avec les plus gros acteurs français de la cybersécurité et de la veille et s'impose aujourd'hui comme le référent français des Dark et Deep Webs.**





CONTACT

Vattana VONG
contact@amossys.fr
+33 (02) 99 23 15 79

4bis Allée du Bâtiment,
35000 RENNES

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

AMOSSYS

Cabinet de conseil et d'expertise en cybersécurité reconnu, AMOSSYS accompagne ses clients dans la sécurisation de leur espace numérique à travers une offre globale de services à haute valeur ajoutée :

Audit : Faites établir un diagnostic précis de la sécurité de vos SI par un prestataire reconnu (qualification PASSI, ARJEL) : audit organisationnel et physique, audit d'architecture, audit de configuration, audit du code source, tests d'intrusion internes/externes.

Conseil : Bénéficiez de notre expertise et de nos retours d'expérience pour optimiser la sécurisation de vos infrastructures/systèmes : pilotage et accompagnement, gestion des risques opérationnels SSI, analyse de risque, homologation de sécurité, formation/sensibilisation des utilisateurs aux bonnes pratiques.

CERT : Bénéficiez d'une intervention rapide en cas d'incident ou de suspicion d'incident lié à la sécurité : réponse à incident, recherche de compromission, recherche d'indicateurs de compromission, analyse et rétro-conception de codes malveillants, accompagnement à remédiation de SI compromis et durcissement du niveau de sécurité.

Evaluation : Faites estimer la sécurité de vos produits et systèmes par un laboratoire agréé (ANSSI) et accrédité (COFRAC) : rédaction ou assistance à la rédaction de cibles de sécurité et d'éléments de preuves, évaluation selon le schéma Critères Communs ou CSPN.

R&D : Enrichissez votre posture cyber des dernières avancées en matière de cybersécurité : études cyber, preuves de concept, conférences, supervision de thèses.

Logiciels innovants sur-mesure : Externalisez intégralement ou partiellement la conception ou la réalisation de vos solutions de cybersécurité : développement intégral de produits cyber, fournitures de briques OEM.

Gage de la fiabilité de ses interventions, AMOSSYS bénéficie de la reconnaissance des plus hautes instances étatiques : Centre d'Evaluation de la Sécurité des Technologies de l'Information (CESTI) agréé par l'ANSSI (agrément systèmes industriels), Prestataire d'Audit de la Sécurité des Systèmes d'Information qualifié pour les besoins de sécurité nationale (PASSI–LPM) et certificateur agréé par l'Agence de Régulation des Jeux En Ligne (ARJEL).

CONTACT

Patrick CANSELL
contact@artem-is.fr
+33 (0) 6 75 65 59 86

215 rue JJ Rousseau
92130 ISSY LES MOULINEAUX
www.artem-is.fr

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

ARTEM

ARTEM DEFENSE

Les activités ARTEM sont dirigées par Patrick Cansell, docteur en Sciences de l'Information et de la Communication, chercheur associé au sein de DICEN-IdF et responsable de l'Enseignement Spécialisé « Intelligence Economique » de l'Ecole des Mines de Paris, co-responsable du Master ISART de l'UPEM. Outre ses activités d'enseignement, il dirige ARTEM INFORMATION & STRATEGIES, ARTEM DEFENSE et ARTEM FORMATION, qui couvrent un spectre large de prestations complémentaires pour des publics professionnels, chercheurs comme étudiants.

Des études sectorielles sur la thématique « cyber »
ARTEM DEFENSE, qui intervient sur le segment Défense et Sécurité, est spécialisé dans l'analyse (études de marché ou sectorielles, monographies). ARTEM DEFENSE réalise des études sectorielles trimestrielles sur des thématiques Défense et Sécurité au profit des entreprises membres du GICAT, notamment sur la thématique cybersécurité / cyberdéfense. ARTEM DEFENSE est également partenaire de grands comptes de la Défense et de la Sécurité dans le cadre d'études technico-opérationnelles (ETO) sur les enjeux et technologies du combat futur au profit de la DGA et des forces armées.

Des séminaires de sensibilisation et de gestion de crise
ARTEM INFORMATION & STRATEGIES propose des formations (sensibilisation, séminaires thématiques - sujets sectoriels ou méthodologies) sur les thèmes de l'intelligence stratégique, de l'analyse des risques et de la gestion de crise. La thématique « cyber » est couverte à travers la réalisation de modules de formation pour des publics étudiants comme professionnels (interventions au profit de grands comptes des domaines Aéronautique ou Cybersécurité, sur des thématiques telles que les risques cyber, l'environnement concurrentiel du secteur, les enjeux de la cybersécurité).

ARTEM INFORMATION & STRATEGIES est également immatriculé en tant qu'organisme de formation.

Plus de 500 exercices de crise, dont une centaine au profit de COMEX de grands comptes, ont été réalisés par nos équipes depuis 2005, tant en France qu'à l'étranger (Italie, Algérie, Belgique, Sénégal, Emirats, Luxembourg, Suisse, Malaisie, Turquie, UK, Qatar, Brésil, etc.) dans le cadre d'actions de prévention du risque, de conseil, de formation / entraînement à la Gestion de Crise / Continuité. Nos clients travaillent dans les secteurs Banque, Assurance, Sécurité, Energie, Grande Distribution, Biotech, BTP ou encore Agro-alimentaire.

CONTACT

Hervé COLLARD
herve.collard@atempo.com
01 64 86 83 00

2, avenue de Laponie
91951 Courtaboeuf Cedex
www.atempo.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

ATEMPO

Atempo

Data Protection Solutions

Atempo est un éditeur de logiciels français spécialisé dans la sauvegarde, l'archivage et la protection des données.
L'offre Atempo consiste en une suite logicielle incluant sa solution de protection des données d'entreprise emblématique, Atempo-Time Navigator (ATN), sa solution de protection des données des postes de travail, Atempo-Live Navigator (ALN), sa solution puissante et évolutive de protection pour des données non structurées, Atempo-Digital Archive (ADA).

Avec leur couverture fonctionnelle et le support d'un vaste éventail de technologies de stockage et d'applications, les solutions d'Atempo répondent aux besoins des organisations, qu'elles soient distribuées ou centralisées jusqu'aux centres de calcul qui manipulent des volumes de données allant de quelques centaines de téraoctets à plusieurs pétaoctets.

Les solutions proposées par Atempo bénéficient d'une solide réputation. Elles sont utilisées par les grands comptes publics (tels que le Ministère de l'Economie et des Finances, le Ministère de la Défense, la SNCF, Ifremer, l'Etablissement Français du Sang…) et de grands groupes privés (Comme la Banque Populaire, la Caisse d'Epargne, Kiloutou, Kiabi, LexisNexis, etc.).
Les solutions Atempo sont distribuées via un réseau de revendeurs et d'intégrateurs informatiques auprès d'une clientèle d'entreprises de taille intermédiaire ou de grands comptes.

Le siège d'Atempo est situé à Paris. L'entreprise est présente en Europe, aux États-Unis et en Asie via un réseau de plus d'une centaine de revendeurs, d'intégrateurs et de fournisseurs de services managés.

Pourquoi choisir Atempo ?
Les solutions d'Atempo sont pensées pour répondre aux besoins spécifiques des entreprises quelle que soit leur taille. Le fonctionnement des solutions simples d'utilisation et didactiques permet de bénéficier :

- D'une capacité à gérer de très gros volumes de données (pétaoctets)
- D'une facilité et rapidité de restauration
- D'une hétérogénéité des environnements supportés
- D'un « Vendor-agnostic » car Atempo reste indépendant vis-à-vis des constructeurs
- D'une qualité du support, basé en Europe
- D'un Licensing Program qui est adapté aux secteurs de marché : collectivités, hôpitaux, éducation, recherche….
- D'une résistance contre la cybercriminalité

CONTACT

Bruno VERNIER
bruno.vernier@atos.net
+33 (01) 73 26 08 49

River Ouest, 80 quai Voltaire
95877 BEZONS

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

ATOS

Pour faire face aux cyberattaques et aux ransomware, Atos propose une approche unique et cohérente liant sécurité et business centrée sur la protection des données et la prévention. Vous bénéficierez d'une expertise fondée sur des années d'expérience s'appuyant sur des produits (Bull Evidian, Bull Trustway, Bull Horus) et des services de sécurité répondant aux exigences de vos organisations.

Partenaire de confiance, Atos, conçoit, développe, exploite et maintient des solutions numériques de pointe alliant puissance de calcul, sécurité et intégration de systèmes. Avec sa forte expertise technologique et plus de 4500 spécialistes cybersécurité dans le monde, Atos accompagne la « transformation numérique » de ses clients en respectant les nouvelles réglementations (LPM - Loi de Programmation Militaire, RGPD – Règlement General sur la Protection des Données, NIS, PCI DSS, HIPAA…).

Le groupe fournit un haut niveau d'expertise et de professionnalisme dans ses services de gouvernance, risques et conformité. Il accompagne ses clients dans le développement et la mise en place des plans stratégiques de politiques de sécurité, alliant un équilibre de l'efficacité opérationnelle de la protection des données et des systèmes d'information et la conformité aux réglementations en vigueur (RGPD/ GDPR).

Le spectre des services d'Atos dans ce domaine comprend, entre autre la protection des données privées et la conformité, l'audit de sécurité, les tests de pénétration, architecture et implémentation des systèmes de détection et remédiation des attaques les plus élaborées. Atos est le partenaire informatique mondial des Jeux Olympiques et Paralympiques et fait partie de l'indice CAC 40.

CONTACT

Jean-Pierre MASSICOT
Jp.massicot@att-fr.com
01 47 16 64 72

99 avenue de la Chataigneraie
92500 Rueil Malmaison

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

ATT

Depuis plus de 10 ans, Advanced Track & Trace développe et fournit aux gouvernements et aux entreprises internationales des technologies avancées pour assurer la sécurité des sociétés et des individus : solutions d'authentification et d'identification, protection de l'intégrité des données et encodage d'informations.
A travers sa plateforme Vary.IDs, ATT génère des milliards d'identifiants uniques pour assurer la sérialisation, la traçabilité et la connectivité des produits et des documents.
Exploitables à plusieurs niveaux (citoyen, représentant de l'autorité, professionnel, expert…), ces solutions sont rapides à mettre en place et offrent un excellent rapport compétitivité-efflcacité.

PROTECTION DE L'IDENTITE & DES DOCUMENTS
Les solutions développées par ATT permettent de sécuriser la signature et toutes les informations-clés d'un document : données textuelles, biométrie, photographie…

Membre fondateur de l'Association Internationale de Gouvernance du Cachet Electronique Visible, et fournisseur des administrations, des institutions et des imprimeries, ATT apporte des solutions clés-en-main pour tous types de documents, aussi bien physiques et numériques : cartes de paiement et d'identité, vignettes, visas, passeports, badges, documents administratifs, ticketing…
ATT a reçu le label France Cybersecurity.

SECURITE DES ECHANGES ET LUTTE CONTRE LES MARCHES ILLICITES
A travers des solutions de smart packaging et de protection des produits, ATT apporte aux industriels et aux institutions douanières des outils fiables et innovants pour assurer l'authentification et la traçabilité sécurisée des produits.

ATT est active dans toutes les zones géographiques et tous les secteurs d'activité sensibles : alcool, tabac, vins, agroalimentaire, pharmaceutique, cosmétique, électronique, pièces détachées, luxe…

PROTECTION DES BILLETS DE BANQUE
Partenaire certifié de la Banque de France, ATT développe des codes de sécurité permettant de prévenir la reproduction frauduleuse des billets de banque.

CONTACT

Aude BRAUNSTEFFER
aude.braunsteffer@bertin.fr
0674688555

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

BERTIN IT

Editeur et intégrateur de solutions logicielles, BERTIN IT propose une gamme de solutions et de services pour la cyber sécurité, la cyber intelligence, la veille stratégique et le traitement automatique de la parole.

Acteur référent du marché, Bertin IT accompagne les marchés privés (banque, assurance, industrie, opérateurs de télécommunications, média, énergie, environnement…) et publics (administrations centrales et défense).

Répondant aux enjeux stratégiques de protection, d'anticipation et d'analyse de leurs marchés, les solutions de Bertin IT délivrent les bénéfices suivants :

- Valorisation des contenus de paroles, multilingues, dans des sources audio et vidéo et transcription d'interactions téléphoniques : solution MediaSpeech®
- Protection de l'intégrité des systèmes d'information et des patrimoines informationnels : solution MediaCentric®
- Confidentialité et innocuité des échanges entre réseaux ou systèmes d'information sensibles : solution Crossing®
- Détection des prémices de cyberattaques et de fuites d'informations fragilisant les systèmes d'information : services Bertin IT à la carte
- Veille stratégique, économique, concurrentielle et e-reputation : solution AMI Entreprise Intelligence

Bertin IT est engagé dans de nombreux programmes de Recherche, notamment dans les domaines de :

- La virtualisation, la cryptologie, la maîtrise des flux de données et l'interopérabilité sécurisée
- Le traitement de l'information et des contenus, l'investigation et la valorisation des données multimédias (Web, TV, Radio) multilingues de sources ouvertes

Grâce à 120 personnes en France et à l'étranger, Bertin IT assure à ses clients un accompagnement spécifique et personnalisé incluant l'étude de leurs besoins, la définition de solutions ad hoc, la stratégie de déploiement et le support tout au long du cycle de vie.

Filiale spécialisée dans les technologies de pointe de l'information, Bertin IT appartient au groupe CNIM. Fondé en 1856, CNIM est un équipementier et ensemblier industriel français de dimension internationale, coté à Euronext Paris. CNIM emploie 2 500 collaborateurs pour un chiffre d'affaires 2016 de 539,9 millions d'euros, dont 55% réalisés à l'export.

CONTACT

Vincent RIOU
vincent.riou@bluecyforce.com
01 45 55 39 98

Tour Montparnasse
33 avenue du Maine 75015 Paris
www.bluecyforce.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

BLUCYFORCE

bluecyforce

Né d'un partenariat entre deux PME françaises, CEIS, société de conseil en stratégie et management des risques cyber, et DIATEAM, société d'ingénierie informatique spécialisée en cybersécurité, le centre bluecyforce répond à un besoin qui n'était pas couvert jusqu'alors : l'entraînement des équipes opérationnelles de cybersécurité dans un environnement similaire à leur environnement professionnel.

En rupture avec la formation traditionnelle, bluecyforce propose ainsi dans ses Cyber Training Centers une offre unique en Europe de formation et d'entrainement opérationnel à la cyberdéfense, ouvert à tous les professionnels, selon des parcours pédagogiques basés sur la pratique.

Tous nos entraînements se basent sur l'utilisation d'un environnement reproduisant des systèmes et réseaux réalistes, y compris des systèmes industriels. Nous intégrons également les solutions de cybersécurité de nos partenaires technologiques (leaders du marché et technologies innovantes). Les instructeurs bluecyforce sont accompagnés d'une « Red Team ». Hackers éthiques professionnels, ils accompagnent les participants dans leur progression en agissant comme de véritables « Sparring-Partners ».

Le centre bluecyforce est basé à Paris, Tour Montparnasse. Nous pouvons également projeter nos moyens chez nos clients, et prévoyons d'ouvrir de nouveaux centres agréés bluecyforce dans le monde courant 2018.

CONTACT

Vincent RIOU
vriou@ceis.eu
01 45 55 39 98

Tour Montparnasse
33 avenue du Maine - 751015 Paris

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

CEIS

Depuis 1997, CEIS accompagne ses clients dans la réussite de leurs projets grâce à une démarche d'intelligence économique, d'analyse stratégique et de maîtrise des risques. Cette démarche nous permet d'apporter une aide à la décision stratégique et opérationnelle qui s'enracine dans une connaissance intime de l'environnement de nos clients.

CEIS intervient principalement sur des thématiques liées aux industries stratégiques (défense, sécurité, aéronautique, finance, énergie, transport, matériaux stratégiques, sport, pharmacie, luxe…), aux marchés émergents, à la cybersécurité et à la transformation numérique. Fort de 80 consultants basés à Paris, d'un réseau de bureaux internationaux (Bruxelles, Doha, Abou Dhabi, Astana) et de partenaires dans plus d'une dizaine de pays, CEIS est intervenu dans près de 120 pays en 2015.

Les missions de CEIS s'articulent autour de 5 axes complémentaires :

- Etudes stratégiques
- Sécurité Economique
- Sécurité Numérique & Cybersécurité
- Communication d'influence & Evènements

CEIS anime également des labs d'innovation et d'expérimentation destinés à l'accélération business des start-up et PME du secteur IT et cybersécurité. Elle anime ainsi le DGA Lab pour le compte de la Direction Générale de l'Armement et de SOPRA-STERIA et a lancé Bluecycforce, 1er centre d'entraînement opérationnel à la cybersécurité en France, début 2017. En tant que co-organisateur du Forum International de la Cybersécurité (FIC) en partenariat avec la Direction Générale de la Gendarmerie Nationale, CEIS est au cœur des enjeux et problématiques de la cybersécurité aussi bien d'un point de vue opérationnel, technologique, industriel ou stratégique. La conjonction de ces différentes expertises nous confère un positionnement unique en France pour délivrer des prestations de conseils de très haut niveau.

CONTACT

François CHASSERY
francois.chassery@certinomis.fr
0 809 109 809

10 Avenue Charles de Gaulle -
94673 Charenton-le-Pont Cedex

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

CERTINOMIS

Certinomis
la confiance, ça se prouve

FRANCE CYBER SECURITY

La dématérialisation est une rupture, un changement de paradigme, elle permet de commercer ou de s'engager sans l'intermédiaire du papier signé. Mais ce changement est doublement source d'inquiétude : nous savons que le piratage est possible, et nous n'accordons pas spontanément confiance à des documents électroniques.

- **Notre rôle : créer les conditions de la confiance**

Pour répondre à ces craintes, Certinomis propose un ensemble de services pour :
- garantir l'identité des intervenants d'un échange électronique,
- donner une date certaine à une transaction, et
- générer des documents opposables juridiquement.

Ces services permettent de se protéger des usurpations d'identité, et de se prémunir contre les contestations. De ces sécurités nait la confiance.

- **Nos moyens : des infrastructures technico-juridiques reconnues**

Nos prestations nécessitent des installations techniques robustes et hautement disponibles pour produire des livrables de nos services de confiance selon les conditions définies dans la réglementation et dans les normes.

La conformité de ces infrastructures et de leur fonctionnement est attestée par des audits réguliers qui se traduisent par référencements (Adobe, Microsoft, Apple, Google, Mozilla), certifications (normes ETSI ou CEN) et qualifications (RGS et eIDAS) : ils sont autant de preuves qui justifient la confiance.

- **Notre Offre : des services à la demande**

À partir de ces infrastructures de confiance reconnues, nous proposons à nos clients des services de confiance qui leur sont adaptés : nous pouvons réaliser nos prestations sur des bases unitaires, ou par tranche de volume ; nos offres peuvent être clés en main ou intégrer des activités du client, toujours avec le même objectif de qualité.

Notre métier d'Opérateur de Confiance Numérique consiste ainsi à vous faire bénéficier à la demande de solutions complètes et hautement qualifiés pour assurer votre sécurité technique et juridique dans le monde virtuel.

CONTACT

Michel GÉRARD
michel.gerard@conscio-technologies.com
06 07 04 92 57

12 rue Vivienne,
75002 Paris

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

CONSCIO TECHNOLOGIES

Conscio Technologies est le spécialiste de la sensibilisation des utilisateurs.

Conscio Technologies, c'est :

- 10 ans d'expérience comme expert de la sensibilisation à la sécurité informatique.
- Plus de 800 000 utilisateurs satisfaits
- Plus de 150 références d'organisations de toutes tailles et de divers secteurs.

Conscio Technologies est également membre d'Hexatrust.

Conscio Technologies offre à ses clients une approche complète de la sensibilisation des utilisateurs comprenant des contenus vidéos et quiz très complets, des solutions logicielles pour la mise en œuvre de vos campagnes, des campagnes de phishing factice, une évaluation de la maturité.

L'offre de Conscio Technologies comporte une riche variété de contenus (46 parcours en SSI et 13 sur le RGPD).

Deux logiciels permettent de mettre en oeuvre les campagnes : RapidAwareness, la solution la plus simple pour lancer une campagne, à la portée de tous, quelques minutes suffisent pour lancer sa campagne et Sensiwave, la solution la plus complète permettant de préparer une campagne à façon paramétrable dans les moindres détails.

Les domaines traités concernent la cybersécurité, le RGPD, les données de santé, la lutte contre le harcèlement.

CONTACT

Barbara GOARANT
communication@c-s.fr
01 41 28 46 94

22 avenue Galilée
92350 Le Plessi Robinson
www.c-s.fr

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

CS

Concepteur, intégrateur et opérateur de systèmes critiques, CS propose des solutions innovantes de confiance numérique et de lutte contre la cybercriminalité pour une protection de bout en bout du Système d'Information et des infrastructures de communication. Du conseil stratégique et opérationnel (RGPD, ISO27000, LPM/NIS) au maintien en condition de sécurité, de la conception d'infrastructures sécurisées à la gouvernance de la sécurité et à l'audit PASSI, CS accompagne ses clients sur l'ensemble de la chaîne de valeur.

Nos solutions :

- SEDUCS : plate-forme d'industrialisation de systèmes d'exploitation minimaux durcis
- TRUSTYBOX : plateforme sécurisée intégrant l'ensemble des services de confiance nécessaires à la sécurisation des données et des échanges dématérialisés certifiés CC EAL3+.
- PRELUDE – SIEM : solution de superviser en temps réel les événements de sécurité.

Agréé CERT (Computer Emergency Response Team), CS accompagne également ses clients dans la mise en œuvre de leur politique de sécurité, la réaction rapide sur incidents de sécurité grâce à son Groupement d'Intervention Rapide (GIR), ainsi que dans le maintien en condition de sécurité de leurs systèmes permettant ainsi d'en assurer la résilience sur tout le cycle de vie.

« CS est aujourd'hui la seule entreprise qui dispose d'une gamme complète de solutions et de produits de sécurité forte entièrement conçue, développée et maintenue en France, labellisées France Cybersecurity. Notre vocation est, plus que jamais, d'apporter des réponses adaptées à la cyberprotection et à la résilience des infrastructures et des systèmes de nos clients. » déclare Khaled Draz, Directeur Général

Spécialisations :
Audit et pentest PASSI, RegTechs (RGPD, LPM, NIS, sectoriel, etc.), Intégration système critique, SIEM/NMS, SOC/NOC, Services de Confiance, cryptographie, CERT/GIR, MCS;

CONTACT

Thomas BOUCHER
tb@datashush.com
+33 (07) 86 87 44 28

45 rue Paul Langevin
33130 BEGLES
http://lockemail.com/

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

DATASHUSH TECHNOLOGY

Datashush Technology SAS «LockEMail.com» est une jeune startup Française (bordelaise) fondée en 2015, elle est soutenue par La région Nouvelle Aquitaine, Bordeaux Unitec et Aquinetic.
La protection des échanges par email est sa priorité.

Associés Français et hébergement en France.

LockEmail chiffre les emails avec des mots de passe et des clés uniques et personnelles, qui ne transitent jamais sur internet.

L'outil LockEMail permet de sécuriser le corps du message et les pièces jointes et permet de protéger tout type de données.

Youtube :
https://www.youtube.com/watch?v=WdgN5-_nzhI

Facebook
https://www.facebook.com/LockEmailByDataShush/

CONTACT

Xavier QUONIAM
xquoniam@denyall.com
+33 1 46 20 96 20

6 avenue de la Cristallerie,
92 310 Sèvres
www.denyall.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

DENYALL

denyall
a Rohde&Schwarz Cybersecurity company

DenyAll, en relation avec l'ANSSI, accompagne les entreprises et les organismes du secteur public dans leur transformation numérique, en s'assurant que les interactions entre utilisateurs sont à la fois faciles et sécurisées.

Les services cloud et les équipements de DenyAll **simplifient le travail des équipes sécurité et DevOps** chargées de la mise en place d'un environnement digital sûr, tout au long du cycle de développement logiciel.

Grâce à un portefeuille complet de produits, nous maitrisons les menaces parvenant du réseau jusqu'à la couche applicative:

- **Des scanneurs de vulnérabilités** pour identifier, classer par ordre de priorité et remédier les vulnérabilités selon l'OWASP Top 10.
- **Une solution d'authentification unique** (Web SSO) pour simplifier et renforcer l'accès des utilisateurs aux applications, en tout lieu et à tout moment.
- Nos **parefeux applicatifs web** pour bloquer les attaques connues et inconnues qui ciblent les applications web, APIs et Web Services et qui reposent sur des technologies modernes (HTML5, JSON, XML, HTTP/2).
- **Un navigateur sécurisé dans un environnement isolé** pour permettre aux utilisateurs de surfer librement et sans danger sur Internet.
- **Un chiffreur Ethernet** pour protéger les organisations contre l'espionnage et la manipulation des données qui sont transportées via Ethernet à travers les interconnexions fibre ou cuivre, les faisceaux hertziens et les liaisons par satellite.

La récente acquisition de DenyAll par Rohde & Schwarz Cybersecurity nous permet de bénéficier d'un environnement idéal pour continuer à innover afin de protéger nos clients **contre les menaces et les cyberattaques de demain.**

Labels :

- **CSPN par l'ANSSI** : L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a qualifié et décerné aux parefeux applicatifs DenyAll son certificat de sécurité de premier niveau (CSPN).
- **Label France Cybersécurité** : DenyAll a reçu le label « France Cybersécurité » décerné par les utilisateurs et le gouvernement, qui récompense la qualité et la performance de nos parefeux applicatifs.
- **Gartner** : Dans le Magic Quadrant 2017 pour les Web Applications Firewalls, Gartner met en avant les moteurs de sécurité avancée et la facilité d'utilisation de DenyAll WAF.

ROHDE&SCHWARZ
Cybersecurity

CONTACT

Elie GASNIER
ega@ecrin.com
33 (0)1 69 07 04 44

Immeuble Odyssée – Bât D 3è étage
2/12 Chemin des Femmes
91300 MASSY

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

ECRIN SYSTEMS

ecrin SYSTEMS
Rugged Computers

ECRIN Systems sert une grande variété de marchés qui ont pour point commun un haut niveau d'exigences techniques, environnementales et sécuritaires évoluant dans des contextes très concurrentiels :

- Aérospatiale, Défense et Sécurité
- Systèmes d'information et de communication
- Transports et Energie
- Equipements industriels

o Proximité, innovation, excellence et engagement, telles sont les valeurs qui nous animent pour apporter à nos clients la bonne solution technologique qui fera le succès de leurs projets.

La Proximité… pour bien vous servir : compréhension de votre besoin, réelle force de conseil en technologies et en architectures systèmes, équipe dédiée à votre projet, réseau de partenaires à l'Export (Europe, BRICS, Moyen-Orient, Asie du Sud-Est, Afrique…), accompagnement à l'export (accords de coopération, mise en place d'OFFSET pour les grands donneurs d'ordres)

L'Innovation… pour imaginer les produits de demain : a « bonne » solution technique à un coût maîtrisé, des produits adaptés aux problématiques actuelles, l'innovation marqueur de notre ADN

L'Excellence… pour dépasser vos exigences : assurance d'une continuité de fonctionnement optimale, garantie d'un Retour sur Investissement (ROI) élevé

'Engagement… pour fortifier notre relation et instaurer un relationnel de qualité et un véritable climat de confiance.

CONTACT

Cathy DEMARQUOIS
cathy.demarquois@atos.net
+33 (0)1 30 80 70 00

Rue Jean Jaures - BP68
78340 Les Clayes
www.evidian.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

EVIDIAN

Bull Evidian

Evidian, leader européen en IAM - Identity & Access Management, propose une suite complète, intégrée et modulaire de gestion des identités et des accès compatible avec la politique de sécurité de l'entreprise et les nouvelles exigences réglementaires (RGPD…). Cette offre permet de gouverner, administrer et sécuriser les accès des utilisateurs à leurs applications de leurs arrivées à leurs départs. Elle renforce leurs authentifications et droits d'accès depuis leur environnement numérique et tous types de terminaux. Evidian simplifie l'accès aux applications avec un Single-Sign-On universel.

Plus de 5.000.000 d'utilisateurs dans plus de 900 organisations dans le monde se connectent chaque jour à leur entreprise et gèrent leurs droits d'accès avec les solutions de gestion des identités et des accès d'Evidian.

L'IAM est une brique majeure de la sécurité des systèmes d'information. La multiplication des données, des applications et des profils des personnes y accédant nécessite de gouverner de façon optimisée les habilitations des utilisateurs aux ressources pertinentes en maîtrisant les risques. Pour ce faire il faut gagner l'adhésion des utilisateurs et des métiers et offrir aux directions informatiques les outils adaptés aux nouveaux cas d'usage et au développement des services dans le Cloud.

Evidian couvre l'ensemble des besoins depuis l'assurance d'identité de l'utilisateur, jusqu'à l'intelligence qui s'opère sur la gestion du cycle de vie de leur identité numérique et de leur accès depuis n'importe quel terminal et pour accéder à toutes les ressources de l'organisation :

Identity Governance and Administration : gestion des identités, habilitations et accès
Identity Analytics and Intelligence : suivi et analyse de l'utilisation du système IAM
Enterprise-SSO : mot de passe unique et sécurisé
Web Access Manager : Web SSO et fédération des identités
Authentication Manager : gestion les moyens d'authentification forte,

Plus d'information : www.evidian.com

CONTACT

Sylvie BEC
Sylvie.bec@gemalto.com
+33 1 55 01 50 00

6 rue de la Verrerie
92190 Meudon
www.gemalto.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

GEMALTO

gemalto
security to be free

Les solutions SafeNet de Gemalto garantissent la sécurité des identités et des données, leur communication entre les organisations et les personnes ainsi que les appareils pour l'Internet des objets en plein essor. Nous protégeons et contrôlons l'accès aux informations sensibles, sécurisons les données dans les environnements virtuels et sur le Cloud, sécurisons les transactions, gérons les risques et garantissons la conformité.

Accès simple et sécurisé
Nos solutions d'authentification forte multi-facteurs, faciles à utiliser, offrent un accès sécurisé aux réseaux et applications de l'entreprise, et protègent et valident les identités des utilisateurs. De nombreux gouvernements et grandes entreprises nous font confiance pour sécuriser leurs informations sensibles, contrôler les accès, protéger les identités, garantir la propriété des données et veiller à la confidentialité des communications.

Confiance dans le Cloud
Nos solutions d'authentification, de chiffrement et de gestion des clés pour le Cloud renforcent la confiance des entreprises en prenant en compte les enjeux cruciaux de la gouvernance, du contrôle et de la propriété. Nous permettons également aux fournisseurs de services Cloud de garantir à leurs clients la protection de leurs données avec des solutions d'authentification et de chiffrement modulables et faciles à déployer.

Protection des données
Nos solutions de chiffrement protègent les données sensibles, aussi bien lors du stockage que de leur transfert. Quel que soit l'emplacement des données (centres de données physiques ou virtuels), nos solutions permettent aux entreprises d'assurer une protection efficace dans toute l'organisation et à se conformer aux nouvelles règlementations. Nos HSMs protègent l'infrastructure cryptographique de nos clients en fournissant des services de chiffrement, de déchiffrement, d'authentification et de signatures numériques pour une large gamme d'applications.

CONTACT

Yann GRIVET
commercial@icodia.com
0230964059

22 rue de l'Erbonière,
35510 Cesson-Sévigné

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

ICODIA

Basé stratégiquement à Rennes depuis 20 ans, Icodia dispose de son propre datacenter sécurisé haute disponibilité.
Acteur atypique du marché, Icodia développe en interne ses solutions nécessaires aux services d'hébergement : sécurisation, supervision, environnements décisionnels, IHM...

Fort d'une expérience de R&D importante, d'une volonté d'innovation permanente et d'une réelle culture de la sécurité, Icodia constitue une véritable valeur ajoutée sur le marché des systèmes connectés. La rencontre des compétences réseau, de l'ingénierie logicielle, de la cybersécurité et de l'IoT, a permis de construire une plateforme d'hébergement avant-gardiste.

L'offre globale d'Icodia repose sur 3 axes.
1/ Des offres d'hébergement sécurisées et supervisées dans son datacenter TIER IV :
La mise en place d'un système à très haute disponibilité vous offre des garanties multiples. Elle doit être adaptée à votre besoin spécifique. Les possibilités techniques que nous vous proposons sont très nombreuses : nous vous accompagnons dans son étude et sa conception, comme pour sa mise en œuvre et son suivi. Il s'agit d'anticiper les problèmes qui pourraient intervenir et de mettre en place les moyens qui les solutionnent.

2/ Un pôle R&D orienté haute disponibilité et cybersécurité :
Nous disposons d'un pôle de recherche et développement qui mobilise l'ensemble de nos équipes.
Nos nombreuses contributions au sein des fondations open-source permettent de conserver un lien permanent avec les communautés.
Nous lions nos recherches en cyber à l'informatique décisionnelle, car nous considérons cet ensemble comme l'avenir.

3/ Des offres d'infogérance et d'audit coordonnées par les meilleurs spécialistes :
Un entretien et des audits réguliers de votre infrastructure sont indispensables. Ils garantissent la prise en charge des pannes et un retour sur incident très rapide.

CONTACT

Coralie HERITIER
info@idnomic.com
0155642200

175 rue Jean-Jacques Rousseau,
9213 Issy-les-Moulineaux

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

IDNOMIC

IDnomic est le leader de la protection et la gestion des identités numériques.

IDnomic est au cœur des préoccupations des utilisateurs qui veulent communiquer, s'identifier et échanger des informations confidentielles en se sentant protégés :

- Les collaborateurs d'une entreprise qui doivent disposer d'un accès sécurisé aux données via tout type de réseau ou d'infrastructure IT et où qu'ils soient.
- Les objets connectés qui doivent être déployés dans un environnement sécurisé et maitrisé pour être utilisés, en toute confiance, par le grand public.
- Les citoyens qui ont besoin de titres d'identité électronique (passeport, titre de séjour, permis de conduire, etc.) non falsifiables lors de leurs déplacements ou pour accéder à un e-service administratif sécurisé.

IDnomic délivre ses services PKI (Public Key Infrastructure) en mode Cloud ou licence.

Basées sur des normes reconnues par de nombreuses instances gouvernementales en France, en Europe et dans le monde, les technologies d'IDnomic apportent les garanties les plus strictes de services certifiés parmi lesquelles :

- La qualification PSCE / PSCO
- La qualification CC EAL 4+
- La classification Secret OTAN
- La certification ETSI
- Le Label France Cybersecurity

CONTACT

Thierry BETTINI
info@ilex-international.com
+33 (0)1 46 88 03 40

51 boulevard Voltaire
92600 Asnières-sur-Seine

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

ILEX INTERNATIONAL

Ilex International est un éditeur de logiciels spécialiste de la gestion des identités et des accès depuis plus de 15 ans, largement reconnu dans le domaine de la cybersécurité.

Sur un marché exigeant et en perpétuelle évolution, Ilex International occupe une place prépondérante grâce à sa capacité d'innovation et à sa flexibilité. Faire le choix d'Ilex International, c'est faire le choix d'une société capable de prendre en compte rapidement vos nouveaux besoins issus d'évolutions technologiques ou réglementaires.

Ses solutions répondent aux exigences de toutes les entreprises et organisations soucieuses de la sécurité de leur système d'information, en France comme à l'international. Elles couvrent le périmètre de l'entreprise et de ses utilisateurs internes mais vont également au-delà de ses frontières en offrant des réponses dédiées aux utilisateurs externes (clients, citoyens, partenaires).

Ilex International s'appuie également sur un solide réseau de partenaires spécialisés (éditeurs, intégrateurs) qui complètent son offre et la rendent plus compétitive. Ses clients bénéficient ainsi d'un panel de technologies et de solutions parfaitement adaptées à leurs attentes, d'une réactivité accrue en ligne avec leurs besoins et d'une couverture géographique et métier optimale.

CONTACT

Jean VILLEDIEU
jean@linkurio.us
0952060855

14 rue Soleillet,
75020 Paris France

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

LINKURIOUS

LINKURIOUS
VISUALIZE GRAPH DATA EASILY

Linkurious conçoit et fournit une solution logicielle d'analyse de données permettant de détecter, d'investiguer et de surveiller des menaces telles que les fraudes informatiques, les cyberattaques, ou les failles de sécurité.

Pallier efficacement aux failles de sécurité ou aux cyberattaques reste un défi considérable pour les analystes et experts en cybersécurité. Les réseaux et infrastructures de plus en plus complexes génèrent aujourd'hui des téraoctets de données hétérogènes au sein desquels il est difficile, parfois impossible, de détecter risques ou comportements inhabituels. Il est essentiel de ramener, à la fois les proportions et la complexité des données produites, à un niveau plus intelligible pour trouver des solutions appropriées et améliorer la sécurité globale.

Avec son logiciel d'analyse et de visualisation de données, Linkurious vous propose de contextualiser, de simplifier et d'accélérer vos investigations afin d'améliorer la sécurité de votre organisation.

Grâce à sa technologie de visualisation, Linkurious Enterprise rend accessible les connections entre une multitude de données, allant de données système à des données issues de rapports publics de vulnérabilité, stockées dans des bases des données de graphes. L'analyse et la visualisation de ces graphes de données sont une approche efficace pour comprendre et surveiller des connexions dynamiques, complexes et multiples.

Linkurious aide ainsi les analystes à prévenir des risques existants et à investiguer des incidents de sécurité. L'analyse des dépendances au sein des systèmes d'information permet par exemple d'identifier des vulnérabilités et d'anticiper des menaces. L'analyse des données relatives à une attaque peut, elle, permettre d'en évaluer la nature et la portée afin de prendre les mesures adéquates.

CONTACT
Christophe TREMLET
christophe.tremlet@maximintegrated.com
04 42 98 14 80

INNOVA CARD, Maxim Integrated Company, ZI Athélia 4 - Le Forum Bât.A - Quartier Roumagoua - 13600 LA CIOTAT

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

MAXIM INTEGRATED

maxim integrated™

Maxim Integrated est un fournisseur de semi-conducteurs mondial qui s'est engagé très tôt dans la sécurité numérique. En effet nous avons mis sur le marché en 1993 le premier microcontrôleur sécurisé. Depuis nous n'avons cessé d'investir dans des solutions à base de circuits intégrés de façon à répondre aux exigences toujours croissantes dans ce domaine. Aujourd'hui environ un terminal de paiement sur trois dans le monde est sécurisé grâce à une solution Maxim.

Avec nos circuits d'authentification et nos microcontrôleurs sécurisés nous avons un des portefeuilles de produits les plus importants de l'industrie.

Nous avons récemment mis au point une technologie de type PUF (Physically Unclonable Function ou fonction non clonable) ou ChipDNA™ permettant la génération de clefs privées avec un niveau de sécurité physique jamais égalé à ce jour.

Nos circuits intégrés s'adressent principalement aux systèmes embarqués. Un des principes en cybersécurité est le concept de « racine de confiance ». L'idée est que pour être sécurisé un système doit s'appuyer sur un élément materiel de confiance sur lequel on peut bâtir la sécurité du système. Nos circuits d'authentification et nos micro contrôleurs sont conçus pour être cette racine de confiance.

CONTACT

Alexandre OSTAPOFF
sales@oikialog.com
01-43-34-09-04

54 rue de Bitche
92400 COURBEVOIE

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

OIKIALOG

OïkiaLog

Intégrateur en sécurité informatique, OïkiaLog accompagne ses clients sur l'ensemble des phases des projets de sécurisation des systèmes d'information les plus sensibles.

SIEM/SOC

Fort de plus de 20 ans d'activité dans les domaines de l'analyse des logs (SIM/SEM/SIEM), les experts d'OïkiaLog capitalisent une expérience unique sur ces sujets. La force d'OïkiaLog vient de la complémentarité de ses équipes qui allient 3 types de profils très complémentaires : expert sur les logs, intégrateur et développeur, tous expérimentés en sécurité des systèmes d'information.

OïkiaLog intervient pour ses clients dans l'ensemble des phases des projets d'exploitation des logs : de la définition du besoin à l'exploitation dans un SOC, en passant par les phases de recherche de solution, d'intégration, d'adaptation, d'industrialisation, de maintien en condition opérationnelle et de formation. La recherche, la définition et la création d'indicateurs pertinents dans l'environnement du client font parties du champ de compétence d'OïkiaLog.

Conseil et intégration en SSI

OïkiaLog revend et intègre une offre de sécurité complète :

- Firewall
- Scanner de vulnérabilité
- SIM/SEM/SIEM
- Contrôle de conformité
- Anti-spam
- Gestion de comptes à privilège
- SSO

Service, audit de sécurité, développement spécifique et formation

OïkiaLog propose à ses clients de préparer le projet sécurité : analyse de l'existant et déduction des besoins spécifiques, aide au choix de solutions : enrichissement de l'existant, développement particulier, solution du marché.

OïkiaLog propose aussi d'évaluer le niveau de sécurité de ses clients par le biais de différents types de tests d'intrusion.

OïkiaLog propose l'intégration des solutions préconisées. Cette intégration est réalisée selon une méthodologie éprouvée de gestion de ce type de projet. La mission d'intégration est confiée à une équipe composée d'un chef de projet et de différents experts techniques alliant de fortes compétences sur les solutions de sécurité ainsi qu'en développement en tous types de langages.

OïkiaLog réalise des formations à la sécurité, ainsi que des modules adaptés aux besoins de ses clients.

CONTACT

Laurent NOE
laurent.noe@oveliane.com
0661168397

54 rue de Bitche
92400 COURBEVOIE

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

OVELIANE

Le contexte actuel de la sécurité est très tendu : les attaquants, créatifs et obstinés, trouvent régulièrement le moyen de contourner les technologies de prévention mise en place par les équipes de sécurité informatique.
La plupart des attaques et en particulier les APT, ont des effets similaires sur leur cible : connexions sur le serveur, élévation de privilège, création de compte, puis ajout ou modification de configuration. Dès lors, l'absence de surveillance des serveurs aura des conséquences dramatiques !

Or, les deux catégories d'outils classiques de sécurité atteignent leurs limites :
• Les outils de protection périmétrique, indispensables mais insuffisants.
• Les outils de détection d'attaque contraints à une course permanente derrière les attaquants.
OVELIANE propose OSE, une autre approche : plutôt que de traquer les attaques, il faut surveiller leurs cibles.

OSE démasque les actions illicites (APT) :
• Altération des composants du système et des applications
• Présence de flux réseaux inhabituels ou injustifiés
• Apparition de nouveaux processus

OSE permet de :
• **Protéger par un contrôle d'intégrité** : étanchéité et suivi des dossiers sensibles, ressources nouvelles et manquantes, contrôle et surveillance (journaux, alarmes), limitation des accès aux protocoles de commande, limitation des accès aux protocoles de réseau ...
• **Détecter les services dangereux ou interdits**, mauvaise configuration, incohérences, droits d'accès anormaux, mots de passe faibles, répertoires et fichiers suspects, modification de fichiers, accès réseau illégitimes ou suspects pour serveurs, ressources nouvelles ou manquantes ...
• **Déployer la politique de sécurité** de l'entreprise sur tous les serveurs Unix, Linux et Windows dans l'organisation : liste des ports / services autorisés, politique de mot de passe, liste des fichiers sensibles, restrictions sur les fichiers partagés, règles d'accès sur le système et les applications ...
• **Contrôler la conformité des systèmes** (référentiels standards, préconisation ANSSI)

CONTACT

Nicolas BACHELIER
nicolas.bachelier@primx.eu
0177726480

27 rue Maurice FLANDIN,
69444 Lyon Cedex 03
www.primx.eu

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

PRIM'X

PRIM'X
CORPORATE ENCRYPTION SYSTEMS

PRIM'X est un éditeur de logiciels packagés dans le domaine de la sécurité Informatique et plus particulièrement dans celui du chiffrement.

Pour une meilleure protection des données sensibles, contre la perte, le vol, la publication et l'espionnage économique, PRIM'X introduit une nouvelle manière d'appliquer le chiffrement dans une entité. Les données sont partout et disséminées à la fois. La classification de l'information est une entreprise ardue, et sa valeur réelle n'est pas celle qu'on lui attribue, mais celle qu'un ennemi lui donne. Il est donc nécessaire d'adopter une politique globale : **Encrypt Everything, Everywhere, and Always.**

Pour PRIM'X, le chiffrement doit être GLOBAL, SIMPLE et TRANSPARENT, AUTOMATIQUE et dirigé par une POLITIQUE DE SÉCURITÉ. Il permet aussi de gérer le DROIT D'EN CONNAÎTRE en cloisonnant cryptographiquement les données, y compris au sein même de l'organisation qui le met en œuvre, entre utilisateurs/services et notamment vis-à-vis des opérateurs techniques.

Les clients de PRIM'X sont principalement des Grands Comptes Européens ainsi que des Administrations et Ministères qui ont opté pour des équipements massifs des logiciels PRIM'X (Etat français, fin 2015 et Conseil de l'Union européenne en 2017).

Les solutions de PRIM'X ont obtenu les labels suivants :
- Certifications Critères Communs EAL3+ et Qualification ANSSI, niveau standard
- Label France CyberSecurity
- Agrément Diffusion Restreinte, Diffusion Restreinte OTAN, Restreint UE et EUROCOR Diffusion restreinte
- Catalogue de l'OTAN et catalogue des produits cryptographiques de l'UE

ZoneCentral
Chiffrement de dossiers et fichiers : espace de travail, serveurs de fichiers, partages, clés USB…

Orizon
Chiffrement des environnements utilisateurs et partagés dans le Cloud.

ZonePoint
Chiffrement de documents dans les bibliothèques SharePoint®.

Zed! et ZedMail
Conteneurs chiffrés pour les échanges, les archives, les emails...

Cryhod
Chiffrement des disques des laptops avec authentification pré-boot.

CONTACT

Eléonore FORGET
eforget@riskeco.com
+33 (01) 55 24 23 16

«38 rue Jacques Ibert
92300 Levallois-Perret»

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

RISK&CO SOLUTIONS

Créé en 1994, le Groupe Risk&Co a su se hisser au rang des leaders français de l'ingénierie et de la gestion des risques en France et à l'international.

Le Groupe exerce aujourd'hui ses activités dans trois domaines majeurs :
• L'activité historique de conseil en intelligence stratégique et en sécurité pour les sites et infrastructures critiques (Risk&Co) ;
• La cybersécurité et l'ingénierie de sûreté (Risk&Co Solutions) ;
• Le déminage en milieu terrestre et maritime et le démantèlement de munitions (Geomines).

Dans chacun de ces domaines, le Groupe offre à ses clients des solutions complètes incluant le diagnostic des risques, la définition de schémas directeurs et l'accompagnement opérationnel à leur mise en œuvre sur le terrain.

Risk&Co Solutions est la filiale technologique du groupe Risk&Co.

Au travers de prestations d'audit, de conseil et d'ingénierie, notre mission est d'assister nos clients, maîtres d'œuvres ou maîtres d'ouvrages, dans la sécurisation physique et logique de leurs infrastructures sensibles.

Démontrées par des références d'envergure internationale, nos expertises portent tant sur des secteurs d'activité clés (énergies, défense, infrastructures, grands sites tertiaires…), que sur des typologies de systèmes - systèmes industriels et systèmes de sûreté/sécurité.

Portés par des équipes pluridisciplinaires, intégrant experts cyber et spécialistes métiers, nos services comprennent l'identification de risques et vulnérabilités (audits, analyses de risques), la réduction de risques (plans d'actions, gouvernance), l'homologation et la mise en conformité réglementaire.

CONTACT
Cathy LESAGE
cathy.lesage@rubycat-labs.com
+ 33(0)2 99 30 21 11

1137 A Avenue des Champs Blancs
35510 CESSON SEVIGNE - France
www.rubycat-labs.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

RUBYCAT

Entreprise bretonne innovante, RUBYCAT-Labs est un éditeur spécialisé en traçabilité et contrôle d'accès sensibles au Système d'Information.
Vos serveurs contiennent des données ou applications sensibles qu'il faut protéger pour garantir la continuité de votre activité, la pérennité de votre entreprise :

- Toute action sur un serveur critique doit impérativement être surveillée, tracée et facilement identifiable.
- Toute personne à droits privilégiés doit être clairement identifiée et son accès restreint.

La solution logicielle PROVE IT de RUBYCAT-Labs adresse les problématiques de Contrôle et d'Auditabilité des accès critiques aux ressources du système d'information.

Ce portail d'accès centralisé aux ressources apporte également une réponse pragmatique et simple à la gestion et la traçabilité des accès aux données sensibles, notamment dans le cadre d'une mise en conformité règlementaire (par exemple pour l'application du Règlement Général de Protection des Données - RGPD).

Intuitive, souple et non invasive, la brique logicielle PROVE IT s'interface facilement dans l'environnement existant (pas d'installation d'agent sur les postes clients ni sur les serveurs cibles) et offre un interfaçage natif avec des concentrateurs de journalisation et solutions de gestion d'évènements de sécurité (SIEM).

La solution PROVE IT est déployée dans des entreprises de toutes tailles (ETI, PME, PMI, ...) et de tous secteurs d'activité : Collectivités, Industrie, Distribution, Hébergeur et Santé qui sont impactés par ces problématiques de traçabilité et de contrôle des utilisateurs à privilèges.

www.rubycat-labs.com

CONTACT

Sergio LOUREIRO
sales@secludit.com
0492911104

2405 route des Dolines
Drakkar batiments C et D
06560 Sophia Antipolis

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

SECLUD IT

SecludIT aide les entreprises qui ont fait le choix du Cloud à renforcer leur sécurité avec une approche préventive du risque : la détection continue et automatique.

SecludIT est un éditeur français de logiciels de détection des failles de sécurité sur les infrastructures virtualisées, Cloud et hybrides.

Membre fondateur de la Cloud Security Alliance, Sergio Loureiro – PDG de SecludIT – a noué de nombreux partenariats avec les principaux acteurs du marché du Cloud comme AWS, Microsoft Azure, Google Cloud Compute, HP ou IBM entre autres pour développer ses solutions.

Les équipes de SecludIT accompagnent les entreprises dans leur transition numérique et notamment dans leur migration vers une infrastructure Cloud. Les besoins en sécurité n'étant pas les mêmes que pour une infrastructure physique, elles doivent se tourner vers une solution adaptée dans le but d'endiguer le risque de cyber-attaques.

Grâce à notre solution de Cloud Analytics vous pourrez :

- Utiliser une seule solution d'analyse compatible Multi cloud
- Inventorier automatiquement tous vos actifs (serveurs, cloud Workloads, réseaux, …)
- Cloner les serveurs à analyser sans affecter la production
- Détecter en continu toutes vos vulnérabilités
- Vérifier le respect des bonnes pratiques de sécurité IaaS
- Obtenir des rapports de risque complets et compréhensibles
- Surveiller en continu votre niveau de risque ANSSI, RGPD, OWASP et PCI DSS
- Suivre un plan d'action simple et efficace grâce à nos propositions de solutions

Label France Cybersécurité :
SecludIT a reçu le « label France Cybersécurité » décerné par les utilisateurs et le gouvernement, qui récompense la qualité et la performance de nos solutions de détection continue des failles de sécurité.



CONTACT

David BIZEUL
david.bizeul@sekoia.fr
0664458429

18-20 Place de la Madeleine,
75008 Paris

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

SEKOIA

SEKŌIA

SEKOIA (50 collaborateurs, 4M€ de Chiffre d'Affaires, 25% d'activité d'innovation, et 200 professionnels de la sécurité formés chaque année) apporte depuis 2008, conseils, expertises et innovations en cybersécurité pour répondre aux enjeux d'un monde volatile, complexe et ambigu. Nous intervenons principalement pour de grands acteurs français et européens.

Quelques exemples de success stories clients en 2017 via SEKOIA :

- Concevoir une solution clé en main de supervision de la sécurité
- Parvenir à traiter efficacement NotPetya
- Simuler une attaque ciblée réaliste pour évaluer les processus de détections et de réaction
- Monter rapidement en puissance sur des besoins de threat intelligence

Nous accompagnons nos clients via nos 4 piliers complémentaires :

• Du consulting pour concevoir, structurer ou repenser l'organisation de la sécurité et accompagner les entreprises dans leurs choix stratégiques, en leur permettant d'identifier les actifs et leurs faiblesses, notamment dans les domaines suivants : transformation numérique des entreprises, la sécurité, la mise en conformité RGDP, analyse de risques.

• Un centre de formation SEKOIA dédié, avec 30 formations au catalogue et 200 stagiaires formés par an, assure depuis 2008, la montée en compétence et la certification des entreprises et des personnes sur tous les sujets liés à la sécurité des SI.

• De l'expertise pour intervenir sur les problématiques techniques les plus complexes notamment pour des missions d'expertise poussée.

Sur le plan défensif, SEKOIA met à disposition son CERT pour limiter les impacts chez ses clients. Nos activités de threat intelligence distribuées sous la marque inThreat sont également accessibles à nos clients pour limiter l'exposition aux menaces.
Sur le pan offensif, SEKOIA dispose d'une équipe interne d'experts spécialisés dans les activités d'audit techniques et de tests intrusifs. Simulation d'attaque ciblée, Pentest hardware, Evaluation d'API, analyse de protocoles font partie des capacités internes.

• Une gamme de produits en mode SaaS qui simplifient l'usage de la sécurité:
o **inThreat** : Threat Intelligence (inThreat.com)
o **DediMISP** : partage d'indicateurs techniques (dedimisp.com)
o **FastIR** : investigations forensics
o **Vudip** : identification des vulnérabilités
o **ViralStudio** : Analyse de code malveillants
o **WotchR** : cybersurveillance

Tous ces produits sont distribués via sekoia.io et sont accessibles via le centre de services SEKOIA associé.

CONTACT

Stéphanie JEGAT
s.jegat@siepel.com
02 97 55 73 74

PA de Kermarquer, impasse de la Manille, 56470 La Trinité-sur-Mer

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

SIEPEL

C'est en 1986 que SIEPEL (Société Industrielle d'Etudes et Protections Electroniques), entreprise à capitaux privés 100% française, a installé à La Trinité-Sur-Mer son siège social et ses unités de production. Notre cœur de métier est la cybersécurité des infrastructures.

Face aux menaces de type anti-compromission et Agressions ÉlectroMagnétiques Intentionnelles (AGREMI) : Impulsion ElectroMagnétique (IEM), Impulsion ElectroMagnétique d'origine Nucléaire (IEMN), High Intensity Radiated Fields (HIRF), nous œuvrons pour la Sécurité des Systèmes d'Information (SSI) et datacenters.
Nous sécurisons également les salles de réunion à propos sensibles.

L'expertise de SIEPEL repose sur la maîtrise de nombreuses capacités techniques et sur le souci permanent d'améliorer sa souplesse opérationnelle. De nombreuses références auprès d'institutions gouvernementales et d'entreprises privées attestent de ces savoir-faire spécifiques.

Deux labels France Cybersecurity (Cage de Faraday anti-compromission hautes performances en 2016 et Mesure d'affaiblissement électromagnétique en 2017) reconnaissent nos capacités professionnelles et expérience.

SIEPEL dispose d'une habilitation de Défense délivrée par l'Administration française, reconnue par l'UE et l'OTAN.

CONTACT

Jean-Luc GIBERNON
jean-luc.gibernon@soprasteria.com
06 81 27 86 52

Tour Manhattan - 5 place de l'Iris
92950 – LA DEFENSE CEDEX

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

SOPRA STERIA

Leader européen de la transformation numérique, Sopra Steria a réalisé un CA de 3,7 Mds euros en 2016 et compte à ce jour un effectif de 40 000 collaborateurs répartis dans plus de 20 pays en Europe et dans le monde. En combinant valeur ajoutée, innovation et performance des services délivrés le Groupe propose l'un des portefeuilles d'offres les plus complets du marché en conseil, intégration de systèmes, édition de solutions métier, infrastructure management et Business Process Services.

Positionné dans tous les secteurs de l'économie – industrie, services, télécommunications et banques notamment – le Groupe est présent de manière significative dans les domaines **aéronautique, naval et nucléaire** pour lesquels il dispose d'une expertise reconnue en ingénierie, développement et maintenance de logiciels critiques. Il apporte ainsi une réponse globale aux enjeux de développement et de compétitivité des grandes entreprises et des organisations.

De plus, Sopra Steria témoigne d'une forte implication dans le secteur **de la Défense et de la Sécurité.** Le Groupe intervient en particulier dans le domaine des SI opérationnels et logistiques au profit des armées ainsi que dans des projets majeurs et en outsourcing d'applications sensibles dans le domaine de la Sécurité intérieure. Les exigences associées en termes de sécurité des systèmes et applications ont justifié la mise en place de structures et de compétences spécifiques qui lui permettent de s'afficher comme un acteur de confiance majeur dans les secteurs ressortissant aux prérogatives régaliennes des États.

Une **offre Cyber transverse** à l'ensemble des secteurs et activités se décline selon une approche globale couvrant l'ensemble du cycle de vie de la sécurité.

CONTACT

Sylvie WUIDART
+33 6 85812426
sylvie.wuidart@st.com

ZI de Rousset BP2 13106 Rousset
Cedex - France

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

STMICROELECTRONICS

ST, un leader mondial sur le marché des semiconducteurs, fournit des produits et des solutions intelligents qui consomment peu d'énergie et sont au cœur de l'électronique que chacun utilise au quotidien. Les produits de ST sont présents partout, et avec nos clients, nous contribuons à rendre la conduite automobile, les usines, les villes et les habitations plus intelligentes et à développer les nouvelles générations d'appareils mobiles et de l'Internet des objets.

Par l'utilisation croissante de la technologie qui permet de mieux profiter de la vie, ST est synonyme de « life. augmented ».

En 2016, ST a réalisé un chiffre d'affaires net de 6,97 milliards de dollars auprès de plus 100 000 clients à travers le monde. Des informations complémentaires sont disponibles sur le site : www.st.com.

CONTACT

Matthieu BONENFANT
matthieu.bonenfant@stormshield.eu
+33.(0) 4 78 14 04 24

1 place Verrazzano
69009 LYON

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

STORMSHIELD

STORMSHIELD

Leader européen de la sécurité des infrastructures digitales et filiale à 100% d'Airbus CyberSecurity, nous proposons des solutions communicantes et intelligentes pour anticiper les attaques et protéger les infrastructures digitales IT et OT.

Notre mission : assurer la cybersécurité et la protection des données des organisations, de leurs collaborateurs et de leurs clients.

Notre expertise se décline en trois gammes de produits complémentaires pour une sécurité sans failles :

- Protection des réseaux informatiques et industriels (Stormshield Network Security) ;
- Protection des postes et serveurs (Stormshield Endpoint Security) ;
- Protection des données (Stormshield Data Security).

L'interaction de nos trois gammes de produits, dans notre approche Multi-Layer Collaborative Security, renforce le niveau de protection des environnements IT, OT et Cloud quel que soit le point d'attaque.

Ces solutions de pointe et de confiance sont certifiées au plus haut niveau européen (Restreint UE, OTAN, ANSSI EAL3+/EAL4+). Présents dans plus de 40 pays via notre réseau de partenaires distributeurs, nous assurons la protection des informations stratégiques d'entreprises de toutes tailles, d'administrations publiques et d'organismes de défense partout dans le monde.

Les technologies Stormshield sont certifiées pour garantir un niveau de protection optimal :

- Restreint Union Européenne
- Restreint OTAN
- Critères Commun EAL3+/EAL4+
- Qualification Standard ANSSI
- Label « France Cybersecurity »

NETWORK SECURITY

ENDPOINT SECURITY

DATA SECURITY

CONTACT

Corinne MURCIA GIUDICELLI
c.murcia@surys.com
+33 (0) 1 64 76 31 00

22, avenue de l'Europe,
77600 Bussy Saint Georges
www.surys.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

SURYS

SURYS

SURYS est leader mondial dans la conception, la production et la commercialisation de systèmes optiques et digitaux de protection des documents régaliens de haute sécurité et d'authentification d'Identité contre la fraude et la contrefaçon. Depuis plusieurs années, SURYS développe son concept de « puce optique » pour sécuriser l'authentification et l'identification, et connecter des documents et des personnes au monde digital.

Les besoins de plus en plus en fréquents de s'identifier pour accéder à des services digitaux ont amené SURYS à concevoir la solution Photometrix™ afin d'accompagner les Gouvernements et les citoyens dans le changement culturel vers une identité numérique. La solution Photometrix™ permet une dématérialisation de l'identité et en ce sens, est une solution de transition optimale d'un point de vue coût et implémentation vers une identité totalement numérique.

Photometrix™ est la combinaison innovante d'une image et d'un code barre 2D qui permet une authentification automatisée du portrait du porteur du document sans connexion réseau. Le Photometrix™ est généré par un mécanisme de codage basé sur des caractéristiques particulières du portrait, de certaines données relatives au porteur du document (nom, date de naissance etc..) ainsi que des informations biométriques. Ces éléments sont ensuite compressés pour représenter seulement quelques octets d'informations et optimiser l'espace requis sur le document.

Le Photometrix™ se contrôle à partir d'un accessoire numérique (téléphone, tablette, etc..) aussi bien sur un document physique que sur un document dématérialisé : Il s'effectue par une App dédiée, pouvant indifféremment vérifier un code physique ou dématérialisé, garantissant ainsi une grande souplesse d'utilisation et une sécurité élevée.
Le Photometrix™ une clé d'accès sécurisée qui ouvrent les portes à une aux multitudes opportunités du monde digital.

CONTACT

Antoine COUTANT
a.coutant@systancia.com
03 89 33 58 20

Actipolis III - Bât. C11
3, rue Paul Henri Spaak
68390 Sausheim

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

SYSTANCIA

Systancia est un acteur européen reconnu sur les marchés de la virtualisation, de la cybersécurité et de la confiance numérique, proposant la nouvelle génération d'infrastructure de mise à disposition des applications centrée sur la sécurité et les utilisateurs : solutions de virtualisation d'applications et VDI, de sécurité des accès externes, de surveillance des utilisateurs à pouvoirs (PAM), d'authentification unifiée (SSO) et de gestion des identités (IAM).

Misant sur l'innovation comme moteur de croissance, Systancia s'appuie sur la valeur technologique de ses produits et la proximité entre ses équipes et ses clients pour répondre aux besoins des utilisateurs et ainsi atteindre 98 % de satisfaction clients.

Depuis plusieurs années maintenant, les ingénieurs de La Forge, le centre de Recherche & Développement de Systancia, travaillent au quotidien pour améliorer l'expérience utilisateur et la sécurité en matière d'accès aux applications. Systancia a notamment été l'un des premiers éditeurs à intégrer les technologies de machine learning dans ses solutions que ce soit pour prédire les usages de l'utilisateur pour un accès en temps réel aux applications ou pour identifier les comportements suspects sur le Système d'Information en temps réel afin de contenir les cybermenaces.

Systancia bénéficie d'une véritable reconnaissance comme en témoigne la Qualification – Niveau élémentaire délivrée par l'ANSSI à sa solution de cybersécurité, qui en fait la seule solution du domaine technique « identification, authentification et contrôle d'accès » à être recommandée par cette autorité nationale pour la sécurité des SI.

CONTACT

Laurent OUDOT
press@tehtri-security.com
+33(0)9-72-50-80-33

13-15 rue Taitbout
75009 PARIS
www.tehtris.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

TEHTRIS

Alors que les intrusions malveillantes se multiplient sur Internet, la société française TEHTRIS, implantée à Bordeaux Métropole, propose une solution nommée eGambit, capable d'unifier les capteurs de Cybersécurité à l'échelle d'une entreprise, déjà déployée en mode protection de grandes infrastructures au niveau mondial.

TEHTRIS est une société française innovante créée en 2010 par des anciens experts opérationnels du Ministère de la Défense. Avec une récompense internationale de la meilleure solution de cybersurveillance dans sa catégorie, ses consultants apportent une contribution technologique, face aux évènements récurrents de cyber-espionnage et de cyber-sabotage. Son expertise est utilisée par des multinationales et des services étatiques à la recherche de certitudes techniques. Ses activités principales sont les tests d'intrusions avancés, ainsi que la lutte et la surveillance contre les attaques numériques.

La solution logicielle française éditée par TEHTRIS, nommée eGambit assure une surveillance nominale face aux cyber menaces diverses et avancées. L'Intelligence Artificielle embarquée dans la solution eGambit a obtenu une récompense internationale suite à une évaluation de tiers indépendants avec des tests reconnus, remportant ainsi l'Award de la meilleure des solutions dans la catégorie d'analyse des menaces en temps réel et en 2017 elle est la 1e solution française à rejoindre VirusTotal.

TEHTRIS a aussi été décorée du Label France Cybersecurity en 2015, du Trophée de l'Innovation en France au IT Innovation Forum en 2016 et classée parmi les 10 meilleurs solutions EndPoint Security mondiaux en 2017 par une revue américaine. Au niveau du Service Public, eGambit est directement disponible dans le catalogue de la centrale des achats UGAP (Union des Groupements d'Achats Publics).

CONTACT

Clarisse GINET
contact@texplained.com
+33 (0)4 89 68 83 20

Arep Center - 1, traverse des Brucs
06560 Valbonne

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

TEXPLAINED

Texplained est le spécialiste de la sécurité des composants électroniques et propose des solutions et services permettant de lutter contre le piratage et la contrefaçon.

L'entreprise conçoit et commercialise des outils d'évaluation de sécurité et des modules de protection des données :

- OUTIL D'ÉVALUATION : Texplained développe et commercialisera à partir de 2016 son logiciel de rétro-conception de puces électroniques permettant l'exploration et l'analyse de composants de tous types. Cet outil opère la reconstitution de la puce sous différents formats - Netlist, GDSII & fichier VHDL - à partir des images haute résolution de son architecture.
- MODULE DE PROTECTION DES DONNÉES EMBARQUÉES : Texplained a conçu et breveté un module digital détectant à la volée l'extraction de code embarqué et réagissant immédiatement pour stopper l'attaque.

De plus, par le biais des ses formations et prestations d'expertise, Texplained accompagne les fabricants de puces, les intégrateurs et les gouvernements sur l'ensemble du cycle de vie de leurs produits électroniques, de leur conception à leur obsolescence en passant par leur fabrication.
Différents types de prestations sont ainsi proposées :

- Conseil en architecture et design de composants sécurisés
- Audits de sécurité de Circuits Intégrés sécurisés
- Recherche de portes dérobées ou « Hardware Trojan » et autres Backdoor sur des échantillons de puces en bout de chaine de fabrication
- Analyse de devices pirates & support à la mise en oeuvre de contre-mesures aussi bien pour les produits déjà sur le marché que pour les générations de composants en cours de développement
- Etude et comparaison de chips concurrents en cas de suspicion de vol de brevet/Propriété Intellectuelle (IP) et élaboration de rapports techniques pouvant servir de preuve lors d'un procès
- Etude de devices obsolètes et non documentés puis portage des fonctionnalités ainsi reconstituées sur une nouvelle cible

Avec une expertise unique sur la réalité des attaques perpétrées par les pirates, et une approche innovante et efficace, Texplained apporte son expertise sur la sécurité des puces de tous types d'applications : IoT, automobile, médical, bancaire, e-gouv, consumer, militaire…

CONTACT
Didier VIRLOGEUX
didier.virlogeux@thalesgroup.com
0608616733

4, Avenue de Louvresses
92622 Gennevilliers

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

THALES

THALES

Thales est l'un des leaders européens de la cybersécurité et le leader mondial de la protection des données. Fort de 64.000 collaborateurs dans 56 pays, Thales a réalisé en 2016 un chiffre d'affaires de 14,9 milliards d'euros. Avec plus de 25.000 ingénieurs et chercheurs, Thales offre une capacité unique pour créer et déployer des équipements, des systèmes et des services pour répondre aux besoins de sécurité les plus complexes. Son implantation internationale exceptionnelle lui permet d'agir près de ses clients partout dans le monde.

L'expertise Thales au service du cyberespace
Face à l'explosion des cyber-menaces, Thales est le partenaire de confiance naturel des institutions militaires, des organismes gouvernementaux, des opérateurs d'infrastructures vitales et des entreprises industrielles et financières.

Présent sur toute la chaîne de sécurité de l'information, Thales propose une gamme complète de solutions et de services depuis le conseil en sécurité et les audits de sécurité, la protection des données, la gestion de la confiance numérique, la conception, la mise au point, l'intégration, la certification et le maintien en conditions opérationnelles de systèmes cybersécurisés, jusqu'au dépistage des cybermenaces, à la détection d'intrusions et à la supervision de la sécurité (centres opérationnels de sécurité en France, au Royaume-Uni, aux Pays-Bas, au Canada et à Hong Kong).

Choisir Thales, c'est bénéficier :
• D'une équipe de 5.000 ingénieurs en informatique critique, dont 2.000 experts en cybersécurité ;
• D'un partenaire fiable, disposant de plus de 40 ans d'expérience dans la protection d'informations classifiées jusqu'au niveau Secret-Défense ;
• D'un acteur global dont les produits et services sont déployés dans plus de 50 pays ;
• D'un prestataire de services fiable et expérimenté, assurant la gestion et la surveillance des systèmes d'information critiques de plus de 100 clients.

Nous comptons parmi nos clients :
• 19 des 20 plus grandes banques mondiales.
• 4 des 5 plus grandes compagnies pétrolières.
• 27 pays membres de l'OTAN.

CONTACT

Jérôme CHAPPE
jerome.chappe@thegreenbow.com
01 43 12 39 32

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

THE GREENBOW

THEGREENBOW

FRANCE CYBER SECURITY

TheGreenBow est un éditeur français de logiciels de sécurité spécialisé dans la protection des données et des communications.

Les logiciels de sécurité TheGreenBow sont reconnus mondialement pour leur robustesse, leur fiabilité et leur ergonomie. Les solutions TheGreenBow sont dédiées à la sécurisation des communications et des connexions distantes (VPN) ainsi qu'à la protection des données confidentielles (chiffrement d'emails).

Avec plus d'un million et demi de licences distribuées à travers le monde, 70% de son chiffre d'affaires à l'international, une expertise de 20 ans dans la cryptographique appliquée et l'obtention de la Certification Critères Communs EAL3+ et de la qualification standard, TheGreenBow est le fournisseur leader des solutions de confiance adaptées aux PME comme aux Grands Comptes, OIV et Administrations.

Les solutions de sécurité TheGreenBow sont inscrites aux catalogues des produits certifiés OTAN et UE. Ils sont aussi référencés aux catalogues UGAP et Ouranos. TheGreenBow est membre fondateur de HexaTrust, membre du Pôle Systematic, détenteur du Label France CyberSecurity, et collabore au plan CyberSécurité de la Nouvelle France Industrielle.

CONTACT

Jean-Louis GUIDOR
jlguidor@tracip.fr
06 45 47 24 22

6 rue Robert Schuman
54850 Messein

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

TRACIP

TRACIP Technologies & Services d'Investigation

TRACIP est la référence privilégiée des Institutions françaises en matière de Police, de Défense et de Justice dans la lutte contre la cybercriminalité.

Son savoir-faire dans la création de laboratoires d'investigation numérique et de récupération de données sensibles ont permis à TRACIP d'apporter des solutions clés en main incluant audit, équipement, formation et accompagnement aux services de ces entités.

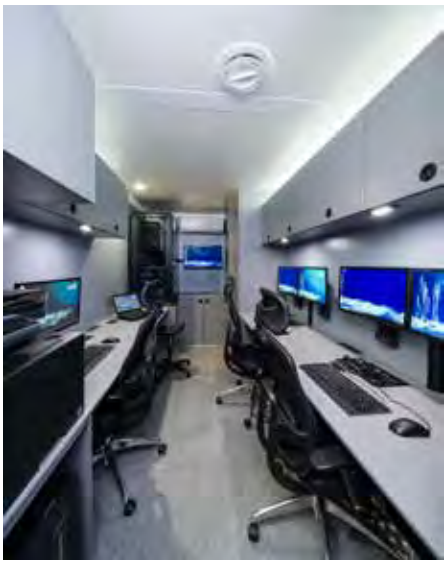
De cette relation étroite et de confiance a émergé, entre autre, le concept de laboratoire mobile, mobil'IT®, qui répond à un besoin opérationnel croissant des enquêteurs cyber.
mobil'IT® est un puissant laboratoire d'investigation numérique, mobile et autonome, qui permet d'accélérer de manière considérable les analyses terrain grâce à un équipement spécialisé, ergonomique et puissant.

De par sa forte expérience dans la conception et la production de laboratoires mobiles, TRACIP a obtenu l'exclusivité pour produire et commercialiser au niveau mondial, un laboratoire mobile ADN, fruit du savoir-faire et de l'innovation de l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN™) et homologué en France par le Comité National de l'ADN.

L'innovation brevetée ayant permis d'aboutir à la création de ce laboratoire offre aux enquêteurs la capacité d'analyser des traces ADN en 2h pour les premiers 21 échantillons, directement sur site, là où une journée est souvent nécessaire, le tout en ressortant 24 marqueurs simultanément. L'analyse est encore accélérée sur les analyses suivantes puisque 21 profils sont ressortis toutes les 30 minutes par la suite.

Les avantages du laboratoire ADN sont nombreux:

- Accélère considérablement le processus de quantification et d'identification des victimes lors d'une catastrophe de masse
- Permet une délivrance rapide du profil ADN d'une personne suspecte
- Limite de manière importante le risque de contamination lors de la manipulation des scellés
- Source d'économie importante avec un coût par analyse significativement réduit



CONTACT

Bernard PROUTS
contact@vocapia.com
+33 (0)1 84 17 01 14

28 rue Jean Rostand
91400 Orsay France

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

VOCAPIA RESEARCH

VOCAPIA research

Making raw audio searchable

Vocapia est une entreprise spécialisée dans le traitement automatique de la parole. Notre suite logicielle, VoxSigma, est dédiée à des utilisateurs professionnels traitant de grandes quantités de données audio.

Les gigantesques volumes de données audio et vidéo multilingues échangées dans le monde numérique d'aujourd'hui nécessitent des outils de plus en plus performants afin d'extraire et d'analyser les informations les plus pertinentes. La suite logicielle VoxSigma couvre la plupart des langues européennes, ainsi que l'arabe, le mandarin, le russe, le pashto, etc. Les systèmes ciblent deux types de données : parole radio/télé diffusée et parole conversationnelle téléphonique. Vocapia fournit des outils de haute performance pour assister les analystes en charge de l'exploitation des données audio dans un cadre judiciaire ou de lutte contre le terrorisme et la criminalité.

Notre vision : faciliter le traitement de grands volumes de données audio multilingues pour les agences gouvernementales dans le cadre du renseignement (OSINT et COMINT).

Analyse de conversations téléphoniques
Les systèmes de reconnaissance automatique de la parole transforment les données audio en documents textuels structurés.

Veille médiatique et indexation audio
Les logiciels VoxSigma permettent aux utilisateurs de traiter et filtrer de grandes quantités d'audio afin d'accéder rapidement aux contenus d'intérêt.

Transcription de la parole
Les systèmes de transcription automatique sont utilisés pour réduire le temps de rédaction des procès verbaux.

Excellence
Forts d'une longue expérience dans la recherche et d'une collaboration proche avec le LIMSI, laboratoire du CNRS, nous concevons des systèmes à la pointe de la technologie, régulièrement classés au meilleur rang mondial.

Une technologie sur mesure
Nous travaillons étroitement avec nos clients afin de leur proposer des systèmes personnalisés et adaptés à leurs applications.

Support rapide et personnalisé
L'assistance aux utilisateurs et aux intégrateurs fait partie intégrante de nos produits et services, pour proposer une solution dans les plus brefs délais.

CONTACT

Edwige BROSSARD
ebrossard@wallix.com
01 53 42 12 81

250 bis Rue du Faubourg Saint Honoré - 75008 Paris
www.wallix.com

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

WALLIX

WALLIX
TRACE, AUDIT & TRUST

Editeur de logiciels de cyber sécurité, WALLIX est le spécialiste Européen de la gouvernance des comptes à privilèges.
Répondant à l'évolution réglementaire récente (NIS/ RGPD en Europe et OIV en France) et aux enjeux de cybersécurité qui touchent l'ensemble des entreprises, le Bastion aide les utilisateurs à protéger leurs actifs informatiques critiques : données, serveurs, terminaux et objets connectés. Cette solution est la première offre du marché certifiée CSPN par l'ANSSI, répondant intégralement à la demande de mise en conformité réglementaire.
WALLIX propose des offres packagées et modulables, s'intégrant facilement dans des environnements techniques existants et évoluant avec les enjeux cybersécurité des entreprises : sécurisez les accès et/ou mots de passe rapidement et faites évoluer la plateforme WALLIX Bastion selon les besoins.
Travailler avec WALLIX et son réseau d'intégrateurs, c'est choisir une démarche projet permettant :

- Une réduction des risques en analysant les comptes à privilèges et les vulnérabilités,
- Une prise de décision accélérée et une détermination rapide des menaces internes et externes potentielles,
- Une approche métier de la gestion des comptes à privilèges selon le secteur d'activité (Santé, Industrie, Gouvernement, Finance…)
- Une solution évoluant avec les architectures techniques (dont la migration vers le Cloud), véritable gain en agilité, productivité et performance.

WALLIX accompagne plus de 540 entreprises et organisations au quotidien dans leur gestion des accès, et le Bastion a été primé aux Computing Security Awards 2016, élu « Best Buy » par SC Magazine et nommé parmi les leaders dans les catégories Produits et Innovation de la gestion des accès à privilèges du Leadership Compass KuppingerCole2017. La société est membre de Bpifrance Excellence, Champion du Pôle Systematic Paris Région et membre fondateur du Groupement Hexatrust. En 2017, WALLIX a été intégré au sein du Futur40, le premier palmarès des sociétés de croissance en Bourse publié par Forbes France.

CONTACT

Sabrina GUIDICELLI
sguidicelli@wooxo.fr
0442016573

TYPE D'OFFRE

POSITIONNEMENT DANS LE CYCLE DE CYBERSÉCURITÉ

NATURE DE L'OFFRE

WOOXO

WOOXO
IT security for business continuity

FRANCE CYBER SECURITY

Editeur français de solutions de protection des données depuis 2011, Wooxo élimine les risques d'interruption d'activité liés à la perte de données informatiques en les sauvegardant contre tous types de sinistres : Physiques, Humains et Cyber.

Wooxo propose une solution complète de reprise d'activité Labellisée France Cybersecurity, du matériel au logiciel, en passant par l'hébergement et le monitoring : un service clé en main à destination des organisations de toute taille en France et en Europe.

Répondant aux plus hautes exigences en matière de sécurité et de confidentialité, nos solutions peuvent héberger des données sensibles comme les données de santé et respectent les conditions du nouveau Règlement Général de la Protection de Données Personnelles.

Les équipes de Wooxo travaillent pour garantir un plan de reprise d'activité efficace, sensibiliser les entreprises aux risques des cyberattaques et rassembler une communauté d'acteurs engagés dans la lutte contre la Cybercriminalité.

Le programme Yoonited Against Cybercrime lancé en 2017 a 3 objectifs :

- Informer et former dirigeants comme les salariés aux bonnes pratiques en matière de sécurité informatique. Ainsi nous diffusons gratuitement des bulletins d'alerte, des livres blancs, des manuels et guides pratiques. Nous organisons également des conférences partout en France pour sensibiliser notre public aux risques cyber.
- Conseiller les chefs d'entreprise grâce à une cellule d'experts en cybersécurité qui propose un audit téléphonique gratuit et personnalisé de leurs installations et les guide vers des solutions concrètes pour protéger leur activité.
- Equiper les TPE/PME avec des solutions adaptées à leurs besoins et effectuer un monitoring pro actif de l'état de leur sauvegarde.

Lauréate de plusieurs distinctions (Les succès du Numérique 2017, Les trophées de la Distribution 2017,...) Wooxo est également membre d'Hexatrust, Cybermalveillance.gouv.fr, Transition numérique et la French Tech.
Une entreprise a impérativement besoin de son système informatique. Le protéger, c'est notre métier.

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME, et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité, de l'identité numérique, des communications sécurisées, de la traçabilité / lutte anti-contrefaçon et de la safe city. 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 environ 850 entreprises réalisant en France près de 9 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (plus de 12% de croissance chaque année depuis 2014). L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) et participe activement à ce titre aux travaux du CoFIS (Comité de filière des Industries de Sécurité). Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).
www.confiance-numerique.fr

La FIEEC rassemble 22 syndicats professionnels dans les secteurs industriels et technologiques de l'électricité, de l'électronique, du numérique et des biens de consommation. Les secteurs qu'elle représente regroupent plus de 3000 entreprises, emploient près de 420 000 salariés et réalisent plus de 98 milliards d'euros de chiffre d'affaires dont 46 % à l'export. A la source et au coeur de la transformation numérique, les groupements membres de la FIEEC rassemblent les entreprises fournissant les technologies et les solutions de sécurité numérique (identité numérique, cybersécurité, traçabilité, sécurité physique/contrôle d'accès, vidéosurveillance,...), ainsi que les entreprises intégrant ces technologies et solutions dans leurs offres « smart » (smart grids, smart industry, smart building, smart city smart health, smart mobility, smart life,...).
www.fieec.fr

Le GICAT, groupement professionnel créé en 1978, compte plus de 200 adhérents qui représentent près de 330 membres, grands groupes, ETI et PME. Ces adhérents couvrent un large spectre d'activités industrielles, de recherche, de services et de conseil au profit des composantes militaires et civiles, nationales et internationales impliquées dans la sécurité et/ ou la défense terrestres ou aéroterrestres. Le GICAT représente les intérêts des industriels français de la Défense et de Sécurité terrestres et aéroterrestres autour de quatre objectifs :

- Organiser le dialogue entre institutionnels et industriels du secteur
- Offrir des services à ses adhérents pour favoriser leur développement en France et à l'international
- Créer un environnement favorable aux échanges entre industriels
- Valoriser les savoir-faire et l'image de l'industrie du secteur.

Le rayonnement international du GICAT s'appuie sur les salons internationaux EUROSATORY en France, APHS à Singapour, Expodefensa en Colombie et ShieldAfrica en Côte d'Ivoire, organisés par sa filiale le COGES, ainsi que sur un certain nombre de salons de défense et/ou de sécurité à l'étranger.
www.gicat.fr

HEXATRUST est née de la volonté commune de PME et ETI françaises, acteurs complémentaires experts de la sécurité des systèmes d'information, de la cybersécurité et de la confiance numérique.
Editeurs et Intégrateurs de solutions innovantes représentatifs de l'excellence française, ils se sont rassemblés pour fournir une gamme de produits et de services performante, cohérente et complète de sécurisation des infrastructures critiques. Cette alliance répond aux besoins des Entreprises, des Administrations et des organisations de toutes tailles, publiques et privées, soucieuses de bénéficier d'offres innovantes d'origine française, couvrant l'ensemble de leurs besoins en matière de sécurité informatique. Forts de leur implantation sur le marché européen, les membres d'HEXATRUST souhaitent également accélérer leur développement international en partageant leur expérience, leurs réseaux et leurs moyens d'accès aux marchés mondiaux.
www.hexatrust.fr

réalisé en lien avec :

Le GICAT et la FIEEC sont membres fondateurs du CICS. Cette plaquette été réalisée dans le cadre des travaux du Conseil des Industriels de la confiance et de la sécurité (CICS). Le CICS rassemble l'industrie de sécurité nationale. Il intervient sur tout le périmètre de la sécurité (équipements et plateformes, systèmes électroniques et numériques, cybersécurité) et a pour vocation de fédérer les positions des groupements de la filière industrielle de sécurité. A travers ses membres (FIEEC, FFMI, GICAN, GICAT, GIFAS, USP Technologies et AN2V), l'association regroupe plus de 80% de l'industrie française de la sécurité.
www.cics-org.fr

Le Comité de la filière industrielle de sécurité (CoFIS) a été mis en place par le Premier ministre en octobre 2013. Il a pour ambition de fédérer les efforts de l'État, des collectivités territoriales, de l'industrie, de la recherche et des grands opérateurs publics et privés, pour développer des solutions de sécurité efficaces et mondialement reconnues. La filière agit au sein d'un marché international très porteur qui couvre des sujets aussi divers que la protection des grandes infrastructures publiques et privées, la sécurité des transports, la gestion des frontières, le secours aux personnes, la lutte contre le terrorisme et la grande criminalité, la gestion de crise ou la cybersécurité. Comme tous les comités de filière soutenus par le gouvernement, le CoFIS vise à développer la compétitivité de nos grands groupes et PME, qui occupent sur le marché de la sécurité une place de premier plan.