CYBERSECURITY

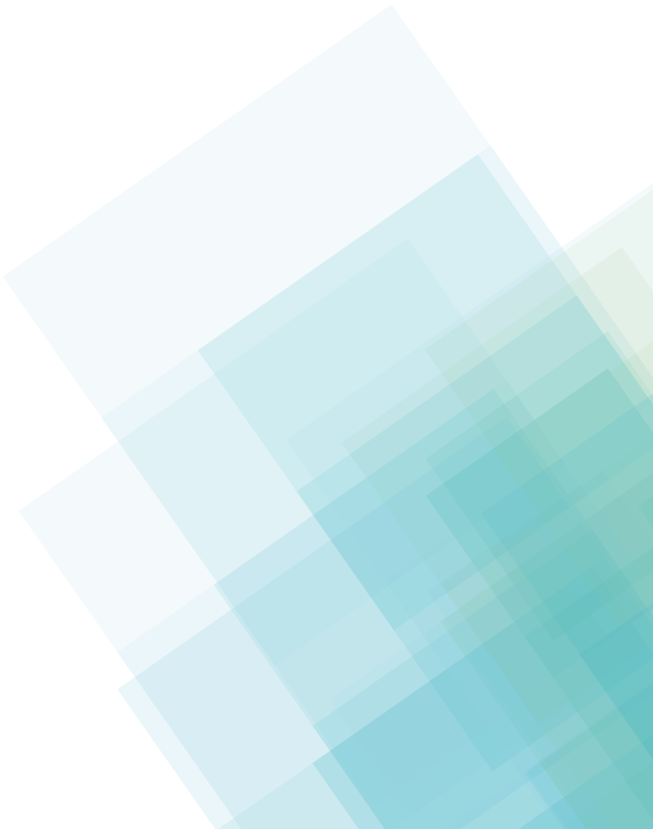
Capability approach

ACN
Alliance pour la Confiance Numérique

FIEEC
FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

GICAT

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY



EDITO

MOUNIR MAHJOUBI,

SECRETARY OF STATE IN CHARGE OF DIGITAL AFFAIRS

Over the past few years, digital technology has become a determining factor in corporate innovation, creating a whole new realm that transcends borders and time zones.
Every single day, as we spend entire swaths of our lives — both physical and virtual — in this realm, the challenge of making it a safe place takes center stage in digital transformation.

The government aims to make this digital realm an area of trust for all citizens and industry players.
However, such trust cannot exist without the commitment of everyone involved, and must reflect our values of freedom, humanism and equality.
France and Europe, sharing this view on digital technology, are currently building a framework specifically adapted to these challenges. Not only does this framework take into account our compatriots' deep interest in privacy issues and the preservation of an open platform fostering innovation while defending net neutrality, it also reflects their desire for technical excellence, which must eventually result in a common European security certification.

Given this context, our solution to this challenge is to construct and develop a dynamic French and European digital security industry.
By focusing on its scientific excellence and web of innovative enterprises ranging from startups to SMEs reputed for the quality of their products and services, which this catalog will showcase, France is poised to become the European leader in digital security.

CYBERSECURITY

Cybersecurity can be defined as the state that information systems should aspire to attain, in which they are able to withstand attempts from cyberspace to compromise the availability, integrity or confidentiality of data (stored, processed or exchanged) and the related services that these systems offer or render accessible.

In an increasingly connected world, cybersecurity is now the core challenge and has become a prerequisite prior to any digital transition.

It covers a very wide spectrum, from national security (defense, homeland security, government administrations, etc.) to vital infrastructures (energy, transport, healthcare, etc.), and the private sector (industries, banks, mobility, businesses, services, etc.), trickling all the way down to individual citizens.

Regardless of whether their motivations are financial, ideological, strategic or geopolitical, cyberattacks now no longer discriminate — as long as it is online, it is fair game, and with graver consequences.

This calls for greater collective awareness: trust is a major building block in developing digital technology and delivering on all the promises that connectivity has made possible. But it can only be built when digital security (security by design) and personal data protection (privacy by design) are integrated into products and solutions when they are still in the design phase.

Users have access to varied expertise and numerous tools to counter these challenges, and this brochure aims to guide them through this process.

IN FRANCE: A DYNAMIC INDUSTRY DEDICATED TO DIGITAL TRUST

Both in cybersecurity as well as in digital trust, France relies on a network of reputable laboratories and an association of businesses with a wide range of skills. Made up of agile and dynamic large corporations and SMEs, this partnership offers a full array of extremely precious skills that have allowed our country to feature among the leading names in these strategic fields.

The cybersecurity

CYBERSECURITY CONSULTANCY

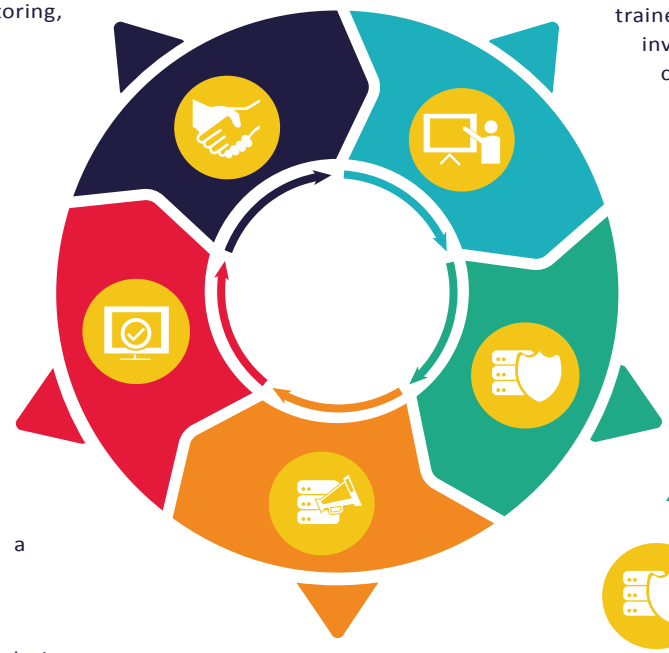
The «cybersecurity consultancy» segment makes it possible to rely on specialized external expertise to better understand the security of information systems.

All organizations need to secure and maintain the security of their information systems.
Due to the complexity and diversity of interconnected systems and technologies, securing an information system requires experts both in information system security and in each technique used in handling information.
These specialists are uniquely qualified to provide relevant, high-level services in governance, monitoring, design/integration

EDUCATION - AWARENESS

The «Education-awareness» segment is an indispensable component in securing an information system.

As each link in the chain of an information system contributes to its security, cybersecurity training is an absolute necessity in order to guarantee the security of the entire system. Such training applies to all employees of a company (directors, management, technicians, employees, etc) and must be adapted to their knowledge and level of technical savvy. From raising awareness of the basic rules of healthy user habits, to the most specialized technical training, or managers being trained to recognize the stakes involved and how to manage cyber incidents; every level of the organization must be trained in order to achieve effective cybersecurity.



INVESTIGATION RESILIENCE- INTELLIGENCE

The "Investigation and Resilience" segment is involved in the aftermath an incident.

The goals of phase are to:
• analyze the incident in order to prevent it from reoccurring
• gather evidence in the event of a malicious act
• enable service continuity

This segment groups all products and solutions that make it possible to minimize the damage caused by incidents and accidents, analyze the facts and where possible, revert to the initial state.

PREVENTION PROTECTION

The «Prevention and Protection» segment acts ahead of an incident and stays relevant throughout the lifetime of the system.

Its role includes:
• the anticipation of threats and vulnerabilities and deducing the potential risks
• the definition of architectures and procedures
• the installation, configuration and maintenance of resources.

This segment involves all products and solutions that allow incidents and accidents to be detected and blocked on an infrastructure.

DETECTION-REACTION

The «Detection and Reaction» segment makes it possible to detect and contain attacks.

The aim here is to:
• detect incidents and accidents
• collect information on traffic and behavior on systems, and analyze such information in order to detect incidents if they had not been reported earlier
• induce the appropriate responses in order to confine such incidents

This segment involves all products and solutions that allow incidents and accidents to be detected and blocked on an infrastructure.

How should this guide be read?

This guide aims to address the queries of organizations contemplating cybersecurity and in search of solutions catering to their needs. To provide readers with the most clarity, solutions have been classified under three main criteria.

The main criterion chosen for the presentation of this guide is the category of the solution (see the 11 categories chosen below).

Categories of cybersecurity solutions

GOVERNANCE, TRACEABILITY AND AUDIT

Security Information and Event Management (SIEM), tracking and management systems

IDENTITY AND ACCESS MANAGEMENT

Access control, identification, authentication and biometric systems

DATA SECURITY AND ENCRYPTION

Data encryption, signature, key management infrastructure (KMI), secure archiving, Digital Rights Management (DRM)

E-MAIL SECURITY

Antispam, mail encryption, secure messaging

APPLICATION SECURITY

Development and application security, testing and modeling

PROTECTION OF MOBILE AND WEB TRAFFIC

Content filtering, application filtering, secure communications

INFRASTRUCTURE AND DEVICE SECURITY

Firewalls, antivirus, anti-DoS, Intrusion Detection Systems (IPS/IDS), Web Application Firewall (WAF), network encryption hardware, Hardware Security Module (HSM)

INDUSTRIAL NETWORK SECURITY

Security and monitoring of industrial networks, device partitioning

AUDIT, CONSULTANCY AND TRAINING

Audit, vulnerability and intrusion testing, risk and threat management, forensics

MANAGED SERVICES AND OPERATIONS

Operations support, Managed Security Service Provider (MSSP), business continuity management, trusted third party

INTELLIGENCE

Collection, processing and analysis of the data mass in cyberspace to deduce relevant information from it

The cybersecurity cycle

CYBERSECURITY
CONSULTANCY

EDUCATION
AWARENESS

PREVENTION
PROTECTION

DETECTION
REACTION

INVESTIGATION
RESILIENCE-INTELLIGENCE

To enrich this approach, we also wished to introduce a second criterion — where the solution stands in the cybersecurity time line, according to its relevance before, during or after a potential incident (see page 5).

Type of solution

We also wished to introduce the concept of the type of solution in order to show the reader whether the solution is a turnkey product or program, a service to integrate a product or program, or a consultancy service.

In the following pages, you will see two tables providing a brief presentation of all the solutions. They will allow you to cross-reference these criteria in pairs, providing you with a dynamic view based on the most relevant criteria. These tables will redirect you to the following pages of this guide, which give detailed descriptions of the solutions offered (part 2) as well as general presentations of the companies offering them (part 3).

PRODUCT/SOFTWARE

SERVICE

CONSULTANCY

Key figures

Digital trust in France in 2016

9 bn €

revenue

60 000

jobs

50% Cybersecurity

50% Digital Security

A sector in full expansion

12,4%

Average yearly growth of the sector from 2014 to 2017

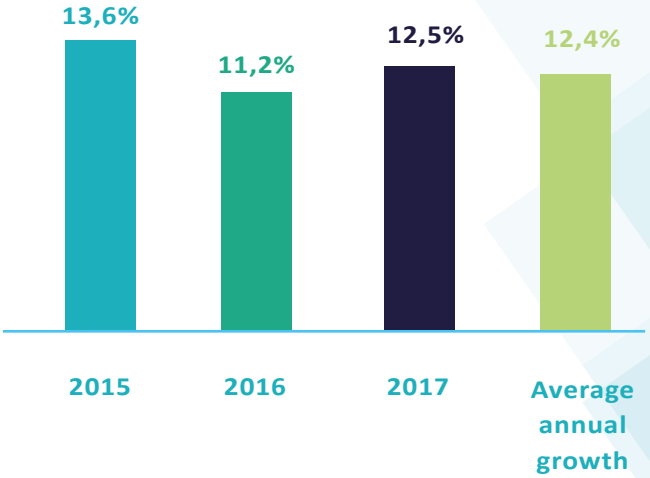
1,1%

Average yearly growth in GDP from 2014 to 2017

12,5%

forecast growth in 2017

Weighted average growth in revenue from digital trust companies in France

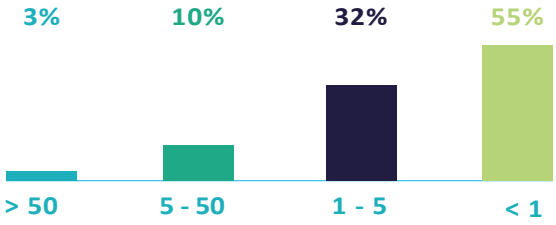


A vibrant network of companies

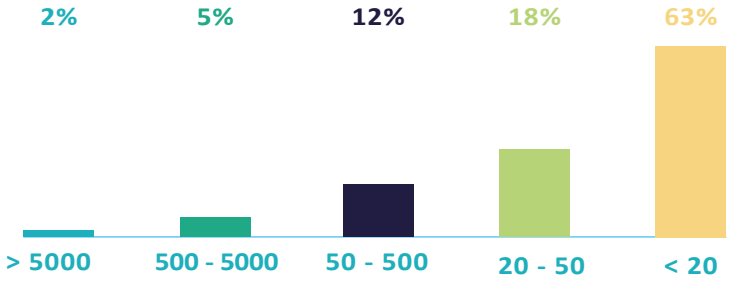
13%
of companies in the sector have revenue of **+5 bn €**

81%
of companies in the sector have fewer than **50 employees**

Companies by revenue
in millions of Euros

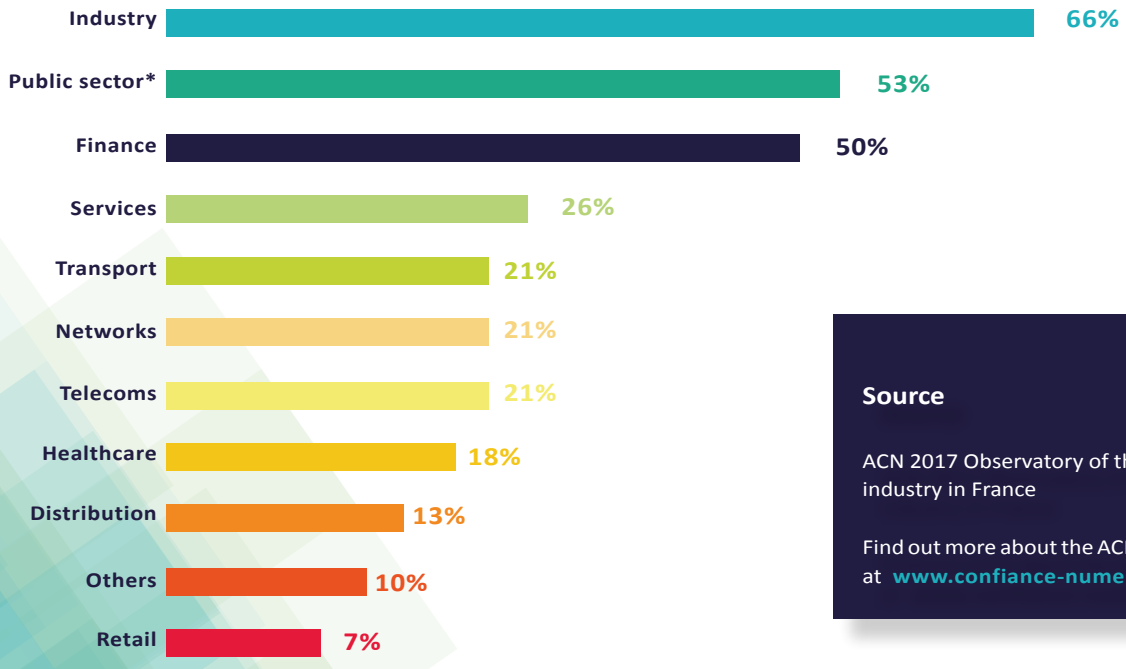


Companies by employees
number of persons



Dynamic market positioning

Presence of companies in client sectors
(% of companies)



Source

ACN 2017 Observatory of the digital trust industry in France

Find out more about the ACN Observatory at **www.confiance-numerique.fr**

* government, security forces, safe city, local authorities, excluding healthcare and transport Source : DECISION

product/software

service

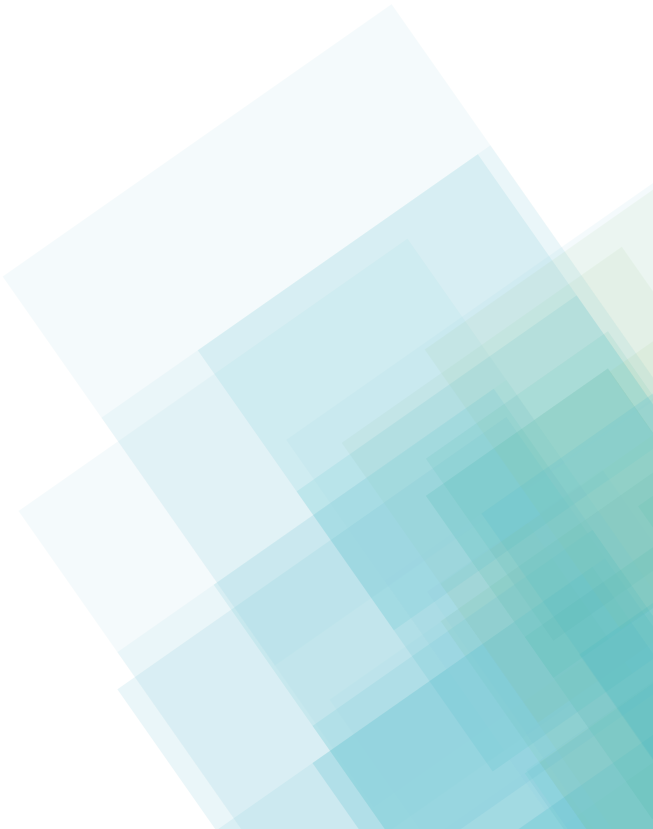
consultancy

	GOVERNANCE, TRACEABILITY AND AUDIT	IDENTITY AND ACCESS MANAGEMENT	DATA SECURITY AND ENCRYPTION	E-MAIL SECURITY	APPLICATION SECURITY	PROTECTION OF MOBILE AND WEB TRAFFIC	INFRASTRUCTURE AND DEVICE SECURITY	INDUSTRIAL NETWORK SECURITY	AUDIT, CONSULTANCY AND TRAINING	MANAGED SERVICES AND OPERATIONS	INTELLIGENCE
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	
STMICROELECTRONICS							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								

	CYBERSECURITY CONSULTANCY	EDUCATION AWARENESS	PREVENTION PROTECTION	DETECTION REACTION	INVESTIGATION RÉSILIENCE- INTELLIGENCE
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					
STMICROELECTRONICS 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					

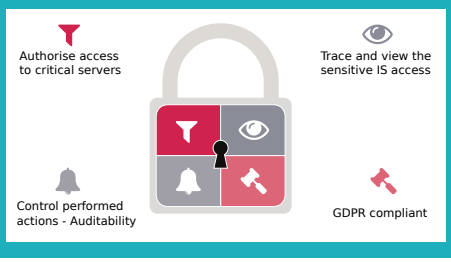


CAPABILITY OFFERS

PRACTICAL SEGMENTATION

GOVERNANCE, TRACEABILITY AND AUDIT

RUBYCAT



PROVE IT

The French software solution PROVE IT from RUBYCAT-Labs hardens the security of sensitive access to your Information System by including the traceability and monitoring of users with privileges (third party management, access control, etc.). You know who, when and how a user has connected to your servers and you can see all actions they performed in real time. Sessions can be saved for later review.

PROVE IT controls, monitors, traces and records the progress of sensitive connections for immediate or delayed viewing (advanced auditing tool).

The new version includes major new features including a native module for enhanced protection of user account credentials with sensitive access.

SOPRA STERIA

SECURE SUSTAINABILITY, DETECTION AND RESPONSE

With a global network of 700 cybersecurity experts recognised by benchmark certifications, our consulting strength relies on a first-class technologic and industrial know-how. Our consultants business and technical expertise enables Sopra Steria's to be a global cybersecurity partner and a reference for cyber trusted operators to fully protect major institutional and economic players' sensitive systems and data with tailored cyber security solutions.

Sopra Steria is fully qualified with regards to the security standards and best practices established by ANSSI, the French National Agency for the Security of Information Systems.

IDENTITY AND ACCESS MANAGEMENT

CERTINOMIS

PKI AS A SERVICE

Certinomis Corporate is a Public Key Infrastructure (PKI) supplied as a service. It enables deploying and managing digital certificates in an organisation by using mutualised competences and resources, thanks to externalisation.

A CUSTOMISED SERVICE

This solution is modular by design: three separate applications deal together, in TLS mode bi-authenticated by digital certificates, to perform the different steps of certificates' lifecycle management.
It means that a client can decide precisely which functions would be performed internally and which ones would be delegated.
Certinomis Corporate offers a wide range of possibilities from complete externalisation, with only variables costs based on volumes of certificates produced, to complete internalisation, with also a progressive integration in its information system of each component.

EVIDIAN

Bull Evidian

WEB ACCESS MANAGER (WAM)

The Bull Evidian Web Access Manager (WAM) is an identity provider, it federates access to web apps supporting SAMLv2, OpenId Connect, WS-Fed protocols. It is also an SSO Web Service Provider for web apps (internal, external, cloud). It secures mobile user access and replaces passwords with a single, strong authentication mode that can be used from PCs, tablets, and other unmanaged devices. Authentication can rely on the France Connect identity provider.

Bull Evidian WAM supports various methods ranging from simple login / password to multi-factor authentication and can use its authentication services, those of a partner's server or SaaS authentication. WAM manages access to Office 365 Web apps.

EVIDIAN

Bull Evidian

IDENTITY SOLUTION, GOVERNANCE & ADMINISTRATION (IGA),

The Bull Evidian Identity solution, Governance & Administration (IGA), identifies and manages the users authorized to access the information system. It defines and updates users' rights, and manages their evolution over time according to a security policy based on roles, organizations, contexts and business rules. The solution relies on business workflow processes for rights administration, provisioning, updating resource access in the enterprise or in the cloud, and for re-certification through regular compliance reviews.

EVIDIAN

Bull Evidian

ENTERPRISE SINGLE SIGN-ON (E-SSO)

Bull Evidian Enterprise Single Sign-On (E-SSO) manages access to enterprise applications and frees the user of their passwords and also allows them to be changed automatically. The SSO can be secured with strong authentication, it offers kiosk mode support for secure sharing of a workstation by multiple users as well as single-sign on to open or lock multiple workstations by user authentication. These mechanisms are frequently used for regulatory compliance reasons.

IDNOMIC

CORPORATE ID

Corporate ID is an open, modular solution designed to create, issue and manage the digital identities of users and devices within a trusted infrastructure.

Corporate ID is based on the following functions:

- Credential Management System: Comprehensive software for the management of digital certificates bearers lifecycle.
- Mobile Guard: Enables companies to extend their security best practices to mobiles and tablets.
- Virtual Guard: Solution that complements the management of digital identities on smart cards and mobile devices by using the Trusted Platform Module (TPM).

IDNOMIC

CITIZEN ID

Solution for the management of the digital identities for citizens. As a technology partner, IDnomic offers solutions for all governments, ministries, agencies and system integrators to ensure maximal security to citizens when they travel or use online services:

- Non-falsifiable electronic proof of identity (passport, visa, drivers license, etc.).
- Access to and controlled reading of sensitive biometric data stored in secure ID documents.

ILEX INTERNATIONAL

ILEX IAM

Ilex International's software offering covers identity and access rights management, user account provisioning, strong and adaptive authentication, access control, SSO and identity federation whatever the use, environment, or type of applications to protect.

Ilex's offer is based on two software suites:

- **Ilex Identity software suite**: identity and authorisation management solutions that match the needs of an organisation according to its size, industry sector and security requirements.

- **Ilex Access software suite**: a comprehensive and modular access management solution allowing you to address strong authentication, WAM, Identity Federation, eSSO and Mobile SSO issues.

SURYS

SURYS

PHOTOMETRIX™ VERS UNE IDENTITÉ DÉMATÉRIALISÉE

Photometrix™ is an optimal hybrid solution to the virtual identity, an innovative mix between a picture and a 2D barcode which allows an offline automated authentication of the card holder's portrait. The Photometrix™ code is generated thanks to an encoding mechanism based on specific characteristics of the picture, some personal details (name, date of birth, etc..) as well as biometric information. The Photometrix™ acts as a secured access to the digital world opening a door to its myriad of opportunities.
The control is performed via a digital support (Smartphone, Tablet, etc..) both on physical and dematerialized document.

SYSTANCIA

Systancia

IPDIVA SECURE

IPdiva Secure is a French cybersecurity solution that provides secured access to selected resources of the IT system for any type of users (roaming users, homeworkers, third party contractors, etc.). With a unique access architecture not requiring any port opening on the IT system, IPdiva Secure provides advanced features in terms of robust security of mobile devices, strong authentication, compliance and integrity monitoring. IPdiva Secure includes a Security Center that allows administrators to verify compliance with best practices at a glance, highlighting any disparity.

IPdiva Secure is the only one solution to have obtained the ANSSI Qualification-Elementary level in the technical domain of identification, authentication and access control.

SYSTANCIA

Systancia

IPDIVA SAFE

IPdiva Safe, is a privileged access management (PAM) solution that enables the video recording of privileged-user sessions, offering advanced real-time analysis capabilities for detecting abnormal or suspicious behaviour, as well as cyberthreats, as of the very first intrusion attempt. IPdiva Safe's intelligent engine also enables the automating of protective actions that stop malicious users.

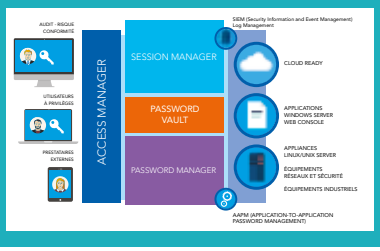
A packaged solution that is very fast to deploy, IPdiva Safe is based on the IPdiva Secure engine, which has obtained ANSSI's CSPN certification and Qualification-Elementary level.

SYSTANCIA

AVENCIS SSOX

Avencis SSOX, a France Cybersecurity labelled solution, is a solution for access control and unified strong authentication (SSO) which guarantees the security of connections while also improving user experience. Avencis SSOX enables more robust primary authentication by offering multi-factor authentication features supporting multiple authentication methods (card, biometric, NFC, etc.) and integrating an OTP module. Avencis SSOX provides advanced features in terms of Out Of Band authentication, password safe, identity aggregation and all access traceability.

WALLIX



WALLIX BASTION

WALLIX Bastion is a Privileged Access Management (PAM) software platform which plays a critical role in the implementation of preventative measures and strengthening of security, via:

- Session Manager: Control access and monitor privileged user sessions, trace all activity, and generate complete audit reports
- Password Manager & Password security

In preventing direct connection to IT infrastructures, WALLIX Bastion protects companies' strategic assets and responds to the "privacy by design" challenges of digital transformation. The Bastion prevents data breaches and ensures rapid compliance with regulations (e.g. GDPR, NIS, LPM, etc.)

WALLIX

BASTION SESSION MANAGER

Privileged accounts are clear targets for hackers aiming to access companies' data and strategic systems. The Bastion Session Manager enables you to monitor all privileged account activity:

- Establish your defense: Implement security policies and authorization practices
- Organize oversight: Complete surveillance and session analysis
- Cut short any malicious attempts with real-time alerts

Bastion Session Manager delivers essential visibility of all privileged account activity (who did what, and when). Fast and simple to deploy, Session Manager easily integrates into the complete WALLIX Bastion platform.

WALLIX

BASTION PASSWORD MANAGER

The Bastion Password Manager strengthens privileged account password security. Whether for an internal or external user, it stores and secures login credentials and simplifies the management of user access permissions:

- Store and secure passwords
- Manage password rotation
- Eliminate application passwords and scripts
- Renew and restart critical service accounts

The Bastion Password Manager allows you to limit potential attack exposure by managing password sharing and privileged user credentials. Fast and simple to deploy, Password Manager easily integrates into the complete WALLIX Bastion platform.

ATT

SEALCRYPT® LARGE-CAPACITY CODE

SealCrypt is a range of 2D codes storing large amounts of offline checkable data, and signed with asymmetric keys. SealCrypt thus guarantees the origin of its emission and the integrity of its contents.

Displayed on tablet, smartphone or physical document, SealCrypt can contain sensitive information, including a photograph.

SealCrypt is also the first secure, biometric storage, offline-verifiable solution, without the use of a chip.

DATA SECURITY AND ENCRYPTION

AIRBUS CYBERSECURITY

ORION MALWARE

Orion Malware is a platform for detection and analysis of malicious codes capable of processing thousands of files and creating detection on new threats. Combining techniques of sorting, static analysis, dynamic analysis and machine learning, Orion Malware is an important collaborative tool for the coordination of SOC teams, incident response and threat intelligence, allowing saving time in investigation.

Orion Malware is offered as an appliance with a full range or in cloud mode via the Check My File portal.

The product brings the latest malicious code analysis techniques and detection rule sets updated regularly by the Cyber Threat Intelligence teams of Airbus Cybersecurity.

ATEMPO

DIGITAL ARCHIVE

Backup, migration and archiving solution for very large data sets

To manage massive data growth and provide long-term data retention, companies need a secure, centrally managed backup and archiving solution.

Atempo-Digital Archive is a complete unstructured data backup and archiving solution enabling users to manually or automatically transfer fixed-content data from one storage location to another. Atempo-Digital Archive indexes all your data sets and enables you to recover historical versions.

DATASHUSH TECHNOLOGY

LOCKEMAIL

A brand new French Tool to protect emails and sensitive data.
Today cyber threats are real, external and internal spying a reality, in addition with new réglementations rules. Companies are forced to protect themselves.
LockEmail is a solution simple to use and install, efficient and secure to protect emails exchanges without changing the usual mailboxes.
All the emails are not protectable but some exchanges need to be protected to stay secret.
Our products are available for MAC, Linux and Windows.
A premium product edited hand to hand with MDK Solution is an encrypted key with our product onboard : Cryptkeymail.
LockEMail.com is an end to end asymetric solution software based on GPG, a mature and proved technology. The encryption range is 4096 bits.
Only the receiver is able to read the message and their attachment.
We protect your sensitive, confidential and private emails.

ATOS

Bull Horus

IOT SECURITY

Bull Horus is the Atos IoT Security suite, a third party solution for the IoE and IoT security. With Bull Horus, the business value of IoT is secured by implementing and managing sustainable long-term security models, crafted to industry sectors. Its solutions and technologies ensure the security of IoT on every level from embedded security (trusted secure element solution – CardOS) to secure communications and objects identity management (trust infrastructure and hardware security modules). Bull Horus also enables decentralized trust between partners with high-security **blockchain** consortiums. Atos is a member of the LoRa Alliance and guarantees IoT communications integrity with the LoRaWAN protocol.

ATOS

Atos

CYBERSECURITY SERVICES

With 4500 cybersecurity experts, Atos delivers end-to-end services from consulting to provisioning remote managed security in order to define and apply an adequate prevention and protection strategy.

Atos supports you in setting up your strategy of cybersecurity, the measurement and monitoring of your cyber risks as well as compliance regulations such as **GDPR** (General Data Protection Regulation), NIS directives, PSD2 etc.

Atos also developed the new generation of SOC (Security Operations Center): **Prescriptive SOC** leverages big data, machine learning and advanced threat intelligence to anticipate and neutralize cyber-attacks.

ATOS

Bull Trustway

DATA PROTECTION

Data protection: **Bull Trustway** is one of Europe's leading data encryption specialists, to ensure the protection of sensitive data and networks against cyber-attacks.

Its product range: Hardware Security Module (HSM), IPsec network encryption and secure storage, has many approvals and certifications in compliance with the new regulations, including GDPR, the General Data Protection Regulation.

Its **Bull Trustway DataProtect solution** provides to customers a centralized key management and encryption solution for all data formats such as virtual machines, databases, files, applications and tokenisation, in the cloud and on-premises.

BERTIN IT

CROSSING®

Bertin IT's CrossinG® secure gateway is designed for sensitive infrastructure. It secures and monitors exchanges of information between networks belonging to separate domains or with different levels of confidentiality. It neutralises attacks on sensitive or remote systems by controlling incoming and outgoing data. Finally, it prevents data in an information system from being extracted via the network.

DENYALL

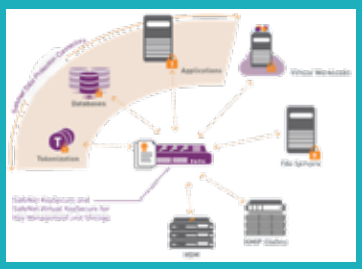
ETHERNET ENCRYPTOR

Protect companies and organizations against espionage and manipulation of data that is transported via Ethernet over landline, radio relay or satellite links.

- Encryption based on port, VLAN or group assignment (multipoint)
- Protect organizations against espionage and the manipulation of data
- Ethernet encryptors for bandwidths from 25 Mbit/s to 40 Gbit/s
- Approved by the German Federal Office for Information Security (BSI) up to the German restricted (VS-NfD) and NATO restricted classification levels

GEMALTO

SAFENET KEYSECURE™



Centrally manage your encryption keys and ultimately own your data with SafeNet KeySecure, the industry leading enterprise key management platform with flexible options spanning FIPS 140-2 Level 3 or 1 validated hardware appliances and hardened virtual appliances.

SafeNet KeySecure offers customers a complete key management and data encryption platform with SafeNet Crypto Pack – a simple licensing option that transforms your key management appliance into a server that includes support for the Gemalto encryption connectors:

- SafeNet ProtectApp (Application-level)
- SafeNet ProtectDB (Column-level database)
- SafeNet ProtectFile (File system-level)
- SafeNet Tokenization (Application-level tokenization)
- SafeNet ProtectV (Full disk virtual machine)

IDNOMIC

OBJECT ID

Object ID is a solution that manages the digital identities of connected objects guaranteeing integrity and confidentiality of sensitive information. The solution combines PKI software and services for the protection of digital identities of objects and their environments.

Usage of Object ID solution are multiple:

- Intelligent Transport System
- Sensor and/or medical equipment authentication
- Smart cities resources optimization
- Network components authentication

MAXIM INTEGRATED

SECURE MICROCONTROLLERS

Maxim Integrated offers a complete panel based on the core Arm® Cortex M. Key protection and core flexibility allow to combine secure storage functions and the support of many cryptographic algorithms (AES, RSA, ECDSA, SHA-x). We also offer a secure element : MAXQ1061. Maxim Integrated has here developed a firmware enabling key secure storage and offering common functions to secure embedded systems as electronic signature or encryption.

Beyond payment terminals, our microcontrollers aim applications as network gateways, programmable logic controllers, decoders etc. They're perfect and complete solutions to secure network, applications, identity management, flow, infrastructures and industrial equipments.

PRIM'X

ZONECENTRAL + ZONEPOINT + ORIZON

ZoneCentral, ZonePoint and Orizon are based on proven security concepts: no passing of documents in the clear (i.e. not encrypted) on servers, no keys stored in the information system, no keys passing via the network, all encryption operations carried out on the terminal (work post, mobile, etc.) with the user key.
ZoneCentral provides files and folders encryption: user workspace, file servers, shares, USB devices, etc.
ZoneCentral cooperates with ZonePoint, Documents encryption for Microsoft SharePoint® libraries and Orizon enables files and folders encryption for Cloud spaces (OneDrive, Dropbox, etc.), to manage NEED TO KNOW for all data at rest of an organisation.

DATA SECURITY AND ENCRYPTION

PRIM'X

CRYHOD

Encryption of laptop computer disks with pre-boot authentication.

For a company, the damages associated with the theft or loss of a laptop amount to far more than just the value of the hardware. Losing the information stored on a laptop's hard disk or the mere communication of that information to a third party can generate all sorts of serious problems: recovery of sensitive information by the competition, damage to brand image, etc., to say nothing of the possible legal and regulatory implications in the event of a breach or an offence.
The Cryhod hard disk encryption solution from Prim'X shields your company from these risks.

STORMSHIELD

STORMSHIELD DATA SECURITY (SDS)

The Stormshield Data Security (SDS) solution guarantees the confidentiality of sensitive data and prevents the leakage of information on all types of media: files, e-mails, virtual disks, Cloud applications such as Office365, and more. It gives users the ability to work with internal and external collaborators securely through encryption. The Cloud & Mobility option preserves the confidentiality of data stored and shared in the Cloud. Confidential data can be accessed from a workstation running on Windows or Mac OSX or from a mobile device (iOS or Android).

SURYS

LE CODE PHOTOMETRIX™

Photometrix™ is an hybrid solution to the virtual identity , done thanks to an encoding mechanism based on special characteristics of the picture and personal details (name, date of birth, etc..) and biometric information. These elements are then compressed to represent only few bytes of information and optimize the space required on the document.

The whole data is then signed using an Asymmetric Cryptographic Signature Algorithm (Elliptic Curve DSA 512bits), in order to prove that the information has been issued by a trusted source. This mechanism guarantees the authenticity of the information with a governmental level of security.

THEGREENBOW

THEGREENBOW VPN CLIENT SOFTWARE *Trusted Secure Connection*

TheGreenBow VPN Client is the first software which enables universal secure connections. Compatible with any IPsec or SSL VPN gateway and compatible with all PKI, it supports various authentication methods like tokens, smartcards, OTP, etc.Easy to deploy into any infrastructure, **TheGreenBow VPN Client** enables to quickly offer all employees a secure connection to the company's Information System.
TheGreenBow VPN Client is available for all devices : Windows, Android, macOS, iOS and Linux. It allows to establish VPN tunnels over all type of network ; 3G, 4G, Wi-Fi, Satellite, etc.
TheGreenBow VPN Client is the unique VPN solution for trusted secure connections, certified CC EAL3+ and qualified for NATO and EU restricted use.

TRACIP

DIGITAL DATA PROCESSING SPECIALIST

TRACIP is a french company that pioneered Data Recovery and Computer Forensics Services in France. Working daily on cases, TRACIP is the leading French Data Recovery & Digital Investigation Laboratory and a leading provider in Consulting, Equipment & Training for Corporations and Government Agencies.

We offer services, equipment and training to Law Enforcement Agencies and Corporations, including:

- Creation of Customized Turnkey Digital Forensic and Data Recovery Laboratories
- DNA mobile laboratory, result of the know-how of the Forensic Research Institute of the National Gendarmerie (IRCGN™)
- Data Recovery, Computer Forensic and Cybersecurity Trainings
- -mobil'IT: TRACIP is the designer and manufacturer of the first forensic mobile laboratory with Data Recovery and Digital Forensic capabilities built for field investigation

WOOXO

ALLROAD BOX PACKAGE

Wooxo offers a full backup and recovery service for professional digital assets. In case of data loss due to cyberattack, fire, flood, theft – your data, softwares and servers are protected and you can quickly restart your activity when needed.

Our "Ready-to-go" package is 100% Made In France and includes: Local storage (Highly Secured Box and encryption of files), Cloud storage (French Datacenters), YooBackup "France Cybersecurity" labelled software, installation and settings, hardware and software monitoring as well as technical support.

E-MAIL SECURITY

ICODIA

ICOCERBERUS.MEL

The hypercube DSS e-mail security solution, able to block unknown malware without relying on signatures.
Icodia's R&D division has developed an antivirus and antispam decision-making filtering platform.
It uses hypercube technologies (OLAP) in order to extract and model threats.
Thanks to its artificial intelligence, decision-making algorithms and machine-learning, it has several levels of response.
It learns by itself (with reverse-engineering, steganography, sandbox), creates new fingerprints and signatures, identifies dubious behavior.
Your organization is protected from cyber threats.
Hosted in Brittany in a secure datacenter, it operates in SaaS.
IcoCerberus.Mel has been awarded the France Cybersecurity label in 2017.

PRIM'X

ZED! ET ZEDMAIL

Encryption of e-mails and encrypted containers for exchanges and archiving.
Zed! allows the creation of encrypted containers to protect files during transport regardless of the channel used (e-mail, removable device, file-transfer, etc.) A .zed container can be compared with a 'diplomatic bag', containing sensitive files that only the identified recipients have the right to read.
ZedMail, integrated with Outlook®, is used to create and automatically read .zed containers from the inbox like any other e-mail. The messages are transferred encrypted on the network and within the company's message server.
A free multi-platform (Windows, Linux, macOS, iOS, and Android) application is available.

APPLICATION SECURITY

ATEMPO

TIME NAVIGATOR

A backup and recovery solution for enterprises which is straightforward to use and fully scalable for all physical and virtual environments.

Atempo's Time Navigator's unique recovery approach with its interface based on its Time Navigation feature. Whatever your platform, your data is restored in 3 clicks including deleted files. **Time Navigator** protects Windows, macOS, Linux and major Unix versions. It proposes hot backup and recovery for databases, mail servers and ERPs. Supports numerous storage architectures such as SAN, NAS, tape libraries, VTL and deduplication storage. Atempo Time Navigator is scalable, combining protection of a simple workgroup to over thousands of enterprise servers. The solution is capable of protecting petabytes of critical data.

DENYALL

VULNERABILITY MANAGER

Proactively detect IT vulnerabilities to monitor your security posture and minimize your attack surface.

- Comprehensive view of all IT vulnerabilities attached to network devices, operating systems, databases and applications.
- Dashboard to report on compliance with regulations and corporate policy and measure progress over time
- Executive and detailed reports with customizable templates for actionable decisions.

DENYALL

WEB APPLICATION FIREWALL

Protect your website, applications and web services from the vulnerabilities of the OWASP top 10.

- Time-tested security, effective against known and unknown attacks
- The ability to combine negative & positive security with user context (time, location, device, etc)
- A productive environment which lets administrators manage policy and optimize data flows visually using a proven workflow approach
- The ability to profile web applications and learn how they work
- The option to replay logged traffic to tune policy, perform forensics analysis
- Virtual patching with DenyAll Vulnerability Manager and 3rd party vendors
- APIs to industrialize deployments

SOPRA STERIA

SOFTWARE DEVELOPMENT GARANTEES

With a recognised expertise across all security-related areas, Sopra Steria is first-class partner to large organisations and companies.

The group offers its clients a highly regarded know-how with fully integrated and confident solutions enabling protection of sensitive information and thus facilitating its clients' digital transformation activities.

Sopra Steria offers broad technical tools in line with specific processes such as design, implementation and operation of Identity and access management (IAM), Public key infrastructure (PKI) and protection against data leakage (via the implementation of DLP and encryption technologies).

PROTECTION OF MOBILE AND WEB TRAFFIC

ATEMPO

LIVE NAVIGATOR

A transparent continuous data protection solution for workstations, laptops and file servers capable of restoring complete machines (system, applications, data) or individual files according to your needs.

Atempo's **Live Navigator** offers users full autonomy to browse file versions to restore the data they need. With built-in powerful source-based and target-based deduplication for endpoint machines and file servers. Live Navigator only sends new and unique data blocks meaning big savings on storage costs. Full multi-site replication is part of Live Navigator's feature set enabling high-speed local recovery with centralized administration.

In the event of losing or damaging your laptop, files can be restored from any web navigator from anywhere in the world. Live Navigator can save the day by recovering your PowerPoint presentation a few minutes just before that key meeting.

CERTINOMIS

SERVER CERTIFICATES

Server certificates guarantee that a software application is operated under the responsibility of an identified organisation.

THREE CATEGORIES :

•Server certificates authenticate software application acting as a server in a client-server exchange, for instance a web site.

•Client certificates authenticate software application acting as a client in a client-server exchange.

•E-Seal certificates make it possible for a software application to seal data, in order to guarantee their origin and their integrity (for instance bills, salary roles etc.).

A MULTIPLE-REFERED OFFER

Certinomis has its own Root Certification Authority that is referenced and qualified in accordance with several requirements grid: French public referee for information safety (RGS), European standards (ETSI 319 411-1 &2), European TLS qualified certificates (eIDAS), referee for TLS server (CAB/F).

Certinomis can thus covered any need of its clients for securing their electronic exchanges.

ICODIA

ICOCERBERUS.WEB

IcoCerberus.Web is an application filtering solution (WAF) with a decision analysis system that blocks threats in real time.

The security of information systems is vital. Evolution of uses must be accompanied by maximum protection, and should not paralyze the activity.

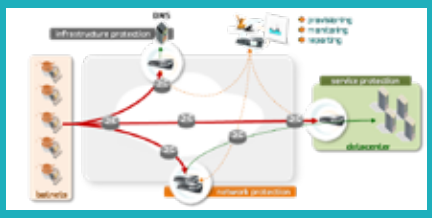
Icodia's R&D team has developed an analytical platform that filters HTTP and HTTPS requests to ensure access for legitimate visitors. Real-time analysis makes it possible to dynamically apply countermeasures. Your applications are protected against cyber threats.

The web responsive administration interface allows you to visualize load curves and modify the set of security parameters.

IcoCerberus.Web has been awarded the France Cybersecurity label in 2018.

INFRASTRUCTURE AND DEVICE SECURITY

6CURE



6CURE THREAT PROTECTION®

Comprehensive and effective European DDoS protection solution.

The 6cure TP solution is used to eliminate in real time malicious traffic aimed at critical services, with a simple philosophy: preserving the performance and integrity of legitimate flows. 6cure TP uses a tried and tested algorithm logic to identify and filter DDoS attacks, even the most complex ones, up to application layer, guaranteeing the normal flow of legitimate requests to protected services.

The advanced security functions provided by the 6cure TP protect your critical assets, such as physical or virtual servers, applications running on those servers, or network equipment such as routers, or infrastructure and hosting services such as DNS, against diverse DDoS threats.

The 6cure Threat Protection solution has received the France Cybersecurity label.

AIR-LYNX

AUTONOMOUS 4G LTE PRIVATE NETWORK

Created in 2013, the French company AIR-LYNX is the manufacturer of an innovative private 4G LTE Radio solution. This all-in-one network, compact, flexible in frequency, secure, broadband, and quick to deploy, can be declined in nomadic or mobile version. The solution integrates through a home application, all the services adapted to the needs of professionals, such as Push to Talk or video. It can be deployed in many scenarios: tactical bubble for civil security, protection of sensitive sites, security of public places, road or rail transport, access to rural Internet, Industry 4.0 or Smart Cities.

Air-Lynx has received many awards, including the MILIPOL 2017 Innovation Award in the Smart and Safe Cities Category.

For more information : www.air-lynx.com

AIRBUS CYBERSECURITY

CYBER DEFENCE CENTRE (CDC)

The 3 Cyber Defence Centres (CDC) of Airbus CyberSecurity located in France, Germany and the UK are unique structures with more than 20 years of expertise in cyber security.

The offer is based on three pillars: prevention-detection-reaction
Active 24/7, the CDC brings together the Cyber expertise of Airbus Cybersecurity From the operator to the expert in incident response and the services of the architect,

Threat Intelligence, threat watch, etc. to ensure real-time security of your digital environment and to oversee your assets.

The CDCs are able to confront all cyber threats, from the most common (ransomwares) to the most sophisticated (APT), alerting you from the first signals of compromise.

ECRIN SYSTEMS

RUGGED COMPUTERS FOR DEFENSE AND INDUSTRY

•Embedded Market Expert for all systems and computers in the industry and defense

In 40 years of existence, ECRIN has built its development around three main activities to become one of the major players in embedded electronics:

• System Integrator: Engineering and ODM services - Original Design Manufacturer- for industrial computer following Design to Build Specifications;

• Manufacturer: designing and manufacturing COTS systems “Ready to your Application”, qualified MIL-STD-810/461 and DO-160 with Modified Services for customer specific requirements

• the integration of industrial computers for Cyber Security, BigData, IIoT and Info-com

This triple competence makes ECRIN a unique partner in the field of Embedded, which is characterized by its strong capacity for innovation and its solid expertise.

OVELIANE

OSE : CONTINUOUS COMPLIANCE AND INTEGRITY MONITORING SOLUTION

The French solution OSE monitors the security level of server and application farms (physical or virtual, local or cloud).

OSE continuously measures all evolutions or deviations on servers against compliance standards or custom security policies.

A set of predefined control and monitoring rules is provided which can be adapted, modified or completed...

A specific module based on the SCAP standard makes it possible to verify that the good practices recommended by the ANSSI are really applied and gives tips to conform to them.

OSE also covers the requests for integrity checks and resilience requirements required in section 32 of the GDPR.

Finally, OSE can be plugged with a SIEM solution and thus can easily be integrated into a SOC.

SECLUDIT

ELASTIC WORKLOAD PROTECTOR

The only Cloud security analysis solution integrating a vulnerability scanner. It monitors continuously IaaS, hybrid and multi-cloud infrastructures. Its patented technology automatically discovers all IT assets and can clone servers without impact on production.

The risk of shadow IT is therefore greatly reduced. Our vulnerability scanner addition and its 60,000 tests strengthen the operating systems, networks, servers, Cloud Workloads monitoring. Our 200 automatic security tests are based on IaaS, CSA and CIS security best practices. EWP classifies the exposure level by criticality using GDPR/ANSSI, OWASP, PCI DSS risk indicators.

SIEPEL

CYBER SECURITY OF THE INFRASTRUCTURES

Cyber security of the infrastructures is our core business. Our experience and know-how allow to position ourselves on this market as a quality provider, with a premium offer:

Products:

- **High-performance shielded rooms**
- **Secure meeting rooms**
- **Architectural shielding with optimized performances**
- **Shielded pouches**
- **Secure boxes**
- **High-performance shielded racks**

SIEPEL

CYBER SECURITY OF THE INFRASTRUCTURES

Services

- **Project ownership assistance**
- **Test plans for approval measurements**
- **Acceptance tests**
- **Shielding effectiveness measurements**
- **Infrastructures measurements**
- **Securing measurements**
- **Maintenance services**
- **Training**

STMICROELECTRONICS

SECURE MICROCONTROLLERS

ST's Secure Microcontrollers devices and turnkey security solutions ensure your peace of mind by protecting your privacy in the fast growing connected digital world.
ST is able to deliver the right solution from traditional smartcard applications, covering SIM, Banking or ID markets, to the latest ones such as Secure Mobile Transactions or Internet of Things Secure Element.

ST's secure MCUs are certified according to the latest security standards (Common Criteria EAL6+, EMVCo, and CUP), they offer a complete range of communication interfaces, both contact and contactless, including ISO/IEC 7816, ISO/IEC 14443 Type A & B, NFC, USB, SPI and I^2C.
Offering a complete solution ranging from a secure operating system embedded in the secure MCU, to full enablement and personalization services, allows ST to offer seamless integration of security features to customers who might not be experts in secure systems.

STORMSHIELD

STORMSHIELD NETWORK SECURITY / STORMSHIELD ENDPOINT SECURITY

Stormshield offers complete, end-to-end solutions to protect infrastructure and endpoints. The Stormshield Network Security (SNS) range is designed to protect the most sensitive infrastructure against all types of threats transparently for users and administrators. These UTM and Next Generation Firewall products combine all network security functions in a single hardware device or virtual appliance.

In addition, the Stormshield Endpoint Security (SES) solution provides next-generation protection for endpoints (servers, workstations, etc.), thanks to its unique behaviour-based technology. This layer of defence, without signatures, blocks the most sophisticated malicious actions and those able to circumvent traditional protection systems, like the most advanced ransomware.

TEHTRIS

E-GAMBIT

The defensive cyber-weapon system

TEHTRIS' flagship product eGambit can monitor and improve IT Security against complex threats like cyber-spy or cyber-sabotage activities. It has already helped companies in China, Brazil, USA and Europe against internal and external cyber threats. eGambit has already caught billions of events related to cybersecurity issues worldwide.

The Artificial Intelligence engine, which is embedded in eGambit, fully created by cutting-edge engineers at TEHTRIS, is already protecting many sensitive infrastructures owned by multinational companies. For instance, it can detect unknown viruses or malwares as it is not based on signatures.

THALES

CYBELS SENSOR

CYBELS Sensor, which benefits from the latest innovations in artificial intelligence, is a trusted probe for detecting cyber-attacks and protecting critical infrastructure and sensitive networks. The solution meets the requirements to help essential operators and companies operating in strategic or sensitive areas to comply with the regulation. Deployed at critical points on the network, CYBELS Sensor analyzes data flows and files to detect attacks and suspicious behavior.

Cybels Sensor can be integrated with an on-premise Security Operations Center or operated by a Managed Security Service Provider.

THALES

THALES

ELIPS

Regulations governing the processing of information with different levels of sensitivity require systems to be completely isolated from each other (for example to protect confidential medical information, as well as trade or defense secrets).

The ELIPS Diode creates a one-way link that prevents leakage of confidential information, making it possible to connect a critical, classified, or strategic network to an unprotected network in order to receive relevant data, without the possibility of transmitting information in the opposite direction.

ELIPS is approved up to Top Secret level for the French market and is certified NATO Secret by the NATO Information Assurance Product Catalogue.

THALES

THALES

MISTRAL

MISTRAL is a government-grade IP (VPN) network security solution. It allows confidential applications to be protected up to Restricted level without degrading quality of service. MISTRAL helps to combat threats associated with the interconnection of local area networks via public infrastructure such as the Internet or carrier networks thanks to an array of high-level security services based around authentication, confidentiality and integrity.

MISTRAL is common criteria (CC) certified at EAL3+ level, and is approved at Restricted level for France, the EU and NATO.

INDUSTRIAL NETWORK SECURITY

C-S

PRELUDE

Prelude is an SIEM: a security information and event management solution.

By centralizing the collection and processing of information from a range of sources, PRELUDE provides a unified view of the state of security to ensure enhanced responsiveness when cyberattacks occur. Based on open standards (IDMEF and IODEF), PRELUDE is a particularly effective, flexible smart security solution, in particular within the operations of an SOC (Security Operation Center).

PRELUDE is the only European 100% SIEM (Security Information and Event Management) alternative to American solutions responding to the requirements of critical operators.

STORMSHIELD

STORMSHIELD NETWORK SECURITY / STORMSHIELD ENDPOINT SECURITY

Stormshield offers complete, end-to-end solutions to protect industrial networks. The Stormshield Network Security (SNS) range's SNi40 solution, available in a rugged physical format, allows optimal protection to be deployed as close to machines as possible. It is the only product on the market with First Level Security Certification (CSPN) for industrial firewalls from ANSSI, allowing it to meet the requirements of the French regulation on the protection of Information Systems of Vital Importance (SIIV).

In addition, the Stormshield Endpoint Security (SES) solution protects industrial terminals and operator workstations running on Windows. This layer of defence, without signatures, blocks the most sophisticated malicious actions and those able to circumvent traditional security systems.

AUDIT, CONSULTANCY AND TRAINING

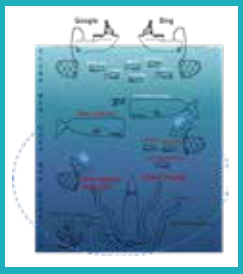
AIRBUS CYBERSECURITY

CYBERRANGE

CyberRange is a platform for cyber training and simulation allowing organizations to take charge of the training of their cyber security experts.

The service reproduces realistic computer or industrial environments in which scenarios can be played that include real cyber-attacks cyber-attacks. CyberRange also proposes to test and experience technical solutions that are on the market

ALEPH NETWORKS



RANGE OF SERVICES

GM Search Dark engine is complemented by a range of services: targeted data feeds, personalized reporting, cyber studies, training ...

aleph-networks monitor and analyze continuously and in an industrialized way thanks to their direct and discrete search engine, the deepest zones of the web, where the heart of Cyber Crime is hidden.

AMOSSYS

EXPERTISE & INNOVATION IN CYBERSECURITY

A reputed company that specialize in consulting and expertise in cybersecurity, AMOSSYS assists its clients in securing their digital space through a comprehensive offer of high value-added services: audit, consulting, CERT, evaluation, risks assessment, R&D, innovative software development.

As a proof of the trustworthiness of its interventions, AMOSSYS earned the recognition of highest French authorities: we are a French Center for the Assessment of the Security of Information Technologies (CESTI) certified by the ANSSI (French National Cybersecurity Agency), a Service Provider in Cybersecurity Audits for the National Safety (PASSI-LPM) and a certifier for the French Online Gambling Regulation Agency (ARJEL).

ARTEM

AWARENESS, SIMULATION AND TRAINING IN RISK AND CRISIS MANAGEMENT

ARTEM INFORMATION & STRATEGIES offers training (awareness seminars - sectoral surveys or methodologies) on the topics of strategic/competitive intelligence, risk analysis and crisis management. The topic «cyber» is covered through the realization of training modules for students as professionals

More than 500 crisis exercises, including > 100 for executive committees, have been carried out since 2005, both in France and abroad (Italy, Algeria, Belgium, Senegal, UAE, Luxembourg, Switzerland, Malaysia, Turkey, UK, Qatar, Brazil, etc.) as part of risk prevention, consulting, training in Crisis / Business Continuity Management. Our clients work for Banks, Insurance, Security, Energy, Armed forces, Aeronautics, Cybersecurity, Retailing, Biotech, Construction or Agribusiness.

BLUECYFORCE

PRACTICAL CYBERSECURITY TRAININGS

Individuals trainings in all cybersecurity's aspects, collectives trainings (management crisis, logics and team processes) and full crisis exercise in team.

All our trainings are based in the use of a reproducing environment of real systems, with real cybersecurity means. Our Red Team constantly study new attacks, new flaws, news techniques in order to include these contents in our trainings.

The Red Team reproduces calibrated and targeted attacks for progressive and realistic training. In bluecyforce, we train to deal with the evolution of today and tomorrows' threats.

CEIS

STRATEGIC CONSULTING & STUDIES

Because the reflection must precede and feed the decision, we follow our customers in understanding their environment and the definition of their transformation and development strategy. Our consultants combine strong expertise in strategic sectors (defense, security, energy, transport, digital) and the mastery of a complete methodological toolbox (animation of seminars, development of scenarios ...). Specialy involved in digital transformation issues, CEIS has a framework contract with the Ministry of the Armed Forces of prospective and strategic studies (EPS) in the field of security of cyberspace and cybersecurity. We thus approach the wholeissues related to security and digital transformation. Our services : Prospective Studies, Strategic Diagnosis, Market Analysis, Strategic follow-up.

CONSCIO TECHNOLOGIES

RAPIDAWARENESS

Conscio Technologies manages an offer covering all aspects of online awareness on cybersecurity and the GDPR.
In terms of cybersecurity the content is very rich and has so far nearly 50 courses.

For the implementation of campaigns two software solutions exist.
Sensiwave: You drive your campaign down to the last detail and can customize the content to fit your environment and your message.

RapidAwareness: This solution offers the advantage of simplicity because with RapidAwareness it is possible to implement a campaign in a few minutes. Our introductory video helps you understand the simplicity of RapidAwareness in 2 minutes: : https://youtu.be/xWpv_yAtAYU

OÏKIALOG

AUDIT RISQUES ET MENACES

The general objective is to study the needs in terms of log analysis and exploitation in order to be able to propose and create relevant indicators cibling the risks and threats to be covered.
More precisely, this study makes it possible to determine:

- what is currently available in terms of log sources
- the required needs in terms of log types to cover the security risks and threats
- a list of the necessary log sources to generate the relevant indicators
- a grid of product choices and help in selecting suitable tools

Concretely, the study provides:

- a grid of needs
- a reflection on threats and the possible data sources to cover them
- a grid of solution choices

RISK&CO SOLUTIONS

SOLUTIONS

1. Identification of threats and vulnerabilities
• Analysing threats and vulnerabilities to identify risks and security targets for a given perimeters.
• Conducting security audits and intrusion tests at organisational and technical levels to identify the main vulnerabilities.

2. Risk mitigation
• Supporting clients and contractors to design secure industrial systems and security systems (access control, CCTV, etc.)
• Integrating and developing high-security solutions.

3. Supporting complex projects
• Cyber security planning in complex projects.
• Ensuring regulatory compliance.

TEXPLAINED

INTEGRATED CIRCUITS AUTOMATED REVERSE ENGINEERING SOFTWARE

Relying on its expertise on ICs security facing piracy and counterfeiting, Texplained is developing a tool that recovers the architecture of any IC, on different formats: Netlist, VHDL description, GDSII.
ChipJuice advantages:

- Versatile: usable for any kind of chip (Smart Card, Microcontroller, microprocessor, FPGA,...)
- Easy to use: Step by step guidance
- Smart: Previous results usable for faster new project
- Optimized: Installable on a standard computer - No need for huge resources
- Powerful: Very fast data processing
- ChipJuice purposes:
- In depth exploration of ICs / Chip Risk Assessment / Hardware Backdoors Research / Technological Intelligence / Analysis for obsolete device replacement

MANAGED SERVICES AND OPERATIONS

SOPRA STERIA

CYBER MANAGEMENT AND MONITORING

With more than 700 experts and advanced Cybersecurity Centres in Europe and around the globe, Sopra Steria is a global cyber security partner and a reference for cyber trusted operators, helping to protect for the protection of major institutional and economic players and their business sectors.

Sopra Steria accompanies its clients in supports its clients with the implementation of detection and response solutions using Security Operations Centres (SOC) with tools such as Security Information and Event Management (SIEM), Detection of Advanced Persistent Threats (APT), Forensics and Crisis management. Our France-based cyber security centre operates for Operators of Vital Importance and sensititive industries.

Sopra Steria is currently being qualified for the detection of security incidents, by ANSSI, the French National Agency for the Security of Information Systems.

INTELLIGENCE

ALEPH NETWORKS

GM SEARCH DARK.

Aleph-networks have developed a specialized search engine that is completely independent of any API to explore the Deep and Dark webs: GM Search Dark.

The monitoring scope and analysis features are unique.
The Dark Web: more than 150 000 Tor sites and more than 10 000 I2P sites are monitored. The **Deep Web:** more than 1 200 'Black Hat' sites are monitored. Or more than 60 million pages indexed, with a **constantly evolving coverage** (+100% in one year).

The data is collected on sites, forums, open market places, connected objects…
GM Search Dark is a unique tool that allows to carry out advanced research and analysis in the deepest and hidden corners of the web.

BERTIN IT

MEDIACENTRIC® / MEDIASPEECH®

Bertin IT creates a secure connection and supervises exchanges of information between sensitive and/or remote networks via its secure gateway, CrossinG®. Its MediaCentric® solution, meanwhile, anticipates cyber-threats, checks for vulnerabilities in the information system, monitors multiple channels in crisis situations and helps prevent terrorist and criminal activities through 24/7, multi-source (web, TV, radio) acquisition capacities and in-depth analysis of multimedia and multilingual content. As an expert in voice technologies, Bertin IT is also strengthening its distinctive positioning with its MediaSpeech® software solution, for generating value from multilingual spoken content from audio and video sources, and phone conversations.

BERTIN IT

CYBER THREAT INTELLIGENCE SERVICES

Bertin IT's cyber threat intelligence services provide guaranteed anticipation and monitoring for its clients' assets. Bertin IT's experts monitor the web and its depths to detect all kinds of threat, from early indications of preparations for a cyber-attack, to the risks of physical attacks, data leaks onto the internet (intentional or not), forgery and distribution networks.

CEIS

SECUINSIGHT - CYBER THREAT INTELLIGENCE

Know the threat, prepare your defenses

With SecuInsight, CEIS offers personnalized services of strategical and operational Cyber Threat Intelligence to its clients. Preparing effectively its cybersecurity is understanding potential attack paths, evaluating external IT risks (data leaks, fraud, reputation, vulnerabilities etc) to anticipate threats likely to affect its organization. The reported data are made actionable by human analysis carried out by our team of consultants and analysts with complementary skills and profiles (analysts, linguists, geopolitical and business experts, lawyers, ethical hackers). They can feed a MISP platform and be presented in a dedicated dashboard, allowing our customers permanent monitoring of IT risk. They can thus optimize their cybersecurity strategy, their choice of solutions and the efficiency of their operational teams.

LINKURIOUS

LINKURIOUS ENTERPRISE

Linkurious is a software company that designs and delivers a graph intelligence platform to detect and investigate threats such as computer fraud, cyber-attacks, or security breaches. Thanks to an intuitive visualization interface, Linkurious Enterprise allows you to investigate your data as graphs of connected entities. The analysis of these graphs offers an exhaustive view of the relationships between the entities composing computer networks and information infrastructures. It lets you identify the vulnerabilities of computer systems or visualize the data related to an attack in order to evaluate its nature and react accordingly.

SEKOIA

SOLUTION INTHREAT

SEKOIA distributes InThreat, a turnkey threat intelligence offer including reports, feeds, a threat intelligence platform and professional services.
inThreat, it's an all-in-one threat intelligence application and available in different packages. Each package corresponds to a company maturity level relating to threat intelligence.

- Threat summary reports allow the customer to understand very quickly what he has to face and take the right decisions according to his business sector.
- Different feeds are available for companies that need to consume indicators of compromise. These feeds are amongst the most valuable and actionalbe on the internet.
- A private sharing solution based on MISP allows each customer to have his own dedicated threat intelligence platform without having to worry about system administration.

VOCAPIA RESEARCH

VOXSIGMA

VoxSigma Features
Real-time speech transcription - Language identification - Speech/non-speech segmentation - Key word spotting - Speaker diarization - Audio-text alignment

Excellence : Owing to our extensive experience in research and longstanding collaboration with the LIMSI-CNRS laboratory, we develop state-of-the-art systems and regularly receive high rankings in international evaluations.

Custom-tailored technologies : We work closely with our clients to offer them customized solutions that are adapted to their applications.

Efficient personalized support : We consider user and integrator support an integral part of our products and services, offering them solutions in the shortest possible time-frame.

COMPANIES INDEX

PRESENTATIONS

CONTACT

Justine BERNAGOU
justine.bernagou@6cure.com
+33 (0) 9 71 16 21 56

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

6CURE

6cure
secure your business

FRANCE CYBER SECURITY

6CURE – GUARANTEEING THE AVAILABILITY OF YOUR DATA

6cure, a French company created in the late 2000s, is specialized in DDoS mitigation. We have built efficient solutions allowing our clients improve their reactivity and resilience against malicious activity targeting the availability of their critical services.
New attack strategies emerge on a regular basis. Continuous developments are needed in terms of functionality, and detection and neutralization strategies in order to be able to counter them.

Areas of expertise: detection and mitigation of multiform cyber attacks, anti-DDoS protection, botnet detection, attack source analysis, computer security incident handling.

The solutions developed by 6cure allow the protection of information systems against even the most complex DDoS attacks and are being used in the following domains:

- Protection of telecom and hosting infrastructure
- Security for DNS infrastructure
- Preserving the availability of services for all types of clients
- Specific protections for e-commerce, banking, insurance and health sectors
- Sovereign solution dedicated to critical infrastructure protection
- Accessible and adapted protection for organizations ranging from SMEs to large enterprises
- DDoS resilience testing

We focus on developing solutions that are simple to use and deploy, interoperable and collaborative, providing crucial visibility for users to confront cyberattacks that have become multifaceted.

Interoperability: with SIEM solutions available on the market.
Management and optimization: of existing security solutions (Firewall, IPS/IDS, etc.).
Complementarity: with already deployed anti-DDoS solutions.

CONTACT

Thierry BUFFENOIR
info@air-lynx.com
+33 (0) 9 81 43 46 46

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

AIR-LYNX

AIR-LYNX is a French manufacturer of private and secure 4G LTE infrastructure radio network. Its solutions are among the most compact and fastest to deploy on the market. Autonomous, these devices allow the very simple implementation of a 4G LTE radio network anywhere, in less than 90 seconds. The range is available in fixed or nomadic versions, including a tactical bubble (a complete network in a 30 kg suitcase), and a ManPack (complete network in a backpack).

AIR-LYNX solutions have other advantages, such as being flexible in frequency, fully secure and resilient. They benefit from advanced security mechanisms, offered as standard in the LTE standard, plus 128-bit AES encryption mechanisms.

The AIR-LYNX private networks can meet connectivity needs in many scenarios : civil security or defense, protection of sensitive sites, securing public places, road or rail transport, maritime transport, access to rural Internet, mines, oil and gas, Industry 4.0, smart and safe cities ...

AIR-LYNX also develops MCPTT services adapted to the needs of professionals, users of PMR for example, which allow LTE-induced broadband to bring the dimension of video transmission and in particular multicast (eMBMS) running on Android Smarphone.

Air-Lynx has received many awards, including the MILIPOL 2017 Innovation Award in the Smart and Safe Cities Category.
For more information : www.air-lynx.com

CONTACT

Laurence THOMAS
laurence.thomas@airbus.com
+33 (0) 1 61 38 62 00

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

AIRBUS

AIRBUS

Based on the Airbus Group experience in defence and security, and with a strong team of more than 700 experts fully dedicated to cyber security, Airbus Cybersecurity puts its offers its expertise and trusted European solutions to all its customers.

With its strong human expertise gained through major cases of incident response, Airbus Cybersecurity's offer includes a wide range of products (Keel back Net, Orion Malware, Cymerius, CyberRange, Stormshield, Ectocryp, SEG, etc.) and Services (SOC, Audits, Consulting, Threat Intelligence, etc.) in cyber security, covering the entire chain of cyber security and the protection of your assets.

In Europe, as well as in the Middle East, defence and security organisations, governments, operators of critical infrastructures or sensitive industries trust in the products and services developed by Airbus Cybersecurity.

Building on its three Cyber Defence Centres (CDC) based in France, Germany and in the UK, Airbus Cybersecurity offers unique structures that dynamically combine threat watch, early detection of attacks and their investigation, thus drastically reducing the time of response and incident handling. The implementation of a strategy through the support of innovation, the recruitment of experts and the development of strategic partnerships (in the area of air transport with SITA for example) allows Airbus CyberSecurity to provide its customers with the technologies and services appropriate to their needs.

With 20% of the annual turnover invested in innovation and R&D, Airbus CyberSecurity remains at the forefront of the latest technological trends in terms of knowledge of the threat, detection and analysis means and innovative techniques of machine learning.

CONTACT

Nicolas HERNANDEZ
nicolas.hernandez@aleph-networks.com
+33 (0) 6 15 68 51 32

333 montée de Buisante,
69480 Pommiers

OFFER CATEGORY

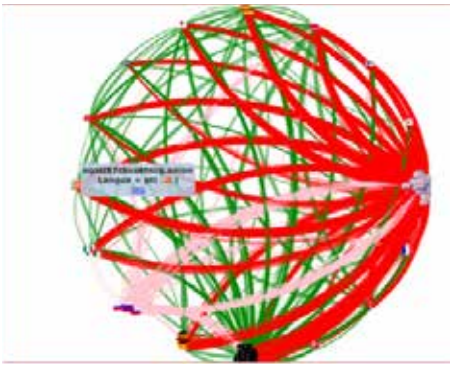
POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

ALEPH-NETWORKS

Aleph-networks grew out of an R&D project in 2010.

Since 2012, we have developed and marketed **two innovative technologies to collect, process, and anonymize Big Data, along with a range of associated services: GrayMatter and SafetyGate.**



SafetyGate is a distributed network technology (p2p) that addresses the risks of transmitting sensitive information.

GrayMatter is a technology for indexing and structuring data in very large volumes, which makes it possible to process all types of data, whatever their format and their origin (Dark Web, Deep Web, OSINT, ...), and to structure them according to business consultation criteria:
- public data of professional social networks,
- data of commercial sites,
- press flow in very large volumes for intelligence-oriented analysis and monitoring,
- etc ...

CONTACT

Vattana VONG
contact@amossys.fr
+33 (0) 2 99 23 15 79

4bis Allée du Bâtiment,
35000 RENNES

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

AMOSSYS

A reputed company that specialize in consulting and expertise in cybersecurity, AMOSSYS assists its clients in securing their digital space through a comprehensive offer of high value-added services:

Audit : Get a precise diagnosis of the cybersecurity of your infrastructure by a trustworthy service provider (French PASSI and ARJEL certifications): physical and organizational audits, architecture audits, configuration audits, source code audits, internal and external penetration tests.

Consulting : Benefit from our expertise and our feedback to optimize the security of your infrastructure and information systems: management and support, management of operational risks, risks assessment, security certifications, formation and awareness training of the users to the best practices.

CERT : Benefit from a fast intervention in case of an incident or suspicious activity related to cybersecurity: emergency response, computer forensics, analysis and reverse engineering of malware, support in the remediation of compromised systems and hardening its security.

Evaluations : Laboratory certified (by the ANSSI) and accredited (by the COFRAC) to conduct Common Criteria or CSPN (French First Level Cybersecurity Certification) evaluations, writing or support in writing security targets and Common Criteria evidence.

R&D : Improve your strategic positioning with the latest progress in cybersecurity: studies, proofs of concept, conferences, doctoral advising.

Innovative software : Fully or partially outsource the design or the implementation of your cybersecurity solutions: integral development of cyber products, suppling of software components.

As a proof of the trustworthiness of its interventions, AMOSSYS earned the recognition of highest French authorities: we are a French Center for the Assessment of the Security of Information Technologies (CESTI) certified by the ANSSI (French National Cybersecurity Agency), a Service Provider in Cybersecurity Audits for the National Safety (PASSI-LPM) and a certifier for the French Online Gambling Regulation Agency (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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

ARTEM

ARTEM DEFENSE

ARTEM companies are managed by Patrick Cansell, PhD in Information and Communication Sciences, associate fellow at DICEN-IdF lab, head of the «Competitive Intelligence» course at the “Ecole des Mines de Paris”, and head of the Master “ISART” (Strategic Intelligence, Risk Analysis and Territories) of UPEM - East-Paris University. In addition to his teaching activities, he created ARTEM INFORMATION & STRATEGIES, ARTEM DEFENSE and ARTEM TRAINING, which cover a broad and complementary spectrum of services for professionals, researchers and students.

Sector studies on the «cyber» topic
ARTEM DEFENSE, which operates in the Defense and Security segment, specializes in Defense sector analysis (market or sector surveys, specific focus).

ARTEM DEFENSE carries out quarterly sectoral studies on Defense and Security topics for the benefit of GICAT members, particularly on the cybersecurity / cyber defense topic.

ARTEM DEFENSE is also a partner of major Defense and Security key industries to carry on technical-operational studies about the challenges and technologies of the future (future issues, future combat) for the benefit of the French MoD and the French armed forces.

CONTACT

Hervé COLLARD
herve.collard@atempo.com
+33 (0) 1 64 86 83 00

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

ATEMPO

Atempo

Data Protection Solutions

Atempo is a French software vendor specializing in data backup, archiving and preservation of data.
Atempo commercializes software solutions for enterprise data protection needs with the flagship product Atempo-Time Navigator (ATN), an endpoint data protection solution, Atempo-Live Navigator (ALN) and an unstructured data protection solution, Atempo-Digital Archive (ADA).

The feature sets of these three products and the extensive compatibility cover for storage and applications make Atempo a solution of choice for all types of organizations: centralized, with or without remote sites, from a few terabytes to several petabytes of data.

Atempo solutions enjoy a solid reputation and are installed and running in many major public institutions (Ministries of Finance and Defense, French Railways, National Blood Bank etc.) and private corporations (Banque Populaire, Caisse d'Epargne, Kiloutou, Kiabi, LexisNexis, etc.).
Distribution is via an established integrator/partner network principally to SMB, mid-size and corporate accounts.
Headquartered in Paris, Atempo is present in Europe, the USA and Asia with a network of over 100 resellers, integrators and MSPs.

Why choose Atempo?

Atempo solutions are designed for companies of all sizes. Simple and straightforward to install and run, customers benefit from:

- Capacity to manage very large data volumes (petabytes)
- Simple and rapid data recovery
- Support of heterogeneous environments
- Vendor-agnostic approach. Atempo remains independent from constructor lock-in.
- Recognized multi-lingual customer support, based in Europe
- Flexible Licensing Program adapted to market sectors: authorities, hospitals, education, research....
- Genuine line of defense against cybercriminality

CONTACT

Cecile LEROUX
cecile.leroux@atos.net
+33 (0) 1 73 26 00 00
River Ouest, 80 quai Voltaire
95877 BEZONS
https://atos.net/en/products/cyber-security

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

ATOS

To fight against cyber attacks and ransomware, Atos offers a unique and logical approach linking security and business focused on the protection of data as well as prevention. You would benefit from expertise based on years of experience resting on a range of products (**Bull Evidian, Bull Trustway, Bull Horus**) and security services answering the needs of organizations.

Trusted partner, Atos, creates, develops, exploits and manages state-of-the-art digital solutions combining calculating power, security and systems integration. Thanks to its technological expertise, Atos assists the digital transformation of its clients while respecting the new legislation ((LPM – "Loi de Programmation Militaire", **GDPR** – "General Data Protection Regulation", NIS, PCI DSS, HIPAA…).

The group offers a high level of expertise and professionalism in its governance services, risks and conformity. It supports its clients in the development and the planning of political strategy security plans, combining a well-balanced operational efficiency of data protection with information systems and conformity with the legislation in force (GDPR).

The spectrum of Atos' services in this area includes, among others, private data protection and compliance, security auditing, penetration testing, architecture and implementation of the most sophisticated attack detection and remediation systems.

Atos also provides **Hoox Smartphone** for secure communication based on Android. Atos is the global IT partner for the Olympic and Paralympic Games and part of the CAC 40 Index.

CONTACT

Jean-Pierre MASSICOT
Jp.massicot@att-fr.com
+33 (0) 1 47 16 64 72

99 avenue de la Chataigneraie
92500 Rueil Malmaison

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

ATT

Advanced Track&Trace

FRANCE CYBER SECURITY

For over 10 years, Advanced Track & Trace has been developing and providing governments and international companies with advanced technologies to ensure the safety of business and individuals: authentication and identification solutions, data integrity protection and information encryption.

Through its Vary.IDs platform, ATT generates billions of unique identifiers for serialization, traceability and connectivity of products and documents.

Exploitable on several levels (citizens, authorities, agents, experts...), these solutions are easy to implement and offer an excellent competitiveness-efflciency ratio.

PROTECTION OF IDENTITY & DOCUMENTS

The solutions developed by ATT secure the signature and all key information of a document: textual data, biometrics, photography...

Founding member of the AIGCEV/VDSIC (Visible Digital Seal International Council), and provider of administrations, institutions and printers, ATT provides turnkey solutions for all types of documents, both physical and digital: payment and identification cards, stamps, visas, passports, badges, administrative documents, ticketing ...

ATT has received the France Cybersecurity label.

SECURITY OF PRODUCTS AND FIGHT AGAINST ILLEGAL MARKETS

Through smart packaging and product protection solutions, ATT provides manufacturers and customs with reliable and innovative tools to ensure the authentication and secure traceability of products.

Founding member of the ITSA (International Tax Stamp Association), ATT is active in all geographical areas and sensitive sectors of activity: alcohol, tobacco, wine, food, pharmaceuticals, cosmetics, electronics, spare parts, luxury goods...

BANKNOTE PROTECTION

As a certified partner of the Banque de France, ATT develops security codes to prevent the fraudulent reproduction of banknotes.

CONTACT

Aude BRAUNSTEFFER
aude.braunsteffer@bertin.fr
+33 (0) 6 74 68 85 55

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

BERTIN IT

BERTIN IT is a software developer and integrator that offers a range of solutions and services for cyber security, cyber intelligence, strategic intelligence and automatic speech processing.

As a leading player on the market, Bertin IT supports both the private sector (in areas such as banking, insurance, industry, telecommunications operators, media, energy and the environment) and public bodies (central administration and defence).

By responding to the strategic issues of protecting, anticipating and analysing their markets, Bertin IT's solutions deliver benefits that include:
• Generating value from multilingual spoken content, from audio and video sources and transcriptions of phone conversations, with its MediaSpeech® solution
• Protecting the integrity of information systems and assets, with its MediaCentric® solution
• Confidentiality and safety of exchanges between sensitive networks or information systems, with its CrossinG® solution
• Detecting the early signs of cyber-attacks and information leaks that leave information systems vulnerable, with Bertin IT bespoke services
• Strategic, economic, competitive and e-reputation intelligence, with its AMI Enterprise Intelligence solution

Bertin IT is involved in numerous research programmes, in areas including:
• Virtualisation, cryptology, data flow management and secure interoperability
• Information and content processing, investigating and generating value from multilingual, open-source, multimedia data (web, TV and radio)

With 120 people in France and abroad, Bertin IT offers its clients bespoke, customised assistance, including a needs analysis, development of ad-hoc solutions, deployment strategy and support for the whole of the life cycle.

Bertin IT is a CNIM Group subsidiary, specialising in cutting-edge information technologies. Founded in 1856, CNIM is a French equipment manufacturer and industrial integrator operating on an international scale, listed on the Euronext Paris index.
CNIM employs 2,500 staff and posted turnover of €539.9 million in 2016, with 55% generated from international sales.

CONTACT

Vincent RIOU
vincent.riou@bluecyforce.com
+33 (0) 1 45 55 39 98

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

BLUCYFORCE

bluecyforce

BLUECYFORCE : Cyber training Center

Born of a partnership between two French SMEs, CEIS, consulting company in strategy and management cyber risks, and DIATEAM, engineering company computer science specialized in cybersecurity, the cyber training center bluecyforce responds to a need that was not covered until then: the training of operational cybersecurity teams in an environment similar to their environment professional.

In break with traditional training, bluecyforce offers in its Centers a unique offer in Europe of training and operational training in cyber defense, open to all professionals, according to pedagogical paths based on practice.

All our trainings are based on the use of an environment that reproduces realistic systems and networks, including industrial systems. We also integrate the cybersecurity solutions of our technology partners (market leaders and innovative technologies). Bluecyforce instructors are assisted by a «Red Team». Professional ethical hackers, they assist the participants in their progression by acting as «Sparring-Partners».

The Cyber Training Center bluecyforce is based in Paris, Montparnasse Tower. We can also deploy our resources in our client's premises, and we plan to open new bluecyforce accredited centers worldwide in 2018.

CONTACT

Vincent RIOU
vriou@ceis.eu
+33 (0) 1 45 55 39 98

Tour Montparnasse
33 avenue du Maine - 751015 Paris

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

CEIS

The digital transformation generates new risks and amplifies certain traditional risks. Companies must anticipate,prepare and react all at once. They must be aware of and monitor the threat, the motivations of the attackers, theirarea of vulnerability, understand good defense practices and have competent and trained human resources.

CEIS assists its clients in managing their cyber risks through a comprehensive offer: consulting and implementation of cybersecurity strategies, audit, crisis exercices, detection and response to incidents, Cyber Threat Intelligence and team training thanks to the capacity of the bluecyforce Cyber Training Centre.

With 80 multi-disciplinary consultants and some twenty associate experts, CEIS provides you with its expertise throughout the entire cycle of your cyber security projects.

CEIS, your Cyber problem solver :

• STRATEGY : Development of Security Policies, Audit of internal and external cyber risks, Asset-based consulting, Strategic studies

• THREAT INTELLIGENCE : Audit of external risks, Strategic analysis of the threat, Monitoring Clear, Deep and Dark Web, Monitoring of Social Networks/ reputational exposure, Leakage of client and collaborator login details, Anti-phishing, Anticipatory attack scenarios

• CAPACITY BUILDING : Audit/Needs analysis, Market analysis, Support for the implementation of cyber security solutions (SOC, CERT), Development of crisis management processes

• INVESTIGATIONS & COMPLIANCE : GDPR compliance, Continuous monitoring of data leaks, Due Diligence and background checks on IT suppliers, Pre-litigation investigations

CONTACT

François CHASSERY
francois.chassery@certinomis.fr
+33 (0) 8 09 10 98 09

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

CERTINOMIS

Certinomis
la confiance, ça se prouve

Digitalisation is a disruption, a change of paradigm that makes possible to deal without signing on paper. But this change is a double source of worrying: we know that hackers exist, and we do not spontaneously trust electronic documents.

• **Our mission : creating the conditions of trust**

To answer this fears, Certinomis is proposing a range of trust services for:
- Guaranteeing the identity of the actors of an electronic exchange,
- Link a transaction to a date that is certain,
- Generate legally opposable documents.

This services make it possible to protect ourselves from identity theft, and to prevent court challenges. From these safeties outcomes trust.

• **Our resources : recognised technical and legal infrastructures**

Our supply requires technical installations that are robust and highly available to produce the deliverables of our trust services in accordance with regulations and standards.

The conformity of our infrastructures and of their functioning is attested by regular audits that result in referencing (Adobe, Microsoft, Apple, Google, Mozilla), certifications (ETSI or CEN standards) and qualifications (French public frame of reference for it security, RGS, and European regulation for electronic identification and trust services, eIDAS) : they are as many evidences justifying trust.

• **Our offer : services on demand**

From these recognised trust infrastructure, Certinomis is proposing to its clients trust services that are adapted to them: we can supply on a unit basis, or by volume; we can activates turnkey solutions, or integrate some part of the client activity in them. But always with the same focus on quality.

Our job of **Digital Trust Operator** consists in making you benefiting on demand of complete and highly qualified solutions that ensure your technical and legal safety in the digital world.

CONTACT

Michel GÉRARD
michel.gerard@conscio-technologies.com
+33 (0) 6 07 04 92 57

12 rue Vivienne,
75002 Paris

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

CONSCIO TECHNOLOGIES

Conscio Technologies is the specialist in user awareness.

Conscio Technologies it's:

• 10 years of experience as an expert in computer security awareness.
• More than 800,000 satisfied users
• More than 150 references from organizations of all sizes and sectors.

Conscio Technologies is also a member of Hexatrust.

Conscio Technologies offers its customers a complete approach to user awareness including very complete video and quiz contents, software solutions for implementing your campaigns, fake phishing campaigns, and maturity assessment.

The Conscio Technologies offer includes a rich variety of content (46 routes in SSI and 13 in the RGPD).

There are two software packages to implement the campaigns: RapidAwareness, the simplest solution to launch a campaign, within reach of all, a few minutes are sufficient to launch its campaign and Sensiwave, the most complete solution to prepare a campaign set up in every detail.
The areas covered are related to cybersecurity, General Data Protection Regulation (GDPR), health data, the fight against harassment.

CONTACT

Barbara GOARANT
communication@c-s.fr
+33 (0) 1 41 28 46 94

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

CS

As a designer, integrator and operator of critical systems, CS offers innovative digital trust and anti-cybercrime solutions for end-to-end protection of Information Systems and communication infrastructures. From strategic and operational advice (RGPD, ISO27000, LPM/NIS) to vulnerability management, from secure infrastructure design to security governance and auditing, CS supports clients throughout the value chain.

Our solutions:

- **SEDUCS:** hardened minimal OS industrialization platform
- **TRUSTYBOX**: secure platform including all trust services required for making data secure and virtual interactions certified CC EAL3+.
- **PRELUDE – SIEM**: solution for real-time management of security events.

Approved by the CERT (Computer Emergency Response Team), CS also supports clients as they implement their security policy, ensures rapid response on security incidents thanks to its Rapid Intervention Group, and provides vulnerability management services on their systems to guarantee resilience throughout their life cycle.

"Today CS is the only company with a complete range of security solutions and products entirely designed, developed and maintained in France, certified France Cybersecurity. Our aim is more than ever to provide responses adapted to the cyberprotection and resilience of our clients' infrastructures and systems." says CEO Khaled Draz.

Specializations:
PASSI Audit and pentest, RegTechs (RGPD, LPM, NIS, sectorial, etc.), Critical system integration, SIEM/ NMS, SOC/NOC, Trust Services, cryptography, CERT/GIR, MCS.

CONTACT

Thomas BOUCHER
tb@datashush.com
+33 (0) 7 86 87 44 28

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

DATASHUSH TECHNOLOGY

Datashush Technology SAS « LockEmail.com » is a young French startup (founded in 2015).

Supported by “La region Nouvelle Aquitaine”, Bordeaux Unitec and Aquinetic “La Banquiz”.
Protecting the Exchange by emails is our priority.

French founders, French owner, Hosted in France.

To palliate disadvantages of conventional security solutions, Datashush Technology bets on innovation. To keep things as simple as possible LOCKEMAIL chose not to use the classic email protocols (SMTP / IMAP,POP), too complex to secure. We have therefore implemented a simple, yet robust, client/server solution, with technologies that are simple and safe to use.

Encrypting your messages = Confidentiality of your correspondence

With LockEMail, your emails on the web are in a safe, you are the ONLY one to own the key, the software using a password you are the only one to know, and the lock location is on your computer or mobile.

LockEmail a simple philosophy All the vulnerable and sensible data are stored on user’s computers (Keys, password, receivers, content).

Youtube: HTTPS://www.youtube.com/watch?v=WdgN5-_nzhl
Facebook: Https://www.facebook.com/lockemailbydatashush/

CONTACT

Xavier QUONIAM
xquoniam@denyall.com
+33 (0)1 46 20 96 20

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

DENYALL

denyall
a Rohde&Schwarz Cybersecurity company

DenyAll works in conjunction with the French authority (ANSSI) and helps organizations go digital by ensuring user interactions are seamless, yet secure.

DenyAll's cloud services and appliances **simplify the job of security and DevOps teams** throughout the software development lifecycle with a comprehensive portfolio:

- **Vulnerability scanners** to identify prioritize and patch OWASP Top 10 vulnerabilities.
- Web Single Sign On solution to simplify and strengthen user access to applications, wherever people connect from and wherever applications are located.
- **Web Application Firewalls** to block known and unknown attacks targeting web applications, the APIs and web services based on modern technologies (HTML5, JSON, XML, HTTP/2).
- **Virtual browsing environment** developed in cooperation with the German Federal Office for Information Security (BSI), is a brand-new solution for secure and comfortable browsing the Internet.
- **Network encryption** to protect companies and organizations against espionage and manipulation of data that is transported via Ethernet over landline, radio relay or satellite links.

The recent acquisition of DenyAll by Rohde & Schwarz Cybersecurity allows us to benefit from an ideal environment to **innovate in application threat intelligence and to take up the challenge of IoT** and mobile applications.

Labels:

- **CSPN by ANSSI**: The National Agency for Information Systems Security (ANSSI) has qualified and awarded DenyAll application firewalls its first level security certificate (CSPN)
- **Label France Cybersecurity:** DenyAll received the label «France Cyber Security Awarded by users and government, which rewards quality and performance of our firewalls applications.
- **Gartner:** In the Magic Quadrant 2017 for Web Applications Firewalls, Gartner highlights advanced security engines and the ease of use of 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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

ECRIN SYSTEMS

ecrin SYSTEMS
Rugged Computers

French company founded in 1976 and incorporated into Convergence Group since 2007, ECRIN Systems benefits from a strong position in the embedded market and industrial computing.
Thanks to the combination of expertise and competence, the Group is positioned as a true global electronic quality partner in computer and system engineering, able to satisfy specifications of the most demanding customers in Mil/Aero & Security, Info-com & Cyber, Transports and Industry.

PROXIMITY
Placing customer at the center of our concerns, we are totally committed in the success of your project.
• SME: human scale reactive company
• Dedicated responsive team to your project
• Worldwide support and cooperation agreements to serve our prime contractors and customers

INNOVATION
With a design department team of 15 engineers and technicians, innovation is at the core of ECRIN Systems' DNA, which devotes each year 7% of its turnover in R&D.

EXCELLENCE
Putting quality at the heart of our value system, we excel in offering you optimum continuity of operation and high return on investment (ROI) to improve your efficiency and productivity.
Management system based on quality processes: ECRIN Systems is ISO 9001:2015 qualified
Environmental Qualification and Compliance: MIL-STD-810, MIL-STD-461, DO-160, GAM EG 13, BV marine, CE, CB, FCC, UL...

COMMITMENT
Faithful in business, we seal trust agreements with our customers and partners to strengthen our relationship

CONTACT

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

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

EVIDIAN

Bull Evidian

Evidian, **European leader in IAM - Identity & Access Management,** offers a complete, integrated and modular identity and access management suite compliant with the company's security policy and with the new regulatory requirements (**GDPR**...). This offer is able to govern, administer and secure users' access to their applications from their arrivals to their departures. It strengthens their authentications and access rights from their digital environment and on all types of terminals. Evidian simplifies application access with a universal **Single Sign-On**.

More than 5,000,000 users in more than 900 organizations around the world connect with every day and manage their access rights with Evidian's identity and access management solutions.

IAM is a major component of information system security. The multiplication of data, applications and profiles of the people accessing them requires to govern in an optimal way the users' authorizations to relevant resources by controlling risks. To do this, we must gain the support of users and businesses and offer IT departments tools adapted to new use cases and to the development of services in the cloud.

Evidian covers all needs from the user's identity assurance, to the intelligence that operates on the life cycle management of their digital identity and their access from any terminal and to access all the resources of the organization:

- **Identity Governance and Administration**: identity management, entitlements and access
- **Identity Analytics and Intelligence**: monitoring and analysis of the IAM system use
- **Enterprise-SSO**: unique and secure password
- **Web Access Manager**: web SSO and Identity federation
- **Authentication Manager**: gestion des moyens d'authentification forte, management strong authentication tools.

More informations:
www.evidian.com and
https://atos.net/en/products

CONTACT

Sylvie BEC
Sylvie.bec@gemalto.com
+33 (0) 1 55 01 50 00

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

GEMALTO

gemalto
security to be free

Gemalto's SafeNet solutions ensure the security of identities and data, and their communication between organizations and people as well as devices in the fast-expanding Internet of Things. We protect and control access to sensitive information, secure data in virtual and cloud environments, safeguard transactions, manage risk and ensure compliance.

We ensure secure, simple access

Our easy-to-use multi-factor authentication solutions provide secure access to corporate networks and applications, and protect and validate the identities of users. Governments and many of the largest companies trust us to secure mission-critical information, control access, protect identities, ensure data ownership and safeguard communications.

We ensure trust in the cloud

Our authentication, encryption and key management solutions for the enterprise cloud create trusted, compliant environments by solving the key challenges of data governance, control and ownership. We also enable cloud service providers to enhance trust in their services with highly scalable and easy to deploy authentication- and encryption-as-a service offerings.

We protect data from interception and theft

Our data-centric encryption provides persistent protection of sensitive data whether at rest or in motion. From physical to virtual data centers, our solutions keep organizations protected, compliant and in control with encryption and key management products that secure sensitive data wherever it is. Our HSMs protect the cryptographic infrastructure of some of the world's most security-conscious organizations, providing robust encryption, decryption, authentication and digital signing services for a wide range of applications.

CONTACT

Yann GRIVET
commercial@icodia.com
+33 (0) 2 30 96 40 59

22 rue de l'Erbonière,
35510 Cesson-Sévigné

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

ICODIA

Strategically based in Rennes since 2000, Icodia owns its high-availability and secure data center.
Atypical actor of the market, Icodia develops his owns solutions necessary to the hosting services : security, supervision, decision-making environments, HMI ...

With strong R & D experience, continuous innovation and a genuine culture of IS security, Icodia is a best added value in the market. The meeting of network skills, software engineering, cybersecurity and IoT has made it possible to build a state of the art hosting platform.

Icodia's global offer is based on 3 main lines.

1/ Secured and supervised hosting offers, in its TIER IV data center:
Implementations of a very high availability systems offers you multiple guarantees. Our goal is to offer the package that best suits your needs. There are many technical possibilities : we advice you for the study and the design, and also for production and monitoring. The aim is to anticipate growth and minimise its detrimental impacts, by solving them before they appears.

2/ An R&D division focused on high availability and cybersecurity:
Our research and development department mobilizes all our teams. Our many contributions within open-source foundations allow us to maintain a permanent link with communities. We build together cybersecurity and intelligence systems, because we picture this as the future.

3/ Facilities management and auditing managed by the best specialists:
Regular maintenance and audits of your infrastructure are essentials. They guarantee fault management and early return to normal functioning.

CONTACT

Coralie HERITIER
info@idnomic.com
+33 (0) 1 55 64 22 00

175 rue Jean-Jacques Rousseau,
92130 Issy-les-Moulineaux

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

IDNOMIC

IDnomic is the leading European provider of trust services for the protection of digital identities.

IDnomic provides peace of mind for users who want to communicate, authenticate, and exchange confidential data safely:

- Employees who must have secure access to data from their multi-channel enterprise objects via any network, anywhere.
- Connected devices which must be deployed in a secure and monitored environment in order to be used with confidence by the general public.
- Citizens who need electronic identity and travel documents when traveling and to access secure e-government services.

IDnomic is a Trusted Third Party that provides PKI (Public Key Infrastructure) both in the cloud and on-premise.

Based on standards recognized by the French government as well as by many governments in Europe and throughout the world, IDnomic technologies provide the guarantee of services that have been certified by the most stringent authorities:

- PSCE / PSCO (Electronic certification service provider) qualification
- CC EAL 4+ certification
- NATO Secret classification
- ETSI certification
- France Cybersecurity Seal

CONTACT

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

51 boulevard Voltaire
92600 Asnières-sur-Seine

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

ILEX INTERNATIONAL

Ilex International is leading software vendor which has been specialising in Identity & Access Management (IAM) for more than 15 years.

Customers appreciate, in addition to the quality of Ilex technologies, the team's reactivity and ability to provide innovative and secure solutions combined with the commitment to quickly integrate new requirements driven by evolving technologies or regulations.

Ilex's recognised technical expertise and business-oriented product line have constantly met the needs of very demanding medium sized and large international organisations who consider IT security as paramount.

Over its 25 years of existence, Ilex International has built a strong and reliable network of specialised partners. Whether they are market leaders or highly specialised consulting firms with strong expertise in IT security, they provide our customers with complementary software or high level consulting and integration services.

CONTACT

Jean VILLEDIEU
jean@linkurio.us
+33 (0) 9 52 06 08 55

14 rue Soleillet,
75020 Paris France

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

LINKURIOUS

LINKURIOUS
VISUALIZE GRAPH DATA EASILY

Linkurious is a software company that designs and delivers a graph intelligence platform to detect and investigate threats such as computer fraud, cyber-attacks, or security breaches.

Dealing effectively with security breaches or cyberattacks remains a significant challenge for cybersecurity analysts. Today, increasingly complex networks and infrastructures generate terabytes of heterogeneous data in which it is difficult, sometimes impossible, to detect risks or unusual patterns. It is essential to reduce both the proportions and the complexity of the data produced to a more understandable level in order to find appropriate solutions and improve overall security.

WITH ITS ANALYSIS AND DATA VISUALIZATION SOFTWARE, LINKURIOUS OFFERS CONTEXTUALIZATION, SIMPLIFICATION AND SPEED UP YOUR INVESTIGATIONS TO IMPROVE YOUR ORGANIZATION SECURITY.

With its visualization technology, Linkurious Enterprise highlight connections between a multitude of data (system data, public vulnerability reports, logs, etc.)

The analysis and visualization of these graphs of data is an effective approach to understand and monitor dynamic, complex and multiple connections.

Linkurious helps analysts prevent existing risks and investigate security incidents. The analysis of dependencies within information systems allows to identify vulnerabilities and to anticipate threats. The analysis of the data related to an attack can help evaluate its nature and range in order to take the appropriate measures.

CONTACT

Christophe TREMLET
christophe.tremlet@maximintegrated.com
+33 (0) 4 42 98 14 80

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

MAXIM INTEGRATED

maxim integrated™

Maxim Integrated is a global semiconductor provider that has been involved very early in digital security: its first secure microcontroller has been launched in 1993. To meet increasing requirements in this area, Maxim Integrated keeps investing in embedded security solutions. Today, worldwide, around one payment terminal on three is protected thanks to a Maxim Integrated solution.

Through our authenticators circuits and secure microcontrollers, Maxim Integrated has one of the largest range of products in industry.

Recently, Maxim Integrated developed a ChipDNA PUF (Physically Unclonable Function) technology producing private keys to provide an unprecedented level of physical security.

Our integrated circuits are mainly designed for embedded systems. One of the main benefits for cybersecurity is the concept of "The root of Trust". To be secure, a system must be based on a trust physical element to build the security of the system. Our secure authenticators and microcontrollers are designed to be this root of trust.

CONTACT

Alexandre OSTAPOFF
sales@oikialog.com
+33 (0) 1 43 34 09 04

54 rue de Bitche
92400 COURBEVOIE

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

OIKIALOG

OïkiaLog

As a Cyber Security consultants team, OïkiaLog helps its customers at all the steps of their security projects.

SIEM/SOC
With more than 20 years of experience in the logs analysis domain (SIM/SEM/SIEM), the OïkiaLog's experts team has gained a unique expertise in these kind of projects.

The OïkiaLog's strength comes from a unique complementarity of its teams that combine 3 types of profiles:
logs analysis experts, developpers and integrators all of them having a strong skill in Cyber Security.

OïkiaLog can manage all phases of SIEM/SOC projects for its customers: from the definition of the need to SOC exploitation
through all intermediate steps such as looking for appropriate solutions, integrating, customizing, industrializing and
maintaining them in operational condition.

The research, definition and creation of relevant indicators in the customer's environment are also part of OïkiaLog's field of competence.

Expertise and integration in Cybersecurity
OïkiaLog resells and integrates a complete security offer:

- Firewall
- Vulnerability scanner
- SIM/SEM/SIEM
- Compliance and integrity checking
- Anti-spam
- Privileged Account Management
- IAM

Service, security audit, specific development and training

OïkiaLog helps its customers to prepare their security project through the analysis of the current state
and the deduction of specific needs, the help in choosing the right solutions (enrichment of what already exists, custom developments or use market solutions).

OïkiaLog also helps its customers to evaluate their level of security through different types of intrusion tests.

OïkiaLog can deploy the solutions it recommends. This integration is carried out according to a proven methodology for managing these types of projects. Such a mission is entrusted to a team composed of a project manager and various technical experts combining strong skills in security solutions deployment and in the creation of custom components in many development languages.

OïkiaLog provides Cyber Security trainings as well as custom modules adapted to the needs of its customers.

CONTACT

Laurent NOE
laurent.noe@oveliane.com
+33 (0) 6 61 16 83 97

54 rue de Bitche
92400 COURBEVOIE

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

OVELIANE

Oveliane

FRANCE CYBER SECURITY

Nowadays, the context of security is very tense: the attackers, always more creative and obstinate, regularly find ways to bypass the prevention technologies set up by the computer security teams to stop them.
Most attacks, and especially APTs, have similar effects on their targets: server connections, privilege escalation, account creation and configuration alteration.
Therefore, the lack of server side security monitoring will have dramatic consequences!

The main two categories of security tools reach their limits here:

- Perimeter protection tools, essential but insufficient
- Attack detection tools forced into a permanent race behind the attackers.

Created by OVELIANE, OSE offers another approach: rather than tracking attacks, let's monitor their targets. OSE unmasks illegal actions (APT):

- Alteration of system components and applications
- Detection of unusual or unjustified network flows
- Appearance of new processes.

OSE allows to:

- **Protect thanks to an integrity monitoring** : tightness and monitoring of sensitive files, new and missing resources, control and monitoring (logs, alarms), ...
- **Detect dangerous or prohibited services** : misconfigurations, inconsistencies, abnormal access rights, weak passwords, suspicious directories and files, file modifications, illegitimate or suspicious network accesses to servers, ...
- **Deploy the enterprise security policy** on all Unix, Linux, and Windows servers in the organization: white and black lists of ports/services, list of sensitive files, restrictions on shared files, password strength policy, network filtering policy to access the system and applications...
- **Monitor systems compliance :** Standards and ANSSI recommendations.

CONTACT

Nicolas BACHELIER
nicolas.bachelier@primx.eu
+33 (0) 1 77 72 64 80

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

PRIM'X

PRIM'X
CORPORATE ENCRYPTION SYSTEMS

FRANCE CYBER SECURITY

PRIM'X is a Software Editor in the field of IT security (CyberSecurity) and more particularly in the area of Encryption.

For better protection of sensitive data, against loss, theft, publication and economic espionage, PRIM'X introduces a new way of using encryption within an organisation. Data is everywhere and widely disseminated. Classifying a company's information is a difficult task; and this information is not given as much value as an enemy would, causing it to be vulnerable. For these reasons, a global policy must be adopted: **Encrypt Everything, Everywhere, and Always.**

For PRIM'X, encryption must be GLOBAL, SIMPLE and TRANSPARENT, AUTOMATIC and SECURITY POLICY-DRIVEN. This also allows the application of RIGHT-TO-KNOW (cryptographic partitioning), even within the organisation that implements it, between users/services and particularly where technical operators are concerned.
PRIM'X's customers are mainly Key European Accounts, as well as Administrations and Ministries that have opted for massive equipment with PRIM'X software (the French state at the end of 2015 and the Council of the European Union in 2017).

PRIM'X's solutions have received the following labels:

- EAL3+ Common Criteria Certifications,
- Standard-Level Qualification from the French State (ANSSI) & French CyberSecurity Label,
- Qualified for protecting data marked DR (Restricted Distribution), NATO Restricted, EUROCOR Restricted and EU Restricted.
- Registered in the NATO catalogue and the EU's catalogue of cryptographic products
- Approved by the Council of the European Union for the protection of data marked EU Restricted

ZoneCentral
File and folders Encryption: user workspace, file servers, shares, USB devices, etc.

Orizon
File and folder Encryption for Cloud spaces.

ZonePoint
Document Encryption for Microsoft SharePoint® libraries.

Zed! and ZedMail
Encrypted bags for exchanges, archives, messages, etc.

Cryhod
Disk encryption with pre-boot authentication.

CONTACT

Eléonore FORGET
eforget@riskeco.com
+33 (0) 1 55 24 23 16

«38 rue Jacques Ibert
92300 Levallois-Perret»

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

RISK&CO SOLUTIONS

The Risk&Co group was created in 1994 and has worked its way up to become one of the leading French and world players in risk engineering and management.

The Group is currently active in three major fields:

- The tradition business of strategic intelligence and safety consultancy for critical infrastructure (Risk&Co)
- Cyber security and safety engineering (Risk&Co Solutions)
- Onshore and offshore mine clearance and stockpile management (Geomines).

The group, in each of the fields, offers comprehensive solutions including risk diagnosis and preparation and operational roll-out of master plans on-site.

Risk&Co Solutions is the technological subsidiary of the Risk&Co group.

Our mission involves securing the physical and data integrity of sensitive infrastructure of our clients both project managers and prime contractors alike. This is achieved through safety audits, consultancy and engineering services.

We have worldwide references backing our expertise in a variety of key sectors (energy, defense, industry, etc.) as well in system types (industrial systems and security/safety systems).

Our versatile teams of experts and cyber specialists provide services including threats and vulnerabilities identification (audits and risk analysis), risk mitigation (action plans, governance), certification and regulatory compliance.

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

RUBYCAT

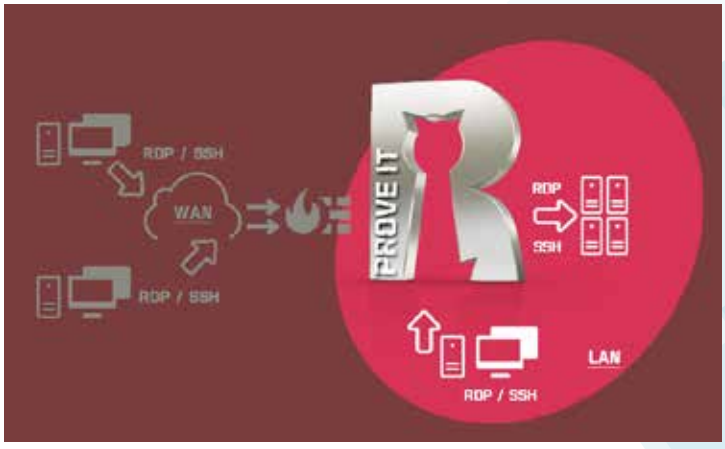
RUBYCAT-Labs is an innovative software company based in Brittany, France. It specialises in sensitive access control and traceability within Information Systems.

Your servers contain sensitive data and/or applications that must be protected in order to ensure the continuity of your business and the sustainability of your company:

- All actions on a critical server must be monitored, traced and easily identifiable.
- All persons granted privileges must be clearly identified and their access restricted. The PROVE IT software solution from RUBYCAT-Labs addresses the issues of Monitoring and Auditability of critical access within Information System resources. This centralised access portal to resources also provides a pragmatic and simple answer to the management and traceability of access to sensitive data, particularly within the context of regulatory compliance (for example for the application of the General Data Protection Regulation - GDPR).

The PROVE IT software module is intuitive, flexible and non-invasive and easily interfaces with the existing environment (no agent installation on client computers or target servers required). It provides native interfacing with logging hubs and security information and event management solutions (SIEM). The PROVE IT solution can be deployed in companies of all sizes (medium sized firms, SMEs, SMIs) and in any sector impacted by issues of traceability and monitoring of users with privileges, including public authorities, industry, retail, hosting and healthcare.

www.rubycat-labs.com



CONTACT

Sergio LOUREIRO
sales@secludit.com
+33 (0) 4 92 91 11 04

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

SECLUD IT

SecludIT helps companies to improve their Cloud security with a preventive approach to risk: continuous and automatic detection.

SecludIT is a French software company who identifies security vulnerabilities on virtualized, cloud and hybrid infrastructures.

Pioneer of Cloud infrastructures security, founding member of the Cloud Security Alliance, SecludIT is a worldwide recognized player for its technologies proven results and cyber risk management approach. SecludIT provides security services and software to help to secure infrastructures and data, Web and e-commerce sites.

The SecludIT teams help companies in their digital transition and in particular in their migration to a cloud infrastructure. Because of the security needs are not the same as for a physical infrastructure, they must choose a suitable solution in order to reduce the risk of cyber-attacks.

Thanks to our Cloud analytics solution, you could:

- Using a unique Analytics solution with several clouds
- Discovering automatically all our IT assets (servers, cloud Workloads, networks, …)
- Cloning your servers to analyze them without impact on production
- Detecting continuously your vulnerabilities
- Checking IaaS best security compliance
- Downloading relevant and comprehensive reports
- Monitoring continuously our cyber risk exposure thanks to our GDPR/ANSSI, OWASP et PCI DSS risk indicators
- Following a simple action plan with our advice

“France Cybersecurity” label:
SecludIT has been received the “France Cybersecurity” label awarded by users and the government, which rewards the quality and performance of our Cloud Security Analytics solution.



CONTACT

David BIZEUL
david.bizeul@sekoia.fr
+33 (0) 6 64 45 84 29

18-20 Place de la Madeleine,
75008 Paris

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

SEKOIA

SEKŌIA

SEKOIA, it's 50 employees, 4M€ turnover, 25% R&D, 200 trained security professionals each year.

Since 2008, the company has been providing cybersecurity consulting, expertise and innovations to respond to the challenges of a volatile, complex and ambiguous world. Our customers are major French and European companies.

Some examples of success stories obtained in 2017 :
• Design a turnkey security monitoring solution;
• Handle efficient NotPetya incident response;
• Simulate a targeted attack to evaluate detection and reaction processes;
• Build a complete threat intelligence capability;

We assist our customers through our 4 complementary pillars:

• Consulting to design, structure or rethink the organization of security and support companies in their strategic choices, by enabling them to identify assets and their weaknesses, particularly in the following areas: digital transformation of companies, security, RGDP compliance, risk analysis.
• A dedicated SEKOIA training center is in place since 2008. It increases the skills and certification level of companies and individuals on all topics related to IT security. 30 courses are available and 200 students are trained each year, .
• Expertise to focus on the most complex topics, particularly for defensive and offensive security.
On the defensive side, SEKOIA offers its CERT to mitigate incidents. Threat intelligence capabilities are also available to our customers to limit exposure on future threats.

On the offensive side, SEKOIA has an internal team of experts specialized in technical audits and penetration testing activities. Targeted attack simulation, hardware pentest, API evaluation, protocol analysis are part of the capabilities.

• A range of products in SaaS mode that simplify the use of security:
o **inThreat:** Threat Intelligence (inThreat.com)
o **DediMISP**: information sharing (dedimisp.com)
o **FastIR:** forensics investigations (fastir.com)
o **Vudip:** vulnerability detection
o **ViralStudio:** malicious code analysis
o **WotchR:** cybersurveillance

All these products are distributed either directly via https://sekoia.io or on MSSP mode.

CONTACT

Stéphanie JEGAT
s.jegat@siepel.com
+33 (0) 2 97 55 73 74

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

SIEPEL

In 1986, SIEPEL, a French private company, set up its headquarter and workshops in La Trinité-Sur-Mer (FRANCE).

Our core business is the cyber security of the infrastructures.

Against the threats of eavesdropping and intentional electromagnetic attacks such as: Electromagnetic pulses, Nuclear Electromagnetic pulse, High Intensity Radiated Fields (HIRF); we secure information systems and datacenters as well as meeting rooms.

SIEPEL's expertise is based on our technical capabilities, and on the continuous ambition to improve our operational flexibility. Many references (governmental institutions and private companies) attest of these specific know-hows.

Two France Cybersecurity labels (high-performance Tempest shielded rooms in 2016 and Shielding effectiveness measurements in 2017) recognize these professional skills and experience.

SIEPEL owns a security clearance which has been delivered by the French Administration and acknowledged by the EU and NATO.

CONTACT

Jean-Luc GIBERNON
jean-luc.gibernon@soprasteria.com
+33 (0) 6 81 27 86 52

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

SOPRA STERIA

A European leader in digital transformation

2016 revenue | employees | sites

TOP 5 of european players

Sopra Steria is a European leader in digital transformation with 2016 revenues of €3.7bn and 40,000 collaborators based in over 20 countries. The group provides one of the most comprehensive portfolios of end to end services in the market including Consulting, System Integration, Software Development, Infrastructure Management and Business Process Services.

Present across nearly all sectors of economic activities – industry, services, telecommunications and banking – the group has significant and well regarded expertise in the aeronautics, naval and nuclear industries. It is able to offer specific software solutions including design, development and maintenance and hence meet leading private and public organisations' demains in terms of development and competitiveness.

In addition, Sopra Steria Group has a strong foothold in the Defense and Security sector with expertise in the provision of operational and logistics information systems to the armed forces as well as critical software outsourcing in the field of homeland security.

The group has also developed tailored structures and specific skills capable of meeting challenges experienced in highly sensitive projects relating to Government issues.

CONTACT

Sylvie WUIDART
+33 (0) 6 85 81 24 26
sylvie.wuidart@st.com

ZI de Rousset BP2 13106 Rousset
Cedex - France

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

STMICROELECTRONICS

life.augmented

FRANCE CYBER SECURITY

ST is a global semiconductor leader delivering intelligent and energy-efficient products and solutions that power the electronics at the heart of everyday life. ST's products are found everywhere today, and together with our customers, we are enabling smarter driving and smarter factories, cities and homes, along with the next generation of mobile and Internet of Things devices.

By getting more from technology to get more from life, ST stands for life.augmented.

In 2017, the Company's net revenues were $8.35 billion, serving more than 100,000 customers worldwide. Further information can be found at www.st.com.

CONTACT

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

1 place Verrazzano
69009 LYON

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

STORMSHIELD

STORMSHIELD

A European leader in digital infrastructure security and a wholly owned subsidiary of Airbus CyberSecurity, we offer intelligent, interconnected solutions to anticipate attacks and protect IT and OT digital infrastructures.

Our mission: to ensure cybersecurity and data protection for organisations, their employees, and their customers.

We offer our expertise in three complementary product ranges to guarantee unbreachable security:

- Protection of computer and industrial networks **(Stormshield Network Security)**;
- Protection of workstations and servers **(Stormshield Endpoint Security)**;
- Protection of data **(Stormshield Data Security)**.

Using our Multi-Layer Collaborative Security approach, our three product ranges interact to reinforce the level of protection of IT, OT, and Cloud environments, regardless of the point of attack.

NETWORK SECURITY

ENDPOINT SECURITY

DATA SECURITY

These trusted, state-of-the-art solutions have earned Europe's highest certifications (EU Restricted, NATO, ANSSI EAL3+/EAL4+). With our network of distribution partners in more than 40 countries, we protect the strategic information of companies of all sizes, government agencies, and defence organisations throughout the world.

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

SURYS

SURYS

Global reference in the field of security, SURYS offers a wide range of optical and digital solutions to authenticate, track & trace documents to fight against fraud and forgeries. SURYS has recently developed the concept of "optical chip" capable of authenticate, identify and securely connect genuine document and consequently people to the digital world.

The ever more frequent needs for self-identification to access digital services had led SURYS to engineer the Photometrix™ solution to support Governments and Clients in the cultural change toward virtual identity. The Photometrix™ solution enables a dematerialization of identities and is an optimal hybrid solution in term of costs and easiness of implementation towards virtual identity.

Photometrix™ is an innovative mix between a picture and a 2D barcode which allows an offline automated authentication of the card holder's portrait. The Photometrix™ code is generated thanks to an encoding mechanism based on specific characteristics of the picture, some personal details (name, date of birth, etc..) as well as biometric information. These elements are then compressed to represent only few bytes of information in order to optimize the space required on the document.

The control is performed via a digital support (Smartphone, Tablet, etc..) both on physical and dematerialized document. The control of the Photometrix™ code is performed using a dedicated app that can control either a physical or a dematerialized code for an even greater flexibility in use and a higher security level.

The Photometrix™ acts as a secured access to the digital world opening a door to its myriad of opportunities

CONTACT

Antoine COUTANT
a.coutant@systancia.com
+33 (0) 3 89 33 58 20

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

SYSTANCIA

Systancia

Systancia is a recognized European software vendor in virtualization, security, and digital confidence, offering the next generation of application delivery infrastructure, focused on users and security: SBC and VDI, external access security, Privileged Access Management (PAM), SSO and Identity and Access Management (IAM).

Leveraging innovation as a growth engine, Systancia relies on the technological value of its products and the proximity between its teams and its customers to meet the needs of users, enabling it to achieve 98% customer satisfaction.

Systancia R&D department works daily to improve user experience and security in terms of access to applications. Systancia was the first software editor to implement machine learning technologies in its solutions to predict the end user behaviour to guarantee real-time access to applications or to detect suspicious behaviour in real-time to hold back cyberthreats.

Systancia benefits from a real recognition, proved by the “Qualification” that ANSSI delivered to its cybersecurity solution, which makes that solution the only solution that the national agency for IT security recommends for identification, authentication and access control.

CONTACT

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

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

TEHTRIS

TEHTRIS Company is "**eGambit**" awarded solution editor, a defensive cyber-weapon system.

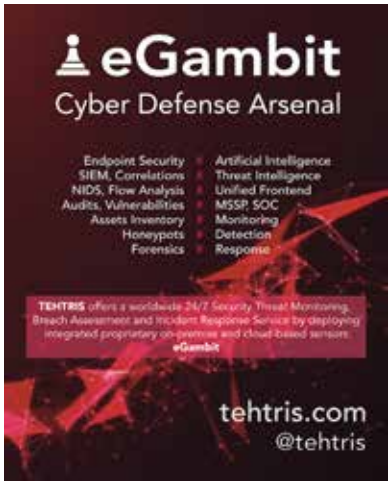
While malicious Internet intrusions and attacks are on the rise with infiltrations from all sides, **TEHTRIS** Company based near Bordeaux (France), offers a solution, a Cybersecurity Product Excellence Award winner, to enhance IT Security in large scale infrastructures: **eGambit**.

TEHTRIS is a French company founded in 2010, specialized in cutting-edge IT security technologies. Its consultants know, understand and master attackers techniques and methods: hackers, business intelligence, computer warfare, etc, as well as the resources needed to counter the current threats.

TEHTRIS team has more than 15 years of experience in sensitive environments or crisis situations worldwide. Therefore, it can ensure efficiency, discretion, trust and above all confidentiality, for all your protection specific requirements or standards.

Its innovative Artificial Intelligence engine, which is embedded in **eGambit**, was just awarded by a recognized independent testing company, as TEHTRIS won the best solution Award in the "Real Time Threat Analysis" category. It is also part of VirusTotal. As an example, eGambit Artificial Intelligence can detect unknown viruses or malwares as it is not based on signatures.

In 2015, TEHTRIS already won the "Label France Cybersecurity", then an innovation prize during the "IT Innovation Forum" in 2016. In 2017, an American magazine appointed eGambit amoung the 10 best EndPoint solutions worldwide. eGambit is offered to the French public sector through the central public purchasing office called UGAP.



CONTACT

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

Arep Center - 1, traverse des Brucs
06560 Valbonne

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

TEXPLAINED

Texplained
HARDWARE SECURITY INSIGHT

FRANCE CYBER SECURITY

Expert in Microchips Security, Texplained offers Solutions & Services to fight against Hardware Piracy and Counterfeiting.

The French Company designs and markets tools for IC security evaluation and improvement:

- EVALUATION TOOL: Texplained's Reverse Engineering software – ChipJuice - allows in-depth exploration and analysis of any type of IC. With ChipJuice, one can digitally recover the chip into different formats - Netlist, VHDL files, GDSII – by using only the high resolution images of its internal structures. ChipJuice will be available on the market mid 2018.

- HARDWARE PROTECTION MODULES: Texplained has created and filed a patent for a digital module that protects ICs against code extraction: the IP detects the attack on the fly and immediately reacts to stop it.

In addition, thanks to its Trainings and Services, Texplained accompanies Chip Makers and Buyers as well as Governments at every stage of their electronic devices lifecycle, from their design to their manufacturing and their obsolescence management.

Different types of Services are offered:

- Secure IC Architecture & Design counseling
- Secure IC Risk Assessments
- Hardware Backdoors research
- Pirate device analysis and support on the improvement of the security of current and next-gen products
- Exploration and comparison of competitors chips in case of IP infringement suspicion, helpful in a trial
- Analysis of obsolete & not documented ICs and emulation of the functionalities on a new target.

With its unique expertise on real world attacks, and its disruptive and efficient methodology, Texplained's expertise on chips security applies to all types of applications: Banking, e-Gov, IoT, Automotive, Medical, Consumer, Military, etc.

CONTACT

Didier VIRLOGEUX
didier.virlogeux@thalesgroup.com
+33 (0) 6 08 61 67 33

4, Avenue de Louvresses
92622 Gennevilliers

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

THALES

THALES

Thales is one of Europe's leading players in the cybersecurity market, and the world leader in data security. With 64,000 employees in 56 countries, Thales reported sales of €14.9 billion in 2016. With over 25,000 engineers and researchers, Thales has a unique capability to design and deploy equipment, systems and services to meet the most complex security requirements. Its exceptional international footprint allows it to work closely with its customers all over the world.

In response to the sharp rise in cyber-related threats, Thales acts as a trusted partner for defense organizations, government bodies, critical infrastructure operators, and industrial and financial companies.

With a presence throughout the information security chain, Thales offers a comprehensive range of services and solutions ranging from security consulting and audits, data protection, digital trust management, cybersecured system design, development, integration, certification and through-life management to cyber-threat intelligence, intrusion detection and security supervision, with Security Operations Centers in France, the United Kingdom, The Netherlands, Canada and Hong-Kong.

By choosing Thales, you benefit from:

- A team of 5,000 critical IT engineers.
- A reliable partner with more than 40 years of experience protecting classified information up to Top Secret level.
- A global player with products and solutions deployed in more than 50 countries.
- An experienced, trusted service provider ensuring management and supervision of critical information systems for more than 100 customers.

Our customers include:
- 19 of the world's 20 largest banks,
- 4 out of the 5 largest oil companies,
- 27 NATO member states.

CONTACT

Jérôme CHAPPE
jerome.chappe@thegreenbow.com
+33 (0) 1 43 12 39 32

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

THE GREENBOW

THEGREENBOW

FRANCE CYBER SECURITY

TheGreenBow is a French Software editor specialized in Data Communication security.

Located in central Paris since 1998, TheGreenBow represents a unique skill set associating the highest level of security and best of breed ergonomics. TheGreenBow Software products are distributed worldwide and appreciated for their stability, reliability and their user-friendliness. TheGreenBow provides solutions for securing remote network connections (VPN).

With over one million licenses distributed worldwide, 15 years of experience in building reliable IT security solutions for corporate businesses and government agencies and a successful Common Criteria EAL3+ certification, TheGreenBow is a leading provider of trusted and scalable Cybersecurity solutions for SMBs, large accounts, government agencies and strategic operators worldwide.

TheGreenBow solutions are referenced in the NATO and EU certified products catalogs.
They are also referenced in the UGAP and Ouranos catalogs.

TheGreenBow is a founding member of HexaTrust, member of the competitive cluster Systematic, member of the Cybersecurity workgroup within the government plan “New Industrial France” and founding member of ECSO.

CONTACT

Jean-Louis GUIDOR
jlguidor@tracip.fr
+33 (0) 6 45 47 24 22

6 rue Robert Schuman
54850 Messein

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

TRACIP

TRACIP
Technologies & Services d'Investigation

TRACIP is the primary partner of government agencies in the field of Police, Defense and Justice in their fight against cybercrime.

Its know-how in the making of digital investigation and recovery of sensitive data laboratories enabled TRACIP to provide turnkey solutions including audit, equipment, training and support to federal agencies.
From this trusted partnership emerged, among other, the mobile laboratory concept - mobil'IT®- which responds to a growing operational need of cyber investigators.

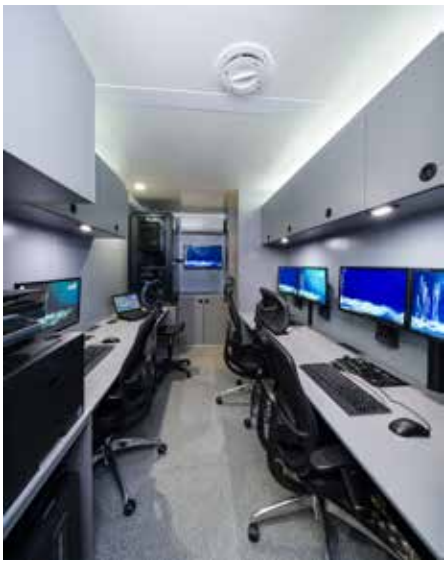
mobil'IT® is a powerful, fully mobile and autonomous digital investigation laboratory which drastically accelerates field investigations with specialized, ergonomic and powerful equipment.

Due to its strong experience in the conception and the production of a range of mobiles laboratories, TRACIP has been awarded the exclusivity to produce and market worlwide a DNA mobile laboratory, result of the know-how of the Forensic Research Institute of the National Gendarmerie (IRCGN™) and approved in France by the DNA National Committee .

The patented innovation that led to the creation of this laboratory offers researchers the opportunity to analyze DNA traces in 2 hours for the first 21 samples, directly on site, when one day is usually required, all of this with 24 markers extracted simultaneously. The analysis is even accelerated on the following analyzes, as 21 profiles emerged every 30 minutes thereafter.

Benefits of mobil'DNA:

Drastically accelerates the process of quantifying and identifying victims in the event of a disaster
Allows rapid delivery of the DNA profile of a suspicious person or victim
Significantly limits the risk of contamination when handling seals
Important savings with a cost per analysis significantly reduced
The DNA laboratory is a proven technology, implemented by the French Gendarmerie in the handling of critical cases.



CONTACT

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

28 rue Jean Rostand
91400 Orsay France
www.vocapia.com

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

VOCAPIA RESEARCH

VOCAPIA research

Making raw audio searchable

Vocapia Research develops leading-edge speech processing technologies that can be used for many applications. Our VoxSigma software suite is designed for professional users needing to process large quantities of audio data.

Faced with the massive amounts of multilingual audio and video data generated in the digital sphere, it has become necessary to dispose of more and more powerful tools to extract and analyze the pertinent information located within this data. Vocapia provides high performance tools to facilitate the work of data analysts, that can be used in the judiciary contexts or the fight against crime and terrorism.

Our systems target two types of data: broadcast speech and conversational telephone speech, and cover most European languages, as well as Arabic, Mandarin, Russian, Pashto...

Our vision
to help governmental agencies process large quantities of multilingual audio data in the workflow of open-source or communications intelligence activities (OSINT & COMINT).

Media monitoring and audio indexing
Our Voxsigma software allows users to process and filter large quantities of audio in order to quickly access contents of interest.

Analysis of phone calls
Our speech processing systems convert the raw audio into structured textual documents that are easily searchable and analyzable.

Speech transcription
Our automatic speech-to-text software can be used to significantly reduce the production time of minutes and exact transcripts.

CONTACT

Edwige BROSSARD
ebrossard@wallix.com
+33 (0) 1 53 42 12 81

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

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

WALLIX

WALLIX
TRACE, AUDIT & TRUST

FRANCE CYBER SECURITY

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NIST/NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.
WALLIX offers packages and modules which easily integrate into existing technical environments and evolve along with businesses' cybersecurity challenges. Secure access and/or passwords to data and systems, and adapt the WALLIX Bastion platform to unique business needs. Working with WALLIX and their network of integrators enables businesses to:

- Reduce risk by analyzing privileges accounts and their weaknesses
- Take decisions and act quickly against potential internal or external threats
- Tailor privileged account management according to sector of activity (Healthcare, Industry, Government, Finance, etc.)
- Adapt the solution to the technical architecture (including Cloud migration), facilitating increased flexibility, productivity, and performance

WALLIX is the first European cybersecurity software vendor to be publicly traded and can be found on EuroNext under the code ALLIX. As one of the leaders of the PAM market, up to 540 major players trust WALLIX to secure access to their data. WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, BPI Excellence, and Pôle Systematic.

CONTACT

Sabrina GUIDICELLI
sguidicelli@wooxo.fr
+33 (0) 4 42 01 65 73

OFFER CATEGORY

POSITION IN THE CYBERSECURITY CYCLE

TYPE OF SOLUTION

WOOXO

WOOXO
IT security for business continuity

FRANCE CYBER SECURITY

Wooxo is a French software publisher since 2011 which provides business security and continuity solutions for all-sized companies. We Backup business data against all types of damages: Physical, Human errors and Cyber threats.

Wooxo offers a "France Cybersecurity" labelled full backup and recovery service. Combining hardware, software, hosting, monitoring and care, it's a ready-to-go package for all-sized organizations in all Europe.

Compliant with the highest requirements in terms of security and confidentiality, our solutions can host sensitive data (regarding health, insurances, etc.) and follow the conditions of the new General Data Protection Regulation (GDPR).

Wooxo teams work to insure an effective Disaster Recovery Plan, increase awareness of companies on cyber threats and gather a community of committed business partners to fight against cybercrime.

The **Yoonited Against Cybercrime program, launched in 2017 has 3 main ideas:**

- To **Inform** and train executives and employees to the good practices of IT security. We freely share cyberattack alerts, white papers, manuals and practical guides. We also have thematic events about "Cybersecurity issues and challenges" to warn about cyberattacks and promote those good practices.

- To **Advise** business executives with a cybersecurity experts team which offers a free personal check-up. After listening to your issues on IT security matters, they give you concrete solutions to protect your activity.

To equip SMEs with customized solutions and monitor them through all the process to ensure the effectiveness of their backup.

Winner of several awards ("Les Succès du Numérique 2017" – Digital Success 2017, "Les trophées de la Distribution 2017" - Trophies of Distribution, etc.) Wooxo is also member of **Hexatrust, Cybermalveillance.gouv.fr, Transition Numérique and the French Tech.**
A company desperately needs its IT system running. Our Job is to protect it.

The Alliance pour la Confiance Numérique (ACN - Alliance for Digital Trust) represents organizations (world leaders, SMEs and mid-sized enterprises) in the digital trust sector, particularly those specializing in cybersecurity, digital identity, secured communications, traceability / anti-counterfeiting and safe city. In this field, France boasts highly efficient industrial cooperation and internationally recognized excellence thanks to world leaders, SMEs, mid-sized enterprises, and the various dynamic actors in the sector. Currently about 850 organizations in France generate a profit of almost 9 billion Euros in this rapidly growing sector (growth of more than 12% every year since 2014). ACN is a member of the Fédération des Industries Electriques, Electroniques et de Communication (FIEEC- Federation of Electric, Electronic and Communications Industries) and therefore actively participates in the work of the CoFIS committee (Comité de filière des Industries de Sécurité). ACN is also a founding member of the ECSO (European CyberSecurity Organization).
www.confiance-numerique.fr

The FIEEC is a federation of 22 professional trade unions in the electrical, electronics, digital and durable consumer goods industry sectors. The sectors that it represents include more than 3000 businesses, employ nearly 420 000 employees, and generate more than €98 billion in revenue, 46 % of which is from exports. At the source and core of digital transformation, member associations of the FIEEC coordinate companies that provide digital security technologies and solutions (digital identity, cybersecurity, traceability, physical security/access control, video surveillance, etc.) as well as companies that integrate these technologies and solutions into their «smart» product offerings (smart grids, smart industry, smart building, smart city smart health, smart mobility, smart life, etc.).
www.fieec.fr

GICAT, a professional group, created in 1978, has over 200 subscribers, representing some 330 members, corporations, mid-market companies and SMEs. These members cover a wide range of industrial, research, service and consulting activities for military and civil organizations, of national or international scope, involved in land and/or air-land security and/or defense. GICAT represents the interests of French land and air-land defense and security industrial players based on four objectives:

- Organizing dialog between the institutional and industrial players of the sector
- Offering services to its members to encourage their development in France and abroad
- Creating an environment favorable to exchange between industrial players
- Developing the industrial expertise and image of the sector

The international ambitions of GICAT are reflected in its international exhibitions, EUROSATORY in France, APHS in Singapore, Expodefensa in Colombia and ShieldAfrica in Ivory Coast, organized by its subsidiary, COGES, and a certain number of other defense and/or security exhibitions overseas.
www.gicat.fr

HEXATRUST was established by a group of French SMEs, mid-sized enterprises, and complementary players specializing in information system security, cybersecurity and digital trust sharing a common desire to pool their expertise.
Publishers and integrators of innovative solutions representative of French excellence, they joined forces to provide a range of high-performance, consistent and comprehensive products and services that secure critical infrastructures. This alliance meets the needs of corporations, administrations and organizations of all sizes, in both the public and private sectors, that seek to reap the benefits of innovative, French-made product offerings that cater to all their information security requirements. Encouraged by their foothold in the European market, the members of HEXATRUST also wish to speed up their international expansion by sharing their experience, networks and resources for accessing markets worldwide.
www.hexatrust.fr

réalisé en lien avec :

The GICAT and FIEEC are founding members of the CICS. This brochure was produced as an initiative by the Conseil des Industriels de la confiance et de la sécurité (CICS -Trust and Security Industry Council). The CICS represents the national security industry. It operates on the entire security perimeter (devices and platforms, electronic and digital systems, cybersecurity) and aims to develop common positions among associations in the security industry. Through its members (FIEEC, FFMI, GICAN, GICAT, GIFAS, USP Technologies and AN2V), the association makes up more than 80% of the French security industry. www.cics-org.fr

The French Prime Minister set up the COFIS (French security industry) committee in October 2013. Its mission is to coordinate the efforts of the state, territorial authorities, industry, research and major public and private operators to develop effective and internationally recognized security solutions. The industry operates within a buoyant international market that covers areas as diverse as the protection of large private and public infrastructures, transport security, border control, rescue missions, anti-terrorism and organized crime, crisis management and cybersecurity. Like all government-backed industrial committees, COFIS aims to increase the competitiveness of our major groups and SMEs, which are at the forefront of the security market.