SAFETY-SECURITY DIRECTORY

– EDITION 2021 –

MINALOGIC
Auvergne-Rhône-Alpes

2020 has seen a massive change in the way we work, the way we do business and the way we live our lives. Undoubtedly, the Covid-19 crisis has been a catalyst for a great number of these changes, especially in terms of security. From health, in terms of the protection of personal data to economic security, in terms of both cybersecurity and digital sovereignty to security in the workplace, meaning working from home and the return to the workplace, security is at the forefront of everyone's minds.

The recent cyberattacks against Colonial Pipeline and the Irish health service's computer systems, creating major disruptions in day-to-day lives, remind us of the vulnerability of critical and healthcare infrastructures.

These examples of attacks are high-profile examples of the kind of assaults that companies, schools, hospitals and other organizations deal with every day, worldwide.

The attacks have only increased during the pandemic when a shift to remote work created even more opportunities for hackers.

Cybersecurity is one of the five themes addressed in this safety – security directory which includes:

- Videoprotection - surveillance,
- Cybersecurity - digital security,
- National security and safety - risk and crisis management - civil security
- Health security
- Economic security

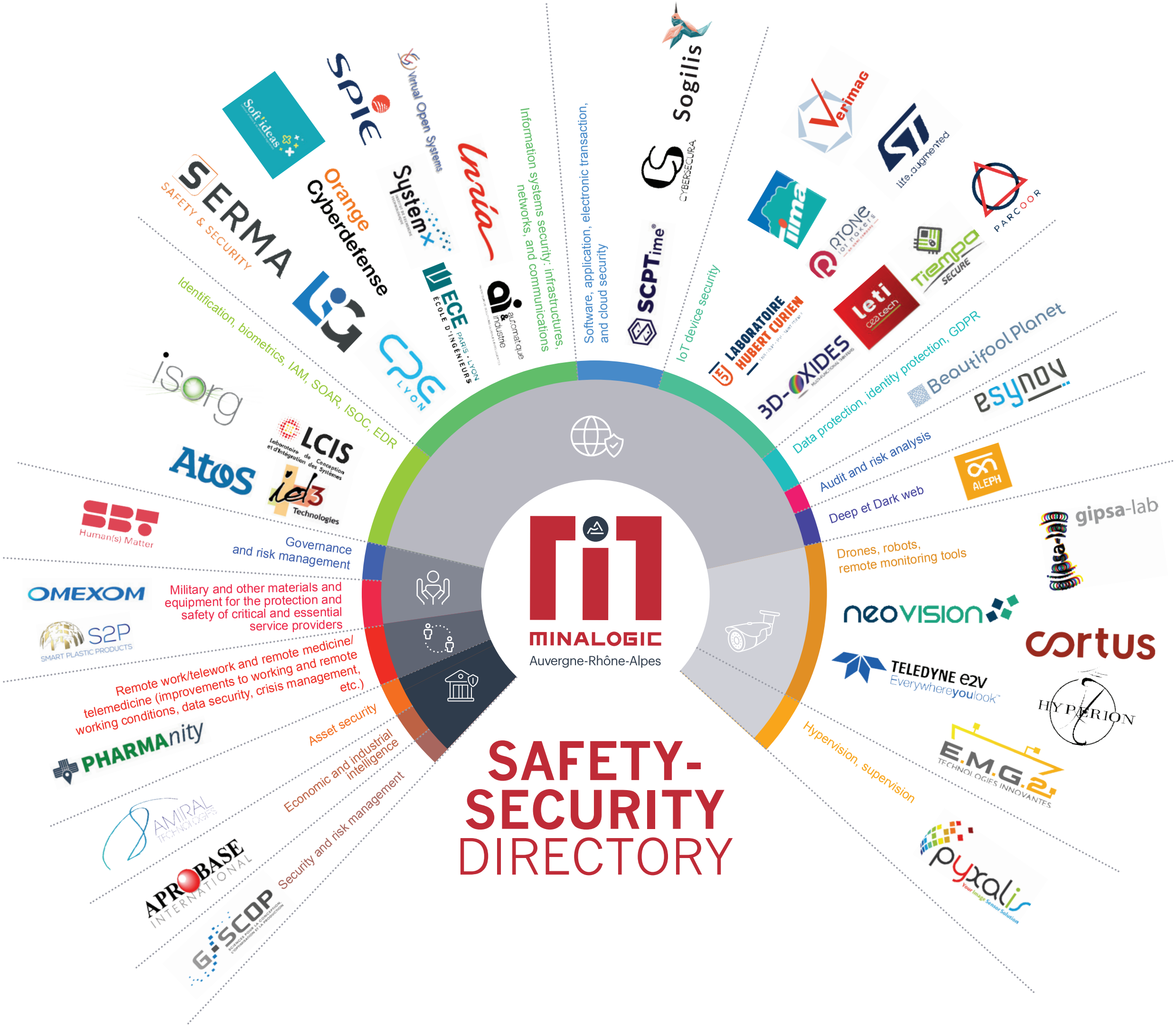
Minalogic is a global innovation cluster for digital technologies based in France's Auvergne-Rhône-Alpes region. We have more than 450 members, including 360 companies of which 330 are innovative SMEs/start-ups as well as cutting-edge research labs and universities in the digital technologies area.

These structures work with digital technologies to address a number of end markets, including security.

In this directory, you will find a panorama of Minalogic's companies and labs with competencies addressing security. This is a first version, which is going to be enriched over time. Our ecosystem is undeniably rich and has a lot to offer.

More than ever, there is an urgency to build a safer digital society.

SAFETY-SECURITY DIRECTORY



MINALOGIC
Auvergne-Rhône-Alpes

Identification, biometrics, IAM, SOAR, ISOC, EDR
isorg, LCIS Laboratoire de Conception et d'Intégration des Systèmes, Atos, ied3 Technologies

Information systems security: infrastructures, networks, and communications
SERMA SAFETY & SECURITY, Soft'ideas, SPIE, Orange Cyberdefense, Systemx, Virtual Open Systems, Inria, ECE ECOLE D'INGENIEURS PARIS · LYON, ai automatique & industrie, CPE LYON

Software, application, electronic transaction, and cloud security
Sogilis, CYBERSECURA, SCPTime®

IoT device security
Verimag, life.augmented, PARCOOR, lima, RTONE, Tiempo SECURE, leti ceatech, LABORATOIRE HUBERT CURIEN, 3D-OXIDES

Data protection, identity protection, GDPR
Beautifool Planet

Audit and risk analysis
esynov

Deep et Dark web
ALEPH

Drones, robots, remote monitoring tools
gipsa-lab, neovision, cortus, TELEDYNE e2v Everywhereyoulook™, HYPERION

Hypervision, supervision
E.M.G.2 TECHNOLOGIES INNOVANTES, pyxalis Your Image Sensor Solution

Governance and risk management
SBT Human(s) Matter

Military and other materials and equipment for the protection and safety of critical and essential service providers
OMEXOM, S2P SMART PLASTIC PRODUCTS

Remote work/telework and remote medicine/telemedicine (improvements to working and remote working conditions, data security, crisis management, etc.)
PHARMAnity

Asset security
AMIRAL TECHNOLOGIES

Economic and industrial intelligence
APROBASE INTERNATIONAL

Security and risk management
G-SCOP

CONTENTS

Economic security: Security and risk management

Economic security: Economic and industrial intelligence

Economic security: Asset security

Health security: Remote work/telework and remote medicine/telemedicine (improvements to working and remote working conditions, data security, crisis management, etc.)

National security and safety - risk and crisis management - civil security: Military and other materials and equipment for the protection and safety of critical and essential service providers

National security and safety - risk and crisis management - civil security: Personnel management and risk awareness

Cybersecurity - digital security: Deep web and dark web

Cybersecurity - digital security: Audit and risk analysis

Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

Cybersecurity - digital security: Data protection, identity protection, GDPR

Cybersecurity - digital security: IoT device security

Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)

Videoprotection - surveillance : Hypervision, supervision

Videoprotection - surveillance: Drones, robots, remote monitoring tools

GSCOP - GRENOBLE INP - UGA

G-SCOP is a multidisciplinary laboratory which has been created to meet the scientific challenges imposed by the ongoing changes within the industrial world. The scope of the laboratory goes from the products conception to the production systems management and is based on strong skills in optimisation.

The creation of the G-SCOP laboratory is, in Grenoble, the culmination point of a very long history of scientific breakthroughs and collaborations in the field of production systems, product design and operational research.

Product / service description

Regarding risk management, G-SCOP has worked on the formalization of risk prediction methods and developed a model-based approach that is applied to industrial systems and crisis management systems.

Contact
Mr Maitre Emmanuel / emmanuel.maitre@grenoble-inp.fr

38000 Grenoble
g-scop.grenoble-inp.fr

Other comptencies :

- National security and safety · risk and crisis management · civil security: Personnel management and risk awareness
- National security and safety · risk and crisis management · civil security: Governance and risk management

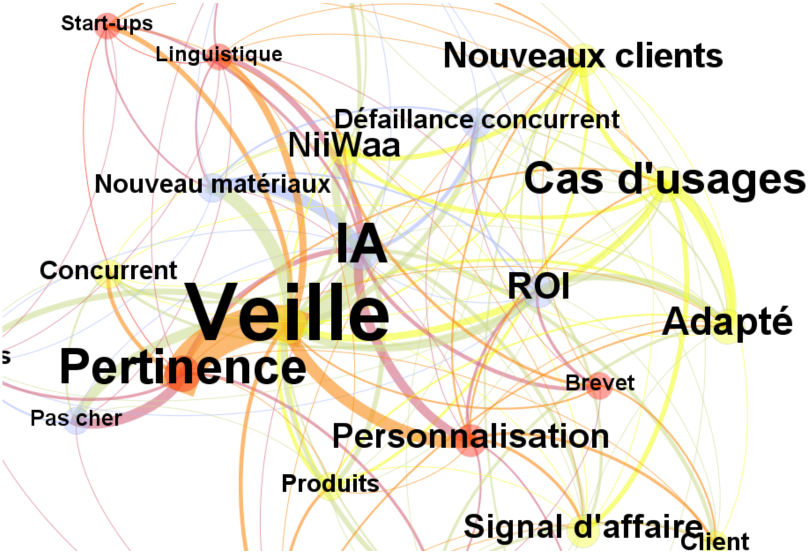
APRO BASE INTERNATIONAL

Competitive Intelligence consultant specialised in native langue intelligence. Our experience extends over more than 30 years, with more than 20 years of continuous services for some customers.

We do not subcontrat our activities abroad and our servers hare located in France. We send to our customer intelligence information that target their field of interest, including safety and security matters.

Product / service description

Surveillance of thousands of targets (suppliers, competitors, clients, prospects, institutions,...) More than 10.000 keywords per query in more than 50 langages



Contact
Mr Lemaire Richard / rlemaire@aprobase.com

73400 Ugine
www.aprobase.com

Other comptencies :

- Videoprotection · surveillance: Drones, robots, remote monitoring tools
- Videoprotection · surveillance: Hypervision, supervision

AMIRAL TECHNOLOGIES

Spin-off of CNRS of Grenoble, Amiral Technologies publishes the DiagFit software for predicting industrial equipment failures using data from sensors.

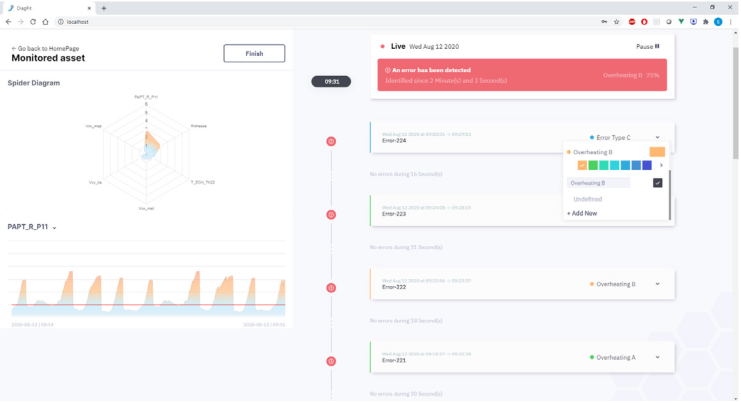
Product / service description

We develop and market DiagFit, our blind failure prediction software for IIoT-enabled equipment. Blind means we predict equipment failures without historical failure data. Magical? No, we invented scientific methods to generate highly discriminant health indicators from industrial time series data issued by sensors.

Some of our use cases are at: https://www.amiraltechnologies.com/our-offer/use-cases/

Target markets

Energy, Transports, and manufacturing



An error has been detected
Identified since 2 Minute(s) and 3 Second(s)
Overheating B 75%

Wed Aug 12 2020 at 09:28:31 -> 09:29:13
Error-224
Error Type C

Overheating B
Undefined
+ Add New

No errors during 16 Second(s)

Wed Aug 12 2020 at 09:24:08 -> 09:28:15
Error-223

No errors during 31 Second(s)

Wed Aug 12 2020 at 09:22:56 -> 09:23:37
Error-222
Overheating B

No errors during 18 Second(s)

Wed Aug 12 2020 at 09:18:37 -> 09:22:38
Error-221
Overheating A

No errors during 30 Second(s)

Contact
Mr Gazikian Simon / simon.gazikian@amiraltechnologies.com

38000 Grenoble
www.amiraltechnologies.com

Other comptencies :

Economic security: Security and risk management

Cybersecurity - digital security: IoT device security

PHARMANITY

Grenoble-based Pharmanity has been supporting pharmacists and their patients for the past seven years. The company's mission is to make it easier for patients to access care and communicate with healthcare providers. Pharmanity has more than 2,000 partner pharmacies across France and offers easy-to-use click and collect, real-time product availability information, prescription transmission, and appointment (pharmacist consultations, Covid testing and vaccination, etc.) services at no additional charge to patients. The result? Easier, more secure access to care for all patients.

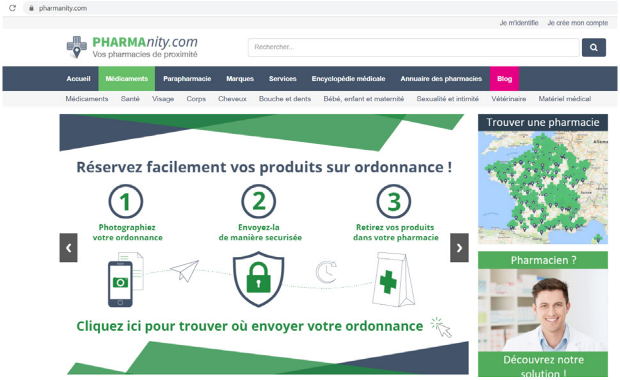
Product / service description

Designed for individual pharmacy customers, Pharmanity.com provides real-time product availability and prices at nearby pharmacies and information about participating pharmacies' areas of expertise, in-pharmacy services, and duty-pharmacy schedules.

Pharmacists can also create their own website with their products, areas of expertise, and services in a way that ensures compliance with French regulations that prohibit pharmacists from advertising. With Pharmanity, pharmacists can also offer online services like prescription transmission, click and collect, and online appointment bookings for in-pharmacy services.

Target markets

Pharmaceuticals, e-health, information technology



Réservez facilement vos produits sur ordonnance !

1 Photographiez votre ordonnance

2 Envoyez-la de manière securisée

3 Retirez vos produits dans votre pharmacie

Cliquez ici pour trouver où envoyer votre ordonnance

Contact
Mr Mottin Samuel / contact@pharmanity.com

38000 Grenoble
www.pharmanity.com

Other comptencies :

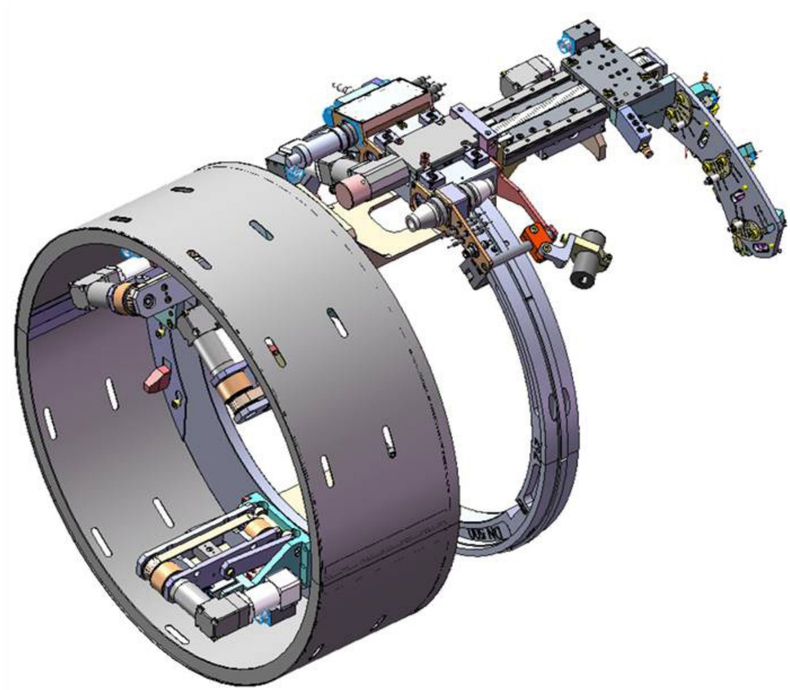
- Health security: Physical and material protection (disinfection, eye solutions, air purifiers, electronic thermometers, thermal cameras, retinal scan software)
- Cybersecurity - digital security: Storage - backup

OMEXOM NDT

Subsidiary of VINCI, specialized in automated non-destructive testing

Product / service description

Non-destructive testing in nuclear power plants



Contact
Mr PONTON Jimmy / jimmy.ponton@omexom.com

26300 Bourg de Péage
www.omexom.com

Other comptencies :

- Videoprotection - surveillance: Drones, robots, remote monitoring tools
- Videoprotection - surveillance: Hypervision, supervision

S2P-SMART PLASTIC PRODUCTS

- S2P (Smart Plastic Products) helps you to facilitate the integration of electronics in your 3D complex products. From designing to industrialization, with reliable industrial processes, we integrate 3D conductive tracks and electronic components directly on plastic or composite parts, with complex 3D shapes. Combined with conventional PCB/Flex technologies, it helps you to integrate electronics in constrained volumes:

- 3D miniaturized antennas

- Full 3D tamper-detection caps to protect against physical penetration for Cybersecurity

- 3D in situ sensors

- 3D integrated LED lighting functions

- 3D interconnexions to remove wires

- Shielding areas, integrated connectors, ...

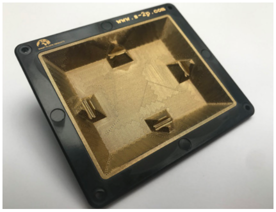
New ergonomic and miniaturized shapes can be then created for your electronic products. Freedom and flexibility of the design give you a real advantage compared to usual solutions, while simplifying the assembly and finally decrease the cost. With a team of experts in plastic, electronics and chemistry, S2P supplies services for designing, prototyping, andmanufacturing of these smart plastic products.

Product / service description

S2P designs and manufactures physical anti-tampering devices to protect against physical intrusion in highly secured electronics systems. We are complementary to other cybersecurity solutions (protocols, software, silicon device security...), in segments where the tamper resistance is mandatory, at a system level : banking, states, military, critical industrial sites, high sensitive IoT, ... We create a complete envelope of protection around the electronic module by integrating a 3D mesh of conductive tracks all over complex 3D surfaces, and associated electronic control and management. Our technology is the most secure way of protecting sensitive modules, while simplifying the assembly and increase the design freedom of the final products. It fully fits with highest level of standards like PCI, FIPS or common criteria eal (ISO 15408).

Target markets

Defense & Security, Critical industries, banking



Contact
Mr Moguedet Mael / mael.moguedet@s-2p.com

01100 Oyonnax
www.s-2p.com

Other comptencies :

Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

Economic security: Anti-fraud/anti-counterfeiting

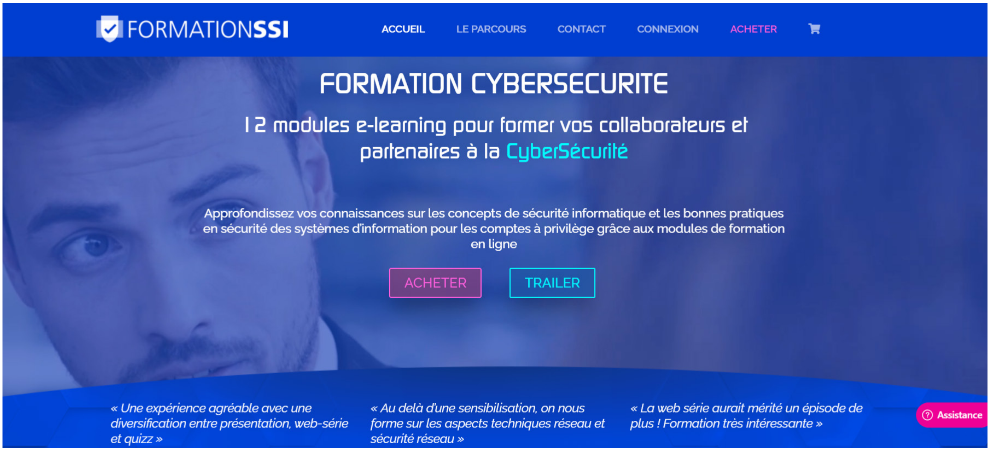
SBT HUMAN(S) MATTER

Human(s) Matter

Specialized in potential detection and skills training, SBT Human(s) Matter has designed various contents and training programs about cybersecurity stakes.

Product / service description

- An online training program dedicated to cyber security with 12 modules. https://www.formation-ssi.com/



FORMATION CYBERSECURITE

12 modules e-learning pour former vos collaborateurs et partenaires à la CyberSécurité

Approfondissez vos connaissances sur les concepts de sécurité informatique et les bonnes pratiques en sécurité des systèmes d'information pour les comptes à privilège grâce aux modules de formation en ligne

« Une expérience agréable avec une diversification entre présentation, web-série et quizz »

« Au delà d'une sensibilisation, on nous forme sur les aspects techniques réseau et sécurité réseau »

« La web série aurait mérité un épisode de plus ! Formation très intéressante »

Contact
Mr TARPIN-BERNARD Franck / f.tarpin@sbt-human.com

69002 Lyon
www.sbt-human.com

Other comptencies :

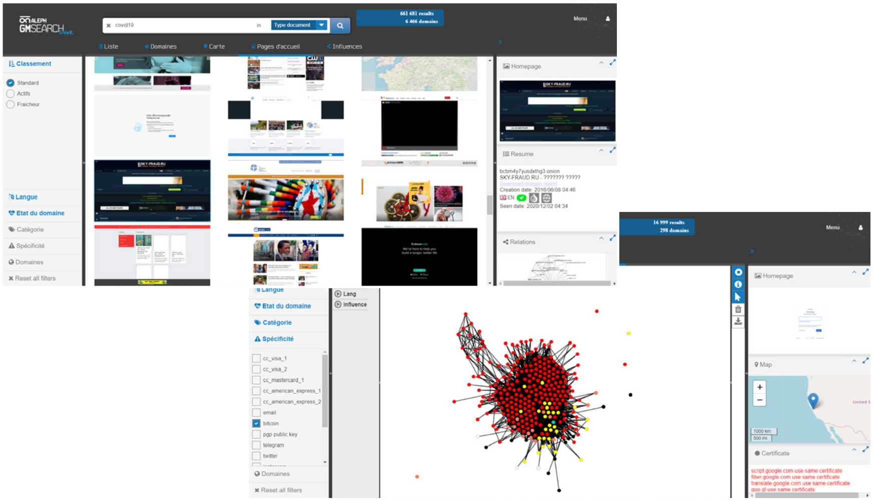
- Cybersecurity - digital security: Data protection, identity protection, GDPR
- Health security: Remote work/telework and remote medicine/telemedicine (improvements to working and remote working conditions, data security, crisis management, etc.)

ALEPH

Aleph produce Cybersecurity and Strategic Intelligence solutions to ensure the safety of individuals, companies, and countries. Also, Aleph monitor and analyse all the layers of the web to detect any form of exposure or leaks of strategic and/or confidential data.

Product / service description

Aleph Search Dark hunts for illegal traces and data on the Deep & Dark webs, maps out these areas, identifies influence clusters, and searches for noteworthy information. Aleph Search Dark is currently the leading search and analytics engine for the Deep & Dark webs. No other independent search engine has such a wide scope and in-depth analysis tools.



Contact
Ms PIONIN Mélina / melina.carano@aleph-networks.com

69 400 Villefranche sur Saone
www.aleph-networks.com

Other comptencies :

- Cybersecurity - digital security: Audit and risk analysis
- Economic security: Economic and industrial intelligence

PLATEFORME TECHNOLOGIQUE ESYNOV

Esynov, the technological platform created within the Grenoble INP - Esisar engineering school in Valence, combines skills and means of investigation for the analysis and characterisation of cyber-physical systems. It contributes to the initial training of the engineering school, continuing education and participates in research projects in cooperation with the LCIS laboratory.

Esynov carries out technology transfer actions for the benefit of companies in the fields of electromagnetic compatibility, radiofrequency, embedded systems, and cybersecurity. These skills are based on high-level technical installations: anechoic chamber, digital security training platform, cybersecurity demonstrators, hardware security evaluation platform, etc.

Thanks to its skills and resources, Esynov provide expertise, audit, and support to companies.

Product / service description

Esynov deploys its expertise in cybersecurity by supporting companies in dealing with cyberthreats:

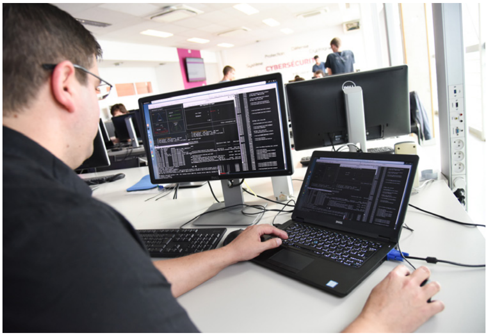
- Integrate and manage cybersecurity issues (training and support)

- Develop a cybersecurity culture and expertise (awareness, training)

- Perform an inventory (security audit, asset mapping, penetration test, vulnerability report, recommendations)

- Implement cybersecurity in a practical and operational way in the company (proposal of an action plan, support for implementation)

- Evaluate the security of a product or a connected system (identify risks, define the right level of security, test and propose countermeasures to secure)



Contact
Mr Blanchard Gabriel / contact@esynov.fr

26000 Valence
www.esynov.fr

Other comptencies :

- Cybersecurity - digital security: IoT device security
- Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

CYBERSECURA

CYBERSECURA

CyberSecura offers consulting and services dedicated to cybersecurity and regulatory compliance. We work with you to secure your information systems and digital products, to govern your security, and to help your organisation achieve compliance with GDPR or obtain a certification. Our part-time model sets your security in the long term, providing maximum cost effectiveness to ensure affordability for any size of business.

Product / service description

A technical white-box audit provides a complete understanding of a system and its existing threats. Our support then enables companies of all sizes to mitigate risks, train teams, and make security a permanent part of the company’s overall operation. We also work with you to promote the security of your business in terms of commercial marketing.

Contact
Mr Rozier David - d.rozier@cybersecura.com

38000 Grenoble
www.cybersecura.com

Other comptencies :

- Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications
- Cybersecurity - digital security: Data protection, identity protection, GDPR

SCPTIME

SCPTime addresses Time cybersecurity issues. In the age of digitalization, Time plays an essential role, and particularly in the field of Cybersecurity. Cryptography, timestamping of logs, interoperability, archiving of sensitive data, diagnostics, SOCs,... Everywhere, Time is an often neglected flaw, whereas hacking of systems by this means constitutes a systemic attack. SCPTime® sets up an infrastructure and a service to broadcast the legal time of a country (UTC) using a new time signal, Secure, Certified, Accurate and Traceable, to address current Time sources vulnerabilities, and to prevent serious consequences resulting from their corruptibility. These new requirements for using reliable and legal time sources are becoming essential to authenticate transactions, qualify processes, and secure synchronization devices. Above and beyond Time cybersecurity, SCPTime® offers a comprehensive time synchronization solution for your networks and devices.

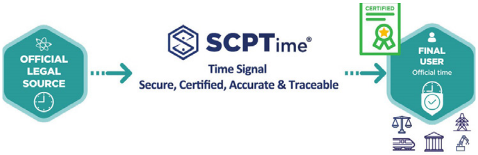
Product / service description

SCPTime® prevents from time signal failures at affordable price, offering full proof cybersecurity and complete traceability of the Time signal provided from its origin (UTC - National atomic clocks) to the final customer. SCPTime® stands out because it is so easy to use and implement ! It is the only system worldwide which provides 100% security thanks to the continuity and traceability of the two-way time signal transmission by :

- Certifying synchronization operations.
- Providing full traceability of the time signal from legal source (UTC) to the end user
- Certifying UTC reference time source.
- Monitoring momentary interruptions, performance deficiencies or synchronization malfunction.
- Switching to an internal micro atomic clock in case of synchronization loss.
- Providing a certified precision, ranging from the subsecond to a few nanoseconds according to applications.
- offering a comprehensive architecture that is more economically efficient than the multiplication of local independent systems.

Target markets

Transportation, Fintech, Critical infrastructures



Contact
Mr TEOT Sébastien - sebastien.teot@scptime.com

38350 La Mure
www.scptime.com

Other comptencies :

- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security
- National security and safety - risk and crisis management - civil security: Military and other materials and equipment for the protection and safety of critical and essential service providers

SOGILIS

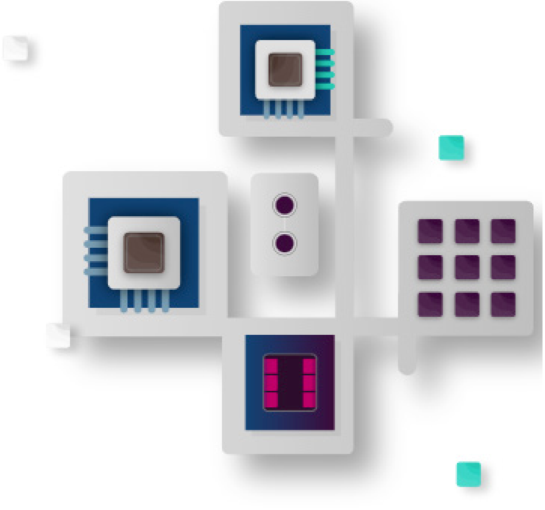
Sogilis is a software service company (50 people) located in Lyon and Grenoble, established in 2008. Our DNA is the software quality based on our methodologies and demonstrated engineering practices.

Product / service description

In a connected world where appliances have their own brain, it's important to power IOT devices with high-quality software, that is reliable, efficient and secure. Every great device is powered by great software.
We help you bring your devices to life with the software they deserve.

Target markets

Software editors, Industry 4.0



Contact
Mr DERBEY MARC - marc.derbey@sogilis.com

38000 Grenoble
www.sogilis.com

Other comptencies :

- Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications
- Cybersecurity - digital security: IoT device security

BEAUTIFOOL PLANET

Beautifool Planet is a French software company specialized in decentralized or distributed software solutions (DLT - Distributed Ledger Technologies), without public blockchain. Since its creation in 2014, the company has developed the EDAFON® technology, a ''private chain'' software engine designed for the business needs of companies, organizations, consortiums of all sizes and all fields: trust, transparency or confidentiality, substitution to a trusted third party, immutability or ephemerality, resilience, non-repudiation of data, digital identification / anonymization, traceability, certification, smart contracts, consensus, ...

Our know-how in decentralized software architecture allows our customers to free themselves from fashionable infrastructures that are complex (tokenization, heavy IT layers), energy consuming (mining, datacenters) and cryptoassets/speculation oriented (cryptocurrency, DEFI) and to keep the sovereignty of their data even in distributed environment. We thus enable the production of multi-sites, multi-third parties, multi-structures applications, with an ethical and green computing approach, also contributing to better ESG commitments.

Product / service description

Our EDAFON® software engine allows :
- create and deploy private and permissioned P2P networks, operating business processes, whether in edge computing, fog or cross cloud
- dynamically share secure distributed registers using blockchain database processes, without any scalability constraints and at controlled costs
- power decentralized information systems directly on users devices (smartphones, appliances, IoT or our ARM EDANOD® mini-boxes) as well as on connected technical devices (IIoT, embedded systems in motion, M2M, ...)
- create decentralized business APIs for D-App/Web3 type applications
- manage regulatory (GDPR...) and data security issues in an innovative way: data partitioning, dissemination and obfuscation processes, allowing to complete classical encryption solutions; business processes directly on data always encrypted (homomorphic encryption), ...

Target markets

All markets - traditional and new business models (B2B, B2C, C2C, D2C ...)

EDGE BLOCKCHAIN for Business
edanod
Embedded DLT powered by edafon®
on connected constrained devices

Contact
Mr PERRIN Bertrand / contact@bfplanet.org

38110 Cessieu
www.bfplanet.org

Other comptencies :

- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security
- Cybersecurity - digital security: IoT device security

3D-OXIDES

3D-oxides is specialized in oxide thin films for a wide range of applications such as photonics, semiconductors, renewable energy or security. In the latest one, we are developing Physical Unclonable Functions that, coupled with a new generation blockchain, will enable Self-Sovereign Identities for objects in the framenwork of IoT.

Product / service description

We are developing SSI for objects. This will enable improved security and Trust for objects in a new generation Internet where objects will be able to manage their own data and transactions without human intermediation nor central platform towards a real time updated digital twin.

Target markets

Full interoperability of our solution will make obsolete market segmentation.

Contact
Mr Benvenuti Giacomo / giacomo.benvenuti@3d-oxides.com

01630 St Genis Pouilly
www.3D-oxides.com

Other comptencies :

- Cybersecurity - digital security: Data protection, identity protection, GDPR
- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

CEA-LETI

CEA-Leti, a technology research institute at CEA, pioneers micro and nanotechnologies, tailoring differentiating applicative solutions that ensure competitiveness in a wide range of markets. The institute tackles critical challenges such as cybersecurity and global security through ICTs;

Its multidisciplinary teams deliver solid security expertise for applications ranging from sensors to data processing and computing solutions, leveraging world-class pre-industrialization facilities. CEA-Leti builds long-term relationships with its industrial partners - global companies, SMEs and startups – and state partners (agencies, ministries) and actively supports the launch of technology startups. CEA-Leti is a member of the Carnot Institutes network

Product / service description

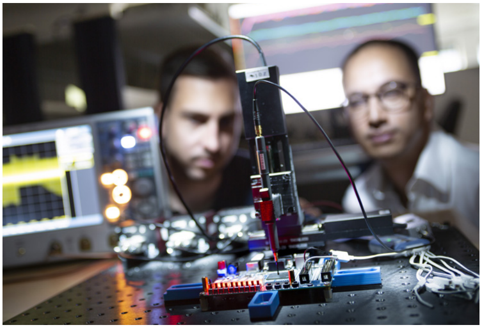
Research activities of CEA-Leti are focusing on :

• Answering the needs of its industrial or state partners in security asssessment and vulnerabilities detection in critical components and electronics. CEA-Leti develops new tools and benches for security assessment. It hosts since 1999 an Information Technology Security Evaluation Facility (ITSEF) which is part of French national certification scheme (managed by ANSSI) and also part of private schemes such as Visa, Mastercard and Fido.

• Developing new technologies to secure depending of its partners needs : chip, electronics and complexe systems that are connected to cyberspace. Results are then transfered to CEA-Leti's industrial or state partners.

Target markets

Defense and security - industries (energy, manufacturing) - health



Contact
Mr Cachard Vincent / vincent.cachard@cea.fr

38000 Grenoble
www.leti-cea.fr

Other comptencies :

- Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications
- Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)

LABORATOIRE HUBERT CURIEN UMR CNRS 5516

The Hubert Curien laboratory is a joint research unit (UMR 5516) of the Jean Monnet University, Saint-Etienne, the National Research Centre «CNRS» and the Institut d'Optique Graduate School.

It is composed of about 90 researchers, professors and assistant professors, 20 engineers and administrative staff and 130 PhD and post-PhD students. This makes the Hubert Curien laboratory with a total of about 240 staff the most important research structure of Saint-Etienne.

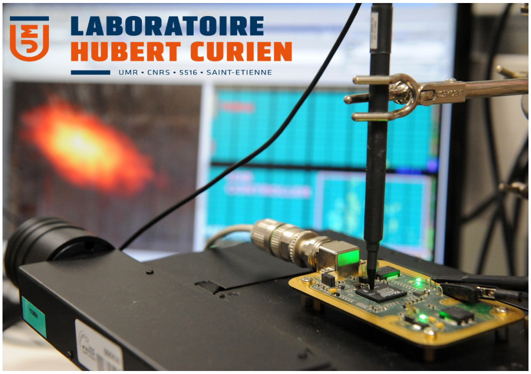
Our research activities are organized according to two scientific departments: Optics, photonics and surface and Computer Science, Security, Image.

Product / service description

Embedded system cybersecurity: hardware security (development of physical attacks by fault injection and side channel analysis and associated countermeasures), architecture of secure microprocessor and secure-by-design System-on-Chip, FPGA security, IP protection and war against counterfeiting, test, design and modeling of random number generation (TRNG & PUF) on silicon.

- Artificial intelligence and machine learning for security: fraud detection and prevention, side channels analysis.

- Software / hardware cryptography: implementation of classical and post-quantum encryption algorithms.



Contact
Mr BOSSUET Lilian / lilian.bossuet@univ-st-etienne.fr

42000 Saint-Etienne
laboratoirehubertcurien.univ-st-etienne.fr

Other comptencies :

- Economic security: Anti-fraud/anti-counterfeiting
- Cybersecurity - digital security: Data protection, identity protection, GDPR

PARCOOR

Parcoor is a startup expert in embedded artificial intelligence that specializes in the field of cybersecurity of connected devices. We are ongoingly developing innovating malware detection solution.

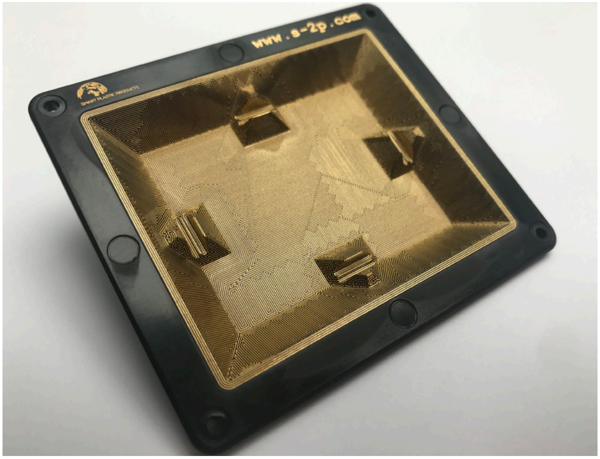
This solution is based on a novel micro-event deep-learning approach for protecting microcontrolers at their hearts.

Product / service description

Parcoor develops embedded malware detection software. Designed specifically to meet embedded constraints (limited resources, bandwidth, real time), our software has several advantages:
- real-time malware detection, including «zero-day» malwares,
- low energy consumption,
- reduced attack surface.

Target markets

Aeronautics, automotive, edge computing



Contact
Mr Capel Denis / denis.capel@parcoor.com

69001 Lyon
parcoor.com

Other comptencies :

- Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)
- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

RTONE

For 14 years now, Rtone has been developing smart and connected products. First, in the field of energy and now in all sectors. Our clients have given us the opportunity to save lives, meet the new needs of today's cities and invent the products we will all find essential tomorrow. Our multi-disciplinary team of 50 allows us to propose a unique offer to our customers who wish to outsource the design of their products.

By blending the skills of a design office experienced in hardware and digital technology with an ecosystem of manufacturing partners, Rtone brings global, innovative solutions to the IoT systems market. Rtone delivers best-fit technical solutions to successfully enhance and secure your transition to the world of connected objects

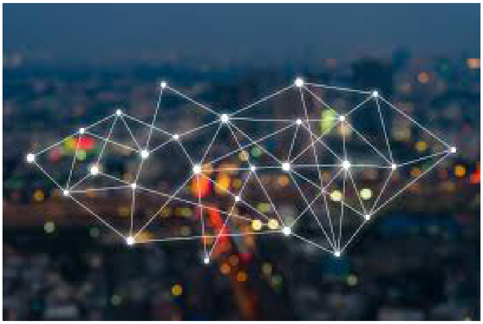
Product / service description

IOT Cyber Testbench aims to develop an automatic vulnerability diagnostic equipment for the Internet of Things in a context of assessment and verification of requirements. safety and security. This solution will allow the designer of connected systems to conduct test and investigation campaigns throughout the design phases to fulfill the goal of a secure design. The solution offers to provide cybersecurity assessments and metrics for non-specialist technicians in the field in order to support them in the validation test design phases and throughout the product lifecycle.

The main objectives of this project are:
- reliability and ease of use,
- the adaptation of the security test coverage,
- repeatability and integration into the product life cycle.

Target markets

Smartcity, SmartHome, Industry



Contact
Mr Midroit Didier / didier@rtone.fr

69009 Lyon
www.rtone.fr

Other comptencies :

- Cybersecurity - digital security: Data protection, identity protection, GDPR
- Cybersecurity - digital security: Storage - backup

STMICROELECTRONICS

life.augmented

We are 46,000 creators and makers of semiconductor technologies, devices, and solutions that start with our employees, with our 100,000 customers, and with our thousands of partners. Together, we design and build products, solutions and ecosystems that address the sustainability and resource management challenges our customers are facing, while helping them seize opportunities they are pursuing.

This is why we have 8,100 R&D employees, invest about 16% of our revenues in R&D every year, and engage in extensive collaboration with leading research labs and corporate partners throughout the world. Moreover, we are continuously investing in our footprint as an independent device manufacturer.

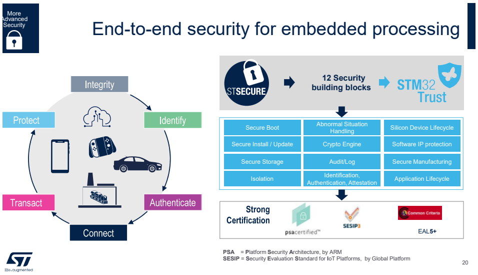
Our 11 manufacturing sites master all aspects of the semiconductor supply chain and offer our customers the quality, flexibility, and supply security they need.

Product / service description

STM32Trust offers a robust multi-level strategy to enhance security in new product designs based on our STM32 microcontrollers and microprocessors augmented with STSAFE secure elements. Mobile security is expanding from the largely deployed SIM technology to the growing NFC, embedded Secure Element (eSE) and embedded SIM (eSIM) technologies in smartphones, tablets. From ST31 secure microcontrollers to ST54 solutions integrating NFC controller, secure element and eSIM, ST offers a complete range of solutions for payment, transit

Target markets

Industrial Platforms Security, Mobile Security, Wearable Security



End-to-end security for embedded processing

Secure Boot	Abnormal Situation Handling	Silicon Device Lifecycle
Secure Install / Update	Crypto Engine	Software IP protection
Secure Storage	Audit/Log	Secure Manufacturing
Isolation	Identification, Authentication, Attestation	Application Lifecycle

PSA = Platform Security Architecture, by ARM
SESIP = Security Evaluation Standard for IoT Platforms, by Global Platform

Contact
Mr Magarshack Philippe / philippe.magarshack@st.com

38000 Grenoble
www.st.com

Other comptencies :

- Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)
- Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

TIEMPO SECURE

Certified security for IC design : security IP cores, software libraries and expert services to secure integrated circuits at the highest and certified levels of security At Tiempo Secure, we deliver secure element IP cores and secure software libraries that are guaranteed to enable Common Criteria EAL5+ or equivalent security certification of any System-on-Chip (SoC) integrating these cores.
We partner with software companies to offer complete secure hardware and software solutions for various security OS and applications, such as JavaCard 3.0.5 OS, iSIM, Web authentication, payment, smart car access and vehicle communication, and their corresponding certifications GSMA, FIDO2, EMVCo and V2X HSM. Major chip manufacturers in Europe, USA and Asia have already trusted us by integrating into their design our secure element IP cores for these applications, and using our security expert services, including Common Criteria certification lab support, and software configuration of HSM servers for secure chip personalization and firmware programming.

Product / service description

TESIC is a CC EAL5+ PP0084 proven/certification-ready secure element IP that is delivered as hard macro for plug-and-play System-on Chip (SoC) integration. Targeted designs are SoCs that require a security enclave highly protected against side-channel attacks and perturbation/fault attacks, and that execute secure software such as iSIM, EMVCo payment, FIDO2 Web authentication, V2X HSM protocol and/or other security routines for the SoC system, including secure boot, secure OTA firmware update, secure storage and secure debug. TESIC includes a secure MCU, secure cryptographic processors and hardware accelerators, security sensors, secure memories and standard interfaces for easy integration and test. Memory sizes, cryptographic accelerators and interfaces can be customized according to customer requirements. TESIC is delivered as a GDS hard macro to the certified fab, with the guarantee to pass CC EAL5+ PP0084 and/or EMVCo security certification of the chip integrating this macro.

Target markets

Chips for connected objects

Contact
Mr MAGINOT SERGE / serge.maginot@tiempo-secure.com

38330 Montbonnot st-Martin
www.tiempo-secure.com

Other comptencies :

- Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications
- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

TIMA (TECHNIQUES DE L'INFORMATIQUE ET DE LA MICRO-ÉLECTRONIQUE POUR L'ARCHITECTURE DES SYSTÈMES INTÉGRÉS)

- Robustness, reliability and test

- Hardware/Software co-design

- Simulation and verification - Low power design

- Hardware security and embedded trust

- Asynchronous design

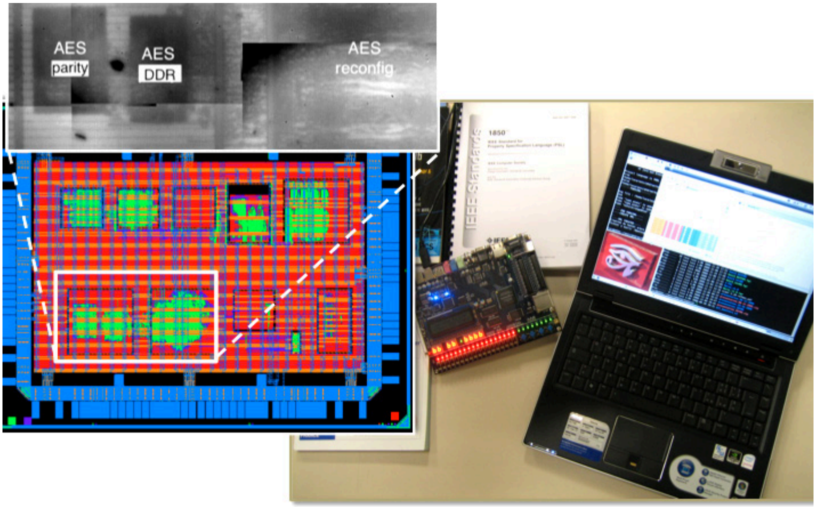
- New sampling and data processing techniques

- MEMS, Smart Sensors and Actuators

- Design of AMS/RF/mmW devices, circuits and systems

- Modeling, control and calibration of AMS/RF devices, circuits and systems

- New hardware computing and digital design



Contact
Mr Di Natale Giorgio / giorgio.di-natale@univ-grenoble-alpes.fr

38031 Grenoble
tima.univ-grenoble-alpes.fr

Other comptencies :

- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security
- Cybersecurity - digital security: Storage - backup

VERIMAG - GRENOBLE INP - UGA

Verimag's work aims at producing theoretical and technical tools to enable the development of qualitycontrolled embedded systems at competitive costs.

During the last fifteen years, Verimag has actively contributed to the development of the state of the art in synchronous languages, model-checking, testing, and system modeling. Verimag's results have numerous industrial applications, notably in tools for software development and embedded systems.

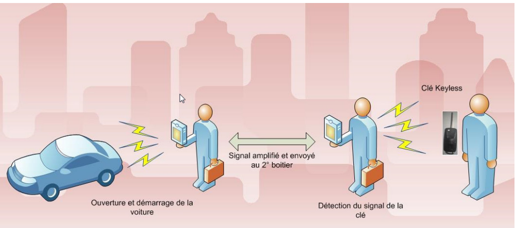
Verimag seeks to maintain a balance between fundamental, experimental, and applied research, in particular through sustained cooperation with industrial and academic partners.

Product / service description

Embedded systems are at the heart of a wide area of applications, including avionics/aeronautics, space, transport, automotive, telecommunications, smart cards, consumer electronics.

Embedded systems are composed of hardware and software components specifically designed for controlling a given application device. Embedded systems are of strategic importance for those sectors of the economy where Europe has traditionally been strong.

Keywords: Embedded systems - Formal Specification - Verification - Test - Simulation - Critical System - Real Time System - Hybrid System - Safety and Security - Synchronous Language - Modeling and Analysis of complex systems - Communication Protocol - Compilation - Static Analysis - Code Generation - Real Time Scheduling - Real-Time UML - SDL


Clé Keyless
Signal amplifié et envoyé au 2° boitier
Ouverture et démarrage de la voiture
Détection du signal de la clé

Contact
Mr Maitre Emmanuel - emmanuel.maitre@grenoble-inp.fr

38401 Saint Martin d'Hères
www-verimag.imag.fr

Other comptencies :

- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security
- National security and safety - risk and crisis management - civil security: Mobility and logistics support equipment and port, airport, rail, and road transportation security

AUTOMATIQUE & INDUSTRIE - AI FRANCE

Automatique & Industrie (AI) is a company specializing in Industrial engineering, automation and SCADA.

AI designs and integrates complete and innovative automated solutions for infrastructure and industry, in France and abroad. Its businesses: consulting, service, integration, training 3 sectors of activity:
- Energy management and energy efficiency in buildings and industries
- Building and infrastructure: Technical Building Management Solutions
- Industry: industrial process control, machine automation 6 fields of application: airport, energy, machine manufacturers, hydroelectricity, solar production monitoring and industrial processes. Automatique & Industrie is a humanly involved company with an active Corporate Social Responsibility (CSR).

Product / service description

AI has dual industrial/automation and network IT skills wich allows to put IT, network and cybersecurity skills at the service of the OT. This global knowledge enables AI to offer the following services :

- Network diagnostics and industrial IT
- Troubleshooting
- State of play
- Reliability Cyber Diagnostic
- State of play
- Technical analysis (mapping, flow study, etc.)
- Human analysis (Study of procedures, management of passwords, versioning, etc.)
- Debrief writing
- Recommendations
- Support for cyber skills development
- Assess the condition of its industrial system
- Developed team competence
- Staff training/awareness
- Support for teams
- Working in synergy with local teams IT and OT
- Network design
- Secure remote access
- Integration of network monitoring into existing production tools (SCADA, alerts...)

Target markets

Industrie, énergie et infrastructure

Contact
Mr BOURGAIN Matthieu - matthieu.bourgain@aifrance.com

38430 Saint-Jean-de-Moirans
www.aifrance.com

Other comptencies :

Cybersecurity - digital security: Audit and risk analysis

National security and safety - risk and crisis management - civil security: Military and other materials and equipment for the protection and safety of critical and essential service providers

ECE PARIS LYON - ECOLE D'INGÉNIEURS

ECE Paris Lyon is a graduate school of engineering in IT. It is a member of the Conférence des Grandes Ecoles and approved by the Commission des Titres d'Ingénieur. As of 2018, it offers the Information Systems and Defensive Cybersecurity program, and each year trains around fifty students in this field.

This program is developed in partnership with Microsoft, Orange Cyberdéfense and Thales, and has been granted the SecNumedu label by Agence Nationale de la Sécurité des Systèmes d'Information.

Product / service description

The Information Systems and Defensive Cybersecurity program spans the fourth and fifth years of study, and includes more than 450 hours of technical courses. These courses cover, among other things, cybersecurity policies, standards and methodologies, IS and network security, identity and access management, incident response, forensics and reverse engineering. The program opens up to positions as cybersecurity consultant, security solution developer, security incident response analyst, security project manager.

Target markets

Industrial Platforms Security, Mobile Security, Wearable Security

Contact
Mr Busca Jean-Michel / jeanmichel.busca@ece.fr

38000 Grenoble
ece.fr

Other comptencies :

- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security
- Cybersecurity - digital security: Audit and risk analysis

ÉCOLE D'INGÉNIEURS EN CHIMIE ET SCIENCES DU NUMÉRIQUE CPE LYON

CPE Lyon offers degree programs in chemical engineering and computer science. As of September 1, 2019, it was one of 205 certified engineering schools in France. The school was formed in 1994 from the merger of ICPI (Institut de Chimie Physique Industrielle), established in 1919, and ESCIL (École Supérieure de Chimie Industrielle de Lyon), established in 1883.

CPE Lyon began offering a degree program in computer science and cybersecurity in the fall of 2019 in partnership with engineering school ITII (Institut des Techniques d'Ingénieurs de l'Industrie de Lyon), and Institution des Chartreux, a private college-preparatory high school.

Product / service description

- Degree programs:
- Computer and communications network engineering.

This program, offered in conjunction with ITII, focuses heavily on network and system security.

- Computer and cybersecurity engineering.

CPE Lyon introduced this program in the fall of 2019 in partnership with ITII and Institution des Chartreux.

Contact
Mr MESSAI Mohamed-Lamine /mohamed-lamine.messai@cpe.fr

69100 Villeurbanne
www.cpe.fr

Other comptencies :

Cybersecurity - digital security: Audit and risk analysis

Cybersecurity - digital security: IoT device security

Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

INRIA GRENOBLE RHÔNE-ALPES (GRENOBLE, LYON)

Inria is the French national research institute for digital science and technology. World-class research, technological innovation and entrepreneurial risk are its DNA.

In 200 project teams, most of which are shared with major research universities, more than 3,500 researchers and engineers explore new paths, often in an interdisciplinary manner and in collaboration with industrial partners to meet ambitious challenges.

As a technological institute, Inria supports the diversity of innovation pathways: from open source software publishing to the creation of technological startups (Deeptech).

Product / service description

Inria has put the construction of a digital trust society at the heart of its strategic plan. This means the Institute plays a significant role in a key research and innovation program for our digital sovereignty, as evidenced by strategic partnerships with key players such as the National Cybersecurity Agency of France (ANSSI). With the prospect of quantum computing, Inria is responsible for continuing or increasing its research and innovation efforts devoted to cybersecurity to help protect French citizens

Calculate from encrypted data, Designing post-quantum cryptography, computing on encrypted data, end-to-end proofs for cryptographic protocols, developing security for the Internet of Things and enhanced protection for citizens' privacy – Inria's major research pathways in the field of cybersecurity are highly focused, with a strong potential for technological transfer.

Contact
Mr BROUN Philippe / philippe.broun@inria.fr

38000 Grenoble
inria.fr

Other comptencies :

- Cybersecurity - digital security: Data protection, identity protection, GDPR
- Cybersecurity - digital security: IoT device security

Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

INSTITUT DE RECHERCHE TECHNOLOGIQUE SYSTEMX

SystemX, a technology research institute, possesses strong know-how in analysis, modeling, simulation, and decision assistance applied to complex systems. It is the only member of France's network of technology research institutes to focus on digital systems engineering. SystemX coordinates multi-partner research projects involving stakeholders from academic research and industrial R&D in a cross-disciplinary and multi-market approach to major scientific and technological hurdles in four priority areas: mobility and autonomous transportation, industry 4.0, defense and security, and greentech and sustainable development. SystemX scientists address the major technological and societal challenges of our time through projects centered around specific use cases. Their work is helping speed up the digital transformation of the industrial and services sectors and of government.

Product / service description

The Cybersecurity Hardening Environment for Systems of Systems (CHESS) is a hybrid simulator designed for the ultra-connected systems of the future. This very versatile and complete environment can support manufacturers through the design, development, modeling, simulation, and testing of tomorrow's digital security innovations to:

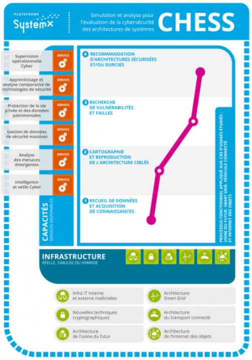
Identify and head off cybersecurity threats with coordinated tools and automated analysis capabilities.

Evaluate the robustness of countermeasures implemented in innovative and realistic use cases.

Added value/Services offered:

Security solutions providers (software and equipment providers, integrators) can use the modelling and simulation tools at CHESS to assess how well their innovative components are protected against threats representative of different use cases.

Critical service providers, banks, manufacturing companies, transportation operators, and other large organizations, as well as integrators, can benefit from the resources available at CHESS to evaluate their architectures and security solutions and determine the best alternatives.


PLATEFORME
SystemX
Simulation et analyse pour l'évaluation de la cybersécurité des architectures de systèmes
CHESS
Supervision opérationnelle Cyber
Apprentissage et analyse comparative de technologies de sécurité
Protection de la vie privée et des données patrimoniales
Gestion de données de sécurité massives
Analyse des menaces émergentes
Intelligence et veille Cyber
SERVICE
CAPACITÉS
SERVICES DISPONIBLES
4 RECOMMANDATION D'ARCHITECTURES SÉCURISÉES ET/OU DURCIES
3 RECHERCHE DE VULNÉRABILITÉS ET FAILLES
2 CARTOGRAPHIE ET REPRODUCTION DE L'ARCHITECTURE CIBLÉE
1 RECUEIL DE DONNÉES ET ACQUISITION DE CONNAISSANCES
PROCESSUS FONCTIONNEL APPLIQUÉ AUX CAS D'USAGES ÉTUDIÉS : USINE DU FUTUR, SMART GRID, VÉHICULE CONNECTÉ ET INTERNET DES OBJETS
INFRASTRUCTURE
RÉELLE, SIMULÉE OU HYBRIDE
Infra IT interne et externe maîtrisées
Architecture Smart Grid
Nouvelles techniques cryptographiques
Architecture du transport connecté
Architecture de l'usine du futur
Architecture de l'Internet des objets

Contact
Mr SCREMIN Lionel / lionel.scremin@irt-systemx.fr

69100 Villeurbanne
www.irt-systemx.fr

Other comptencies :

Cybersecurity - digital security: IoT device security

Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

LIG - GRENOBLE INP - UGA

LIG focuses on the fundamentals of Computer Science and experimental developments while taking into account new societal challenges.

The 5 focus Areas are :
- software and information system engineering
- formal methods, models, and languages
- intelligent systems for bridging data, knowledge and humans
- interactive and cognitive systems
- distributed systems, parallel computing, and networks

Product / service description

The LIG has 24 research teams, several of which have activities related to security and safety.

For example, validation, which concerns both software and models, with a particular interest in validating the security of computer systems, or network security (characterization of applications, detection of anomalies, cyber attacks, IoT security).

Contact
Mr Maitre Emmanuel / emmanuel.maitre@grenoble-inp.fr

38401Saint Martin d'Hères
www.liglab.fr

Other comptencies :

- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security
- Cybersecurity - digital security: Storage - backup

SERMA GROUP

SERMA
SAFETY & SECURITY

SERMA is one of the French leaders in safety and cybersecurity, expert in security and safety of IoT, embedded, industrial or information products and systems. With 200 experts, SERMA offers a unique service integrating Consulting, Expertise, Evaluation, Supervision and Maintenance in security conditions, Training. The areas of expertise and sectors of intervention (notably finance/ industry) provide the company with a unique coverage of offers and sectors of activity.

Product / service description

SERMA covers the full spectrum of cybersecurity: from attack to defence and the implementation of solutions. The security of information systems is a major issue within organisations and even more so since the health crisis of 2020. The opening up of these information systems to the company's users, partners and service providers exposes them to new threats. These new landscapes and ecosystems present security challenges for which expert support is essential. It is essential for businesses to: Know their information system resources and define the sensitive areas to be protected, in order to ensure those resources are used in a controlled, well-reasoned manner. Implement strategic plans, road maps, approaches and measures to assess the risks and define the security objectives to be achieved using state-of-the-art methodologies such as EBIOS Risk Manager. Monitor the security of these sensitive areas in a suitable and regular manner by combining approaches at the infrastructure, application and functional levels. Supervise the security of critical assets through adapted and actionable services through an SOC or managed services. This process takes place over the long term and incorporates technical, organisational, legal and human means. SERMA makes its expertise available to you and supports you in your large-scale projects and in the performance of high added value services.

Target markets

Industry Banking Services

Contact
Ms BOUSQUIE Florie / f.bousquie@serma.com

33600 Pessac
www.serma-safety-security.com

Other comptencies :

- Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)
- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

ORANGE CYBERDEFENSE

Orange Cyberdefense leverages a comprehensive portfolio of solutions and hands-on experience to help companies secure their business and their data across the entire threat lifecycle, with core activities that include:

- Constantly monitoring new and emerging threats, leaks, and fraud schemes.

- Identifying customers' critical assets and data; developing security strategies and ensuring effective implementation.

- Implementing and executing the most appropriate technology to protect customers' organizations.

- Monitoring customers' IT environments and cyberspaces for suspicious events and breaches.

- Assessing, containing, and responding to events.

Orange Cyberdefense key figures:

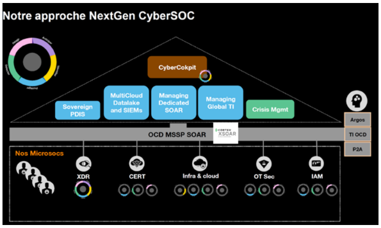
- 2,500 experts
- 26 detection centers in 13 countries
- 50 billion events analyzed daily
- 200 malicious sites detected and shut down daily
- 24% growth in 2019

Product / service description

- Orange Cyberdefense can detect in real time both known and unknown threats to monitored infrastructures managed by us or by third parties. Our security event intelligence services leverage advanced analytics generated by our proprietary data collection and correlation engine. Powered by our unique database of cybersecurity threat intelligence, our engine correlates around 50 billion events from customers' logs every day. Every month, more than 1,500 events are classified as real security incidents by our CyberSOC experts.
- All Orange Cyberdefense CyberSOC customers benefit from native integration of the engine for real-time monitoring via SIEM, EDR and NTA (network traffic analysis)
- Automated detection of abnormal behavior through machine learning or deep learning
- Security orchestration, automation, and response (SOAR) tools

Target markets

Our detection services can be tailored to meet the needs of organizations of different sizes according to the resources they have available.


Notre approche NextGen CyberSOC

Contact
Mr VALLET Gérald / gerald.vallet@orange.com

69002 Lyon
orangecyberdefense.com

Other comptencies :

Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

Cybersecurity - digital security: IoT device security

Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications

SOFT'IDEAS

Soft'ideas is a start-up, which develops innovative and comprehensive software solutions, to provide deep technical answers to problems encountered, particularly in industry, but still unresolved or at least not completely. Soft'ideas provides expertise in, in all activities with computer sciences requirements such as industrial IT energy, aeronautics, defense, petrochemicals and indoor geolocation and path finding.

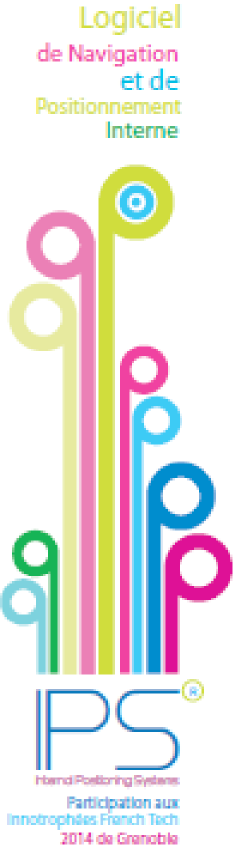
Cyber Security Expertise : Military FRANCE for export delivery, Automotive (EliteCyber / Thales pour Renault Nissan), Enedis (electrical PWR supply metering).

Product / service description

Advice & Expertise, Audit Defensive Architecture & Countermeasures, Risk Analysis, Vulnerability Analysis, PenTest.

Target markets

Defence, Automotive, ePower Plant.



Contact
Mr SAHIRI Ali / a.sahiri@softideas.fr

38100 Grenoble
softideas.fr

Other comptencies :

- Cybersecurity - digital security: IoT device security
- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

SPIE ICS

SPIE ICS is a French digital services company and a subsidiary of SPIE, the independent European leader in multi-technical services in the areas of energy and communications. SPIE ICS supports the digital transformation of mid-sized and major customers with a global offer of ICT solutions.

Product / service description

The concepts of security and cybersecurity differ in the nature of the risks addressed. SPIE ICS offers a convergent 360° approach to security information systems. This involves taking a systemic approach to protection against malicious acts (theft, fraud, attacks, incivilities, terrorism, etc.), technical, physical, chemical or environmental risks (industrial accidents, fire, etc.) and cyber threats, with a view to regulatory compliance.

Design, integration, supervision or hypervision, as well as infrastructure maintenance are covered thanks to SPIE ICS' expertise and its certifications with software publishers and manufacturers.

Our teams capitalize on their expertise in sensitive customer environments.

The activity carries the ExpertCyber label developed by Cybermalveillance.gouv.fr

Target markets

Industry & services, health, public sector

Contact
Mr Lombard Arnaud / a.lombard@spie.com

92240 Malakoff
www.spie-ics.com

Other comptencies :

Videoprotection - surveillance: Hypervision, supervision

Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)

VIRTUAL OPEN SYSTEMS

Virtual Open Systems is an innovative, agile and dynamic SME software company specialized in virtualization, cyer security, Linux and embedded software for automotive, IoT edge, cloud computing solutions.
The company delivers most efficient architectures products and services for heterogeneous embedded multi-core platforms that increase value to its customers, help them to lower costs, to reduce time to market, while enhancing their value proposition.

Product / service description

Virtual Open Systems provides virtualization solutions for mixed-critical systems. VOSySmonitor is a key company product component to execute concurrently, on a single hardware platform, functionalities of different functional safety levels, compliant to ISO-26262 certification. VOSySmonitor: a low latency certified monitor layer for mixed-criticality systems on arm architecture VOSySmonitor is the software foundation component of the company's VOSySmcs and VOSySIoT software products, which are meant respectively for Automotive and IoT edge market segments. VOSySmonitor guarantees, when compared to traditional type-1 hypervisors, by its architecture design the best isolation of safety critical functionalities. VOSySmcs: automotive mixed-criticality virtualization product software stack VOSySmcs consists of a full fledged software stack to support modern generation of car virtual cockpits where the concurrent execution of In-Vehicle Infotainment (IVI), Instrument Digital Cluster and Body Control Module (BCM) can be consolidated on a single hardware platform, thus simplifying complexity, maintenance and costs of heterogeneous Electronic Component Units (ECU). The open nature of the VOSySmcs architecture breaks traditional vendor lock-in practices while unchaining innovation. VOSySIoT: an end-to-end iot software stack product developed for processing of iot applications VOSySIoT is an end to end IoT edge software stack, which is intended to protect and isolate the collection and processing of critical data. Industrial IoT, health monitoring, smart home, building, city, green energy, are market segments which benefit from VOSySIoT mixed-critical software product

Target markets

Automotive, drones, Industrial IoT, health, smart city/buildings, green energy

Contact
Mr Paolino Michele / m.paolino@virtualopensystems.com

38000 Grenoble
www.virtualopensystems.com

Other comptencies :

Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

Cybersecurity - digital security: IoT device security

Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)

ATOS DIGITAL SECURITY

The #1 in Europe and a global leader in cybersecurity – With a global team of over 6,000 security specialists and a worldwide network of Security Operation Centers (SOCs), Atos offers end-to-end security partnership. Our portfolio is bringing the power of Big Data Analytics and Automation to our customers for more efficient and agile security controls.

Also, our portfolio is built on 6 large building blocks which are all linked to Analytics and Automation. Therefore, all of our clients require more resources to protect their critical data: personal data, intellectual property, financial data, etc.

Product / service description

Atos offers a full spectrum of advanced detection and response services around the clock and across the globe: We have developed the next generation SOC, MDR Security Operation Center dedicated to preventing breaches by leveraging big data and supercomputing capabilities and automating security responses. We provide CERT services, with threat intelligence, CSIRT Services and vulnerability management. Our Advanced Detection and Response services establish highly resilient security practices to counter Advanced Persistent Threats (APT), SOC Services and context-aware IAM.

Contact
Mr Moret Chris / chris.moret@atos.net

38000 Grenoble
atos.net

Other comptencies :

- Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications
- Cybersecurity - digital security: IoT device security

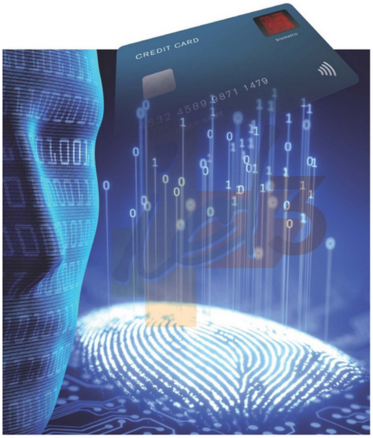
ID3 TECHNOLOGIES

id3 develops innovative solutions in the fields of artificial intelligence and biometrics to guarantee the identity of citizens, identify security threats, secure access to premises and goods, strengthen border security and secure payments and transactions.

Product / service description

Match on card: smart card embedded matching algorithm for offline biometric verification (face or fingerprint) BioSeal is the solution for securing your digital or physical documents. It generates a secure visible electronic seal that will contain both the key information of the document and the biometric identity of its owner.

Automatic biometric identification system: Our AFIS / ABIS provides the strongest protection against theft and identity theft. It consolidates and securely stores biographic and biometric data acquired by remote enrolment stations. It interfaces with our proprietary biometric engines to ensure the uniqueness of each identity. Translated with www.DeepL.com/Translator (free version)



Contact
Mr Lepetit Laurent / laurent.lepetit@id3.eu

38120 Le Fontanil Cornillon
www.id3.eu

Other comptencies :

- Cybersecurity - digital security: Data protection, identity protection, GDPR
- Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

ISORG

Isorg was founded in 2010 by a team of senior executives and technical experts from the hi-tech electronics and optical industries, offering complete solutions for large-area image sensors. The company's core technology successfully integrates printed photodiodes on different substrates to enable large-area image sensors for the smartphone and security markets and extended applications in medical X-ray imaging, non-destructive testing. Isorg's flexible, thin and light sensors allow various ways for integration with different form factors. Riding on our core competence on Organic Photo Diode (OPD) sensor technology and optics design, we aim to become the leading provider of large-area organic image sensor solutions. Isorg works closely with our customers to develop products and solutions meeting their specific requirements. We support delivery of our products from low to high volume with the Limoges factory and our major manufacturing partners.

Product / service description

Isorg, a spin-off from CEA-LITEN, was created in May 2010 in Grenoble. Being a pioneer in organic photodetectors and large area sensors, Isorg offers complete fingerprint sensor solutions with an excellent level of maturity recognized in two key markets: the consumer smartphone market and the security & identity market. Isorg is the first company in the world to offer a turn-key solution which enables fingerprint captures across the full screen surface of smartphones, as presented at CES 2020 in Las-Vegas under the pavilion of the CEA. The level of security offered by Isorg is increased tenfold. It therefore favours many applications that need higher security such as banking applications (wire transfers and mobile payments of larger amounts), health (monitoring of personal health, access to medical records) or daily uses by citizens (remote home control, password wallet, secure safe). For the security & identity market, Isorg is the first solution provider in the world to be certified (last January) by the FBI in the category of optical sensors based on organic photodiodes. This certification is the key to enter the global market which asks for this recognition for different types of applications such as border control, access control, citizen identity, police control, electronic voting, attendance control, etc.

Target markets

smartphone, security and ID, biometrics

Contact
Mr BERNARDIN Nicolas / nicolas.bernardin@isorg.fr

87068 Limoges
www.isorg.fr

Other comptencies :

- Cybersecurity - digital security: Data protection, identity protection, GDPR
- Economic security: Anti-fraud/anti-counterfeiting

LCIS - GRENOBLE INP - UGA

LCIS
Laboratoire de Conception et d'Intégration des Systèmes

In a world where distributed and pervasive systems are ubiquitous (IoT, connected objects, smart homes, etc.), particularly in critical applications (autonomous vehicles, aeronautics, medical applications, etc.) or security applications (smart cards, access control, etc.), operational safety and security are two key issues.
To ensure the safety and security of these systems, their design must be approached in a global manner, as a flaw or vulnerability in one element can compromise the entire system.

Product / service description

The CTSYS group of the LCIS laboratory is made up of researchers from different disciplines (electronics, computer science, telecom) who study the different elements of embedded systems: from hardware to application. Particular attention is paid to the interaction between hardware and software. From hardware to software, the group's main research areas are: hardware security of embedded systems, software verification and testing, dependability of embedded systems, safety and security in networks of connected systems, safety and security of distributed and pervasive applications. The main application areas of the group's research are: the Internet of Things (including RFID systems), sensor networks, Smart-* environments (Home, Building, Car, etc), the transportation industry...

Contact
Mr Maitre Emmanuel / emmanuel.maitre@grenoble-inp.fr

38000 Grenoble
lcis.grenoble-inp.fr

Other comptencies :

Cybersecurity - digital security: IoT device security

Cybersecurity - digital security: Software, application, electronic transaction, and cloud security

PYXALIS

Pyxalis is a French company specializing in the design and manufacturing of high-performance CMOS image sensors, meeting the challenges of today and tomorrow, with off the shelf or custom solutions.

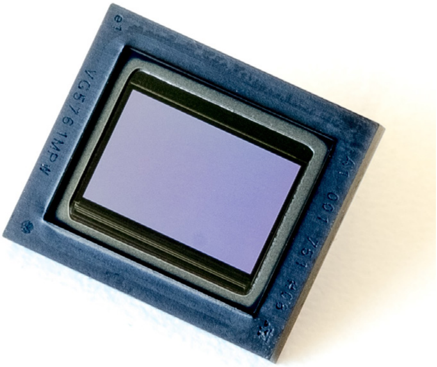
Pyxalis products find their spot in medical imaging, the environment, safety and safety, with a particular focus on space development. Created 10 years ago in the Grenoble Imaging valley, Pyxalis offers a unique set of digital imaging skills, ranging from custom pixel design, advanced digital circuits and embedded algorithms, thanks to a multidisciplinary team of 40 people. The primary characteristics of Pyxalis image sensors are image quality above all, sensitivity in low light levels but also a perfect adaptation to the specifications of each application thanks to flexible and very programmable architectures.

Product / service description

HDPYX 230-G is a global shutter low noise and high dynamic sensor designed for most challenging environments. It offers excellent image quality in 16bits straight from the sensor output over a temperature range of -40 to 105 degrees C, making it suitable for embedded mobile, outdoor or vehicle-mounted applications for defense purposes. It also has a standard MIPI interface, making it compatible with many of the commercial's embedded digital platforms. It comes in several versions: monochrome, color but also color / near infrared, which gives it excellent properties in night vision.

Target markets

Defense / Surveillance / aerospace



Contact
Mr Dupont Benoit / benoit.dupont@pyxalis.com

38430 Moirans
www.pyxalis.com

Other comptencies :

- National security and safety - risk and crisis management - civil security: Military materials and equipment and protective equipment (fire safety, search and rescue, combat, anti-terrorism)
- Videoprotection - surveillance: Drones, robots, remote monitoring tools

HYPERION SEVEN

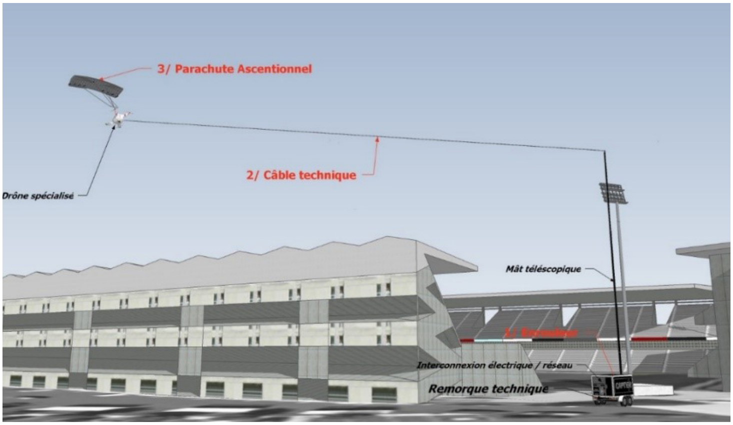
Hyperion Seven is developing a patented security concept around a lightweight and tamper-proof wired drone bringing together connected technologies. These innovations make our solution the first multi-sensor flying object that never falls.

Product / service description

Our solution, which cannot be hacked, is easily adaptable to any type of context, with the capacity to carry 4Kg of sensors (at a minimum), in unlimited duration, with a significant flow of data facilitating postprocessing in real time on the ground. Knowing that the drone and its payload can be safely repatriated if necessary. Thus, we are responding in an innovative way to the needs of territorial and public surveillance, in particular by having the possibility of simultaneously embedding optical, sonic and chemical sensors.

Target markets

We are targeting the territory and public security market



Contact
Mr NIER Olivier / olivier.nier@hyperionseven.com

38640 Claix
www.hyperionseven.com

Other comptencies :

Videoprotection - surveillance: Hypervision, supervision

National security and safety - risk and crisis management - civil security: Detection of explosives, prohibited substances, trafficking

EMG2

EMG2 offers innovative technologies for the optimization of your projects. Whether in the form of components, modules, electronic boards, or integrated platforms, our solutions are ready to be configured and easily deployed. Such versatile and often complementary products provide effective and even original answers for a wide variety of needs.
As a result of its solid experience, wide vision of the electronics market, and recognized network of partners, EMG2 can recommend solutions that will efficiently meet your requirements. Its teams of experts actively support you through your projects and requests, embracing longterm relationships and ensuring customer satisfaction.

Product / service description

NATvision is a comprehensive environment for the development and deployment of sophisticated video and image processing solutions with significant compute resources to support artificial intelligence and machine learning algorithms. It is based on the combination of various technological hardware and software bricks in order to constitute a complete platform capable of acquiring multiple video streams, according to various protocols and of processing them in real time with synchronization options.

NATvision is thus a very high performance, modular and versatile solution, but it is also fully reconfigurable and scalable to adapt to many use cases like visual inspection functions (quality control, anomaly detection, industrial vision), analysis and fusion (medical imaging for example) or for video surveillance and public security (aggregation of multiple streams, Filtering and analysis, Compression and recoding)

Target markets

Machine vision - defense and security - intrumentation

Contact
Mr Besseau Anthony / anthony.besseau@emg2.com

91140 Villebon-sur-Yvette
emg2.com

Other comptencies :

- Cybersecurity - digital security: Information systems security: infrastructures, networks, and communications
- Cybersecurity - digital security: Storage - backup

CORTUS

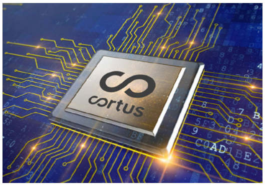
In a world where distributed and pervasive systems are ubiquitous (IoT, connected objects, smart homes, etc.), particularly in critical applications (autonomous vehicles, aeronautics, medical applications, etc.) or security applications (smart cards, access control, etc.), operational safety and security are two key issues.
To ensure the safety and security of these systems, their design must be approached in a global manner, as a flaw or vulnerability in one element can compromise the entire system.

Product / service description

Cortus offers a full range of ASIC design services, including firmware and software. These are some of the areas in which we have expertise:- Mixed-Signal [ADC, DAC, TRNG, PLL..] Analog [LDO, Charge pumps, Sensors, PLL, Bandgap, DC/DC, PMU...] Processors [RISC-V ISA, Cortus ISA, compact low power to high performance, Multicore, Caches, MMU, CoProcessors, AMBA Buses, Lock-step...] Digital [DDR, USB, Ethernet, CAN Low Power, Internal Memories, External memory interfaces, FPGA, SystemC modelling...] Security [Encryption/decryption, Hashing, Uniform execution time, TRNG, Monitoring, Secured CPUs, SPA/DPA resistance, Secure compiler, ISO14443, ISO 7816...] Protocols [IoT, Comms, ...] Functional Safety [Dual core lockstep, TMR, IEC 61508] Software [Compilers & Tools, Security tools, Debugger and JTAG i/f, IDEs, ISS] Real Time Operating Systems If you need something different to make you better than your competitors, then talk to us. We may well be able to come up with exactly what you need. Our highly experienced experts with their wide domain knowledge backed with our extensive IP portfolio will enable Cortus to architect the optimal silicon solution for your product. Cortus has a track record of making their customers successful. We have a wide range of experience. RF [Sub-GHz, LNA, Mixers, Fractional N Synthesis ...] System Architecture [Low Power, Power Management, FPGA Prototyping/Implementation, HW/SW Tradeoff...]

Target markets

IoT/NB-IoT,
Automotive,
HPC/AI



Contact
Mr Chapman Michael / michael.chapman@cortus.com

34130 Mauguio
www.cortus.com

Other comptencies :

Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)

National security and safety - risk and crisis management - civil security: Mobility and logistics support equipment and port, airport, rail, and road transportation security

GIPSA-LAB - GRENOBLE INP - UGA

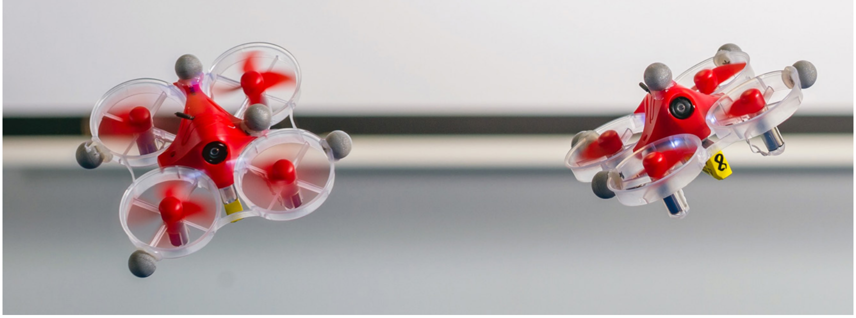
Gipsa-lab is a CNRS research unit joint with Grenoble-INP (Grenoble Institute of Technology), Université Joseph Fourier and Université Stendhal. It has agreements with INRIA, Observatoire des Sciences de l'Univers de Grenoble and Université Pierre Mendes France.

With 350 people, including about 150 doctoral students, Gipsa-lab is a multidisciplinary research unit developing both basic and applied researches on complex signals and systems. Gipsa-lab is internationally recognized for the research achieved in Automatic Control, Signal and Images processing, Speech and Cognition.

The research unit develops projects in the strategic areas of energy, environment, communication, intelligent systems, Life and Health and language engineering. Thanks to the research activities, Gipsa-lab maintains a constant link with the economic environment through a strong partnership with companies.

Product / service description

The research focuses on the development of safe and autonomous navigation systems as well as on the development of advanced functions such as manipulation or contact drones. This activity brings together people from the fields of command control, image analysis, real time systems, mechanics and electronic engineers around the realization of prototypes of flying robots.



©Cyril Fresillon / GIPSA-lab / CNRS Photothèque

Contact
Mr Maitre Emmanuel / emmanuel.maitre@grenoble-inp.fr

38401 Saint Martin d'Hères
www.gipsa-lab.fr

Other comptencies :

- Videoprotection - surveillance: Hypervision, supervision
- Cybersecurity - digital security: Identification, biometrics, identity and access management (IAM), security orchestration, automation and response (SOAR), information security operations center (ISOC), endpoint detection and response (EDR)

NEOVISION

Neovision is a company specialized in artificial intelligence. Its ambition is to make artificial intelligence accessible to all. It provides its customers with tailor-made and turnkey AI solutions through personalized support. Based in Grenoble and mainly composed of engineers and doctors in artificial intelligence, the company was founded in 2014 by three engineers in applied mathematics from Ensimag. Expert in algorithms and data science, the company is specialized in machine learning, deep learning and image analysis applications. Neovision constantly monitors the latest advances (scientific publications, open source software, databases, etc.) and invests in R&D on promising topics, in order to provide its customers with high-performance, state-of-the-art innovations.

Product / service description

Through its service offers, Neovision supports you in integrating AI into your company by relying on an efficient and proven methodology. In addition to its customized training offer, Neovision will help you define your AI strategy, and then design and validate the best AI solution for you. Finally, Neovision develops and industrializes the solution to facilitate its integration and generate a real ROI. Capitalizing on its experience and recognized expertise in computer vision, Neovision offers mature and ready-to-deploy technologies for image recognition, OCR and activity characterization. In addition, it also offers you data analysis software tools. Coupled with Neovision's expert support, they will help you considerably analyze your data and accelerate your AI projects.

Target markets

With hundreds of projects to its credit, Neovision is involved in various fields of activity such as industry, digital, health, smart city, environment and energy.

Contact
Mr Poissard Mathieu / mathieu.poissard@neovision.fr

38000 Grenoble
neovision.fr

Other comptencies :

Economic security: Anti-fraud/anti-counterfeiting

Videoprotection - surveillance: Hypervision, supervision

TELEDYNE E2V

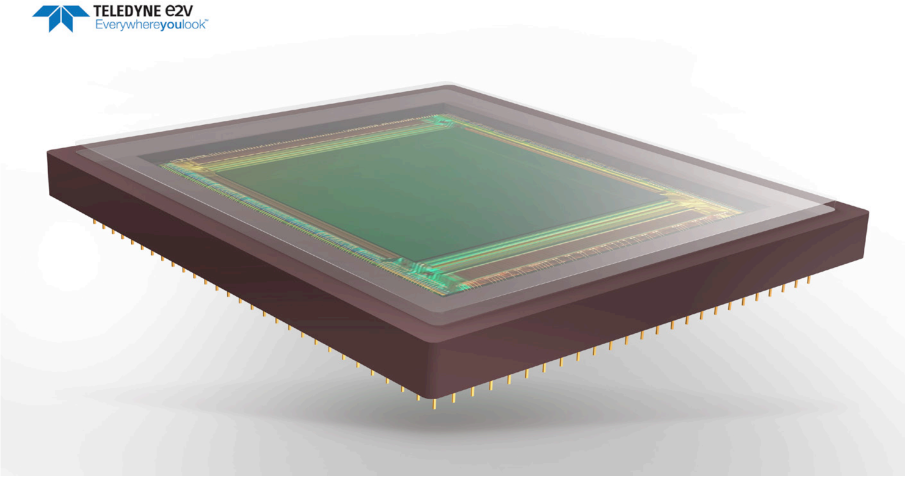
World-Leading Expert in High-Performance CMOS Imagers and Subsystems Standard or customized products for professional applications, The best low noise, low light performances, AI ready and customizables, Module ready if you like a quick Time to market.

Product / service description

CIS - Cmos imaging sensors Standard or Customs covering 1.3 to 67 Mpixels resolutions Low noise, high speed, global shutter, 3D time of flight, Optics integrated modules, with Mipi interface.

Target markets

Security, defense, industrial



Contact
Mr Hector Vincent / vincent.hector@teledyne.com

38000 Saint Egrève - Grenoble
www.teledyneimaging.com

Other comptencies :

- Videoprotection - surveillance: Hypervision, supervision
- Health security: Remote work/telework and remote medicine/telemedicine (improvements to working and remote working conditions, data security, crisis management, etc.)

MINALOGIC

Auvergne-Rhône-Alpes

MINALOGIC GRENOBLE

Maison Minatec - 3, Parvis Louis Néel - 38054 Grenoble Cedex 9 - France
Tel: +33 4 38 78 19 47

MINALOGIC LYON

Campus Région Numérique - 78 route de Paris - 69260 Charbonnières-les-Bains - France

MINALOGIC SAINT-ETIENNE

Bâtiment des Hautes technologies - 20 rue Benoît Lauras - 42000 Saint-Etienne - France

contact@minalogic.com - www.minalogic.com

www.graphistegrenoble.fr

Our public-sector partners

Our private-sector partners