SECURIT

TOWARDS RESILIENT SMART CITIES & TERRITORIES

Project Deliverable

D2.3 - Cybersecurity and security sector offers analysis 1
Mapping of security solutions offers

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Deliverable information	
Grant Agreement	N°101005292
Project Acronym	SecurIT
Project Title	New industrial value chain for Safe, sECure and Resilient cIties and Territories. Call: H2020-INNOSUP-2020-01-two-stage - Cluster facilitated projects for new industrial value chains
Type of action	IA Innovation action
Revision	V1.1
Due date	31/01/2022
Submission date	31/01/2022

Dissemination level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission)	
RE	Restricted to a group defined by the consortium (including the Commission)	
CO	Confidential, only for members of the consortium (including the Commission)	

Version	Date	Document history	Stage	Distribution
V0	14/01/2022	Document Creation	Draft	Consortium
V1	31/01/2022	Document review	Final	EC
V1.1	10/02/2022	Correction of misspellings	Final	Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table of content

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Abstract

The SecurIT project aims at supporting innovative technological solutions in the field of security, developed by 60+ consortiums of European SMEs, that are granted with a prototype or demonstrator voucher, through a top-notch selective process of 2 Open Calls. In fine, the project will support collaborative projects that will create a new industrial value chain.

This document has been developed as part of WP2 "*SecurIT Challenges definition*", Task 2.2 "*Mapping of security solutions offers*". This is the first release of this task, focusing on the products / services / solutions available in the domain of security, with a focus on the deeptech clusters in the SecurIT consortium. This mapping is in the shape of a catalogue of solutions proposed by 87 European companies (mainly SMEs), belonging to the ecosystems of the SecurIT consortium. It will be used to identify potential matching with the needs and applications during the open calls of SecurIT, especially for the matchmaking among potential applicants. This mapping will be updated before the second open call as the security sector is constantly

Authors (organisation)

Pôle SCS (leading organisation) with contributions from CenSec, HSD, L3CE, LSEC, SAFE, Systematic

Reviewers (organisation)

SAFE Cluster

Keywords

Security, Cybersecurity, Sensitive infrastructure protection, Disaster resilience, Public space protection, SME, catalogue, competences, products, solutions, services

Legal notice

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Introduction

This report is a mapping (catalogue) of security solutions, that are applicable to the SecurIT domains and challenges, namely:

Cybersecurity

Operations & optimisation of communication networks and alert systems

Identification and access control

Zone security and perimeter protection

Prior to crisis: prediction, risk knowledge and assessment

During crisis: communication and warning systems

After crisis: post event analysis and recovery

Detection and alert (real time)

Analysis

Decision making

Data protection, cybersecurity, cybercrime

Those security solutions have been identified by SecurIT cluster partners, based on the products/services/expertise provided by the companies of their ecosystem.

This deliverable is the first release, on a series of 2 mappings that will be delivered in the course of the SecurIT project.

The identified solutions proposed by companies (mainly SMEs), have been classified according to the to the above-mentioned SecurIT domains and challenges in terms of use cases and applications, and also according to their technological focus, in three main areas:

- **Cybersecurity**: the mapping has been done according to the taxonomy for cybersecurity as proposed by the European Cyber Security Organisation (ECSO)[1]. This taxonomy classifies cybersecurity capabilities. Five designated capabilities – identify, protect, detect, respond, recover – present concrete competences and means to mitigate, resolve, monitor and analyse cyber-related threats:
    - **IDENTIFY** – for the better organisational understanding of the IT infrastructure and cybersecurity readiness to manage cyber risks to individuals, systems, assets, data and capabilities.

[1] https://www.ecs-org.eu/documents/uploads/ecso-cybersecurity-market-radar-taxonomy-table.pdf https://www.ecs-org.eu/documents/publications/605de1e3a768a.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

- **PROTECT** – for appropriate safeguards to reduce the attack surface and to ensure the availability, integrity, confidentiality, auditability and performance of the critical IT services.
- **DETECT** – for appropriate tools to identify the nature and the scope of cyber-attacks carried out on the entity.
- **RESPOND** – for appropriate measures to effectively mitigate the detected cybersecurity incidents.
- **RECOVER** – appropriate action plans to bounce back from cyber-attack and to restore any capabilities or services affected

- **Cyber-physical security services**: this area covers security services that are based on cyber systems (digital) applied into a physical context/use case
  - **Audit, planning and advisory services** (e.g.: Security audit, vulnerability and intrusion testing, and risk and threat assessment)
  - **System integration and implementation services** (e.g.: Implementation and integration, interoperability testing)
  - **Management and operations services** (e.g.: Security system management and operations)
  - **Security training services** (e.g.: IT / cyber-security education and training)

- **Other security products and solutions**: this area covers all the other technological products and solutions (including digital but not exclusively) that are applicable to security context/use case.
  - **Identification and authentication** (e.g.: identification, accreditation and authentication systems for persons (including with biometrics); e.g. PIN and chip cards, identity cards, passport systems, etc.; Identification and authentication of materials, goods and equipment (e.g. vehicle recognition, protection against forgery and counterfeiting))
  - **Intruder detection and alarm/Fire detection**, alarm and suppression
  - **Detection and screening for dangerous or illicit items or concealed persons** (e.g.: screening of persons, baggage, cargo; Specialised detection for CBRNE (chemical, biological, radiological, nuclear, and explosives) and other risks)
  - **Observation and surveillance (localised)** (e.g.: Video and other observation and surveillance systems (e.g. CCTV) including video analytics etc.)
  - **Observation and surveillance (wide area)**
  - **Tracking and, tracing, positioning and localisation** (e.g.: Tagging and tracking devices and systems (e.g. bar code, RFID, Wi-Fi-based)
  - **Tracking, localisation and positioning of hazardous substances and devices** (e.g. radioactive materials, hazardous chemicals, etc.))
  - **Command, control and decision support**
  - **Intelligence and information gathering**
  - **Vehicles and platforms** (e.g.: aircraft; UAVs; robotic platforms)
  - **Equipment and supplies for security services**

The next section classifies the identified solutions (by company names) firstly according to the SecurIT domains and challenges, and then accordingly to their technological focus.

Then, one presentation sheet per company is available (in total 87 companies).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Domain #1 - Sensitive infrastructure protection

AKIDAIA
Algodone
ALL4TEC
Alpha Strike Labs
APEX Solutions
Aquilae
Arbit Cyber Defence Systems
aXite Security Tools
Bubo Initiative
CASD
Ceeyu bv
CFLW Cyber Strategies
Chapter8 BV
CII Telecom
Codean
co-dex.EU
Compumatica
CS Group
Cyberium
Derant
DeveryWare
DYNFI
Eagle Shark Cyber Defence
EclectiIQ
EONEF
EZAKO
Firmalyzer bvba
FOXSTREAM
Global Smart Solutions
HARUSPEX
Hermitage solutions
Hudson Cybertec
IC REP
IDECSI
Intigriti nv
IoT Trust
IPCOMM
Isuna
KALIMA systems
KLETEL
Komsetas
LIUM
Lorenz Technology
Montimage
NEOWAVE
NOVASECUR
OLVID
OXIBOX
Phished.io
Pontem IT
PROHACKTIVE
PRYSM
RECIPROQ IT
Red Alert Labs
SCILLE PARSEC
SECURE IC
SecuredNow
SENSIVIC
Setinstone
SIKUR
SmartGlobal
SMITHS DETECTION
STID
STIMSHOP
SYNEXIE
TEHTRIS
The Danish Institute for Fire and Security Technology
Toreon cvba
TPL
TrustHQ
Ucrowds
UniText
Videtics
Wisekey
X-Systems BV
ZAFEHOUZE
Zybersafe Aps

Domain #2 - Disaster resilience

Algodone
ALL4TEC
APEX Solutions
Aquilae
Ceeyu bv
CII Telecom
Codean
co-dex.EU
CS Group
Cyberium
DeveryWare
DIGINOVE
Eagle Shark Cyber Defence
EDICIA
EONEF
EZAKO
Firmalyzer bvba
Global Smart Solutions
Hermitage solutions
Hnit-Baltic
Hudson Cybertec
IDECSI
Intigriti nv
IoT Trust
IPCOMM
Isuna
KALIMA systems
KLETEL
Lorenz Technology
MIDGARD
PATROLAIR
Phished.io
Pontem IT
PRYSM
RECIPROQ IT
Red Alert Labs
SCILLE PARSEC
SECURE IC
SmartGlobal
SMITHS DETECTION
SYScience
TEHTRIS
The Danish Institute for Fire and Security Technology
Toreon cvba
TPL
TrustHQ
Ucrowds
UniText
VSM
X-Systems BV
ZAFEHOUZE
Zybersafe Aps

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Domain #3 - Public spaces protection

Acrux cyber services
Algodone
ALL4TEC
Alpha Strike Labs
APEX Solutions
Aquilae
Arbit Cyber Defence Systems
aXite Security Tools
Bubo Initiative
CASD
Ceeyu bv
CII Telecom
co-dex.EU
Compumatica
CS Group
DeveryWare
DROON
Eagle Shark Cyber Defence
EclectiIQ
EDICIA
EONEF
EZAKO
Firmalyzer bvba
Global Smart Solutions
HARUSPEX
Hnit-Baltic
Hudson Cybertec
IC REP
IDECSI
IoT Trust
IPCOMM
KALIMA systems
Kibernetinis saugumas
Lorenz Technology
MIDGARD
Montimage
PATROLAIR
Phished.io
Pontem IT
PRYSM
RECIPROQ IT
Red Alert Labs
SCILLE PARSEC
SECURE IC
SENSIVIC
SIKUR
SmartGlobal
SMITHS DETECTION
STIMSHOP
SYNEXIE
TEHTRIS
The Danish Institute for Fire and Security Technology
Toreon cvba
Ucrowds
Videtics
Wisekey
X-Systems BV
ZAFEHOUZE
Zybersafe Aps

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Cybersecurity

IDENTIFY	AKIDAIA	Montimage	Lorenz Technology
	Algodone	NEOWAVE	Pontem IT
	ALL4TEC	NOVASECUR	Red Alert Labs
	Alpha Strike Labs	PATROLAIR	SENSIVIC
	Aquilae	Phished.io	SIKUR
	Arbit Cyber Defence Systems	Firmalyzer bvba	SmartGlobal
	Ceeyu bv	Global Smart Solutions	SMITHS DETECTION
	Chapter8 BV	Hnit-Baltic	STID
	CII Telecom	Hudson Cybertec	The Danish Institute for Fire and Security Technology
	Codean	IPCOMM	TPL
	Compumatica	Isuna	TrustHQ
	Cyberium	KALIMA systems	Wisekey
	DROON	KLETEL	
	EONEF	Komsetas	
	EZAKO	LIUM	

PROTECT	Acrux cyber services	IC REP	Red Alert Labs
	AKIDAIA	Intigriti nv	SCILLE PARSEC
	Algodone	IPCOMM	SECURE IC
	Alpha Strike Labs	Isuna	SENSIVIC
	Aquilae	KALIMA systems	Setinstone
	Arbit Cyber Defence Systems	Komsetas	SIKUR
	Ceeyu bv	LIUM	SmartGlobal
	Chapter8 BV	MIDGARD	STID
	CII Telecom	Montimage	STIMSHOP
	Codean	NEOWAVE	SYNEXIE
	Compumatica	OLVID	TPL
	DIGINOVE	OXIBOX	TrustHQ
	DROON	PATROLAIR	UniText
	Eagle Shark Cyber Defence	Phished.io	Videtics
	EONEF	Pontem IT	Wisekey
	EZAKO	PROHACKTIVE	X-Systems BV
	Firmalyzer bvba	PRYSM	ZAFEHOUZE
	Hermitage solutions	RECIPROQ IT	Zybersafe Aps
	Hnit-Baltic	SecuredNow	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

DETECT	AKIDAIA Algodone Alpha Strike Labs Aquilae Arbit Cyber Defence Systems aXite Security Tools Ceeyu bv Chapter8 BV CII Telecom Codean co-dex.EU Compumatica CS Group DROON	DYNFI Eagle Shark Cyber Defence EDICIA EONEF EZAKO Firmalyzer bvba FOXSTREAM Global Smart Solutions Hermitage solutions KALIMA systems Komsetas LIUM Phished.io	Hnit-Baltic IPCOMM RECIPROQ IT Red Alert Labs SCILLE PARSEC SECURE IC SENSIVIC SIKUR SmartGlobal TPL Videtics ZAFEHOUZE Zybersafe Aps
RESPOND	Acrux cyber services AKIDAIA Algodone ALL4TEC Alpha Strike Labs Aquilae Arbit Cyber Defence Systems aXite Security Tools Ceeyu bv Chapter8 BV CII Telecom co-dex.EU Compumatica	Cyberium DIGINOVE DYNFI Eagle Shark Cyber Defence EDICIA EONEF EZAKO Hnit-Baltic IC REP IoT Trust IPCOMM LIUM NEOWAVE	NOVASECUR OLVID Phished.io Red Alert Labs SCILLE PARSEC SECURE IC SENSIVIC SmartGlobal TPL TrustHQ Videtics ZAFEHOUZE Zybersafe Aps
RECOVER	Acrux cyber services AKIDAIA Algodone ALL4TEC Alpha Strike Labs Aquilae	Ceeyu bv Chapter8 BV DIGINOVE EONEF Hnit-Baltic IPCOMM	Komsetas NEOWAVE SIKUR SmartGlobal SMITHS DETECTION

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Cyber-physical security services

AKIDAIA
Algodone
Alpha Strike Labs
Aquilae
aXite Security Tools
Ceeyu bv
Chapter8 BV
CII Telecom
Compumatica
DeveryWare
DROON
Eagle Shark Cyber Defence
EONEF
EZAKO
Hnit-Baltic
IDECSI
IoT Trust
IPCOMM
Isuna
KALIMA systems
KLETEL
Komsetas
LIUM
Montimage
NEOWAVE
SCILLE PARSEC
SENSIVIC
SIKUR
SmartGlobal
STID
STIMSHOP
SYNEXIE
The Danish Institute for Fire and Security Technology
TPL
Ucrowds
UniText
Videtics

Other security products and solutions

Acrux cyber services
AKIDAIA
Algodone
ALL4TEC
Alpha Strike Labs
APEX Solutions
Aquilae
Arbit Cyber Defence Systems
aXite Security Tools
Bubo Initiative
CASD
Ceeyu bv
CFLW Cyber Strategies
Chapter8 BV
Cyberium
Derant
DYNFI
Eagle Shark Cyber Defence
EZAKO
Global Smart Solutions
HARUSPEX
Hermitage solutions
IC REP
Intigriti nv
IoT Trust
IPCOMM
KALIMA systems
Komsetas
MIDGARD
PATROLAIR
Phished.io
Pontem IT
PROHACKTIVE
Red Alert Labs
SCILLE PARSEC
SIKUR
SMITHS DETECTION
SYScience
Toreon cvba
TPL
Videtics
VSM
X-Systems BV

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Acrux cyber services

The company

UAB Acrux cyber services is an information technology company that provides its services to public and private sector entities both in Lithuania and abroad. The company specializes in software development and cyber security services.

Proposed offer for security

UAB Acrux cyber services is developing a product which is targeted to identify infected websites for chosen countries. Detection is performed using various techniques. Detection in the future will be fully automated for several detection methods with an optional human analyst for the most advanced detection method. All detected infections are recorded and can be replayed for the forensic purposes. The primary targeted user of this product are national CERTs. At a moment the product is in the initial stages and its product (list of infected websites in Lithuania) is provided as a service to the Lithuanian national CERT. The results of this product are much wider / broader compared to any commercial security vendor - e.g. Antivirus, etc.

Linguistic Recognition: NLP Algorithm developed by Acrux cyber services team allows to identify the author of a text similarly as you can identify a person by fingerprints.

Thus, it is possible to de-anonymize criminals who publish on forums or social networks. You can also identify "troll factories", bots or publications of user groups acting on the same instruction. As part of R&D, the algorithm showed an accuracy of 87% on data from the politician subforum on reddit. The algorithm is resistant to typos and language distortion.

Contact

Vilnius, Lithuania https://acruxcs.com info@acruxcs.com

Cluster member L3CE

Specific market sector

Government

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Type of solutions

		Linguistic Recognition
Cybersecurity	> DETECT	> Detection Processes *(Underground/Darkweb investigation, Social Media & Brand Monitoring)*
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)* > Communications > Analysis *(Fraud Investigation, Forensics)*
Other security products and solutions	> Observation and surveillance (wide area)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

AKIDAIA

The company

AKIDAIA provides an innovative and digital access control solution which works without Internet and without infrastructure. Easy to install. Fast to manage. With your smartphone and your digital key you can open all electrified opening systems.

Proposed offer for security

Patenting technology to control the access everywhere, even the most isolated areas:

1. The offline Akidaia Minibox, plug'n'play on all opening systems, portals, gates, doors, etc.
2. The backoffice to follow and manage accesses with a phone number.
3. The secured mobile application is a digital keychain, communicating via encrypted Bluetooth Low Energy to answer the Akidaia Minibox offline defy.

Contact

Nice, France

https://www.akidaia.com

contact@akidaia.com

Cluster member

Specific market sector

Security, Identification and Access Control

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Identification and access control, Zone security and perimeter protection)

Type of solutions

Cybersecurity	> PROTECT	> Identity Management & Access Control *(Access Management Authentication, Authorisation, Identity Management)*
Other security products and solutions	> Identification and authentication > Tracking and, tracing, positioning and localisation	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Algodone

The company

ALGODONE has been created in Montpellier (France) to propose IoT secure management platforms dedicated to objects in very hostile environments

Proposed offer for security

Algodone technology is made of a licence server (Saas) and of hardware security IP's to be embedded in Electronic systems, Asics, Microcontrollers or FPGA to secure transactions and data transfers between distant management platform and objects in networks

Contact

Montpellier, France http://www.algodone.com support@algodone.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Defence, Aerospace, Industry 4.0, Automotive

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Detection and alert (real time), Data protection, cybersecurity, cybercrime)

Solutions

SALT™

Cybersecurity	> PROTECT	> Identity Management & Access Control *(Authentication Authorisation, Identity Management)* > Data Security (*Data Leakage Prevention, Cloud Access Security Brokers, Hardware Security Modules (HSM))* > Information Protection Processes and Procedures > Protective Technology *(Remote Access/VPN, IoT Security, PC/Mobile/End Point Security, Mobile Security /Device management, Backup / Storage Security)*
	> DETECT	> Anomalies and Events *(Intrusion Detection)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

ALL4TEC

The company

ALL4TEC designs and distributes risk analysis tools for cybersecurity.

Proposed offer for security

Risk management tool and risk analysis tool. ALL4TEC is labelled by the French agency ANSSI for EBIOS Risk Manager method

Contact

Change, France http://www.all4tec.com lac@all4tec.net

Cluster member

Specific market sector

All sectors

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Analysis)

Solutions

Agile Risk Manager & Agile Risk Board

Cybersecurity	> IDENTIFY	> Governance & Risk Management *(Security Certification, Governance, Risk & Compliance (GRC))* > Risk Assessment > Risk Management Strategy > Supply Chain Risk Management
Cyber-physical security services	> Audit, planning and advisory services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Alpha Strike Labs

The company

Alpha Strike Labs is an innovative German company in the field of cyber open source intelligence. With the help of global internet scans we identify potential attack surfaces of a company/agency on the Internet.

Proposed offer for security

Alpha Strike Labs' decentralized search engine scans the entire Internet (2.8 billion routed IP addresses) for various specific network services, systems, or vulnerabilities. We identify your digital attack surface from the perspective of a real attacker. We detect your systems regardless of whether they are hosted by you or a third party such as a cloud provider. In addition, we can also audit your service providers as part of supply chain security.

Contact

Berlin, Germany https://www.alphastrike.io office@alphastrike.io

Cluster member

CenSec

Specific market sector

Big companies (all sectors), National Cyber Security Agencies

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #3 - Public spaces protection (Analysis, Data protection, cybersecurity, cybercrime)

Solutions

Cyber Open Source Intelligence (Cyber OSINT)

Cybersecurity	> IDENTIFY	> Asset Management *(IT Service Management)* > Risk Assessment > Supply Chain Risk Management
	> PROTECT	> Maintenance *(Vulnerability Management)*
	> DETECT	> Security Continuous Monitoring *(Cyber Threat Intelligence, Security Operations Center (SOC))*
Cyber-physical security services	> Audit, planning and advisory services	
Other security products and solutions	> Intelligence and information gathering	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

APEX Solutions

APEX SOLUTIONS
THINKING OUT OF THE BOX

The company

APEX solutions has the vision of becoming a leading private R&D partner for new risk approaches (innovative methodologies, fast-running models, GIS-based solutions…).

Proposed offer for security

Development of fast-running risk models and geographic data analysis of stakes.Some applications : blast propagation in urban configurations (ANR URBEX project), GIS-database processing for fire and rescue services, physical protection modelling for critical infrastructures, modelling of CBRN-RE threats...

Contact

Flaujac-Gare, France https://apex-solutions.fr/ contact@apex-solutions.fr

Cluster member

SAFE

Specific market sector

First-responders, local authorities, private companies, critical infrastructures, etc.

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis)

Solutions

EPIC, URBEX, REMORA, BIM2SIM,

Cyber-physical security services	> Audit, planning and advisory services
Other security products and solutions	> Command, control and decision support > Intelligence and information gathering > Equipment and supplies for security services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Aquilae

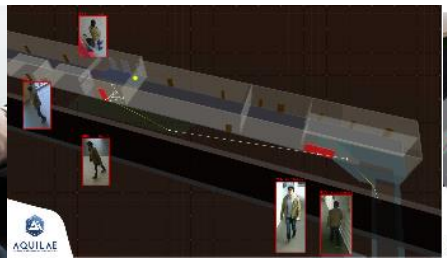
The company

French software editor in video analytics, Aquilae offers, via its patented technology in tracking and unsupervised learning, a reliable solution for automatic anomaly detection and real-time tracking of its source.

Proposed offer for security

Video analysis solution to detect anomalies:

- Intrusion detection
- Abnormal crowd movements
- Unsupervised anomaly detection
- Abandoned/unauthorized object detection
- Help to find a person: person and vehicle tracking



Contact

Rosières-près-Troyes, France www.l-aquilae.com contact@aquilae.tech

Cluster member

Specific market sector

Industry, logistics, defence, city, public facilities

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Solutions

Visia, Abnormality detection and people tracking, AI.track

Other security products and solutions	> Intruder detection and alarm/Fire detection, alarm and suppression > Observation and surveillance (localised) > Tracking and, tracing, positioning and localisation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Arbit Cyber Defence System

The company

Arbit delivers a full range of certified and accredited cross domain solutions for high security networks - both in the server room and on the battlefield.

Proposed offer for security

The Arbit Data Diode 10GbE handles data import and the Arbit Trust Gateway handles release of data. In addition they can be combined to enable remote desktop between separated networks (Arbit Desktop Gateway) and enable users to acces webservices on separated networks (Arbit Web Gateway).

Contact

Hvidovre; Denmark https://arbitcds.com info@arbitcds.com

Cluster member

CenSec

Specific market sector

Defence, Defence industry, Law enforcement, Government, Criritcal infrastructure and Intelligence

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Zone security and perimeter protection)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Arbit Data Diode/Arbit Trust Gateway

Cybersecurity	> PROTECT	> Data Security *(Data Leakage Prevention)* > Protective Technology *(Content Filtering & Monitoring, Firewalls / NextGen Firewalls, Anti Virus/Worm/Malware)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

aXite Security Tools

The company

aXite Security Tools is a Dutch cybersecurity company with a focus on data-driven solutions for both Information Technology and Operational Technology (OT).

Proposed offer for security

aXite Security Tools developed an intelligent and patented OEM independent platform including a Gatekeeper to execute zero trust access control and active defence in-depth for OT End Point protection at field level for operational equipment in the field of airport security and for critical infrastructure.

Contact

The Hague, Netherlands www.aXite-SecurityTools.com lars.willemsen@security-tools.nl

Cluster member

HSD securitydelta.nl

Specific market sector

Airports and critical infrastructure

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Identification and access control)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Data protection, cybersecurity, cybercrime)

Solutions

AX-BOX Change Control, AX-BOX Gatekeeper, AX-MANAGE Platform

Cybersecurity	> IDENTIFY	> Governance & Risk Management *(Governance, Risk & Compliance (GRC))*
	> PROTECT	> Identity Management & Access Control *(Access Management, Intrusion Protection)*
	> DETECT	> Anomalies and Events *(Intrusion Detection)*
	> RESPOND	> Mitigation *(DDoS protection)*
Cyber-physical security services	> System integration and implementation services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

BUBO Initiative

The company

BUBO INITIATIVE provides turnkey solutions for cybersecurity, developped especially for small and medium size companies. BUBO INITIATIVE is able to ansewer to their needs in terms of cybersecurity: adapted solutions, easy to use and already customised to their requirements.

Proposed offer for security

- Bubo SENTRY, for easy and quick visualising of the level of security maturity of a given activity, with consolidated indicators and thematic dash boards
- Bubo HUNT, for warning and monitoring of security events
- Bubo FLIGHT, to delegate the use of the Bubo Cybersec tools.
- Bubo NEST, to train staff to Bubo Cybersec solutions

Contact

Gardanne, France https://bubo-cybersec.com/ l.valat@bubo-cybersec.com

Cluster member

Specific market sector

Cybersecurity

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Bubo SENTRY, Bubo HUNT, Bubo FLIGHT, Bubo NEST

Cybersecurity	> PROTECT	> Identity Management & Access Control *(Access Management)* > Maintenance *(Vulnerability Management)*
	> DETECT	> Anomalies and Events *(Intrusion Detection)* > Security Continuous Monitoring *(SIEM / Event Correlation Solutions, Cyber Threat Intelligence, Security Operations Center (SOC))*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

CASD

The company

CASD, specialised in industrial image processing, was created to design solutions for high-performance digital CCTV.

Proposed offer for security

CASD with the VisiMax TM range offers recorders and software for recording, visualising and replaying with CCTV cameras.

Contact

Veurey-Voroize, France https://casd.fr/ casd@casd.fr

Cluster member

Specific market sector

Video Management System for public and private end-users

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Zone security and perimeter protection)

Domain #3 - Public spaces protection (Detection and alert (real time))

Solutions

VisiMAX VMS

Other security products and solutions	> Observation and surveillance (localised) (e.g.: Video and other observation and surveillance systems (e.g. CCTV) including video analytics etc.) > Observation and surveillance (wide area)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Ceeyu

The company

Ceeyu.io is an innovative and dynamic start-up company providing and servicing a cybersecurity ratings (digital footprinting) and third party risk management platform (TPRM).

Proposed offer for security

Ceeyu platform continuously monitors the digital footprint and supply chain. By passively gathering security and information disclosure related data. Ceeyu algorithm provides specific security rating that objectively, and transparently, measures the company's security posture. Self-assessment questionnaires help to stay on top of the third party risks via our built in third party risk, or TPRM, framework.

Contact

Bonheiden; Belgium www.ceeyu.io hello@ceeyu.io

Cluster member

LSEC

Specific market sector

Government, Enterprise, Financial Services, Energy, Retail, Industry, Pharma, ICT, Healthcare, Transport, Utilities, Water, Essential Services, digital and online services

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Zone security and perimeter protection)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)
Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making)

Solutions

		Digital Footprinting, TPRM
Cybersecurity	> IDENTIFY	> Asset Management > Governance & Risk Management > Risk Assessment, > Risk Management Strategy > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control, > Maintenance
	> DETECT	> Anomalies and Events > Security Continuous Monitoring > Detection Processes
	> RESPOND	> Communications, > Mitigation
	> RECOVER	> Recovery Planning, > Improvements
Cyber-physical security services	> Audit, planning and advisory services, > System integration and implementation services > Management and operations services	
Other security products and solutions	> Intelligence and information gathering	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

CFLW Cyber Strategies

The company

Propelled by its ambition to disrupt criminal activities that abuse cyberspace and emergent technologies, CFLW provides solutions at the intersection of strategy and technology to stay secure in the digital transformation and to navigate through the cyber-physical convergence.

Proposed offer for security

Dark Web and Virtual Assets are often abused to support online crimes. CFLW Intelligence Services help to combat these avenues abused by cybercriminals. Based on long track record services are developed as Dark Web Monitor and Virtual Assets (Cryptocurrencies) analytics. Dark Web Monitor (DWM) is an open-source intelligence (OSINT) platform that provides strategic insights and operational perspectives into criminal and fraudulent activities arising from exploitation of the Dark Web and Virtual Assets.

Contact

Gravenzande, Netherlands https://cflw.com info@cflw.com

Cluster member

HSD securitydelta.nl

Specific market sector

Law Enforcement, Cyber Security Organisations, Finance/FinTech

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Solutions

CFLW Intelligence Services, Dark Web Monitor

Cybersecurity	> DETECT	> Security Continuous Monitoring *(Cyber Threat Intelligence)* > Detection Processes (*Social Media & Brand Monitoring, Underground/Darkweb investigation)*
	> RESPOND	> Analysis *(Fraud Investigation, Forensics)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Chapter8

The company

Next-level pentesting. Chapter8 doesn't solely focus on hacking (red) or defending (blue). Chapter8 uses years of experience in high-profile environments to combine the two in Assignments that result in mutual improvement and real-time security gains for its clients.

Proposed offer for security

(Continuous) Purple Teaming is as close to an actual breach as you want to get. Our Hacker will perform advanced adversary simulation while our Hunter sharpens your defensive measures, actively helping you to trace down Hacker. Our Healer will analyse other facets of your forensic readiness and translate the Purple Team findings to the boardroom.

Contact

The Hague, Netherlands https://chapter8.com questions@chapter8.com

Cluster member HSD securitydelta.nl

Specific market sector

High value information, vital infrastructure, government

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Identification and access control)

Solutions

(Continuous) Purple Teaming

Cybersecurity	> IDENTIFY	> Risk Assessment > Risk Management Strategy
	> PROTECT	> Maintenance *(Penetration Testing / Red Teaming)*
	> DETECT	
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)*
	> RECOVER	> Improvements (Post incident reviews & consulting)
Cyber-physical security services	> Audit, planning and advisory services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

cii télécom

The company

cii telecom, a software publisher, is specialized in telecommunications solutions since 1990. Leader in public alert automaton solutions, voice servers, mass SMS sending solutions, etc. We work daily to connect people for more security, efficiency and peace of mind.

Proposed offer for security

téléalerte is a hosted alert call automation solution (SaaS). This solution is intended for the prevention of risks via the distribution of alert messages, by automatic telephone calls, sending of faxes, sending of SMS, sending of emails, sending of notifications (smartphone application alert&moi and Oyé-Oyé), sending messages on Twitter, Facebook, on pager, on variable message signs, on Vigie® (intelligent speakers) and siren triggering.

Contact

Le Mans, France
www.cii-telecom.fr
pjauneau@cii-telecom.fr

Cluster member

Specific market sector

Local authorities, hospitals, first responders, police, Seveso infrastructures, large companies, integrators

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Operations & optimisation of communication networks and alert systems)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis)

Solutions

téléalerte-mediaSig®

Cybersecurity	> IDENTIFY	> Risk Assessment > Supply Chain Risk Management
	> RESPOND	> Communications *(Crisis Communication)*
	> RECOVER	> Improvements (Post incident reviews & consulting)
Other security products and solutions	> Observation and surveillance	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Codean

The company

Criminal hackers are getting smarter every day. To combat them, we are helping out ethical hackers: we are building a Review Environment that makes the work of security analysts 2 times as fast (and up to 10 times faster for certain tasks).

Proposed offer for security

Most security analysts use an Integrated Development Environment (IDE) to analyze software, even though IDE's are designed for writing software. We have developed a 'Review Environment' that replaces the IDE. It is tailor made for security analysis: it has features ranging from keeping track what is reviewed, to symbiotic taint analysis. It automates mundane analysis tasks, and decreases the effort to write reports, so security analysts can focus on finding vulnerabilities. This enables security experts to deliver more quality in less time.

Contact

Utrecht, Netherlands https://codean.io/ arthur@cocean.io

Cluster member HSD securitydelta.nl

Specific market sector

Software security

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Solutions

		Codean Review Environment
Cybersecurity	> PROTECT	> Information Protection Processes and Procedures *(Static Application Security Testing (SAST), Application Security)* > Maintenance *(Penetration Testing / Red Teaming)*
Cyber-physical security services	> Audit, planning and advisory services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

co-dex.eu

The company

Growth company developing a Low-code & No-code development platform for governance and security solutions. GDPR & compliance management made easy to protect data, reputation and regulatory requirements.

Proposed offer for security

Digital register of data processing activities, Privacy and cookie policy generator, Online data processor agreements inventory, Incident management process, Inventory of IT assets (handling personal data storage), low-code & no- code development platform - cloud based…

Contact

Langemark-Poelkappelle, Belgium www.co-dex.eu info@co-dex.eu

Cluster member

LSEC

Specific market sector

SME-focused for GDPR and Security compliance; integrator and security-process oriented for no-code - low-code platform

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Solutions

no-codex, security compliance, co-dex

Cybersecurity	> IDENTIFY	> Asset Management, > Business Environment, > Governance & Risk Management, > Risk Assessment, > Risk Management Strategy, > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control, > Maintenance
	> DETECT	> Anomalies and Events, > Security Continuous Monitoring
	> RESPOND	> Response Planning, > Communications, > Analysis, > Mitigation, > Improvements
	> RECOVER	> Recovery Planning, > Improvements, > Communications
Cyber-physical security services	> Audit, planning and advisory services, > System integration and implementation services, > Management and operations services, > Security training services	
Other security products and solutions	> Identification and authentication, > Intruder detection and alarm, > Detection and screening for dangerous or illicit items or concealed persons, > Observation and surveillance, > Tracking and, tracing, positioning and localisation, > Command, control and decision support, > Intelligence and information gathering	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Compumatica secure networks

The company

Compumatica is a Dutch cyber security manufacturer specialized in crypto (network encryption, e-mail encryption) and network segmentation (firewall, Diode). The products have different security certifications from The Netherlands, European Union and NATO

Proposed offer for security

Compumatica offers a post quantum proof line encryption solution to encrypt data on L2, L3 and L4 of the OSI-Model, up to 100Gbps. The CryptoGuard is a 100% European product, certified by The Netherlands, European Union and NATO and used for more than 15 years by the Dutch government.

Contact

Uden, Netherlands www.compumatica.com info@compumatica.com

Cluster member

HSD securitydelta.nl

Specific market sector

Government

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

CryptoGuard, MagiCtwin Diode, CompuWall

Cybersecurity	> PROTECT	> Data Security *(Encryption)* > Protective Technology *(IoT Security, Firewalls / NextGen Firewalls)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

CS Group

The company

Designer, integrator & operator of intelligent and cyberprotected mission-critical systems.

Proposed offer for security

CS GROUP is a large French company with a complete range of high IT & OT cybersecurity services, solutions and products.

Contact

Le Plessis Robinson, France www.csgroup.eu communication@csgroup.eu

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Defence & Security, Aerospace, Nuclear

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Solutions

CS Cybersecurity, TrustyBox, SEDUCS MCS, SEDUCS Performer, Prelude SIEM, CERT-CS, Crimson

Cybersecurity	> IDENTIFY	> Asset Management, > Business Environment, > Governance & Risk Management, > Risk Assessment, > Risk Management Strategy, > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control, > Data Security, > Maintenance, > Protective Technology
	> DETECT	> Anomalies and Events, > Security Continuous Monitoring
	> RESPOND	> Response Planning, > Mitigation
	> RECOVER	> Improvements, > Communications
Cyber-physical security services	> Audit, planning and advisory services, > System integration and implementation services, > Security training services	
Other security products and solutions	> Identification and authentication, > Observation and surveillance, > Command, control and decision support	

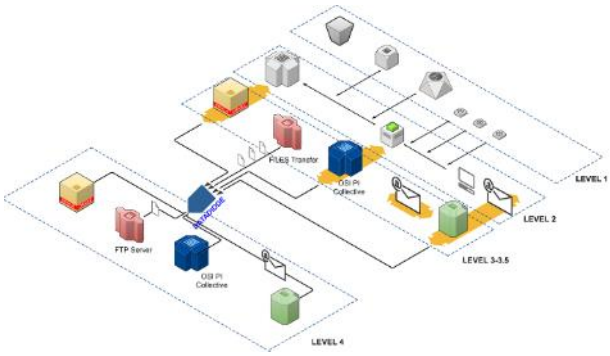
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Cyberium

The company

We are pure players in cyber security for industrial networks and systems. We offer solutions (hardware datadiodes, secure remote access, USB Kiosk), advice in the context of cyber risk management, threat profile, audits and intrusion tests, training relating to IEC / ISA 62443 , cyber risk management and industrial cyber security awareness.

Proposed offer for security



Products:

- CyberDiode: hardware datadiode - unidirectional communication - and associated software for applications
- DiD-USB - Full Defence-in-Depth protection against USB malware / removable media (including multi-engine A / V software and USB "diode")
- DiD-RemoteAccess, a real protocol break and multi-layered solution to considerably reduce the spectrum of attacks and allow true Defence-in-Depth secure remote operations.

Services:

- OT training
- OT risk management, risk assessment, Vulnerability Assessment, Maturity Assessment

Contact

Montpellier, France | https://cyberium.solutions | stan@cyberium.solutions

Cluster member

Specific market sector

Critical infrastructures & Government

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Solutions

Cybersecurity	> IDENTIFY	> Business Environment > Governance & Risk Management *(Governance, Risk & Compliance (GRC))* > Risk Assessment > Risk Management Strategy
	> PROTECT	> Awareness and Training > Maintenance *(Penetration Testing / Red Teaming)* > Protective Technology *(Remote Access / VPN, Mobile Security /Device management)*
Cyber-physical security services	> Audit, planning and advisory services > Security training services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Derant

The company

Leading experts in Network Detection and Response. Offers solutions for detecting even the most advanced hackers. SaaS-solution available.

Proposed offer for security

Network Detection and Response solution with advanced anomaly. Detects even very advanced hackers. Offered as self-service, managed or SaaS-solution.

Contact

Denmark www.derant.com info@derant.com

Cluster member

CenSec CENTER FOR DEFENCE, SPACE & SECURITY

Specific market sector

Public, private, utility, financial, medico, defence, IOT/production, critical infrastructure

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Solutions

Derant Angle

Cybersecurity	> PROTECT	> Data Security *(Data Leakage Prevention)* > Maintenance *(Vulnerability Management)* > Protective Technology *(IoT Security)*
	> DETECT	> Anomalies and Events *(Intrusion Detection)* > Security Continuous Monitoring *(Cyber Threat Intelligence, Security Operations Center (SOC))* > Protective Technology *(Remote Access / VPN, Mobile Security /Device management)*
	> RESPOND	> Analysis *(Forensics)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Deveryware

The company

Deveryware is leader in investigative technologies and services for global security. The Group's offer, covers digital forensics and investigation, real time geolocation, cybersecurity, anti-fraud services, crisis management and emergency communications.

Proposed offer for security

Cyber incident response by **TRACIP** (Deveryware group) : this offer allows for intervention in several incident scenarios, including: incident response on computer parks following ransomware infections and website defacement. We identify the infectious elements and trace their origin, recover all or part of the lost data and secure all the evidence for analysis to enable you to file a complaint.

CAIAC is a geographic information system (GIS) for business continuity planning and crisis management. Customizable GIS that brings together open data and proprietary data to better manage emergency situations. To Display and share the situation (up to 450 data layers available, depending on the country) and facilitate collaborative decision-making.

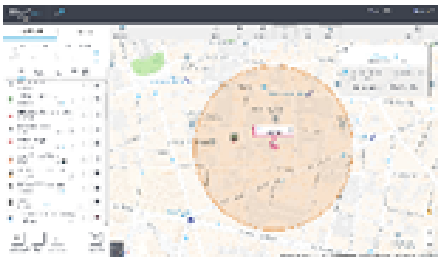
The « Field k'IT backpack » offers digital investigators a light and compact version of the existing kit (« Field k'IT stormcase). Tracip (Deveryware group) offers a complete kit including all the equipment, accessories and software essential to start an investigation in the field. The « Field k'IT backpack » is an urban kit that fits in a backpack. It incorporates the most important equipment of the stormcase kit (hexib'IT laptop, external blocker, duplicator).

"MOBIL'SECURITY" by Tracip (Deveryware Group): Mobile security screening gate for large events. Mobil'Security is a transportable screening station, strictly equivalent to fixed airport equipment, and can be deployed in a few hours. It can be deployed in a few hours and is strictly equivalent to fixed airport equipment. It allows an hourly throughput of 500 to 2000 people depending on the models (including PRM access).

Deveryware has developed a unique solution for the analysis of telephony investigation data: DeveryAnalytics Telephony Data. It enables to:

- detect contacts and interactions between individuals
- update networks
- save time and increase the investigative capacity of investigators

The solution has been adopted by the French Gendarmerie Nationale



DeveryLoc is an automated geolocation information processing system for targets that alleviates investigators' workload and contributes to the success of their missions. Thanks to DeveryLoc, users can:

- obtain the geolocation of beacons or mobile phones (in cooperation with telecom operators)
- set alerts to be informed of relevant events
- analyze position histories, etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Contact

Paris, France https://deveryware.com/ alain.soulier@deveryware.com

Cluster member

Specific market sector

Cybersecurity, Digital Forensics, business continuity planning and crisis management, Identification and access control

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Zone security and perimeter protection)
Domain #2 - Disaster resilience (After crisis: post event analysis and recovery)
Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Data protection, cybersecurity, cybercrime)

Solutions

Cybersecurity	> PROTECT	> Identity Management & Access Control *(Access Management)*	**MOBIL'SECURITY**
	> RESPOND	> Response Planning *(Crisis Management)* > Analysis *(Forensics)* > Mitigation *(Data Recovery* *Incident Response Services (CSRIT aaS))*	**CAIAC** **Field k'IT backpack** **TRACIP**
Other security products and solutions		> Observation and surveillance (localised) > Observation and surveillance (wide area) > Tracking and, tracing, positioning and localisation > Tracking, localisation and positioning of hazardous substances and devices > Intelligence and information gathering	**DeveryLoc** **DeveryAnalytics** **Telephony Data**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Diginove

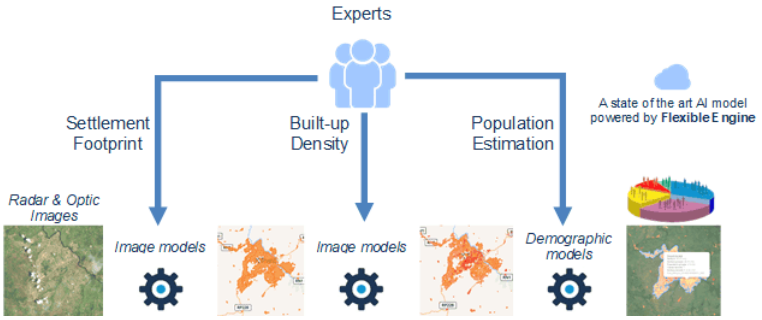
The company

Expert in image processing, DIGINOVE provides:
- DEXELIA: solutions for digitization, automatic recognition and compression of documents
- TELECENSE: accurately identifies and characterizes settlement areas and evaluates population distribution and trends, by leveraging satellite images.
- Solutions for user ground segments of defence satellites, as a subcontractor of Airbus-DS: compression, visualization, transmission and part of processing

DIGINOVE is an alumnus of ESA-BIC Sud-France and Copernicus Accelerator, supported by Connect-By-CNES and a member of the SAFE Cluster.

Proposed offer for security

TeleCense helps Companies, Authorities, International Organizations and Labs to assess and anticipate population growth and migration in emerging countries.



Contact

Aix-en-Provence, France www.diginove.com contact@diginove.com

Cluster member

Specific market sector

Insurance - Reinsurance - Public sector

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, After crisis: post event analysis and recovery)

Solutions

TeleCense

Other security products and solutions > Other

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

DROON

The company

Droon is expert in blockchain based solutions for cybersecurity, data protection, digital trust and collaboration, as Electronic vote, Data masking solutions or secured contract management, using permissioned blockchains, tokenisation and secured APIs.

Proposed offer for security

RansomDataProtect

RansomDataProtect allows to encrypt and mask sensitive or confidential information inside documents (word, Excel, Powerpoint), mails or Databases. Users creates "Circles of confidentiality" with approved Members who can decrypt and unmask / re-mask information. Documents can be shared, lost, stolen, ... readers will be able to read the documents, work on it, but won't be able to retrieve or reveal the hidden information. This is a solution of Selective Static Data Masking / Pseudonymisation.

Contact

Maisons-Alfort, France www.ransomdataprotect.com philippe.ogier@droon.io

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

All sectors facing risks of data leaks for sensitive (personal, medical) or confidential (legal, commercial, technical, …) data.

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

RansomDataProtect

Cybersecurity > PROTECT > Data Security *(Data Leakage Prevention, Encryption)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

DynFi

The company

DynFi provides two softwares: an Open Source Firewall and a Central Management System compatible with leading Open Source firewalls.

Proposed offer for security

DynFi Firewall is a complete perimeter firewall system that offers many network protection mechanisms. With DynFi Manager you will have at your fingertips a centralized management solution to administer several hundred devices.

Contact

Paris, France

https://dynfi.com

info@dynfi.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Transversal to all markets

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Zone security and perimeter protection)

Solutions

DynFi Firewall, DynFi Managed Services

Cybersecurity	> PROTECT	> Protective Technology *(Remote Access / VPN, Content Filtering & Monitoring, Firewalls / NextGen Firewalls, Unified Threat Management (UTM), Anti Spam, Anti Virus/Worm/Malware)*
	> DETECT	> Anomalies and Events *(Intrusion Detection)* > Security Continuous Monitoring *(SIEM / Event Correlation > Solutions, Security Operations Center (SOC))*
	> RESPOND	> Mitigation *(DDoS protection)*
Cyber-physical security services	> System integration and implementation services > Management and operations services	
Other security products and solutions	> Command, control and decision support	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Eagle Shark Cyber Defence

The company

Eagle Shark Cyber Defence is part of the Eagle Shark group. A private held cooperate intelligence agency with a strong focus on prevention and recovery within cyber security

Proposed offer for security

A software based Cyber Risk Assessment tool, the purpose of the CRA tool is to asses a companies maturity towards random cyber attacks.

Contact

Copenhagen, Denmark www.ESCD.dk crs@eagleshark.dk

Cluster member

Specific market sector

All sectors

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Eagle Shark CRA

Cybersecurity > IDENTIFY > Risk Assessment *(Risk Management solutions & services)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

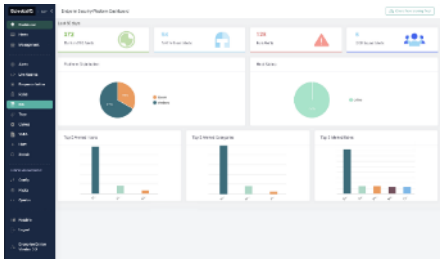
EclecticIQ

The company

EclecticIQ is a global provider of threat intelligence, hunting and response technology and services.
Stay ahead of rapidly evolving threats and outmaneuver your adversaries by embedding Intelligence at the core™ of your cyberdefenses.
We operate worldwide with offices and teams across Europe and UK, North America, India and via value-add partners.

Proposed offer for security

EclecticIQ Platform is an open and extendable platform that delivers threat intelligence automation and collaboration, forensic depth endpoint visibility, and threat detection and response. It helps you solve endpoint security, security operations, and threat intelligence challenges. Our solutions consist of modular products that let you customize capabilities to meet your specific needs.



Contact

Amsterdam, Netherlands www.eclecticiq.com info@eclecticiq.com

Cluster member

HSD securitydelta.nl

Specific market sector

Government, critical infrastructure, large enterprises and cyber security service providers.

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

EclecticIQ Intelligence Center, EclecticIQ Endpoint Response

Cybersecurity	> IDENTIFY	> Risk Assessment > Risk Management Strategy > Supply Chain Risk Management
	> PROTECT	> Protective Technology *(PC/Mobile/End Point Security)*
	> DETECT	> Anomalies and Events *(Fraud Management, Intrusion Detection)* > Security Continuous Monitoring *(Cyber Threat Intelligence Solutions, Security Operations Center (SOC))*
	> RESPOND	> Mitigation *(DDoS protection)*
Cyber-physical security services	> Security training services	
Other security products and solutions	> Intelligence and information gathering	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

EDICIA

The company

EDICIA is the software editor of CITY ZEN® a unique urban security platform. By combining business know-how and AI, CITY ZEN® allows a city or territory to govern its urban security continuum, while improving the performance of the means and resources dedicated to the safety and tranquillity of the citizen in the public space.

Proposed offer for security

CITY ZEN combining AI / ML at the heart and digital business services, delivers 3 levels of high added value activities:
- Anticipation of events, planning and dispatching of resources from the command center
- Dynamic and collaborative front and back office management of the daily activities of agents and operational managers
- Analytical observatories of delinquency, fraud and urban security

Contact

Nantes, France | www.edicia.fr | secretariatgeneral@edicia.fr

Cluster member

Specific market sector

Cities, Ministries, Public Transport, Public Spaces (Stadium, Shopping Centers, Airports, Rail Station, etc.)

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making)

Solutions

CITY ZEN

Other security products and solutions	> Intruder detection and alarm/Fire detection, alarm and suppression > Tracking and, tracing, positioning and localisation > Command, control and decision support > Intelligence and information gathering

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

EONEF

The company

EONEF is a French startup that develops and commercializes a tethered balloon inflated with helium equipped with antenna or camera to monitor extended sites. The height allows to be free of buildings or vegetation and cover large territories.
With this offer EONEF addresses 3 markets:

- Security & Safety for private industry, outdoor events and defence
- Telecommunication Emergency
- Wildlife conservancy

Proposed offer for security

EONEF is able to integrate various of its client's payload on one of its multi-purpose balloons (10m3 or 20m3 balloon).

- EO-20, 20m3, equipped with an EO/IR camera for surveillance
- Payload 1 to 5 kg.
- Electric winch with automatic rewinding and deployment.
- Ground balloon docking station for easy maintenance and safety of the system.
- Remote-controlled Day/Night camera with live image feedback (optional: automation of perimeter rounds and alert feedback).

Contact

Bobigny, France

https://eonef.com/

julie.dautel@eonef.com

Cluster member

Specific market sector

Security & Safety for private industry, outdoor events and defence
Telecommunication Emergency
Wildlife conservancy

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Operations & optimisation of communication networks and alert systems, Zone security and perimeter protection)

Domain #2 - Disaster resilience (During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time))

Solutions

EONEF - Tethered balloon surveillance camera

Cybersecurity	> IDENTIFY	> Business Environment, > Risk Assessment
	> DETECT	> Detection and anti-intrusion
	> RESPOND	> Communications
Other security products and solutions	> Observation and surveillance (wide area)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

EZAKO

The company

Ezako is ta startup based in Paris and in Sophia Antipolis / France. Ezako is a startup specializing in Artificial Intelligence and Deep Learning. Ezako is the editor of Upalgo, an automatic anomaly detection solution.

Proposed offer for security

Ezako is the editor of Upalgo, an anomaly detection solution. Upalgo identifies abnormal data activity and alerts users. With Upalgo's deep learning technology, security monitoring becomes more efficient and less expensive.

Contact

Paris & Sophia-Antipolis, France https://ezako.com/en/ contact@ezako.com

Cluster member

Specific market sector

Telecom, Automotive, Defence

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Detection and alert (real time))

Solutions

		Upalgo
Cybersecurity	> DETECT	> Anomalies and Events *(Fraud Management, Intrusion Detection)* > Security Continuous Monitoring *(SIEM / Event Correlation Solutions, Cyber Threat Intelligence Solutions, Security Operations Center (SOC))* > Detection Processes *(Underground/Darkweb investigation, Honeypots / Cybertraps, Social Media & Brand Monitoring)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Firmalyzer

The company

Firmalyzer is a leading provider of IoT vulnerability management and firmware analysis solutions to IoT vendors and enterprises.

Proposed offer for security

Firmalyzer developed IoTVAS to fill a crucial gap in the existing asset and vulnerability management solutions by accurate device discovery and risk. Firmalyzer enables IoT device manufacturers and their customers to discover and prioritize such risks in an automate, accurate and proactive way by performing global-scale security analysis of OT and IoT device firmware files assessment

Contact

Antwerp, Belgium www.firmalyzer.com contact@firmalyzer.com

Cluster member

LSEC

Specific market sector

IoT developers, device manufacturers, device operators, Industry, Telecom, ICT

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Data protection, cybersecurity, cybercrime)

Solutions

IoTVAS, Firmware Security Analysis

Cybersecurity	> IDENTIFY	> Asset Management, > Business Environment, > Governance & Risk Management, > Risk Assessment, > Risk Management Strategy, > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control, > Information Protection Processes and Procedures, > Maintenance, > Protective Technology
	> DETECT	> Security Continuous Monitoring, > Detection Processes
	> RESPOND	> Response Planning, > Analysis, > Mitigation, > Improvements
Cyber-physical security services	> Audit, planning and advisory services, > System integration and implementation services, > Management and operations services	
Other security products and solutions	> Identification and authentication, > Intruder detection and alarm, > Vehicles and platforms, > Equipment and supplies for security services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

FOXSTREAM

The company

Foxstream is a leading French specialist in innovative AI-powered video analytics software solutions. Foxstream is mainly present in the security / video surveillance market with an efficient infrastructure protection solution. Foxstream is present in France and abroad.

Proposed offer for security

Foxstream offers solutions in the security aera - outdoor intrusion detection, protection of the buildings. Today, several hundred sites (Seveso sites, solar plant, warehouses, car dealership, etc.) are secured by these solutions. Foxstream is also present in the "Flow Management" sector (Counting, waiting time, counting, etc.) in shops, airports and museums.

Contact

Vaulx-en-Velin, France www.foxstream.fr jb.ducatez@foxstream.fr

Cluster member

Specific market sector

Security - Video surveillance

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Zone security and perimeter protection)

Solutions

FoxVigi

Other security products and solutions

> Intruder detection and alarm/Fire detection, alarm and suppression
> Observation and surveillance (localised)
> Command, control and decision support
> Intelligence and information gathering

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Global Smart Solutions

The company

Global Smart Solutions develops a hardware and software solution to optimize rescue management. The Little Alert Box is a resilient and intelligent monitoring and communication device.

Proposed offer for security

The Little Alert Box offers resilience and real time monitoring with intelligent data analysis. The Little Alert Box can detect anomalies and alert automatically via Wi-Fi & satellite.

Contact

Labège, France https://globalsmartrescue.com/ aya.radi@globalsmartrescue.com

Cluster member

Specific market sector

Rescue management, Security & Monitoring, Smart Cities

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Operations & optimisation of communication networks and alert systems, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Solutions

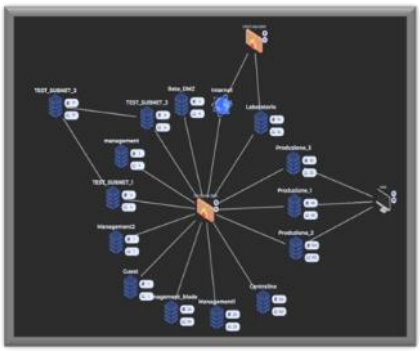
	Little Alert Box	
Cybersecurity	> IDENTIFY	> Risk Assessment > Supply Chain Risk Management
	> RESPOND	> Response Planning *(Crisis Management)*
	> RECOVER	> Improvements
Other security products and solutions	> Identification and authentication > Intruder detection and alarm/Fire detection, alarm and suppression > Observation and surveillance (wide area) > Command, control and decision support > Intelligence and information gathering	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Haruspex

The company

A digital-twin based solution that finds all the cyber-threats to your systems, and neutralizes them all with the minimum effort required.



Proposed offer for security

An AI-based cyber-solution that finds all the potential cyber-threats and adopts the minimum number of countermeasures to neutralize all the risks.

Contact

La Spezia, Italy

www.haruspexsecurity.com

info@haruspex.it

Cluster member

Specific market sector

Cybersecurity

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Zone security and perimeter protection)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Solutions

		H-PAR
Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management)* > Governance & Risk Management *(Security Certification Governance, Risk & Compliance (GRC))* > Risk Assessment > Risk Management Strategy > Supply Chain Risk Management
	> PROTECT	> Maintenance *(Patch Management, Vulnerability Management, Penetration Testing / Red Teaming)* > Protective Technology *(IoT Security, PC/Mobile/End Point Security)*
	> DETECT	> Anomalies and Events (*Intrusion Detection)* > Security Continuous Monitoring *(SIEM / Event Correlation Solutions, Cyber Threat Intelligence, Security Operations Center (SOC))*
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)* > Analysis *(Fraud Investigation, Forensics)*
	> RECOVER	> Improvements
Cyber-physical security services	> Audit, planning and advisory services > Management and operations services	
Other security products and solutions	> Command, control and decision support > Intelligence and information gathering	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Hermitage Solutions

The company

Responsu has been working towards a more secure society since 2012 and has already helped hundreds of various professionals to gain and improve their cybersecurity skills. Since 2019 started developing cybersecurity awareness platform to everyone within organizations

Proposed offer for security

Responsu cybersecurity awareness online training platform empowers organizations to build a strong cybersecurity culture and helps companies of all sizes and industries turn their employees into "human firewalls", reduce costs, simplify training administration and strengthen IT security posture

Contact

Vilnius, Lithuania www.responsu.com paulius@hermitage.lt

Cluster member L3CE

Specific market sector

All, but especially regulated GDPR, ISO.

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Responsu trainings platform

Cybersecurity	> PROTECT	> Awareness and Training
Cyber-physical security services	> Security training services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Hnit-Baltic

The company

Hnit-Baltic is an exclusive Esri distributor in Lithuania, Latvia and Estonia, providing geospatial analyses and solutions for all domains, including Public Safety, Emergency Management and Disaster Resilience

Proposed offer for security

We offer our services and expertise for combining and analysing geospatial data within the ArcGIS platform and applying the best selection of ArcGIS tools for your organizations specific needs and goals

Contact

Vilnius, Lithuania

www.gisbaltic.eu

info@hnit-baltic.lt

Cluster member

Specific market sector

Public Safety, Emergency Management and Disaster Resilience

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Decision making)

Solutions

	ArcGIS System	
Cybersecurity	> RESPOND	> Response Planning
Cyber-physical security services	> System integration and implementation services	
Other security products and solutions	> Tracking and, tracing, positioning and localisation > Command, control and decision support > Intelligence and information gathering	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Hudson Cybertec

The company

Cybersecurity Expert for Industrial Automation and Control Systems (IACS). We are an independent cybersecurity solution provider with years of experience in cybersecurity for Operational Technology.

Proposed offer for security

Hudson Cybertec provides services like professional security assessments, OT monitoring, consultancy & implementation, advanced OT cybersecurity Training & Workshops. As an internationally recognized Subject Matter Expert in cybersecurity for Industrial Automation & Control Systems we are specialized in the international cyber security standard (IEC 62443) and use it for assessments and developing policies & procedures.

Contact

The Hague, Netherlands www.hudsoncybertec.com info@hudsoncybertec.com

Cluster member

Specific market sector

Water management & drinking water, Road- and water infrastructure, Food & Feed, Chemical, Oil & gas, Storage and transhipment, Marine, Building Automation, and others

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems)
Domain #3 - Public spaces protection (Detection and alert (real time), Data protection, cybersecurity, cybercrime)

Solutions

OT Insight asset identification, IACS security business impact assessment, IEC 62443 readiness, OT Insight Compliance module, IACS security risk assessment, IACS Security Consultancy, Tabletop training/serious gaming, IACS patch management, IACS vulnerability management, IACS Security pentesting, OT Insight network anomaly module, OT Insight SIEM module, IACS Security Incident management, IACS Security crisis management, IACS Security business continuity, IEC 62443 Audit

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management)* > Business Environment, > Governance & Risk Management > Risk Assessment, > Risk Management Strategy, > Supply Chain Risk Management
	> PROTECT	> Awareness and Training, > Maintenance
	> DETECT	> Anomalies and Events, > Security Continuous Monitoring
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)*
	> RECOVER	> Improvements
Cyber-physical security services	> Audit, planning and advisory services, > Security training services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

IC REP

The company

Representative and distributor of electronics components and systems, including Flexxon for secure data storage solutions

Proposed offer for security

. Portable PC protected against ransomwares, illegal copying and cyberattacks
. SSD with embedded AI against ransomwares, cyber attacks and physical attacks
. Secured SD/µSD cards including several features, such as encryption, private partition, read-only
. Secured USB drives with several features, such as encryption, private partition, read-only possible.
. Military SSD with self destruct feature, secure erasing, encryption, protection against power cut off and overloads
. Protection and anti-piracy
. Anti-fraud and authentication

Contact

Septèmes les Vallons, France https://icrep.fr/ philippe@icrep.fr

Cluster member

Specific market sector

Cybersecurity

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Cybersecurity	> IDENTIFY	> Business Environment > Governance & Risk Management *(Governance, Risk & Compliance (GRC))* > Risk Assessment, > Risk Management Strategy > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control *(Authentication)* > Data Security *(Data Leakage Prevention, Encryption)* > Protective Technology *(Backup / Storage Security)*
	> DETECT	> Anomalies and Events, > Security Continuous Monitoring *(Cyber Threat Intelligence)* > Detection Processes
	> RESPOND	> Analysis *(Fraud Investigation)*, > Mitigation *(Takedown Services)*
Other security products and solutions	> Equipment and supplies for security services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

IDECSI

IDECSI
Enterprise Security

The company

First monitoring and detection platform communicating with users. IDECSI helps you resolve security and remediation issues related to access, rights, sharing, and configurations in Microsoft 365 cloud and on-premises environments.

Contact

Paris, France

www.idecsi.com

contact@idecsi.com

Cluster member

Systematic
Paris Region Deep Tech Ecosystem

Specific market sector

Large companies & MB

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Data protection, cybersecurity, cybercrime)

Solutions

IDECSI ADVANCED MONITORING, IDECSI AUDIT & ANALYSIS

Cybersecurity	> DETECT	> Security Continuous Monitoring *(SIEM / Event Correlation Solutions)*
	> RESPOND	> Analysis *(Forensics)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Intigriti

The company

Founded in 2016, Intigriti set out to conquer the limitations of traditional security testing. Today, the company is recognised for its innovative approach to security testing, impacting both security awareness and researcher's lives. Intigriti is a community-based ethical hacking platform.

Proposed offer for security

Intigriti helps companies protect themselves from cybercrime. Our community of ethical hackers provides continuous, realistic security testing to protect our customer's assets and brand. Our interactive platform features real-time reports of current vulnerabilities and commonly identifies crucial vulnerabilities within 48 hours.

Contact

Antwerpen, Belgium | www.intigriti.com | info@intigriti.com

Cluster member

LSEC

Specific market sector

ICT, Transport, Entertainment, HR, Public Authorities, Non Profit, Pharma, Automotive, Financial Services, etc.

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (After crisis: post event analysis and recovery)

Solutions

		ethical hacking, bug bounty platform
Cybersecurity	> IDENTIFY	> Asset Management, > Business Environment, > Governance & Risk Management, > Risk Assessment, > Risk Management Strategy, > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control, > Awareness and Training, > Protective Technology, > Information Protection Processes and Procedures, > Maintenance, > Protective Technology
	> DETECT	> Anomalies and Events, > Security Continuous Monitoring, > Detection Processes
	> RESPOND	> Response Planning, > Mitigation, > Improvements
Cyber-physical security services		> Audit, planning and advisory services, > System integration and implementation services, > Management and operations services, > Security training services
Other security products and solutions		> Identification and authentication, > Intruder detection and alarm/Fire detection, alarm and suppression, > Tracking, localisation and positioning of hazardous substances and devices, > Command, control and decision support, > Intelligence and information gathering, > Vehicles and platforms (e.g.: aircraft; UAVs; robotic platforms), > Equipment and supplies for security services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

IoT Trust

The company

Red Alert Labs is helping organizations trust IoT devices throughout their entire life-cycle. We are revolutionizing the way companies secure by design, assess and certify their connected solutions through innovation.

Proposed offer for security

IoTsTrust provides businesses with a cost-effective and scalable solution to assess the level of cybersecurity of connected ICT / IoT products from third-party vendors. We directly engage suppliers from all over the world with efficient evaluations and validate the results with accredited laboratories.

Contact

Alfortville, France www.iotstrust.com contact@redalertlabs.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Horizontal Market approach: Business Users/Buyers/Distributors of Connected Products

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management)* > Business Environment > Governance & Risk Management *(Security Certification, Governance, Risk & Compliance (GRC))* > Supply Chain Risk Management
	> PROTECT	> Maintenance *(Penetration Testing / Red Teaming)* > Protective Technology *(IoT Security, PC/Mobile/End Point Security)*
Cyber-physical security services		> Audit, planning and advisory services > Certification & Security Evaluation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

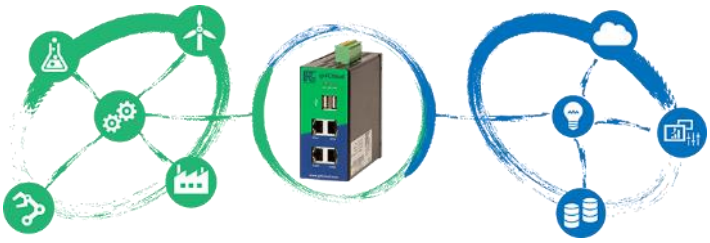
IPCOMM

The company

IPCOMM GmbH focus is on the development of industrial gateways and inter-network communication solutions. With over twenty years of experience we are able to offer solutions to almost any digital communication problem.

Proposed offer for security

ip4Cloud is able to extract information from existing systems with critical processes and transmit it to IT applications, cloud services, and SCADA systems for further processing.



Contact

Nuremberg, Germany https://www.ipcomm.de/ info@ipcomm.de

Specific market sector

Forward-looking manufacturing concepts provide for the connection of previously independent controllers, fieldbus devices, and SCADA systems to each other, as well as to the IT or IoT environment, as investment protection for existing plants/controllers.

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Analysis, Data protection, cybersecurity, cybercrime)

Solutions

	ip4Cloud, IPCOMM individual solutions	
Cybersecurity	> IDENTIFY	> Governance & Risk Management (*Governance, Risk & Compliance (GRC)*) > Risk Assessment > Risk Management Strategy > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control *(Access Management)* > Data Security *(Encryption)* > Protective Technology *(IoT Security, PC/Mobile/End Point Security)*
Cyber-physical security services	> System integration and implementation services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Isuna

The company

Isuna is a Regulation Technology company focused upon increasing resilience to cyber threats and building awareness of mitigation measures. We work with SMEs to help them save money by more easily understanding and implementing their cyber security needs.

Proposed offer for security

We provide a complete governance, risk and compliance platform. Our platform allows our clients to easily assess their cyber maturity, plan for improvements and save money by using the community to support them. We partner with www.nen.nl to apply ISO27001 to the cyber security needs of any size of business. Together we have simplified the standard, making it more understandable and achievable.

Contact

The Hague, Netherlands www.isuna.net info@isuna.net

Cluster member HSD securitydelta.nl

Specific market sector

Range of sectors including FinTech, Academic and Governmental

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, After crisis: post event analysis and recovery)

Solutions

Cybersecurity		**Cyber Compliance Platform**
	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management IT Service Management, Risk Assessment)* > Business Environment > Governance & Risk Management *(Security Certification, Governance, Risk & Compliance (GRC))* > Risk Assessment, > Risk Management Strategy > Supply Chain Risk Management
	> PROTECT	> Awareness and Training *(Awareness Trainings)* Protective Technology *(PC/Mobile/End Point Security)*
	> DETECT	> Security Continuous Monitoring *(Cyber Threat Intelligence Solutions)*
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)* > Communications
	> RECOVER	> Recovery Planning *(Business Continuity/Recovery Planning)* > Improvements *(Post incident reviews & consulting)*
Cyber-physical security services	> Audit, planning and advisory services > Management and operations services, > Security training services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

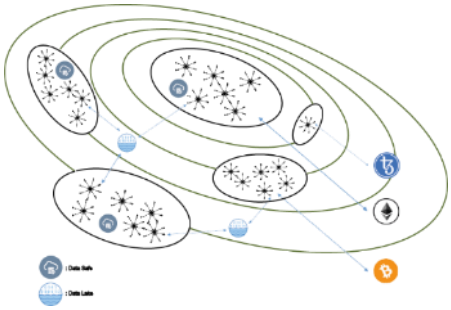
Kalima Systems

The company

Kalima Systems is a blokchain for IoT protocol. We provide software and hardware to collect transport and share IoT data with Kalima Blockchain.

Proposed offer for security

Kalima Systems goal is to create a new standard for Blockchain IoT applications.
More generally Kalima is a new way to interconnect objects, people and services with trust and to bring new possibilities to monetize data. We empower enterprise and developers to build the next generation of sustainable Blockchain applications building bridges between the physical and the digital world.



Contact

Paris, France

https://www.kalima.io/

info@kalima.io

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Data protection, cybersecurity, cybercrime)

Solutions

Kalima Blockchain

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management)* > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control *(Access Management, Authentication, Authorisation, Identity Management)* > Data Security *(Data Leakage Prevention, Hardware Security Modules (HSM))* > Protective Technology *(Wireless Security, IoT Security, PC/Mobile/End Point Security, Mobile Security / Device management, Backup / Storage Security)*
	> DETECT	> Anomalies and Events *(Fraud Management, Intrusion Detection*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Kibernetinis saugumas

The company

Research in the cybersecurity area; defence of the web portals; penetration testing

Proposed offer for security

We are developing a product which is targeted to identify infected websites for targeted country. It allows to see much more detailed situation. Detection is performed using various techniques. All detected infections are recorded and can be replayed for the forensic purposes. At a moment the product is used as a service by Lithuanian national CERT.

Contact

Vilnius, Lithuania https://tyrimai.esec.lt darius@esec.lt

Cluster member L3CE

Specific market sector

The primary targeted user of this product are national CERTs

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Data protection, cybersecurity, cybercrime)

Solutions

Websites infection detection and forensic system "WebReplicator"

Cybersecurity	> DETECT	> Security Continuous Monitoring *(Cyber Threat Intelligence)* > Detection Processes *(Underground/Darkweb investigation, Honeypots / Cybertraps, Social Media & Brand Monitoring)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

KLETEL

The company

For more than 30 years, Kletel designs and develops for its customers specific softwares that answer to their professional requirements. Kletel team is also deeply involves in R&D in the medical domain and e-health.

Proposed offer for security

The Bkube solution is a new product specially addressed to SMEs in order to protect their data from cyber attacks.
- First all-in-one automatic backup box, Mac and PC compatible
- Invisible backup solution on network: non-sensible to cyber attacks during data backups. The box disk is not accessible via network. Only the proprietary application can send files. Then it is no longer possible to modify them. Recovery is only possible in the event of a problem.
- Possibility of recovering previous versions of files, so possibility to recover an older version of a file that would have been modified.
- Integrated monitoring system: The monitoring system sends the user an alert of the backups that have been made. It notifies the user in case of problems, last backup made, remaining space on the disk and when backups that have not been made.

Contact

Nice, France | http://www.kletel.net/ | kletel@kletel.net

Cluster member

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #2 - Disaster resilience (After crisis: post event analysis and recovery)

Solutions

		BKUBE
Cybersecurity	> IDENTIFY	> Asset Management *(IT Service Management)* > Business Environment > Risk Assessment
	> PROTECT	> Data Security *(Encryption)* > Information Protection Processes and Procedures *(Static Application Security Testing (SAST), Application Security)* > Maintenance *(Penetration Testing / Red Teaming)* > Protective Technology *(Sandboxing, Backup / Storage Security)*
	> RESPOND	> Mitigation *(Data Recovery)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

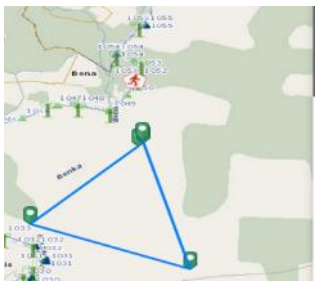
Komsetas

The company

The main activities of the company are the sale and maintenance of computer equipment, the design and manufacture and installation of electronic systems, the development and integration of information systems, sale and servicing of software.

Proposed offer for security

GIS Siena is an integrated software package for the protection of the zone. GIS Siena displays real-time signals received from optoelectronic and detection equipment on monitor screens and informs the system operator with an audible signal. All active events are displayed on the map with the corresponding icons.



Contact

Vilnius, Lithuania www.komsetas.lt tomas@komsetas.lt

Cluster member

Specific market sector

All market sectors in need of real-time perimeter protection.

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Zone security and perimeter protection)

Solutions

Zone security

Optoelectronic and detection equipment integration for positioning, localisation, tracking

Other security products and solutions	> Observation and surveillance (wide area) > Tracking and, tracing, positioning and localisation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

LIUM

The company

Lium is developing a tethered balloon solution which is able to onboard a performant camera and an artificial intelligence. This will able to survey large aeras during a wide period.

Proposed offer for security

Lium is a french start-up which develops unmanned tethered airships with embedded cameras. These balloons aim to help to survey sensitives sites such as nuclear sites, seveso sites and warehouse. What we offer is a long lasting solution to guarantee safety.

Contact

Orange, France https://www.lium-tech.com/ guilain@lium-tech.com

Cluster member

Specific market sector

Sensitive Sites

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Solutions

Other security products and solutions

> Observation and surveillance (localised)
> Observation and surveillance (wide area)
> Vehicles and platforms (e.g.: aircraft; UAVs; robotic platforms)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Lorenz Technology

The company

Lorenz Technology provides intelligent drone and robot solutions for the port and security segment.

Proposed offer for security

AI Link: A platform-agnostic edge-computing unit that enables drones and robots with global connectivity, controls UGV/UAV, and streams data to a cloud platform.
Hive: A cloud platform that allows to plan autonomous drone and robot missions, and displays/stores data.

Contact

Odense, Denmark https://www.lorenztechnology.com/ cbu@lorenztechnology.dk

Cluster member

Specific market sector

Ports, Airports, Security

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making)

Solutions

AI Link & Hive

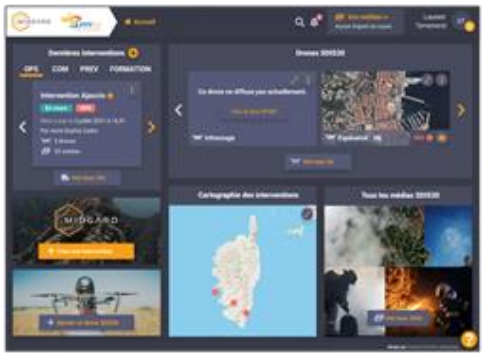
Other security products and solutions	> Intruder detection and alarm/Fire detection, alarm and suppression > Observation and surveillance (localised) > Observation and surveillance (wide area) > Tracking, localisation and positioning of hazardous substances and devices > Command, control and decision support > Intelligence and information gathering > Vehicles and platforms (e.g.: aircraft; UAVs; robotic platforms)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

MIDGARD

The company

MidGard is developing an decision support platform for Civil Security actors that allows firefighter drone data to be stored, visualized and analyzed automatically using Artificial Intelligence modules in order to plan their interventions.



Contact

Ajaccio, France https://www.midgard-ai.com/ contact@midgard-ai.com

Cluster member

Specific market sector

Civil Security

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Analysis, Decision making)

Solutions

MidGard.AI

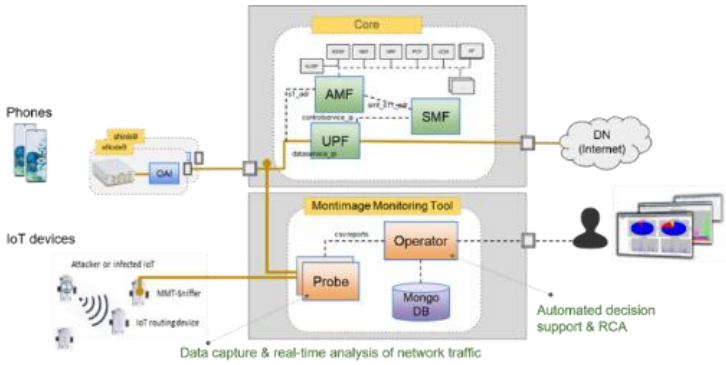
Cybersecurity	> PROTECT	> Identity Management & Access Control *(Access Management)* > Protective Technology *(Backup / Storage Security)*
Other security products and solutions		> Observation and surveillance (localised) > Observation and surveillance (wide area) > Command, control and decision support > Intelligence and information gathering

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Montimage

The company

Montimage develops innovative solutions for network monitoring, rapid and secure deployment of 4G / 5G networks and analysis of activities and business data (eg manufacturing process).



Proposed offer for security

A monitoring framework, MMT, of tools and services to protect and assess the quality of networks, including 4G/5G and IoT mobile networks ranging from physical to application network layers, business activity, and manufacturing processes. It includes intrusion detection and prevention (MMT-Probe), Cyber Threat Intelligence services (Cartimia), Root Cause Analysis (MMT-RCA), IoT sniffing (MMT-IoT), and pentesting/training tools (MI Cyberrange).

Contact

Paris, France https://www.montimage.com edgardo.montesdeoca@montimage.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Network administrators and operators, public administrations, Industry 4.0

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

MI Cyberrange, MMT-Probe, MMT, 5Greplay, MI Cyberrange, MMT-IoT, Cartimia, MMT-RCA, Montimage services, Montimage training

Cybersecurity	> PROTECT	> Awareness and Training *(Cyber Ranges)*, > Protective Technology *(PC/Mobile/End Point Security)*, > Data Security *(Data Leakage Prevention)* > Information Protection Processes and Procedures *(Application Security)* > Maintenance *(Penetration Testing / Red Teaming)* > Protective Technology *(Wireless Security, IoT Security, PC/Mobile/End Point Security, Mobile Security / Device management, Firewalls / NextGen Firewalls, Unified Threat Management (UTM))*
	> DETECT	> Anomalies and Events *(Intrusion Detection)* > Security Continuous Monitoring *(SIEM / Event Correlation Solutions, Cyber Threat Intelligence Solutions)*
	> RESPOND	> Analysis *(Forensics)*, > Mitigation *(DDoS protection)*
Cyber-physical security services		> Audit, planning and advisory services, > Security training services
Other security products and solutions		> Intelligence and information gathering

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

NEOWAVE

The company

NEOWAVE is a company specializing in strong authentication and secure transactions.

Proposed offer for security

NEOWAVE is a French company specialized in the design, manufacturing and marketing of strong authentication devices based on secure elements and digital certificate. We offer 3 product ranges: ID 2.0 solutions for logical and/or physical access control, FIDO range for strong authentication on the Web and in the cloud and Smart card readers for the implementation of multiple secure applications.

Contact

Gardanne, France

www.neowave.fr

contact@neowave.fr

Cluster member

Specific market sector

Cybersecurity, digital trust and Identity Access Management markets

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Identification and access control)

Solutions

FIDO range, ID 2.0 solutions

Cybersecurity	> PROTECT	> Identity Management & Access Control *(Access Management, Authentication, Authorisation, Identity Management)* > Data Security *(PKI / Digital Certificates, Encryption, Cloud Access Security Brokers, Digital Signature)* > Protective Technology *(Remote Access / VPN, IoT Security, PC/Mobile/End Point Security, Mobile Security / Device management, Sandboxing)*

Other security products and solutions	> Identification and authentication > Equipment and supplies for security services

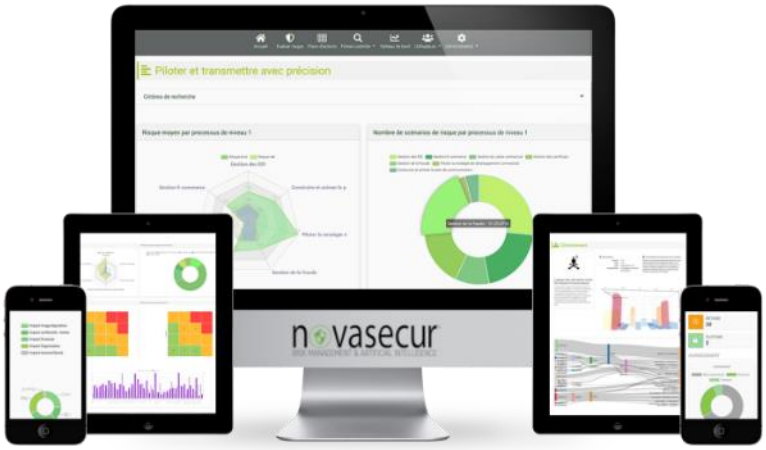
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Novasecur

The company

As software publisher and major player in Risk management, Novasecur develops the only modular solution covering all functionalities essential for risk management. Its ergonomics are user-oriented. Its integration is fast.

Its configuration capacity is great and its technological capacity to scientifically process all the data using Data Analytics and Artificial Intelligence makes it possible to industrialize their processing, to increase their informative value by providing recommendations concrete actions and bring a rapid return on investment.



Proposed offer for security

SIGR software : Information system for risk management

Contact

Aix-en-Provence, France http://www.novasecur.com/ Beatrice.rouillard@novasecur.com

Cluster member

Specific market sector

Cybersecurity

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Solutions

Cybersecurity	> IDENTIFY	> Governance & Risk Management *(Governance, Risk & Compliance (GRC))* > Risk Assessment
	> PROTECT	> Identity Management & Access Control *(Access Management)*
	> DETECT	> Anomalies and Events *(Fraud Management)* > Security Continuous Monitoring *(Cyber Threat Intelligence)*
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Olvid

The company

The most secure messaging app in the world. Olvid is the first instant messenger certified Security Visa (CSPN) by the French National Cybersecurity Agency (ANSSI). Only cryptography can guarantee true security of your communications. Do not rely on servers that may jeopardize this security.

Contact

Paris, France

https://olvid.io

contact@olvid.io

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

All sectors where secure communications matter.

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Solutions

Cybersecurity	> PROTECT	Data Security *(Encryption)* > Protective Technology *(PC/Mobile/End Point Security)*
	> DETECT	> Anomalies and Events *(Fraud Management, Intrusion Detection)* > Security Continuous Monitoring *(SIEM / Event Correlation Solutions, Cyber Threat Intelligence Solutions, Security Operations Center (SOC))* > Detection Processes *(Underground/Darkweb investigation, Honeypots / Cybertraps, Social Media & Brand Monitoring)*
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)* > Communications
	> RECOVER	> Recovery Planning *(Business Continuity/Recovery Planning)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Oxibox

The company

Oxibox ensures no company is subjected to data loss ever again. Our innovative technology ensures the capacity of all companies to be back in business instantaneously after a cyberattack.

Proposed offer for security

Oxibox protects data during its whole lifecycle. It allows for the creation of secure enclaves, isolated from the production network, protected from attackers and ransomwares. In a nutshell it ensures backups are ransomware-proof, usable, and allows for one-click restoration.

Contact

Guyancourt, France https://www.oxibox.com/fr/ julien@oxibox.fr

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

All companies and sectors with a current focus on SMBs and public entities.

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Solutions

Oxibox, Pxobpx

Cybersecurity	> PROTECT	> Protective Technology *(Backup / Storage Security)*
	> RESPOND	> Mitigation *(Data Recovery)*
	> RECOVER	> Recovery Planning *(System Recovery, Business Continuity/Recovery Planning)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

PATROLAIR

The company

PATROLAIR provides Services and products to improve UAV operations for parapublic and civil security missions.

Proposed offer for security

Helicopters/Airplanes and UAV's are complementary in security mission. Operations can be improved by creating a teaming (advanced cooperation) between both aircrafts operating in a same mission. UAV's detect, collect information and provide data's to helicopter crew who can save time to react or rescue people.

Contact

Venelles, France www.patrolair.com contact@patrolair.com

Cluster member

Specific market sector

Search and Rescue - Police – Firefighting, etc.

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #2 - Disaster resilience (During crisis: communication and warning systems)

Domain #3 - Public spaces protection (Detection and alert (real time), Decision making)

Solutions

MANNED UNMANNED TEAMING

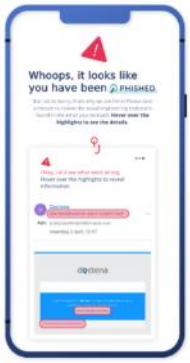
Other security products and solutions	> Command, control and decision support > Vehicles and platforms (e.g.: aircraft; UAVs; robotic platforms)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Phished.io

The company

Innovative CyberSecurity growth company focused on supporting organisations protecting their employees, building the human firewall. By creating solutions to protect in an office and home environments, Phished contributes to a safer internet.



Proposed offer for security

Phished is an AI-driven cybersecurity training platform, educating your employees on a broad range of cybersecurity topics using advanced, automated phishing simulations. Tailor-made learning based on personal knowledge and experience. Automated Cybersecurity Training.

Contact

Leuven Belgium https://phished.io/ info@phished.io

Cluster member

LSEC

Specific market sector

Enterprise, SME, public services. Media, Healthcare, Government, ICT, Financial Services, etc.

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Identification and access control, Zone security and perimeter protection)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management IT Service Management, Risk Assessment)* > Risk Management Strategy, > Supply Chain Risk Management
	> PROTECT	> Awareness and Training, > Information Protection Processes and Procedures *(Application Security)*, > Maintenance *(Patch Management, Vulnerability Management, Penetration Testing / Red Teaming)* > Protective Technology *(PC/Mobile/End Point Security, Mobile Security / Device management, Content Filtering & Monitoring)*
	> DETECT	> Security Continuous Monitoring (*Cyber Threat Intelligence Solutions, Security Operations Center (SOC)*) > Detection Processes *(Underground/Darkweb investigation, Honeypots / Cybertraps, Social Media & Brand Monitoring)*
	> RECOVER	> Communications *(Communications coaching & consulting)*
Cyber-physical security services	> Audit, planning and advisory services > Security training services	
Other security products and solutions	> Identification and authentication > Detection and screening for dangerous or illicit items or concealed persons	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Pontem IT

The company

Pontem IT offers an easy to operate affordable tool to defend companies critical processes and infrastructure from various external threats.

Proposed offer for security

Controller to temporarily physically isolate networks with the simple push of a button e.g. isolate production network from IT. Buys your business vital time by separating the most crucial part of your infrastructure, allowing critical processes to continue. Useful in the early hours of worldwide ransomware attacks or other highly potent vulnerabilities. Allowing disconnection, thread assessment, and reconnection in a uniform and simplified way across multiple (redundant) links simultaneously. All of this is done in a fool proof method including visual feedback providing real time insight to the operators, and therefore raising overall security awareness level.

Contact

Leiden, Netherlands www.pontemit.com info@pontemit.com

Cluster member

HSD securitydelta.nl

Specific market sector

Businesses that operate infrastructure, production facilities, factories with connected controllers to IT or internet.

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Insulator by Pontem, Insulator awareness and control training, Zoning your network by Pontem consultancy, Secureya VPN

Cybersecurity	> IDENTIFY	> Governance & Risk Management *(Governance, Risk & Compliance)* > Risk Assessment, > Risk Management Strategy
	> PROTECT	> Identity Management & Access Control *(Access Management)* > Awareness and Training , > Protective Technology *(Remote Access / VPN, IoT Security, Firewalls / NextGen Firewalls)*
	> DETECT	> Security Continuous Monitoring *(Security Operations Center (SOC))*
	> RESPOND	> Response Planning *(Incident Management)* > Mitigation *(Cyber Security Insurance)*
	> RECOVER	> Recovery Planning *(System Recovery, Business Continuity/Recovery Planning)*, > Improvements *(Post incident reviews & consulting)* > Communications *(Communications coaching & consulting)*
Cyber-physical security services	> Security training services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

ProHacktive

The company

ProHacktive is a preventive cybersecurity software company located in Région SUD. We are in a series A roadshow after having raised 2 million Euros since January 2020.

Proposed offer for security

ProHacktive has developed an innovative preventive, automatic and permanent cybersecurity solution to identify and issue alerts as soon as a known vulnerability is present on a network. The easy-to-understand administration interface provides an overview of all connected devices and associated risks in real time.

Contact

Gap, France | https://prohacktive.io | egd@prohacktive.io

Cluster member

Specific market sector

SME, institutions (local authorities, hospitals), large companies

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Solutions

		Sherlock
Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management)* > Risk Assessment
	> PROTECT	> Data Security *(Data Leakage Prevention* > Information Protection Processes and Procedures *(Application Security)* > Maintenance *(Patch Management, Vulnerability Management, Penetration Testing / Red Teaming)* > Protective Technology *(Remote Access / VPN, IoT Security, PC/Mobile/End Point Security)*
	> DETECT	> Security Continuous Monitoring *(Security Operations Center (SOC))*
Cyber-physical security services	> Audit, planning and advisory services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Prysm

The company

Prysm Software develops and markets AppVision™, an open-architecture control-command platform. It enables to manage fire and security systems (video, access control, intrusion, intercom, analytics, etc.), building management and SCADA systems, third-party applications, cybersecurity tools and new technologies (drones, robotics and Big Data) in a single interface.

Proposed offer for security

AppVision™ is an open-architecture control-command platform. It enables to manage fire and security systems (video, access control, intrusion, intercom, analytics, etc.), building management and SCADA systems, third-party applications, cybersecurity tools and new technologies (drones, robotics and Big Data) in a single interface.

Contact

Aix-en-Provence, France www.prysm-software.com david.fiorina@prysm.fr

Cluster member SAFE

Specific market sector

AppVision is efficient in any vertical

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making)

Solutions

	AppControl, AppVision, AppVideo	
Cybersecurity	> DETECT	> Anomalies and Events *(Intrusion Detection)* > Security Continuous Monitoring *(SIEM / Event Correlation Solutions, Security Operations Center (SOC))*
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)*
Cyber-physical security services		> System integration and implementation services > Management and operations services > Security training services
Other security products and solutions		> Identification and authentication > Intruder detection and alarm/Fire detection, alarm and suppression > Detection and screening for dangerous or illicit items or concealed persons > Observation and surveillance (localised) > Tracking and, tracing, positioning and localisation > Command, control and decision support > Intelligence and information gathering

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Reciproc-IT

The company

Incorporated in 2015, RECIPROC-IT is a consulting firm specializing in Information Systems security. Building up on our skills and expertise, we developed Oligo.rm, our Risk management platform.

Proposed offer for security

Oligo.rm, based on Ebios RM methodology, is a Risk management platform, providing a transversal response to cybersecurity threats: Digitizing risk analysis and control on a collaborative platform, Instating and spreading a culture of learning and awareness of cybersecurity threats, Evangelizing our clients in a continuous improvement process that places the business at the heart of action plans.

The concern about cyber risks is growing and the market is looking for tools to conduct a cyber risk reduction policy. In France, Ebios RM is considered as the industry standard in terms of methodology, both by companies and consulting firms, our solution based on this Ebios RM is labeled by the ANSSI, so we address the public and private sectors. Also, the SME market is lagging behind in the understanding of the security of their information systems. We are addressing this market first and foremost to evangelize and simplify access to cybersecurity. We want to provide these companies with the tools they need to carry out a real policy of continuous improvement in terms of security with a digital tool that will enable them to reduce costs and gain in efficiency.

Contact

Puteaux, France https://reciproc-it.com baya.lonqueux@reciproc-it.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Oligo.RM targets mainly the SME market.

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)
Domain #3 - Public spaces protection (Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Solutions

OLIGO.RISK MANAGEMENT

Cybersecurity	> IDENTIFY	> Governance & Risk Management > Risk Assessment > Risk Management Strategy > Supply Chain Risk Management

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Red Alert Labs

The company

Red Alert Labs is an independent IoT security lab and a cybersecurity consulting agency helping organizations trust IoT devices throughout their entire life-cycle.

Proposed offer for security

We offer a broad range of services to improve the security of your connected products and solutions through Consultancy, Evaluation, Certification, Tools and Trainings.

Contact

Alfortville, France https://www.redalertlabs.com/ roland.atoui@redalertlabs.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

IoT Horizontal Market

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

RA-IoT S-SDLC Services based on OWASP, RAL-IoT BIA based on ISO 22301, RAL-IoT Security Certification, RAL- GRC, RAL- IoT Risk Assessment, RAL- Static Analysis, RAL- Source code review, RAL- Vulnerability Assessment Techniques, RAL - Connected Device Penetration, RAL- Information Security Policy, RAL-Business Continuity Plan, RAL - Evaluation/Consulting

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management)* > Business Environment > Governance & Risk Management *(Security Certification, Governance, Risk & Compliance (GRC))*, > Risk Assessment
	> PROTECT	> Awareness and Training > Information Protection Processes and Procedures *(Static Application Security Testing (SAST), Application Security)* > Maintenance *(Patch Management, Vulnerability Management, Penetration Testing / Red Teaming)*
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)* > Communications > Analysis *(Fraud Investigation, Forensics)* > Mitigation *(Cyber Security Insurance, DDoS protection, Data Recovery, Incident Response Services (CSRIT aaS), Takedown Services)*, > Improvements
	> RECOVER	> Recovery Planning *(System Recovery, Business Continuity/Recovery Planning)* > Improvements *(Post incident reviews & consulting)* > Communications *(Communications coaching & consulting)*
Cyber-physical security services		> Audit, planning and advisory services > System integration and implementation services > Management and operations services, > Security training services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

SCILLE PARSEC

The company

SCILLE is an open source software editor specialized in the cybersecurity of sensitive data sharing on the Public Cloud.

Proposed offer for security

PARSEC is a "Zero Trust" software solution for secure document sharing, certified by the ANSSI, which guarantees the confidentiality, authenticity, traceability and integrity of sensitive and confidential data shared on the Public Cloud. The ergonomics is that of a virtual USB key synchronized between trusted users.

Contact

Saint-Médard-en-Jalles, France https://parsec.cloud thierry.leblond@scille.fr

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Cybersecurity of sensitive data in "Zero Trust" mode

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #2 - Disaster resilience (During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Cybersecurity	> PROTECT	> Data Security *(Encryption, Cloud Access Security Brokers)* > Protective Technology *(Backup / Storage Security)*
	> RESPOND	> Communications > Mitigation *(Data Recovery)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Secure-IC

The company

With presence and customers across 5 continents, Secure-IC is the rising leader and only global provider of end-to-end cybersecurity solutions for embedded systems and connected objects.

Proposed offer for security

Secure-IC provides patented Silicon-proven and cutting-edge protection technologies, integrated Secure Elements and security evaluation platforms to reach compliance with the highest level of certification for different markets (such as automotive, AIoT, defence, payments & transactions, memory & storage, server & cloud). Secure-IC's integrated Secure Elements are embedded in millions of chips for smartphones, laptops, automobiles, smart meters, passports and more and protect the devices all along their lifecycle.

Contact

Cesson-Sévigné, France https://www.secure-ic.com/ contact@secure-ic.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Protection technologies to the electronic industries.

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)
Domain #3 - Public spaces protection (Analysis, Data protection, cybersecurity, cybercrime)

Solutions

		Securyzr™, Expertyzr™, Laboryzr™
Cybersecurity	> IDENTIFY	> Asset Management, > Governance & Risk Management > Risk Assessment, > Risk Management Strategy
	> PROTECT	> Identity Management & Access Control > Awareness and Training, > Data Security *(PKI / Digital Certificates, Data Leakage Prevention, Encryption, Hardware Security Modules (HSM), Digital Signature)*, > Maintenance *(Penetration Testing / Red Teaming)*, > Protective Technology *(IoT Security, PC/Mobile/End Point Security, Mobile Security / Device management)*
	> DETECT	> Anomalies and Events, > Security Continuous Monitoring *(SIEM / Event Correlation Solutions, Cyber Threat Intelligence Solutions)*
	> RESPOND	> Mitigation *(Data Recovery)*
	> RECOVER	> Improvements *(Post incident reviews & consulting)* > Communications *(Communications coaching & consulting)*
Cyber-physical security services	> Audit, planning and advisory services, > System integration and implementation services, > Management and operations services, > Security training services	
Other security products and solutions	> Identification and authentication	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

SecuredNow

The company

For embedded device manufacturers who need to asses the security of their product SecuredNow is a solution that provides insight at any stage of the product lifecycle. Unlike product security audit performed by subcontractors our product is always available to you at any given moment of time straight from your facility.

Proposed offer for security

Provide vendors/manufacturers an automated security analysis of their product show where security vulnerabilities are, during their creation phase. Reducing risk & cost after retail deployment.
Tests are to reduce likelihood for attack types such as:

- Exploitation
- Glitching
- Side Channel
- Information leakage

Contact

Amsterdam, Netherlands www.securednow.com peter.myakoshin@exsetlabs.com

Cluster member L3CE

Specific market sector

Embedded Systems, IoT

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Solutions

Cybersecurity	> PROTECT	> Maintenance *(Vulnerability Management, Penetration Testing / Red Teaming)* > Protective Technology *(IoT Security)*
Cyber-physical security services		> System integration and implementation services > Management and operations services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

SENSIVIC

The company

French company founded in 2015, SENSIVIC has created an AI system for the detection of sound events in real time.

Proposed offer for security

Automatic smart audio detectors for anomalous noises, GDPR compliant. SENSIVIC detectors continuously analyse the usual sound activity and detect unusual sound events (gunshots, car shocks, verbal assaults drilling tools, screams...). Standalone detectors. Privacy respect by design.

Contact

Orléans, France www.sensivic.com contact@sensivic.com

Cluster member SAFE

Specific market sector

Public spaces, major events, sensitive infrastructure protection, industry and services

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Zone security and perimeter protection)
Domain #3 - Public spaces protection (Detection and alert (real time))

Solutions

	SENSIVIC sound detectors range	
Cybersecurity	> PROTECT	> Protective Technology *(IoT Security)*
	> DETECT	> Anomalies and Events *(Intrusion Detection)*
Other security products and solutions	> Observation and surveillance (localised)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Set In Stone

The company

Set In Stone is a French Startup founded in 2020. We help companies to limit risks related to data exchange between their collaborators and external actors.

Proposed offer for security

Set In Stone is THE safe registered letter of corporate mailboxes. Our traceability is ensured by Blockchain.
Set In Stone is intuitive, Made In Europe and serving your data sovereignty.

Contact

France https://setinstone.io/ thomas.benoit@setinstone.io

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Supply chain, Industry

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems)

Solutions

	Set In Stone messaging	
Cybersecurity	> IDENTIFY	> Supply Chain Risk Management *(Supply chain risk monitoring solutions & services)*
	> PROTECT	> Data Security *(Data Leakage Prevention)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

SIKUR

The company

Sikur is a cybersecurity technology innovator, dedicated to protect sensitive information through passwordless authentication, encryption and by securing endpoints.

Proposed offer for security

Critical Systems and Devices Management. The product uses the best safety practices and complies with the main global regulations. The channel between the user and the device is fully encrypted, using industry standard protocols and offering extensive possibilities for integration with existing systems through APIs (Application Programming Interfaces).

Contact

Sophia-Antipolis, France https://www.sikur.com contact@sikur.com

Cluster member

Specific market sector

Industry, Utilities, Smart Cities, Healthcare, Oil and Gas, Government, Military, Corporative

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Identification and access control)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Sikur Connect, Sikur ID, Sikur ID SDK, Sikur One, Sikur Messenger

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management IT Service Management, Risk Assessment)* > Governance & Risk Management *(Governance, Risk & Compliance (GRC))* > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control *(Access Management, Authentication, Authorisation)* > Data Security *(PKI / Digital Certificates, Data Leakage Prevention, Encryption, Cloud Access Security Brokers, Digital Signature)* > Information Protection Processes and Procedures (*Application Security)* > Protective Technology *(Remote Access / VPN, IoT Security, PC/Mobile/End Point Security, Mobile Security / Device management)*
Other security products and solutions		> Identification and authentication > Observation and surveillance (localised)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Smart Global Governance

The company

Smart Global Governance provides a SaaS Risk management platform that allows companies to better manage and monitor their various risks and compliance requirements in a single tool. Based on low code technology, it offers an open, intuitive, and flexible architecture solution.

Proposed offer for security

Intuitive and modular integrated risk management platform:

- Foster teamwork
- Orchestrate existing software and data
- Easily leverage existing data and information
- Progressively activate from 1 to 9 modules to meet your additional needs
- Get a global view, in real time
- Gain up to 30x more efficiency

Contact

Valbonne, France www.smartglobalgovernance.com hello@smartglobalgovernance.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Finance, Health, Insurance, retail, industry

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #2 - Disaster resilience (Prior to crisis: prediction)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Smart Global Governance

Cybersecurity	> IDENTIFY	> Business Environment Governance & Risk Management *(Security Certification, Governance, Risk & Compliance (GRC))* > Risk Assessment
	> RESPOND	> Response Planning *(Incident Management)* > Analysis *(Forensics)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Smiths Detection

The company

Smiths Detection is a global leader in threat detection and security screening technologies. We deliver the solutions needed to protect society from the threats and illegal passage of explosives, prohibitive weapons, contraband, biological threats, toxic chemicals and narcotics.

Proposed offer for security

1. HI-SCAN 6040DV is an advanced X-ray inspection system for automatic detection of explosives and liquids in bags and parcels. Equipped with optional iCMORE weapon for automatic detection of pistols, revolvers, knives. The ideal solution for efficient screening in high threat applications such as airports, building entrances, government facilities, embassies, banks.
2. LCD 3.3 is a portable device detecting and identifying chemical warfare agent (CWA) and toxic industrial chemical (TIC)

Contact

Vitry-sur-Seine, France www.smithsdetection.com marie-helene.fer@smithsdetection.com

Cluster member

Specific market sector

Urban security / Defence

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making)

Solutions

HI-SCAN 6040DV (detection/screening for dangerous or illicit items)

LCD 3.3 (detection for CBRNE)

Other security products and solutions	> Detection and screening for dangerous or illicit items or concealed persons > Equipment and supplies for security services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

STiD

The company

For over 25 years, STid has been inventing and offering identification solutions for physical and logical high-security access control, as well as Automatic Vehicle Identification (AVI) and industrial asset tracking - using cutting-edge RFID, NFC, Bluetooth and Internet of Things (IoT) technologies.

Proposed offer for security

ARCHITECT range - RFID, NFC and Bluetooth multi-technology scalable Readers for high-security access control applications
STid Mobile ID - Mobile Access Control Solution
ATX - ATEX & IECEx RFID rugged readers and tags for contactless identification in hazardous areas
SPECTRE Access range - UHF & Bluetooth multi-technology and long range Readers for vehicle identification
SPECTRE Industry & Extreme range - UHF long range rugged readers for all your track & trace applications
SPECTRE GATE - Mobile and autonomous RFID gate for all the industrial and logistics applications
BE.WEAPON / BE.Tools - Digital armory management Solution and Tools management

Contact

Gréasque, France

www.stid.com
www.stid-security.com
www.stid-industry.com

info@stid.com

Cluster member

Specific market sector

Government - Banking & Financial - Defence - Education - Healthcare - Energy / Oil & Gas - Enterprise & Corporate - Sports & Events - Transportation - Aerospace - Automotive

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Identification and access control)

Solutions

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management)* > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control *(Access Management, Authentication, Authorisation, Identity Management)*
Other security products and solutions	> Identification and authentication > Tracking and, tracing, positioning and localisation > Tracking, localisation and positioning of hazardous substances and devices > Equipment and supplies for security services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

STIMSHOP

The company

STIMSHOP's Wi-Us technology brings wireless communication without radio waves. Relevant in environments where radio waves do not work for secured wireless data transfer, measurement, strong authentication, geolocation.

Proposed offer for security

Integrate wireless ultrasound Wi-Us technology in any electronic system or existing device with its SDK, libraries and MULTISONIC electronic card.

Contact

Paris, France

www.wi-us.eu

contact@stimshop.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Constrained environments (Nuclear, Aeronautics, Naval, Defence) and Security (authentication, access control, geolocation)

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

ucheck.in, Wi-Us, DOOT, MULTISONIC, SECUMETER, HBEACON, UMIX

Cybersecurity	> IDENTIFY	> Tracking
	> PROTECT	> Identity Management & Access Control *(Authentication, Identity Management)* > Data Security *(PKI / Digital Certificates, Encryption, Hardware Security Modules (HSM), Digital Signature)* > Protective Technology *(Wireless Security, IoT Security, PC/Mobile/End Point Security, Mobile Security / Device management, Sandboxing)*
	> RESPOND	> Communications
Other security products and solutions	> Identification and authentication > Tracking and, tracing, positioning and localisation > Tracking, localisation and positioning of hazardous substances and devices	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

SYNEXIE

The company

SYNEXIE is a company specialised in web and mobile IT development, but especially in network infrastructure and cybersecurity, since the creation of the company. SYNEXIE works with more than hundred customers in the South French regions.

Proposed offer for security

Management of computer equipment and supplies (maintenance, monitoring)
Acquisition and installation of cybersecurity solutions.

- Antispam, antiphising : vade secure
- Web & mobile filtering : Olfeo, Rohde & Schwarz
- Encryption : Prim'X
- Firewall : Stormshield, Fortinet
- MFA : InWebo, Wallix
- Antivirus : Trend Micro, Bit Defender, Symantec

Contact

Toulon, France | http://www.synexie.fr | mnicod@synexie.fr

Cluster member

Specific market sector

Cybersecurity

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

Active Directory, InWebo, Azure AD, Office 365, PRIM'X, OoDrive, YouSign, Stormshield, Prim'x, InWebo, InTune (Azure), Olfeo, Stormshield, Fortinet, VadeSecure Cloud, Vade for Office 365, Trend Micro, Bit Defender, Broadcom/Symantec

Cybersecurity	> PROTECT	> Identity Management & Access Control *(Access Management, Authentication)* > Data Security *(PKI / Digital Certificates, Data Leakage Prevention, Digital Signature)* > Protective Technology *(Remote Access / VPN, PC/Mobile/End Point Security, Mobile Security / Device management, Sandboxing, Firewalls / NextGen Firewalls, Unified Threat Management (UTM), Anti Spam, Anti Virus/Worm/Malware, Backup / Storage Security)*
	> DETECT	> Security Continuous Monitoring *(Security Operations Center (SOC))*
	> RESPOND	> Response Planning *(Incident Management, Crisis Management)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Syscience

The company

Syscience helps customer to develop complex systems, to capture needs, identify risks, and define the most appropriate architecture.

Proposed offer for security

We developped a SaaS software and a methodology to identify risks associated to complex systems. Our methodology enables people to analyse systems with many complex components, identify associated risks and define the best architecture to minimise the risks.

Contact

Villebon sur Yvette, France www.syscience.fr pascal.krapf@syscience.fr

Cluster member

Specific market sector

Transportation systems (eg autonomous vehicle)

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Solutions

	Syscience Workshop	
Cybersecurity	> IDENTIFY	> Business Environment > Risk Assessment > Risk Management Strategy
	> RECOVER	> Improvements *(Post incident reviews & consulting)*
Cyber-physical security services	> Audit, planning and advisory services > System integration and implementation services > Management and operations services > Security training services	
Other security products and solutions	> Vehicles and platforms (e.g.: aircraft; UAVs; robotic platforms)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

TEHTRIS

The company

TEHTRIS is the world leader in the automatic neutralization of cyber attacks without human action. Our mission : to fight against cyber espionage and cyber sabotage

Proposed offer for security

TEHTRIS offers the only European eXtended Detection and Response platform that automatically kills known and unknown cyber attacks, without human interaction. TEHTRIS XDR is efficient 24/7 to keep your systems and your business up and running.

Contact

Paris, France https://tehtris.com/en/ marketing@tehtris.com

Cluster member

Specific market sector

All sectors

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Data protection, cybersecurity, cybercrime)

Solutions

TEHTRIS EDR inventory & shadow IT, TEHTRIS Ticketing tool / TEHTRIS SOAR, TEHTRIS EDR / Compliance module, TEHTRIS XDR PLATFORM, TEHTRIS Identity and Access Management Tools for TEHTRIS XDR platform, TEHTRIS Academy, "TEHTRIS pre-production environment, TEHTRIS PoC environment on-demand, TEHTRIS CWPP Cloud Workload Protection

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management IT Service Management, Risk Assessment)* > Business Environment, > Governance & Risk Management *(Governance, Risk & Compliance (GRC))*, > Risk Assessment
	> PROTECT	> Identity Management & Access Control *(Access Management, Authentication, Authorisation, Identity Management)* > Awareness and Training *(Awareness Trainings, Cyber Ranges)* Protective Technology *(PC/Mobile/End Point Security)* > Data Security *(Cloud Access Security Brokers)* > Information Protection Processes and Procedures *(Application Security)* > Maintenance *(Patch Management, Vulnerability Management)* > Protective Technology
	> DETECT	> Anomalies and Events *(Fraud Management, Intrusion Detection)* > Security Continuous Monitoring, > Detection Processes
	> RESPOND	> Response Planning *(Incident Management)*, > Communications, > Analysis *(Fraud Investigation, Forensics)*, > Improvements
Cyber-physical security services	> Audit, planning and advisory services, > System integration and implementation services > Management and operations services , > Security training services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

The Danish Institute for Fire and Security Technology

The company

Fire and security technology are the core areas of DBI. We work to create optimum security conditions by performing research, development and advisory services.

Proposed offer for security

DBI offers advisory services within a wide range of security related areas. Our team consist of experts within risk management, public spaces protection, crisis management, preparedness planning and business continuity management.

Contact

Hvidovre; Denmark https://brandogsikring.dk/ hro@brandogsikring.dk

Cluster member CenSec

Specific market sector

SMEs, large enterprises, public sector

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Analysis, Decision making)

Solutions

	DBI Advisory services
Cyber-physical security services	> Audit, planning and advisory services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Toreon

The company

Coach in Digital Security. Each digital environment is characterised by specific concerns and challenges. At Toreon we respond to the specific needs of our customers. We identify, advise and guide the implementation with tailor-made solutions to increase the maturity of their security.

Contact

Antwerpen, Belgium www.toreon.com info@toreon.com

Cluster member

LSEC

Specific market sector

Healthcare, Public Sector, Utilities & Industry, Software Builders

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making)

Solutions

Cybersecurity	> IDENTIFY	> Asset Management, > Business Environment, > Governance & Risk Management, > Risk Assessment, > Risk Management Strategy, > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control *(Access Management, Authentication, Authorisation, Identity Management)* > Awareness and Training *(Awareness Trainings, Cyber Ranges)* > Data Security, > Information Protection Processes and Procedures, > Maintenance, > Protective Technology
	> DETECT	> Anomalies and Events > Security Continuous Monitoring, > Detection Processes
	> RESPOND	> Response Planning, > Communications, > Analysis, > Mitigation
	> RECOVER	> Recovery Planning, > Improvements, > Communications
Cyber-physical security services	> Audit, planning and advisory services, > System integration and implementation services, > Management and operations services, > Security training services	
Other security products and solutions	> Identification and authentication > Intruder detection and alarm/Fire detection, alarm and suppression > Observation and surveillance (localised) > Intelligence and information gathering > Vehicles and platforms (e.g.: aircraft; UAVs; robotic platforms)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

TPL Systèmes

The company

For more than 30 years, TPL Systèmes has been designing and manufacturing radiocommunications equipment and solutions for first aid and public alert. As well as digital radio technology widely disseminated to forest fire departments.

The main activity of TPL Systèmes is the development, manufacture and distribution of professional radio communication equipment. The objective of TPL Systèmes is to provide comprehensive and innovative solutions to public security actors. The company based in Sarlat (24) is headquartered and which also houses the manufacturing unit for our products, and in Toulouse (31) which houses our R&D office. TPL is now present in more than thirty countries.

Proposed offer for security

P25 Siren Controller is an innovative warning siren control kit for the population. This innovative product integrates several communication vectors allowing the triggering of the siren. Our product adapts to all public safety radio networks thanks to its exceptional versatility.

Contact

Sarlat la Canéda www.tplsystemes.com info@tplsystemes.com

Cluster member

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Operations & optimisation of communication networks and alert systems)

Domain #2 - Disaster resilience (During crisis: communication and warning systems)

Solutions

P25 Siren Controller

Other security products and solutions	> Intruder detection and alarm/Fire detection, alarm and suppression

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

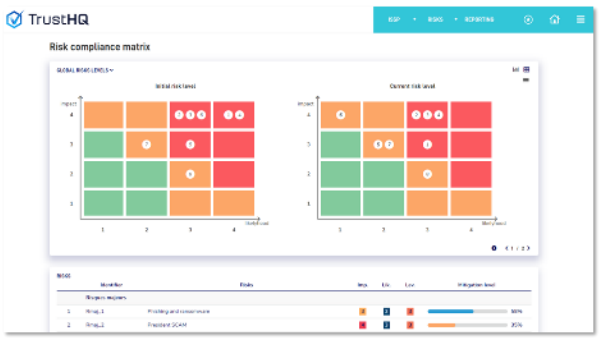
TrustHQ

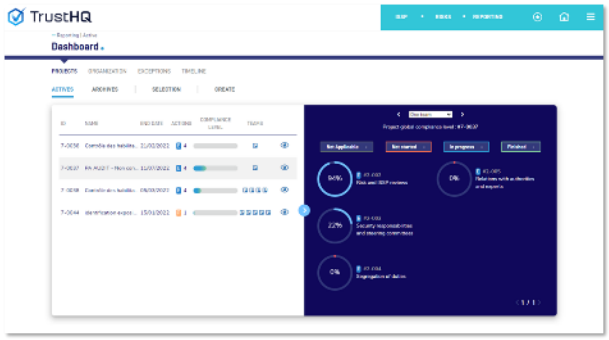
The company

Helping CISO automate compliance, risk management and cybersecurity Governance workflows.

Proposed offer for security

TrustHQ is the single cybersecurity platform for CISOs.
Trust Headquarters helps CISO manage: Cyber risks, Supply chain risk & compliance, Internal compliance to ISP and dozens of standards, Cybersecurity audits. Helping CISOs save time on risk management and compliance.





Contact

Paris, France | https://trusthq.com | gf@trusthq.com

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Banking / Industry / E-Commerce / Cloud services / Retail

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems)

Domain #2 - Disaster resilience (During crisis: communication and warning systems)

Solutions

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management IT Service Management, Risk Assessment)* > Business Environment Governance & Risk Management *(Security Certification, Governance, Risk & Compliance (GRC))* > Risk Assessment > Risk Management Strategy > Supply Chain Risk Management
Cyber-physical security services	> Audit, planning and advisory services > Management and operations services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

uCrowds

The company

uCrowds offers crowd simulation in your local building, infrastructure, or city. We offer a program and an engine that's ready to be integrated in your software solution.

Proposed offer for security

We offer a realistic, interactive, real-time crowd simulator. Our engine can be integrated (directly, or via a Unity/Unreal plugin) into your software solution, e.g. to power your digital twin or Metaverse. Our simulator (SimCrowds) enables users to set up and run crowd simulations themselves.

Contact

Utrecht, Netherlands https://ucrowds.com/ roland@ucrowds.com

Cluster member HSD securitydelta.nl

Specific market sector

Infrastructural design, Events, Gaming, Training, Covid-19

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Operations & optimisation of communication networks and alert systems)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, During crisis: communication and warning systems, After crisis: post event analysis and recovery)

Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making)

Solutions

	SimCrowds / uCrowds engine
Other security products and solutions	> Observation and surveillance (localised) > Observation and surveillance (wide area) > Command, control and decision support

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

UniText

The company

StartUp to offer Lean Management tooling and Collective Intelligence capture and capitalization.SaaS, Intranet, Portal. Asynchronous and remote collaboration.

Proposed offer for security

The UniText concept is cybersecured as its root database works in write only, and access rights are propagated and managed in a "village" community and neighbourhood.

Contact

Orsay, France www.LesAmisDeUnitext.fr philippe.jarrin@unitext.fr

Cluster member

Systematic Paris Region Deep Tech Ecosystem

Specific market sector

Generalist

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity)

Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment, After crisis: post event analysis and recovery)

Solutions

Cybersecurity	> IDENTIFY	> Asset Management *(Software & Security Lifecycle Management IT Service Management, Risk Assessment)* > Business Environment Governance & Risk Management *(Security Certification, Governance, Risk & Compliance (GRC))* > Risk Assessment > Risk Management Strategy > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control *(Access Management, Identity Management)* > Awareness and Training
	> DETECT	> Anomalies and Events *(Fraud Management)*
	> RECOVER	> Recovery Planning *(System Recovery, Business Continuity/Recovery Planning)* > Improvements *(Post incident reviews & consulting)* > Communications *(Communications coaching & consulting)*
Cyber-physical security services		> Audit, planning and advisory services > Security training services
Other security products and solutions		> Command, control and decision support > Intelligence and information gathering

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Videtics

VIDETICS

The company

The core activity of VIDETICS consists in developing video analytics tools powered by AI through software solutions specific to the world of Smart Cities, offering to provide humans with the most relevant elements for decision making. The purpose is to generate alerts and statistical data in real time thus enabling infrastructure managers to anticipate and prevent traffic congestion or avoid danger before it arrives.

Proposed offer for security

VIDETICS Perception is the fusion of a robust, optimized and controlled inference and data aggregation pipeline with knowledge and experience of the safety market going from the client needs to the way information, configuration and schedule of analytics ought to be set and controlled by security operators and safety professionals. Centred around those two main pillars, Perception gets the best of both worlds. Indeed stemming from years of knowledge about security related technologies, our innovation is compatible with every IP CCTV camera on the market and interfaces itself with the main video management systems and automation SDKs. Our solution is ready to easily integrate new SDKs and communication protocol by design and provide a cross-platform client which allows you to fully control your intelligent video analytics installation and how it communicates with your entire security infrastructure from any devices you deem fit to. Furthermore leveraging the advent of deep learning and today's research that keeps reaching new heights, Perception thoroughly optimizes all AI analytics which allows us to bring out the full potential of the devices we use and make those ground-breaking analytics real-time and highly efficient.

Contact

Valbonne, France | https://www.videtics.com | contact@videtics.com

Cluster member

POLE SCS

Specific market sector

Smart City, Smart Port, Smart Building, Private enterprise, Industry

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Zone security and perimeter protection)
Domain #3 - Public spaces protection (Detection and alert (real time), Analysis)

Solutions

Cybersecurity	> DETECT	> Anomalies and Events, *Intrusion Detection)*
	> RESPOND	> Analysis *(Forensics)*
Other security products and solutions	> Intruder detection and alarm/Fire detection, alarm and suppression > Observation and surveillance (localised), > Observation and surveillance (wide area)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

VSM

The company

Specialized in simulation for 30 years, VSM opened a training center in 2014 in Istres with 3 main products coming from R&D projects :

- ESTHEL : SAR and CSAR mission simulator
- SAGOD : hoisting simulator for people involved in the aerial safety field
- HWTC : pool for sea survival training sessions (including HUET)

Contact

Pelissane, France www.vsm.fr benoit@vsm.fr

Cluster member SAFE

Specific market sector

security, safety

Positioning along the value chain

Integrator of solutions for final users

SecurIT domains & challenges

Domain #2 - Disaster resilience (After crisis: post event analysis and recovery)

Solutions

Cybersecurity	> PROTECT > Awareness and Training
Other security products and solutions	> Equipment and supplies for security services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Wisekey

The company

WISEKEY secures the identity of people and devices. As Public or Private CA, WISEKEY delivers certificates (SSL / TLS X509) and offers managed infrastructure (Managed PKI) for connected objects that can be protected in secure microcontrollers developed and distributed by WISEKEY.

Proposed offer for security

1.Semiconductors for digital security applications, including secure NFC, secure microcontrollers, secure IoT, secure smart card readers;
2. Digital identity and Public Key Infrastructure (PKI) technology, including different trust services, an ID verification platform for mobile and website applications

Contact

Meyreuil, France www.wisekey.com gradenac@wisekey.com

Cluster member

Specific market sector

Energy / Medical / Mobile / Transport / Manufacturing / Corporate

Positioning along the value chain

Solution supplier for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Identification and access control)

Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

mPKI INeS, Ines and WISE ID, Certify ID, VaultIC / MS6003, Card reader AT, NanoSeal

Cybersecurity	> PROTECT	> Identity Management & Access Control *(Authentication, Authorisation, Identity Management)* > Data Security *(PKI / Digital Certificates, Encryption, Digital Signature)* > Protective Technology *(IoT Security)*

Other security products and solutions	> Identification and authentication > Tracking and, tracing, positioning and localisation > Tracking, localisation and positioning of hazardous substances and devices

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

X-Systems

The company

Safeguarding the European society with state-of-the-art cutting-edge Privacy-By-Design and Security-By-Default Secure Mobile IoT technologies.

Proposed offer for security

Providing Cyber-Physical Preemptive Security technologies to secure organizations preventively in the field of secure and private communications.

Contact

The Hague, Netherlands https://x-systems.com/ info@x-systems.com

Cluster member HSD securitydelta.nl

Specific market sector

Government, Enterprises, NGO's

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Zone security and perimeter protection)
Domain #2 - Disaster resilience (During crisis: communication and warning systems)
Domain #3 - Public spaces protection (Detection and alert (real time), Decision making, Data protection, cybersecurity, cybercrime)

Solutions

Cybersecurity	> PROTECT	> Data Security *(Encryption, Hardware Security Modules (HSM))* > Protective Technology *(Wireless Security, IoT Security, PC/Mobile/End Point Security, Mobile Security / Device management, Sandboxing)*
	> DETECT	> Anomalies and Events *(Intrusion Detection)* > Security Continuous Monitoring *(Security Operations Center (SOC))* > Detection Processes *(Underground/Darkweb investigation, Honeypots / Cybertraps, Social Media & Brand Monitoring)*
	> RESPOND	> Communications, > Analysis *(Forensics)* > Mitigation *(Cyber Security Insurance, DDoS protection, Data Recovery, Incident Response Services (CSRIT aaS), Takedown Services)*, > Improvements
	> RECOVER	> Recovery Planning *(System Recovery, Business Continuity/Recovery Planning)* > Improvements *(Post incident reviews & consulting)* > Communications *(Communications coaching & consulting)*
Cyber-physical security services	> Other	
Other security products and solutions	> Identification and authentication > Intruder detection and alarm/Fire detection, alarm and suppression > Detection and screening for dangerous or illicit items or concealed persons > Observation and surveillance (localised) (wide area), > Tracking and, tracing, positioning and localisation, > Command, control and decision support > Intelligence and information gathering, > Equipment and supplies for security services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

ZAFEHOUZE

The company

ZAFEHOUZE ApS, have created the most advanced, yet simple solution for accessing IT-resources, services and applications - without the risk of compromization.

Proposed offer for security

ZafePass is the Swiss-Army knife of Access to IT-resources, services, application and/or data. Support all forms of cloud services and of course own data-center. Its easy to implement, its highly scalable, flexible and agile - and it help you gain full control of your eIT-environment.

Contact

Brøndby, Denmark https://zafehouze.com nea@zafehouze.com

Cluster member

CenSec

Specific market sector

All

Positioning along the value chain

Solution supplier for final users
Technological supplier for integrator
Integrator of solutions for final users

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems, Identification and access control, Zone security and perimeter protection)
Domain #2 - Disaster resilience (Prior to crisis: prediction, risk knowledge and assessment)
Domain #3 - Public spaces protection (Detection and alert (real time), Analysis, Decision making, Data protection, cybersecurity, cybercrime)

Solutions

Cybersecurity	> IDENTIFY	> Asset Management, > Business Environment, > Governance & Risk Management, > Risk Assessment, > Risk Management Strategy, > Supply Chain Risk Management
	> PROTECT	> Identity Management & Access Control, > Awareness and Training, > Data Security, > Information Protection Processes and Procedures, > Maintenance, > Protective Technology
	> DETECT	> Anomalies and Events, > Security Continuous Monitoring > Detection Processes
	> RESPOND	> Response Planning, > Communications, > Analysis, > Mitigation > Improvements
	> RECOVER	> Recovery Planning, > Improvements > Communications
Cyber-physical security services	> Audit, planning and advisory services, > System integration and implementation services, > Management and operations services, > Security training services	
Other security products and solutions	> Identification and authentication, > Intruder detection and alarm/Fire detection, alarm and suppression, > Detection and screening for dangerous or illicit items or concealed persons, > Observation and surveillance (localised) (wide area) > Tracking and, tracing, positioning and localisation, > Tracking, localisation and positioning of hazardous substances and devices, > Command, control and decision support, > Intelligence and information gathering, > Vehicles and platforms (e.g.: aircraft; UAVs; robotic platforms), > Equipment and supplies for security services	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Zybersafe Aps

The company

Danish developer of market leading hardware based encryption devices for high capacity ethernet connections. Encrypting 1 Gbps, 10 gbps and 100 Gbps links without latency and with no compromise on security.

Proposed offer for security

Zybersafe will offer protection of high capacity WAN links with layer 2 hardware based encryption. We will offer knowledge sharing, participation in proof-of-concept projects and technical workshops.

Contact

Taastrup, Denmark www.zybersafe.com info@zybersafe.com

Cluster member

Specific market sector

Defence, Public, Health Care, Critical Infrastructure

Positioning along the value chain

Technological supplier for integrator

SecurIT domains & challenges

Domain #1 - Sensitive infrastructure protection (Cybersecurity, Operations & optimisation of communication networks and alert systems)
Domain #2 - Disaster resilience (During crisis: communication and warning systems)
Domain #3 - Public spaces protection (Data protection, cybersecurity, cybercrime)

Solutions

		Zybersafe TraficCloak
Cybersecurity	> PROTECT	> Data Security *(Data Leakage Prevention, Encryption, Hardware Security Modules (HSM))* > Protective Technology *(Remote Access / VPN, Firewalls / NextGen Firewalls)*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292