

# SecurIT

## Final event

Paris, 21st May 2024



# Agenda of the day

---

10h20 – 10h30 **Opening remarks**

10h30 – 11h00 **SecurIT & results**

11h00 – 11h15 **EU Commission's insights**

11h15 – 12h30 **Keynotes & experience sharing** on EU innovation policies & funding opportunities



**12h30 – 14h00 LUNCH**



14h00 – 15h15 **Panel discussion** - Fostering innovation uptake in security domain : how to connect innovative SMEs & end users?



**15h15 – 15h45 BREAK**



15h45 – 17h00 **Awards ceremony**



17h00 – 18h30 **NETWORKING/COCKTAIL**



# Opening remarks

---



**Marek Przeor**  
Team Leader Cluster Policy  
DG GROW  
European Commission



# Introductory session

## SecurIT project results presentation

**Adeline Gleizal**

SecurIT Project Coordinator

SAFE Cluster



# WVUJ LE CATALYSEUR



What is and who is behind SecurIT ?

# SecurIT project in a nutshell



SecurIT is a European project issued from  
*H2020 INNOSUP-01-2018-2020 Call - Cluster facilitated projects for new industrial value chains*



**Project start date** 01/09/2021

**Duration** 3 years

**Consortium** 8 partners

**Global Budget** 5M€ - *including 3,5M€  
dedicated to SMEs*





# SecurIT's network

---

## 8 Consortium members

# LE CATALYSEUR



New industrial value chain for  
**safe, secure and resilient cities  
& territories**

Safe & Secured  
Critical Infrastructures



INNOVATIVE  
DIGITAL SOLUTIONS  
FOR SECURITY



Disasters Resilience



Spaces Protection



THROUGH SMEs SUPPORT



Access to market



3 521 000€  
funding available



Matchmaking



Visibility &  
Support



[securit-project.eu](http://securit-project.eu)

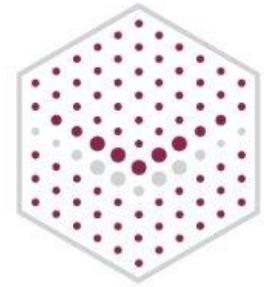
SecurITproject  
 SecurIT20  
 securit-project



**Adeline Gleizal**  
**SAFE**  
French Security,  
defence and  
aerospace  
Innovation Cluster



**Ulrich Seldeslachts**  
**LSEC**  
Belgian  
Cybersecurity  
Cluster



**LSEC**  
LEADERS IN SECURITY  
www.lsec.eu



**Marielle CAMPANELLA**



**Anaïs MISPOLET**

**SCS** - French IT Cluster



**Egidija Versinskiene**



**Sigute Stankeviciute**



**Jaroslav Urbanovič**



**Edmundas Piesarskas**



**Evaldas Bružė**

**Lithuanian Cybercrime Center of Excellence for Training, Research & Education (L3CE)**



**Paul COUMANS**

**HSD** - Security Cluster based  
in the Netherlands



**Léo BENEDETTI**

**SYSTEMATIC** - French IT Cluster



**Emmanuelle CALLERAND**



**Sofie JENSEN**

**CENSEC**  
Danish defence,  
space & security  
cluster



**Mie Zacher Linnet**



# FundingBox



**Urszula SOBEK**



**Ola SKALKA**



**Weronika GASIOR**

## **FUNDING BOX**

Polish non for profit  
private entity for  
innovation  
management

# 19 Ambassador clusters

- Widening geographical coverage & extending dissemination of the project
- Belgium, Bulgaria, Denmark, Estonia, Finland, Germany, Italy, Ireland, Latvia, Lithuania, Luxembourg, Norway, Poland, Portugal, Romania, Spain, Sweden, the UK
- Outreach: **+19 countries, 2700+ SMEs**



# 7 Advisory Board members and associated experts





# 3 main objectives

## 1. Support European security SMEs

in the development of innovations for safer & more resilient territories & cities



## 2. Fund the development of collaborative projects

For prototyping & experimentation of technological solutions in security

Taking into account ethical, legal & societal challenges

## 3. Promote cross-border cooperation

between SMEs & other innovation actors



permitted through cascade funding and the allocation of grants to third-parties (SMEs)

# 2 types of Instruments offered

Through 2 selective Open Calls

14 projects funded

## Prototyping

development of prototyping solutions for end-users or integrators at MVP stage (Minimum Viable Product)

**74K€ grant/project**



## Demonstration

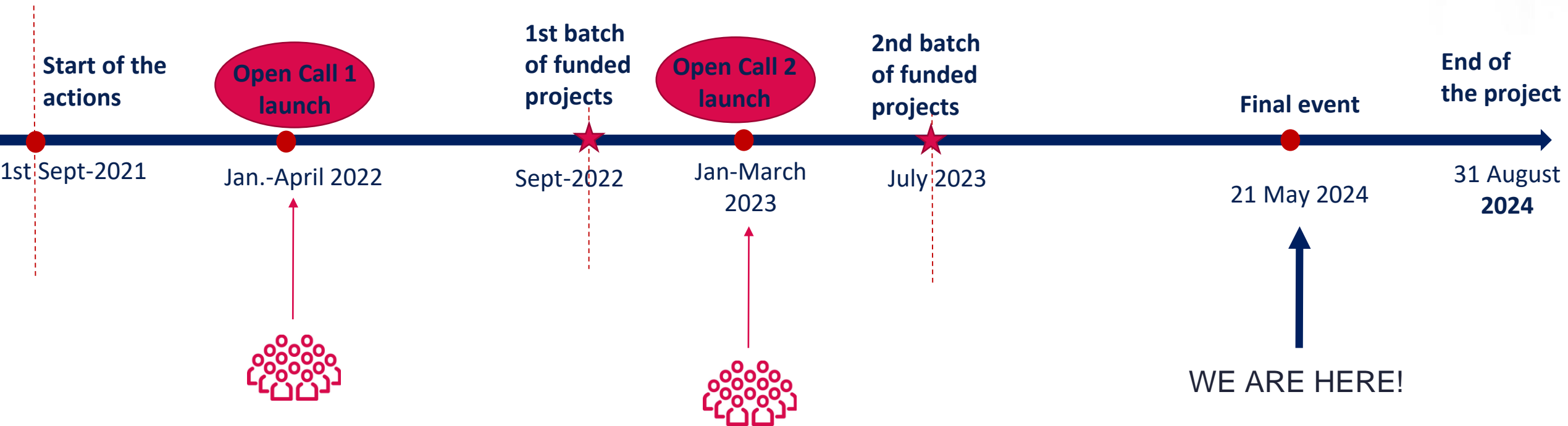
New solutions in cybersecurity & digital applications applying to security solutions ready to pilot at a large scale at short-term

**88K€ grant/project**



28 projects funded

# Timeline of the project



WE ARE HERE!



# SecurIT: a market-pull orientation

- SecurIT operates as a **sourcing of innovative non mature solutions**;
- **Process of consultations** to end-users and integrators realized upon start of project to collect common needs and gaps in security;
- **Dedicated workshops** reuniting security practitioners organized at EU level;
- **3 domains and 11 related-challenges identified** for the Open Calls ;
- SecurIT aims at funding projects that reply to identified needs and gaps.



# 3 areas of identified needs



DOMAIN #1

**Sensitive  
infrastructure  
protection**



DOMAIN #2

**Disaster  
resilience**



DOMAIN #3

**Public spaces  
protection -  
major events**



# Domain 1



## DOMAIN #1

### Sensitive infrastructure protection



Sub-domains	Challenges and potential areas of needs
Cybersecurity	1.1. Development of cybersecurity solutions for sensitive infrastructure protection
Operations	1.2. Optimisation of communication networks and alert systems
Identification and access control	1.3. Development and optimisation of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk
Zone security and perimeter protection	1.4. Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions

# Domain 2



DOMAIN #2

## Disaster resilience



Sub-domains	Challenges and potential areas of needs
<i>Prior to crisis – prediction:</i> <b>Risk knowledge and evaluation</b>	<b>2.1.</b> Optimisation of prediction of disaster
<i>During the crisis:</i> <b>Mass communication and warning systems</b>	<b>2.2.</b> Optimisation of communication and warning systems in case of disaster
<i>After the crisis:</i> <b>Post event analysis and recovery</b>	<b>2.3.</b> Development of solutions for a better recovery

# Domain 3

## DOMAIN #3

### Public spaces protection – major events



Sub-domains	Challenges and potential areas of needs
Detection, alert and behaviour analysis	3.1. Gather and manage real time information
Analysis	3.2. Analyse and extract pertinent and potentially crucial information as quickly as possible
Command and control (resource management) and decision-making support	3.3. Communication networks and post-event analysis
Data protection and cybersecurity – cybercrime	3.4. Detection

# 2 competitive calls launched at EU scale



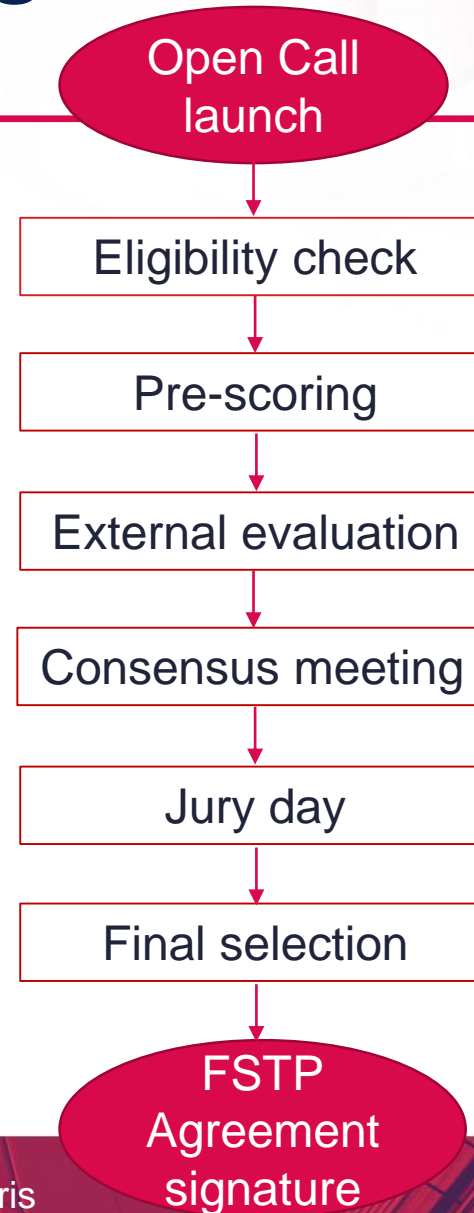
- 2 Open Calls
- Open for 2 to 3 months
- **1 dedicated platform** to collect applications
- Open Call 1 was open January – April 2022
- Open Call 2 was open January – March 2023
- Disseminated at wide scale around the EU MS and above



# A competitive selection process



- A **high-level selection process** in several steps
- To ensure the selection of **the best innovative projects**
- External evaluation was done by **independent top-notch experts**
- Auditions of pre-selected projects during Jury days in Paris and remote





# SECURIT

## Open Call #1 Figures

**240** SME  
applicants

from **33**  
countries

**111** Project  
proposals



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



# Open Call 1 Results



**377** Started Applications



**111** Submitted applications

**68%**  
applications from  
international  
consortia

**PROTOTYPING  
INSTRUMENTS**



**DEMONSTRATION  
INSTRUMENTS**



## FROM 3 DOMAINS

DOMAIN #1

**Sensitive infrastructure  
protection**



DOMAIN #2

**Disaster resilience**



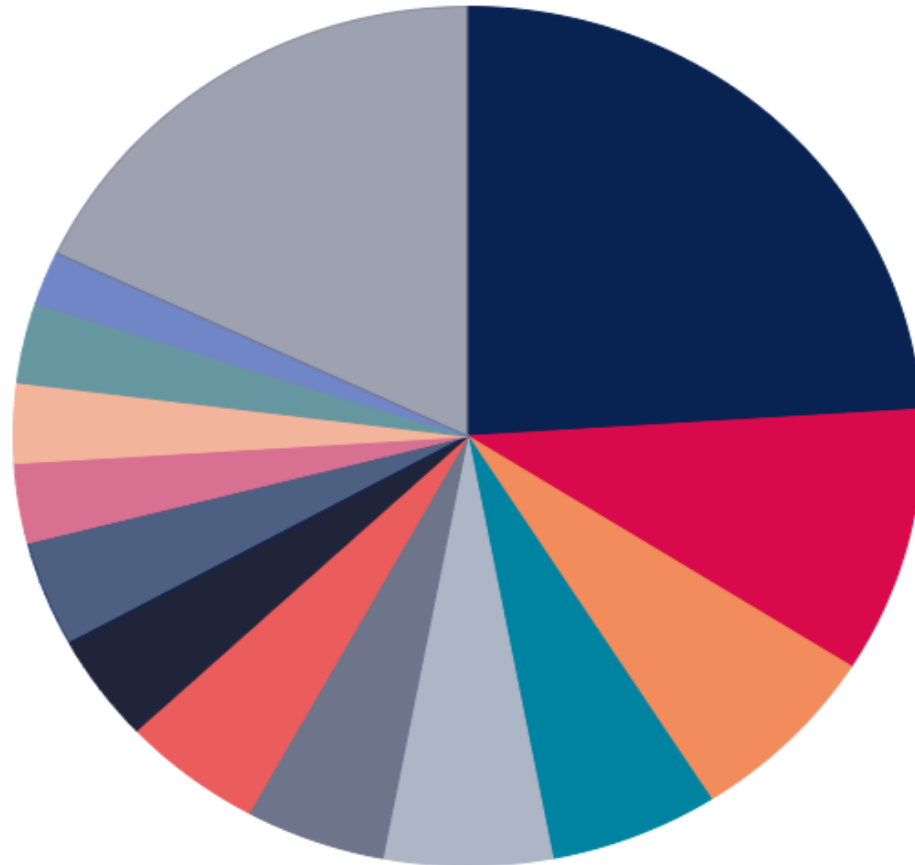
DOMAIN #3

**Public spaces protection -  
major events**



# 240 SME applicants from 33 countries

Countries of the applicants (%)



## 33 countries

France

Italy

Spain

Greece

Netherlands

Denmark

Germany

Finland

Poland

Belgium

United Kingdom

Lithuania

Estonia

Other countries\*



\*Others: Austria, Bulgaria, Croatia, Cyprus, Czech Republic, Hungary, Ireland, Israel, Latvia, Luxembourg, Malta, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Sweden, Switzerland, Ukraine.

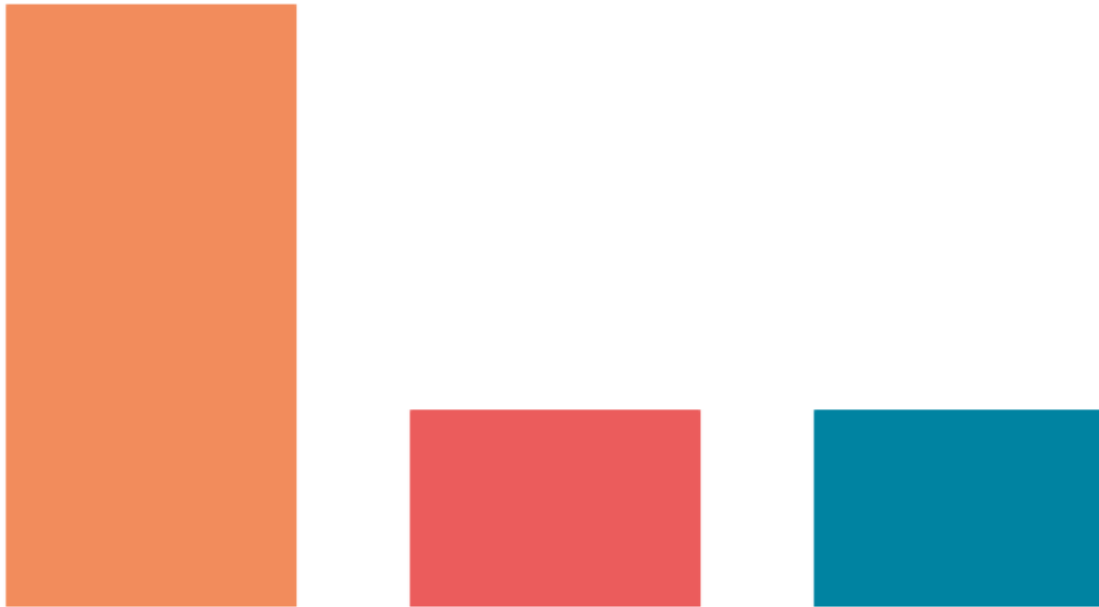
# OC1 – repartition of applicants per domains

## Selected Domains

Domain #1 Sensitive infrastructure protection

Domain #2 Disaster resilience

Domain #3 Public spaces protection – major events



Domain 1 – Sensitive infrastructure protection – gathered the most project proposals, with 67 applications on the 111 submitted, against 22 for Domain 2 – Disaster resilience – as well as for Domain 3 – Public spaces protection & Major events.

Most of the submitted projects are tackling the development of **cybersecurity solutions for the protection of sensitive infrastructures** and challenges of **detection and location of intruders in protected perimeters (Domain 1)**.

Proposals tackling the **optimisation of disasters prediction** and of **warning systems** were also numerous (Domain 2), as well as solutions **gathering and managing real time information**, and for the **quick analysis of crucial information** (Domain 3).



**SECURIT**

#1st BATCH 

# 21 innovative projects

**TOWARDS RESILIENT SMART CITIES & TERRITORIES**



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

# OC1 – 21 projects funded - 48 European SMEs – 17 countries

ITTI

LORENZ  
TECHNOLOGY

Wear

GEO  
KINESIA

FOX  
STREAM  
INTELLIGENT VIDEO

FOKUS  
TECH

SCOTT  
BROWNRIGG

Avian  
Digital Forensics

AIRSENSE  
ANALYTICS

WALLIX  
CYBERSECURITY SIMPLIFIED

sparkd

avantools

MION

GIM  
ROBOTICS

COVR

exponential  
space

LMAD  
Enabling the future of delivery

JANUSID

MITHRIL SECURITY

Logo with a gear and a stylized 'K' inside a black circle.

EDICIA

grifonline  
a real world

ALTPRO

Protech-X

APEX SOLUTIONS  
THINKING OUT OF THE BOX

Level7  
Internet Service Provider

AST  
ADVANCED SECURITY TECHNOLOGIES

Logo with a stylized 'R' inside a blue square.

HELIKITES

40  
TECHNOLOGIES

DATA TEK  
inženjering računarskih sistema

LUFTBORN

Odin S

DEFORA  
NETWORKS

Cyberium

cetrac

Logo with a stylized '2' inside a blue square.

Logo with a stylized '2' inside a blue square.

ezako  
time series solutions

Beia  
CONSULT INTERNATIONAL

VWA VZ

DEVERYWARE  
Committed to Better Security

AzurIA

Techcom

Logo with a stylized 'A' inside a blue square.

Skopos.AI

Logo with a stylized 'A' inside a blue square.

NUUK

asvin  
iterato

wirelessconnect

Nocode-x

LANACCESS

Logo with a stylized 'A' inside a blue square.

# Domain 1 – Sensitive Infrastructure protection – OC1 – 14 projects

### BIM2SIM



**Digital Forensics Cloud Lab SaaS**

### ARSP



**AUTOMATIC MONITORING AND THREAT DETECTION**

### CyberSec2SME



**SECURVERSE**



### IDEAS



**INSIOTA**



### VASCREEN



**RASAD**



### ShowID




**DIAC**



### Kaleidoscope



**Cyber Trapper**



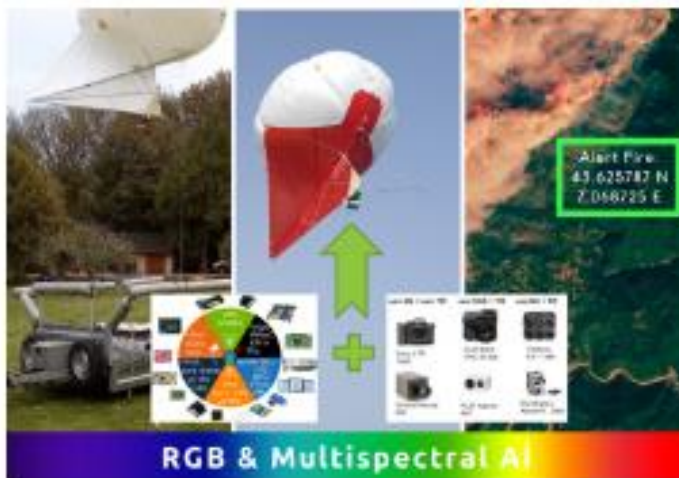
### ROGID



# OC1 – Domain 2 – Disaster resilience – 3 projects



## Helia



### RGB & Multispectral AI

Easy to transport and fast to launch  
High altitude (120m-3km) for large FoV  
Operational in high winds (up to 90km/h)  
Multi risks (several SecurIT domains covered)  
Low maintenance cost, autonomous 24H/24H

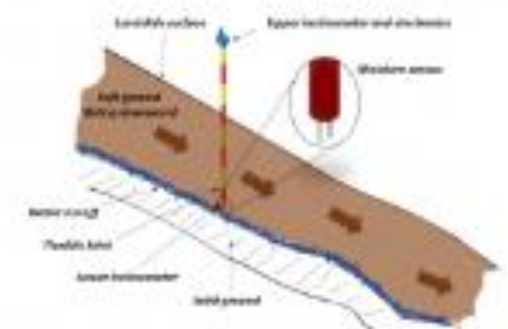
## PIM-SAT-M



## SLOPEGUARD

### Design of the ROD

2 inclinometers  
+  
Moisture Sensor  
+  
Electronics



# OC1 - Domain 3 - Public spaces protection-major events – 4 projects

## FusionSec



## ZENITH



## C-SHIELD



## SecuRAIL





# SECURiT

## Open Call #2 Figures

**271**  
SME  
applicants

from **38**  
countries

**130**  
Project  
proposals



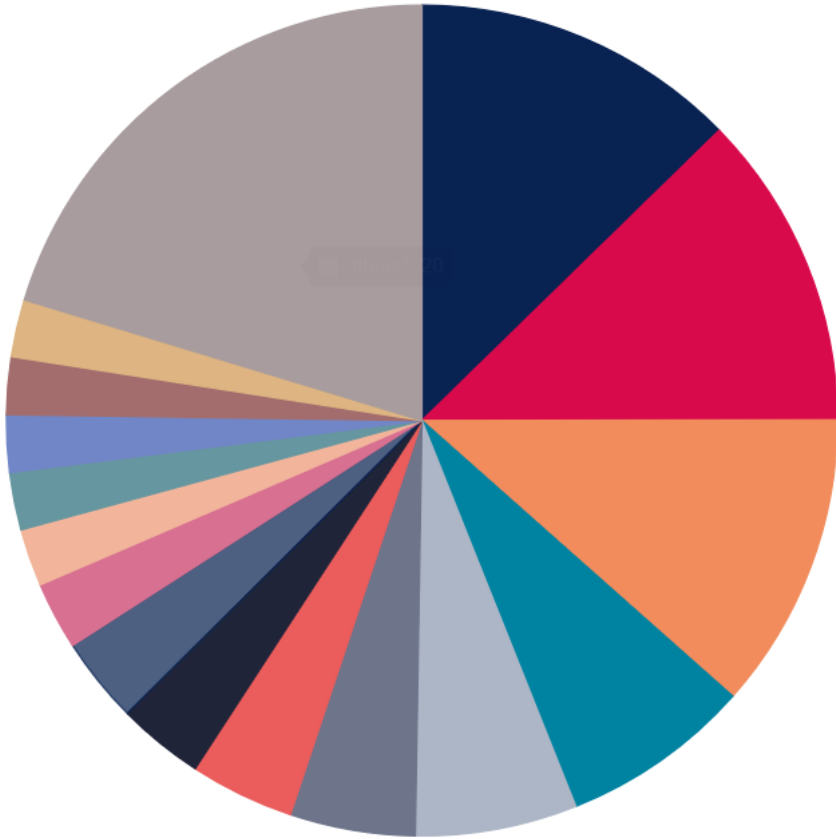
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292



# OC2 - 130 submitted applications from 38 countries

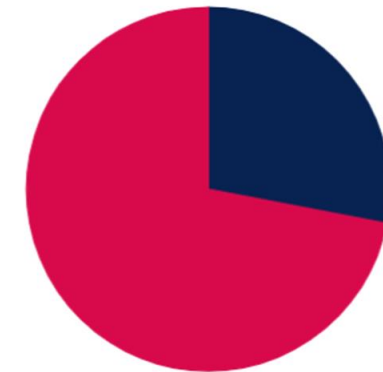
## 25 EU-countries and 13 non-EU countries

Countries of the applicants (%)



Italy
France
Spain
Greece
Germany
Netherlands
Belgium
Estonia
Poland
Denmark
Lithuania
Portugal
Cyprus
Romania
United Kingdom
Others*

Cross-border collaboration (%)



Located  
in the  
same  
country

Located  
in  
different  
countries



# SECURIT

#2nd BATCH 

Kick-off meeting for Call 2 Projects

Vinçotte July 5 2023

# 21 innovative projects

**TOWARDS RESILIENT SMART CITIES & TERRITORIES**

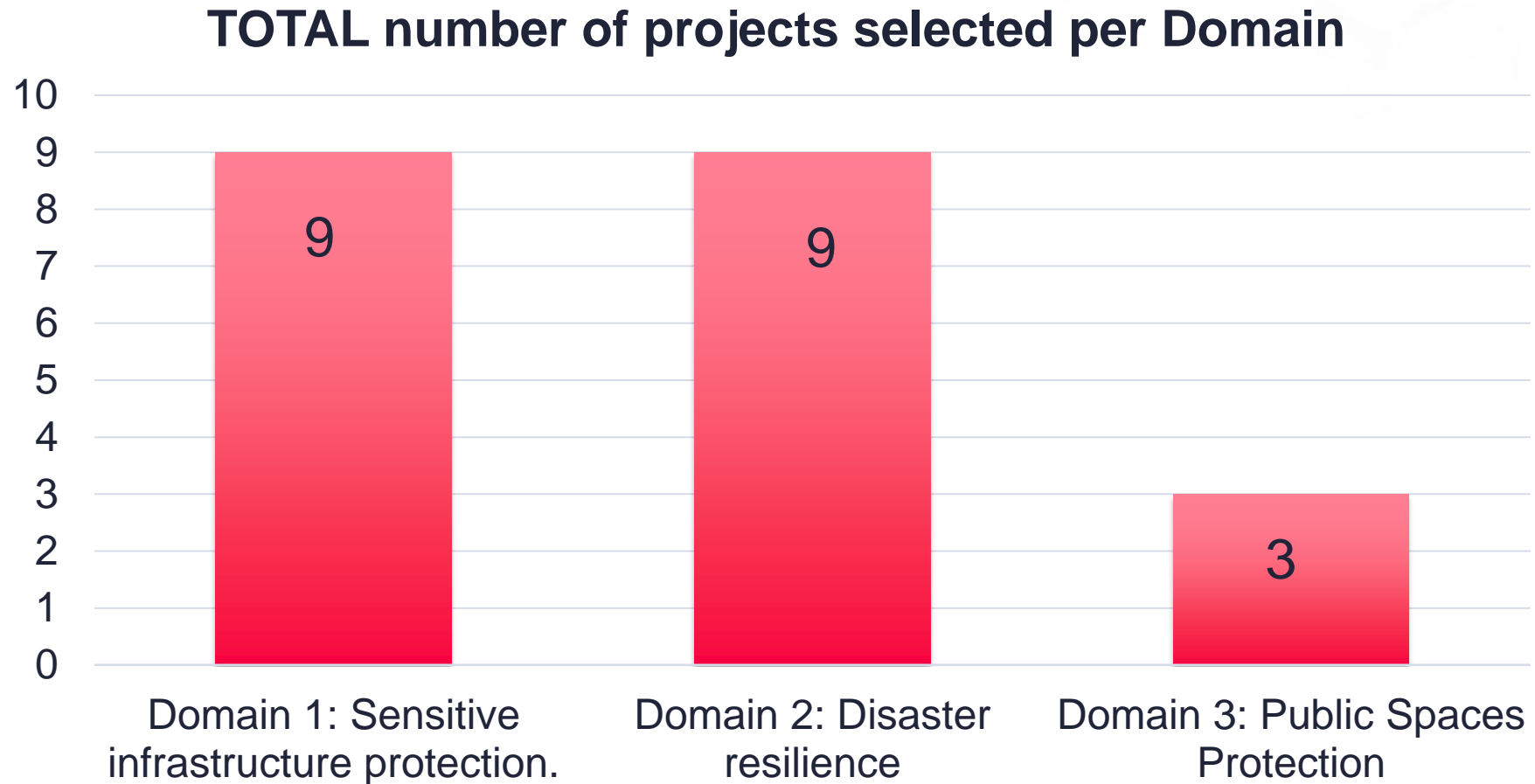


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

# OC2 – 21 projects funded - 47 European SMEs – 17 countries



# OC2 - Winners Domaines - 47 SMEs

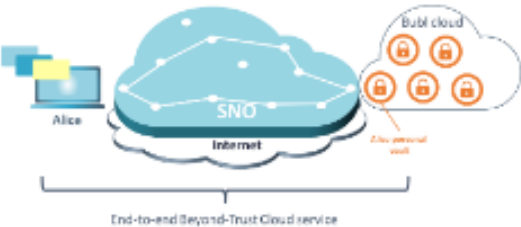


# OC2 - Domain 1 – Sensitive Infrastructure protection – 9 projects

## AIA Guard



## INVISIBuBL



## DISCGRID



## EV Safe



## OPTIMIZ NETWORK



## RS2DG



## FlowGuard



## AIRA



## Smart Diri

# OC2 - Domain 2 – Disaster resilience – 9 projects



## ERMINE



## ERRATA



## AI Disaster Emergency Com'



## ReBriNet, Resilience Bridge Net



## WUI-Secure



## SYLVIACARE



## ServAL Management



## NOCCRO



## RESPO-C



# OC2 - Domain 3 - Public spaces protection - major events – 3 projects

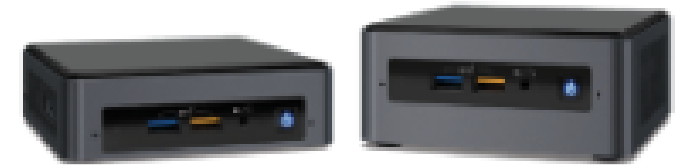
## SAFE- FESTIVALS



## AIR-T4S



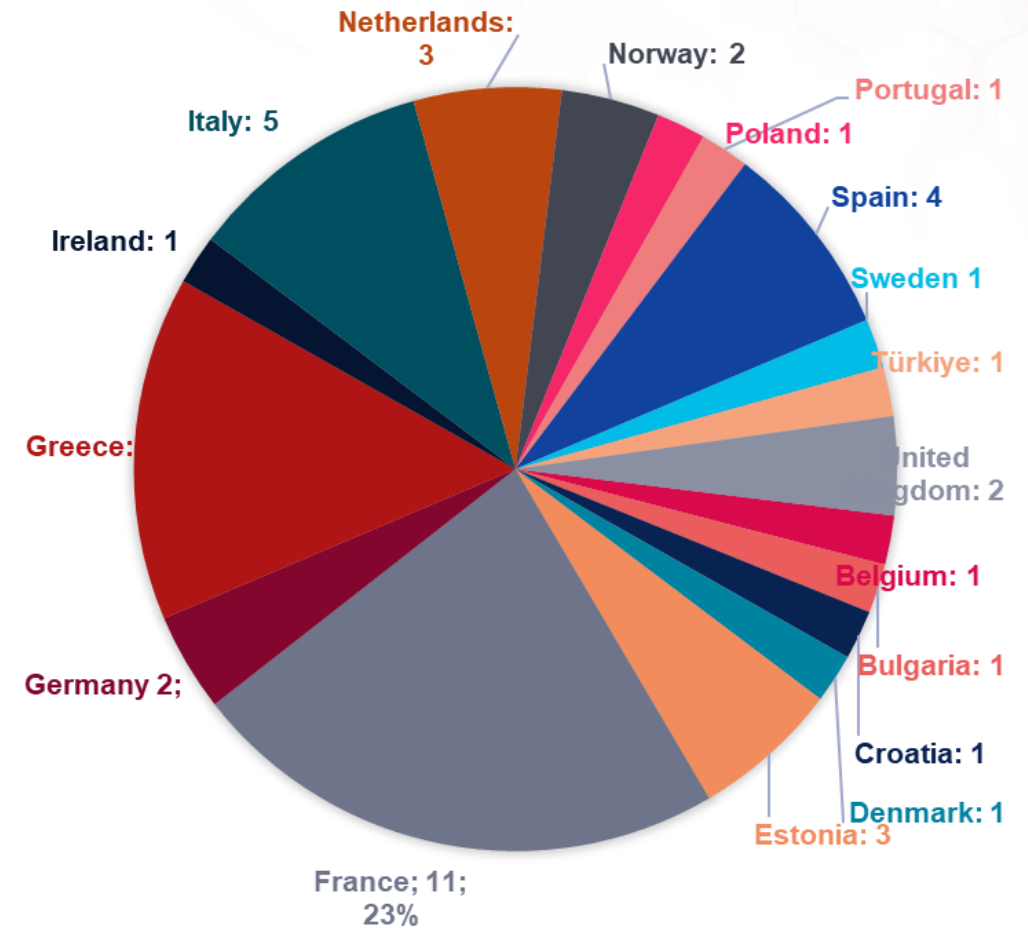
## CMD





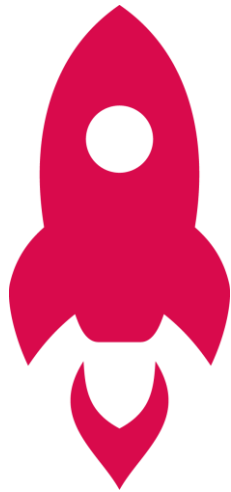
# International collaboration

- **95 SMEs** from 23 different countries for both Open Calls
- **40 international consortia** composed of 2 or 3 SMEs from different countries
- **30 consortia of 2 SMEs** from 2 different EU MS
- **10 consortia of 3 SMEs** from 3 different EU MS
- **7 projects met during matchmaking sessions** organized by the consortium



OC2 countries repartition

# SecurIT in figures



- **3,5 M€ distributed** as direct funding to SMEs
- **74K€ funding** to develop prototypes
- **88K€ funding** to develop demonstrators
- **60K€/ SMEs** as a maximum
- **95 SMEs received funding** from the European Commission
- **42 projects and solutions** developed towards safer and more resilient cities and territories
- **28 demonstrations** and experiments performed
- **14 prototypes** developed
- **129 security solutions** mapped at EU level



# SECURIT

## Open Calls Figures

A total of

**42**

funded  
projects

**95**

beneficiary  
SMEs

From **23**  
different  
countries



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





# SECURiT

## Open Calls Figures



**Domain 1**  
Sensitive  
infrastructure  
protection

**23**  
projects



**Domain 2**  
Disaster  
resilience

**12**  
projects

**Domain 3**  
Public spaces  
protection –  
major events

**7**  
projects



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

# SecurIT acts as an Innovation Booster



## Domain 1 - Sensitive infrastructure protection

- **16 demonstrators** (8 in Open Call 1 and 8 in Open Call 2)
- **7 prototypes** (6 in Open Call 1 and 1 in Open Call 2)



## Domain 2 - Disaster resilience

- **6 demonstrators** (3 in Open Call 1 and 3 in Open Call 2)
- **6 prototypes** (Open Call 2)



## Domain 3 - Public spaces protection – major events

- **6 demonstrators** (3 in Open Call 1 and 3 in Open Call 2)
- **1 prototype** (Open Call 1)

**28 demonstrators**

**14 prototypes**

Solution Providers

Security solutions

Search by domains & challenges

Business clusters

Search

✕

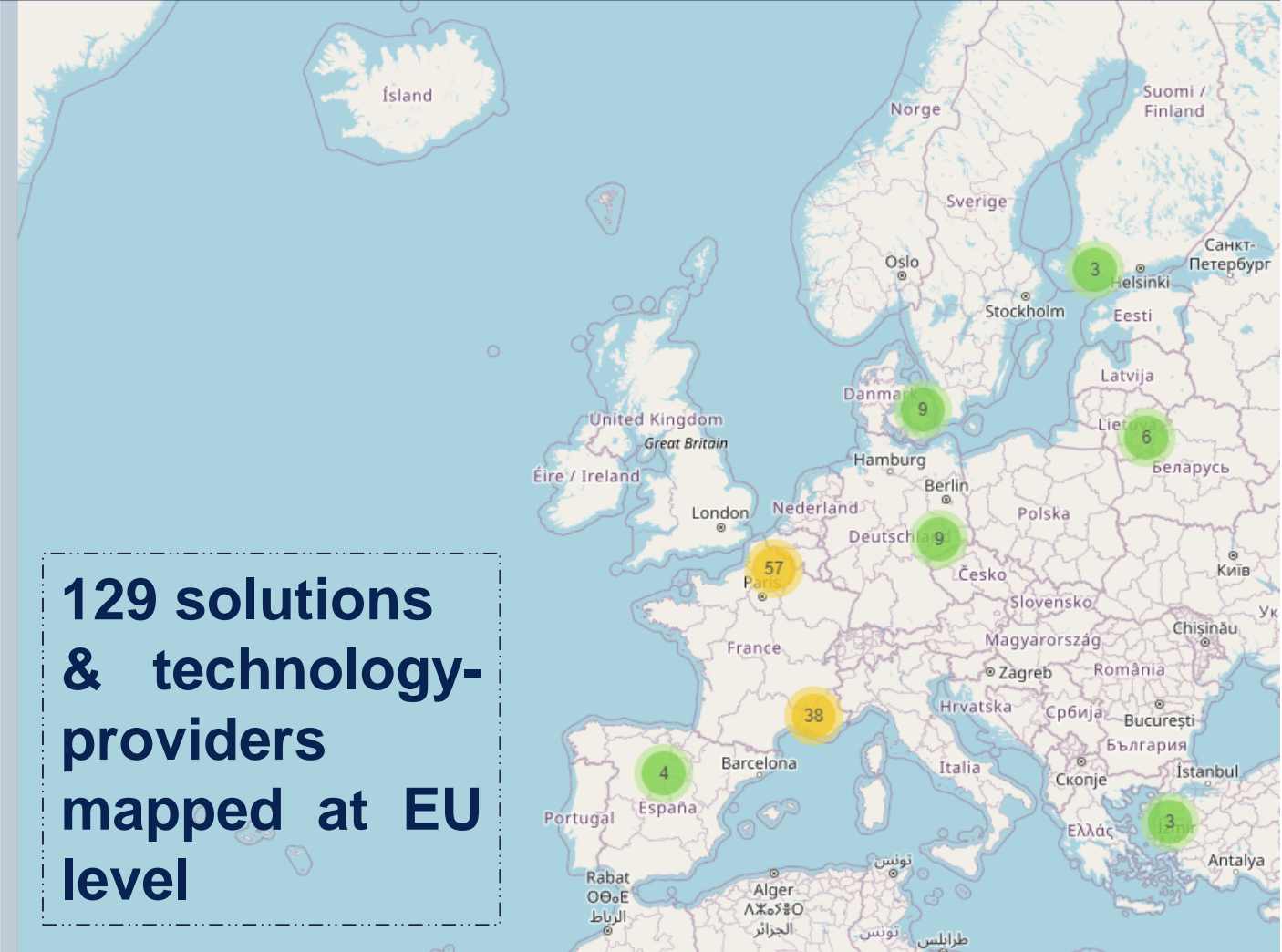
Country

Select

Company Name ▼	Country
Acrux cyber services	Lithuania
Agendum Ltd	Finland
AIRSENSE Analytics GmbH	Germany
AKIDAIA SAS	France
Algodone	France
ALL4TEC	France
Alpha Strike Labs GmbH	Germany
APEX solutions	France
Aquila	France
Arbit Cyber Defence Systems ApS	Denmark

No. of results: 129

Export to: PDF



# Creation of a platform with 56+ funding instruments & strategies at EU level

## REGIONAL INVEST




## Welcome to Regional Invest

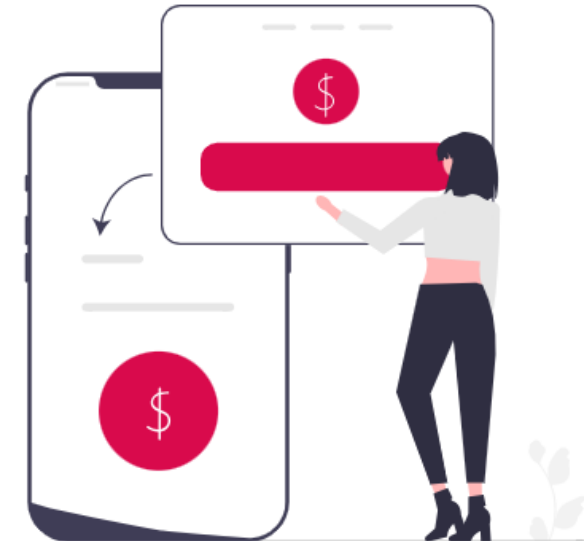
Your Gateway to Strategic Financing

Our application simplifies the complex world of funding by tailoring options to your location and internal strengths. Filter and find financing methods perfectly suited to your specific situation:

- **Location-Based:** Explore local grants, subsidies, and regional investment programs.
- **Strengths-Focused:** Leverage your internal skills and industry focus for targeted financing.
- **Development Insights:** Gain valuable strategies and support for growth.

Unlock your financial potential with Regional Invest. Welcome to a smarter, strategic approach to financing. Get started today!

 **Search our database**



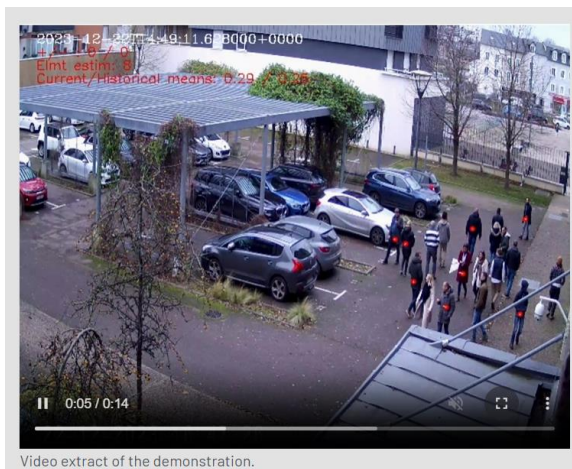
SecurIT is also...



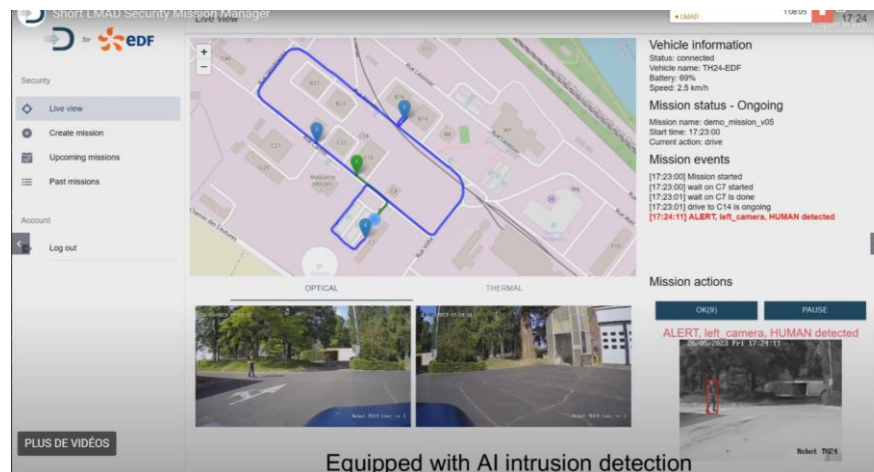
- **30+** dissemination events
- **6** physical consortium meetings in 3 countries (FR, NL, LT)
- **20+** webinars held by SecurIT partners
- **150+** consortium & coordination online meetings in 3 years
- **5** Work packages & **19** tasks achieved



# Demonstrations and experiments with end-users



**CMD project**



**ARSP project**



**Securail project**

About 30 demonstrations successfully realized (or to be realized) reuniting diverse end-users: Lithuanian police, soft target operators, critical infrastructure operators, etc.

# Ethics, transparency and conflict of interest

- Ethics was taken seriously by SecurIT
- Code of Conduct drafted to ensure **transparency and impartiality** in selection process
- Ethic expert and monitoring throughout the development phase of the laureate projects



## I. WHY WE IMPLEMENT THIS DOCUMENT

FundingBox is a SecurIT Partner responsible for organizing open calls, evaluation of the proposals, and providing support to the management of the financial support to third parties (FSTP) in the SecurIT Project.

In order to ensure the proper management and distribution of public funds, we implement this document to ensure the impartiality and transparency of the whole SecurIT process.

We would like you to know how to:

- keep impartiality during SecurIT open call, evaluation and FSTP management,
- recognise a conflict of interest and what to do to avoid it,
- react if you recognise a conflict of interest.

## II. WHO SHOULD USE THIS DOCUMENT

This document is addressed to all persons having a direct or indirect impact on who will be provided with the financial support or/and in what amount. You should read and follow this document if:

- you participate in evaluation process (for example - as an evaluator or member of the Selection Committee);
- your opinion might affect decisions on granting FSTP (for example, if you act in the capacity of an advisor or ethical evaluator) or you are involved in such decisions;
- your opinion might affect decisions on payment of the grant (for example you assess the progress of the FSTP recipient, evaluate KPIs) or you are involved in such decision making process;
- you decide on the progress of the FSTP recipient within the project stage or about termination of its participation.

So it is addressed to evaluators, experts, employees, managers, members of the managing bodies, engaged in the project at an individual level - hereinafter referred to as the **persons involved**, but also to the consortium Partners as Legal Entities.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 1010012362.



# Conclusions and lessons learned



- Managing a 5M€ project is **not always seamless...**
- Some **difficulties in the daily management** of the project were met, but overcome by the consortium

**Adjustments** in the FSTP between Open Call 1 and 2:

- ✓ Jury day OC1 was held in presence mode while Jury day OC2 was held online => **more participants could be auditioned**
- ✓ The challenges were further detailed following OC1 for OC2 => **it changed the no. of applications per challenges received**
- ✓ The number of evaluators per application decreased between OC1 and OC2 => **more proposals were evaluated in OC2**
- ✓ Awards competition was included in order to **distribute the budget to the most promising projects.**

# Cascade funding – outcomes & benefits for companies

**Cascade funding,**  
a highly valuable  
instrument to push  
SME to access  
agile EU funding



**Innovation  
booster & great  
trigger** to foster  
collaboration  
among suppliers  
& end-users on a  
high sensitive  
market such as  
security

**Stimulate  
concrete  
international  
collaboration**  
among SMEs,  
tech providers,  
security  
specialist & end-  
users

**Vital role of  
Clusters** as  
catalysts to  
innovation projects

*With good knowledge of  
their ecosystem, ability  
to design, organise  
calls, answering the  
needs of the market*

# Benefits for companies

- Calls tailored to the capacity and needs of SMEs
- **Visibility at EU level** to the funded SMEs
- **Efficient support & follow-up by the SecurIT partners**, ensuring high quality outcomes (all projects successfully completed)
- Market-oriented **KPIs**, with focus on technical achievement & business perspectives
- Several projects **have gone beyond & obtained additional EU/national funding to upscale** their solution



# Success stories & post-SecurIT collaboration

## CYSSME

- Cybersecurity and Data Protection for Small, Medium and Micro Enterprises (CYSSME) - European Union's Digital Europe Programme
- EU project involving **2 consortium partners from SecurIT + 2 SecurIT funded SMEs**



- **Objective:** facilitate access to cybersecurity resilience technologies with personalized strategy, based on an SME-use case definition approach.

CYSSME - CyberSecurity for SMEs supported by the EC



## LEAD-Pro

- EU project involving **1 consortium partner from SecurIT + 1 SecurIT funded SME**
- **Follow-up of FUSIONSEC project** : platform aiming at supporting LEA/First responders with multi-stakeholder powerful command & control, & situational awareness toolset.
- **End-user engagement:** with several demonstrations (Latvian National Police, Valencia & Barcelona Police, Madrid Municipality)
- **SecurIT** : mentorship & facilitation service = additional funding granted through Horizon Europe (CL3-2023-SSRI-01-02)
- 3 end-user org. to participate in a solution maturation process with large-scale demos to address threats of public space protection in Latvia, Spain, & Lithuania.



# To go beyond : sustainability and projects clustering initiative

- **Market Need:** in response to the enhanced complexity of security challenges, security practitioners have recognized the necessity for a diverse array of tools and innovative solutions capable of addressing threats within the broader spectrum of security concerns.
- **Objective:** to involve field practitioners in participating in demonstrations, providing the opportunity to showcase innovations from a holistic perspective.
- **Piloting:** Public Space Protection – Lithuanian national police
  - **6 Clustered projects selected:** AI disaster communication, AIR-T4S,CMD, ERRATA, ReBriNet, Safe Festivals
  - **2 stages demonstrations executed:**
    - Filtering relevant functionalities by innovation experts of LT police
    - Large scale demonstrations (involving 100 field practitioners)
    - Testing in real-life scenarios





[Securit-project.eu](https://securit-project.eu)



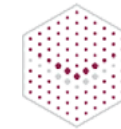
@SecurIT Innosup



@SecurITproject



@SecurIT20



**LSEC**  
LEADERS IN SECURITY

POLESCS

**L3CE**

**HSD**

**Systematic**  
Paris Region Deep Tech Ecosystem

**CenSec**  
CENTER FOR DEFENCE, SPACE & SECURITY



**FundingBox**



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

# Agenda of the day

10h20 – 10h30 **Opening remarks**

10h30 – 11h00 **SecurIT & results**

**11h00 – 11h15 EU Commission's insights**

11h15 – 12h30 **Keynotes & experience sharing** on EU innovation policies & funding opportunities



**12h30 – 14h00 LUNCH**



14h00 – 15h15 **Panel discussion** - Fostering innovation uptake in security domain : how to connect innovative SMEs & end users?



**15h15 – 15h45 BREAK**



15h45 – 17h00 **Awards ceremony**



17h00 – 18h30 **NETWORKING/COCKTAIL**



# European Commission: EISMEA's insights

---



**Virginie Perron**  
Project Adviser  
EISMEA Unit I.01 - EU and Place-  
based Innovation Ecosystems

European Innovation Council and  
SMEs Executive Agency (EISMEA)

**European Commission**

# Agenda of the day

10h20 – 10h30 **Opening remarks**

10h30 – 11h00 **SecurIT & results**

11h00 – 11h15 **EU Commission's insights**

11h15 – 12h30 **Keynotes & experience sharing** on EU innovation policies & funding opportunities



12h30 – 14h00 **LUNCH**



14h00 – 15h15 **Panel discussion** - Fostering innovation uptake in security domain : how to connect innovative SMEs & end users?



15h15 – 15h45 **BREAK**



15h45 – 17h00 **Awards ceremony**



17h00 – 18h30 **NETWORKING/COCKTAIL**



# Keynotes and experience sharing on EU innovation policies and funding opportunities



## Focus on security domain



**Giannis Skiadaresis**

Area Coordinator for Strengthening  
Security Research and Innovation (SSRI)  
Innovation and Security Research Unit  
DG HOME  
European Commission

## Focus on digital domain



**Noël Marciniak**

Deputy Head of the Guidance  
and Partnership Office  
NCC-FR operator  
ANSSI - National Agency for  
Information Systems Security

## SecurIT post-collaboration



**Ulrich Seldeslachts**

CEO of LSEC  
Partner of CYSSME project



**SECURiT**

TOWARDS RESILIENT SMART CITIES & TERRITORIES

# Lunch Break

Until 14h00



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



**SECURiT**

TOWARDS RESILIENT SMART CITIES & TERRITORIES

# Lunch Break

Until 14h00



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

# Agenda - Afternoon sessions

- 14h – 15h15 **Panel discussion** - Fostering innovation uptake in the security domain : how to connect innovative SMEs and end users and what challenges remain?

15h15 – 15h45 BREAK

- 15h45 – 17h00 Awards ceremony
- 17h00– 18h30 **NETWORKING/COCKTAIL**

# PANEL DISCUSSION - Fostering innovation uptake in the security domain : how to connect innovative SMEs and end users and what challenges remain?



**Joris den Bruinen**

General Director

The Hague Security  
Delta (HSD)



**Sylvain Chapon**

Global Business Unit  
Technology Dpt  
Relationship  
Manager

ENGIE



**Thierry Nagellen**

Research Director  
Augmented Customers  
and Collaborators

Orange Innovation



**Luigi Rebuffi**

Secretary General

European Cyber  
Security Organisation  
(ECSO)



**Chris Singer**

Director  
Policing & Security  
Specialist

Resilience Advisory  
Network  
(RAN)

Moderator



**Eva Škruba**

Capability Manager

European Anti-  
Cybercrime Technology  
Development Association  
(EACTDA)



**SECURiT**

TOWARDS RESILIENT SMART CITIES & TERRITORIES

# Afternoon Break

30 minutes

Until 15h45



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

# Agenda - Afternoon sessions

- 14h – 15h15 **Panel discussion** - Fostering innovation uptake in the security domain : how to connect innovative SMEs and end users and what challenges remain?

15h15 – 15h45 BREAK

- 15h45 – 17h00 **Awards ceremony**

- 17h00– 18h30 **NETWORKING/COCKTAIL**

# Awards ceremony



The three best collaborative projects of Open Call 1 and of Open Call 2 will be awarded:

## OC 1 Prizes



- 2 demonstration projects receiving €10.000 each
- 1 prototype project receiving €7.500

## OC 2 Prizes



- 2 demonstration projects receiving €10.000 each
- 1 prototype project receiving €7.500

# Awards – Selection process

- Participants had to produce a short video presenting their project and its interest, highlighting its innovation, added value and impact. They also had to answer some questions about the project in the application form.
- All projects were rated on a scale of 1 to 5 according to these evaluation criteria.

N°	CRITERIA	SCORE
1	The solidity of the project in terms of market fit, commercialization, or development strategy	1 - 5
2	The degree of innovation, from a security perspective, that should be generated by the participation in the SecurIT project	1 - 5
3	Involvement of end-users during and after the project	1 - 5
4	Quality of the video: time management, clarity, convincing, visual, originality	1 - 5

Each criterion will receive a score from 1 to 5, 1 being the lowest and 5 the highest as follows:

1 VERY POOR	2 POOR	3 SUFFICIENT	4 GOOD	5 VERY GOOD
-------------	--------	--------------	--------	-------------

# Awards – Candidates



- A total of **27 participants**

- OC1 Demonstration (6):

**ARSP**

**C-SHIELD**

**DIAC**

**FUSIONSEC**

**HELIA**

**PIM-SAT-M**

- OC1 Prototype (3):

**BIM2SIM**

**SECURAIL**

**VASCREEN**

# Awards – Candidates

- OC2 Demonstration: (11)

**AIA GUARD      SAFE-FESTIVALS**  
**AIRA            SERVAL MANAGEMENT**  
**AIR-T4S**  
**DISCGRID**  
**EV-SAFE**  
**FLOWGUARD**  
**INVISIBUBL**  
**OPTIMIZ-NETWORK**  
**RESPO-C**

- OC2 Prototype: (7)

**AI DISASTER EMERGENCY COM'**  
**ERMINE**  
**NOCCRO**  
**REBRINET**  
**SMART DIRI**  
**SYLVIACARE**  
**WUI-SECURE**

# SecurIT Awards



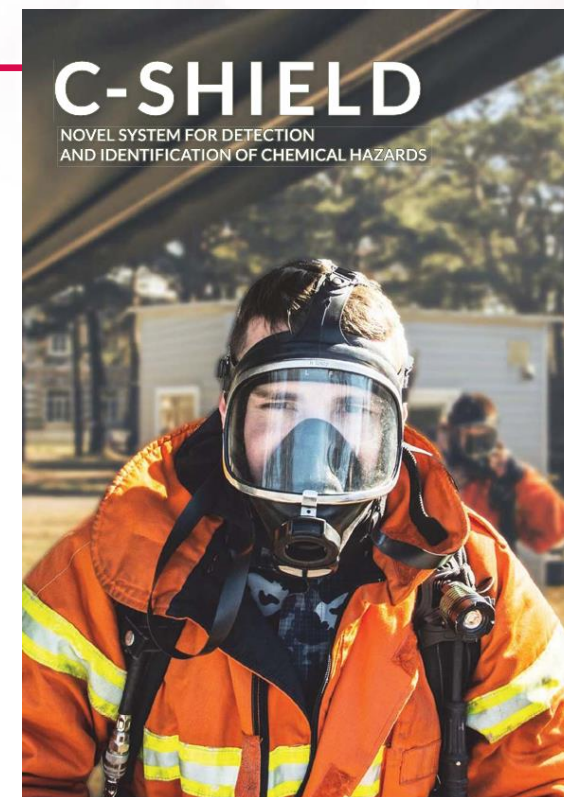
**And the winner is...**



# Demonstration project - Open Call 1

- **C-SHIELD** - *Chemical detection and identification system*
- Project partners : ITTI (Poland) & AIRSENSE (Germany)

itti



This project has received funding from



**SECURiT**



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

# C-SHIELD IMPROVED CHEMICAL DETECTION & IDENTIFICATION SYSTEM

Krzysztof Samp, [krzysztof.samp@itti.com.pl](mailto:krzysztof.samp@itti.com.pl)

Paris, 21.05.2024

**itti**



ITTI Sp. z o.o.  
[www.itti.com.pl](http://www.itti.com.pl)

SecurIT Final event - 21st May 2024, Paris

ul. Rubież 46  
61-612 Poznań

Tel. (61) 622 69 85  
Fax. (61) 622 69 73

## C-SHIELD – BASIC INFO



- Focus on **detection of chemical hazards** with the use of **heterogeneous sensor nodes**
- Based on two different detection technologies, namely **Ion Mobility Spectroscopy (IMS)** and **Flame Photometric Detection (FPD)**
- Technologies are combined via a hardware unit called a **sensor node**
- The node is equipped with a dedicated **data fusion software**, which combines and processes the sensors signals
- The applied data processing algorithms will help **reduce false alarms** as well as **estimate the class and ID of the detected substance**
- This will, ultimately, **increase the situational awareness** of the end-users in the area of interest

CBRN



# C-SHIELD – TECHNICAL INFO

- Technology readiness: **currently TRL 8**
- **Stationary and mobile version**
  - e.g. on Unmanned Ground Vehicles
- **Wide scope of detected chemical agents**



Commercially  
available  
sensors



Dedicated  
translator



Sensor node



GUI



## CHALLENGES AND SCENARIOS

- The C-SHIELD system is an answer for the challenges reported by the end-users, such as **IFAFRI** or **ENCIRCLE**:
  - Real time detection and analysis of hazard
  - Ability to detect a large spectrum of agents
  - Fast and reliable identification of the hazardous substances
  - Remote acquisition of the data
  - Responders' safety
- Exemplary scenarios:
  - Civil security – **Toxic Industrial Chemicals (TIC)**
  - Military – **Chemical Warfare Agents (CWA)**



## FUTURE PLANS AND NEEDS

- Commercialisation
  - Looking for interested **end-users and customers**
  - Finding suitable **business model**
- Product development:
  - Implementation of system tools like: **dispersion engine, radiation field simulator**
  - Integration of **Radiological (done), Biological Threat Detectors**
  - **Expanding Data Fusion** concept and algorithm with additional measurements and tests



This project has received funding from



**SECURIT**



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

# — THANK YOU FOR YOUR ATTENTION

Krzysztof Samp, [krzysztof.samp@itti.com.pl](mailto:krzysztof.samp@itti.com.pl)

**itti**



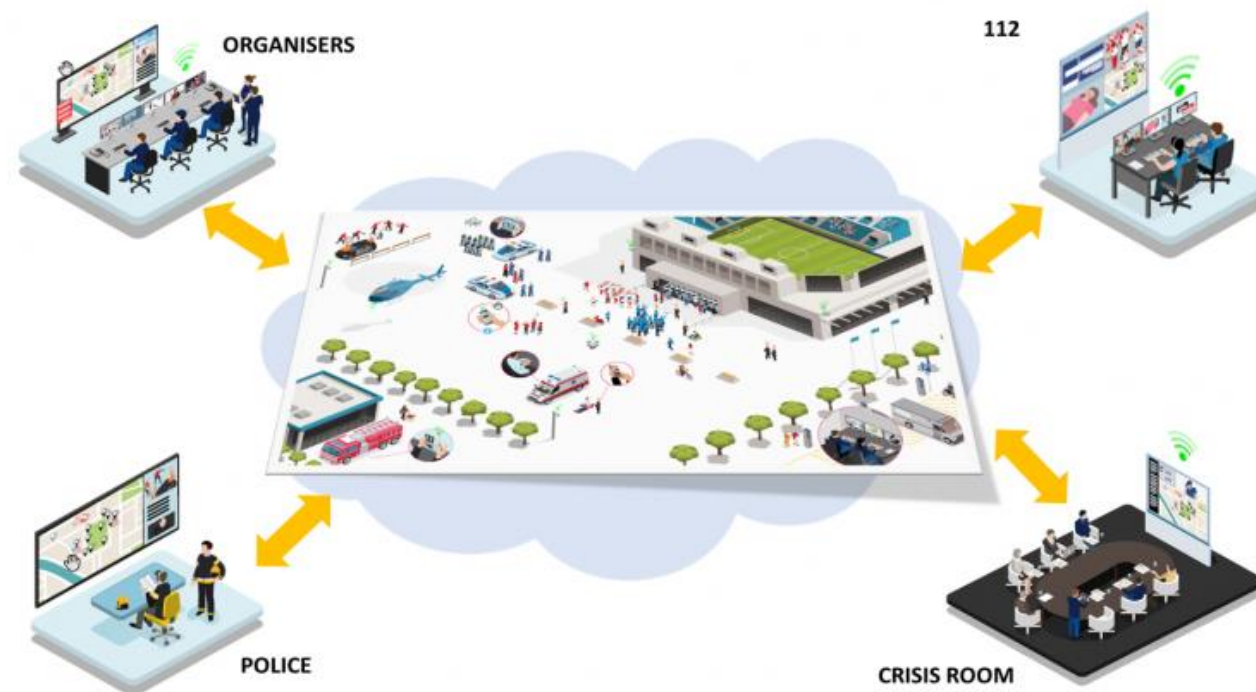
ITTI Sp. z o.o.  
[www.itti.com.pl](http://www.itti.com.pl)

ul. Rubież 46  
61-612 Poznań

Tel. (61) 622 69 85  
Fax. (61) 622 69 73

# Demonstration project - Open Call 1

- **FUSIONSEC** – *Ensure the security of your events*
- Project partners : NUUK TECHNOLOGIES (Spain) & ITERATO (Lithuania)





# FusionSec

Ensure the security of your events

BY

**NUUK TECHNOLOGIES**  
**SL.**  
Spain

**ITERATO**  
Lithuania

# Customer problem



- Isolated systems, devices and data
- Hard involvement of ad-hoc forces or volunteers
- Sluggish usage of new technologies, e.g. IoTs, drones
- High cost, difficult to use solutions



# FusionSec

**Interact, communicate and take decisions collaboratively**



Different security bodies collaborate in one platform



Real time tracking and full visibility of event stuff and infrastructure objects



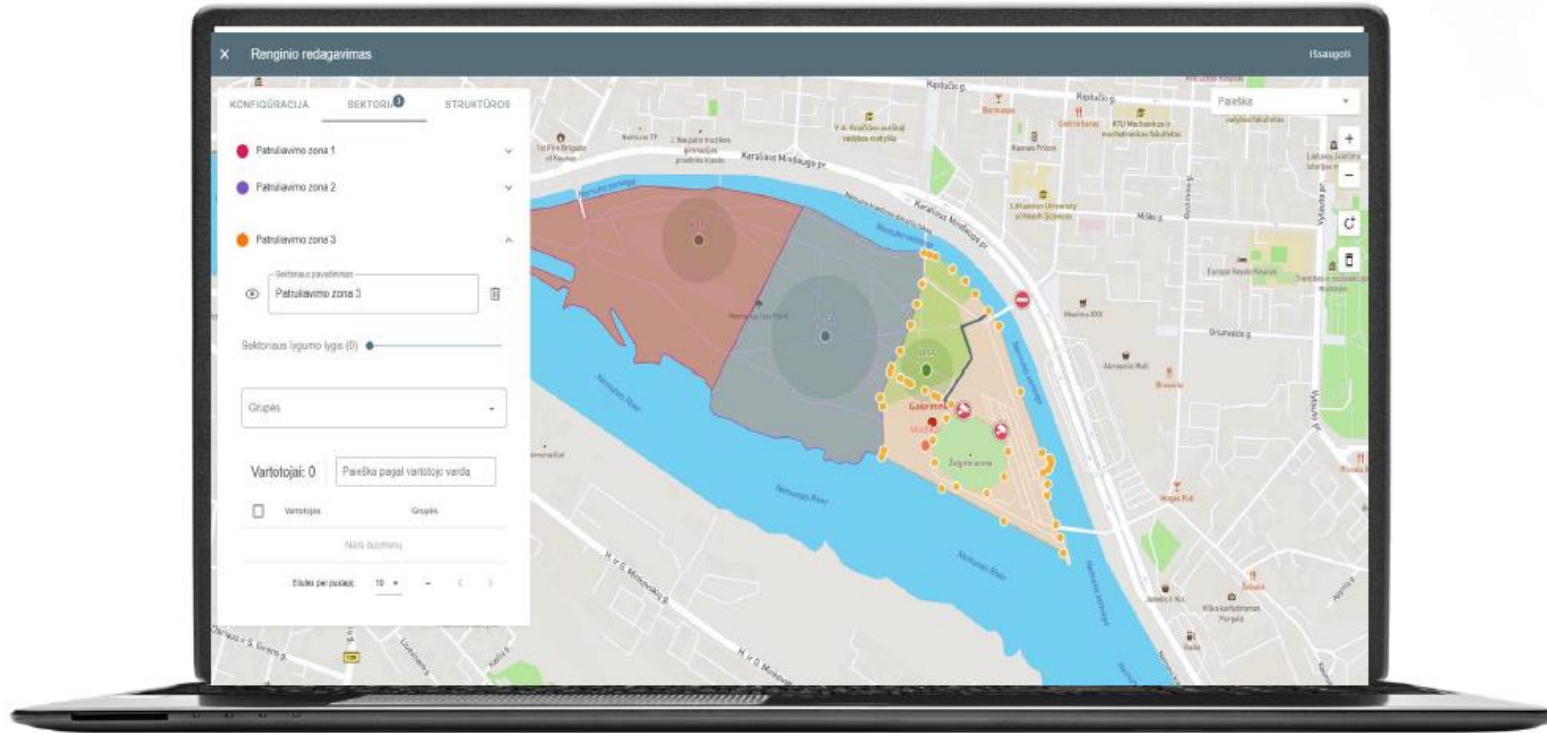
Awareness empowered by new technologies (IoTs, drones, ect.)



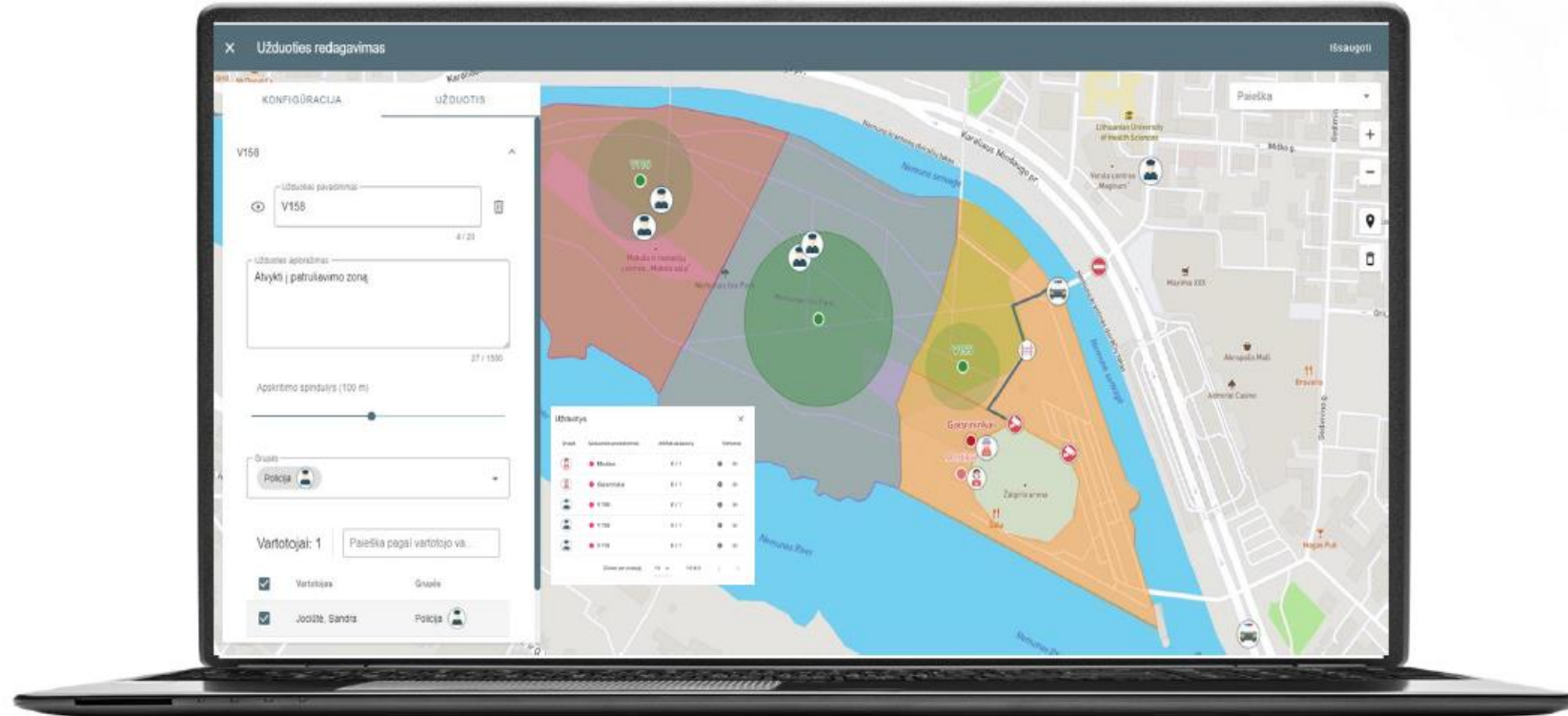
Easy jump in for ad-hoc security forces involvement



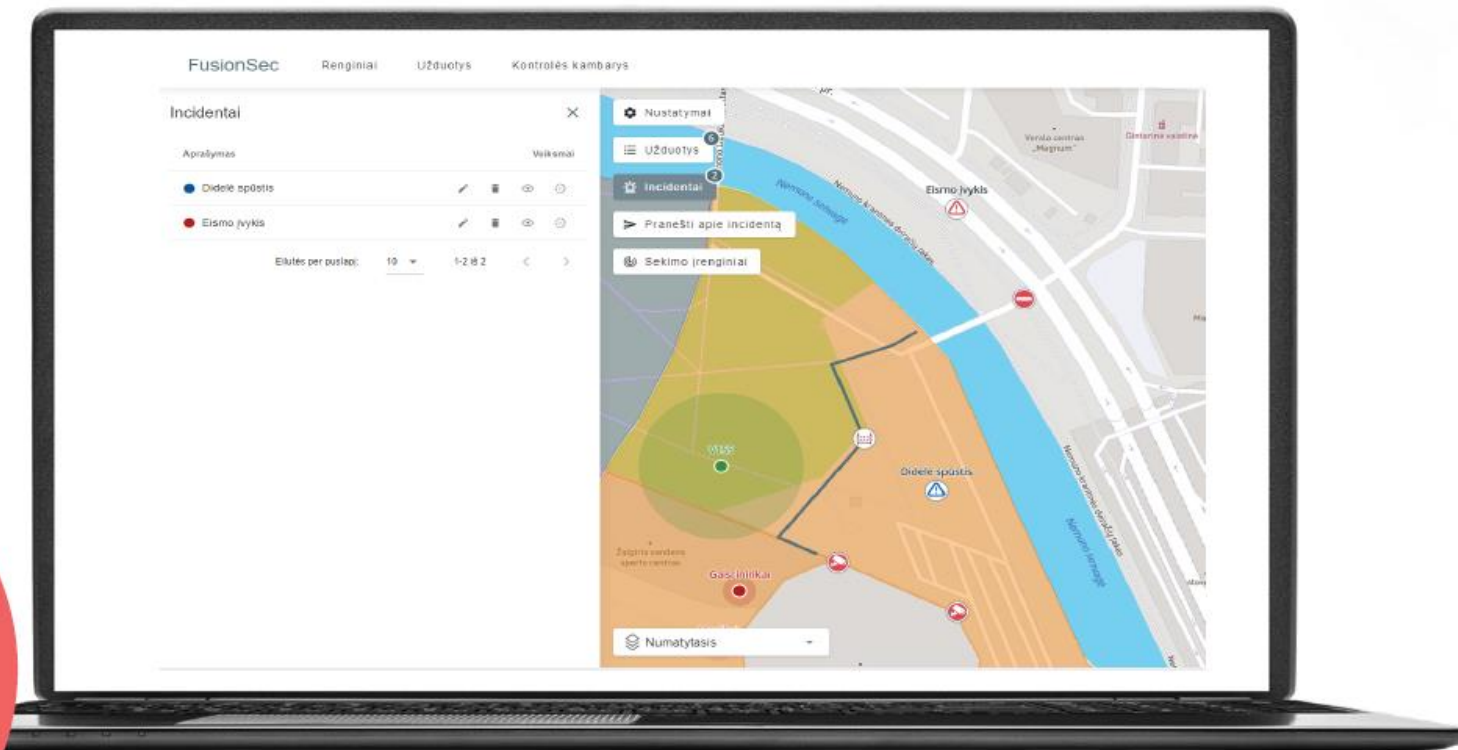
# Plan your event



# Manage tasks



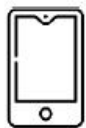
# Manage incidents



# Integrated video streams



From drones



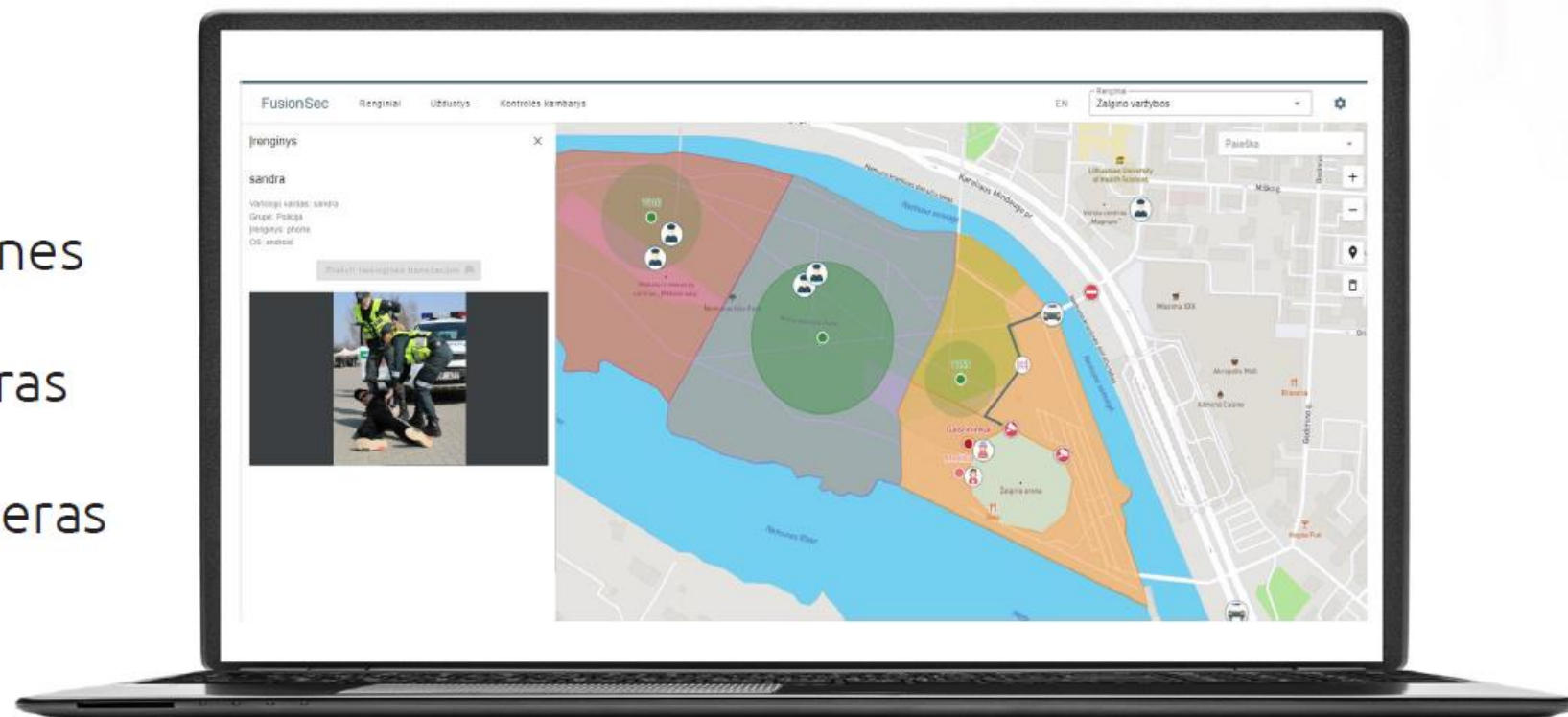
From mobile phones



From CCTV cameras



From mobile cameras



# Event monitoring in Real Time

Creating situational awareness through:





# Pilot event

Alytus city birthday

2023-06-16

# Internet setup



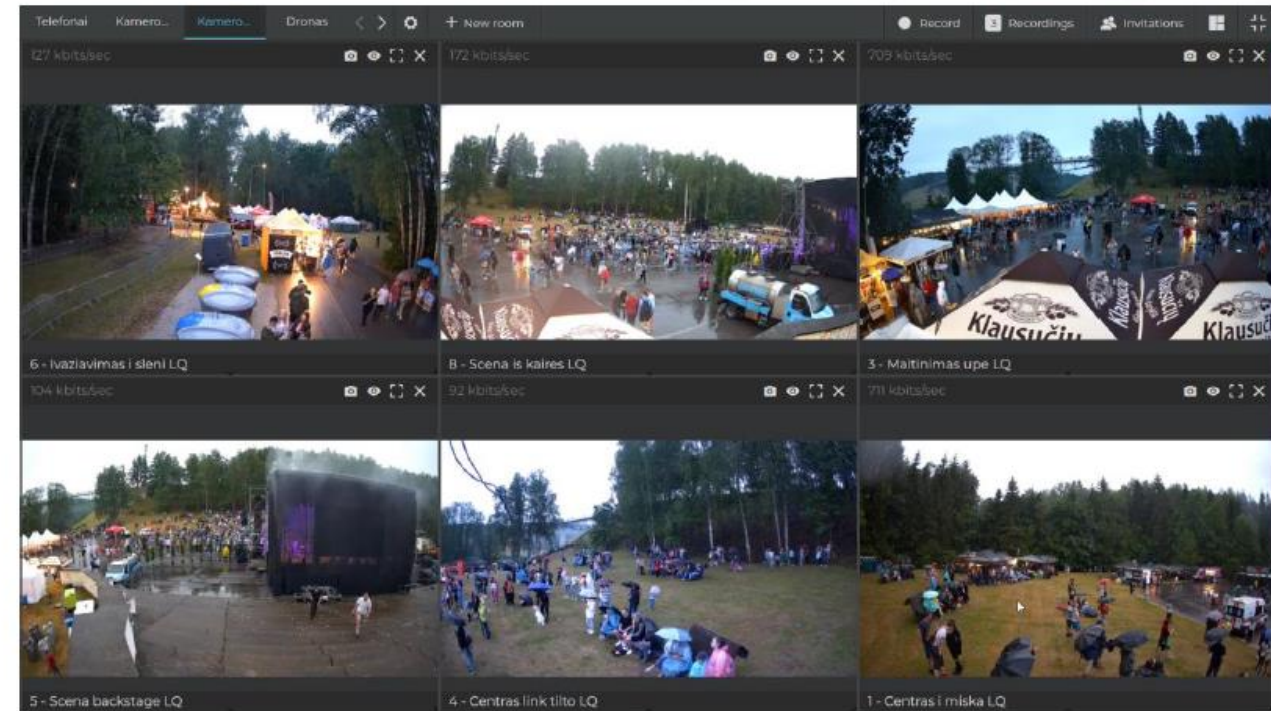
# Event planning



# Briefing for police officers



# Event monitoring – control room



# Benefits

---



Better security forces coordination



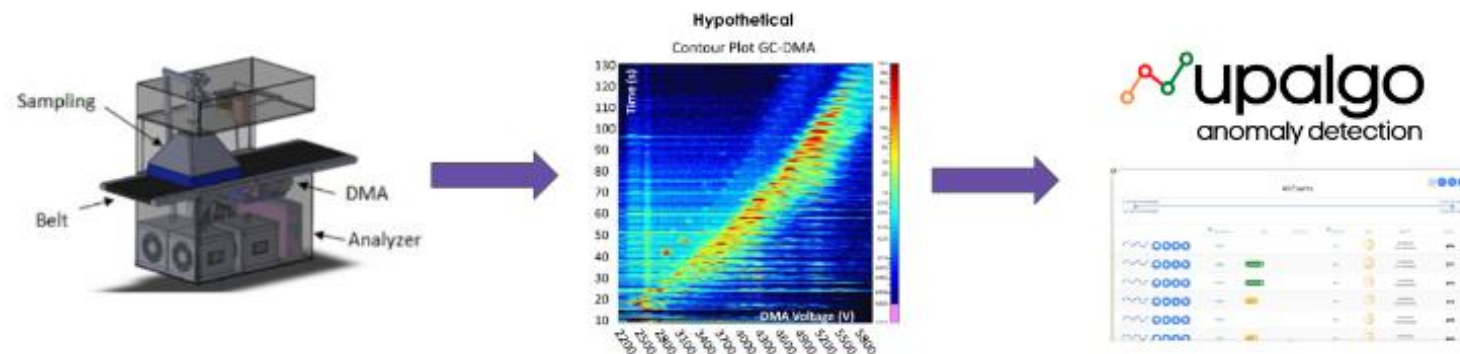
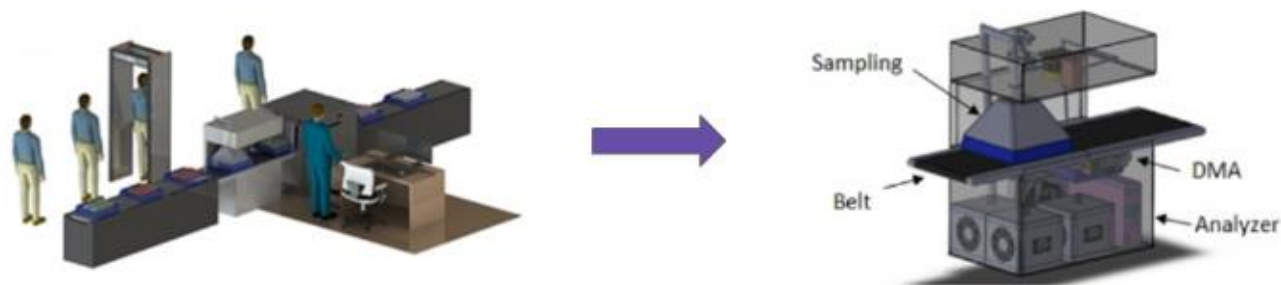
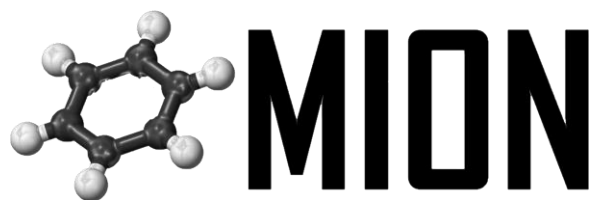
Quicker response to incidents



Increased productivity

# Prototype project - Open Call 1

- **VASCREEN** – *Detection of potentially harmful substances in luggages and goods*
- Project partners : EZAKO (France) & Mion Technologies (Spain)





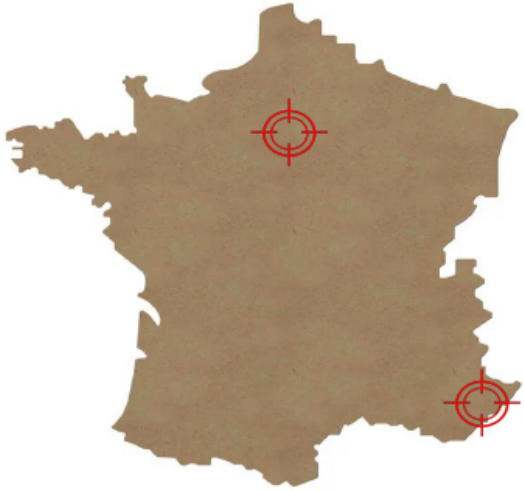
ezako



**MION**

**VASCREEN**  
High-resolution VApor SCREENer

# Ezako x MION - AI innovation from Europe



Ezako - AI startup based in Paris & Sophia-Antipolis.

Specialized in data, analytics for sensors and machine learning.

Mion - SME based in Palencia.

A technological leader in vapor detection.

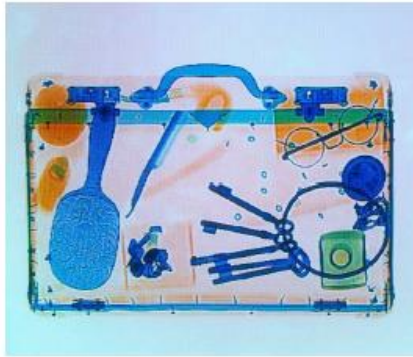
Specialized in the Identification, characterization, detection and monitoring of different substances



# Problem - Actual luggage screening solutions are not good enough

Actual solutions pose **several problems** :

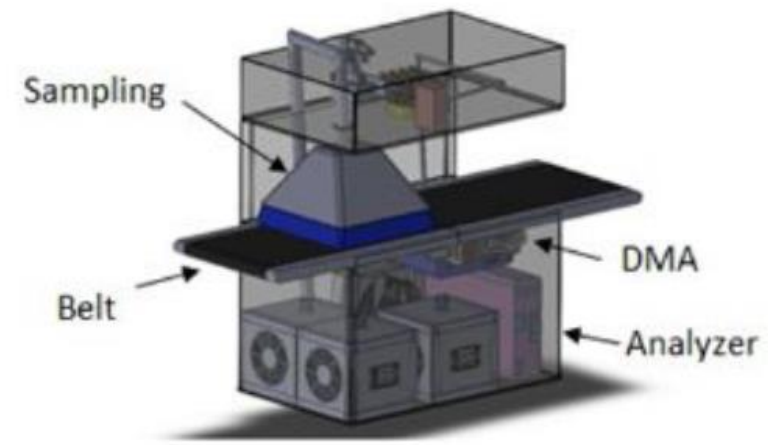
- expensive
- intrusive
- non-efficient
- depending on an operator



## Solution - VASCREEN

VASCREEN is a **new solution** that permits the detection of potentially harmful substances in luggage and goods.

- A non-target analysis system
- 4 times cheaper than X-ray analysis (less than 10 cts)
- More efficient with a Detection Rate (DR) > 90%
- Detection of new and unknown threats



# Results - VASCREEN

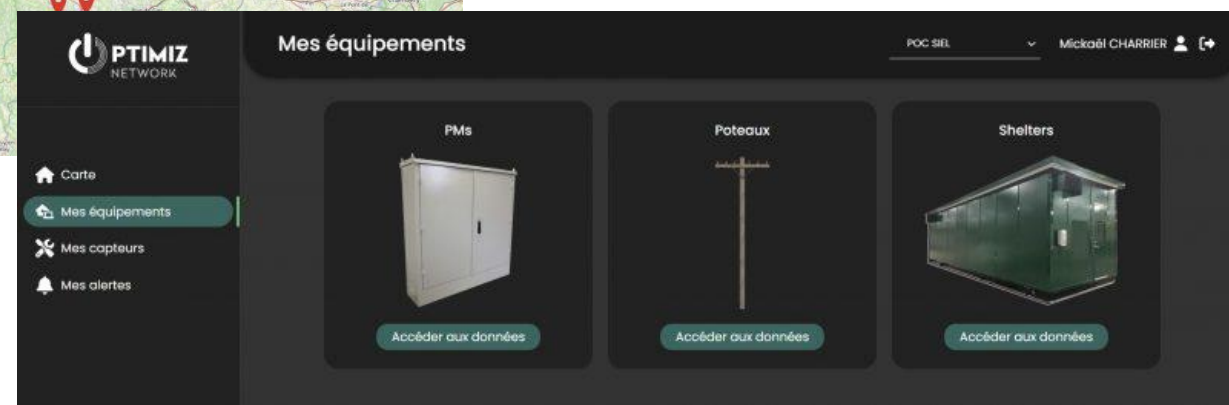
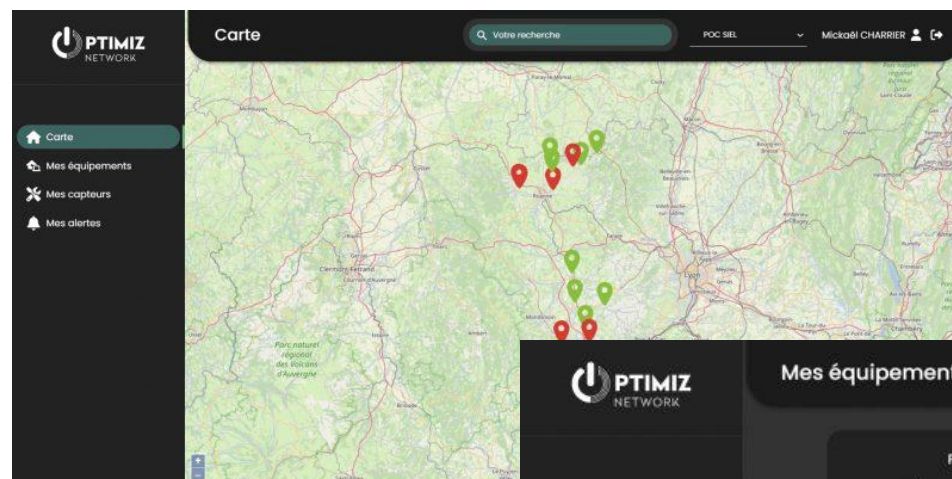
We achieved :

- sensitivity: 24087 counts / pg
- weight: from 50 kg to 25 kg
- processing time: from hours to 1 sec
- detection rate: over 70%



# Demonstration project - Open Call 2

- **OPTIMIZ-NETWORK** – *Securing, monitoring and optimizing infrastructure*
- Project partners : OPTIMIZ NETWORK (France) & ZARIOT (Ireland)



# SECURITY & SUPERVISION OF NETWORK INFRASTRUCTURES



IoT & Smart Solutions



# **Problem Statement : An ultra-sensitive infrastructure**

Without **Control, Security** or **Supervision**



**Weather hazards**



**Organizational risks**



**Business risks**



**Cybersecurity**

# Project Context : France THD plan & European deployments



- 30 billions € invested (France)
- Objective : 100% Fiber 2025



**« We are *ruining* everything we have worked so hard to do »**  
Cédric O – Secretary of State for the Digital Economy



- Towards 100% fiber in Europe
  - 200M subscribers for UE
1. Explosion of costs
  2. Risks
  3. Economic consequences

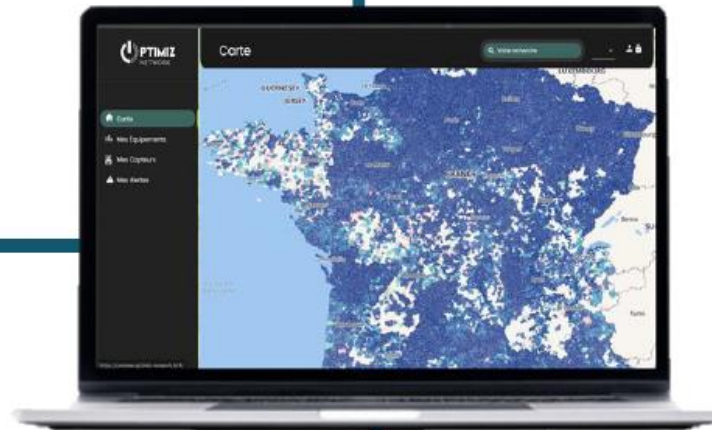
## FTTH : A CORNERSTONE FOR EUROPE'S DIGITAL AMBITIONS !

# Our Solution : Monitoring platform and physical security

## For Infrastructure Operators

### Data Collection :

- IoT Sensors
- Smart NFC Tags
- Blockchain
- Ensure complete traceability and data integrity



### Features :

- Alerts
- Maintenance prediction (AI)
- Installation status
- User access management
- Reporting & logs

### Users :

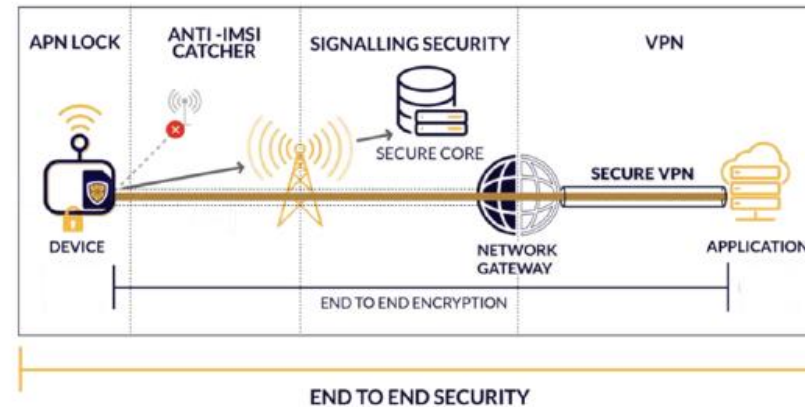
- Management team
- Network Administrator (NOC)
- Operations manager
- Field staff

# Partnership : OPTIMIZ-NETWORK & ZARIOT

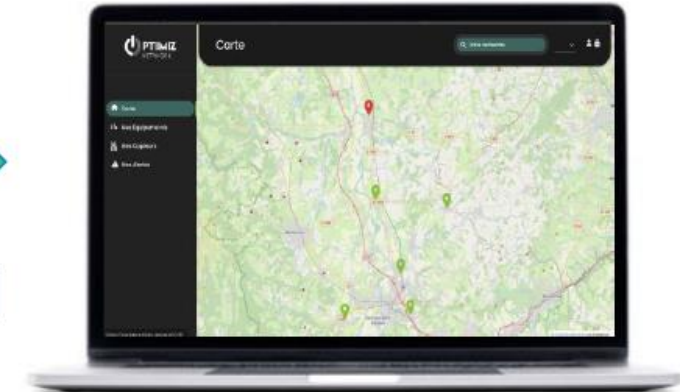
## Collection of Data



## Core network & Connectivity



## Platform IoT Core & Monitoring :



# What get Network Operators ?

## Better customer services

- Service continuity
- Communication restoration
- Better control of subcontracting
- Better network quality
- Better service quality
- Better reporting

## TCO's carbon foot print improvement

- Eliminate unnecessary work
- Intervention planning
- Reduce travel

## Security

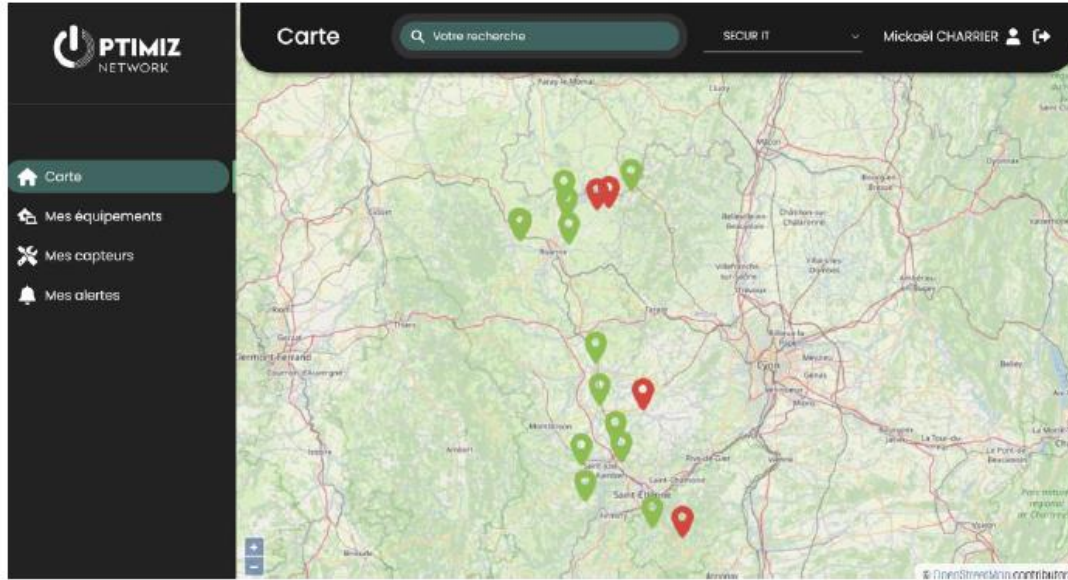
- Access control
- Traceability

## Law

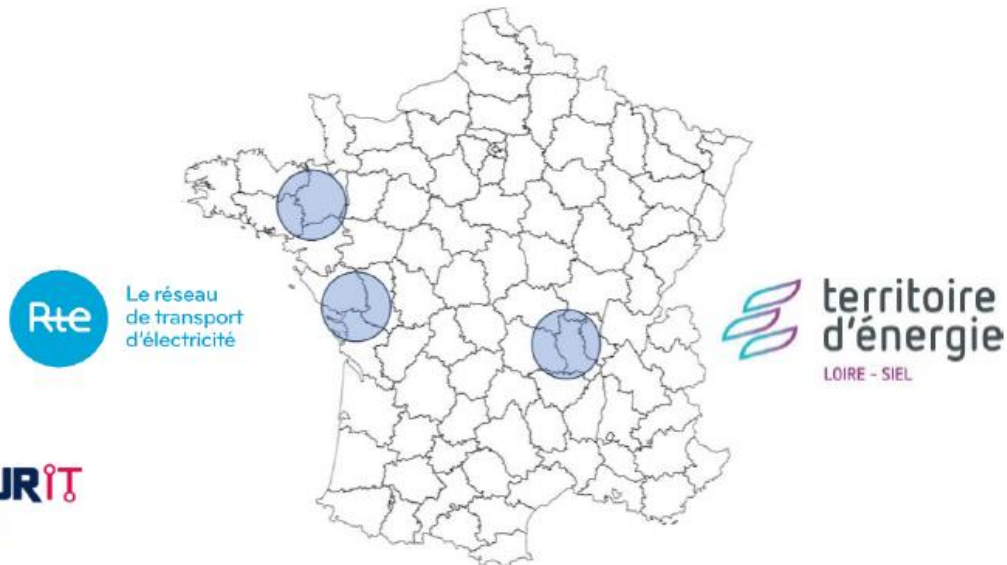
- Clarify responsibilities
- Improving the requirements base
- NIS2 compliance



# Partnerships & Deployments



Equipments	Poles	Cabinets	Shelters
Equipment considered	11	2	13
Sensor type	<ul style="list-style-type: none"> <li>Tilt</li> <li>Temperature</li> </ul>	<ul style="list-style-type: none"> <li>Temperature</li> <li>Humidity</li> <li>Door open contact</li> </ul>	<ul style="list-style-type: none"> <li>Temperature</li> <li>Humidity</li> <li>Door open contact / water detection</li> </ul>
Sensors qty	22	6	39
Use Cases	Monitoring of inclination and shock of poles	Door opening monitoring	Equipment access control
	Soil moisture level control	Water leak detection	Control of energy consumption



## Innovation & Benefits



## BLOCKCHAIN, IoT & AI



**UX** UI  
design



# Impact & Future Perspectives

## Current Impact :

- Transforming the way sensitive networks are managed
- Guarantee enhanced security for critical infrastructures
- Maintain the installations


## Future Perspectives :

- Geographic and industrial expansion
- Continuous innovation thanks to AI
- Ongoing engagement with end users to address future security challenges

**WE ARE PROUD OF OUR JOURNEY AND  
THE RESULTS ACHIEVED SO FAR**

**OUR COMMITMENT TO INNOVATION AND  
SECURITY REMAINS STEADFAST**

# Big Thank you to the Team !

							
<b>Mickael CHARRIER</b>	<b>Gérald GRANGIS</b>	<b>Abdelhadi BOUACHRINE</b>	<b>Ayman KHERRATI</b>	<b>Kyllian SENRENS</b>	<b>Charles BERNARD</b>	<b>Ines VOJNOVIC</b>	<b>Hrvoje MALETIC</b>
<b>Fondateur</b>	<b>Associate</b>	<b>DevOps</b>	<b>Developer</b>	<b>Developer</b>	<b>CTO</b>	<b>Engineer</b>	<b>Business</b>
CEO & Project Director / Telecom expert	CSMO & Cyber & DPO & Facilitator	IoT and Cybersecurity engineer Infrastrcuture	Project / Full stack	Project / Full stack	CTO / Security Manager	Software Engineer / Help integration	Business Development Commercial partnership
							

This project has received funding from



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



[contact@optimiz-network.fr](mailto:contact@optimiz-network.fr)



06 50 96 03 98



**B**âtiment des **H**autes **T**echnologies  
20 Rue Professeur Benoît Luras, 42000 Saint-Étienne



# Demonstration project - Open Call 2

- **EV-SAFE** – *Protecting EV Charging Infrastructure*
- Project partners : EV LOADER (Greece), Grid One (Croatia) & TEXNOMAT (Greece)





Protecting EV Infrastructure from cyber threats

This project has received funding from



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



Christos Stefanatos  
Product Lead  
[evloader.com](http://evloader.com)

A dark blue Tesla Model 3 is parked on a paved road that curves along a rocky, elevated landscape. The car is positioned on the right side of the frame, facing towards the left. In the background, a sprawling city with numerous buildings is visible, nestled in a valley. Beyond the city, a range of mountains stretches across the horizon under a hazy, overcast sky. The foreground consists of a rocky, uneven terrain with some sparse vegetation.

# 5 million new EV registrations expected by 2025

---

Source: [European Environment Agency](#)

Cyber Attacks  
to EV charging stations  
can disrupt essential  
infrastructure

---



Threat 1:  
DDOS: Distributed denial of  
service

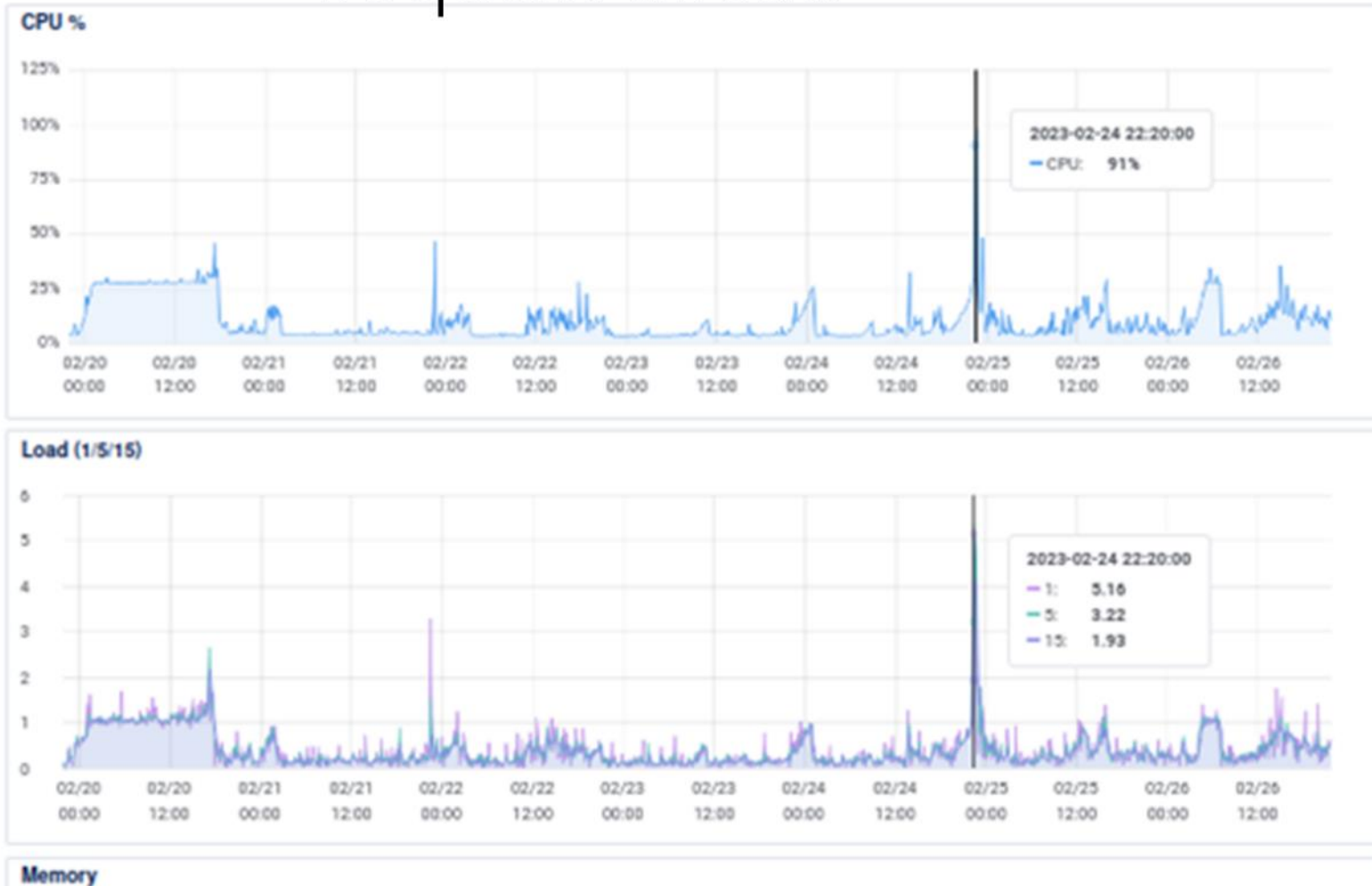
Result:

- Vehicle unable to charge
  - Drivers cannot unplug cables  
from vehicles already charging
- 



# DDOS attacks are a real and frequent threat!

Select period  
7 days



 **LOADER**  
evloader.com

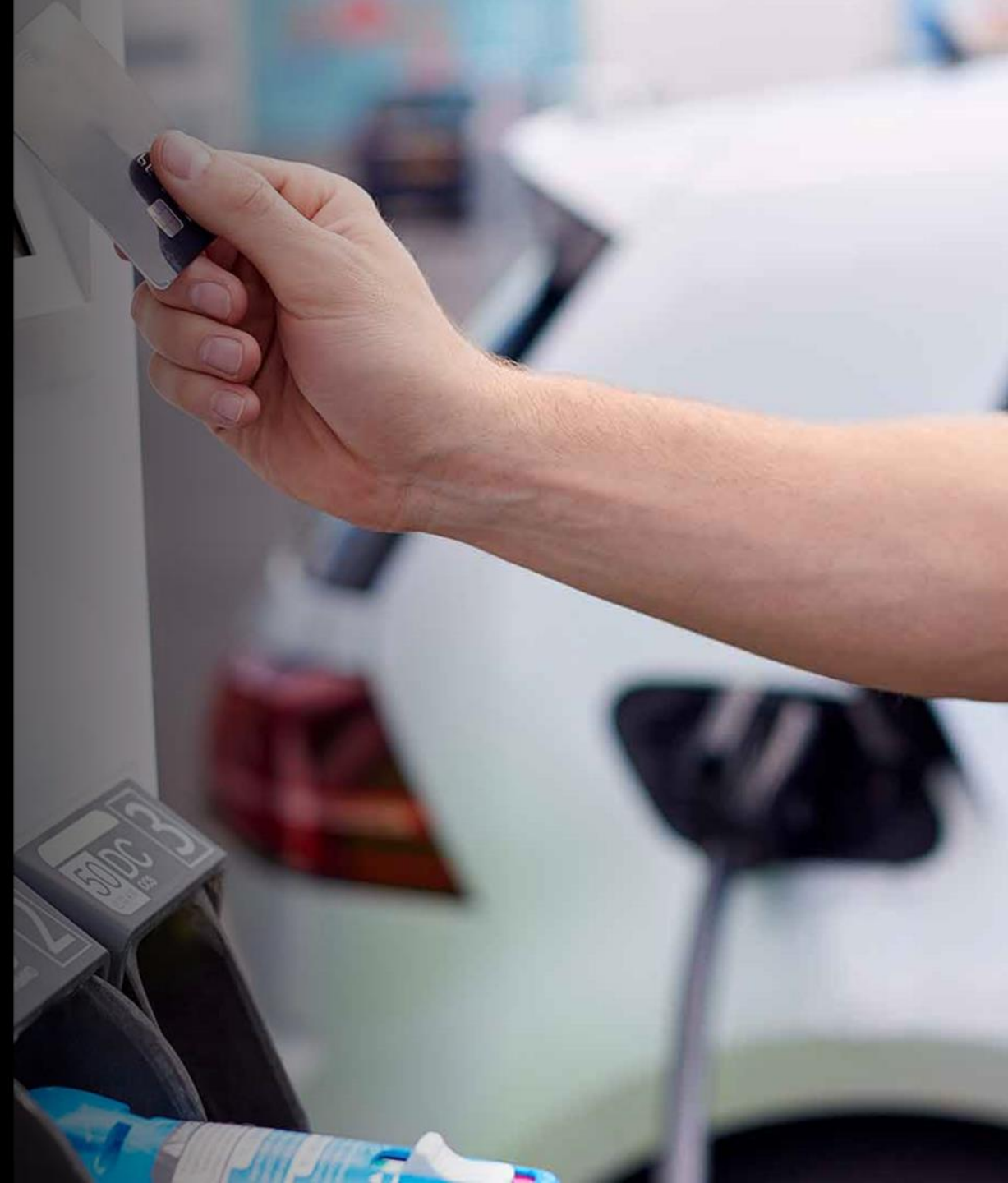
Friday 24<sup>th</sup> of February  
2023, 22:30



## Threat 2: Man in the Middle Attack

### Result:

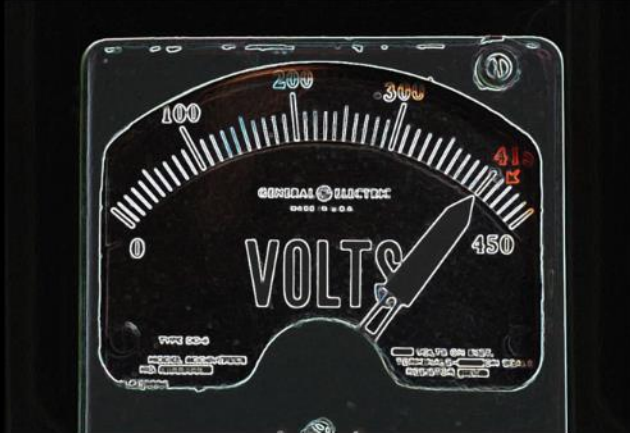
- PII Theft and Financial Fraud
  - Altered settings in the charging station
- 



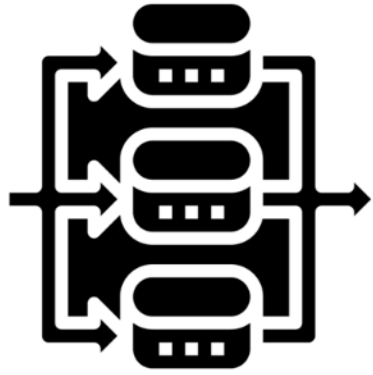
## Threat 2 (continued): Man in the Middle Attack

### Result:

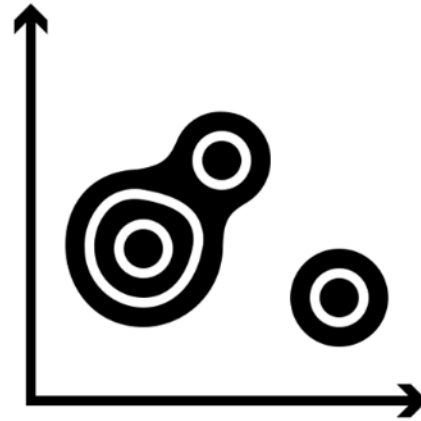
- Load Management Settings tampered
- Malicious actors can cause blackouts



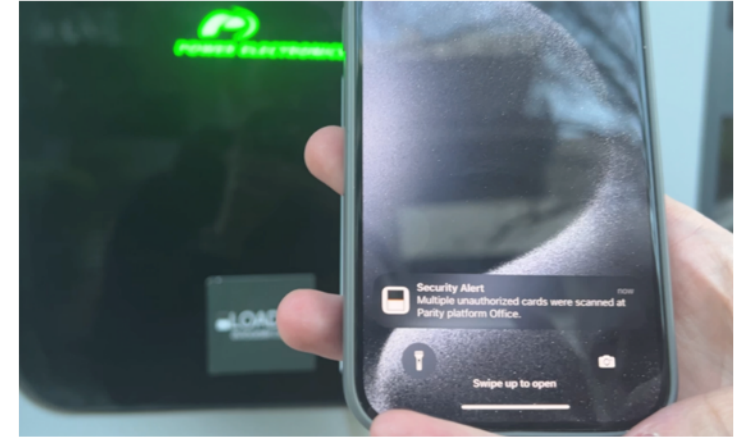
# Solution: EV Charging Station Cybersecurity Framework for CPOs



Encrypted Websocket connections  
+ Auth Passwords



SIEM: Analyze time series to quickly  
identify anomalies/outliers in real  
time



Quickly Identify and respond to  
issues

# EV Safe Project :

## Develop, deploy and test a scalable security framework for CPOs



Develop interoperable software components



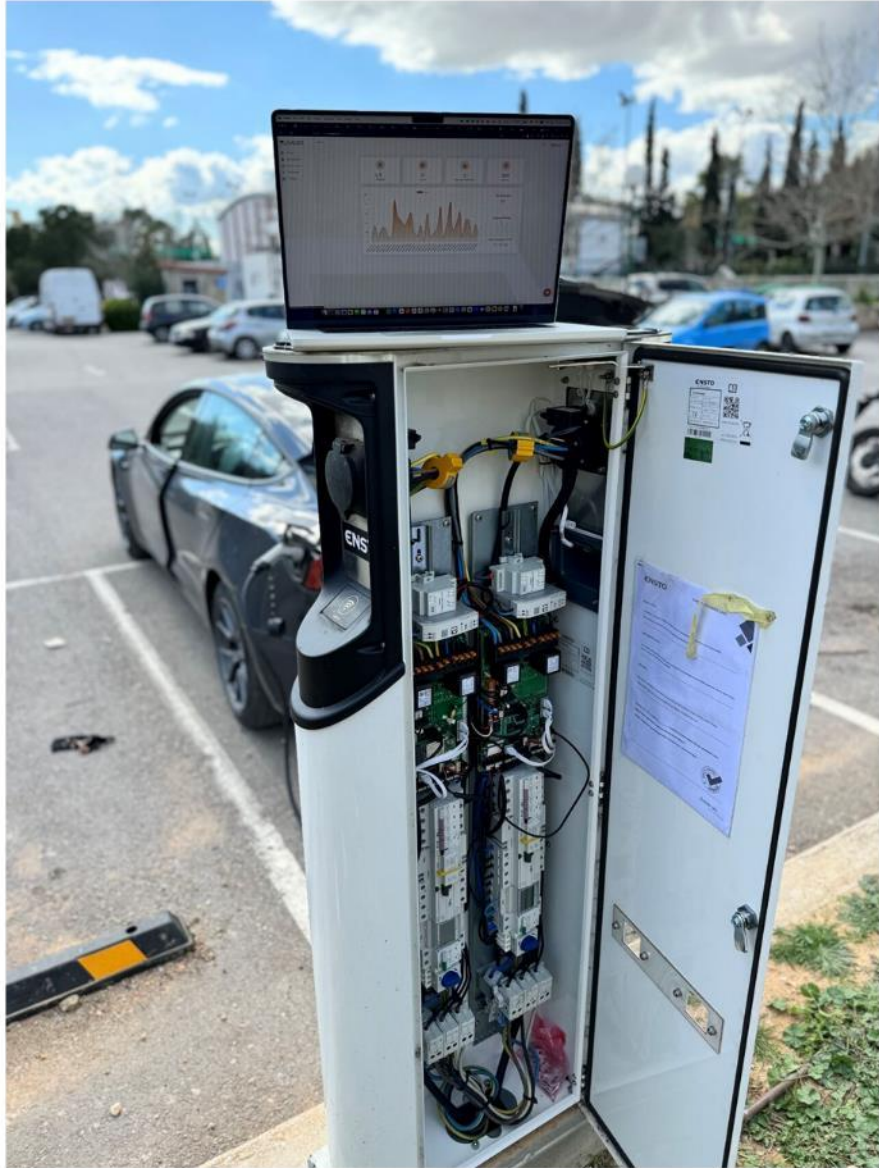
Test tools in pilot locations,  
Simulate Threat Scenarios

ABB

Shell Recharge

IONITY

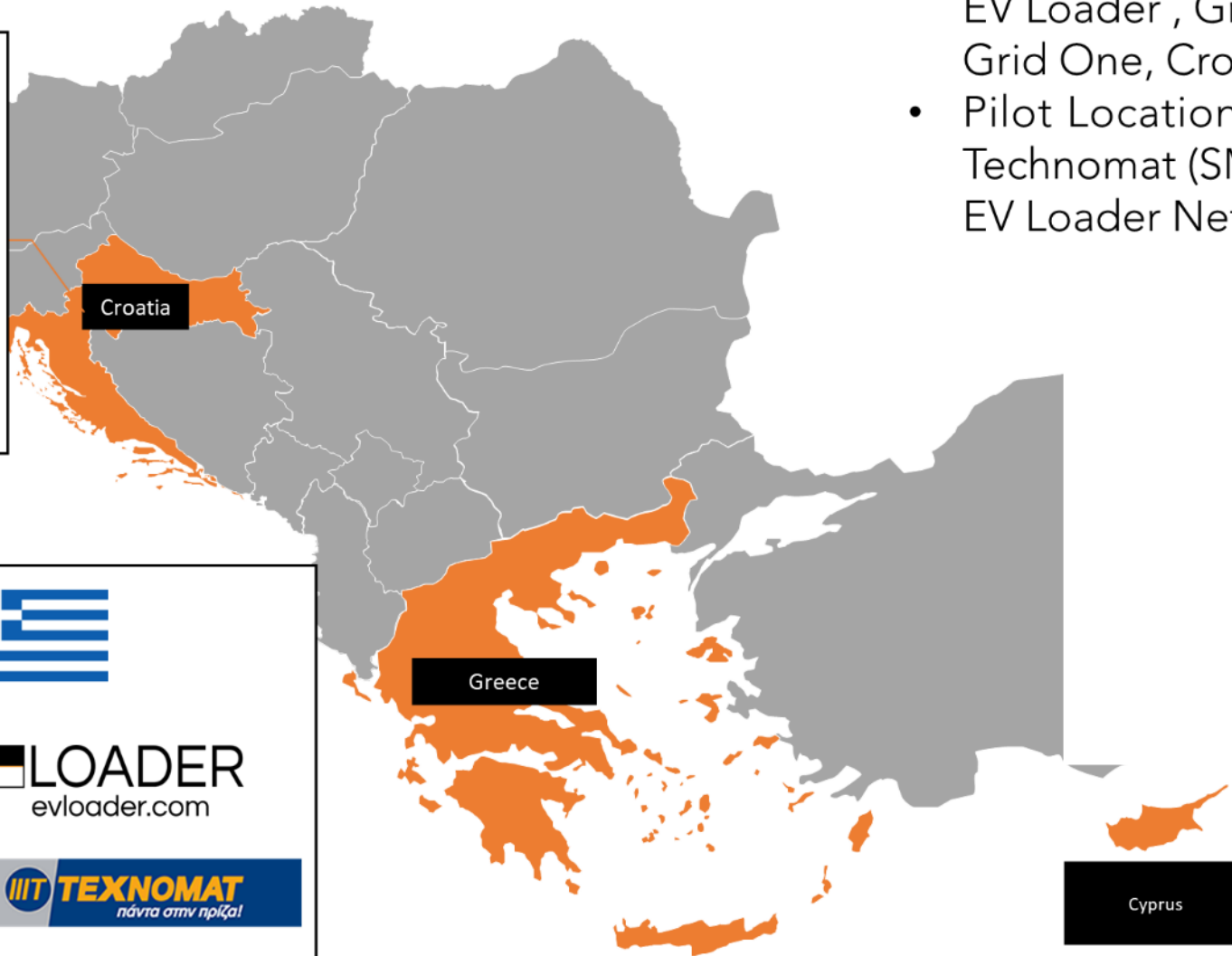
Provide tools to EV charging and  
energy metering stakeholders  
Release Whitepaper for security Best  
Practices

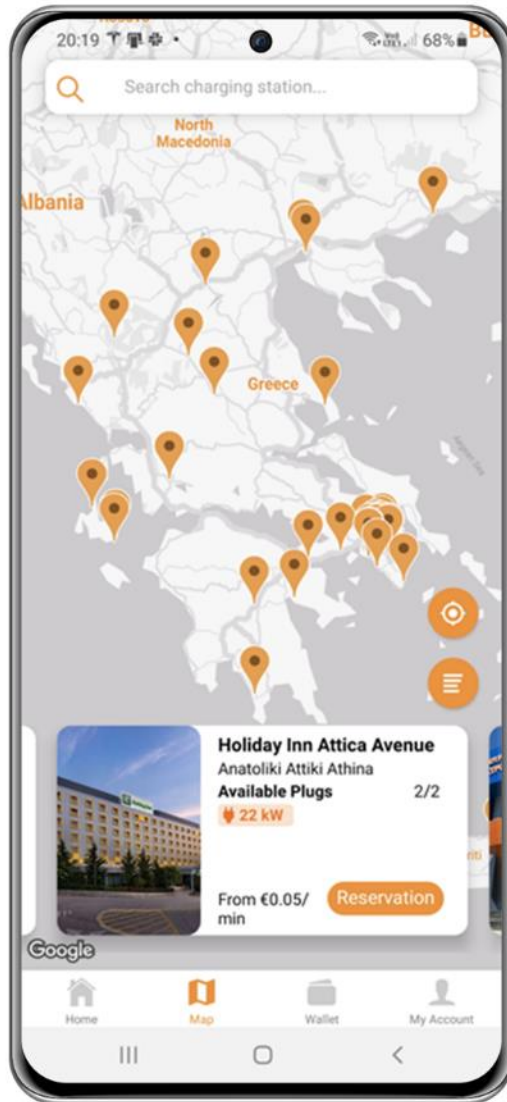


# Consortium Partners



- Technology Developers  
EV Loader , Greece  
Grid One, Croatia
- Pilot Locations  
Technomat (SME Partner),  
EV Loader Network





EV Loader manages chargers in more than 200 locations in Greece focusing on hotels



Municipality  
of Athens



Holiday Inn



# Looking for a pilot partner for EV charging in Horizon EU Projects?



National Technical  
University of Athens

**EPU**  
N · T · U · A



Partner in Horizon projects:

- [ICT-49-2020 - : I-ENERGY](#)

CL5-2022-D3-01- ENPOWER  
CL5-2023-D3-01 - Crete Valley

Collaborating with:  
EU partners include  
Utilities, Universities,  
DSOs



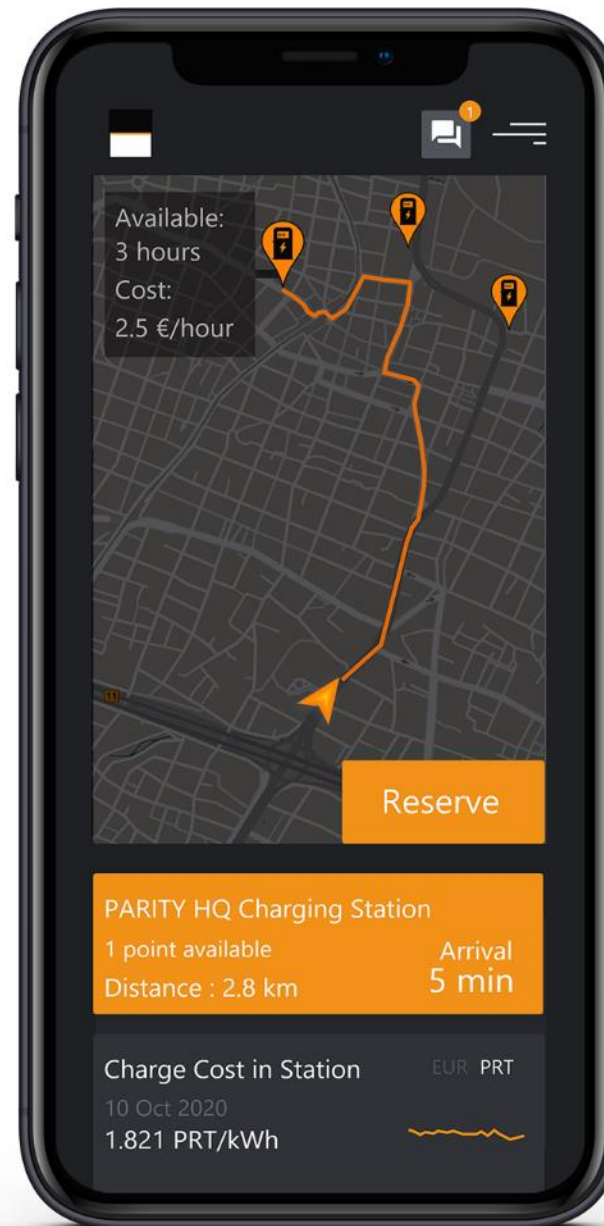


C.Stefanatos@evloader.com



Visit the website:

[evloader.com](https://evloader.com)



# Prototype project - Open Call 2

- **ERMINE** - *Innovative smart system disaster resilience*
- Project partners : Phasegrowth (Estonia) & Ecording (Turkey)



# ERMINE

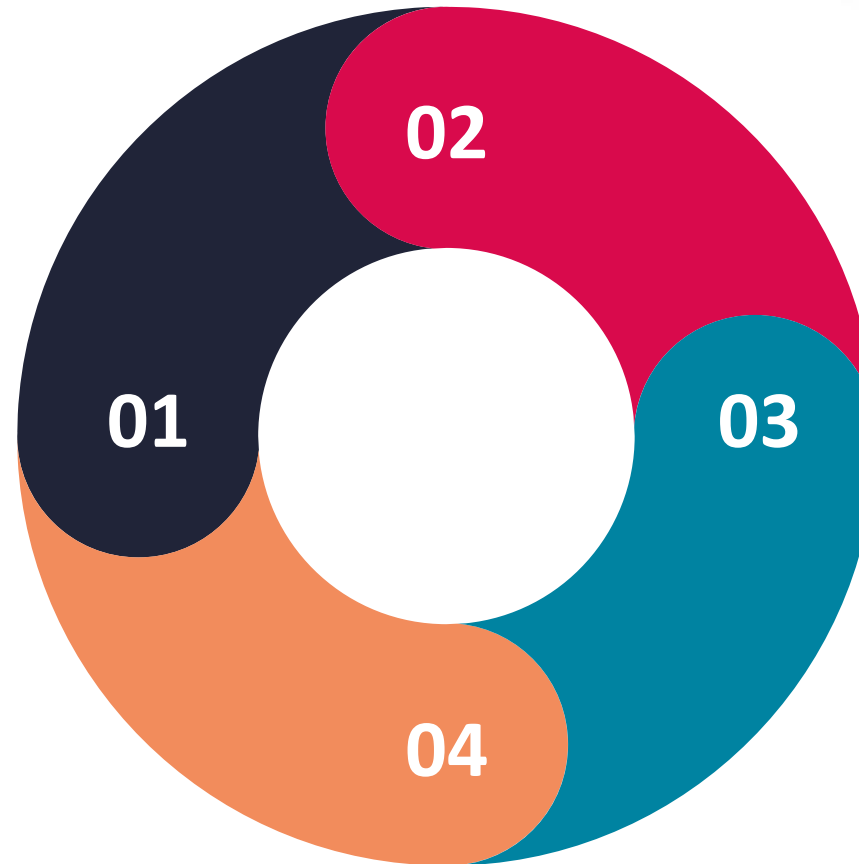
- **Project Title:** innovativE smaRt systeM for dlsaster resilieNcE (ERMINE)
- **Consortium Members:** Phasegrowth OU (Estonia), Ecording (Turkey), and associate partners from first responders
- **Funding:** SecurIT Prototyping Instrument 2, 2023 call



# Methodology


**Data Sources:** Copernicus satellite imagery, EGNOS geospatial data, UAV imagery, historical data records

**Data Fusion:** Harmonization of historical hazard records, satellite data, and real-time UAV data



**Hazard Modeling:** Development of wildfire and flood models using deterministic, empirical, and AI-based methods (pilot disasters) and cascading effects model

**Behavioral Modeling:** Analysis of public response to hazards; simulation of behaviors in Turkey, Bulgaria, and Estonia



## Cascading Effects Simulator (CascEffSim)

- Integrates hazard data, behavioral models, and risk assessments
- Simulates individual and group behaviors based on demographics using AgentBased Modeling
- Uses Monte Carlo simulations to estimate likelihood and impact of cascading events with Risk Assessment
- Generates simulations for various disaster scenarios, aiding in preparedness and response through Scenario Planning





## ERMINE on the road

- **Phase 1:** Design (July-August 2023): System architecture design and data integration plans
- **Phase 2:** Development (September - December 2023): Completion of hazard models, behavioral models, and CascEffSim tool, alpha and beta testing with end-users
- **Phase 3:** Validation (January-June 2024): Full-scale validation in Turkey and adjustment of the models
- **Phase 4+:** Market uptake and scaling (July 2024 onwards): recurring monthly revenue target of €12,000 at minimum and expansion to at least 40 subscribed users, add additional disaster models, validate and collect fees. Rollout in Estonia and Bulgaria, then elsewhere

## ERMINE is grateful to:



- Our mentor Marielle Campanella, who has been our guiding star, angel guardian and challenger on the way to success.
- First responders and volunteers in TR, EE and BG.
- The SecurIT consortium
- Other SecurIT startups and consortia that we have learned from.
- Last but not least, our families and friends for allowing us to spend a lot of time away from them working on the project.



**SECURiT**

TOWARDS RESILIENT SMART CITIES & TERRITORIES

# Congratulations to all!

Thank you!



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

# SMI2G

Security Mission Information & Innovation Group

2024 Brokerage Event  
**22 & 23 May**

Campus Cyber,  
La Défense, Paris

See you tomorrow!



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



[Securit-project.eu](https://securit-project.eu)



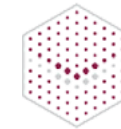
@SecurIT Innosup



@SecurITproject



@SecurIT20



**LSEC**  
LEADERS IN SECURITY

POLESCS

**L3CE**

**HSD**

**Systematic**  
Paris Region Deep Tech Ecosystem

**CenSec**  
CENTER FOR DEFENCE, SPACE & SECURITY



**FundingBox**



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