SECURIT

TOWARDS RESILIENT SMART CITIES & TERRITORIES

Project Deliverable

D2.5 Synergy Analysis with the European Structural and Investment Funds. A Review of Other Innovation Support Practices

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	V0.1
Due date	29/02/2024
Submission date	29/02/2024

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
V0.1	18/11/2023	Document Creation	ToC	L3CE
V0.5	15/02/2024	Most of the text provided	Draft	L3CE
V0.6	20/02/2024	Document review	Draft	Systematic
V1.0	29/02/2024	Final version	Final	L3CE

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

Table of Contents

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

List of Figures

List of Tables

List of Abbreviations

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

Authors (organisation)

L3CE

All Partners

Reviewers (organisation)

Systematic

Keywords

Funding, instruments, programmes, European, support, synergies, security

Legal notice

The information and views set out in this application form are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

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

1. Introduction

1.1 Aims of the document

To fulfil the aim of Task 2.3, we conducted an analysis of European Structural and Investment Funds (ESIF) and aligned them with a portfolio of 84 SMEs. This analysis encompassed 8 regions, wherein we identified successful cases of cooperation and collaboration between Member States (MS) and regional entities, totalling 8 cases.

Further, deliverable analyses synergies between the European Structural and Investment Funds (ESIF) and various other regional funding mechanisms operating within the partner regions of SecurIT consortium. The overarching objective is to identify opportunities for securing supplementary funding that can be allocated towards enhancing the SMEs portfolio and supporting other initiatives arising from the SecureIT project. This task required the development and presentation of a robust methodology for effectively mapping the diverse funding instruments available to specific projects The aim is to ensure that SMEs operating in Secure IT ecosystem can obtain concrete benefits from these funding instruments.

Additionally, our report introduces novel approaches, supportive tools, and services designed to assist SMEs in overcoming the typical challenges that hinder their ability to accelerate the innovation, penetrate new markets, engage with new customers, and secure additional funding.

1.2 Structure of the document

Section “Support of projects in security domain” describes methodology of mapping projects to financial instruments, followed by actual results of the mapping.

Section “Analysis of practices” is dedicated to the analysis of process and identifying best practices considering following views:

1. Identification of new, trending, and innovative ways addressing security sector challenges and practice to be shared for adoption and upscale to the EU level strategic initiatives.
2. Identification of successful MS or region of cases of cooperation and collaboration strategies and integral solutions between security sector end-users.

The scope of those activities within the Task 2.3 in quantitative measures included analysis of 8 regions and 12 cooperation and collaboration MS/Regional success cases identified.

This Section describes several selected success stories that illustrates how SMEs effectively navigated challenges and utilised supportive mechanisms provided by SecurIT consortium. These success stories aimed to showcase the role of ecosystems to foster innovations in growing EU security market.

Further a more generic subject – good practice is analysed, that can be applied in certain circumstances.

Last Section concludes all document and provide a condensed remainders on main lessons learnt, recommendations and how take-aways of the Task can be used further.

1.3 Relations with other deliverables

This document will provide input to D4.3. Exploitation and Sustainability plan, which will detail the exploitable outcomes of the project and lay the groundwork for activities beyond the project conclusion.

Specifically, deliverable D2.5 produced the tool for facilitating to SME’s access to information about financing opportunities. As task for producing this deliverable exhausted its dedicated efforts, D4.3 is requested to consider the potential for its further use and update. Steps might be taken to ensure its continued availability, as it falls within the realm of exploitable outcomes.

This deliverable receives inputs from identified success of the funded projects, methodologies developed, and best practices established.

The “Public” dissemination level of this document shapes disclosure level. As there are no agreement with funded SMEs on disclosure of information, document contains only aggregated information and cases are described only on the project level. Descriptions are limited to the publicly available descriptions of funded projects.

2. Support of projects in security domain

The allocation of funding for selected innovations projects is a model of functioning of SecurIT project. Recognizing the importance of nurturing innovation, SecurIT team discovered and implemented additional measures to foster the growth of these projects. This led to the incorporation of various support services such as mentoring, legal and ethical guidance, end-users' engagement, matchmaking events to facilitate finding relevant partners and resources.

To ensure the sustainability of selected innovative projects, among other efforts, Task T2.3 had to develop methodology and produce mapping of projects to potential funding sources.

It's important to emphasize that sustainable funding is essential for ensuring the continuity and progress of these projects. There exists a wide array of funding instruments that SMEs could potentially leverage to accelerate their innovations. Unfortunately, due to asymmetry of information and limited resources, SMEs aware of only a fraction of these opportunities.

This discrepancy highlights the need for deeper analysis of available funding opportunities and identifying and prioritizing the most relevant to SMEs respective industries.

2.1 Methodology

Initial design of the Task included mapping projects to two types of documents: funding instruments and strategic documents. The value of link with funding instruments is rather obvious, while to strategic instruments needs some explanation. Different EU MS prioritize the development of technologies differently, driven by their unique security concerns and threat landscapes. This divergence in priorities can lead to the differences in the procurement of various security solutions. Recognising these particularities, we can provide valuable insights into market potential, suitable geographical partners or even manufacturing areas. Thus, it is essential to align these priorities with funding and procurement instruments to effectively address complexity of security needs.

During the starting stage of the project the initial list of potentially relevant strategic documents and funding instruments were gathered from partner countries. The list of strategic documents contained 20 different documents from 8 geographies: Belgium, Poland, France, Denmark, Netherlands, Italy, Lithuania, and EU were analysed as a separate region. Most of them were cybersecurity focused, some of them contained higher level priorities.

For example, in Lithuania 4 such documents were examined:

- Programme for the European Union funds' investments in 2021–2027 (includes European Regional Development Fund (ERPF), Cohesion Fund (CF), European Social Fund+ (ESF+))[1]

[1] Link for uploads: https://www.bing.com/ck/a?!&&p=d4fcb51aa19f99a7JmltdHM9MTcwOTA3ODQwMCZpZ3VpZD0wN2ZjYjRhNC05ZGI0LTY0YjYtMzU5Yi1hNjFjOWNhOTY1ZmUmaW5zaWQ9NTE4NQ&ptn=3&ver=2&hsh=3&fclid=07fcb4a4-9db4-64b6-359b-a61c9ca965fe&psq=Programme+for+the+European+Union+funds%e2%80%99+investments+in+2021%e2%80%932027+(includes+European+Regional+Development+Fund+(ERPF)%2c+Cohesion+Fund+CF)%2c+European+Social+Fund%2b+(ESF%2b))&u=a1aHR0cHM6Ly8yMDIxLmVzaW52ZXN0aWNpam9zLmx0L3VwbG9hZHMvZG9jdW1lbnRzL2RvY3MvMjAyMi0wOS84NzdlN2RhZGUwZDQxYTM4YjQwNWU0ZmM1NDU4Y2Q5MTc0Yzc2ZDcwOTE1OGYyOTkzMGFkZmQ5M2RhNDk0MWZkLmRvY3g&ntb=1

- Cybersecurity strategy[2],
- EU Strategy for the Baltic Sea Region (action plan)[3],
- Smart specialization[4].

The initial list of funding instruments was produced with 20 instruments from these geographies. Description of funding instruments was developed. Strategic documents were described by priorities, while information on funding instruments, besides source, name, and priorities, also included information on target organizations, international funding possibilities, target scope, due dates, periodicity, and some other information.

With SecurIT First Open Call selected projects funding instruments were matched.

However, it appeared difficult to identify any meaningful links. There were few reasons for this:

- Different taxonomy used in projects definitions,
- Too high-level description of priorities,
- Most documents are written in the national languages and address national contexts,
- Mapping “all to all” situations and others.

It also requires extensive time-consuming reading of instruments’ descriptions while trying to identify possible matches with selected projects. Thus, we attempted to identify the universal approach that could be applied across different countries and funding instruments. We decided to “decompose” projects to features that can be subject of funding instruments or strategic documents. So relevant elements of the project could be matched with the funding instruments.

The list of such features was developed. It contained 5 categories:

1. **Techniques** – what techniques are employed in the solution to generate the output e.g. AI (ML), laser, CBRN, biometry and others? These technologies may be eligible for financial support or considered strategic priorities regardless of their specific application area.
2. **Process** - the outcomes of a solution can encompass various processes or their components, which may become the subject of national priorities and eligible for financial support. Examples include data sharing, forensics, etc.
3. **Applications** - can solution be applied in other area beyond security.? This allows us to identify other domains that can be relevant for potential adjustment of innovation. Financial instruments might be very different from the ones for security domain, but highly relevant to SME's.
4. **Development support** - what would be the subsequent stages for advancing innovation towards market readiness? There are instruments supporting prototyping, validation, productization and other stages of innovation transition to the market.
5. **General** - what other relevant activities can be funded? In most cases those would be participation in exhibitions, development of marketing materials, search of partners etc. Specific funding instruments can be available for such actions.

Such decomposition was also applied for financial instruments and strategic documents. A complete list of all features is provided in Annex 1.

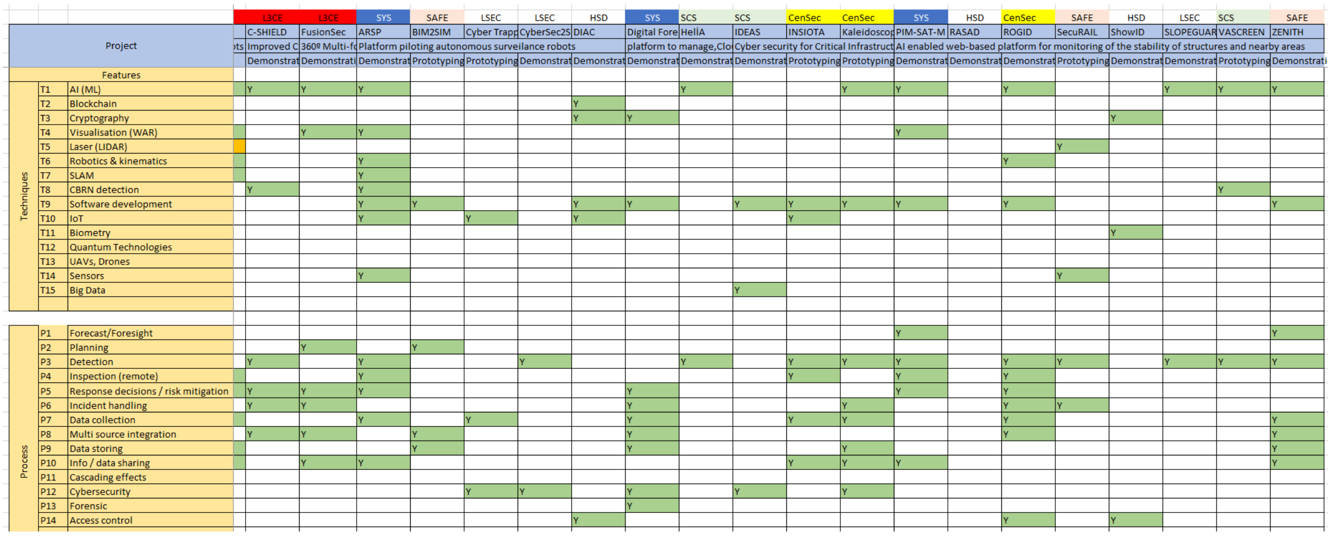
As all funded projects, funding instruments and strategic documents were described by the features, the matrix was produced matching funding instruments with the relevant features of to be funded project. An illustration of the data collected is provided below.

[2] 2019-EN-KibernetineSaugumoStrategija-el.pdf (kam.lt)

[3] Action plan (eusbsr.eu)

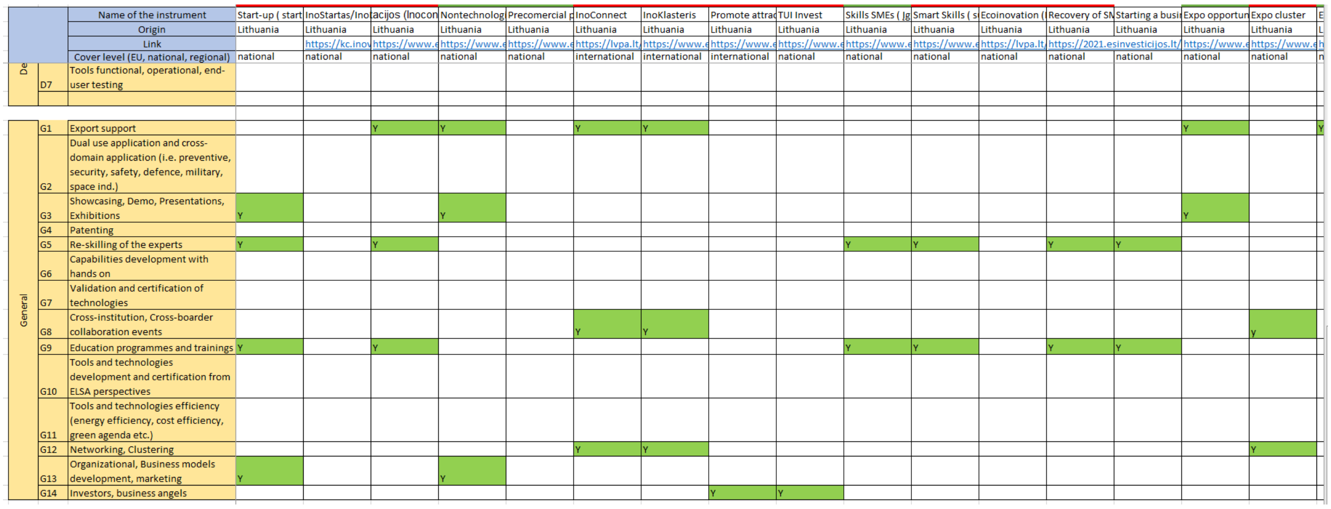
[4] Smart specialization | Ministry of the Economy and Innovation of the Republic of Lithuania (lrv.lt)

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



			L3CE	L3CE	SYS	SAFE	LSEC	LSEC	HSD	SYS	SCS	SCS	CenSec	CenSec	SYS	HSD	CenSec	SAFE	HSD	LSEC	SCS	SAFE
Project			C-SHIELD	FusionSec	ARSP	BIM2SIM	Cyber Trapp	CyberSec2S	DIAC	Digital Fore	HelİA	IDEAS	INSIOTA	Kaleidoscop	PIM-SAT-M	RASAD	ROGID	SecuRAIL	ShowID	SLOPEGUAR	VASCREEN	ZENITH
			Improved C	360º Multi-fc	Platform piloting autonomous surveilance robots					platform to manage,Clo		Cyber security for Critical Infrastruct			AI enabled web-based platform for monitoring of the stability of structures and nearby areas							
			Demonstrat	Demonstrati	Demonstrat	Prototyping	Prototyping	Demonstrat	Demonstrat	Demonstrat	Demonstrat	Demonstrat	Prototyping	Prototyping	Demonstrat	Demonstrat	Demonstrat	Prototyping	Demonstrat	Demonstrat	Prototyping	Demonstrati
Features																						
Techniques	T1	AI (ML)	Y	Y	Y						Y			Y	Y		Y			Y	Y	Y
	T2	Blockchain							Y													
	T3	Cryptography							Y	Y									Y			
	T4	Visualisation (WAR)		Y	Y										Y							
	T5	Laser (LIDAR)																Y				
	T6	Robotics & kinematics			Y												Y					
	T7	SLAM			Y																	
	T8	CBRN detection	Y		Y																Y	
	T9	Software development			Y	Y			Y	Y		Y	Y	Y	Y		Y					Y
	T10	IoT			Y		Y		Y				Y									
	T11	Biometry																	Y			
	T12	Quantum Technologies																				
	T13	UAVs, Drones																				
	T14	Sensors			Y													Y				
	T15	Big Data										Y										
Process	P1	Forecast/Foresight													Y							Y
	P2	Planning		Y		Y																
	P3	Detection	Y		Y			Y			Y		Y	Y	Y		Y	Y		Y	Y	Y
	P4	Inspection (remote)			Y								Y		Y		Y					
	P5	Response decisions / risk mitigation	Y	Y	Y					Y					Y		Y					
	P6	Incident handling	Y	Y						Y				Y			Y	Y				
	P7	Data collection			Y		Y			Y			Y	Y			Y					Y
	P8	Multi source integration	Y	Y		Y				Y							Y					Y
	P9	Data storing				Y				Y				Y								Y
	P10	Info / data sharing		Y	Y								Y	Y	Y							Y
	P11	Cascading effects																				
	P12	Cybersecurity					Y	Y		Y		Y		Y								
	P13	Forensic								Y												
	P14	Access control							Y								Y		Y			

Figure 1. Illustration of the funded projects features breakdown.



		Name of the instrument	Start-up (start	InoStartas/Ino	acijos (Inocon	Nontechnologi	Precomercial p	InoConnect	InoKlasteris	Promote attrac	TUI Invest	Skills SMEs (Jg	Smart Skills (s	Ecoinovation (I	Recovery of SM	Starting a busi	Expo opportun	Expo cluster	E
		Origin	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	Lithuania	L
		Link		https://kc.inov	https://www.e	https://www.e	https://www.e	https://lvpa.lt/	https://www.e	https://www.e	https://www.e	https://www.e	https://www.e	https://lvpa.lt/	https://2021.esinvesticijos.lt/		https://www.e	https://www.e	h
		Cover level (EU, national, regional)	national	national	national	national	national	international	international	international	national	national	national	national	national	national	national	national	n
De	D7	Tools functional, operational, end-user testing																	
General	G1	Export support			Y	Y		Y	Y								Y		Y
	G2	Dual use application and cross-domain application (i.e. preventive, security, safety, defence, military, space ind.)																	
	G3	Showcasing, Demo, Presentations, Exhibitions	Y			Y											Y		
	G4	Patenting																	
	G5	Re-skilling of the experts	Y		Y							Y	Y		Y	Y			
	G6	Capabilities development with hands on																	
	G7	Validation and certification of technologies																	
	G8	Cross-institution, Cross-boarder collaboration events						Y	Y									y	
	G9	Education programmes and trainings	Y		Y							Y	Y		Y	Y			
	G10	Tools and technologies development and certification from ELSA perspectives																	
	G11	Tools and technologies efficiency (energy efficiency, cost efficiency, green agenda etc.)																	
	G12	Networking, Clustering						Y	Y									Y	
	G13	Organizational, Business models development, marketing	Y			Y													
	G14	Investors, business angels								Y	Y								

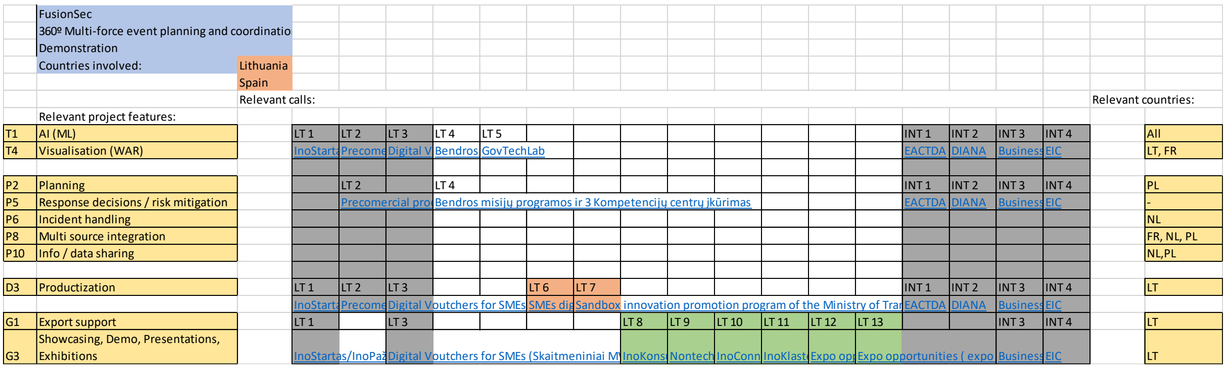
Figure 2. Illustration of the funding instruments features breakdown.

The structured data provided the opportunity to make a manual mapping of projects and funding instruments.

2.2 Result of mapping

First results of mapping were provided for projects from the First Open call. Mapping was done manually. Example of the results is provided below.

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



	FusionSec																				
	360º Multi-force event planning and coordinatio																				
	Demonstration																				
	Countries involved:	Lithuania																			
		Spain																			
		Relevant calls:																		Relevant countries:	
	Relevant project features:																				
T1	AI (ML)		LT 1	LT 2	LT 3	LT 4	LT 5									INT 1	INT 2	INT 3	INT 4		All
T4	Visualisation (WAR)		InoStarta	Precome	Digital V	Bendros	GovTechLab									EACTDA	DIANA	Business	EIC		LT, FR
P2	Planning			LT 2		LT 4										INT 1	INT 2	INT 3	INT 4		PL
P5	Response decisions / risk mitigation			Precomercial pro		Bendros misijų programos ir 3 Kompetencijų centrų įkūrimas										EACTDA	DIANA	Business	EIC		-
P6	Incident handling																				NL
P8	Multi source integration																				FR, NL, PL
P10	Info / data sharing																				NL,PL
D3	Productization		LT 1	LT 2	LT 3			LT 6	LT 7							INT 1	INT 2	INT 3	INT 4		LT
			InoStarta	Precome	Digital Voutchers for SMEs			SMEs dig	Sandbox	innovation promotion program of the Ministry of Tran						EACTDA	DIANA	Business	EIC		
G1	Export support		LT 1		LT 3					LT 8	LT 9	LT 10	LT 11	LT 12	LT 13			INT 3	INT 4		LT
G3	Showcasing, Demo, Presentations, Exhibitions		InoStartas/InoPaž		Digital Voutchers for SMEs (Skaitmeniniai M\					InoKons	Nontech	InoConn	InoKlast	Expo opp	Expo opportunities (expo			Business	EIC		LT

Figure 3. Example of the project mapping to funding instruments.

The mapping results are based on the features that are relevant to the project. In the example case 10 features were selected as relevant, most of them are process related. The table provides matches of interest to funding instruments. The table indicates that there are 13 funding instruments from Lithuania and 4 international ones, that can be considered for further analysis. As it can be seen most of the national funding instruments can be used for export support, some for technological development and productization. Mapping results were developed for the funded projects of Open call 1 and Open call 2. Mapping was expanded to include “relevant countries”. The intention of this column was to indicate countries, where certain feature is clearly prioritised, so solution developers can search for partners there, consider evaluating funding possibilities or examine demand.

Results of mapping for projects selected in SecurIT Open call 1 and Open call 2 was produced and are demonstrated in Annex 2.

2.3 Production of the tools

After the mapping approach was updated and “decomposition” to features made, it become clear that mapping can be made more flexible and automated.

Though Description of Action does not mandate such deliverable, we deemed it important to produce the tool to enhance the access to the funding information for SMEs.

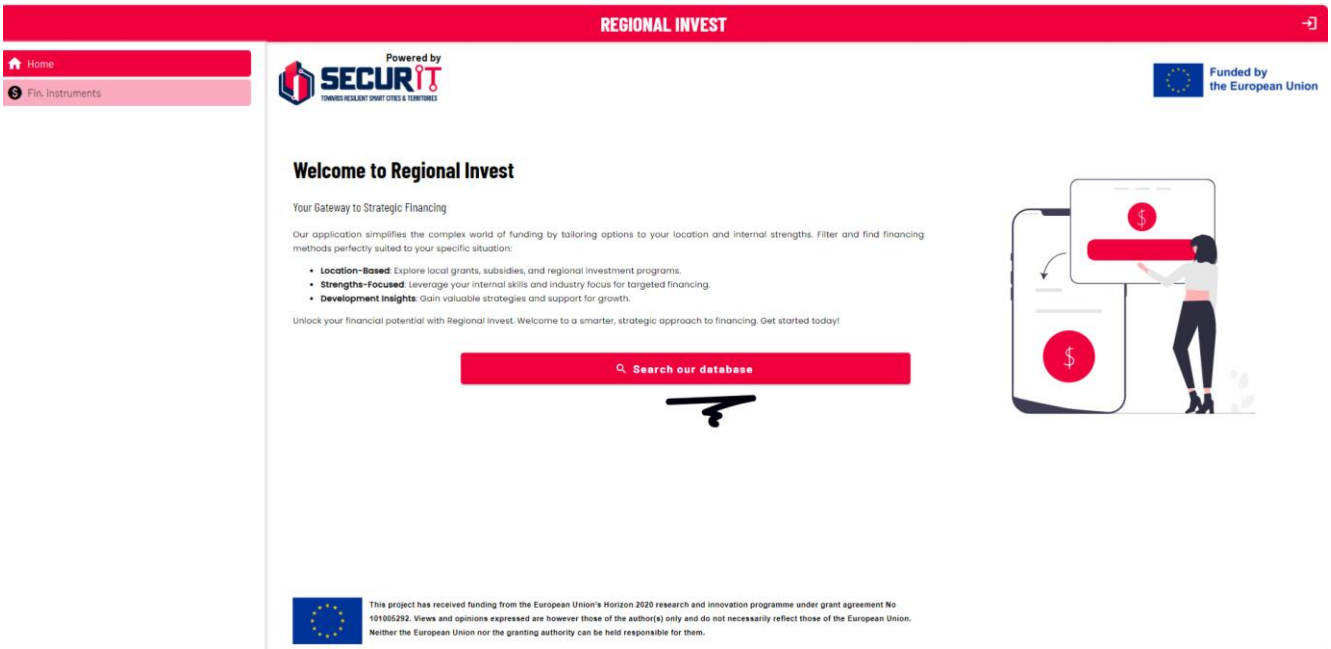
Tool will be made available to all interested entities through SecurIT web page (SecurIT – Towards resilient smart cities & territories (securit-project.eu)).

One of the project partners – LSEC – volunteered to develop the tool with Belgian company “Co-dex”. A simple tool was developed, containing all initial selection of funding instruments and strategic documents. It is available at: https://financing.digitalsecuritycatalyst.com

Further a short description of the tool is provided.

The entrance interface is very simple and functional options contain only the searching and log-in possibilities.

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



REGIONAL INVEST

Home
Fin. Instruments
Powered by SECURIT TOWARDS RESILIENT SMART CITIES & TERRITORIES
Funded by the European Union

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:

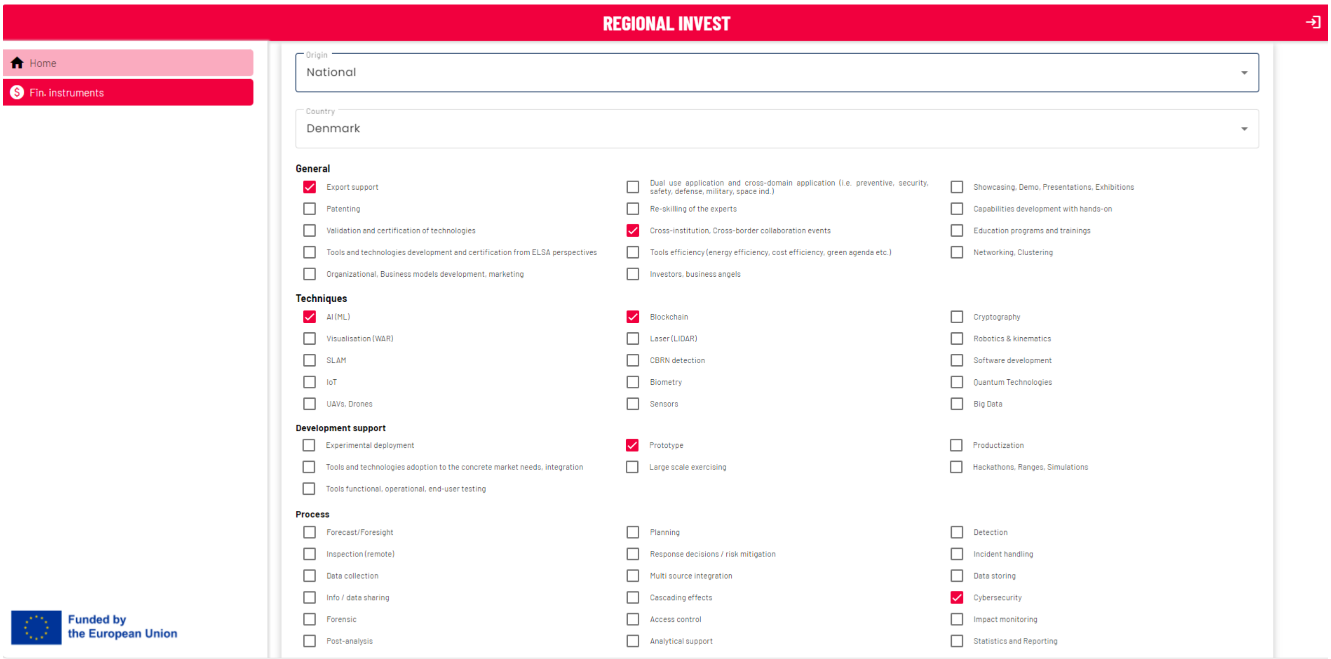
- **Location-Based**: Explore local grants, subsidies, and regional investment programs.
- **Strengths-Focused**: Leverage your internal skills and industry focus for targeted financing.
- **Development Insights**: Gain valuable strategies and support for growth.

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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Figure 4. Initial interface of the tool.

Users, this is publicly available, can search the database. They can choose between National and International instruments. Also, can make the selection of relevant features for their activities.



REGIONAL INVEST

Origin: National

Country: Denmark

General

☑ Export support
☐ Patenting
☐ Validation and certification of technologies
☐ Tools and technologies development and certification from ELSA perspectives
☐ Organizational, Business models development, marketing
☐ Dual use application and cross-domain application (i.e. preventive, security, safety, defense, military, space ind.)
☐ Re-skilling of the experts
☑ Cross-institution, Cross-border collaboration events
☐ Tools efficiency (energy efficiency, cost efficiency, green agenda etc.)
☐ Investors, business angels
☐ Showcasing, Demo, Presentations, Exhibitions
☐ Capabilities development with hands-on
☐ Education programs and trainings
☐ Networking, Clustering

Techniques

☑ AI (ML)
☐ Visualisation (WAR)
☐ SLAM
☐ IoT
☐ UAVs, Drones
☑ Blockchain
☐ Laser (LIDAR)
☐ CBRN detection
☐ Biometry
☐ Sensors
☐ Cryptography
☐ Robotics & kinematics
☐ Software development
☐ Quantum Technologies
☐ Big Data

Development support

☐ Experimental deployment
☐ Tools and technologies adoption to the concrete market needs, integration
☐ Tools functional, operational, end-user testing
☑ Prototype
☐ Large scale exercising
☐ Productization
☐ Hackathons, Ranges, Simulations

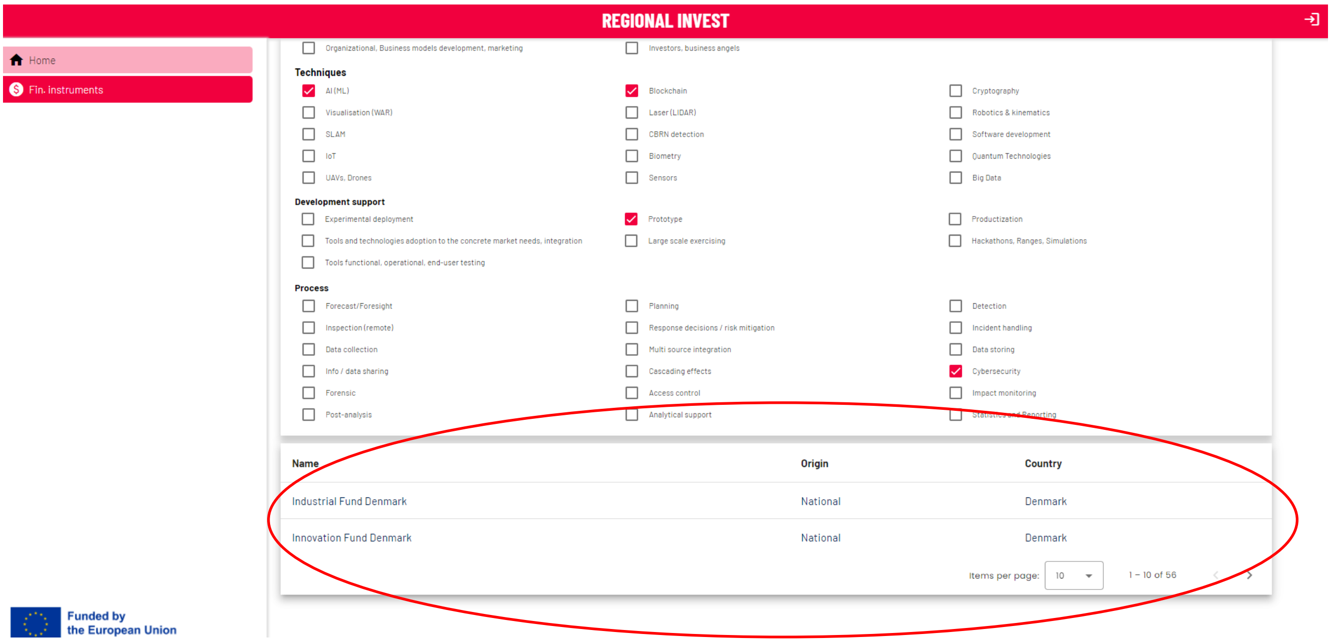
Process

☐ Forecast/Foresight
☐ Inspection (remote)
☐ Data collection
☐ Info / data sharing
☐ Forensic
☐ Post-analysis
☐ Planning
☐ Response decisions / risk mitigation
☐ Multi source integration
☐ Cascading effects
☐ Access control
☐ Analytical support
☐ Detection
☐ Incident handling
☐ Data storing
☑ Cybersecurity
☐ Impact monitoring
☐ Statistics and Reporting

Figure 5. Example of the user search.

Results can be found at the bottom of the page.

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



REGIONAL INVEST

□ Organizational, Business models development, marketing
□ Investors, business angels

Techniques

☑ AI (ML)
☑ Blockchain
□ Cryptography
□ Visualisation (WAR)
□ Laser (LIDAR)
□ Robotics & kinematics
□ SLAM
□ CBRN detection
□ Software development
□ IoT
□ Biometry
□ Quantum Technologies
□ UAVs, Drones
□ Sensors
□ Big Data

Development support

□ Experimental deployment
☑ Prototype
□ Productization
□ Tools and technologies adoption to the concrete market needs, integration
□ Large scale exercising
□ Hackathons, Ranges, Simulations
□ Tools functional, operational, end-user testing

Process

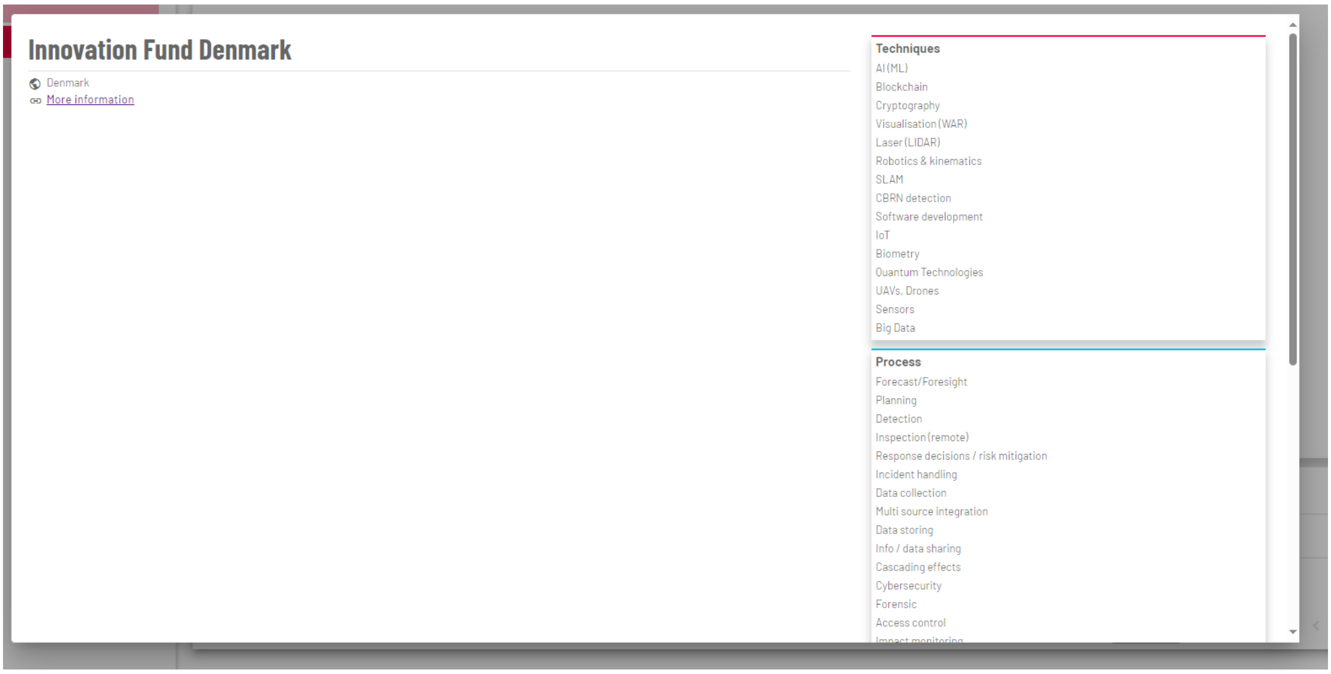
□ Forecast/Foresight
□ Planning
□ Detection
□ Inspection (remote)
□ Response decisions / risk mitigation
□ Incident handling
□ Data collection
□ Multi source integration
□ Data storing
□ Info / data sharing
□ Cascading effects
☑ Cybersecurity
□ Forensic
□ Access control
□ Impact monitoring
□ Post-analysis
□ Analytical support
□ Statistics and Reporting

Name	Origin	Country
Industrial Fund Denmark	National	Denmark
Innovation Fund Denmark	National	Denmark

Items per page: 10 ▾   1 – 10 of 56

Figure 6. Example of the user search results.

Each of the instruments can be opened to see more information.



Innovation Fund Denmark

Denmark
More information

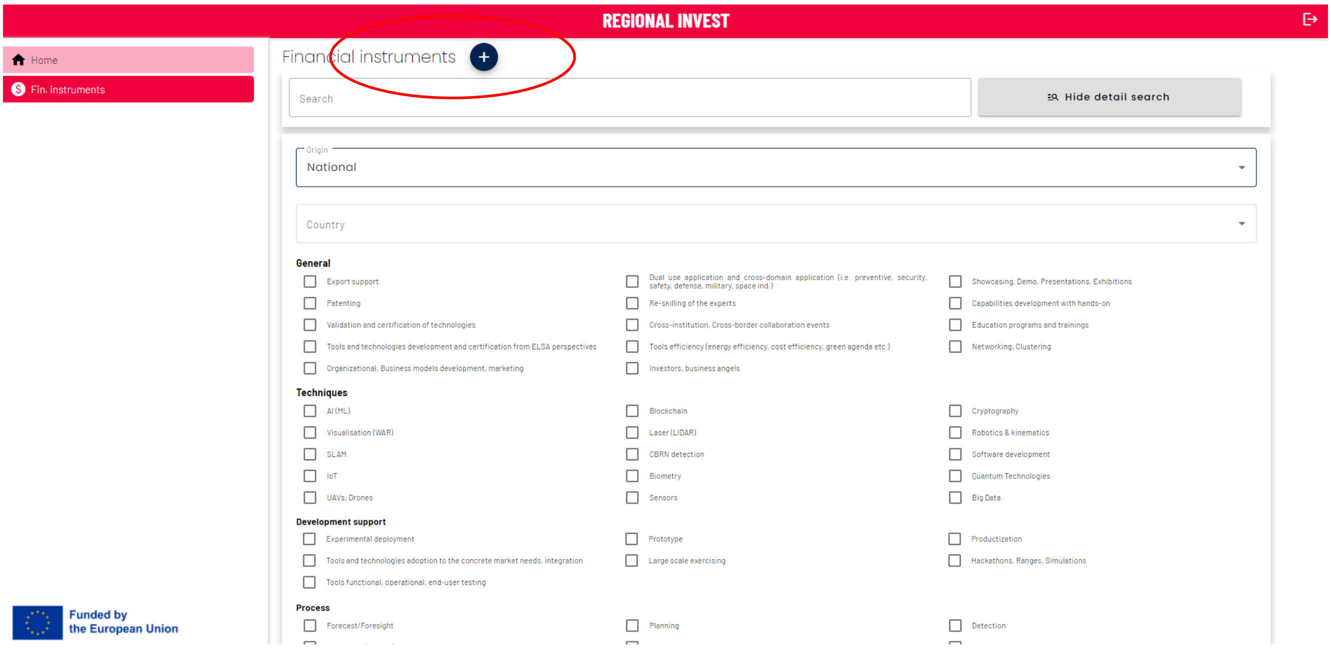
Techniques
AI (ML)
Blockchain
Cryptography
Visualisation (WAR)
Laser (LIDAR)
Robotics & kinematics
SLAM
CBRN detection
Software development
IoT
Biometry
Quantum Technologies
UAVs, Drones
Sensors
Big Data

Process
Forecast/Foresight
Planning
Detection
Inspection (remote)
Response decisions / risk mitigation
Incident handling
Data collection
Multi source integration
Data storing
Info / data sharing
Cascading effects
Cybersecurity
Forensic
Access control
Impact monitoring

Figure 7. Example of the user search results.

There are some additional functionalities for the partners authorised to add, edit and delete funding instruments or strategic documents. As you log-in to tool (users can search for the instruments without log-in), there is additional interface to handle information.

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



REGIONAL INVEST

Home

Fin. instruments

Financial instruments +

Search

Hide detail search

Origin
National

Country

General

☐ Export support
☐ Dual use application and cross-domain application (i.e. preventive, security, safety, defense, military, space ind.)
☐ Showcasing, Demo, Presentations, Exhibitions
☐ Patenting
☐ Re-skilling of the experts
☐ Capabilities development with hands-on
☐ Validation and certification of technologies
☐ Cross-institution, Cross-border collaboration events
☐ Education programs and trainings
☐ Tools and technologies development and certification from ELSA perspectives
☐ Tools efficiency (energy efficiency, cost efficiency, green agenda etc.)
☐ Networking, Clustering
☐ Organizational, Business models development, marketing
☐ Investors, business angels

Techniques

☐ AI (ML)
☐ Blockchain
☐ Cryptography
☐ Visualisation (WAR)
☐ Laser (LIDAR)
☐ Robotics & kinematics
☐ SLAM
☐ CBRN detection
☐ Software development
☐ IoT
☐ Biometry
☐ Quantum Technologies
☐ UAVs, Drones
☐ Sensors
☐ Big Data

Development support

☐ Experimental deployment
☐ Prototype
☐ Productization
☐ Tools and technologies adoption to the concrete market needs, integration
☐ Large scale exercising
☐ Hackathons, Ranges, Simulations
☐ Tools functional, operational, end-user testing

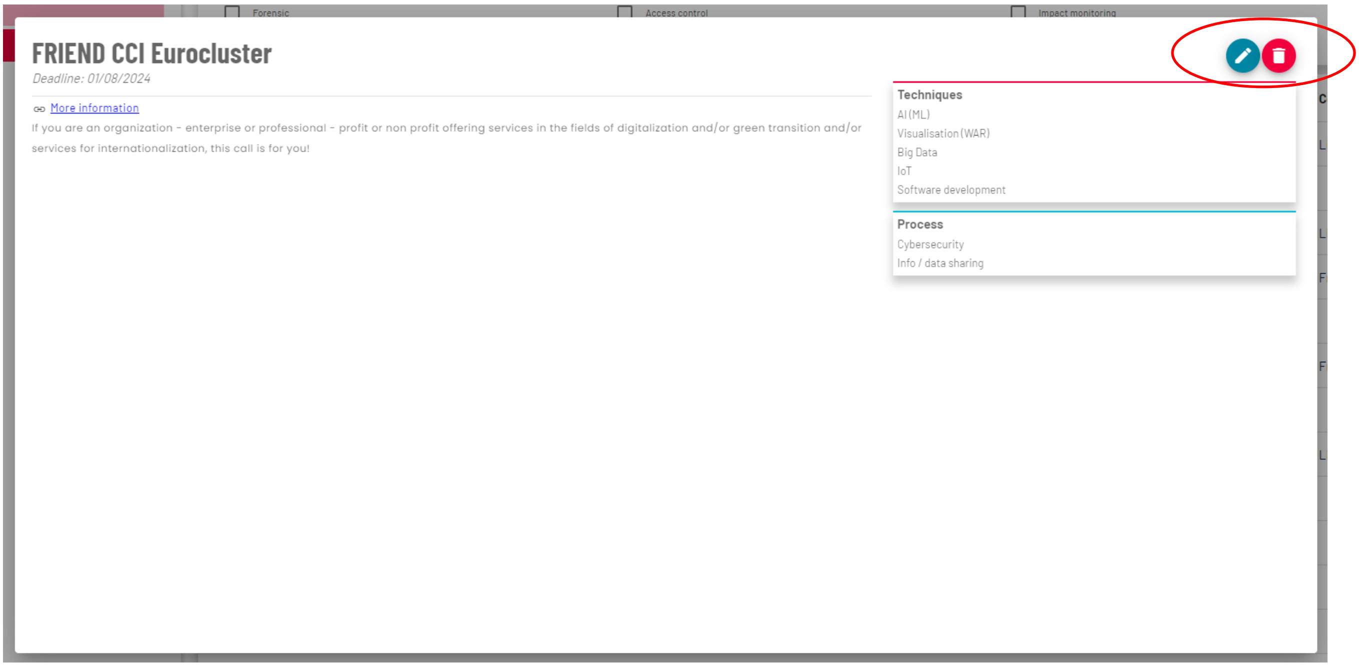
Process

☐ Forecast/Foresight
☐ Planning
☐ Detection

Funded by the European Union

Figure 8. Interface of the authorised users.

By clicking on the highlighted "+" bottom authorised users can add new instruments. They also have the ability to modify instruments that are already stored in the database.



☐ Forensic ☐ Access control ☐ Impact monitoring

FRIEND CCI Eurocluster

Deadline: 01/08/2024

More information

If you are an organization - enterprise or professional - profit or non profit offering services in the fields of digitalization and/or green transition and/or services for internationalization, this call is for you!

Techniques
AI (ML)
Visualisation (WAR)
Big Data
IoT
Software development

Process
Cybersecurity
Info / data sharing

Figure 9. Editing interface for authorised users.

Development of simple tool allows all funded projects to search for the funding instruments according to their needs.

This tool can be expanded further and provide a good ground for EU level funding instruments management in security domain. Exploitation of the tool will be explored further in the exploitation

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

deliverable. Some challenges and lessons learnt while developing this tool will be presented in the dedicated finalising section (Section 4 “Conclusions”).

The developed tool is very user friendly, can be used without specific training. There might be other technological solutions that can be employed to further improve functionality, like semantic search or AI / ML based search engines. But it is worth noting, that technology is not the most important component to make simplified access of funding instruments for SMEs operating in the security domain across EU. Maintenance, taxonomy, dissemination can be mentioned as a few other aspects that can make this tool effective.

This section provided the outlook of activities in Task 2.3 and main results achieved. During the implementation of the project approach have been adjusted and outcomes have changed, but the supportive nature of the task remained unchanged. We consider that current developments are more sustainable and can bring value and be developed further beyond the project implementation time. Some of the achievements of the funded projects and supported by SecurIT activities are provided in the next section.

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

3 Analysis of practices

3.1 Approach

There are no doubts that SecurIT core activities involve supporting SME's by funding their activities. Additionally, mentoring, legal & ethical review along with most tasks outlined in SecurIT were provided to facilitate development of the projects beyond funding.

It is rather difficult to quantify impact of those activities. Thus, this section outlines some examples of successful further development, considering that SecurIT project also added significant financial and soft value for those projects or SME's.

During execution of SecurIT project, which was specifically targeted to SME's working with security sector, 2 Open Calls for funding rounds were completed. Follow-up managers, which were assigned to mentor the funded projects identified barriers and challenges that SME's face developing offerings in security sector. Further in this report, we discuss some of them having the greatest impact. They further will be used to evaluate how instrumental to success cases were analysed different models and approaches to overcome them.

- **Difficulties in keeping pace with the complex and changing regulatory environment.**

  The security landscape is dynamic, with fast evolving threats and risks, while abundantly regulated. SMEs find it challenging to stay ahead of regulatory changes that influence the security market. Furthermore, SME might try to develop a solution based on innovative technology, which has not yet passed regulatory scrutiny on national and EU levels, which makes it specifically risky endeavour. Furthermore, this regulatory impact is also influencing the innovation process in itself: companies and their innovations must prove regulatory compliance even before entering the market.

- **Lack of understanding of end-user needs, requirements, and priorities by SMEs.**

  SMEs are typically very much technology and product driven and oriented, eager to tackle a specific end user problem from a single sometimes naive perspective from the world, without considering the complexities of typical day to day operational constraints. However, realities of security end-user organizations are very much shaped by strict regulatory compliance, process driven nature, very acute priorities, and established ecosystems, which is not always well understood by companies in general, and by SMEs in particular developing solutions and immersed in totally different realities Due to sensitivity of the security sector, they tend to limit their engagements with end-user organizations. With limited communication and understanding of sector realities SMEs too often develop solutions which do not fit or do not address priorities of their intended market.

- **Challenges maintaining and establishing new collaborations with relevant stakeholders.**

  SMEs, especially those without established networks, may find it challenging to connect with relevant stakeholders, hindering potential collaboration opportunities. It is very often that SME developing an innovative solution does not have a track record in the security sector, which makes it even more difficult to establish trusted relationships. Established networks of practitioners tend to be very closed communities that are reluctant to share their needs and gaps with SMEs or participate in collaborative innovation development processes. This difficulty results in inefficiencies across various stages of the innovation creation, including development, alignment with end-user expectations and uptake by end-user.

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

- **Very long innovation adoption time by end-user aka longer than anticipated sales cycles.**

  Even in the cases when end-user finds the innovation very valuable to be adapted, the time of integrating solution into existing ecosystems can be extremely long. Moreover, innovation procurement is a subject to diverse regulations, and its implementation varies across different Member States. Additionally, procurement organizations face challenges in clearly defining the procurement object, which is inherently specific to each MS. The struggle lies not only in the uniqueness of the innovation procurement process itself, but also in the varying capabilities of procurement organizations to articulate and specify the innovation procurement objectives. It's worth noting that very long-time horizon of innovation procurement can be very challenging for SMEs, especially considering that full user acceptance is not guaranteed.

- **Financial restraints and limited access to financial instruments.**

  Securing funding for innovation projects can be challenging for SMEs. This is a generic problem which most of SME's experience. Larger companies can typically spread developments and risks and cover financial resources through their daily operations and balance sheets. For SMEs with limited financial means, this is a challenge. Furthermore, banks may view innovations too risky, and alternative funding sources may be limited due to financial liabilities of SMEs. Moreover, national funding instruments are often scattered and tend to focus on individual elements or specific stages rather than providing sustained financial support throughout the entire innovation development and adoption cycle. This fragmented approach hinders the seamless progression of innovations from conception to widespread implementation.

  In more concerning scenarios, the most promising innovations may be acquired by the third countries, leveraging them for their own advancement. This not only impedes the progress of innovation within the originating country of EU, but also potentially contributes to the technological and economic development of other nations e.g.: China, USA etc.

All projects selected for funding in the SecurIT project during the 1st and 2nd Open call underwent evaluation. 6 projects, involving 12 SMEs each, were selected as success stories.

The successes of the 6 presented projects spanned across several key milestones. These milestones include the establishment of new collaborations, successful entry into previously unexplored markets, effective recognition of new funding instruments, and the exploration of innovative business perspectives. Furthermore, it is important to take into account SMEs' ability to integrate into new ecosystems, and gain benefits from them.

In the light of this, we created evaluation factors that will assist us in determining whether a project qualifies as a success story that could be followed by other SMEs. Each project will be assessed based on these evaluation factors. Important to note, that presented evaluation factors are cumulative. Not every project achieves significant progress in each of the factor. Naturally, not every factor is relevant for specific project's situation. But generally, we consider, that the more evaluation factors are satisfied, more probable success one can expect.

Criteria 1: Recognition.

Recognition can manifest in various forms, including securing additional funding, receiving awards, and acquiring new contracts.

Guiding questions that aid in showcasing consortium's engagement beyond the SecureIT project:

- Has the consortium pursued any applications for EU and national funding instruments beyond SecureIT project?
- Has the project already obtained additional funding, whether through government grants, private investors, or other funding sources?

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

- Has the project entered service contracts with integrators/end-users?

Criteria 2: Established new collaborations and ventured into new markets.

By attracting new partnerships, the innovation can gain access to additional expertise, and ecosystems that could help in accelerating its developments.

Guiding questions that aid in showcasing consortium's engagements beyond the SecureIT project:

- Does the innovation attracted new stakeholders, partners and established new collaborations?
- Does the innovation expand into previously unexplored geographical areas or customer segments?
- What type of collaboration forms have been established? (e.g.: joint ventures, research partnerships, licensing agreements, distribution agreements, etc.)

Criteria 3: Innovation deployed in Operational Environment.

One of the most compelling criteria demonstrating the success of the project is the acceptance of the innovation and its deployment in end-user/integrator operational environment.

Guiding questions that aid in showcasing up-take of innovation by integrator/end-user beyond SecureIT project:

- Has the innovation been implemented in real-life operational environment?
- End-user testimonials or feedback showcasing the benefits of innovation on end user's operations can be provided.

All funded projects were reviewed under those criteria. Further we provide success stories of 12 SMEs. Some of them first met during match making events, des they succeed to illustrate the success.

3.2 Success cases

FusionSec

This innovation was designed to equip police patrols with the tools needed to be exceptionally well-prepared for managing incidents and achieving security goals during large public events.

FusionSec project has not only achieved significant results during its 12-month implementation but has also demonstrated growth beyond the initial scope of the Secure IT project. The project has successfully navigated challenges faced by many SMEs and demonstrated flexibility in responding to the needs of security market.

Criteria 1: Recognition.

FusionSec results became the foundation for a new proposal, drafted and presented in response to the HORIZON-CL3-2023-SSRI-01-02 call. The project, titled "LEAD-PRo Law Enforcement Assistance for Disaster Prediction and Recovery Optimization," was submitted on the 23rd of November 2023. The project is led by SME.

SMEs took the risk of investing in bidding for EU funding, which is new and complex area for them. This journey was made possible with strong support of SecureIT ecosystem, which played a crucial role in guiding and assisting SMEs throughout every stage of proposal development.

Criteria 2: Established new collaborations and ventured into new markets.

New collaborations*:* SecureIT has laid the foundation for new collaborations that extend beyond the boundaries of the SecureIT project. The FusionSec has raised significant interest from the Lithuanian, Latvian and Spanish LEAs. The formal partnership has been established with the commitment of 3 LEAs to participate in the new LEAD-Pro initiative. It was agreed to collaborate on advancing the platform, incorporating new functionalities to create a more tailored and effective solution. In addition, a new partnership has been established with CERTH (Greece RTO) and ISACA. These partnerships aim to provide essential services to streamline the productization of the solution, making it market ready.

New markets: SecureIT facilitated the establishment of FusionSec connections with organizations that could open new market opportunities for SMEs. One such organization was EACTDA, which supports EU LEA in innovation uptake activities. The negotiations with EACTDA are still in the progress. Furthermore, the FusionSec platform has great potential for use in other applications, such as effective public transport organization and rescue operations for missing people. Currently, the application is being tested by Klaipedos Sventes NGO, responsible for organizing the largest national events in Lithuania. The Lithuanian police intend to acquire the solution after the completion of the 12-month testing period.

Criteria 3: Innovation deployed in operational environment

Even though FusionSec is currently a prototype and not a finalized product, LT police decided to deploy this innovation into their operational environment for testing over the course of 12 months. LT police after the initial tested of solution, has shared testimonials, providing feedback on how the FusionSec platform has improved their operational procedures. Furthermore, during Kick-off meeting of OC- 2, LT police shared the results of real-life demonstrations and highlighted the benefits they experienced utilizing the solution.

PIT-SAT-M

PIT-SAT-M is an AI enabled web-based platform for monitoring of the stability of structures and nearby areas, using satellite data. The project was led by GeoKinesia (ES) that was responsible for the 2 solution pilots in Spain (Rules dam) and France (Amfreville bridge).

Criteria 1: Recognition.

Project partner GeoKinesia (ES) applied for additional funding and got selected under Horizon Europe CL4 following call: Copernicus downstream applications and the European Data Economy (HORIZON-EUSPA-2022-SPACE-02-54). The MOSMIN project is carried out by 12 partners from 6 countries. Its goal is to develop holistic, full-site services for the geotechnical and environmental monitoring as well as valorisation of mining-related deposits based on a combination of EO and in situ geophysical data. The mail objective is to improve the efficiency and reliability of monitoring, maximise resource utilisation and help mitigate environmental risks and the impact of mining operations.

Having been selected for additional funding is more a sign of recognition for GeoKinesia's expertise rather than a further development of the solution itself. The use of satellite data for ground monitoring will not be used there to assess the stability of structures but rather the environmental impact of mining operations.

Criteria 2: Established new collaborations and ventured into new markets.

GeoKinesia is becoming a leading monitoring service provider in Latin America and Mexico and intend to start promoting the platform, rather than traditional monitoring service upon the project completion.

Currently, apart from the traditionally target mining industry, they monitor a number of highways, trolleybus line and metro line under construction (surface) in Mexico City, Mexico, dams in Bolivia, a road in India. They also see a lot of potential in promoting early warning service and large areas monitoring, we are already in negotiations with several potential customers.

Throughout SecurIT GeoKinesia gained some visibility in Europe and succeeded in the organization of two demonstration with 2 different types of end users: Setec, a leading French geotechnical company and the local government of Andalusia (Spain).

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

BIM2SIM

BIM2SIM aims at developing a prototype digital technology brick to automatically extract security- and safety-related information from standard building description file formats.

Criteria 1: Recognition through securing further funding and receiving awards, new contracts.

The solution developed by APEX solution under BIM2SIM is to be used for simulation project funded by national funds in France (research agency and defence entity).

The success of the prototype project permits to go beyond and to use some bricks to go further. In that sense, SecurIT funding was crucial to the development and scalability of the solution.

Criteria 2: Established new collaborations and ventured into new markets.

The project brought the attention of other national stakeholders and funding agencies.

CyberSec2SME

The objective of the CyberSec2SME executed by the companies Lupasafe (NL) and Beia (RO) project was to give board members, the assurance they need on the information security of their organisation and their vendors in the supply chain. The assurance covered people, processes and the IT.

Critical Infrastructure are attractive targets for hostile entities. While many critical infrastructures have implemented cyber security technologies, the issue of cyber risks identification across employees, contractors and service providers remains a major concern, implying to require Contractors/Service Providers to prove that they also have implemented (expensive) cyber security systems.

The solution was successfully deployed at BEIA and Port of Galati endpoints, and risk data was collected from BEIA and Port of Galati employees for reporting and analysis. Tests were performed on employees, including cyber awareness, phishing, and dark web tests. Next the solution was tested by purposely introducing errors and vulnerabilities. The Lupasafe solution detected the vulnerabilities in time, and BeiA followed up on the findings. Multiple critical vulnerabilities were a result of outdated software and insecure configurations, emphasizing the importance of continuous monitoring and up–to–date security measures to reduce the risk of cyber-attacks.

Lupasafe also performed phishing tests. Spearphishing is a common method used by hackers to target critical infrastructure. Lupasafe performed phishing tests on the employees of BeiA, demonstrating the effectiveness of their cyber security measures.

Criteria 1: Recognition.

CyberSec2SME results and specifically the Lupasafe solution and Lupasafe as a Beneficiary became part of a new project under the CYBER-03 Digital Europe Program UPTAKE CYSSME. CYSSME (Cyber Security Maturity Improvement and Data Protection for Micro Enterprises, Small and Medium Enterprises started December 1st, 2023, for the next three years using the Lupasafe platform to further improve Cybersecurity of European MEs and SMEs. The CYSSME partners together with Lupasafe aim to provide a

Next to this, Lupasafe also participated in the Horizon Innovation Action call IA-HORIZON-CL3-2023-CS-01-01 aiming to further enhance the current solution. Together with partners with complementary technical solutions, the idea of the Innovation Action is to demonstrate this in different additional sectors (Industry) and showcase the security improvements and compliance of manufacturing devices and healthcare systems.

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

Together with the largest SME-association in Belgium, a joint proposal was prepared to target 1250 SMEs in their phishing campaign.

Lupasafe also gained various new customer successes, especially with communes in the Netherlands, auditors in Austria and some enterprise customers throughout Europe. More than 40 customers got signed up, next to some additional Managed Services Provides. Lupasafe was successful raising additional capital, in order to further grow its business.

Criteria 2: Established new collaborations and ventured into new markets.

Thanks to the SecurIT project, new collaborations were established amongst some of the SecurIT-partners, together with the SecurIT mentor and amongst other SecurIT participants. This led to the development of the joint European funding proposals and today the execution of the CYSSME-project together with SecurIT-partners LSEC and L3CE, and other participant co-dex.eu. Additional collaborations were set up with AST (Advanced Security Technologies) and the project Cybertrapper. Thanks to SecurIT, introductions were made into some European ports such as the Port of Antwerp and Rotterdam.

Beyond the communes and critical infrastructure Lupasafe was able to enter into the domain of SMEs, and is getting closer to retail, industry and healthcare markets as a result of the collaboration with SecurIT and the funded CYSSME.eu-project. Lupasafe is also capable of reaching further with its solution supporting auditors for NIS2-compliance, together with auditor-partners in the project.

Criteria 3: Innovation deployed in Operational Environment

The innovative development that was initiated within the Cybersec2SME-project were further operationalized beyond the demonstrator, into the market and are now being made commercially available for customers to use. Today’s Lupasafe solution includes both the analysis, the assessment and the operational dashboard showing an overview of part of the security standing and provides situational awareness to the company management.

Additional components and innovative insights are being added (for instance for further compliance under NIS2), also together with partners. These innovations will be deployed both with existing customers and will serve to target new customers.

RASAD

Belgian-based NoCode-X and French Wallix joined forces to create a platform for Rapid and Secure application development aimed specifically for the security domain. NoCode-X offers a platform allowing rapid application development without writing a single line of code. Wallix is European leader in Identity and Access Management and authentication technologies. The RASAD-project allowed organizations to easily digitize & automate any process with tremendous speed and a guaranteed level of cyber security.

In the end RASAD allowed NoCode-X to further become an innovative platform that empowers organizations to swiftly build secure applications without writing a single line of code. Thanks to RASAD, the NoCode-X development platform allowed traditional barriers of application development to reduce up to 90% reduction in time to market compared to conventional methods.

The solution was successfully deployed to seamlessly move and dispatch critical financial data, including CODA files and bank statements, from the SFTP server of the Bank of Belfius to various destinations within the intricate systems of the Municipality of Koksijde. Traditionally, such projects demanded extensive custom coding, time–consuming configurations, and meticulous maintenance. However, RASAD offered an alternative approach that transformed this process. The speed at which the financial data was moved and dispatched was unprecedented, resulting in significant time savings for both the Bank of Belfius and the Municipality of Koksijde. Moreover, the security of sensitive financial

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

data was upheld to the highest standards, thanks to RASAD's automatic data encryption & auditing features.

Criteria 1: Recognition.

Such a remarkable achievement has not gone unnoticed. Both the Bank of Belfius and the Municipality of Koksijde are now looking into the possibility of continuing their collaboration with RASAD. The effectiveness and efficiency brought about by RASAD have not only streamlined their operations but also laid the foundation for a potentially long–lasting partnership with the platform. In conclusion, the successful implementation of RASAD in this financial data integration project stands as a testament to the platform's transformative capabilities. It not only accelerated data movement but also fostered ongoing collaboration between three important institutions, ushering in a new era of efficiency and security in financial data management.

RASAD results and specifically the NoCode-X solution and NoCode-X as a Beneficiary became part of a new project under the CYBER-03 Digital Europe Program UPTAKE CYSSME. CYSSME (Cyber Security Maturity Improvement and Data Protection for Micro Enterprises, Small and Medium Enterprises started December 1st, 2023, for the next three years using the NoCode-X platform to further improve Cybersecurity of European MEs and SMEs. The CYSSME partners together with Lupasafe aim to provide a

Next to this, the NoCode-X platform is being used for different additional application re-engineering projects. These include online platforms data integration, swift forms building with multiple layers of access and control and development of online versions of different audit trails and forms; allowing to further expand the platform and technology. Thanks to the initialisation, the company was able to hire 2 FTEs, and is further looking to expand with an additional number of FTEs in 2024.

Criteria 2: Established new collaborations and ventured into new markets.

The RASAD project lead the interest in replicating the solution that originated from the demonstrator, into proposing as a package solution to other communes and organisations with similar challenges, in collaboration with the bank.

Thanks to the SecurIT project, new collaborations were established amongst some of the SecurIT-partners. This led to the development of the joint European funding proposals and today the execution of the CYSSME-project together with SecurIT-partners LSEC and L3CE, and other participant Lupasafe. Additional collaborations were set up with AST (Advanced Security Technologies) and the project Cybertrapper. Thanks to SecurIT, introductions were made into some Dutch Ministries and municipalities.

Beyond the communes, the financial services markets, NoCode-X is entering the domain of healthcare looking to facilitate the process of human imaging processing, as well as the transport sector – facilitating the compliance and process for international transport, energy market facilitating the process for delivery and processing of certificates for carbon and in high-tech. NoCode-X provided for partner LSEC, the platform for the Regional Invest activities of the SecurIT-project in collaboration with SecurIT partner L3CE. This will be maintained by LSEC beyond the SecurIT-project together with NoCode-X.

Criteria 3: Innovation deployed in Operational Environment.

The innovative developments that were developed within the RASAD-project were further operationalized beyond the demonstrator and are being used today by the commune and the bank in daily operations. Beyond, the platform is being used for different other applications and has been further improved by NoCode-X in newer versions to facilitate new requirements. These incremental changes facilitate new demands but are being used in operations by various customers. New developments are being investigated such as to use of AI, supporting further the NoCode development, by suggesting the

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

use of components or reuse of existing instruments. Also, for other services, searches and translations, this will be used by the platform to facilitate developments.

Additional components and innovative functionalities are being added, also together with partners. These innovation ns will be deployed both with existing customers and will serve to target new customers.

VASCREEN

Criteria 1**: Recognition**

After the funding of SecurIT, the two SMEs (MION / Spain and EZAKO / France) wished to explore further prototype development for their technology, which could be applicable to different market sectors.

They successfully applied to the cascade funding call for demonstration projects, launched by the Silicon Eurocluster project (Single Market Program).

Based on this funding (80 k€), they have launched the MAISOR project in October 2023. The goal of MAISOR is addressing the detection of fraudulent olive oil and it will develop a volatile analysis sensor based on a very innovative analytical instrument supported by Edge-AI implemented in a microelectronics system.

The application market is different than the security market (even though it deals with food security) but the developed technology, especially the microelectronics system with edge-AI is fully relevant to the VASCREEN goals.

The MAISOR project will run till June 2024.

Criteria 2: **Established new collaborations and ventured into new markets**

The relationship between MION and EZAKO came from a matchmaking event organised by the INNOSUP project Galatea.

SecureIT facilitated the establishment of relationships between the 2 SMEs MION and EZAKO, which then applied to the Silicon Eurocluster cascade funding, related to electronic development, and their new project MAISOR is addressing food security (but could also be relevant to agrifood, health, security).

Criteria 3: **Innovation deployed in Operational Environment**

VASCREEN is a prototype, and not yet a finalised and industrial product. Demonstration has been done in lab environment. And MION has approached transport companies such as DHL to present them their prototype.

3.3 Clustering practices

One of the tasks in the scope of T2.3 was to search for innovative ways to support SMEs in the security domain. Such examples of good practices could be found among clusters within SecurIT project as well as outside the project. This section describes some good practice examples that can be considered for extension to security and other domains.

It is important to note, that the SecurIT project also provided some examples of good practice. The two most relevant examples are funding tool, making users easy and understandable way to get information about relevant funding, and project clustering approach, that can be used further by clusters and included in other cascading funding initiatives.

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

The initial identification of practice to consider as good was made among the cluster organizations within the project. A detailed description of the clusters and services provided in previous section. As it is concluded in that part of the document, there were not any specific practice that proved to provide very good results among partners. Most of clusters provide common services, those can be considered as a good practice, but no innovative approach identified.

During the project implementation period there were numerous interactions with different initiatives and organizations. From all spectrum two models were selected to consider as good practice, that can be extended to other domains as well as more used by security domain.

Project clustering as innovation acceleration practice

Besides the tool for search of funding instruments, another methodology has been developed during the project implementation with the aim of accelerating innovation by actively involving a wide range of end-users who may have an interest in the innovation. This section is dedicated to the concept of "projects clustering approach" that was developed as the insight of the project.

While this initiative has not been explicitly addressed in any of the official deliverables, this document provides a comprehensive elaboration on it. Furthermore, in D.4.3 Sustainability and Exploitation Plan, there will be additional elaboration on how this concept can be leveraged as an exploitable outcome.

One of the project partners working in SecurIT project with end-user national police observed, that interests of the end-user were never limited to the specific project, tool, or solution. They tend to suggest that it is solving its specific need and was keen to be exposed to broader spectrum of ideas/technologies addressing their issues.

After several successful attempts to connect end-users, we find it a promising approach to expose end-user to the variety of projects addressing broader security issues, so that they could match their interests.

This approach would enable SMEs to interact with end-users from various domains and MS obtaining instant feedback on the relevance of their solutions. Simultaneously, end-users can benefit from exposure to a wider array of innovative technologies tailored to their specific areas of interest.

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 individual threats within the broader spectrum of security concerns. The missing components can often be found in other sectors, projects, or security domains.

The SecureIT project focuses on advancements in 3 Security Domains:

- Sensitive Infrastructure Protection
- Disaster Resilience
- Public Space Protection

Through two Open calls, 42 innovative projects have been selected, showcasing the most promising innovations developed by SMEs that address and resolve various security concerns within these specific domains.

However, despite the significant accomplishments of the SecureIT project, only a small number of security practitioners have actively participated in the demonstrations and offered feedback on the relevance and usability of the technology. Furthermore, majority of them has connections with SMEs and possesses prior collaborative experience exceptionally on the national level and specifically focused on innovations that target specific threats and security issues within their operational domain.

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

Following the demonstrations of Open Call 1 projects outcomes, we observed that certain innovations received exceptionally positive feedback from practitioners. As a result, these innovations have the potential to offer significant benefits in practical applications for much broader audience of practitioners on EU and regional levels.

Moreover, through the clustering of projects, a synergistic effect can be achieved. This approach showcases how the results achieved by each project can complement one another, and how multiple innovations can collectively address various aspects of societal security challenges.

A few advantages can be outlined:

- **Broader engagement of security practitioners:** By organizing demonstrations, workshops, or webinars that the clustered projects can serve as a platform to engage a wider audience and of security practitioners. These events provide an opportunity for in-depth discussions, knowledge exchange, and feedback sessions, encouraging practitioners to actively participate and explore the applicability of innovations in their specific contexts.
- **A valuable feedback loop for technology providers:** The clustering approach is beneficial for technology providers, offering them the opportunity to be engaged in co-creation processes with diverse end-users. This engagement ensures a continuous flow of invaluable feedback, allowing providers to have a deeper insight into end-users operational processes while practitioners can benefit from well-tailored solutions.
- **Exploring new avenues for SMEs:** This approach initiates new collaborations that could provide access to new knolwdge, funding instruments, markets, new clients that SMEs might not have had on their own.
- **Faster Adoption and Implementation:** Receiving positive feedback on the suitability of innovation from various practitioners across multiple MS can promote its adoption and implementation. Awareness that certain practitioners have already successfully implemented these innovations could trigger a snowball effect, encouraging others to also consider adopting them.
- **Learning from Failures:** Not all innovations may succeed equally. Clustering projects allows for shared learning from both successes and failures. Consortiums can analyse and learn from each other's experiences, refining their approaches and avoiding pitfalls.

In summary, employing a project clustering approach, coupled with the demonstrations and effective communication, can significantly contribute to broadening the scope and geography of innovation and increasing numbers of end-users benefiting from them.

The approach was described in practical steps of implementation.

1. Discussing and naming the end-user centric areas. This exercise has to be very practical, taking into account real problems that our existing end-users are solving, and thematic subjects, technologies which SecurIT projects are working on.
2. Clustering/grouping SecurIT projects around end-user centric areas.
3. Assigning follow up manager who will be responsible for the cluster event and process facilitation activities.
4. Organizing separate events for every identified cluster with relevant end-users. Coordinate the synchronization of demonstrations across projects. Arrange presentations tailored for security practitioners.
5. Actively involve security practitioners in participation and collect feedback. Verify the relevance of demonstrations for end-users by discussing use case scenarios with domain practitioners.
6. Organize follow-up sessions to delineate the next steps for new projects.
7. Engage different stakeholders who have an interest in security innovations development and uptake.

The initial clustering was made in SecurIT project.

Various innovations in the domain of Public Space Protection may centre on different aspects of security, including crowd control, surveillance, communication, or emergency response. Grouping these projects together through clustering we can establish a comprehensive security ecosystem that effectively tackles multiple facets of public event security. 7 projects from the Open call 2 were clustered to this domain:

- Safe Festivals
- AIR-T4S
- CMD BOX
- AI-Disaster Emergency Com Communication
- ERRATA
- RESPO Communication
- Serval Management

First responders from Lithuania, France, municipalities, and private entities involved in organizing public events have shown significant interest in participating in demonstrations of the project's outcomes. This demonstrates that certain tools or solutions could be integral components of broader solutions, yet they all share the common goal of ensuring the security of public spaces.

Concentrating on safeguarding critical infrastructure protection, Open Call 2 projects have been positioned to address the specific needs of CI operators. Notably, these solutions encompass innovations such as advanced threat analysis methods and AI-based technologies. Grouping the projects, we highlight the flexibility of these advancements to provide advantages to different critical infrastructure (CI) operators, such as those in water supply, distribution system operators (DSO), and more. 4 projects from the Open call 2 were clustered to this domain:

- DISGRID
- RS2DG
- EV-Safe
- Flowguard

Lithuanian electricity distribution grid already expressed the interest to participate in demonstrations.

SecurIT cluster ecosystem

The structure of SecurIT project consortium is based on clusters. Just for remainder there are 8 different entities in the project providing different services for their members.

In addition to this SecurIT partners succeeded in the contractualization of 20 Ambassador Clusters since the beginning of the project. The list includes clusters from Romania, Ireland, UK, Poland, Luxembourg, Italy, Estonia, Spain, Germany, Belgum, Sweden, Finland, Portugal, Lithuania, Latvia, and Bulgaria. More details on ambassador clusters provided in Annex 3.

The main purpose of the action with ambassador cluster was to increase the outreach of the project dissemination activities in other European regions and to attract SMEs from countries where there is no SecurIT partner.

Ambassador Clusters have also been contributing to the Task 2.3 by providing inputs on local funding opportunities that were not identified by SecurIT partners, because not being available in their regions or countries. Identification of some innovative mechanisms to support SMEs was also made among them. Overall contributions from Ambassador Clusters were limited but helpful in the building of the “Regional Invest” platform (see below).

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

With the aim to identify some innovative ways to support SMEs SecurIT project clusters were asked to identify services they provide also adding some other than traditional services.

	Services \ Clusters	L3CE	SAFE	LSEC	Pole SCS	HSD	Systematic	CenSec	FundingBox
Test before invest	Prototyping							Y	
	Fostering the integration, adaptation of various technologies		Y		Y		Y		
	Concept validation	Y	Y		Y		Y	Y	
	Testing and experimentation with digital technologies (SW)	Y							
	Demonstration activities	Y	Y				Y	Y	
	Knowledge and technology transfer	Y			Y	Y		Y	
Ecosystem and Networking Services	Networking	Y	Y		Y	Y	Y	Y	
	Incubator/accelerator support				Y			Y	
	Voice of the customers						Y	Y	
	Visioning and strategy development	Y	Y		Y		Y	Y	
	Awareness creation	Y			Y	Y	Y	Y	
	Technology road mapping	Y	Y		Y	Y		Y	
	Consolidation for dissemination / demonstrations				Y			Y	
Funding Support	Access to funding	Y	Y		Y	Y	Y	Y	
	Investor's support				Y		Y		
	Support in consortia building and application development	Y	Y		Y	Y	Y	Y	
Training & Skills	Short-term advanced training courses (e.g.: digital skills, specific technologies, etc.)	Y	Y				Y		
	Short-term soft skills training courses	Y							
	Mentoring	Y			Y		Y	Y	
	Hosting of training, events	Y	Y		Y	Y	Y	Y	

Table 1. Service structure of SecurIT project clusters.

The table provides a clear description of services provided by SecurIT project clusters. It can be seen that they are focused on rather traditional ones: networking, access to funding, hosting of different events. All the services in the table are relevant for SME's and support their development, but none of new, innovative services were identified during the analysis. Similar no innovative mechanisms were identified within ambassador cluster.

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

European Anti-Cybercrime Technology Development Association- EACTDA

The aim of EACTDA is development of technology solutions for EU LEA to use them in their fight against crime.

It is important to note that most innovations in security technology are typically developed through EU research funding mechanisms such as FP7, Horizon 2020, and Horizon Europe. Nonetheless, the maturity of these solutions often falls short of meeting the requirements for operational deployment in the existing ecosystems of end-user organizations.

It is worth noting, that most of EU research projects conclude with exploitation plans that outline clearly defined strategies for implementing and leveraging technology by end-user organizations. However, these plans often lack detailed explanations regarding who will assume responsibility for the final stages of implementation, known as the "last mile" activities.

The absence of a responsible entity capable of assuming leadership and offering comprehensive support to end-user organizations has led to only a small portion of innovations reaching their intended recipients.

In response to these challenges EC has endorsed the establishment of organization that brings together various stakeholders, including academia, industry, and EU law enforcement agencies to collaborate towards a common objective of expanding the deployment of innovations in the operational processes of European public security organizations.

The EC tasked EACTDA to establish a long-term and sustainable ecosystem that consistently provides innovative tools ready for operational use by European public security practitioners, primarily for digital investigations.

Following the priorities set by EUROPOL and End-User Advisory Board, EACTDA oversees EU research projects to identify the most promising and sufficiently mature innovations. Furthermore, EACTDA offers a range of supplementing services and funding instruments aimed at facilitating the transition of innovations from the research laboratory to operational deployment.

Innovation up-take requires specific local knowledge and attention, thus EACTDA developed a concept of National Node that plays a leading role in driving the adoption of innovation at national level. To conclude, today EACTDA is a strong player within the EU innovations ecosystem.

On the one hand it contributes to bolstering the digital forensic capabilities of EU LEA and on the other hand it actively collaborates with industry and academia to champion the innovations in cybercrime domain.

Two security domains, namely Disaster Resilience and Public Space Protection of SecureIT, are of significant interest to EU LEAs. Innovations aimed at tackling the challenges within these domains could potentially ranked among the top priorities for the End- User Advisory Board of EACTDA.

Moreover, there exist numerous synergies between EACTDA and SecureIT projects. While SecureIT projects finalizes its activities with real-life demonstrations for end-user organizations, EACTDA is particularly interested in the subsequent stages of innovation maturation and adoption by all EU MS LEAs.

This implies that if an innovation is recognized by EACTDA, it can assume a mentorship role and utilize new funding instruments to finalize the product and conduct demonstrations for a large audience of EU LEAs. This process not only aids in refining the innovation but also facilitates its widespread adoption and implementation within the EU security landscape.

The next steps to establish better links and to test possibilities is inviting the EACTDA team to participate in real-life demonstrations of the innovations developed by the projects and collaborate on the development of a roadmap for selected innovations.

Defence Innovation Acceleration for the North Atlantic-DIANA

It is noteworthy that many innovations developed with a specific focus on civil security, possess significant potential for addressing various challenges faced by defence sector. To accelerate the innovations with potential dual-use applications, NATO has initiated the program known as DIANA.

This program is designed to cultivate the advancement of the next generation of dual-use, deep tech solutions, along with the startups dedicated to their development.

The program is focused on the disruptive technologies in the field of big data, artificial intelligence (AI), autonomy, quantum, biotechnologies and human enhancement, energy and propulsion, novel materials and advanced manufacturing and space – specifically where they are dual-use (civilian and defence) and deep tech in nature.

Similar to EACTDA, DIANA seeks to establish a robust connection with innovators, investors, and industry partners. This aims to create an effective ecosystem that not only supports, but also nurtures the development and adoption of innovations by relevant stakeholders.

To accelerate the progress of innovations DIANA offers well-tailored benefits that align with the specific needs, interests, and contributions of targeted stakeholders:

- **Innovators:** DIANA provides innovators with funding to advance technology development, facilitates access to test and evaluation resources, and offers curated exposure to investors and end users.
- **Investors:** DIANA advice investments in companies addressing program challenges and engaging in DIANA's accelerator program. Showcasing that technologies emerging from accelerator hold promising market opportunities.
- **Industry partners:** DIANA is actively seeking established companies to become part of industrial partnership network. Collaboration with high-performing companies across defence and non-defence sectors, offering opportunities for mentoring, joint events, and other forms of support within DIANA's innovation ecosystem.

Considering the challenges elaborated in the outlined in previous sections, the DIANA program can play a significant role in supporting SMEs to overcome most of them by providing:

- Grants to support technology development and demonstration, and participation in the DIANA accelerator programme.
- 10+ accelerators across the Alliance, with more planned over the coming years.
- 90+ test centres (with more planned) across the Alliance where entrepreneurs can de-risk and demonstrate and validate their proposed dual-use technological solutions.
- Mentoring from scientists, engineers, industry partners, end users, and government procurement experts.
- An investor network associated with the Allied Capital Community for trusted third-party funding.
- Opportunities to demonstrate technology in operational environments.
- Pathways to market within the NATO enterprise and 31 Allied markets.

SecurIT project organised a several meetings with DIANA program coordinators to investigate additional opportunities and paths for leveraging innovations within SecurIT ecosystem. However, further in-depth

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

discussions are required to explore how the ecosystems of EACTDA, DIANA, and SecurIT can collaborate effectively in this regard.

Two examples of relevant good practice are expected to be further explored in the deliverable on exploitation.

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

4. Conclusions

4.1 Lessons learnt

While performing activities in related to support funded projects, some challenges were faced, and some lessons were learnt. Those are shared in this section. Most of them are related to the development of tool for funding instruments, others are broader and concentrate on providing general support for

SME's growth issues.

As funding instruments searching tool is considered as one of the potentially sustainable tools, that can be taken over and developed further, there are some experiences to be shared:

- In most cases funding instruments are described by programmes and calls. Calls are usually very circumstantial, while programmes are general. It is easier to include programmes in the tool, as they are long term and cover wide range of features. But those are of a limited relevance to SME's. The same can be said about the strategic documents. Both are too complex and are not providing relevant condensed information for solution providers. Further development and application of the tool should be focused and limited to calls.
- Variety of calls to be included in the search database is much wider than directly connected to the domain, security in our case. Calls might be domain agnostic and might be not even related to technological developments. Application of some of security related innovative solutions goes beyond the sector and can be used in other domains. This makes selection and inclusion of calls much wider and complex.
- Maintenance of the tools is very critical as calls have limited duration. Keeping tool updated and securing that due date calls are automatically removed is an important functionality.
- Possibilities to include national funding instruments was limited to the countries represented in project. Funded project overed much wider landscape of EU. In some cases, funded projects have been able to search only for international instruments, as national or regional ones were not included in the database. Such tool can provide much bigger value of wide range of security related funding instruments are included in the database.
- The breakthrough in mapping exercise was made by introduction of the features. Applied taxonomy allowed to unify SME's perspective with language used in the programmes or calls description. Such approach can help in developing any similar tools in security or other domains. It also is technology agnostic, so despite the technological realization this can help.
- The current availability of similar tools is very limited (at least during the project implementation not of such was identified) and they are needed. Most of clusters and similar eco-systems support members with funding advises, but this is time consuming and occasional service. We can see the clear opportunity, at least in cybersecurity domain, to scale the tool with the help of NCP's. Even being cybersecurity centred, it can be valuable for other security domains as well.

Looking from the broader perspective might be said that different eco-systems provide SMEs with established services. While more simple tools and facilitation, consolidation of efforts are more needed.

It was also learnt in the project, that identification of any significant innovative ways to support SME's id challenging, as most of mechanisms are project based, lack continuity, not cover most challenging stages of solutions development and are single SME oriented.

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

4.2 Concluding remarks

The deliverable thus can be concluded with the following:

- Selected projects were well mentored during the project and were supported in different ways. This support resulted in some successful progressions that are described as Success stories.
- Linking projects to the funding instruments resulted in sustainable instrument, prepared knowledge base can be developed further and used beyond the project lifetime.
- There are several observations provided, that allow this or any other similar tool to be deployed.
- Identification of innovative instruments to support SMEs was less fruitful, two examples as EU wide initiatives are provided that can be considered as relevant to security domain.
- Large security clusters and ecosystems are not always equipped to provide SMEs with the necessary support in accelerating innovations The experiences of specialized organizations like EACTDA and DIANA provide as practical examples of how-to successfully bring innovation to end-user overcoming challenges such as lack of trust, long-term references. and sufficient funding.

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

Annex 1

Complete list of features

Techniques	T1	AI (ML)
	T2	Blockchain
	T3	Cryptography
	T4	Visualisation (WAR)
	T5	Laser (LIDAR)
	T6	Robotics & kinematics
	T7	SLAM
	T8	CBRN detection
	T9	Software development
	T10	IoT
	T11	Biometry
	T12	Quantum Technologies
	T13	UAVs, Drones
	T14	Sensors
	T15	Big Data

Process	P1	Forecast/Foresight
	P2	Planning
	P3	Detection
	P4	Inspection (remote)
	P5	Response decisions / risk mitigation
	P6	Incident handling
	P7	Data collection
	P8	Multi source integration
	P9	Data storing
	P10	Info / data sharing
	P11	Cascading effects
	P12	Cybersecurity
	P13	Forensic
	P14	Access control
	P15	Impact monitoring
	P16	Post-analysis
	P17	Analytical support

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

	P18	Statistics and Reporting

Development support	D1	Experimental deployment
	D2	Prototype
	D3	Productization
	D4	Tools and technologies adoption to the concreate market needs, integration
	D5	Large scale exercising
	D6	Hackathons, Ranges, Simulations
	D7	Tools functional, operational, end-user testing

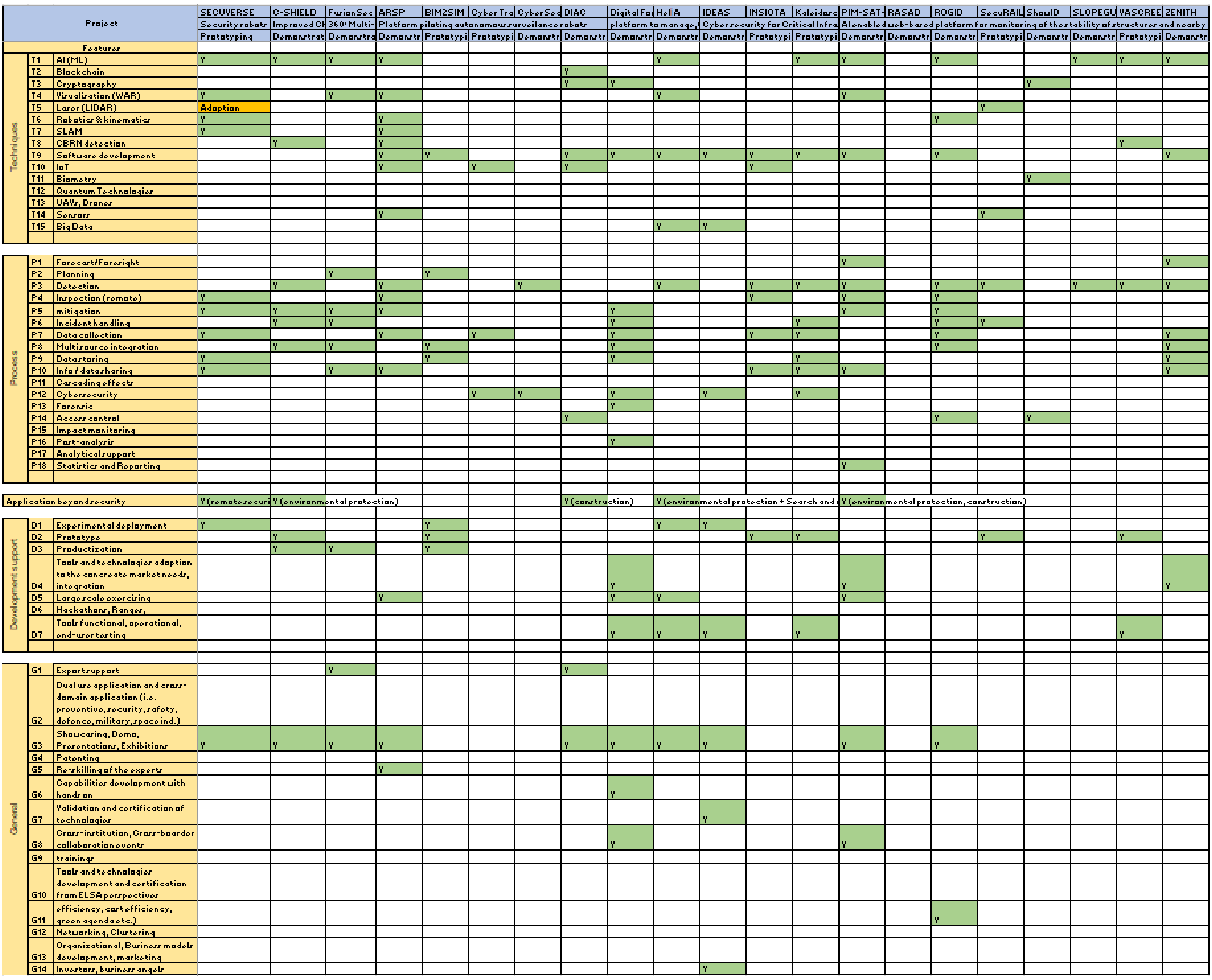
General	G1	Export support
	G2	Dual use application and cross-domain application (i.e. preventive, security, safety, defence, military, space ind.)
	G3	Showcasing, Demo, Presentations, Exhibitions
	G4	Patenting
	G5	Re-skilling of the experts
	G6	Capabilities development with hands on
	G7	Validation and certification of technologies
	G8	Cross-institution, Cross-border collaboration events
	G9	Education programmes and trainings
	G10	Tools and technologies development and certification from ELSA perspectives
	G11	Tools efficiency (energy efficiency, cost efficiency, green agenda etc.)
	G12	Networking, Clustering
	G13	Organizational, Business models development, marketing
	G14	Investors, business angels

Complete list of features.

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

Annex 2

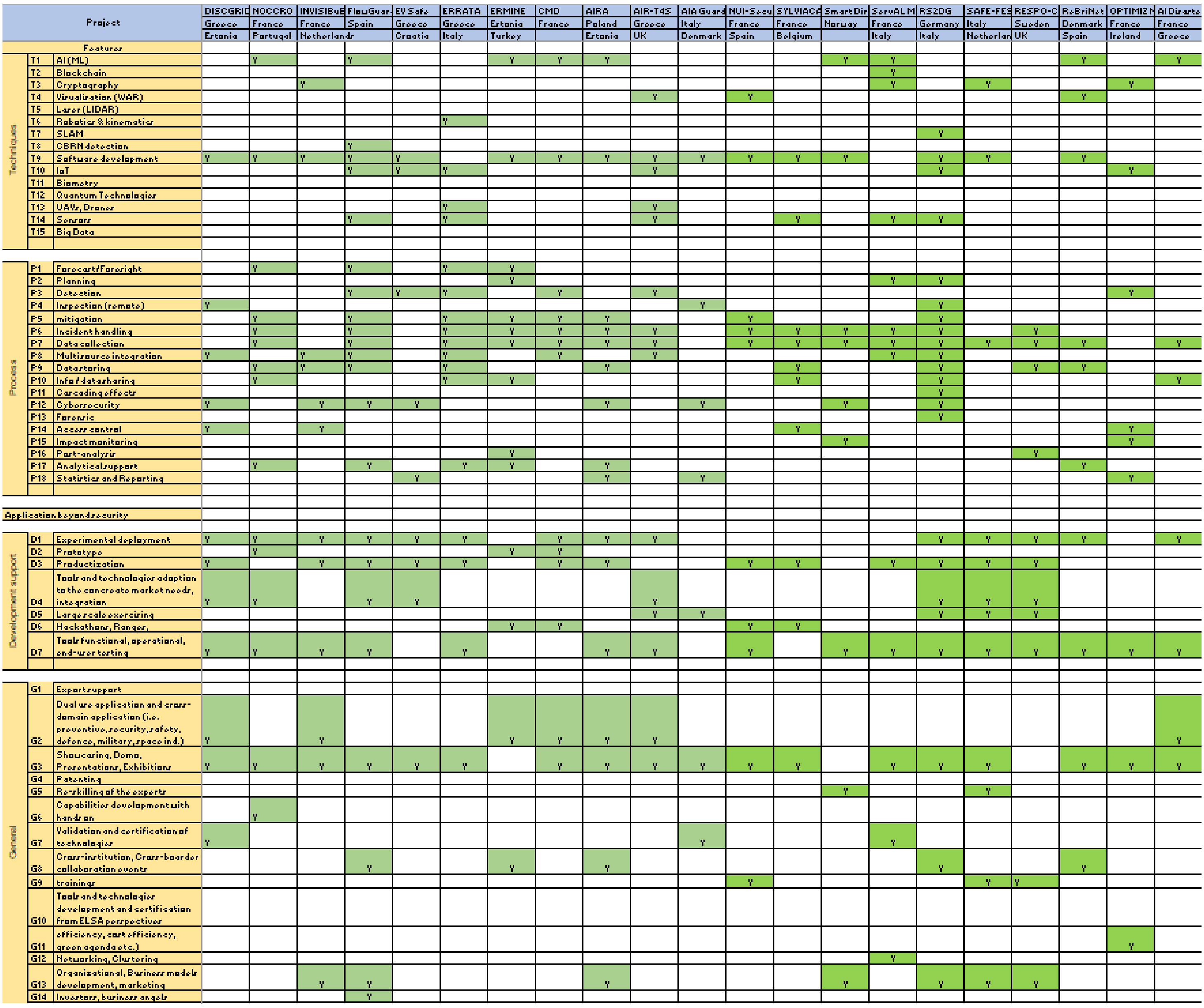
Full map of funded projects breakdown of features. Open call 1.



Project			SECUVERSE	C-SHIELD	FusionSec	ARSP	BIM2SIM	Cyber Tra	CyberSec	DIAC	Digital Fa	HoliA	IDEAS	INSIOTA	Kaleidosc	PIM-SAT-	RASAD	ROGID	SecuRAIL	ShouID	SLOPEGU	VASCREE	ZENITH
			Security robots	Improved Ch	360° Multi-	Platform piloting autonomous surveilance robots					platform to manage,		Cybersecurity for Critical Infra			AI enabled web-based platform for monitoring of the stability of structures and nearby							
			Prototyping	Demonstrat	Demonstra	Demonstr	Prototypi	Prototypi	Demonstr	Demonstr	Demonstr	Demonstr	Demonstr	Prototypi	Prototypi	Demonstr	Demonstr	Demonstr	Prototypi	Demonstr	Demonstr	Prototypi	Demonstr
Features																							
Techniques	T1	AI (ML)	Y	Y	Y	Y						Y			Y	Y		Y			Y	Y	Y
	T2	Blockchain								Y													
	T3	Cryptography								Y	Y									Y			
	T4	Virualization (WAR)	Y		Y	Y						Y				Y							
	T5	Laser (LIDAR)	Adaption																Y				
	T6	Robotics & kinematics	Y			Y												Y					
	T7	SLAM	Y			Y																	
	T8	CBRN detection		Y		Y																Y	
	T9	Software development				Y	Y			Y	Y	Y	Y	Y	Y	Y		Y					Y
	T10	IoT				Y		Y		Y				Y									
	T11	Biometry																		Y			
	T12	Quantum Technologies																					
	T13	UAVs, Drones																					
	T14	Sensors				Y													Y				
	T15	Big Data										Y	Y										
Process	P1	Forecast/Foresight														Y							Y
	P2	Planning			Y		Y																
	P3	Detection		Y		Y			Y			Y		Y	Y	Y		Y	Y		Y	Y	Y
	P4	Inspection (remote)	Y			Y								Y		Y		Y					
	P5	mitigation	Y	Y	Y	Y					Y					Y		Y					
	P6	Incident handling		Y	Y						Y				Y			Y	Y				
	P7	Data collection	Y			Y		Y			Y			Y	Y			Y					Y
	P8	Multisource integration		Y	Y		Y				Y							Y					Y
	P9	Datastoring	Y				Y				Y				Y								Y
	P10	Info / datasharing	Y		Y	Y								Y	Y	Y							Y
	P11	Cascading effects																					
	P12	Cybersecurity						Y	Y		Y		Y		Y								
	P13	Forensic									Y												
	P14	Access control								Y								Y		Y			
	P15	Impact monitoring																					
	P16	Post-analysis									Y												
	P17	Analytical support																					
	P18	Statistics and Reporting														Y							
Application beyond security			Y (remote securi	Y (environmental protection)						Y (construction)		Y (environmental protection + Search and r				Y (environmental protection, construction)							
Development support	D1	Experimental deployment	Y				Y					Y	Y										
	D2	Prototype		Y			Y							Y	Y				Y			Y	
	D3	Productization		Y	Y		Y																
	D4	Tools and technologies adaption to the concreate market needs, integration									Y					Y							Y
	D5	Large scale exercising				Y					Y	Y				Y							
	D6	Hackathons, Ranges,																					
	D7	Tools functional, operational, end-user testing									Y	Y	Y		Y							Y	
General	G1	Expert support			Y					Y													
	G2	Dual use application and cross-domain application (i.e. preventive, security, safety, defence, military, space ind.)																					
	G3	Showcasing, Demo, Presentations, Exhibitions	Y	Y	Y	Y				Y	Y	Y	Y			Y		Y					
	G4	Patenting																					
	G5	Re-skilling of the experts				Y																	
	G6	Capabilities development with hands on									Y												
	G7	Validation and certification of technologies											Y										
	G8	Cross-institution, Cross-boarder collaboration events									Y					Y							
	G9	trainings																					
	G10	Tools and technologies development and certification from ELSA perspectives																					
	G11	efficiency, cost efficiency, green agenda etc.)																Y					
	G12	Networking, Clustering																					
	G13	Organizational, Business models development, marketing																					
	G14	Investors, business angels											Y										

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

Full map of funded projects breakdown of features. Open call 2.



		Project	DISCGRID	NOCCRO	INVISIBuE	FlowGuar-	EV Safe	ERRATA	ERMINE	CMD	AIRA	AIR-T4S	AIA Guard	NUI-Secu	SYLVIACA	Smart Dir	ServAL M	RS2DG	SAFE-FES	RESPO-C	ReBriNet	OPTIMIZ N	AI Disaste
			Greece	France	France	Spain	Greece	Greece	Estonia	France	Poland	Greece	Italy	France	France	Norway	France	Germany	Italy	Sweden	Denmark	France	France
			Estonia	Portugal	Netherlands		Croatia	Italy	Turkey		Estonia	UK	Denmark	Spain	Belgium		Italy	Italy	Netherlan	UK	Spain	Ireland	Greece
		Features																					
Techniques	T1	AI (ML)		Y		Y			Y	Y	Y					Y	Y				Y		Y
	T2	Blockchain															Y						
	T3	Cryptography			Y												Y		Y			Y	
	T4	Visualisation (VAR)										Y		Y							Y		
	T5	Laser (LIDAR)																					
	T6	Robotics & kinematics						Y															
	T7	SLAM																Y					
	T8	CBRN detection				Y																	
	T9	Software development	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y		
	T10	IoT				Y	Y	Y				Y						Y				Y	
	T11	Biometry																					
	T12	Quantum Technologies																					
	T13	UAVs, Drones						Y				Y											
	T14	Sensors				Y		Y				Y			Y		Y	Y					
	T15	Big Data																					
Process	P1	Forecast/Foresight		Y		Y		Y	Y														
	P2	Planning							Y								Y	Y					
	P3	Detection				Y	Y	Y		Y		Y										Y	
	P4	Inspection (remote)	Y										Y					Y					
	P5	mitigation		Y		Y		Y	Y	Y	Y			Y				Y					
	P6	Incident handling		Y		Y		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y		Y			
	P7	Data collection		Y		Y		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y		Y
	P8	Multisource integration	Y		Y	Y		Y		Y		Y					Y	Y					
	P9	Datastoring		Y	Y	Y		Y			Y				Y			Y		Y	Y		
	P10	Info/ datasharing		Y				Y	Y						Y			Y					Y
	P11	Cascading effects																Y					
	P12	Cybersecurity	Y		Y	Y	Y				Y		Y			Y		Y					
	P13	Forensic																Y					
	P14	Access control	Y		Y										Y							Y	
	P15	Impact monitoring														Y						Y	
	P16	Post-analysis							Y											Y			
	P17	Analytical support		Y		Y		Y	Y		Y										Y		
	P18	Statistics and Reporting					Y				Y		Y									Y	
Application beyond security																							
Development support	D1	Experimental deployment	Y	Y	Y	Y	Y	Y		Y	Y	Y						Y	Y	Y	Y		Y
	D2	Prototype		Y					Y	Y													
	D3	Productization	Y		Y	Y	Y	Y		Y	Y			Y	Y		Y	Y	Y	Y			
	D4	Tools and technologies adaption to the concreate market needs, integration	Y	Y		Y	Y					Y						Y	Y	Y			
	D5	Large scale exercising										Y	Y					Y	Y	Y			
	D6	Hackathons, Ranges,							Y	Y				Y	Y								
	D7	Tools functional, operational, end-user testing	Y	Y	Y	Y		Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y
General	G1	Export support																					
	G2	Dual use application and cross-domain application (i.e. preventive, security, safety, defence, military, space ind.)	Y		Y				Y	Y	Y	Y											Y
	G3	Showcasing, Demo, Presentations, Exhibitions	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y	Y
	G4	Patenting																					
	G5	Re-skilling of the experts														Y			Y				
	G6	Capabilities development with hands on		Y																			
	G7	Validation and certification of technologies	Y										Y				Y						
	G8	Cross-institution, Cross-boarder collaboration events				Y			Y		Y							Y			Y		
	G9	trainings												Y					Y	Y			
	G10	Tools and technologies development and certification from ELSA perspectives																					
	G11	efficiency, cost efficiency, green agenda etc.)																				Y	
	G12	Networking, Clustering															Y						
	G13	Organizational, Business models development, marketing			Y	Y					Y					Y		Y	Y	Y			
	G14	Investors, business angels				Y																	

Annex 3

Detail information on ambassador clusters.

Name	Localisation	Number of SME members	Domains	Website	Short description
Cluj IT cluster	Cluj-Napoca, Romania	70	ICT	https://www.clujit.ro	Cluj IT Cluster is an innovative cluster association founded in October 2012 in Cluj-Napoca. The cluster includes over 90 members, IT companies, 14 universities, 2 institutes of the Romanian Academy, other research-development-innovation institutes, institutions from the public administration sector and support communities, creating a community which aims to increase the competitiveness of the IT sector, the visibility of the Romanian IT industry, as well as positioning Cluj as a digital innovation hub. Cluj IT fully supports digital transformation of processes in the relationship between the various sectors and the achievement of interoperability between systems at national and European levels.
Cyber Ireland	Ireland	80	Cyber	https://cyberireland.ie/	Cyber Ireland is the national cyber security cluster organisation of Ireland. It is an Industry-led body, built on cluster development best practice, with the support of academia and government, focused on addressing the needs and challenges of the cyber security sector in Ireland.
Cyber Wales	UK	400	Cybersecurity products and solutions	www.cyberwales.net	CyberWales is a representative body with the aim of being the Heart and the Voice of the cyber-Communities in Wales. CyberWales is a registered CIC and the Management Team, the Cluster Managers and the Steering Committee all strive to provide a platform for Members to find guidance, share news, ideas and best practice, to encourage collaboration through Clusters, events and competitions and to identify Opportunities for the cyber-Communities in Wales to thrive and grow.

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

CyberMadeIn Poland	Poland	40	Cyber	https://cybermadeinpoland.pl/en/home-page	The #CyberMadeInPoland cluster was created as a platform for cooperation and promotion of the Polish cybersecurity industry. Its purpose is to shape and develop safe cyberspace in Poland and to promote Polish companies abroad. The cluster also aims to stimulate the cooperation of the sector with scientific institutions, public administration entities, international corporations, industry and trade chambers, and other partners.
Cybersecurity Luxembourg	Luxembourg	79	Cybersecurity	https://www.cybersecurity-luxembourg.com/	The promotion of the Luxembourg cybersecurity ecosystem is made through the national brand "CYBERSECURITY Luxembourg", an integral part of the toolbox intended to enhance and strut promotion of Luxembourg in the field of cybersecurity. Cybersecurity is a key component in the efforts to promote all aspects of the digital transformation and develop its data-driven economy. Th initiative is part of the national cybersecurity strategy, The market mapping gathers all 300+ entities (public and civil sectors) involved in cybersecurity.
DITECFER	Italy	100	Railway technologies	https://www.ditecfer.eu/en/	DITECFER Cluster is the leading railway cluster in Italy. It is a technology-driven cluster, and its focus is on research and innovation, internationalisation, promotion of training for the members and education courses on the Tuscan territory for young talents. DITECFER is very active in EU-funded projects, where it has been coordinating four, so far, for helping SME members in addressing key challenges following new approaches and methodologies (e.g. in internationalisation, in adoption of advanced technologies, etc.).
Estonian Defence Industry Association	Estonia	16	Defence & security	https://defence.ee/	Defence Estonia Cluster is a network for international cooperation and export to enhance the cooperation between Estonian companies, R&D institutions and clients (triple helix). Cluster and its members participate in international projects and programs to increase export capability and sales of the Estonian companies on the defence and security markets.

GAIA	Basque Country, Spain	306	Engineering, Electronics, Computing, Telecommunications and Gamification.	https://www.gaia.es/	GAIA is the Association of Applied Knowledge and Technology Industries in the Basque Country and brings together over 306 companies in this sector. Its objective is to be a benchmark in Collaborative Innovation for the creation and implementation of globally competitive solutions based on own Knowledge and Technology.
Hamburg Aviation	Germany	210	Logistics, aviation & renewable energy	https://www.hamburg-aviation.de/en/windrove-pioneering-urban-air.html	The players in Hamburg Aviation form a powerful alliance of business, science and politics. Their goals: to network the companies, organisations and institutions of Hamburg Aviation, to promote the development of specialist personnel, to expand knowledge transfer, and to improve the commercial and economic environment. A further aim is to identify and fill gaps in the process chain, to produce innovations and to open up new areas of competency. The Windrove Network promotes the commercial use of drones in the Hamburg metropolitan region. Since 2017, Windrove has been bringing together users, designers, and suppliers of drone-based services and products. Open, solution-driven networking promotes the further development and the safe and fair deployment of commercial UAV applications across a variety of industries and uses, including security applications.
Infopole	Belgium	130	ICT, Big Data, Cyber	https://clusters.wallonie.be/infopole/en	INFOPOLE is the network of digital players that brings together digital ecosystems in order to promote business and innovation through partnership. Creator of opportunities, stimulator of cross-sector innovation, the cluster acts as a major transversal player in the Digital Wallonia digital strategy.
Mobile Heights	Lund, Sweden	86	Digital health, digital society, digital manufacturing & materials	http://www.mobileheights.org/	Mobile Heights is a non-profit ICT cluster organisation and networking community promoting innovation and growth in the digital world by connecting business, academia and society. Mobile Heights was founded in 2009 by Sony, Ericsson, Telia Company, the Regional Council of Skåne, Lund University and Malmö University. Mobile Heights has its headquarters in Lund, Sweden and is a Gold Label Cluster.

Tampere Safety and Security cluster	Tampere, Finland	230	National Security and Defence Industry	https://businesstampere.com/business-environment/business-ecosystems/tampere-region-safety-and-security-ecosystem/tampere-region-safety-and-security-cluster/	Finland is among the top countries for its safety in the world and it tops multitude of statistics year after year. Tampere region represents diverse set of competences provided by different actors. Companies, voluntary organizations, research institutes and authorities work together for safety and security. There are more than 250 organisations related to safety and security in the region Organizations with national level responsibilities such as Police University College, National Technical Research Centre VTT, Finnish Safety and Chemicals Agency Tukes and Finnish Defence Forces. Universities cater for needs of diverse set of industries and sectors providing good availability of competent workforce and opportunities for R&D collaboration. Tampere Region Safety and Security Cluster has been in operation since 2011 - provides easy access to local ecosystem.
TICE.PT	Centre, Portugal	32	ICT& Electronics	https://www.tice.pt/en	The TICE.PT aims to promote and leverage networking strategies for the sector. Network between companies and R&D centres, to induce a renewal active in national economic context, producing positive effects on national offering, enhanced by innovation and knowledge, creating export capacity and added value in domestic products.
AERTIC Agrupación Empresarial Innovacora del sector TIC de La Rioja	Logrono, Spain	104	ICT	www.aertic.es	The Cluster of the Information and Communications Technology Sector of La Rioja began its activity in July 2010 as an instrument to channel the interests and needs of a broad technological sector linked to ICTs in La Rioja. Currently we are 104 associates.
ICT Cluster	Sofia, Bulgaria	280	ICT	http://www.ictcluster.bg/	Foundation "Cluster Information and Communication Technologies" was created in 2005 by representatives of the Bulgarian ICT business. Acting as an umbrella organization of Bulgaria ICT Industry, ICT Cluster has 10 members (ICT associations

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

					and ICT clusters), which includes more than 280 ICT SME from different segments of the ICT Industry and 6 Bulgarian technical universities. ICT Cluster is a strategic cluster initiative of Bulgarian ICT business. The mission of the organization is to increase the competitiveness of Bulgarian ICT industry by support of ICT SME growth, promotion of ICT cluster excellence and creation of new business opportunities through cross- border, cross-industry and cross-cluster collaboration.
Digital Innovation Zone	Iasi, Romania	134	AI & Cybersecurity for manufacturing and healthcare	https://digital-innovation.zone/en/home/	DIZ it was funded in 2019 as a private not-for-profit initiative between the Regional Development Agency North-East, 6 universities (Technical University Iasi, Medical University Iasi, Al.I.Cuza University Iasi, Vasile Alecsandri University Bacau, Stefan cel Mare University Suceava, Life Sciences University Iasi), 5 chambers of commerce, 2 clusters / industry associations and several private companies in tech & digital marketing. Since 2020 we are a fully operational DIH in JRC website focused on Artificial Intelligence and advanced digital skills. Starting 2022, we developed the EDIH capabilities of our consortium, and we are part of several industry & DIH associations at EU level, such as DIH2, I4MS, Change2Twin certified DIH, EEN node, EIT Health & EIT manufacturing ecosystems. Although technology focus is on AI, cybersecurity is one of our main technologies, that is part of the test-before-invest (demonstrator) services, provided by our main associate partner, Technical University Gh. Asachi Iasi.
BCCS Cluster	Vilnius/Kaunas, Lithuania	15	Cybersecurity	https://bccs.tech/	BCCS Cluster is a consortium of private and public organizations that support the growth and development of the fintech and Web3 industry with knowledge, talent, and technology.
Latvian IT Cluster	Latvia	70+	AI & Advanced digital skills for Agrifood, manufacturin	https://itbaltic.com	Latvian IT Cluster DIH is a tech community with strong focus on internationalization, cross-sectoral collaboration and digitalization. Their competences and know-how are formed from 30+implemented local and international projects, playing a major role in increasing the global competitiveness of the Latvian IT companies. As the regional digital innovation hub, LITC serves as a go-to partner in digitalization initiatives. Advocating the development of sustainable industries through

			g, healthcare andiIndustry		digital tools, we act as a facilitator within the ecosystem, built in collaboration with universities, scientific institutions, government, corporates, industry and local champions (operating in traditional and high potential industries).
Northern European Cybersecurity Cluster	Finland (Cross-border initiative: Germany, Danemark, Latvia, Lithuania, Norway, Sweden)	400	Cybersecurity and Information Security	https://necc.network/	The Northern European Cybersecurity Cluster (NECC) promotes information security and cybersecurity related cooperation and collaboration in the Northern European region in order to enhance integration into the European Digital Single Market. The NECC has created a trusted competence network with various tested collaboration models among companies, academia, public sector and end-users. The cluster-type collaboration model is beneficial for all participating stakeholders and supports the EU&apos;s contractual Public-Private Partnership (cPPP). The NECC will be working towards more compelling business, cybersecurity and research environment for attracting more investments, resources and new innovation into the region.

Detail information on ambassador clusters.

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