

# Financial Support to SMEs for Innovative Security Solutions

LSEC, Leaders In Security – Webinar

December 20th 2021 - 12h00-13h30



# Agenda

- Objectives of SecurIT;
- Cascade Funding – Financial Support Mechanism
- Schedule and finance timing
- Themes covered by the project
- How to prepare?
- Support from the Partners and the Digital Catalyst
- Catalogue of partners
- Becoming evaluator
- Q&A Session (via Zoom chat – or invited into panel)

# The SecurIT project

*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*

**DG/Agency UE**

EISMEA - European Innovation  
Council and SMEs Executive Agency  
(previously EASME)

**Duration**









3 years (until 08.24)

**Consortium**

8 partners

**Budget for SMEs**

3,5M€

	<b>France</b>	Security and Aerospace cluster	Coordinator
	<b>Belgium</b>	CyberSecurity cluster	Partner
	<b>France</b>	IT Cluster	Partner
	<b>Lithuania</b>	Lithuanian Cybercrime Center of Excellence for Training, Research and Education	Partner
	<b>Netherlands</b>	Hague Security Delta – Security Cluster	Partner
	<b>France</b>	IT Cluster	Partner
	<b>Denmark</b>	Cluster: security, defence, space, cybersecurity	Partner
	<b>Poland</b>	Non profit private organisation Innovation Management	Partner

# The SecurIT Project



- **Main Objectives**

- Support European SMEs in the field of Security in the **development** and **integration** of **innovative solutions** in the field of **security** within a new integrated, competitive and global value chain
- Cofinancing and supporting the development of collaborative projects allowing to prototype and/or demonstrate technological solutions in the domain of security, taking into account ethical, legal and societal issues;
- Promote international collaboration between SMEs and other innovative actors

- **How ?**

Financing vouchers through Cascade Funding

- **When ?**

2 Open Calls for Collaborative Projects – first in January 2022

# Cascade Funding – Financial Support to Third Parties FSTP

- **Cascade Funding:** 3.5mio EUR to be distributed by the projects, made available by the EC.

- **Advantages?**

The EC introduced cascade funding in its H2020 Research and Innovation to :

- Reduce the gap between access to finance and the SMEs;
- Adapt the European funding system to smaller structures - more market and sector orientated;
- Becoming more agile in innovations

- **How?**

Project Partners (security oriented associations, clusters and poles) were selected after a call for proposals in 2020:

- Part of the budget is for the management and operations (selection, monitoring and support) of the Open Calls (1 and 2);
- Calls allow to finance the support activities for and by the SMEs.

# For SMEs (Small and Medium Sized Enterprises)

- The SecurIT project will organize and coordinate the European projects, for support to innovation and coordinate the action in terms of selection and follow-up of the activities:
  - Call open during 3 months (end of January – end of April);
  - "Light" applications (5-15 pages) in English;
  - Evaluations by independent experts and coordinated by the project teams;
  - Projects up to 12 months;
  - Funding through « lump sum » amounts ;
  - Contracting via SAFE (French cluster/pôle partner);
  - Regular reporting;
  - Light consortium agreement and Intellectual Property (IP) and Data Protection Management;
  - No double financing



# “Open Call” Schedule

Two calls for project submissions and access to finance.

1st «Open Call » : opens 25th of January 2022 - closes on April 26th 2022

2<sup>nd</sup> « Open Call » : opens in February 2023 - closes in May 2023

Submission of proposal via <https://securit.fundingbox.com/>

## Funded projects :

- Consortium of European SMEs - non-European SME welcome - but not financed
- Innovative digital solutions (AI ; Big Data ; CyberSecurity , etc.)



# Funding

For each Open Call, selection and support of 21 projects (prototypes and demonstrators) developed by 42 European SMEs

## Mini-grant for pre-selected projects



Jury Day Mini-grant



1 000 € / project



63 projects - 126 SMEs

## Prototyping



Consortium of minimum 2 European SMEs (security & cybersecurity)



Maximum 12 months



74 000 € / project



TRL minimum 5-6



14 projects - 28 SMEs

## Demonstration



Consortium of minimum 2 European SMEs (security & cybersecurity)



Maximum 12 months



88 000 € / project



TRL minimum 7-8



28 projects - 56 SMEs

# Open Call Information & Application



## Where to find information about the Open Calls?

- **SecurIT website** for general information about the program : <https://securit-project.eu/>)
- **Application forms and submission of the application** : <https://securit.fundingbox.com>
- Technical problems and support : [info.securit@fundingbox.com](mailto:info.securit@fundingbox.com).
- Independent evaluators with the SecurIT-project will select **up to 21 projects in Open Call 1 to develop prototypes and demonstrators in the domain of Security and CyberSecurity** with the support framework and funding mechanism of the SecurIT-project.
- Project need to be submitted by consortia of (at least) 2 SME's – ideally from two different European Member States, of which at least **one technology supplier** and which is relevant to one of the **identified challenges and needs** described in section 3.2 of the « **Guide for applicants** ».

# General Conditions

- SecurIT offers two types of instruments with **fixed funding support**:
- **Prototyping** : development of prototype solutions for the end users and / or innovative security technology integrators; with at least a Minimal Viable Product (MVP).
- **Demonstrators** : for new applications with innovative security technology and digital applications for security solutions, ready to be deployed at large scale and in a short term
- The selected consortia participate in a program that will support them for maximum 12 months and will receive :
  - **Up to € 74 000** per prototyping project (**maximum € 60 000 / SME**)
  - **Up to € 88 000** per demonstration project (**maximum € 60 000 / SME**)
- The consortium can only submit a proposal in one of the instruments, depending on the maturity of the solution, during an Open Call.
- We aim to select up to **7 Prototyping projets** and up to **14 Demonstrators per Open Call**

# Elegibility Criteria

- The SecurIT-project will verify the **eligibility of all submitted proposals** before the deadline to submit (application form online available) - <https://securit.fundingbox.com/>
- *The « **Guide for Applicants** »* will detail the following:
  - Eligibility criteria – section 3
  - Funding amounts
  - Requirements for the applications
  - Key Contacts and other useful information for the applicants
- Non-eligible proposals will be excluded from further participation and won't be able to receive any funding.

# Evaluations

- In different stages:
  - 1) **Automated eligibility assesment** (completeness, reviewed in English, before the deadline, informed Declaration on Honour)
  - 2) **Pre-scoring** (with over 60 Proposals submitted)
  - 3) **Evaluation by Independent External Experts**
    - i. Evaluation of each proposal by three independent external experts according to the following criteria (evaluators note each criterium on a scale from 0 to 5) :
      - i. Excellence (Ambition and Innovation)
      - ii. Impact (Market potential, competition, strategy)
      - iii. Implementation (Consortium, resources, legal framework)
      - iv. Transversal Criteria (contribution to the environment, low-carbon economy, equality, gender balance and societal and ethical impact)
  - 4) **Consensus meeting** (3 external experts, moderated by SecurIT-partners)
  - 5) Invitation to attend **Jury Day** - and pitch – present the proposal



Funding for projects developing innovative digital solutions around three main challenges and themes:

DOMAIN #1



**Sensitive infrastructure  
protection**

DOMAIN #2



**Disaster resilience**

DOMAIN #3



**Public spaces protection  
– major events**

# 1. Critical/Sensitive Infrastructure Protection

The security of sensitive sites is a major concern, confirmed by recent events, in a context of social unrest, terrorist threats and even a pandemic..

Targeted end-users: safety director of vital importance and Seveso\* classified industrial facilities; airports; hospital infrastructure; operators (electricity, gas, telecom...), NIS/2 and ECI-CIP/EPCIP\*

Proposals should consider the following requirements : maintainability, acceptable pricing, analysis anticipation, interoperability with existing solutions

SecurIT Domains	Sub-domains	N°	Challenges
<b>Domain #1: sensitive infrastructure protection</b>	Cybersecurity	1	Development of cybersecurity solutions for sensitive infrastructure protection
	Operations	2	Optimisation of communication networks and alert systems
	Identification and access control	3	Development and optimisation of identification and access control for rapid access in the site all while ensuring that no one and nothing that enters poses a security risk.
	Zone security and perimeter protection	4	Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and all barrier to clock intrusions

## 2. Disaster Recovery

Need of instruments for better prevention and preparedness, technologies for first and second responders, and where relevant for citizens, and overall societal resilience. The innovative technologies can help to detect; analyze and treat to prevent major natural events. Climate-related risks and extreme events; geological disasters, such as wildfires; earthquakes, tsunamis; pandemics)..

Targeted end users: first responders; cities and territories.

Proposals should consider the following requirements : implication and acceptance on citizens, transparency. continuity of operations.

SecurIT Domains	Sub-domains	N°	Challenges
Domain #2 - Disaster resilience	Prior to crisis – prediction: Risk knowledge and evaluation	5	Optimisation of prediction of disaster
	During the crisis: Communication and warning systems	6	Optimisation of communication and warning systems in case of disaster
	After the crisis: Post event analysis and recovery	7	Development of solutions for a better recovery

### 3. Public spaces protection – major events

A more connected city, integrating Artificial Intelligence, Cloud computing and Big Data, where the population takes on a more active role in serving the community.

Targeted end users : cities and territories (security of public roads); train station; venues open to the public (eg: stadiums; concert zone etc.).

Proposals should consider the following requirements : legal constraints, GDPR & eprivacy

SecurIT Domains	Sub-domains	N°	Challenges
<b>Domain #3 - Public spaces protection – major events</b>	Detection and alert	8	Gather and Manage real time information
	Analysis	9	Analyse and extract pertinent and potentially crucial information as quickly as possible
	Decision Making	10	Communication networks and post -event analysis
	Data protection and cybersecurity – cybercrime	11	Detection

# How to prepare?

- **Identify and Analyze** the domains and requirements, eligibility conditions – consortium, maturity level (prototype / demonstrator)
- **Block your agenda** for the Open Call and matchmaking event, for the proposal drafting
- Documentation available from **25/01/2022 latest**



Guide for applicants  
FAQ  
Proposal templates

- Online information sessions:  
European – and national January / February / March 2022



**Matchmaking platform** to detail – share your competences and ideas  
find partners on European level

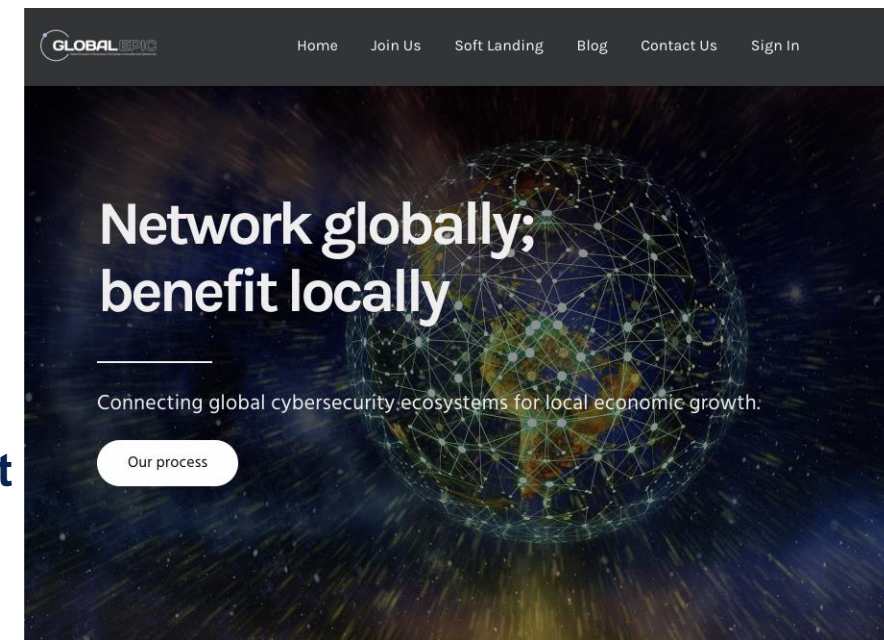
- **Follow our developments and news**  @SecurIT Innosup  @SecurIT20
- **Supported** by the clusters (pôles) of the SecurIT consortium and our ambassador cluster - partners



# Direct Support by



- Digital Security Catalyst – supporting digital transformation of manufacturing & security industry
- Support in the **definition of requirements and project**, of our Members for development of proposals
- Support in searching for **consortium partners – local & international**
  - International network of clusters globally
  - SecurIT partners & clusters
  - Ambassador cluster
  - End users and system integrators for deployments
- Support in the **preparation of the candidates & pre-assessment**
  - Advisory and reviews for improvements
  - Suggestions on missing elements

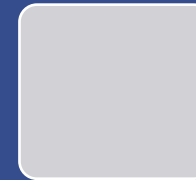


# Security Solutions Catalogue (under development)

- **Security Solutions catalogue** (expertise / products / services) in Europe with a focus on Members of the partners clusters (pôles) of the SecurIT consortium
  - **Market and Competitive Analysis**
  - **Vendor – Technology Solution Provider references**
  - List of products / services in relation to setting up consortia – partners for the Open Calls of SecurIT
  - **Visibility and Value Creation of competences** in relation to the competences and ecosystems in Europe
  - Basis for **Made In Europe CyberSecurity Label of Excellence**
- Publishing in February 2022
- **To be listed : reach out to your cluster or**  
[securit-catalogue@lsec.eu](mailto:securit-catalogue@lsec.eu)



**CyberSecurity - Identify / Protect / Detect / Respond / Recovery**



**Cyber-Physical Security Services** Audit,  
risk assessment  
Training



**Other security products & services**  
Monitoring, surveillance  
Tracking & tracing  
Detection, Alarms  
Vehicles and Platforms

Solution  
supplier to final  
end-users

Technological  
provider for  
integrator

Integrator of  
solutions for final  
end-users

# Call for Independent External Experts - Evaluators



Project proposals will be reviewed by **External Expert Evaluators**

Per project 3 reviewers



Specific mission limited in time and scope - Remunerated

Need for Confidentiality – Avoidance of conflict of interest - Independence

All in English



Seeking for complementary profiles (industrial / technical / academic / institutional) and expertises (physical security / digital, safety, cyber, IoT, IA)



Training : expectations, analysis, criteria, reporting

Schedule :

**January / February 2022 : launch for expert search**



End of April 2022 :  
attribution.

Final selection of evaluators in function of their candidatures received. Proposal

May - June 2022 :  
June 2022 :

Expert evaluations (offline)  
Consensus meetings followed by jury day (expert panel)

# Dashboard



Open Call 1:  
**January 25th – April 26th 2022**

Webinars, Support Sessions, B2B sessions and matchmaking, support from your local clusters & ambassador partners



Evaluating Proposals:  
**May – June 2022**



Funding & project follow-up:  
**July 2022 :** signing agreement and transfer of prefinancing of 20% of the project  
**December 2022:** intermediate reporting – review meeting  
**July 2023:** final deliverables received, commented. Final paiement of the remaining 80% following obtained results and positive evaluation.



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



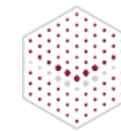
@SecurIT Innosup



@SecurITproject



@SecurIT20



**LSEC**  
LEADERS IN SECURITY

POLESCS

**L3CE**

**HSD**

**Systematic**  
Paris Region Deep Tech Ecosystem

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



**FundingBox**



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



# **Save the Date!**

## **Opening of Open Call 1 : 25 Jan. 2022**

**Ulrich Seldeslachts**  
MD LSEC  
[securit@lsec.eu](mailto:securit@lsec.eu)

**Richard Chisnall**

**Neil Adams**



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