Ref. Ares(2024)6038710 - 26/08/2024

SECURIT

TOWARDS RESILIENT SMART CITIES & TERRITORIES

Project Deliverable

D4.3 Exploitation and Sustainability plan

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	V7
Due date	August 31st 2024
Submission date	August 31st 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	20-11-2022	Document Creation	Draft	Internally (HSD)
V1	14-04-2023	SecurIT Midterm version (during 1st open call)	Draft	Project partners
V4	21-02-2024	SecurIT version	Draft	Project Partners SecurIT
V5	16-06-2024	SecurIT version	Draft	Project partners
V6	1-07-2024	SecurIT version	Draft	Internally (HSD) and Project Partners review: L3CE & SAFE
V7	31-08-2024	SecurIT version	Finished	Public

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

Table of content

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

Abstract

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

This report outlines the Sustainability and Exploitation Plan for SecurIT, a comprehensive framework designed to ensure the long-term viability and impactful utilization of the SecurIT project's outcomes. The SecurIT project has significantly advanced innovation and developed robust security solutions across Europe. Supporting over 95 SMEs, the project achieved notable success in 42 projects.

Sustainability strategies are devised to maintain and support SecurIT's operations beyond the initial funding period. The exploitation plan details how the innovations and solutions developed by SecurIT will be leveraged to generate value for stakeholders. It highlights commercialization opportunities, intellectual property management, and pathways for technology transfer. Specific actions include engaging with industry leaders, facilitating uptake by potential end-users, and promoting awareness through targeted dissemination activities.

By focusing on sustainability and exploitation, SecurIT ensures that the developed solutions can be further enhanced and brought to market, benefiting a wide range of stakeholders. The project provided tailored support and visibility at the EU level for SMEs, improved collaboration among clusters, and created a robust foundation for continuous advancements in security technologies.

Authors (organisation)

Security Delta (HSD)

Reviewers (organisation)

Pôle SCS, Systematic, SAFE Cluster, L3CE, LSEC, CenSec, FundingBox

Keywords

Sustainability, exploitation, SMEs

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

Section 1 – Management summary: The strategic advancement from SecurIT to Meta Clustering

The aim of the SecurIT project was threefold:

- To support the development and integration of innovative security solutions in a new industrial value chain (and services)
- To co-finance and support the development of collaborative projects allowing the prototyping and experimentation of technological solutions in the field of security, taking into account the ethical, legal and societal challenges of this sector
- Promote cross-border cooperation between SMEs and other innovation actors in this sector.

KPIs

The SecurIT project has achieved significant milestones, fulfilling key performance indicators (KPIs) that demonstrate its success and impact:

- Innovation and technology development: successfully developed and tested cutting-edge security solutions for 42 projects with 95 SME's involved in these projects.
- Funding utilization: efficiently utilized allocated funds to achieve project goals and deliverables.
- Collaborative efforts: fostered strong partnerships with key stakeholders across Europein the (digital) technology and security domain.

Results

The results of the SecurIT project highlight its effectiveness and the foundation it has established for future growth:

- Enhanced Security Solutions: deployment of advanced (cyber)security technologies that address current and emerging threats.
- Increased market reach: expanded the reach of the solutions to new markets and industries.
- Economic impact: generated economic benefits through job creation and business growth in the digital security sector.
- Positive stakeholder feedback: received positive feedback from partners, end users, and customers, validating the project's success.

Lessons learned

One critical lesson from the SecurIT project is the importance of market internationalization and connecting with end users and customers. Expanding our market reach and securing additional funding are essential for maximizing impact. Following the significant achievements of the SecurIT project, it is crucial to build on this success. This could potentially be done by advancing to the next phase: meta clustering. This strategic move aims to expand our impact, facilitate internationalization, and enhance market reach, ultimately driving growth and innovation in digital security. Meta clustering will be enhanced by focusing on the advantages of clustering and cascade funding (Financial Support for Third Parties FSTP), see below.

By engaging in meta clustering, we can leverage the collective strengths of multiple clusters to achieve these goals. For example, by collaborating with clusters from Spain (AEI Cybersecurity and Advanced Technologies), France (SAFE, Systematic and Pôle SCS), Belgium (LSEC), Ireland (Cyber Ireland), Sweden (Mobile Heights/Compare), Denmark (CenSec), Lithuania (L3CE), Germany (Security Network Munich), and Poland (Fundingbox). Finally, The European Cyber Security Organisation (ECSO) can provide support in navigating international markets and advancing our technological readiness levels

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

(TRLs). Focusing on higher TRLs and direct market engagement will ensure our solutions are market-ready and meet the needs of end users.

Advantages of clustering in Europe

Clustering in Europe offers several strategic advantages:

- Collaborative innovation: facilitates knowledge sharing and collaboration among clusters, enhancing innovation and technological development.
- Market expansion: provides access to diverse markets across Europe, allowing for greater market penetration and customer reach.
- Resource optimization: enables efficient utilization of resources by sharing expertise, infrastructure, and funding opportunities.
- Strengthened competitiveness: this enhances the competitive edge of SMEs by connecting them with leading clusters and industry leaders.

Advantages of cascade funding

Cascade funding provides substantial benefits for advancing projects like SecurIT:

- Increased financial support: cascade funding/FSTP offers additional funding opportunities, enabling projects to scale and achieve greater impact.
- Simplified access: cascade funding/FSTP streamlines the funding process, making it easier for SMEs and startups to access financial resources.
- Encourages innovation: cascade funding/FSTP supports innovative projects and encourages the development of cutting-edge solutions.
- Reduces financial risk: cascade funding/FSTP distributes funding across multiple recipients, reducing the financial risk for individual projects.

Long term impact of the SecurIT Project

The long-term impact of the SecurIT project extends across societal, IT/cybersecurity, economic development, and innovative SMEs:

- Societal impact: enhances societal security by deploying advanced (cyber)security solutions that protect critical infrastructure and personal data.
- IT/Cybersecurity: drives advancements in IT and cybersecurity, setting new standards for security technologies and practices.
- Economic development: contributes to economic growth by fostering innovation, creating jobs, and supporting the digital economy.
- Innovative SMEs: empowers SMEs by providing them with the resources, funding, and networks needed to innovate and succeed in the competitive digital security market.

In conclusion, meta clustering represents a strategic leap towards greater impact and innovation in digital security. By expanding horizons, leveraging funding opportunities, and enhancing our market presence, we are set to achieve new heights with the SecurIT project. Together we aim at fostering a collaborative ecosystem that drives innovation, economic growth, and enhances security across Europe.

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

Section 2 – Sustainability & Exploitation of the SecurIT-project

Section 2.1 – Overview of the SecurIT Project

SecurIT is a collaborative European project that aims to promote a new industrial value chain for safe, secure, and resilient cities and territories. It did so through supporting and co-financing the development of collaborative projects involving multiple European partners. This permitted to experiment and developinnovative solutions in the field of security. **SecurIT was structured in three major axes:**

1. It demands analyses of use cases on the security market. These has been developed with integrators and final users.
2. It supports development of innovative technological security solutions in the TRL 5-8 stages.
3. It played a matchmaking role. This role is important to facilitate consortium building for the application for the 2 open calls.

SecurIT supports 42 collaborative projects developed by 95 European SMEs selected through two cascade funding open calls. The project was led by 7 European clusters and 1 European SME. To ensure that the selected projects' funding outcomes provide longer-term benefits, both for their target group/sector and the broader European market, it is important to assess how they anticipate and execute plans and actions that will facilitate extended results. The impact that the SecurIT project thus aims to create is the following:

Table 2.2- (a).2 SecurIT exploitable results

Nº	Product Result	Exploitation Route	Progress at M18	Progress at M36
1	Analysis Reports	The state of play of both integrators/end-users (representing the demand side) and security solution providers (offering smart solutions) sides, and of regional strategies with regards to these two sectors and related value chain will be described in respective analysis reports. Those are the basis for further developing the required strategies to reach the relevant	*Analyses of all mentioned aspects are underway.* *In the case of the solution mapping, an interactive platform has been launched on the SecurIT website.*	*Analyses of all mentioned aspects are done (deliverables are done).* *In the case of the solution mapping, an interactive platform has been launched on the SecurIT website.* *We are connecting end-users to solution*

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

		SME's and to build trans-sectoral collaboration cases also after the project.		*providers and will continue to do so.*
2	Intimate knowledge about and build trust among the consortium partners	The consortium partners have been intensively collaborating during the 36 months. This results in an intimate knowledge of each other's ecosystem. Together with the built-up of mutual trust, this will be a strong basis for future cross-sectoral and international collaborations.	*After 18 months there are already multiple collective and bilateral acts of cooperation*	*After 36 months there are multiple collective and bilateral acts of cooperation. We are exploring follow up actions for after the SecurIT project.*
3	Built-up service portfolio	The activities developed within the SecurIT project, and the knowledge and experience achieved with give the opportunity to enlarge the service portfolio of the consortium partners, certainly on an international and cross-sectoral level. Several services will be developed, often by tailoring already available services, to optimally support the building of value chains on security applications. The consortium partners can develop business models to continue these services after the project has finished. Examples of possible services are training, matchmaking, seminars etc. (e.g. training, coaching, matchmaking …)	*Several initiatives are being explored: both in terms of linking service portfolios of SecurITprojects with consortium partners and in looking at follow-up business models*	*Several initiatives are being explored: both in terms of linking service portfolios of SecurITprojects with consortium partners and in looking at follow-up business models. The experience from the SecurIT project, our best practices and lessons learned are useful building blocks for the future.*
4	Security roadmap for the SMEs	The SMEs that are participating in the project be able to make a start with or further develop their roadmap on security. Technical knowledge and experience will be built up, but also market	*At M18 of SecurIT, the OC1 projects are at their M6 marker. First indicators of developing security roadmaps can be seen*	*At M36 of SecurIT, the OC1 and OC2 projects are at their all done and validated by the committee of consortium partners. .*

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

		knowledge is gained, and business relations will be built. All this can be exploited by the SMEs to develop and grow their business further successfully.	*from the different SMEs. These will also be included as lessons in the Sustainability and Exploitation Plan.*	*First indicators of developing security roadmaps can be seen from the different SMEs. These are see in the Sustainability and Exploitation Plans,*
5	Large stakeholder database	The wider ecosystem get to know the results of the SecurIT project via dissemination and communication activities. Success stories help to increase awareness of the importance and expected benefits of the application of security technologies in operational environments. Regional policy and related strategies can be positively influenced by all the positive results achieved within the project.	*At the M18 point, the SecurIT consortium has undertaken multiple communication and dissemination activities, largely surrounding the Open Calls. Approved OC1 projects are inter alia actively disseminating their participation through conference presentations and publishing papers.*	*At the M36 point, the SecurIT consortium has undertaken multiple communication and dissemination activities, largely surrounding the Open Calls. Approved OC1 and OC2 projects are inter alia actively disseminating their participation through conference presentations and publishing papers. On our LinkedIn channel (SecurIT Innosup we have regularly communicated about the progress of the projects, the projects itself and the final event in May 2024. There are multiple success stories that can be found in D5.2.*

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

Section 2.2 – Introduction Sustainability and Exploitation Plan

The Exploitation/Sustainability plan is part of WP4 of the project, related to Monitoring and Impact Management. The objective of the Exploitation/Sustainability Plan is to summarize potential exploitation paths for each involved project and ensure the sustainability of the overall SecurIT initiative beyond its original timeline. This document presents the items, strategies, and opportunities for exploiting the project and collaborative project results. To enable a comprehensive and sustainable capitalization of the project developments, this deliverable also provides an extended impact assessment overview of the collaborative projects supported throughout its lifetime for enabling parties, notably for SMEs to build upon the results achieved in their endeavours.

This Exploitation and Sustainability plan will assess how the EU-funded project SecurIT can ensure long-term and structural beneficial outcomes and projects in a sustainable manner. The plan is divided into 7 main sections (excluding the introduction and conclusion). First, **a management survey is given. Second,** the process/input of the clusters is **analysed** and explained. This is done by identifying the main activities carried out by the different clusters that led to the identification of the exploitable assets. The **third** section contains a description of these assets as well as their prospective beneficiaries and the exploitation routes that have been planned to ensure their sustainability. **Fourth**, the Consortium partners' exploitation plan is included in section three. This is divided into the common plan of the **project;** the separate coordinating clusters' exploitation plans and the 42 use cases/solutions that can be considered as direct sustainable output of the SecurIT project. **Fifth**, the impact assessment provides information about how the coordinating clusters measured the impact of the SecurIT project, both on the individual projects and on the field of digital security solutions. This also includes evaluations of the clusters, the funded projects, and a measurement of effectiveness (with some average statistics gathered from the SecurIT project). In section **six,** the benefits for external stakeholders are analysed. Finally, section **seven** gives the concluding remarks for the document and project.

Section 2.3 – Monitoring (how did the clusters monitored and supported the SMEs)

The most crucial period for the monitoring of projects is during the execution phase of the projects. During this period, the SecurIT partners were assigned projects to monitor based on geographical location, earlier contact, and, if necessary, other criteria like affinity with the subject matter. In this process, the guiding cluster is referred to as the 'Follow-Up Manager' (FUM). For both Open Calls, each of the clusters were assigned three different projects to monitor, six in total.

The process of monitoring was done on different levels and in multiple ways. Most importantly, the follow-up managers scheduled a monthly meeting with the contacts of each of their projects. These meetings were designed to discuss the developments of the product, their ability to stick to the schedule, to keep track on progress or identify potential delays, and to update the consortia on any news from the SecurIT organisers. Besides these monthly meetings, the projects were asked to deliver a follow-up plan in Month 1, a midterm report halfway through their project at Month 6 and a final report at the end

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

of the funding period (Month 12). More information on these reports have been included under section 4. Last, the projects consortia were asked to fill in a questionnaire which assessed their progress regarding the arrangement of the final demonstration. Internally the SecurIT clusters reported on the progress of their assigned projects during the regular meetings among SecurIT consortium members and FUM and additionally in scheduled mini committee meetings, according to the milestone review process established. These meetings were implemented to discuss the above-mentioned reports that were delivered by the consortia during the project.

Section 2.4 – Best practices: how were ways to ensure sustainability identified.

During the selection process in both Open Calls, projects' applicants were asked about various topics that could be an indication of the sustainability and exploitation potential of their proposals. Indicators like **ambition, innovation, market opportunity/potential**, **the possibility for growth/expansion**, and **market size** were, amongst others, key indicators (like **feasibility of the project implementation**) in selecting which projects would be most suitable to receive SecurIT funding. Through selecting on these criteria from the start, the SecurIT partners ensured that there was sufficient sustainability and exploitation potential in all proposals selected.

We have asked for an exploitation plan by all participating projects, to see if and how their projects are sustainable.

The result from this is that all projects have implemented a clear, objective strategy on their sustainability of the project and their exploitation after the SecurIT project. All projects have displayed this in their Final Reports, that are available. Finally, the sustainability and exploitation sections have been reviewed by the Follow Up Manager and a mini committee to ensure its soundness.

Section 3 – Sustainability – main exploitation routes of SecurIT assets

This section provides a detailed description of the ways in which the SecurIT project ensures the sustainability of its actions and projects including through the promotional exploitation of the project. All clusters contributed through a joint effort to the successful implementation of these activities. However, for each activity a lead partner was designated, who had the main responsibility for this specific activity (in line with their contributions to the project developments).

There are 5 subsections which describe the assets, namely:

1. Call for proposals – Methodology and materials
2. Collaborative projects funded under the SecurIT calls for proposal
3. SecurIT matchmaking: the approach and lessons learned
4. SecurIT communication materials (identity, website & tools)

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

5. IoT4Industry European Cluster Network, Ambassador clusters, other EU initiatives and regional initiatives
6. SecurIT funding instruments mapping tool
7. SecurIT projects clustering approach

Section 3.1 – Call for proposals

The Open Call process is explained in the Guide for Applicants document, also included in WP3 deliverable D3.3. and D3.5. In these deliverables, it is stated how the SecurIT open calls process works.

Open call results

During the first SecurIT open call, we received 111 complete collaborative projects' proposals from 240 SMEs applicants. During the second open call, 130 applications were completed, from 271 SMEs applicants. After an eligibility check and pre-scoring, 60 proposals were evaluated by external experts for the first call and 80 for the second open call. A total of 29 projects were invited to pitch their proposal during the jury day for the first call and 37 for the second Open Call. As a result, 21 collaborative projects were funded from the first open call and 21 from the second.

Promotional activities – related to the open calls.

SecurIT undertook many different dissemination activities, which were aimed at attracting SMEs to register for the open calls for the SecurIT project, and to offer a matchmaking service to prospect SMEs.

The promotion took mostly place online but also through some events and fairs. The SecurIT project has an active social media presence on LinkedIn and Twitter, garnering thousands of impressions and likes during the open call periods. This social media promotion was under the guidance of the Pole SCS cluster and collaboration with FBA and FBC as the open calls managers. Videos, infographics, gifs, and other design elements in line with the SecurIT visual identity were published on these platforms. The same SecurIT style was also reflected in the physical promotional materials like flyers, banners, posters, etc. to ensure coherence and recognizability of the project. These materials were also distributed by the partner clusters at events like the Mobile World Congress 2022, IoT World Congress 2023 in Barcelona, Wolrd AI Cannes Festival in 2022 and 2023, and finally at the SMI2G 2024 in Paris to promote the SecurIT project's results.

Another form of promotion of the SecurIT project was results-based. During the first open call period, the partner clusters created a mapping of innovative European security solutions. This mapping gave the involved companies a platform to showcase their solutions and gain exposure, and additionally informed them about the existence of the SecurIT project. On the website, there are currently 134 solutions providers, and 166 security solutions displayed.

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

Sustainability and exploitation of the calls for proposals.

There are lessons learned from the SecurIT project which could help as a case/inspiration for other Cascade funding projects. In D3.6 some of these lessons learned are already mentioned, for example:

- **Preparation for the open call:**
    - Special attention was given to the proper explanation of the type of applicants that are eligible for funding, especially when the open call required a particular type of participant – consortia of at least 2 SMEs from the security domain, with a special focus on cross-border collaboration. In this case, additional efforts were dedicated to agreeing on the common understanding of the eligible participants in terms of consortium composition. This approach works well throughout the whole open call, which was proved by the high number of projects submitted by cross-border consortia (around 71% of applications were submitted by consortia composed of SMEs from different countries).
- **Selection process:**
    - One of the key selection stages was pre-scoring, which is an optional phase allowing the automatic scoring of applicants as an initial quality screening and an important management of open calls. Given the high number of applications in 1st Open Call and prediction of similar interest in SecurIT 2nd open call, much attention was given to the revision of pre-scoring criteria during the preparation phase. As a result, the pre-scoring in the 2nd open call was tailored exactly to the kind of applicants the Selection Committee was looking for. For instance, SMEs with less experience in European projects were given higher priority (i.e. higher scores) as opposed to those with many EU funding projects. This and other criteria were carefully considered to align with the overall project objectives of promoting innovation and giving access to funding to SMEs in the security sector.
    - Continuing recommendations from lessons learned during the 1st Open Call, the Jury Day in 2nd Open Call was organised as a hybrid online/physical event. That way, the applicants invited to Jury Day did not need to fulfil formal requirements regarding the basic formal check (for mini grant) and their participation in the pitches was more manageable for the SMEs, as well as for the management of the open call by the Consortium. The Jury met physically and sharing one space, especially during the Jury Day Consensus Meeting, was helpful in providing a dynamic environment for discussions and reaching final decisions efficiently.

During the projects' implementation, the organizers of the SecurIT project (7 clusters and 1 SME) held meetings every two weeks to inform each other of the status of the projects. This would help us to see if there is help needed or if projects were on schedule, regularly. This approach keeps all parties sharp and is recommended to be implemented in similar future projects to guarantee the quality of the output of projects.

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

Finally, the process of mini committees to check the quality of the Reports from the projects (Follow Up Plan, Mid-Term Report and Final Report) is a definite recommendation for future projects and lesson learned. This process guaranteed the quality of the projects at their end, as well as ensuring the Follow Up Managers understanding of their projects by explaining what their projects were about. Ensuring projects deliver a quality report and letting the FUM's explain projects to peer organizers ensures quality in the totality of the project.

In conclusion, the methodology and approach used by the SecurIT project in open calls is a useful case for other European projects/Cascade funding projects, that could be replicated in other type of collaborative projects where selection and monitoring of sub-projects is implied. The clear guidelines in selection process via the open calls, criteria for the selection day, monitoring of the projects up by Follow Up Managers, regular check ins with the organizers of the SecurIT projects and mini-committee meetings amongst FUM's can be successfully used in different projects if implemented similarly.

Section 3.2 – Collaborative projects funded under the SecurIT calls for proposal.

Funded projects

During two open calls, a total of 42 projects received funding from the SecurIT project. This can be regarded as the most important output of the program and in line with the INNOSUP initiative objectives. Mainly, the development of their respective innovative solutions within the security domain in the context of international cooperation. We promoted the funded projects as use cases via our social media platforms. These use cases serve as figurehead of SecurIT, as inspiration for new innovations and, as a means of knowledge sharing. These use cases are listed under Chapter 4 in this document.

Target group

The SecurIT project was aimed to support SMEs through funding, matchmaking, and advice. Mainly, the goal was to boost the development of innovative, digital security solutions by European companies. Also, to increase the internal strength of the digital security network, and to inform and inspire users by providing a security solution mapping platform. The calls and the matchmaking services were also intended to facilitate cross-European collaboration.

Section 3.3 – SecurIT matchmaking: the approach and lessons learned.

In this subsection, the matchmaking process is explained and elaborated on further, through the following points:

- ➔ WP3 matchmaking SecurIT for the 2 Open Calls
- Use of the B2B platform from SYSTEMATIC
- Wide dissemination and encouragement to book meetings
- At least 1 funded project met through this. Partners from 7 out of the 42 funded projects were registered to at least one of the matchmaking sessions and had at least one meeting.
- Please find below a synthesis of the 4 matchmaking sessions' results:

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

Open Call n°	Date	Nb of registrants	Nb of bilateral meetings	Nb of applications		Nb of selected projects	
				OC1	OC2	OC1	OC2
OC1	17.02.22	42	23	6	1	4 (IDEAS, VASCREEN, ZENITH, FusionSec)	1 (ServAL Management)
	17.03.22	31	14	3	2	1 (RASAD)	0
	Total	**73**	**37**	**9**	**3**	**5**	**1**
OC2	18.01.23	22	7	n/a	2	n/a	0
	08.02.23	19	5	n/a	2	n/a	1 (ERRATA)
	Total	41	12	n/a	4	n/a	1

All in all, the process of matchmaking through the SecurIT project was succesfull for at least 7 projects out of the 42 in total that finished at the end of SecurIT. This demonstrates that the efforts by the SecurIT project in facilitating matchmaking in the sense that it does, does work to help SME's connect to each other and possibly engage in projects with each other.

The SecurIT Solutions Mapping tool provides an excellent continuation of this matchmaking process. With this tool people can use to see companies and the different solutions they offer from various countries. Allowing people to look for themselves if they see interesting companies/solutions and possibly engage with them.

Section 3.4 – SecurIT communication materials (identity, website & tools)

In this subsection, a brief overview of the communication strategy that has been used to disseminate the SecurIT project is identified. A complete overview of the different communication channels and results are described in the D5.1 and D5.2.

The following keywords indicate what kind of information was used for communicating:

- Website: https://securit-project.eu/
- LinkedIn: https://fr.linkedin.com/company/securit-project
- Videos:
    - Short version: https://www.youtube.com/watch?v=tmsG71iMt54
    - Long version: https://www.youtube.com/watch?v=lRL6uCcV424
- Cluster organisations (social) media funnels
- Dark Blue/Red theme on the website and all social media communication
- Re-occurring hexagons.
- Etc.
- An overview of the different communication channels and results are described in the D5.1 and D5.2

All dissemination used for the SecurIT went via SecurIT LinkedIn channel. We communicated regularly on the different projects and their achievements.

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

Section 3.5 – SecurIT European Cluster Network, Ambassador clusters, other EU- and regional initiatives.

In this subsection, the value of the creation of a cluster network as basis for the SecurIT project is explained. Briefly, the inclusion of the ambassador clusters will be mentioned and the possibility for future cooperation in EU or national/regional initiatives. More information can be found in deliverable D5.2.

This section will have the following structure:

- Description of the cluster network (international dimension/internal cooperation/external cooperation/sustainability/networks):
    - The consortium of the SecurIT project gathers 7 complementary European security clusters and 1 private entity. SAFE, CenSec and HSD are security market-oriented, with close collaboration with the practitioners and the capability to involve them for the use cases and testbeds identification. SPR, LSEC, L3CE, SCS are deep techs oriented, with a capacity to analyse the potential of disruptive innovations. SAFE, CenSec, are security solutions-oriented, as LSEC and L3CE are cyber security oriented and SCS, HSD and SPR are security and cyber security solutions-oriented. These clusters represent globally 11,4% of the EU security turnover. Funding Box is a European leader in supporting innovators' funding.
    - The international dimension and cooperation is highlighted in the fact that the clusters come from different European countries. This way our combined networks have collaborated to ensure the best results for the project.
- Inclusion of ambassador clusters (including the value of the built networks)
    - Description:
        - Ambassador clusters's engagements planned in the SecurIT project at the submission stage to increase dissemination outreach. This is especially relevant given the objectives of the project –to attract SMEs in consortia of two partners from two different EU Member States- and the composition of the consortium – gathering seven clusters from five different European regions and countries (Ile-de-France, Provence Alpes Côte d'Azur, Flanders, South Holland, Central Jutland, Lithuania). Even if the seven clusters involved are representative of the security sector in EU (gathering 11.4% of EU Security turnover), the objective is also to increase the outreach in other European regions and to attract SMEs from countries where there is no SecurIT partner. As established at the proposal stage, the objective is to create a network of ambassador clusters, gathering at least 10 clusters formally engaged.
    - Impact:
        - As a result, to the first recruitment campaign before the end of the First Open Call, 14 Ambassador Clusters has signed up (out of 36 contacted), covering 13 countries.
- Future collaboration between (ambassador and organising) clusters in future EU initiatives.]
    - See the Management Summary at the start of this report for this.

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

Section 3.6 – SecurIT Funding Instruments Mapping Tool.

The Funding Instruments Mapping Tool (available to all interested entities through SecurIT web page (SecurIT – Towards resilient smart cities & territories (securit-project.eu): https://financing.digitalsecuritycatalyst.com). The tool created as part of T2.3 provides a convenient platform for SMEs to easily search for funding instruments tailored to their specific requirements.
The prototype of the tool was initially introduced within the SecureIT projects. However, the subsequent exploitation path of the tool heavily relies on ownership, as a critical factor essential for ensuring maintenance support and widespread accessibility to SMEs across the EU.

In this context, the tool was presented to the Innovation Agency Lithuania, serving as the national NCP for the Digital Europe programme. On the national level Agency acts as the primary contact for offering guidance, practical information, and assistance to national SMEs across all aspects of the DE program. Furthermore, Agency holds responsibility for most national funding instruments aimed at supporting innovations development and acceleration in Lithuania. They acknowledged the significant potential of the tool and confirmed their commitment to regularly contribute insights on available calls and funding instruments.
However, ownership of the tool solely at the national level wouldn't bring the desired benefits. Engaging all Member States is imperative to ensure the vitality and wide usability of this technology.

Thus, a centralized approach proves to be the most valuable as it provides a comprehensive overview of available funding instruments in EU and supports cross-border collaboration. From this perspective, we are exploring several options that could be considered as potential paths for further exploitation of the Tool:

- The European Cybersecurity Competence Center (ECCC) seems a highly suitable candidate for owning the tool, primarily due to its robust ecosystem. This ecosystem includes a network of National Coordination Centers for Cybersecurity (NCC), which can greatly facilitate seamless collaboration and information exchange between the NCCs and owner of the platform. By leveraging this network, the ECCC has strong potential to advance the tool transforming it into EU platform, serving as a one-stop shop for SMEs and other stakeholders.
- ECSO emerges as an alternative option for maintaining and scaling the tool. Given the organization's overarching goal of fostering the development of cybersecurity communities and strengthening the European cybersecurity ecosystem, integrating the tool aligns seamlessly with its objectives. By leveraging its resources and existing ecosystem, ECSO can provide valuable support for the tool's enhancement and expansion. Furthermore, with its focus on accelerating innovation within the cybersecurity domain, ECSO can contribute significantly to maximizing the tool's impact and usability.

Moving forward, our next steps involve leveraging established ecosystem of SecurIT to introduce the tool to national NCPs, ECCC- NCCs, and ECSO. Through this outreach, we aim to identify the most suitable candidate to take ownership of and further develop the tool after the project ends.

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

Section 3.7 – Project clustering approach

The project clustering approach outlined in D2.5 has gained a strong support from both end-users and integrators. This approach offers a novel and more efficient method to engage a broader community of users, providing them with a wider range of functionalities to address the specific problem or challenge. Piloted during the SecurIT project, this approach was deemed successful and has been chosen to continue with selected innovations.

Our next steps after the SecurIT project ends involve the development of acceleration strategy for the first stack of clustered projects specifically focused on Public Space Protection. The primary aim of our future effort is to sustain the momentum of innovation by leveraging tools and support services developed and tested during the implementation of SecurIT. This includes facilitating demonstrations, engaging end-users, conducting ELSA assessments, and accelerating the utilization of new funding instruments.

Additionally, it's important to highlight the role of the ecosystem established by the SecurIT project that was tested as reliable and structured framework for the development, testing, and implementation of innovative solutions. This collaborative and multi-faceted approach could be exploited as the best practice on national projects based on cascade funding to accelerate the innovations.

Section 4 – Consortium partners' exploitation plan

The exploitation plan is under divided into three different parts. In the first section the common plan is lined out, which consists of the explanation of the three follow-up plans that have been delivered by the funded projects during the process. In the second section, 42 projects/solutions are included that can function as illustration and examples. In the last section, the different exploitation plans of all included clusters are listed.

Section 4.1 – Common plan

To ensure concrete results that align with the desired output of the SecurIT project and can ensure some sustainability, the funded projects are asked for a Follow-Up Plan in month 1, a Mid-Term Report in month 6, and finally a Final Report in month 12 of the funding process.

The month 1 follow-up sets the frame and clarifies expectations on what the consortia need to adhere to during the project period. This document also serves as a baseline against which further progress is measured. The month 6 follow-up is a midterm report that is used to evaluate the progress in the first half of the project and to revise the expectations for the second half of the project. The month 12 follow-up is the final report that is used to evaluate the achieved results of the project and indicates future exploitation of the project (beyond the initial project period).

The three documents ask the consortia multiple questions that can be (in)directly linked to exploitation and sustainability. In the table below, these different questions are listed per follow-up report, including a short explanation of the question. Most questions throughout the documents can be directly linked to

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

each other, as the questions build on similar questions as asked in the previous report. However, some questions in the M12 report are not related to the questions in the other reports. Additionally, after the follow-up plan and the midterm report, we learned that it is important to specifically elaborate on the practical input that you are asking for. This helps to prevent very short, vague, or unclear answers.

Questions (in)directly linked to sustainability/exploitation		
Month 1	**Month 6**	**Month 12**
Please describe the expected key milestones that you will achieve during the project and indicate a time for when you expect to achieve them (you can use the description from the proposal). Please be specific in your description. *Through these milestones, we can not only measure how far the projects have come, but also how results and resources have been exploited and how outcomes have helped reach both long- and short-term outcomes.*	Please describe the key milestones that you have achieved during the first half of your project period. Please be specific in your description. If there are any deviations, please explain why this is the case and which corrective measures you will use in order to get your project back on track.	Please describe the key milestones with dates that you have achieved during the entire project period (and mentioned in the Follow Up Plan M1). Please be specific in your description. If there are any deviations from the deliverables you planned at the beginning of the project, please explain why this is the case.
Please describe the dissemination activities that you expect/plan to execute during the project period (e.g. informing about the project in national media, newsletters, during national events etc.). Please be specific in your description. *Dissemination activities help to increase the visibility of the developed solution. This has a positive influence on the longevity of the solution and is thus part of the sustainability of the SecurIT project*	Please describe the dissemination activities that you have participated in in the first half of your project period (both in terms of those activities mentioned in the first Follow Up Plan and additional ones). If there are any deviations, please explain why this is the case and which corrective measures you will use in order to get your project back on track.	Please describe the dissemination activities that you have participated in during the entire project period (both in terms of those activities mentioned in the first Follow Up Plan M1 and additional ones). What were successful dissemination activities, and how did you measure them? If there are any deviations from the deliverables you planned at the beginning of the project, please explain why this is the case.

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

Employment created / safeguarded due to the Project (estimation) *While not explicitly mentioning exploitation and sustainability, this question asks about the employment that the individual SecurIT projects have either created or safeguarded. The employment created gives an indication of the exploitation of SecurIT funds.*		Employment created / safeguarded due to the Project (evaluation)
Impact on turnover due to the project (estimation) *This question again indirectly indicates the sustainability of projects as the greater the (positive) impact on turnover, the greater investment on further development can be made, and the more likely a project is sustainable in the long-term. It also points to the exploitation of the SecurIT funds provided.*		Impact on turnover due to the project (evaluation)
Contribution of the project to new or significantly improved products launched. *This question talks mainly about the exploitation of the project. Namely, it enquires how the project results have been exploited to (help) create new or significantly improved products.*		Contribution of the project to new or significantly improved products launched.
Describe how you expect to exploit the knowledge and progress developed in the project (and how it will be used after the project is finished) *This question is designed to directly measure the exploitation of the different funded projects.*	Please describe how you have exploited the knowledge and progress developed and obtained in the project period so far. Please be specific in your description.	Please describe how you have exploited the knowledge and progress developed and obtained in the project period so far. Please indicate what your plans are for future exploitation beyond the SecurIT support program. Please be specific in your description.
		What are the challenges you need to overcome to ensure a successful future of the project / demonstrator / prototype? *This question is designed to get an insight in the (maturity of the) vision of the companies on the future of their project*

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

		What is your vision of the end-product as a start for new/further collaboration with new or current partners for new security innovations? *This question addresses the future collaboration possibilities for the companies that participated in the SecurIT project.*
		Commercialization strategy -> elaborate on long-term vision of the marketing strategy. How do you propose to get into the right networks, attract more potential clients, create your own brand. What will be the focus of your marketing strategy? *This question specifically focuses on the commercial/marketing aspect of the solution.*

Section 4.2 – Coordinating clusters' exploitation plans

In this section, each of the organising clusters provides information about their own exploitation of the SecurIT project. This provides an overview of how the SecurIT project benefitted the organisational clusters and their respective networks throughout different countries. Each cluster provides an explanation of their own exploitation strategy and are asked to list different practical indications of this.

SAFE Cluster	
Exploitation plan: **(Please elaborate on the specific exploitation strategy for your own purpose, and list the different practical indications of this)**	SecurIT is an interclustering project that permitted to enhance clusters collaboration at European level. SAFE was the coordinating entity of the overall project for the 3-year duration and coordinated activities with all the partners. With this position, SAFE also asserted its vital and pivot role within collaborative projects. SecurIT permitted the following: - 21ollaborat cooperation between ecosystems - to lead to other types of initiatives: other EU funded projects and other types of activities matchmaking members etc. - visibility also at EU level and beyond to collaborate further.

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

Pole SCS	
Exploitation plan: **(Please elaborate on the specific exploitation strategy for your own purpose, and list the different practical indications of this)**	The following assests are the main results that Pôle SCS could exploit beyond SecurIT Gained know-how for the implementation, monitoring and management of cascade funding Cooperation network: developed cluster network on both digital and security domains. The collaboration between security and digital clustrts is a strong part in SecurIT. Visibility: Pôle SCS presented and communicated about SecurIT, during various events, via various media. Moreover via SecurIT, increased visibility of the cluster's activities. Use cases: the challenges and use cases both identified by SecurIT and 22ollabora by the funded SMEs have provided relevant and powerful material for awareness activities on security subjects. Other funding initiatives: Pôle SCS intends to reuse learnings from the project.

L3CE	
Exploitation plan: **(Please elaborate on the specific exploitation strategy for your own purpose, and list the different practical indications of this)**	L3CE operates within an ecosystem where close 22ollaborateon between different stakeholders drives the development and implementation of innovations with the specific focus on Law Enforcement Agencies (LEA). Our activities are centred around practical implementations that remains significant challenge in innovations development path. L3CE will dedicate significant effort to leverage the outputs of SecurIT. This involves offering a service package aimed at facilitating the transition of innovations from LAB to real- life applications by: Providing secure environment for experimentation ELSA assessment Facilitation of demonstrations/end-user's engagement Use case scenario development for testing and validation Trainings As a National Node within the SecureIT ecosystem, L3CE possesses a comprehensive understanding of national LEA challenges faced in the realm of public space protection. Leveraging this expertise, we have initiated the planning process for demonstrating clustered projects like Safe Festivals, AIR-T4S, and CMD, involving collaboration of LT Police, EACTDA and other interested stakeholders. Should these demonstrations prove successful, the Financial Instruments Mapping tool developed by the SecurIT will be utilized to identify new funding mechanisms for advancing maturity and operationalizing the innovations. Furthermore, we planning to utilise a diverse range of communication channels to effectively raise awareness about success stories and achievements

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

LSEC	
Exploitation plan: **(Please elaborate on the specific exploitation strategy for your own purpose, and list the different practical indications of this)**	LSEC – Leaders in Security is a not for profict (vzw) Belgian-based SME, a spin-off of KU Leuven university that was established over 2 decades ago to support knowledge and expertise sharing amongst cybersecurity experts in Belgium and Europe. Today, the organisations operates as a Digital Security Catalyst, facilitating it's original mission of knowledge and expertise sharing in various domains of cybersecurity and making the connection to other sectors and domains such as manufacturing & industry, healthcare, finance & insurance, energy & utilities, transport & logistics, retail & commerce, ICT & media, and more. LSEC is a network of cybersecurity services and solutions providers, research organisations, intermediaries and uses technology innovations to support innovative developments in cybersecurity and with cybersecurity technologies in other domains. The SecurIT exploitation plans for LSEC are the following: - For LSEC as an organisation: o Exploit SecurIT and LSEC brand recognition and European dimension of LSEC with existing and future LSEC stakeholders, European industrial partners and global strategic partners, aiming to result in new collaborations and further expansion of image and branding, getting new customers and industrial collaboration projects and innovative developments o Exploit the SecurIT project and SecurIT results towards the European innovative security development companies seeking for further assistance in going to market or growing within and beyond Europe; showcasing results of support programs, and results of collaboration between companies, showing results of mentoring and demonstrations building – resulting in new collaborative projects, investments and further growth of the results and the ecosystem, showcasing results in Europe and beyond o Exploit SecurIT resulting projects (Demonstrators and Prototypes), using developed technologies to apply into other sectors, domains, developing new collaborations, developing new joint projects, aiming to result in new European deployment activities and exploiting towards end-users, resulting in new interactions with end-users, new joint industrial project developments and deployment of European technologies - For LSEC towards its members and stakeholders : o LSEC Members and stakeholders are organisations and individuals of different industrial sectors, mainly Cybersecurity, but equally critical infrastructures such as finance, energy, telecoms, transport, … LSEC has been, and will continue to exploit the SecurIT results and finding, both from the project level, as well as from the individual projects from Open Call 1 and 2, and their respective participating companies in answering some of the specific needs addressed by the companies (eg ports, law enforcement, SMEs, …), addressing new challenges coming from changes in regulatory landscapes (NIS2, NIS, DORA, Cyber Resilience Act, Cyber Solidarity Act, Medical Devices Regulations, …) – to which many of the stakeholders (including also non-profit industry associations) have to try to answer. The exploitation by LSEC is for instance by means of

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

	addressing some regulatory topics (eg NIS2) and having the SecurIT-participants present their solutions, or immediately go to an installation and development. ○ LSEC stakeholders include private equity investors with a focus on new technologies, including cybersecurity and security. LSEC will continue to exploit the SecurIT results of prototypes and demonstrators, in the first place by supporting a set of companies with continuous growth potential and investor interest, both from a financial as well as from a corporate investment perspective. This type of exploitation leverages the results from SecurIT as a project, in getting more attention, a faster commercial demonstrator or technology proof of concept, allowing for lowering the barrier for additional capital needs and investments taking place. Examples are companies such as Lupasafe, Diri and others. ○ Thanks to the LSEC exploitation activities, including the setup of direct interactions with both LSEC Members (Cybersecurity experts, including advisory, system integrators, …) additional business relations are being created, in the forms of partnerships, collaborations, reselling agreements, … following the introductions and exploitation efforts by LSEC. - Towards Open Call participants (both the ones that were able to execute Protoypes and Demonstrators and the ones that were not selected): ○ Exploitation of the SecurIT results to stimulate others to participate in the second and other potential Open Calls (from other – future projects – such as the Digital Europe Program CYSSDE – project, organizing Open Calls for the deployment of cybersecurity technologies and regulation; CYSSDE is also focusing on Critical Infrastructures, and allows for pentesting. These activities will be exploiting further the developments of SecurIT and SecurIT Open Call participants; but more importantly will also reach out to exploit the Open Call participants to participate again in other calls. ○ Exploitation of SecurIT results to support the further development of the participants, both helping them using the right information from SecurIT results to further shape their go-to-market, and potentially new product innovations.

CenSec	
Exploitation plan: **(Please elaborate on the specific exploitation strategy for your own purpose, and list the different practical indications of this)**	The following aspects describes how CenSec has exploited the results of the SecurIT project: - As the national Danish cluster organisation for the defence, space and security industries in Denmark, CenSec has throughout the project period informed our members and other relevant stakeholders about the project, especially when it comes to the funding opportunities in order to attract more Danish and Nordic SMEs to apply for the two open calls. This experience has been valuable and meant an increased number of applications from the Nordics countries applying for open call 2. - The SecurIT project has further been described and shared on our own website, in order to share insights on the project with our members and wider ecosystem

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

	- The SecurIT project architecture has worked when it comes to defining domains and challenges, and involving end-users, and this experience will be reuse going forward. - Insights into cascade funding mechanisms has been very valuable - As responsible for the WP4 on monitoring and impact assessment, CenSec has gained great insights and experience with follow up mechanisms and procedures and have utilized this experience on other projects with great results. - The good collaboration and diversity in skills and experience among the other SecurIT consortium partners have meant an increased insights into various technical topics, but also of project organizational character, and have fertilized the grounds for a closer and stronger collaboration going forward, hopefully with the concrete results of further project collaboration opportunities among the partners. - The initiative by L3CE of the project clustering approach, has created a new way of operationalizing the process and dialogue between projects and end-users as it has made it more accessible for end-users to engage as they get more at once with less efforts. The initiative is inspirational and is something CenSec will try to roll out in a national context with local authorities. - Together, all the learnings obtained during the SecurIT project will be utilized in other projects and initiatives going forward

Security Delta HSD	
Exploitation plan: **(Please elaborate on the specific exploitation strategy for your own purpose, and list the different practical indications of this)**	Our exploitation is on the one hand aimed at the projects from this innovation programme. On the other hand, its' aim is to connect other Dutch viable research and innovation projects with other funding opportunities. We are hoping to help the projects be sustainable for the future, so their results will be oriented long-term. We will try to do so by connecting the different parties to our network of over 275+ partners. By connecting them to different stakeholders from the Public/Private/Government sector (triple helix) we hope to provide them with partners to help exploit their solutions. We have already introduced the SAFE Festivals team into the Dutch AI Coalition (NLAIC) and added one of their project partners (who is involved with the University of Eindhoven/Tilburg) to our working group Safety Peace and Justice. By doing so, they gain access to our network in the AI domain. Furthermore, we connected the SAFE Festivals team to several other stakeholders/partners of ours and presented them possible future collaborations and business opportunities (for example; connection to Argaleo B.V. Digital Twin and Crowd Safety Manager). Finally, by collaborating with SecureIT Consortium partners, we hope to better help the participating projects. For example, L3CE introduced the thought of clustering projects together, this will help external stakeholders get a better overview of the different solutions provided by the participating companies in the SecurIT project. During the SecureIT programme we have informed our partners and ecosystem of the opportunities within the SecureIT programme as well as on other relevant European research and innovation funds.

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

	The learnings and cooperation within the project and with our international partners have built a solid system on which we can expand in the years to come. For example, we would be able to connect Dutch SME's to SME's in other countries in their international research and innovation goals.

FundingBox	
Exploitation plan: **(Please elaborate on the specific exploitation strategy for your own purpose, and list the different practical indications of this)**	When managing open calls, FundingBox not only provides project-specific strategies to attract the right types of applicants, but also strives to address long-term goals of the project and its own development and growth goals. In this sense, when users register on the FundingBox platform to apply to open calls, they have the option to sign up to receive further funding opportunities emails and alerts in the future. The applicants are then added to a database of potential future applicants in other open calls, expressions of interest or as FundingBox services users.

Systematic	
Exploitation plan: **(Please elaborate on the specific exploitation strategy for your own purpose, and list the different practical indications of this)**	Systematic Deep Tech cluster will as a follow up strategy enable its members developing security solutions to have access to a wide network of potential European partners (e.g. project partners but also Ambassador Clusters) to engage commercial or R&D partnerships. As WP5 leader, the methodology developed to disseminate project information has been successful, reaching out to countries not represented in the consortium, and will be reapplied to similar initiatives in other EU-funded projects. In relation to the work carried out in other Work Packages, the cluster will draw from and add to its portfolio its experience in : designing and applying a monitoring and validation method on cascade funded projects (WP4), organising matchmaking sessions and information webinars on open calls (WP3), engaging experts from the security sector and identify technological gaps and challenges (WP2). As an addition to these elements, further projects will be submitted towards the support of innovative security SMEs in their R&D and growth activities, with and without SecurIT subgranted SMEs that are part of Systematic's network. Systematic is committed to sustain the SecurIT community that was built after the project's end by continuously animating its social media channels and website.

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

Section 4.3 - Projects

In this section the 42 projects funded by the SecurIT project are included to embody the sustainability of the SecurIT project and to display the outcome of their delivered solutions.

OPEN CALL 1 PROJECTS:

ARSP	
Involved Companies:	LMAD (France), GIM Robotics (Finland) & LANACCESS TELECOM (Spain)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	LMAD (France) is building a solution to manage all security missions and robots from a single platform. This robot & mission manager agnostic platform will help security companies to manage various robots at various sites for various missions on a single platform. First step of that platform and the team is to integrate & deploy a robotic solution with a surveillance AI managed by the first version of that platform. LANACESS (Spain) provides the video surveillance & detection capacities (hardware, AI) GIM (Finland) is providing its capacities software/hardware regarding the need for autonomous navigation robot

BIM2SIM	
Involved Companies:	APEX Solutions (France) & Scott Brownrigg Limited (United Kingdom)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 6 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	BIM2SIM has developed a prototype digital technology brick to automatically extract security-and safety-related information from standard building description file formats. Building Information Modelling (BIM) is becoming a collaborative must-have for architects, urban planners and in the construction industry. Standard file formats are readily available, and could be extended to provided security-related information as well. A final processing method coded in the Unreal game engine has been developed by APEX solutions in order to perform intrusion simulations, taking the advantage of existing non-playing characters (NPCs) AIs to model the behaviour of “red team” and “blue team” agents.

C-Shield	
Involved Companies:	ITTI Sp. Z o.o (Poland) & AIRSENSE Analytics GmbH (Germany)

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

Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: Domain #3 - Public Space protection
Description of the delivered Product:	The C-SHIELD project is dedicated to the development of an innovative system for chemical hazard detection. The solution is based on two different detection technologies, namely Ion Mobility Spectroscopy (IMS) and Flame Photometric Detection (FPD). The two commercially available sensors are combined via a hardware unit called a Sensor Node, which is a point detector and can easily be carried by one-person and operated on the move. During the first 6 months of the project, the team of engineers has prepared two dedicated translators, one for each sensor. The translators are responsible for acquiring sensor data, unification of the data into one format, data pre-processing and analysis. During the project lifecycle, all core requirements have been met and the final version of the C-SHIELD system consists of: • dedicated translators for each sensor, • the Sensor Node which is the heart of the system and serves as internal data processing unit, • the data fusion component enabling the system to classify and identify data from different sensors

Cyber Trapper	
Involved Companies:	Datatek doo Beograd (Serbia), ADVANCED SECURITY TECHNOLOGIES (Greece) & Avantools (Greece)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 7 Domain: #1 Sensitive Infrastructure Protection
Description of the delivered Product:	Our solution is an independent device based on AI that can protect users from attacks from the Internet. With Cyber Trapper IoT cloning and AI based Central Threat Intelligence, we are capable of detecting even unknown attacks, never seen before - with the very first attack attempt against cloned device, the whole group will get immunity against that type of attack and that specific attacker. Institute Mihailo Pupin Belgrade (as the leading Serbian R&D institution in information and communication technologies (ICT), as well as the biggest and the oldest ICT institute in Southeastern Europe with mr Veljko Vucurevic, deputy director) will be supporting our project in the means of testing the solution and later promoting it for broader use and project achievement which is the first place collective immunity.

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

CyberSec2SME	
Involved Companies:	Skopos Security Labs B.V. (Netherlands) & Beia GmbH (Austria)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	The project aims to secure the supply chain of the Port of Galati in Romania, a crucial component of the Romanian economy that handles over 10 million tonnes of cargo each year. The implementation of Lupasafe software on partner BeiA GmbH systems is a key part of the project. Lupasafe is a cyber security risk management platform that provides continuous monitoring of the supply chain, identifying any vulnerabilities or breaches in credentials. In conclusion, cyber threats know no boundaries, and it is essential to be proactive in managing these risks. Continuous monitoring of cyber security risks across the supply chain of suppliers is crucial for protecting critical infrastructure from devastating cyber attacks. By implementing a comprehensive cyber security strategy that includes continuous monitoring of cyber security risks, businesses can identify and mitigate potential risks before they become a problem, protect their operations, and ensure the safety of the wider community. The CyberSec2SME project is an excellent example of how businesses can protect their operations and the community from the catastrophic effects of cyber attacks.

DIAC	
Involved Companies:	Asvin GmbH (Germany) & Odin Solutions (Spain)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	Access control tool; In the DIAC Project, we have developed a solution that aims to solve most of the problems that current access control systems have, using innovative solutions and avoiding direct user interaction with access control through the Disposable Identity Framework. A Disposable Identity is a contextual and temporary identity, limited in terms of scope, time, location allowing end users to show specific and limited information/credentials to validate for a service, in our case, access control of the building. The disposable identify element of our solution gives an edge over existing access control solution. The technical architecture consists of Access Control Terminal, DID Mobile App and DID Platform. The DID App, developed using angular framework, facilitates user login, registration and access management. The Access Control Terminal validates Disposable Identity using the DID platform. Disposable identity generation & validation, user management

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

	and access permission management services are provided by the DID platform. Disposable Identity is a contextual and temporary identity, limited in terms of scope, time, location allowing end users to show specific and limited information/credentials to validate for a service, in our case, access control of the building. The solution was validated against the defined key performance indicators with 3 demonstrations, in asvin lab, OdinS office and Murcia University building.

Digital Forensics Cloud Lab SaaS	
Involved Companies:	AVIAN Digital Forensics (Denmark), Luftborn Aps (Denmark) & Mithril Security (France)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 9 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	During the project, Avian Cloud has evolved from a concept and a desire to meet the next-era requirements to Digital Forensics and eDiscovery labs as cloud adoption evolves into a real product ready to make a great impact in the industry. Now, we offer the world's first one-click Digital Investigations cloud platform that enables government and enterprises to use their favourite Digital Investigations and eDiscovery tools in the cloud 10-100x faster than ever before. A highly secure platform offering isolated tenants per subscription and unique Confidential Computing options. Automatic self-service provisioning in minutes to enable, manage and automate case tasks using best-of-breed industry technologies within Digital Forensics, Incident Response and eDiscovery.

FusionSec	
Involved Companies:	NUUK Technologies SL. (Spain) & UAB Iterato (Lithuania)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domains: #2 - Disaster Resilience & #3 - Public Spaces protection.
Description of the delivered Product:	With the help of SecurIT project we were able to built the IoT platform that helps to create a smoother collaboration between public and private forces during mass events. It significantly shortens the communication chain. FusionSec provides a framework for the planning of events, by allowing the workflow, task planning and location into a map of agents in different layers, will allow real-time (RT) tracking of team members & will enable the visualization in virtual rooms of the multimedia content relevant to all the event (drones, CCTV cameras, bodyworn cameras,

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

	smartphone cameras, IoT sensors, etc) to both operative and tactical resources (on-site through smartphones/tablets or command posts) as well as strategic resources (crisis rooms). The testimonies of our users attest to the unmistakable advantages of FusionSec. It's a testament to amplified efficiency, and heightened productivity for security forces collaborating in public mass events. The Lithuanian police and Alytus County police are particularly enthusiastic about FusionSec, recognizing its potential to revolutionize event security, streamline communication and bolster situational comprehension. Furthermore, the municipality representatives have commended FusionSec for its seamless integration with their operations, enabling them to promptly report incidents like traffic jams through the FusionSec mobile app. The immediate visibility of these incidents to the police officers ensures swift action and resolution.

Helia	
Involved Companies:	AzuriA (France) & Allsop Helikites LTD. (United Kingdom)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 7 Domain: #2 - Disaster Resilience
Description of the delivered Product:	HeliA is a versatile aerostat lifting a multispectral camera with embedded AI for real time detection and alert of hazards in full autonomy. The demonstration case is the wild fires disaster, by alerting the operators, then supporting the firemen and surveying the fire restart.

IDEAS	
Involved Companies:	Cetrac.io (France), Cyberium SAS (France) & Protech-X (Denmark)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	Firewalls today provide insufficient security for industrial networks that are extremely vulnerable to cyber-attacks. Pure hardware-based system enabling 2-way communicationsIDEAS enables full bi-directional communications between systems on the IT and OT networks (SCADA, DCS, RTU..), and provides best in-class protection against outsider network attacks.

INSIOTA	
Involved Companies:	Defora Networks (Germany), 4.0 technologies EU s.r.o (Czech Republic) & CKIN s.r.l (Italy)

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

Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 7 Domain: #1 – Sensitive Infrastructure protection
Description of the delivered Product:	INSIOTA provides an integrated platform, automating a range of IT-Security tests on computer systems and networks. The constant tests help ensure any gap is detected and can be mitigated before a real attacker can abuse them. While the underlying infrastructure of the platform is environment- agnostic, the focus of the project is on systems part of the “Internet of Things.” (IoT) The target environment for the INSIoTA testbed was located in the public space of a European city, monitoring the quality of the environment in a “Smart Street.” Criteria like traffic information and air quality were critical in this context, as the street contained one of few bridges in a city of 100.000 inhabitants, connecting a Police Department to a Fire Brigade on either side. The INSIoTA platform was extended as a solution for the offline analysis of firmware images for these sensors, in order to help protect the infrastructure deployed in case of physical compromise of the sensors deployed publicly. As a result of this project the sensors for this environment can be analysed for the presence of security vulnerabilities prior to deployment, thereby streamlining quality control and strengthening the security posture without requiring additional manpower

Kaleidoscope	
Involved Companies:	Level 7 (Italy), Grifonline S.r.l. (Italy) & Wireless Connect Ltd. (Ireland)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 7 Domains: #1 Sensitive Infrastructure protection & #3 - Public Spaces protection
Description of the delivered Product:	The Kaleidoscope platform has been developed by three European ISPs with a large experience in telecommunications and cybersecurity. The goal of the Kaleidoscope project is to provide a future-proof architecture that is able to quickly evolve and adapt to more complex DDoS attacks. The SecurIT open call #1 has permitted to design the whole architecture and to discover the technological challenges as well as establish a long-term path that will enrich the Kaleidoscope platform with new features and more complex traffic analysis modules. At the end of the Kaleidoscope project, the platform has reached a good level of maturity and it will be offered in the near future to European telecom/ISP, service providers, software companies

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

	and system integrators. The Kaleidoscope platform is able to scale, thanks to its modular design and the future research will enhance it with AI capabilities. The Kaleidoscope consortium also welcomes companies that want to investigate on how the Kaleidoscope platform can help them in defending their assets (e.g. services, critical infrastructure, etc.) from DDoS attacks

PIM-SAT-M	
Involved Companies:	GeoKinesia SL (Spain) & Exponential Space Holding S.r.l. (Italy)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #2 - Disaster Resilience
Description of the delivered Product:	Within the scope of the project, we developed an AI enabled, platform-based remote sensing tool, which provides reliable and sufficient information on the area or object stability. The underlying technology is InSAR, the key advantages are a) better coverage of large areas as well as “thin” infrastructures b) automatically generated early warnings c) web-based platform and dashboard. We also were able to showcase the solution. This is a highly cost effective and convenient tool, which equip our customers with valuable and near real time information on the area or object stability and automatic early warnings on a web-based platform.

RASAD	
Involved Companies:	Co-dex.eu bvba (Belgium) & Wallix sa (France)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 9 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	Belgian-based NoCode-X and French Wallix join 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 developmet without writing a single line of code. Wallix is European leader in Identity and Access Management and authentication technologies. The RASAD-project will be developed with the support of the EC via the European SecurIT- project. Using RASAD, organizations can easily digitize & automate any process with tremendous speed and a guaranteed level of cybersecurity. Offering both a reduction in build-cost as well as a higher level of quality compared to traditional development. Next to authentication & authorization the platform is smart enough to decide whether to impose security measures such as encryption on data at rest, auditing logs, blocking unauthenticated access, and much more.

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

ROGID	
Involved Companies:	Lorenz Technology aps (Denmark) & Foxstream S.A.S. (France)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure protection & #2 - Disaster Resilience
Description of the delivered Product:	The ROGID project demonstrated how robot guards can add value to high-level security operations for companies when detecting intruders. In the ROGID project, the French video analytics firm Foxstream (FS) and the European robotics company Drone Volt(DV) will develop a robot guard solution for the Hans Christian Andersen Airport (HCAA) in Odense. Having HCAA as an end-user in the project, ROGID addresses specifically challenge 4: "Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions". HCAA is a colocated active airport and an Uncrewed Aerial System (UAS) Test Center, and hence, the area requires high-level security. HCAA is interested in testing robots as part of their security operations and would like robots to detect intruders on the perimeter. HCAA is hoping to eventually replace manual perimeter patrols by car with robots because HCAA believes a robotic solution will be more effective in spotting intruders at night than human guards due to vision impairments. A robotic solution would also have less negative impact on the environment.

SecuRAIL	
Involved Companies:	FOKUS Tech d.o.o. (Slovenia) & ALTPRO d.o.o. (Croatia)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 6 Domain: #3 - Public Spaces protection
Description of the delivered Product:	The system provides reliable detection of dangerous situations at railway stations. It automatically detects passengers or objects that fall from the platform onto the track, suspend the traffic and alerts the security staff. New features can be added, such as "trap and drag" accident detection, which prevents a train from dragging behind a passenger or other object grabbed by a train door. The system is particularly well-suited for lines with autonomous trains and stations where installing platform screen doors may not be feasible.

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

SECUVERSE	
Involved Companies:	WeAr S.r.l. (Italy) & Exwayz SAS (France)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 7 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	Secuverse is an autonomous inspection and monitoring system, based on an immersive Metaverse and Artificial Intelligence platform that includes a digital-twin model of a target facility, a LIDAR scanner, an Automated Guided Vehicle (AGV), and AI algorithms for intruder detection. Our goal is to develop an autonomous robotic agent that can patrol sensitive infrastructure, monitoring possible intruders and anomalies, and represent them in the digital twin model of the facility. Remote operators can inspect this rich data ecosystem through a metaverse immersive interface, in order to visualise threats and intruders detected through an AGV-mounted LIDAR scanner and perform mission-control task by communicating with robotic agent on-field.

ShowID	
Involved Companies:	JanusID B.V. (Netherlands) & Covr Security AB (Sweden)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #1 - Sensitive infrastructure protection
Description of the delivered Product:	Access control tool; We have developed the ShowID app and customer portal that provides the universal company badge enabling instant visitor authorization at controlled facilities, ensuring that no one and nothing that enters poses a security risk. The ShowID app supports 1) ID verification, biometry and liveness detection (to ensure it is the right person) and 2) secure electronic ticketing and cryptography (to ensure it is this person's authorization and not someone else's). The ShowID portal manages all transactional data and provides user centric identity control (to ensure personal and transactional data is correct, safe, and properly managed). ShowID runs on commonly available devices: standard smartphones. tablets and desktops. No need to purchase, install and maintain specific hardware

SLOPEGUARD	
Involved Companies:	Techcom Srl (Italy) & Sparkd Ltd. (Ireland)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #2 - Disaster Resilience

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

Description of the delivered Product:	As part of the SlopeGuard project, aimed at predicting shallow landslides, the consortium completed the conception, design and construction of the sensor that will be used to collect the data. This is a flexible but durable rod, which will be implanted in the ground at a depth of approximately 2m. The data collected by its accelerometers and soil moisture sensor will be transmitted to a web portal where it will be monitored and analysed. At the same time, the development of machine learning algorithms for anomalies detection and - in the future - to predict shallow landslides has been completed. The data collected by the SlopeGuard sensors, together with Techcom landslide dataset have been used for the development and refinement of the algorithms.

VASCREEN	
Involved Companies:	Ezako (France) & Mion Technologies (Spain)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 6 Domain: #1 - Sensitive Infrastructure protection
Description of the delivered Product:	VASCREEN technology allows the detection of potential threats inside luggage or other goods in checkpoints by the analysis of the vapors around. VASCREEN allows the scan of one item (luggage) in less than 1 min based on a radically novel Multidetector Differential Mobility Analyzer (MDMA), coupled with an automatic air sampling system supported by Deep Learning (DL) recognition algorithms. This new technology has some advantages over the SoA: i) it does not require the removal of electrical items from the luggage, ii) it is much cheaper (<0.1€ per item), iii) it allows the detection of chemical, biological and explosive threats, including new threats, iv) the result does not depend on the interpretation of one operator (automatic), v) it is not intrusive, vi) the FAR (False Alarm Rate) is much lower, and vii) the DR (Detection Rate) is much higher

ZENITH	
Involved Companies:	EDICIA (France) & DEVERYWARE (France)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #3 – Public Spaces protection
Description of the delivered Product:	EDICIA and CHAPSVISION launched in mid-September 2022 the #ZENITH (ZEN Information TecHnology) project, supported by the European project SecurIT Innosup. After 12 months of work, thanks to CHAPSVISION expertise in semantic analysis and to Edicia knowledge of city security, we can extract geo-chronolocalized security relative events from Twitter. The #ZENITH urban security platform aims to detect weak signals from any type of textual data, including social networks, to help cities better anticipate imminent risk situations, and improve the resilience of cities.

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

OPEN CALL 2 PROJECTS:

AIA GUARD	
Involved Companies:	Datrix SPA (Italy), Rheasoft (Denmark)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 9 Domain: #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	AIA Guard is an end-to-end solution that automatically analyses your entire machine learning workflow with particular attention to data poisoning, model interpretability, data leakage and adversarial machine learning, designed for data scientist that would use AIA Guard to receive adversarial samples and feedback to handle the models they are implemented on intending to use. AIA Guard is a project developed by Datrix with the support of Rheasoft. Datrix is a tech company group specialised in Augmented Analytics and Machine Learning, listed on Euronext Growth Milan. Rheasoft is an IT development company operating within a wide range of IT aspects, including application development, data migration, complex integrations, and cloud development. The solution is composed of three modules: - Adversarial Attacks Defence: focuses on defending against adversarial attacks on machine learning models, improving the robustness of AI systems against such attacks. - Data Anonymization and Privacy Preservation: focuses on protecting sensitive information and privacy within the AI ecosystem. By anonymizing data used for training and inference, the solution ensures compliance with privacy regulations and minimises the risk of data breaches. - Interpretability for AI Transparency: focuses on enhancing the interpretability of AI models, providing insights into their decision-making processes, allowing users to better understand and trust the model outputs thus helping the adoption of AI technologies.

AI DISASTER EMERGENCY COM	
Involved Companies:	HighWind (France), GAGDPR (Greece)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #2 – Disaster Resilience
Description of the delivered Product:	AI-enhanced Disaster communication solution for the population. Plugged on the EU-ALERT emergency text-message system, it emulates through smartphones' web browsers, an emergency communication interface called "Disaster Mode", capable to signal position & situation, send pictures and have an AI-sorting of the emergency sent to a digital map "HQ Interface" available for local authorities and emergency dispatchers. Designed to reduce emergency call centers' congestion during large scale scenarios, the solution immediately identify most critical

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

	persons with a patented AI algorithm, crossing the analysis of traumas, context and emotions in order to assess the nature and severity of a situation. Fully GDPR compliant, the solution requires no installation and can be used by both the population and authorities by clicking an URL web-link.

AIRA	
Involved Companies:	ISSP (Poland), ENKID Global (Estonia)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5/6 TRL Level end: 8/9 Domain: #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	AIRA, an innovative platform aimed to automate evidence-based security risk assessments. As a SaaS platform AIRA enhances investigation accuracy, reduces time, and increases productivity in proactive risk discovery and breach response. With AIRA software, organizations can respond to cyberattacks, conduct full-scale compromise assessments in less than 10 days, and discover initial findings in just 1 hour. AIRA is a single tool that streamlines this process with automated artifact collection and data enrichment, built-in static and dynamic analysis, pattern comparison, report generation, and risk scoring. This enables the investigation to be completed in a matter of hours with automation or in a matter of days with the analyst's involvement. While the industry average time is nearly 2 months.

AIR-T4S	
Involved Companies:	Thridium (UK), Robosurvey Ltd (Greece)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8/9 Domain: #3 - Public Spaces protection
Description of the delivered Product:	AIR-T4S blends the on-the-ground excellence of T4S to fuse in real-time all the necessary information regarding the management of crowd safety and the operational supremacy stemming from the aerial support of the AIROUS platform. Enhanced crowd distribution, dynamic evacuation routing, real-time visualisations and optimal resource planning and management, will be provided through the platform's common operational picture, events management, task allocation and the security crew mobile app. The integrated AIR-T4S platform as a public spaces threat detection and response management platform delivering increased preparedness against different types of threats (terrestrial and aerial – terrorism acts, intruders) and support the enhanced crowd safety during Major Events.

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

CMD	
Involved Companies:	Neuroo (France), MA2 (France)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #3 - Public Spaces protection and #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	The CMD project team made of neuroo and MA2 members is proud today, to release one of the most advanced, production-ready video-based public panic detection feature, completing our set of events' detection and alerting functionalities. Panic can lead to stampedes, trampling, or crushes as people attempt to flee or find safety, resulting in injuries or fatalities. This new feature can detect panic within a crowd in real time and enable security personnel to take proactive responses, within seconds.

DISCGRID	
Involved Companies:	Internet Identity, Security and Privacy Solutions P.C. (ExcID) (Greece), Guardtime OÜ (Estonia)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	DISCGRID's goal is to enhance the security of smart-grid firmware supply chain. The main building block of DISCGRID approach is an append-only, immutable, Transparency Registry where information about software artifacts, related to the released firmware, is recorded. This information can then be used to verify the validity of those artifacts. An important property of the Transparency Service is that it is auditable, hence at any time a third-party auditor can verify that information has not been removed or modified. Additionally, an auditor can notify firmware providers or DSOs for new entries in the registry: these entries may correspond to legitimate activities or to an ongoing attack. DISCGRID implements a transparency service, which includes a registry, enhanced with Guardtime's KSI blockchain. Furthermore, it develops tools for firmware providers to securely store their artifacts signing keys, and for DSOs to easily validate the security properties of received firmware.

ERMINE	
Involved Companies:	Phasegrowth (Estonia), Ecording (Turkey)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 7 Domain: #2 – Disaster Resilience

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

Description of the delivered Product:	The ERMINE project has successfully navigated initial delays with disaster management authorities in Bulgaria, Turkey, and Estonia, achieving key deliverables across various work packages. A diverse set of representatives of the domestic disaster management authorities from the three countries were engaged, from surveying their needs to consulting them in the development of the prototype, asking them to validate the models for the disaster propagation and human reactions to calamities. Extensive research has informed the development of the ERMINE architecture, focusing on human behavior modeling in disaster scenarios. Work on natural hazard detection using AI and geospatial data is progressing well, with the aim of developing a multi-hazard digital twin. The project also includes an effective outreach plan, promoting awareness and engagement through various platforms. Despite early challenges, the project remains on track and is delivering promising results.

ERRATA	
Involved Companies:	INSIGHIO (Greece), Vertliner (Greece), APOGEO Space (Italy)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #2 – Disaster Resilience
Description of the delivered Product:	ERRATA is an automated UAV and Satellite empowered Sensing platform operating in confined hazardous areas, like storage facilities, mines, or tunnels.

EV SAFE	
Involved Companies:	Parity Platform P.C. (Greece), Grid One Ltd (Croatia), Technomat SA (Greece)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	EV Safe proposal aims to deploy interoperable software tools and services aimed at Electric Vehicle Charge Point Operators (CPOs) to help them detect and remediate attacks against Electric Vehicle Charging Station (EVCS) infrastructure. EVSC Infrastructure is exposed to significant cyber risks that can affect the functioning of essential parts of the economy and transportation sector.

FLOWGUARD	
Involved Companies:	AirTrace Technologies SL (Spain), Neoradix Smartgreen, SL (Spain)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6

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

	TRL Level end: 9 Domain: #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	The FLOWGUARD project marks a pivotal advancement in water treatment security, reaching its mid-term with remarkable achievements. We've successfully gathered and refined extensive historical data on water networks, setting a robust foundation for our cutting-edge analysis. Our team has pioneered the integration of Graph Neural Network (GNN) algorithms to map the intricate network of water distribution, ensuring high fidelity in modeling. Notably, we've developed a baseline model employing XGBoost, which has already demonstrated promising potential in detecting anomalies and that will serve as a comparing standpoint for our graph neural networks (GNN) developments. Our current efforts are concentrated on fine-tuning the GNN's performance, leveraging MLOps strategies to optimize its predictive accuracy. Throughout the process, our milestones have been meticulously documented via the Weights and Biases platform, ensuring transparent progress tracking. Our work not only enhances the security of critical infrastructures like water treament plants but also sets a new standard for utilizing AI in public utility monitoring. Stay tuned for further updates as we continue to push the boundaries of technology for the safety and security of our water systems and the society as a whole.

INVISIBUBL	
Involved Companies:	Snowpack (France), Bubl B.V. (Netherlands)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure Protection and #3 - Public Spaces protection
Description of the delivered Product:	Develop a novel integrated user-to-provider beyond-trust cloud service by integrating Bubl.cloud novel approach to cloud data storage with Snowpack's SNO invisibility overlay network unique properties. As a result, Bubl.cloud will not be the trusted third party for its users' cryptographic keys and Bubl attack surface will get cloaked.

NOCCRO	
Involved Companies:	RIVAGES Waves'n See (France), Viewsurf (France), Salpicos Contagiantes Unipessoal Lda (Beachcam MEO) (Portugal)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 6/7 Domain: #2 – Disaster Resilience
Description of the delivered Product:	The NOCCRO project addresses several technical challenges to implement the first European network of coastal webcams. So far, French and Portuguese manage to gather video flux from different beach and surf cams all along the European Atlantic coast. A special care has been taken

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

	in the sites selection in order to obtain a wild range of beach types in terms of sediments, coastal morphology, waves characteristics, etc. The main challenge was to ensure a robust data acquisition system while maintaining a good quality of views and images. We are now testing the capacity of our IT infrastructure to scale at network level.

OPTIMIZ NETWORK	
Involved Companies:	OPTIMIZ NETWORK (France), Zariot (Cellulys IOT, Ireland)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	The OPTIMIZ NETWORK - ZARIOT project aims to deploy a solution for securing, monitoring and optimizing telecom infrastructures. These infrastructures are more than ever very sensitive places. Thousands of network subscribers can be impacted in the event of voluntary or involuntary damage to a physical element of the network and the risks for the security and confidentiality of data are numerous. We have therefore designed a solution by exploiting the new technologies of the IoT (Internet Of Things) coupled with our supervision platform. Thanks to this we are able to optimize the operation of the network by transmitting to the manager, all the useful and relevant information thanks to an alert system (opening of a door, presence of water, fall of a pole, etc.). We are also going further by equipping the most important technical points (cabinets and shelters) with an electronic half-cylinder to ensure access control. To ensure secure IoT communication and data exchange with our servers and database, we work closely with our partner ZARIOT. In addition to offering international network coverage, we can guarantee our customers total security since communications can be encrypted between ZARIOT and Optimiz-Network and have centralized management.

ReBriNet – Resilience Bridge Net	
Involved Companies:	Social Tech Projects ApS (Denmark), ConnectingBrains (Spain)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 7/8 Domain: #2 – Disaster Resilience
Description of the delivered Product:	ReBriNet, “Resilience Bridge Net“, is a cutting-edge technology designed to help the coordination and decision-making of first and second responders by providing during all the operation real-time information directly from local communities affected by the disaster. Local communities will be able to report crucial information through a digital web module that can be integrated in existing web/mobile emergency solutions that enhances cross-communication capabilities with inclusive and effective communication.

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

RESPO-C	
Involved Companies:	Massive Dynamic Sweden AB (Sweden), MHK Consulting (UK)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #2 – Disaster Resilience
Description of the delivered Product:	Enhance Citizen Engagement App (CEA) -> By providing real-time information about raging fires and how to prevent and react to wildfires, citizens can act more engaged and responsible, which consequently aids volunteering groups in fighting fires.

RS2DG	
Involved Companies:	GridData GmbH (Germany), ResilTech S.R.L (Italy)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 8 Domain: #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	RS2DG aims to integrate, enhance and demonstrate a previously prototyped software solution, called Security & Resilience (S&R) component, that will detect cybersecurity threats as well as anomalies in the electrical measurements.

SAFE-FESTIVALS	
Involved Companies:	STAM S.R.L. (Italy), D-Visor B.V. (Netherlands), CNTRL B.V. (Netherlands)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 6 TRL Level end: 8 Domain: #3 - Public Spaces protection
Description of the delivered Product:	SAFE-FESTIVALS will deliver an engaging simulation platform based on the Unity gaming engine and framework, for organizers, municipalities and security actors of festivals and crowded events in (semi-) public spaces to develop security strategies through collaborative immersive training

SERVAL MANAGEMENT	
Involved Companies:	Global Smart Rescue (France), Kalisio (France), Prendoquota (Italty)
Type of solution (prototype/demonstrator):	Demonstrator
TRL-Level + Domain:	TRL Level start: 7 TRL Level end: 9

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

	Domain: #2 – Disaster Resilience and #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	To address the issue of disaster resilience the three respective European companies GSR, Kalisio and Prendoquota are offering a secure demonstration of a hardware and software system called ServAL Management to help improve response to crises and technological disasters. Notably, it first enables the acquisition and analysis of environmental measures, and secondly provides operational teams in the field with the means to optimise the environmental investigations strategy. Last but not least, the system is easily deployable in a timeframe compatible with operational requirements during a disaster. Kalisio is taking care of the integration of the data acquired by GSR's Little Alert Boxes that are secured by Prendoquota's Blockchain technology.

SMART DIRI	
Involved Companies:	Diri AS (Norway), Homesourcing AS (Norway)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 7 Domain: #1 - Sensitive Infrastructure Protection
Description of the delivered Product:	Smart Diri: Revolutionizing Cyber Risk Management for a Safer Future with decision support automation. This project cracks open cybersecurity for non-experts, empowering society to manage risks and protect social stability. Diri is a centralized GRC software solution that identifies, assesses, andresponds to cyber risks. It enhances disaster resilience and optimizes prediction of interconnected infrastructure risks. The goal of this project is to prototype machine learning for major improvements within cyber security. This innovation will save time, improve quality, and provide crucial knowledge for cyber resilience. The project consortium consists of the Norwgian companies Diri AS and Homesourcing AS. Where Diri AS pioneers state of the art research and development for machine learning in cyber risk management. Homesourcing AS contributes software development expertise know- how for the creation of user-centric solutions ensuring Smart Diri's alignment with real-world needs and opportunities.

SYLVIACARE	
Involved Companies:	SYLVIACARE (France), TIMBTRACK (Belgium)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 6 Domain: #2 – Disaster Resilience
Description of the delivered Product:	The SYLVIACARE project mainly involves specific and consequent software development concerning sensors, communication network, edge computing, web interface.

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

	The two members of the consortium, SYLVIACARE and TIMBTRACK, worked hard to build detailed specifications that are key success materials for an efficient software development process and to mitigate the risks of failure during the integration part of the project: make all the equipment to perfectly communicate between each other. The software development process has then been launched in December by each team. TIMBTRACK analysis on the communication interface has been done and the software development phase is initiated to reach a first version in February.

WUI-SECURE	
Involved Companies:	ATRISC (France), Tecnosylva (Spain)
Type of solution (prototype/demonstrator):	Prototype
TRL-Level + Domain:	TRL Level start: 5 TRL Level end: 7 Domain: #2 – Disaster Resilience
Description of the delivered Product:	The exposure and vulnerability of communities at the wildland-urban interface (WUI) is increasing as we see a significant rise in adverse weather conditions and wildfire activity. Communities and built areas in these zones where human activity and wild vegetation intermingle face a greater risk of being negatively impacted by fire events. WUI-Secure will be an effective modelling tool that incorporates both wildfire propagation modelling with building vulnerability and risk assessment. This tool, based on expert knowledge, will integrate information on wildlife behaviour and WUI vulnerability to identify the most-vulnerable zones and at- risk assets of a community at the time of a wildfire event. It will provide valuable information for fire services, first responders, industry, and other key decision makers, as well as encourage better protective and preventative action from local authorities and community members.

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

Section 5 - Impact Assessment

In this section the assessment of the impact of the SecurIT project will be evaluated. Impact is evaluated in 2 fields; increase of TRL level from the 42 projects and by exploitation and sustainability section in Final Report.

The TRL Level increase is a valuable method of assessing impact, as the SecurIT project has helped the project to achieve better levels with their solution. The sustainability and exploitation sections are good measurements of impact because they showcase the availability of the projects to think how their solution could be developed more/brought to market to make a difference in the world.

Section 5.1 - Evaluation framework: What framework did we use to evaluate the impact.

In this section, the theoretical evaluation framework that is used to evaluate the impact is identified, illustrated, and explained. The framework is based of the exploitation and sustainability sections in the Final Reports of the 42 projects. These sections gave the 42 projects the opportunity to formulate a strategy for the development of their solutions for year 1, 3 and 5 after the project. The projects can show that with SecurIT as a starting point, they have thought of a strategy for their solution and how with it they can make a difference in the world (and thus be impactful).

Also, impact from the SecurIT project is measured below in some graphs/documentation for example from the average TRL increase from the projects, their expected and created employment through the SecurIT project etc. By showing these average statistics (and outliers), the reader gets a good overview of that what has been done in the SecurIT project has actually helped the SMEs to develop over a year and to ensure a higher chance of creating a successful solution.

Section 5.2 - Evaluation tools: What did we do to receive the right data/information to use as basis for evaluation.

We asked each project to indicate a section in the final report towards each project's Exploitation and Sustainability in the future, as well as an assessment and evaluation of the time within the SecurIT project. With this, we can monitor what impact has been generated by the SecurIT project.

The following questions have been asked regarding Exploitation of each project:

1. Please describe how you have exploited the knowledge and progress developed and obtained in the project period so far. This can be internal (within one of your companies) or external.
2. What was most successful in your exploitation activities? Briefly expand on the action and success
3. Please indicate what your plans are for future exploitation beyond the SecurIT support program. Please be specific in your description. Please remember that the Final event organized in the Spring 2024 (as mentioned in the introduction to this report), also is an opportunity for you to exploit the knowledge obtained in the project period and to develop your project further.

The following questions have been asked regarding Sustainbility of each project:

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

1. What are the challenges you need to overcome to ensure a successful future of the project? Please describe 3-5 challenges and how you plan to overcome these challenges.
2. Do you need any further collaboration partner(s) or new partnerships for a successful commercialisation of your solution. And if yes, which types of collaboration/partnerships do you need? Please be as concrete as possible, so, if possible, the SecurIT consortium can assist in the facilitation of a collaboration/partnership.
3. Commercialization strategy: please elaborate on your long-term vision of the marketing strategy incl. how do you propose to attract more potential clients, get into the right networks, and create your own brand. What will be the focus of your marketing strategy?

Finally, the projects have been asked in the final report to indicate an overall assessment and evaluation of their (up to) 12-month project period during SecurIT.

Main questions:

1. ''Please elaborate and sum up on the entire project period, and identify what has worked well, what has been challenging and what corrective measures you have taken to keep your project on track.''
2. *You are also welcome to include a comment on your relations and collaboration with the SecurIT consortium and let us know if we can improve in some respects.*
3. *Based on the above provided assessment and evaluation, please provide a rating on a scale of 5-1 for the following aspects:*
    a. *The collaboration with and guidance of my dedicated follow up manager has worked well (regular meetings etc.)*
    b. *The SecurIT process and structure has worked well (from the open call process, jury day selection, regular meetings, payment installments frequency, progress reports etc.)*
    c. *The SecurIT project created new business opportunities for my organisation (open up new markets, new customers etc.)*
    d. *In my opinion, the SecurIT project has helped to strengthen the visibility of European SMEs in the security market/industries.*

➔ By asking these questions in the Sustainability and Exploitation sections, projects were challenged to think of how their solution can be implemented in the future, forcing them to think of a strategy to create impact. This is an example of how the SecurIT project has thought of ways to make projects think about making impact and a difference in the world with their innovative solutions.

➔ The most common answers found in all 42 Final Reports in the exploitation sections were:

- Expansion into new markets: the plan is to leverage enhanced capabilities to enter new geographical markets, particularly in regions where advanced security solutions are in high demand.

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

- Product diversification: utilizing the insights gained, projects aim to develop new product lines that address emerging security challenges, such as IoT security and AI-driven threat detection.
- Strategic partnerships: projects will continue to forge partnerships with key stakeholders in the security industry to co-develop innovative solutions and share best practices.

Section 5.3 - Overall evaluation supported by data/information (supported by average statistics from the project).

In this section, the effectiveness of the SecurIT project is analysed by evaluating different outputs of the project. A good example of a measurement we can use here is the increase in TRL-level of the funded projects. This shows what impact the SecurIT project has on the development of solutions and therefore the increase in security in the three different domains. The effectiviness is enhanced by displaying some average statistiscs from the SecurIT project.

During the SecurIT project, effectiveness can be measured through the mains of TRL level increase. There was a distinction between projects, clustering them into two categories: prototype projects and demonstration projects. For the demonstration projects, there were stricter guidelines for increasing TRL then for prototyping projects.

- **Prototyping instrument**: targeting companies having already carried out a feasibility study, and having the need develop a prototype, spend efforts in miniaturisation, testing, etc. (TRL 6).
- **Demonstration / pilot instrument**: targeting companies having already developed and tested a prototype, with the need to demonstrate its efficiency on a larger scale (TRL 7-8 and beyond).

See the table below for a more concrete example of what has been looked at in the project development.

	Prototyping	***Demonstration***
Eligible expenses	Development of prototype	Development and execution of (large scale) demonstration, testing, validation
TRL of envisaged project	N/A	TRL 5 at the start, at least TRL 7 at the end, preferably TRL 8 or higher.
Maximum financial contribution to entire projects (2/more beneficiary SMEs)	74.000 euro	88.000 euro
Funding rate	Up to 80% of total expenses	Up to 80% of total expenses
Time frame	Up to 12 months	Up to 12 months
Number of funded collaborative projects		42

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

Average statistics from the SecurIT project (presented during Final Event Paris May 2024)

General statistics from Open Calls:

- Open Call 1: 240 SME applicants from 33 countries resulting in 111 project proposals, of which 21 projects were selected.
- Open Call 2: 271 SME applicants from 38 countries resulting in 130 project proposals, of which also 21 projects were selected.
- 95 SMEs received funding from the European Commission
- 3,5 M€ distributed as direct funding to SMEs
- 74K€ funding to develop prototypes
- 88K€ funding to develop demonstrators
- 60K€/ SMEs as a maximum

This shows that SecurIT acts as an Innovation Booster:

- 42 projects and solutions developed towards safer and more resilient cities and territories
- 28 demonstrations and experiments performed
- 14 prototypes developed

The companies partaking in the SecurIT project have benefitted in the following manner:

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

Finally, we have also **created the following two tools** with the SecurIT project:

- Security Solution Mapping Tool
    - Showcasing 129 solutions & technology-providers mapped at EU level
    - Website: https://mapping.securit-project.eu/
- Regional Invest Tool
    - Creation of a platform with 56+ funding instruments & strategies at EU level
    - Website: https://securit-project.eu/regional-invest-tool/

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

Section 6 - External Stakeholders and Benefits

This includes the targeted external stakeholders as well as the benefits that could arise for them by the implementation of SecurIT. This includes the listing of all benefits, as they are caused by the SecurIT project. The main stakeholders that benefit from the SecurIT project are the SMEs of the funded projects, the organizing clusters and ambassador clusters. Moreover, the broader industry benefits of the innovation and development that have been initiated, enabled, or boosted by the SecurIT project.

Benefits for external stakeholders	
SMEs of the funded projects	- Calls tailored to the capacity and needs of SMEs - Visibility at EU level to the funded SMEs - Efficient support & follow-up by the SecurIT partners, ensuring high quality outcomes (all projects successfully completed) - Market-oriented KPIs, with focus on technical achievement & business perspectives - Several projects have gone beyond & obtained additional EU/national funding to upscale their solution
Organizing clusters	- Improved collaboration between different clusters and organizations. - Becoming central hubs for security innovation and knowledge dissemination. - Enhanced mechanisms for sharing knowledge and best practices.
Ambassador clusters	- Improved collaboration between different clusters and organizations. - Becoming central hubs for security innovation and knowledge dissemination. - Building a reputation as leaders in security innovation and research.
Broader Industry	- Overall improvement in the security posture of the industry. - Reduction in industry-wide risks associated with cyber and physical threats. - Acceleration of innovation through collaborative research and development. - Regulatory compliance: support in achieving compliance with evolving security regulations and standards.

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

Section 7 - Concluding remarks

In this section, the main concluding remarks of the document will be provided. *Here we have summarized the different sustainable outcomes of the SecurIT project.*
This plan can be used as a template for future sustainability plans for (European/international) cooperation and/or collaboration.

The SecurIT project has demonstrated significant advancements in fostering innovation and developing robust security solutions across Europe. This comprehensive initiative supported numerous SMEs through targeted funding and strategic collaboration, achieving notable success in multiple key areas.

The SecurIT project successfully fostered innovative security solutions and promoted cross-border collaboration among SMEs, achieving significant milestones in 42 projects involving over 95 SMEs across Europe. Moving forward, the project's evolution into meta clustering aims to amplify impact and market reach in digital security.
By leveraging the strengths of clusters across Europe and facilitating internationalization, meta clustering enhances collaborative innovation, expands market access, optimizes resources, and boosts SME competitiveness. This strategic transition is supported by cascade funding, simplifying access to financial resources and reducing risk while fostering a dynamic ecosystem that drives innovation and economic growth in European digital security.

The impact of the SecurIT project is evident in the significant increase in Technology Readiness Levels (TRL) of the participating projects. By focusing on exploitation and sustainability, the project ensured that the solutions developed could be further enhanced and brought to market. The evaluation framework and tools used effectively captured the advancements and benefits generated, demonstrating the project's contribution to innovation and technological development.

The executive summary highlights the statistical achievements of the SecurIT project, including the participation of 240 SMEs from 33 countries in the first open call and 271 SMEs from 38 countries in the second open call. The project distributed 3,5 million euros in direct funding, resulting in the development of 42 projects and solutions aimed at creating safer and more resilient cities and territories. Additionally, the project created tools such as the Security Solution Mapping Tool and the Regional Invest Tool to further support innovation and investment in security technologies.

The SecurIT project provided numerous benefits to external stakeholders, including SMEs, organizing clusters, ambassador clusters, and the broader industry. SMEs received tailored support and visibility at the EU level, while clusters improved collaboration and became central hubs for security innovation. The broader industry benefited from enhanced security measures, accelerated innovation, and improved regulatory compliance.

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

Sustainability was a core focus of the SecurIT project, ensuring that the innovations and solutions developed would have lasting impacts beyond the project's timeline. By supporting the commercialization of developed solutions and fostering long-term partnerships, the project laid the groundwork for continuous advancements in security technologies. The main exploitation routes included ongoing support for funded projects, strategic matchmaking, and leveraging communication materials to enhance visibility and impact.

In conclusion, the SecurIT project has significantly contributed to the development and deployment of innovative security solutions across Europe. Through strategic funding, collaboration, and sustainability efforts, the project has created a robust foundation for continued advancements in security technologies, benefiting a wide range of stakeholders and promoting a safer, more resilient future.

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