D4.1
Plan for Dissemination, Exploitation and Communication Activities

Project Name	Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands
Project acronym	SECURE-NET
Grant agreement no.	101217315
Call	HORIZON-WIDERA-2024-TALENTS-03
Type of action	HORIZON-CSA
Project starting date	1 September 2025
Project duration	48 months
Deliverable Number	D4.1
Deliverable name	Plan for Dissemination, Exploitation and Communication Activities
Lead Beneficiary	University of Tartu
Type	R — Document, report
Dissemination Level	PU – Public
Work Package No	WP4
Due Date	February 2026
Submission Date	27 February 2026
Version	1

Funded by the European Union

Funded by the European Union under Grant Agreement No 101217315. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them.

Editor

- Kęstutis Kapočius (KTU)
- Raimundas Matulevičius (UTARTU)

Contributors

- Raimundas Matulevičius (UTARTU)
- Vaclav (Vashek) Matyas (MUNI)
- Hendrik Pillmann (RIA)
- Liina Kamm (CYBER)
- Kęstutis Kapočius (KTU)
- Rimantas Butleris (KTU)
- Robertas Ulinskas (ITS)
- Dimka Karastoyanova (RUG)
- Batina, L. Lejla (RUN)
- Durga Lakshmi Ramachandran (KEYS)
- Serhii Sharyn (PNU)
- Volodymyr Shcherbiak (POE)
- Mubashar Iqbal (UTARTU)

Reviewers

- Rimantas Butleris (KTU)
- Mubashar Iqbal (UTARTU)
- Lukas Daubner (UTARTU)

SECURE-NET Consortium

Participant organization name	Short name	Country
University of Tartu	UTARTU	Estonia
Masaryk University	MUNI	Czechia
Estonian Information System Authority	RIA	Estonia
Cybernetica AS	CYBER	Estonia
Kaunas University of Technology	KTU	Lithuania
UAB IT Solutions	ITS	Lithuania
University of Groningen	RUG	Netherlands
Radboud University	RUN	Netherlands
Keysight Technologies Netherlands Riscure BV	KEYS	Netherlands
Vasyl Stefanyk Carpathian National University	PNU	Ukraine
Joint-stock company “Prykarpattyaoblenergo”	POE	Ukraine

Abbreviations

CA	–	consortium agreement
CKPI	–	communication key performance indicator
DEC	–	dissemination, exploitation, communication
DKPI	–	dissemination key performance indicator
EKPI	–	exploitation key performance indicator
GA	–	grant agreement
ICT	–	information and communication technologies
IP	–	intellectual property
IPR	–	intellectual property rights
M	–	project month
MI	–	monitored communication channels performance indicators
O	–	project objective
PCDP	–	personal career development plan
PQC	–	post-quantum cryptography
TA	–	target audience group
WP	–	work package

Executive Summary

This deliverable presents the SECURE-NET dissemination, exploitation and communication (DEC) efforts and expected results. It covers the life cycle of the SECURE-NET project's DEC activities, including the definition of objectives, target audiences, key messages, visual identity, tools and channels, actions, performance indicators, and their monitoring principles. These aspects are discussed separately in terms of communication, dissemination and exploitation tasks, while outlining the existing overlaps. The initial communication channels' performance overview is also included. The plan for dissemination, exploitation and communication activities will be updated by August 2028.

Table of Contents

List of Figures

List of Tables

1. Introduction

SECURE-NET is a project for Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands. Its main objectives [1] are to

- Develop a comprehensive framework for cross-sectoral staff secondments and for developing research and innovation talent skills.
- Provide research and innovation talents from partner organisations with domain-specific knowledge and transferable skills.
- Strengthen cross-sectoral and cross-border collaboration between partners.
- Enhance the international profile and visibility of the widening partners

Communication, dissemination and exploitation activities should help achieve the SECURE-NET project's objectives. SECURE-NET intends to contribute to the development of personnel's skills, scientific and training results, and to their sharing within the ecosystem. It should support partners in sharing their achievements both at the national and international levels across different sectors.

The purpose of this document is to outline the **detailed strategy, specifications, and instruments to** set up and describe the infrastructure for project communication, dissemination, and exploitation. The following five communication, dissemination and exploitation objectives are defined:

- **O1: Share research results**: it means sharing SECURE-NET research results and building an international and regional reputation.
- **O2: Invite to collaborate**: it means inviting to collaborate and supporting the update of the SECURE-NET research and innovation results.
- **O3: Provide training and awareness**: it means providing training and awareness of the SECURE-NET results.
- **O4: Inform about achievements**: it means informing the targeted audience about SECURE-NET activities and achievements.
- **O5: Ensure sustainability**: it ensures the long-term sustainability of SECURE-NET activities.

The document is structured as follows: Section 2 details the communication strategy and plan. Section 3 overviews the dissemination strategy and plan. Section 4 presents the exploitation strategy and plan. Finally, Section 5 summarises and concludes this deliverable.

2 Communication Strategy and Plan

Communication aims to inform, promote and communicate the project's activities and results. This section discusses the SECURE-NET communication objectives, target audience, key messages, tools and channels, and monitoring activities. The section also presents the SECURE-NET visual identity and funding statement.

2.1 Communication Objectives

The overall purpose of the SECURE-NET communication activities is to inform, promote and communicate the SECURE-NET activities and results. Regarding communication, O1 aims to build the SECURE-NET partners' reputations by communicating news and information about key advances, breakthroughs, and other achievements related to talent exchange during the SECURE-NET project. O2 aims to communicate scientific results and invite new scientific and industrial collaborators through articles, posts, and appearances online, at public events, and in traditional media. Providing training and awareness (O3) aims to inform of upcoming or past training and other public activities, and to attract new participants. The goal of O4 is to communicate the project's achievements.

2.2 Target Audience

The target audience is selected to facilitate cross-sectoral sharing of the SECURE-NET research results, strengthen collaboration, and enhance the international and regional profile and visibility of the SECURE-NET activities. Four groups are defined:

TA1: Academic community – researchers in the field of cybersecurity and ICT, and more specifically, security certification, secure cyber-physical systems and critical infrastructures, post-quantum cryptography, and human-centric aspects of cybersecurity.

TA2: Companies – cybersecurity solutions, ICT, (post-quantum) cryptography; security certification; critical infrastructure operators; spin-offs and emerging entrepreneurs.

TA3: Policy-makers and public authorities dealing with state/EU/Ukrainian data and computer systems, digital and critical infrastructures, and cyber defence; also, national education policymakers and research organisations' administrators.

TA4: General public – any person or organisation interested in European cooperation or developments in cybersecurity, with special emphasis on youth and young female students, as females are still underrepresented in ICT.

For instance, to achieve O1, O2, and O3, the **academic community** (TA1) should receive updates on the advances of SECURE-NET partners and identify avenues for future research and advanced training opportunities offered by SECURE-NET to academics from outside the consortium. SECURE-NET will inform **companies** (TA2) about how the SECURE-NET results could improve commercial services. It should settle potential avenues for further research and cooperation (O2). To achieve O1, O3, and O4, the **policymakers and public**

authorities (T3) should receive messages about SECURE-NET research results. The SECURE-NET partners will explain how to ensure the safety and smooth operation of the European digital society and protect EU digital infrastructures against potential cyberattacks. The project aims to raise awareness among the **general public,** with emphasis on youth and female students (T4), by providing training and awareness (O3) and informing about the project's achievements (O4).

2.3 Key Messages

SECURE-NET communication messaging themes stem directly from the project objectives and communication goals. It is important to note that communication on the project or partner websites, social networks, media, and other channels will often overlap with or accompany dissemination and exploitation activities and, therefore, must cover the target groups and messages outlined in the project proposal. Table 1 presents the concept of the key messages communicated to the target audience groups.

2.4. Tools and Channels

Key communication channels for disseminating and exploiting results will include the project *website* and two *social media* profiles (i.e., LinkedIn and Facebook). In addition, SECURE-NET will rely on partners publishing project-related messages (e.g., news and announcements) on their institutional websites and social network profiles. SECURE-NET will prepare an annual press release; all partners will be requested to communicate about the project events, achieved milestones and important research results. SECURE-NET will also introduce the project *brochure*, which partners can print on demand. Communication efforts will overlap with dissemination activities and will therefore rely on other channels outlined in Section 3.2 of this plan.

2.4.1 Project Website

The SECURE-NET website (see Figure 1) will serve as the central hub for sharing project-related information. It is hosted at the Kaunas University of Technology (the lead for WP4 on Dissemination, Exploitation, Communication, and Sustainability). The SECURE-NET website's URL is

https://securenet.isk.ktu.lt/

The Website will ensure independence of the SECURE-NET communication and dissemination activities regarding the state of the social media channels. The navigation plan of the SECURE-NET website is given in Figure 2:

Table 1: SECURE-NET Communication Messages Grouped by the Target Audience

Target audience		Concepts of the key communication messages
TA1		• SECURE-NET and its partners are proficient and productive innovators in cybersecurity and ICT • SECURE-NET and its participants are open for academic or applied collaboration in cybersecurity and ICT • Participating widening universities are excellent destinations for researchers, post-docs, and PhD students
TA2		• SECURE-NET results can be used to improve commercial services and products • SECURE-NET seeks cross-sectoral collaboration in partner countries in the fields of cybersecurity and ICT • Cross-sectoral secondments and training collaboration are beneficial to the field
TA3		• SECURE-NET research and results, as well as researchers and innovators with improved knowledge and skills, can help ensure the safety and smooth operation of the European digital society and protect EU digital infrastructures against potential cyberattacks • Cross-sectoral secondments and training collaboration is beneficial to the field
TA4:	General public	• Partners are conducting interesting and relevant research in the field of cybersecurity, including human-centric aspects of cybersecurity • The project has received funding from the EU and aims to ensure the cybersecurity of digital and critical infrastructures and operations in partner countries and the EU
	Youth	• Cybersecurity is an exciting field of research with growing importance for the EU which has many applications in the private and public sectors
	Young female students	• ICT in general and cybersecurity specifically are interesting and important research fields and not only they are accessible to but would benefit greatly from more women getting involved • All partner universities promote gender balance and welcome talented students without prejudice against gender

- **Home page.** It provides brief information about the project and its partners, with quick buttons to read more. The footer of this and all other website pages contains the EU flag, funding statement and links to SECURE-NET social network pages.
- **Login**. Website administration login page that leads to content management tools. Login is *not* accessible directly from the website and is available only to those who know the direct link.
- **About.** It provides a summary of SECURE-NET goals and expected contributions, along with the link to the project details on the European Commission website.
- **Partners**. It provides a list of partners, each with its logo. *Partner info pages* present short profiles of each partner along with relevant external links to institutional/ company websites.
- **News**. It provides a list of project news posts. Posts will cover major planned project events and other key developments as necessary. *News posts* are full-text pages of

the posts. Each one will be accompanied by an interactive photo gallery when appropriate.

- **Events**. It shows a calendar of project events. *Event details* provide the key information about each event, such as date, website, venue, map, and URL.
- **Training**. It provides a list of publicly available project outputs related to training and raising awareness of the SECURE-NET topics of interest, including downloadable presentations, links to videos, and other materials as needed.

Figure 1: Landing Page of the SECURE-NET Website
(design subject to change)

- **Project deliverables.** It lists the planned SECURE-NET deliverables (only PUBLIC) with download links where appropriate.
- **Publications**. It provides a list of SECURE-NET research publications along with external links to websites hosting the papers.

Project deliverables and other materials that are considered sensitive and cannot be made publicly accessible will not be published on the website. The SECURE-NET project's results (non-sensitive) will be freely available without registration, meaning the website will also serve as the project's results exploitation environment.

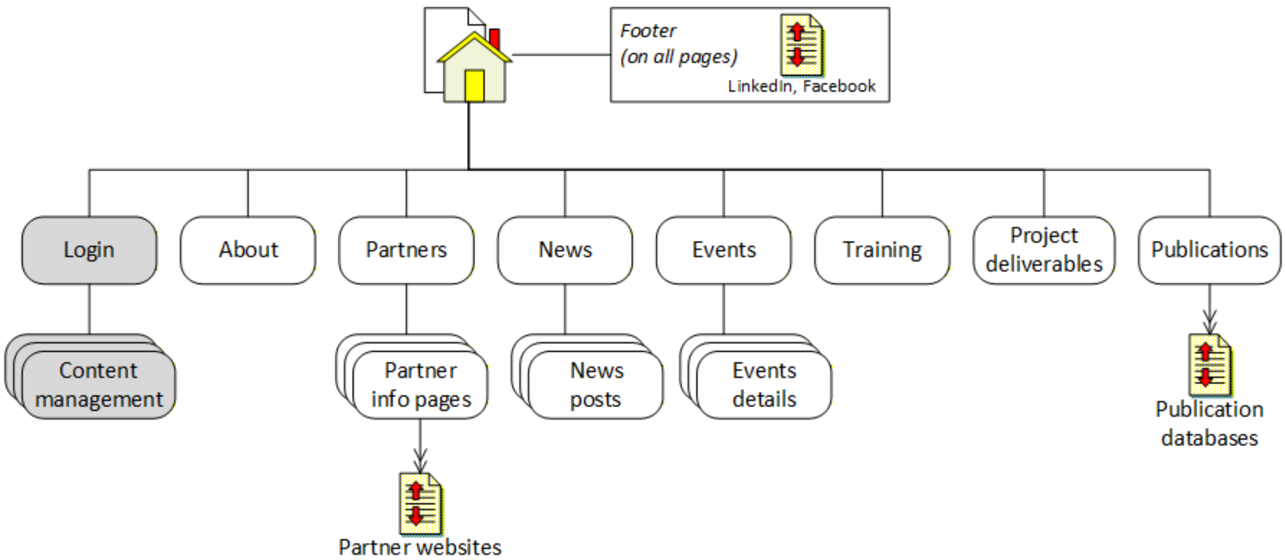


Figure 2: Navigation Plan of the SECURE-NET Website

The **News** page will also serve as the official SECURE-NET newsletter, providing unrestricted access to reports and photos from key project events. The news will also cover follow-up common project initiatives, notable results of projected secondments, and other project-related developments as necessary.

The SECURE-NET website is built using the WordPress content management system. As of February 2026, configuration is as follows: WordPress version 6.9.1, PHP version 8.3.30, MySQL database management system version 11.4.9 and 9 plugins (see Table 2)). Three key considerations led to the choice of WordPress:

- It's an open-source system,
- It has a good track record and high popularity, and
- There is a wide choice of free high-quality plug-ins.

These reasons mean that the platform is reliable, secure and constantly updated, while website content management principles are relatively easy to learn to newcomers and familiar to experienced users. The website is hosted at Kaunas University of Technology. Backup copies of the code and all the data are made every Monday, Wednesday, and Saturday. Backups are stored on the KTU infrastructure. Plugins used to manage the website were chosen with flexibility, reliability, security, and usability in mind. The list and version numbers as of February 2026 are given in Table 2. Note that the list of plugins used may change.

Table 2. SECURE-NET Website Plugins as of February 2026

Name | Provider	Version	Features and choice considerations
Gutenberg | Gutenberg Team	22.5.3	It is a standard part of WordPress installation. The plugin provides early access to new block editor and site editor capabilities before they reach WordPress core. Using it supports more flexible page construction and allows the site to benefit from upcoming editor improvements sooner.
EditorsKit | Munir Kamal	1.40.6	Is used to extend the standard Gutenberg editor with extra blocks and productivity tools, making page building faster and more consistent.
Embed Any Document | Awsm Innovations	2.7.12	It enables documents (PDF, PPT, DOC, etc.) to be displayed directly inside a page, which is ideal for sharing deliverables, presentations, and internal materials.
Matomo Analytics – Ethical Stats. Powerful Insights. | Matomo	5.6.1	It is used to track website performance monitoring indicators described in Section 2.6.1. It maintains a strong focus on privacy and GDPR-friendly analytics compared to many alternative third-party trackers. At the same time, it provides actionable insights without relying on an external ecosystem.
NextGEN Gallery | Imagely	4.0.5	It is used to manage image collections in a structured way. It simplifies presenting project photos or event highlights in a more polished format than basic WordPress galleries and is mostly used when building project news posts pages.
Otter – Page Builder Blocks & Extensions for Gutenberg | Themeisle	3.1.4	It adds a set of additional Gutenberg blocks that make it easier to create modern-looking pages and sections. This helps the site maintain a professional visual style.
Safe SVG | 10up	2.4.0	It allows uploading and using SVG graphics while sanitizing the files to reduce security risks associated with raw SVG uploads.
Starter Sites & Templates by Neve | Themeisle	1.2.24	It provides ready-made layouts and starter templates that speed up initial site setup and future page creation. It helps keep design consistent and reduces the effort required to build new pages from scratch. Website is using one of the free graphical user interface templates provided in this set.
The Events Calendar | The Events Calendar	6.15.16	It supports creating and publishing upcoming meetings, workshops, training and other SECURE-NET events in a clear calendar format. It improves communication and planning by giving visitors and team members a single, easy-to-find place for scheduled activities.

2.4.2 Social Media Channels

To reach wider audiences while maintaining a targeted approach, SECURE-NET will use dedicated profiles on two social media channels. The contents of posts on these pages will replicate news published on the project's website and will also provide or repost additional information on relevant events in related projects. They will also serve as community and network-building tools, allowing project participants and anyone interested in SECURE-NET to use features such as profile following, commenting, tagging, reposting SECURE-NET posts, and more. Considering that the project is aimed at both specialist audiences and at a wider public, SECURE-NET will use:

- LinkedIn (see Figure 3): https://www.linkedin.com/company/secure-net-enhancing-cross-sectoral-collaboration-in-cybersecurity/
- Facebook (see Figure 4): https://www.facebook.com/enhancing.collaboration.in.cybersecurity/

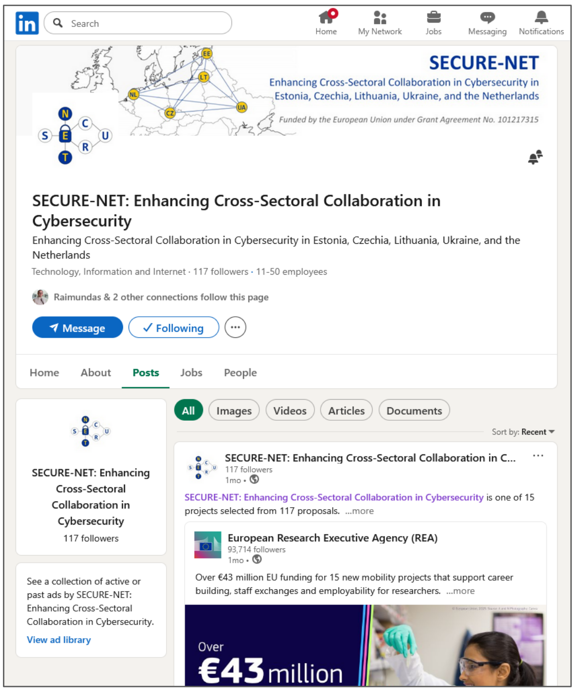


Figure 3. SECURE-NET LinkedIn Landing Page

Figure 4. SECURE-NET Facebook Landing Page

2.5 Action Plan and Timeline

Communication will be carried out to support the project implementation plan outlined in [1]. Table 3 presents the main communication activities and the expected timeframe regarding the key SECURE-NET dissemination activities. The choice of channels for each communication activity will be determined by the specific needs and circumstances.

Table 3. Key SECURE-NET Communication Activities

Events	Expected timeframe	Communication activities
4 parallel training events for (a) researchers/ innovators and (b) support staff	M12, M24, M36, M47	• Publicising upcoming events as necessary. • Releasing news posts during events as necessary. • Communicating the results of events.
4 webinars on implementing cybersecurity measures in times of war	M7-M24	• Publicising upcoming events as necessary. • Communicating the results of events.
Secondments	Throughout the project	• Communicating the results after the completion of secondments. • Secondments, especially shorter ones, may be grouped by their nature or timing. • Additional communication releases during the secondments as necessary.
Local SECURE-NET related events	Throughout the project	• Publicising upcoming events as necessary. • Publishing news posts on relevant channels after the events, as necessary.

2.6 Monitoring

2.6.1 Performance Measurement

Communication progress and effectiveness will be monitored by collecting performance metrics from the project website and social network pages, and by tracking the key performance indicators outlined in the SECURE-NET grant agreement. Table 4 presents the performance indicators for the communication tools. To monitor the project website, the Matomo Analytics plug-in will be used, while social network profiles will be monitored using LinkedIn and Facebook tools. The list of indicators is adjusted to the capabilities of the monitoring tools and fully covers the metrics outlined in the project proposal. Demographic data of social network profiles' followers and/or visitors will also be aggregated. Data will be collected every three months.

2.6.2 Key Performance Indicators

In addition to the SECURE-NET communication tool monitoring, key performance indicators listed in Table 5 will also be tracked. The listed communication outputs will cover project events, achieved milestones, important research results, and other relevant information. The results reflect the goals outlined in [1] and must be achieved by the end of the project, but all efforts will be made to exceed these numbers. Note that setting intermediate goals for these indicators would be unproductive and imprecise given the nature of the activities they relate to.

Table 4. SECURE-NET Communication Tool Performance Indicators

Communication tool	Monitored indicators
Project website	MI1. **Website visits** – the number of user activity sessions. MI2. **Unique visits** – the number of unique user visits within the specified time frame. MI3. **Average visit duration** – average amount of time visitors spent on the website during a single session. MI4. **Pageviews** – number of times any page of the website has been visited, MI5. **Unique pageviews** – number of sessions during which any page was viewed at least once. MI6. **Actions per visit** – average number of interactions visitors had with the website during a single visit.
LinkedIn social channel	MI7. **Page views** – number of times the page has been viewed. MI8. **New followers** – the increase in the number of profile followers over the given period. MI9. **Unique visitors** – number of distinct users who have visited the profile. MI10. **Reactions** – number of emotional reactions (emojis) to content available on the page. MI11. **Members reached** – number of unique LinkedIn users who have seen the content. MI12. **Impressions** – number of times the content was displayed on user's screen, regardless of whether it was engaged with or not. MI13. **Engagement rate** – percentage of people who liked, commented, shared or clicked the content. MI14. **Clicks** – the number of times signed-in LinkedIn users clicked on the post, company name, or logo. MI15. **Follower demographics** – information (e.g., location, industry, job function, and seniority) about the followers' profile.
Facebook channel	MI16. **Views** – the number of times your content was played or displayed MI17. **Viewers** – the number of accounts that have viewed your content at least once. MI18. **Content interaction** – the number of likes or reactions, saves, comments, shares and replies on your content, including ads. MI19. **Link clicks** – the number of clicks, taps or swipes on links within your content, including ads. MI20. **Visits** – the number of times your Page or profile was visited. MI21. **Follows** – the number of times accounts followed you in the selected time period. MI22. **Followers** – the total number of followers of the Facebook Page or profile. This is calculated as the number of follows minus the number of unfollows over the lifetime of your Facebook Page or profile. MI23. **Age & gender** – aggregated demographic data is based on a number of factors, including age and gender information users provide in their Facebook MI24. Information about followers – including **top cities**, and **top countries**

Table 5. SECURE-NET Communication Key Performance Indicators

Key performance indicator	Expected value, M48
CKPI1. Number of popular science articles	10 (2 per involved country)
CKPI2. Number of articles or podcast appearances for Europe-wide media	2
CKPI3. Number of project news posts on the project website	12
CKPI4. Number of project news posts on dedicated Facebook and LinkedIn pages	12 on each
CKPI5. Number of press releases	20 (1 per involved country; monitored annually)

2.6.3 Reporting

Reporting on the progress of communication, dissemination and exploitation activities will be carried out in accordance with the plan outlined in [1] (see Table 6; the grey rows represent the current document). Non-sensitive deliverables will be published on the project's website.

Table 6. Deliverables of SECURE-NET Dissemination, Exploitation and Communication Activities

Deliverable number	Name	Level	Due date
D4.1	Plan for dissemination, exploitation and communication activities	Public	M6
D4.2	Interim Report on DEC activities	Public	M24
D4.3	Updated plan for dissemination and exploitation including communication activities	Sensitive	M36
D4.4	Final report on DEC activities	Public	M47
D4.5	SECURE-NET long-term sustainability strategy	Sensitive	M48

2.6.4 Performance of the LinkedIn social media channel

Figure 5 presents the performance of the SECURE-NET LinkedIn social media channel. It is illustrated using metrics of Page views (a), New Followers (b), Unique visitors (c), Reactions (d), Members reached (e), Impressions (f), Engagement rate (g), and Clicks (h).

On the 20th of February 2026, the SECURE-NET LinkedIn social media had 130 followers. Visitor demographics information is presented in Figure 6 in terms of location (a), industry (b), job function (c), and seniority (d). Hence, to date, the visitors from the Tallinn Metropolitan Area, Estonia (9%, see (a)) are the majority SECURE-NET followers. Most followers (22% see (b), 21,5%) represent the higher education industry. Regarding the job function, most followers are in information technology (18%, as shown in (c)), and the majority are seniors (37%, as shown in (d)).

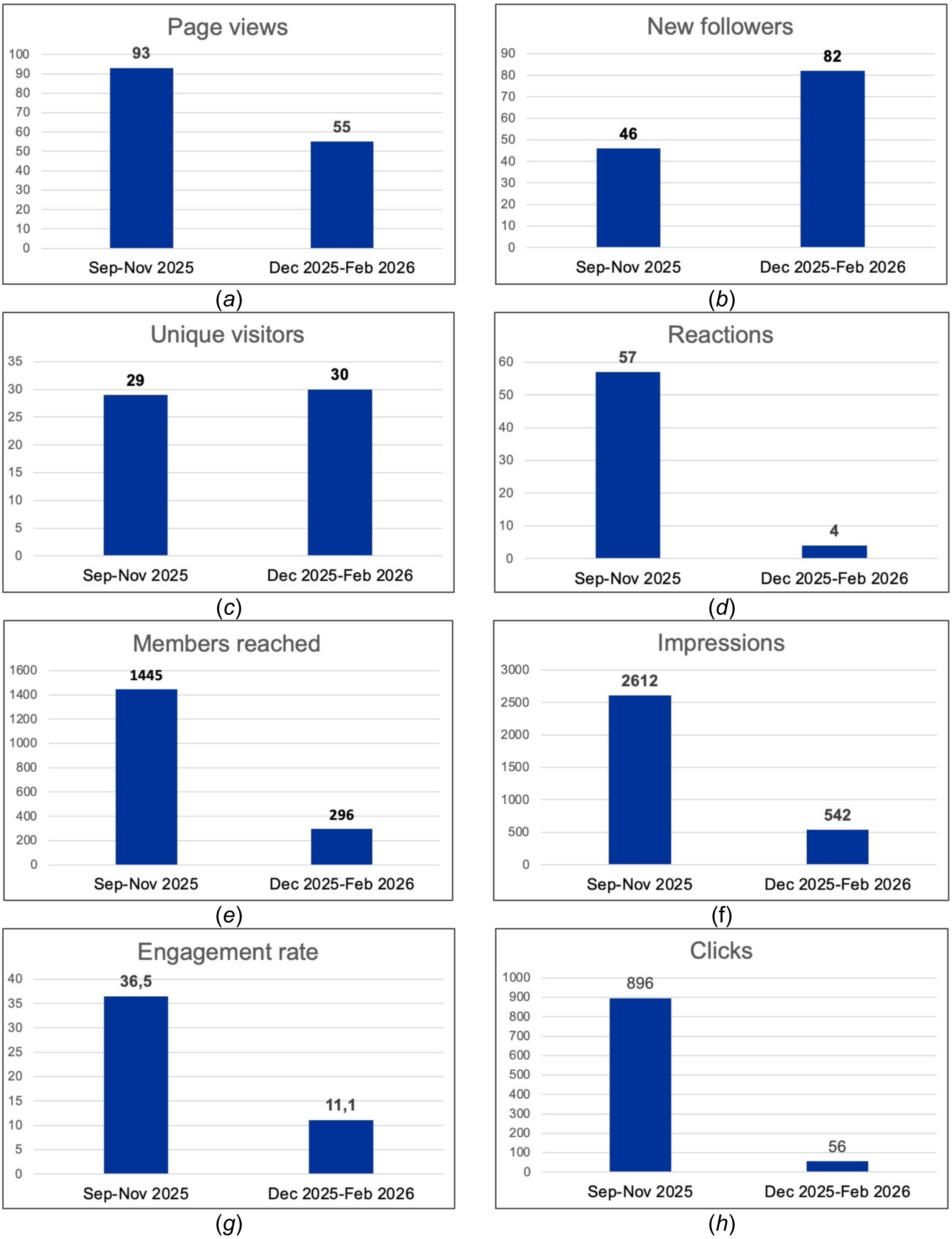
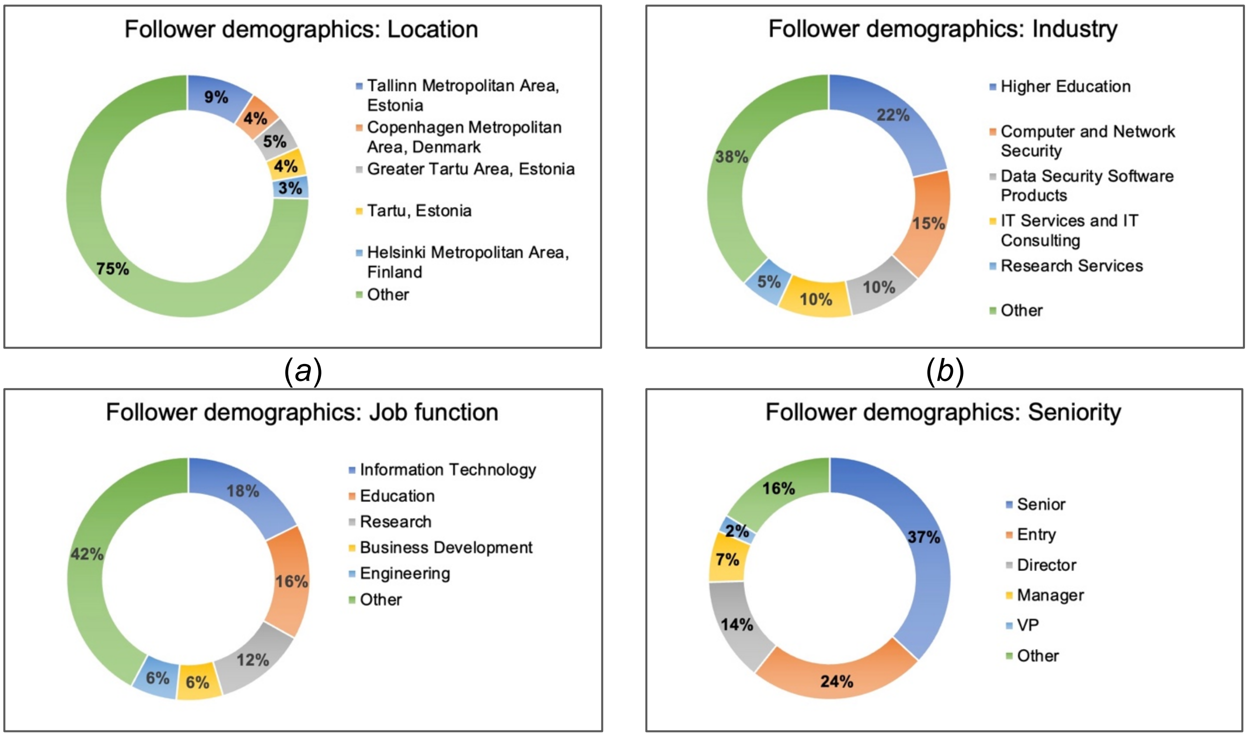


Figure 5. Performance of SECURE-NET LinkedIn Social Media Channel



(c) (d)

Figure 6. Follower Demographics of SECURE-NET at LinkedIn Social Media Channel (February 2026)

2.6.5 Performance of the Facebook social media channel

Figure 11 presents the performance of the SECURE-NET Facebook social media channel. It is illustrated using metrics of Views (a), Viewers (b), Contents interaction (c), Link clicks (d), Visits (e), and Follows (f). On the 24th of February 2026, the SECURE-NET Facebook social media had 102 followers. Information about visitors (gender, top cities, and top countries) has not yet been obtained, as this metric is available from 100 followers who are not also friends.

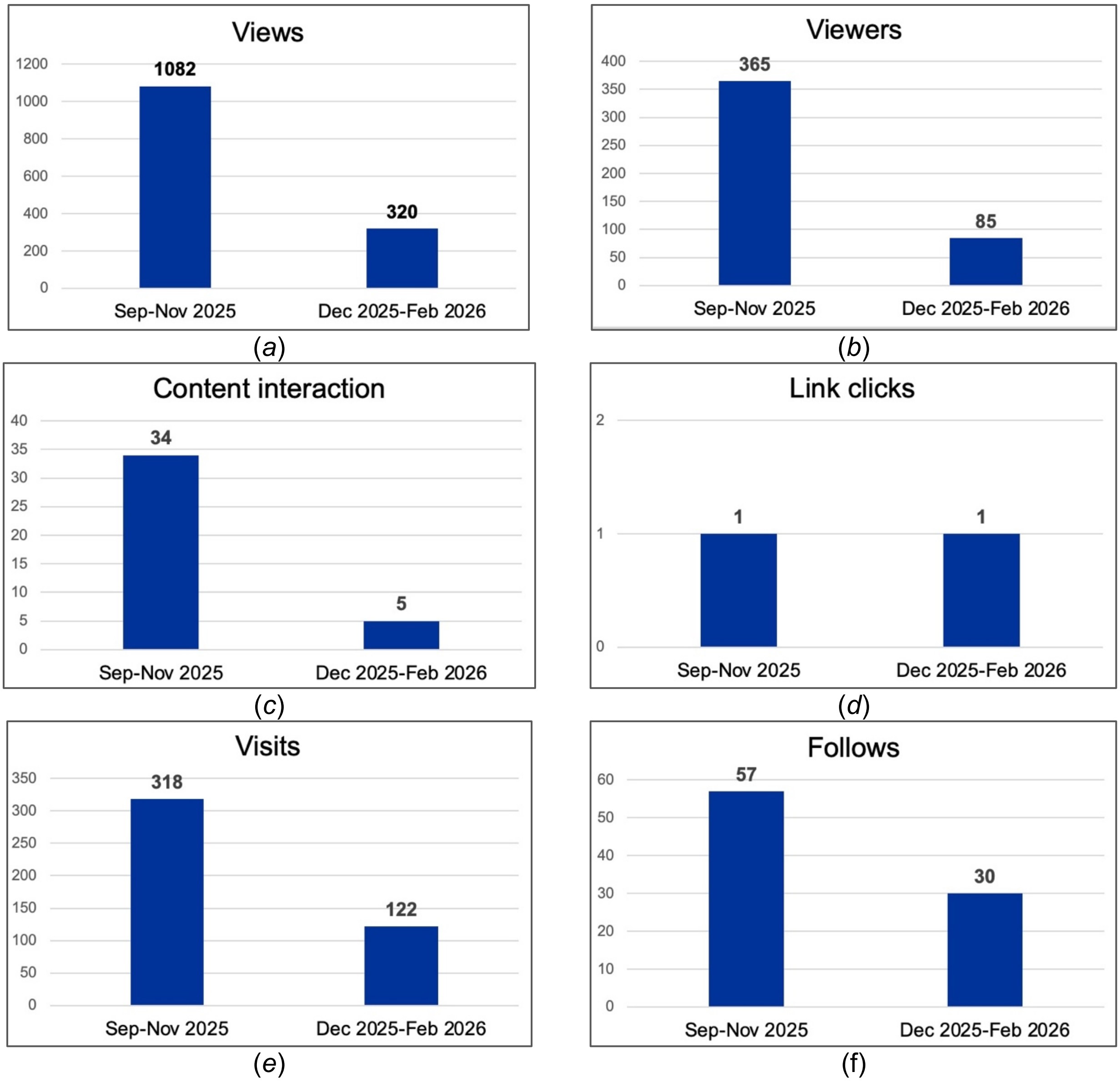


Figure 7. Performance of SECURE-NET Facebook Social Media Channel as of February 2026

2.7 Visual Identity

2.7.1 Logo and Colour Palette

All SECURE-NET communication must include the project logo, which features the project abbreviation and graphics reminiscent of computer network diagrams. The logo is available in four variants (see Figure 7):

- regular or main version,
- light, - to be used on dark backgrounds,

- light on background, - to be used on light backgrounds, alternative to the main version,
- black/white, - to be used for B&W materials.

All versions of the logo are made available to project partners in raster (.png) and vector (.svg) formats.

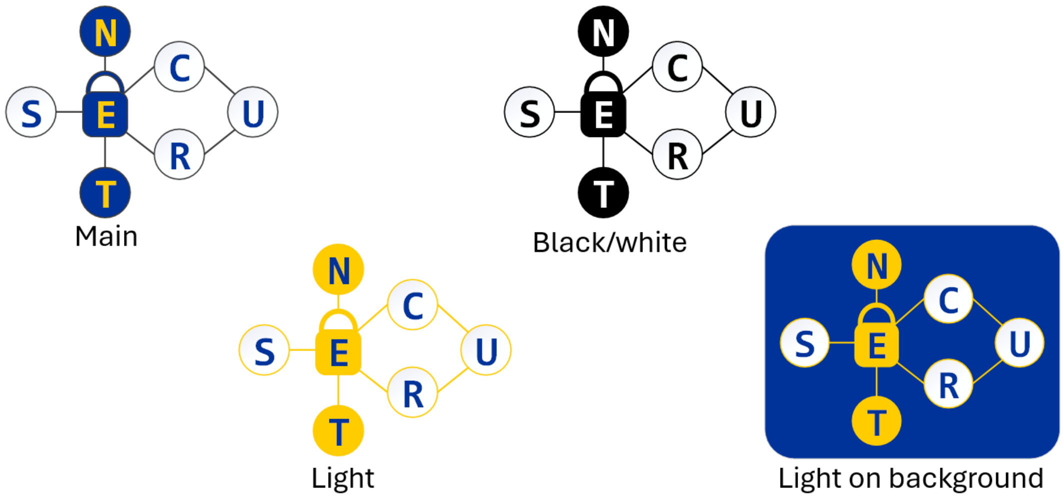


Figure 8. Variants of the SECURE-NET Project Logo

The colours used in the 1st, 2nd, and 3rd versions of the logo also serve as the project's colour palette. They have been picked using the flag of the European Union as a reference and are as follows:

- Egyptian Blue – #003399; R: 0, G: 51, B: 153;
- Bright Amber – #FFCC00; R: 255, G: 204, B: 0;
- white – #FFFFFF;
- black – #000000.

If necessary for increased aesthetic appeal or legibility of text/graphics, both lighter and darker hues of Egyptian Blue and Bright Amber can be used.

2.7.2 Documentation Templates

Two templates will be used by project partners when preparing project deliverables and any intermediate outputs used within the project:

- Document template available to all project members in .docx and .rtf formats.
- MS PowerPoint presentation template in .pptx format.

Both templates use the same colour scheme and font. This report is based on the document template. A presentation template, on the other hand, allows for the quick creation of distinguishable, consistent presentations throughout the project's activities. The template includes 8 content slide layouts and one cover slide layout. All 9 layouts are available in light and dark versions, providing flexibility (see Figure 8 for a title slide example in both layouts). Dark slides are recommended for emphasis, while light ones are best suited for presentation of routine information or learning materials.

Figure 9. SECURE-NET Presentation Template Title Slide Layouts

2.8 Funding Statement

Any communication or dissemination activity related to the project will have to include the following funding statement and disclaimer (translated into local languages where appropriate):

> *Funded by the European Union under Grant Agreement No. 101217315. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency.*

Neither the European Union nor the granting authority can be held responsible for them.

In addition to the above, all outputs related to SECURE-NET (including media releases, conference or seminar posters or presentations, informational brochures) and any results of actions will display the European flag (emblem) and short funding statement, which can be translated into other languages where appropriate. Horizontal and vertical variants are possible (see Figure 9 for the default colour versions in English), along with the available variations provided on the European Commission Download Centre for visual elements[1]. These visual elements can't be altered by adding any other visual marks, brands or text. Note that when displayed alongside other logos (e.g., those of beneficiaries or sponsors), the emblem must be at least as prominent and visible as the other logos.

Funded by the European Union

Funded by the European Union

Figure 10. Default Variants of the European Flag Emblem

2.9 European General Data Protection Regulation

The personal data of secondees will be handled in line with the GDPR. We will collect only non-sensitive information (for reporting purposes, etc.). As the number of secondees is below 100 and the collected data cannot be anonymised, we will collect informed consent from secondees and provide detailed explanations on how their information will be used [1]. Project website and social network pages' performance data will be collected and managed in accordance with GDPR regulations. Further details are given in the SECURE-NET Data Management Plan [5].

[1] https://ec.europa.eu/regional_policy/information-sources/logo-download-center_en

3 Dissemination Strategy and Plan

Dissemination aims to make knowledge and results publicly available. This section presents the SECURE-NET dissemination target groups, potential dissemination channels, and planned dissemination activities. It also discusses briefly how dissemination will be monitored.

3.1 Dissemination Target Groups

Table 7 presents the relationship between the targeted audience and channels used for dissemination. To disseminate SECURE-NET's outcomes (O1) to the academic community (TA1) and demonstrate the quality of its research and findings, trusted professional networks with a wide reach will be used. These include peer-reviewed articles in high-impact journals, participation in leading academic conferences with presentations, posters, and tutorials, and dissemination through SECURE-NET partners' networks and other networks (such as SPARTA, CyberSec4Europe, CHESS, CCAT, QARC, and others). The research results will be published in conference proceedings and journals, potentially including use cases, experimentation results, or datasets. The published articles will be disseminated through the publishers' portals and uploaded to the Zenodo platform <*https://zenodo.org/communities/secure-net*>. The SECURE-NET project aims to share the research results as open access. The research results will be shared. Research results will also be disseminated as conference presentations.

The SECURE-NET partners will also engage with the companies (TA2) to demonstrate the quality of research (O1), provide training and awareness (O2), and inform about the SECURE-NET achievements (O4). In addition to the above dissemination channels, the partners will use direct interactions during the SECURE-NET project events, conferences, and trade shows (e.g., interactions with the European Cyber Security Organisation (ECSO), start-up competitions, incubation spaces in partner countries, training and business consultancy services offered by SECURE-NET beneficiaries (e.g., RIA, KEYS).

The policy-makers and public authorities (TA3) will be approached through participation in leading academic conferences with presentations/posters and through direct interactions during project events and conferences with regional/national policy-makers. The SECURE-NET aims to inform policy-makers and public authorities about its achievements (O4). We will also consider interactions with the European Union Agency for Cybersecurity (ENISA), the EDPB, and the Directorate-General for Communications Networks, Content and Technology.

The SECURE-NET partners will inform the general public (TA4) about the project achievements (O4) through direct interactions, popular science articles, and popular science events.

Table 7: Dissemination Target Audience, Objectives and Channels

Channels/ targets	TA1. Academic community	TA2. Companies	TA3. Policy-makers and public authorities	TA4. General public
Articles at the conference proceedings and scientific journals	**O1**: Share research results			
Conferences	**O1**: Share research results **O3**: Provide training and awareness:	**O1**: Share research results **O3**: Provide training and awareness:	**O4**: Inform about achievements	
SECURE-NET partner networks	**O4**: Inform about achievements	**O4**: Inform about achievements		
Direct interactions		**O1**: Share research results **O3**: Provide training and awareness:	**O4**: Inform about achievements	**O4**: Inform about achievements
Startup competitions, trade shows		**O3**: Provide training and awareness **O4**: Inform about achievements		
Popular science articles				**O4**: Inform about achievements
Popular science events				**O4**: Inform about achievements

3.2 Dissemination Channels

Table 8 explicates the dissemination channels for the separate target audience. Next, in this section, we present the lists of journals and magazines for publishing scientific results, conferences to submit and publish the SECURE-NET scientific results, workshops/conferences organised by the SECURE-NET partners, public events, workshops, and training schools, and SECURE-NET targeted networks and organisations.

Table 8: Dissemination Target Audience, Objectives and Channels

Target Audience	Dissemination Channels
TA1	• Peer-reviewed articles in high-impact journals; Open Access publishing. • Participation in leading academic conferences with presentations/posters. • Dissemination through SECURE-NET partners' and other networks, such as SPARTA, CyberSec4Europe, European Quantum Communication Infrastructure (EuroQCI), and others.
TA2	• *Channels listed next to TA1.* • Direct interactions during project events, conferences, and trade shows, such as Cyber Security and Cloud Expo. • Interactions with the European Cyber Security Organization (ECSO). • Start-up competitions, incubation spaces in partner countries, training and business consultancy services offered by SECURE-NET beneficiaries (RIA, KEYS).
TA3	• Participation in leading academic conferences with presentations/posters. • Direct interactions during project events and conferences with regional/national policymakers. • Direct interactions with the European Union Agency for Cybersecurity (ENISA), EDPB and the Directorate-General for Communications Networks, Content and Technology.
TA4	• Popular science articles based on research articles produced by the consortium published in national media, popular science journals, science news portals and European media, particularly written by/or showcasing research done by female team members. • Guest lectures for students; engagement in European Researchers' Night, European Women Researchers' Day and celebration of International Day of Women and Girls in Science in February.

The SECURE-NET project partners will target international journals and magazines to disseminate the project's research results and build an international reputation. Table 9 provides a sample of the target journals and magazines.

To disseminate research results and build an international reputation, invite collaboration, and support the uptake of R&I results, the SECURE-NET partners will write and publish scientific papers at international and regional conferences and workshops. Table 10 lists several venues which the project partners will target.

To invite regional and international scientific communities to collaborate on SECURE-NET activities, the partners will organise scientific workshops at well-recognised international conferences. Table 11 lists a few SECURE-NET-associated workshops that partners plan to organise.

Table 9: Journals and Magazines for Publishing Scientific Results

Journal / Magazine	Publisher	Website
Computers & Security (COSE)	Elsevier Ltd.	https://www.sciencedirect.com/journal/computers-and-security
Journal of Information Security and Applications (JISA)	Elsevier Ltd.	https://www.sciencedirect.com/journal/journal-of-information-security-and-applications
Computer Standards & Interfaces (CS&I)	Elsevier Ltd.	https://www.sciencedirect.com/journal/computer-standards-and-interfaces
International Journal of Information Security (IJIS)	Springer	https://www.springer.com/journal/10207
Journal of Cryptographic Engineering	Springer	https://www.springer.com/journal/13389/
IEEE Transactions on Dependable and Secure Computing (TDSC)	IEEE	https://www.computer.org/csdl/journal/tq
IEEE Security and Privacy	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
IEEE Transactions on Information Forensics and Security	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206
ACM Transactions on Privacy and Security (TOPS)	ACM	https://dl.acm.org/journal/tops
Journal of Cybersecurity	Oxford University Press	https://academic.oup.com/cybersecurity/pages/about
IEEE Access	IEEE	https://ieeeaccess.ieee.org/
PeerJ Computer Science	PeerJ	https://peerj.com/computer-science/
Computer Networks	Elsevier Ltd.	https://www.sciencedirect.com/journal/computer-networks
Complex Systems Informatics and Modeling Quarterly (CSIMQ)	RTU Press	https://csimq-journals.rtu.lv/csimq

To raise awareness and provide training on SECURE-NET results, the SECURE-NET project partners will deliver workshops, seminars, and lectures. Partners will also participate in public events to inform the public about the project's activities and achievements, and to engage citizens and the societal sector. Table 12 presents a sample of venues for SECURE-NET training, workshops, and public events.

Potentially, different target audiences will form networks at both the national and European levels, including governmental institutions (national/EU), EC Agencies, and other European projects. Table 13 lists networks, organisations, and projects for disseminating the SECURE-NET achievements.

Table 10: Conferences to Submit and Publish the SECURE-NET Scientific Results

Conference (workshop)	Acronym	Website
International Conference on Advanced Computer Information Technologies	ACIT	https://acit.tech/
International Conference on Applied Cryptography and Network Security	ACNS	http://jianying.space/acns/
International Conference on Availability, Reliability and Security	ARES	https://www.ares-conference.eu/
International Conference on Business Informatics Research	BIR	https://bir2025.rtu.lv/
International Conference on Information Systems Engineering	CAiSE	https://caise-conference.diag.uniroma1.it/
ACM Conference on Computer and Communications Security	CCS	https://www.sigsac.org/ccs/CCS2026/
Conference in Cryptographic Hardware and Embedded Systems	CHES	https://ches.iacr.org/
Detection of Intrusions and Malware & Vulnerability Assessment	DIMVA 2026	https://www.dimva.org/dimva2026/
European Symposium on Research in Computer Security	ESORICS	https://sites.google.com/di.uniroma1.it/esorics2026/home
IEEE European Symposium on Security and Privacy	EuroS&P 2026	https://eurosp2026.ieee-security.org/
Conference on Computer Science and Intelligence Systems	FedCSIS 2026	https://2026.fedcsis.org/
International Symposium on Foundations & Practice of Security	FPS	https://hub.imt-atlantique.fr/fps2025/
International Conference on Historical Cryptology	HistoCrypt	https://histocrypt.org/
Nordic Conference on Secure IT Systems	NordSec	https://www.nordsec.org/conferences/
Practices of Enterprise Modelling	PoEM	https://poem2025.unige.ch/
Research Challenges in Information Science	RCIS	https://www.rcis-conf.com/rcis2025/
Security and Cryptography for Networks	SCN	https://scn.unisa.it/scn26
International Security & Privacy Conference	SEC	https://ifipsec.org/
International Conference on Security and Cryptography	SECRYPT	https://secrypt.scitevents.org
USEMIX Security Symposium	Usenix Security	https://www.usenix.org/conference/usenixsecurity26

Table 11: Workshops/Conferences Organised by the SECURE-NET Partners

SECURE-NET-associated workshop	Venue	Timing
International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I)	ARES	Annually
International Baltic Conference on Digital Business and Intelligent Systems (Baltic DB&IS)	-	Biannual
International Conference on Information and Software Technologies (ICIST)	-	Annually
Information Society and University Studies (IVUS)	-	Annually

3.3 Open Science

As defined in [1], the partners will be committed to open science principles when publishing articles and papers. The open science practices will include:

- Open access (OA) to publications.
- Early open sharing of research (including presentations and training material). Specifically, at the latest at the time of publication (to the conference or journal), a machine-readable electronic copy of the published version or the final peer-reviewed manuscript accepted for publication will be deposited in the ZENODO platform <*https://zenodo.org/communities/secure-net*>.
- Encouraging the reproducibility of research outputs.

More information on data management can be found in D5.2 Data Management Plan [5].

3.4 Planned Dissemination Activities

Training events for researchers and innovators. To transfer knowledge between academic and non-academic partners on central topics in cybersecurity that are of common interest, we will organise four in-person consortium-wide training events, covering advances, cutting-edge methodologies, challenges, and gaps in the following areas:

- ***Secure cyber-physical systems*** (M12). The SECURE-NET partners will share their research and development on safeguarding data in such systems and implementing measures to detect and respond to threats that could impact physical operations.
- ***Security certification*** (M24). The SECURE-NET partners will discuss advances in security certification methods and the development of security certification labels for devices, software, and organisations.
- ***Human-centric aspects of cybersecurity*** (M36). The SECURE-NET partners will share best practices and educational innovations in teaching cybersecurity to (future) professionals, as well as ways to improve the usability of cybersecurity solutions.
- ***Post-quantum cryptography*** (M47). The SECURE-NET partners will share their innovations in developing cryptographic systems that are secure against both quantum and non-quantum computers, while interoperable with existing communication protocols and networks.

Table 12: Public Events, Workshops, and Training Schools for SECURE-NET Dissemination

SECURE-NET-related event	Country	Website
EU Cyber Acts	EU	https://eucyberact.org/
CYBERSEC EXPO & FORUM, European Cybersecurity Forum	EU	https://2025.cybersecforum.eu/
ENISA European Cybersecurity Skills Conference	EU	https://www.enisa.europa.eu/events/european-cybersecurity-skills-conference-2026
ENISA European Cybersecurity Certification Conference	EU	https://www.enisa.europa.eu/events/2026-european-cybersecurity-certification-conference
it-sa Expo&Congress	EU	https://www.itsa365.de/en/it-sa-expo-congress
Cyber Security & Cloud Expo Europ	EU	https://cybersecuritycloudexpo.com/europe/
Cybersec Europe	EU	https://www.cyberseceurope.com/
CYBERSEC EXPO & FORUM	EU	https://www.cybersecforum.eu/2026/en/
International Cyber Security Trade Fair	EU	https://cybersecurityexpo.pl/en/
INCYBER Forum Europe	EU	https://europe.forum-incyber.com/en/home-en/
Cybertech Europe	EU	https://italy.cybertechconference.com/
Cyber Security World Madrid	EU	https://www.techshowmadrid.es/en/cyber-security-world
SICUR, Madrid, Spain.	EU	https://www.ifema.es/en/sicur
Infosecurity Europe	World	https://www.infosecurityeurope.com/
Cloud & Cyber Security Expo	World	https://www.techshowlondon.co.uk/cloud-cyber-security
Black Hat Europe	World	https://blackhat.com/
International Security Expo	World	https://www.internationalsecurityexpo.com/
INCYBER Forum Europe / FIC	World	https://www.forum-fic.com/en/home/
Küberinnovatsioon	Estonia	https://kuberinnovatsioon.cs.ut.ee
Estonian Summer School on Computer and Systems Science (ESSCaSS)	Estonia	https://courses.cs.ut.ee/t/esscass2026/
DevConf	Czech Republic	https://www.devconf.info/cz/
Prague Cyber Security Conference	Czech Republic	https://www.praguecyber.com/
Europen	Czech Republic	https://www.europen-packaging.eu/
Santa's Crypto Get-Together	Czech Republic	https://mkb.tns.cz/index.short.html.en
ONE Conference	Netherlands	https://one-conference.nl/
Kyiv International Cyber Resilience Forum (KICRF)	Ukraine	https://cyberforumkyiv.org/en
EXPERT SECURITY	Ukraine	https://expert-security.com.ua/en/
Security 2.0	Ukraine	https://bezpeka.ua/
CYBERSECURITY	Ukraine	https://kiberbezpeka.bezpeka.ua/

Table 13: SECURE-NET Targeted Networks/Organisations

Name	Country/ region/ type	Website
Network Security Monitoring Cluster	Czech Republic	https://www.nsmcluster.com/en/
CESNET	Czech Republic	https://www.cesnet.cz/
Cyber defence unit of the Defence League	Estonia	https://www.kaitseliit.ee/en/cyber-unit
International Centre for Defence and Security	Estonia	https://icds.ee/
Foundation CR14	Estonia	https://cr14.ee/
Startup Estonia	Estonia	https://startupestonia.ee/focus-areas/cybertech
eGovernment Academy: National Cyber Security Index	Estonia	https://ncsi.ega.ee
European Cybersecurity Competence Centre (ECCC)	EU	https://cybersecurity-centre.europa.eu/
European Cyber Security Organisation (ECSO)	EU	https://ecs-org.eu
European Network and Information Security Agency (ENISA)	EU	https://www.enisa.europa.eu
Strategic programs for advanced research and technology in Europe (SPARTA)	EU	https://www.sparta.eu/
Cyber Security Network of Competence Centres for Europe (CyberSec4Europe)	EU	https://cybersec4europe.eu/
Cyber Security Excellence Hub in Estonia and South Moravia (CHESS)	EU	https://chess-eu.cs.ut.ee/
Cybersecurity Certification and Assessment Tools (CCAT)	EU	https://cordis.europa.eu/project/id/101225878
Quantum-Resistant Cryptography in Practice (QARC)	EU	https://cordis.europa.eu/project/id/101225691

Training events for support staff. In parallel to the four events for researchers and innovators, SECURE-NET partners will organise mutual learning activities for the support staff of our partners to build R&I support capacity in both the academic and non-academic sectors. Support staff of diverse profiles (e.g., grant consultants, technology transfer officers, project managers, and HR staff) will share best practices in areas such as identification of relevant funding sources and proposal writing, with a focus on innovation grants such as European Innovation Council funding, project management, organisation of technology transfer and IP protection, impact and researcher assessment. An important aspect of these events will be building stronger connections among participants so that support staff can, for example, exchange information on partner searches within their institutions when relevant.

Practical aspects and challenges of implementing cybersecurity measures in times of war. The last strand of the mutual learning events builds on the unique experiences of our Ukrainian partners in cybersecurity during wartime. POE and PNU, a large regional Ukrainian electricity distribution system operator and a Ukrainian university, respectively, will lead a series of webinars for partners to share their experiences and best practices in implementing new cybersecurity measures to address external threats. The webinars will provide an opportunity to discuss the remaining or emerging issues that still need to be addressed in that area and, together with all partners, explore ways to integrate them into their research and innovation activities.

In addition to the direct benefits to participants in secondments and mutual learning events from both widening and non-widening countries, the new knowledge will be disseminated across partner organisations, with a focus on knowledge diffusion activities in widening institutions. Local seminars will be organised to transfer knowledge from SECURE-NET participants to other staff, strengthening the R&I human capital base in other countries.

3.5 Monitoring

Monitoring of SECURE-NET results dissemination success is closely related to partners' performance, the success of the scientific results, and the number of trained cybersecurity specialists, support staff, and other participants to whom the project’s results are disseminated. Table 14 presents key performance indicators to be monitored during the project. Reporting on dissemination activities will be conducted alongside communication reporting, as indicated in Table 6.

Table 14: SECURE-NET Dissemination Key Performance Indicators

Key performance indicators	M24	M48	4 y. after	8 y. after
DKPI1. Number of scientific papers on cybersecurity in high-impact journals (co-)authored by SECURE-NET teams	1	4	6	8
DKPI2. Number of trained cybersecurity specialists in joint events	20	40	80	100
DKPI3. Number of trained support staff in joint events	10	30	40	50
DKPI4. Number of participants at the seminars on practical aspects and challenges of implementing cybersecurity measures in times of war	20	40	-	-

4 Exploitation Strategy and Plan

The purpose of exploitation is to make concrete use of the project's results. In this section, the SECURE-NET exploitation activities, expected results activities and monitoring activities are overviewed. It also presents a brief discussion on potential exploitation barriers, their mitigation strategies and intellectual property management.

4.1 Exploitation Activities and Expected Exploitable Results

The nature of SECURE-NET dictates that the set of exploitable results comprises the project's outcomes and deliverables, which are flexible by design. The outline of exploitation activities and the nature of expected results in connection to planned SECURE-NET activities is given in Table 15. The projected exploitable results are grouped as follows:

- Various results of individual secondments. The planned secondments will serve as a key source of exploitable results. The tentative timeline and contents of all secondments are outlined in the SECURE-NET secondment strategy [2] and the personal career development plans [3].
- Recommendations based on a series of webinars on the challenges of implementing cybersecurity measures in times of war. This result will be released as a publicly available SECURE-NET deliverable D3.1. Due date is M24.
- Recommendations for strengthening local innovation ecosystems based on the outcomes of secondments within the same widening countries. This result will be released as a publicly available SECURE-NET deliverable D2.3. Due date is M42.

4.2 Monitoring

Monitoring of SECURE-NET results exploitation success is closely intertwined with monitoring of the project's communication and dissemination activities outlined in Sections 2 and 3. There are, however, exploitation-specific key performance indicators (see Table 16) that will have to be monitored not only during the project but also after its completion. Reporting on the results will follow the DEC deliverables production plan outlined in Section 2.6.3 of this document.

Table 15: SECURE-NET Exploitation Activities and Types of Exploitable Results

<table>
<tr><th>SECURE-NET activities</th><th>Exploitation activities</th><th>Types of exploitable results</th></tr>
<tr><td>35 Individual secondments involving 31 talents[2]:
• 16 researchers going on cross border secondments to non-academic partners,
• 9 innovators going on cross-border secondments to academic partners,
• 6 researchers going on local innovation ecosystems strengthening secondments.</td><td>• Carry out research studies,
• Carry out feasibility studies,
• Develop new techniques or update existing ones,
• Design, develop and/or implement new products,
• Specify, develop and/or deploy new services,
• Improve existing products or services,
• Design and develop prototypes of specialised tools or products,
• Develop cross-sectoral cooperation ideas,
• Integrate any of the above into activities of the sending institution by extending or developing study courses, policy and operational frameworks, etc.,
• Define recommendations based on the outcomes of said activities.</td><td>• New or updated technique,
• New/updated product,
• New/updated service,
• New/updated prototype or proof of concept,
• State-of-the-art review/study or feasibility study,
• Knowledge transfer package,
• New joint project proposal or its draft,
• Recommendations,
• New or extended training/study course.</td></tr>
<tr><td>Consortium-wide mutual learning activities[3]:
• 4 training events for researchers and innovators on M12, M24, M36, and M47,
• 4 co-located training events for support staff,
• 4 webinars on the topics related to the challenges of implementing cybersecurity measures in times of war.</td><td rowspan="2">• Deliver public lectures and talks
• Create and share recordings training materials,
• Conduct discussions, round tables, idea generation workshops,
• Present demonstrations or case studies based on work done within the project,
• Develop new joint project proposals,
• Seek out new partnerships between project participants and other academic and non-academic institutions, companies, and organisations,
• Define recommendations based on the outcomes of said activities.</td><td rowspan="2">• Presentation materials
• Recordings
• Demos
• Case studies
• New project proposals
• New partnership agreements
• Recommendations
• Other results</td></tr>
<tr><td>Local training seminars by seconded researchers and innovators at their home their sending organisations as necessary.</td></tr>
</table>

[2] See deliverable D1.1 for more details [2].
[3] See more in SectiAn 2.

Table 16: SECURE-NET Exploitation Key Performance Indicators

Key performance indicators	M24	M48	4 y. after	8 y. after
EKPI1. Number of staff going on cross-sectoral secondments/exchanges/visits	10	31	62	>100
EKPI2. Number of joint proposals, involving at least 3 SECURE-NET partners	1	3	6	12
EKPI3. Number of cross-sectoral collaboration projects	3	7	12	18
EKPI4. Number of new/updated techniques, products, services, prototypes, etc.	0	3	7	15
EKPI5. Number of student theses co-supervised across sectors	0	2	5	10
EKPI6. Percentage increase in the # of international staff (average across universities and businesses in widening countries)	0%	0%	2%	5%
EKPI7. Percentage increase in the # of international students (average across universities in widening countries)	0%	0%	2%	5%
EKPI8. Number of new partnerships between actors in the academic and non-academic sectors (involving widening countries)	0	2	5	10
EKPI9. Percentage increase of female representation in leading academic positions in ICT/computer science/cybersecurity (in widening countries)	0%	0%	2%	4%

4.3 Potential Barriers for Exploitation and Mitigation Strategies

Potential barriers to the success of exploitation activities are outlined in the Risk Management Plan, available in [4]. The potential barriers include risks associated with the SECURE-NET *secondment strategy* (e.g., the project milestones are not met, hindering results; the secondment strategy is not utilised by partners; major changes in personal career development or secondment plans; and similar), risk related *to personnel and intended audience* (e.g., key personnel are unavailable; talents not properly supported by host institutions; failure of talents to implement their experience and knowledge gained from secondments at their home institution), risks associated to *secondments in Ukraine* (e.g., sensitivity of cybersecurity topics, particularly during wartime; restricted access to data and data management in Ukraine during high alert or energy/security incidents; threats to health, life, and property due to Russia's ongoing war against Ukraine; and similar), risk linked to *technology use* (e.g., a loss of connectivity or power interruptions affecting experiments or meetings), and risk related to the *quality of the results* (e.g., presentations, case studies, or methodologies may differ in depth or clarity, reducing learning effectiveness; lessons learned during workshops and exchanges may not translate into practical improvements or follow-up actions, and similar). Mitigation measures (e.g., regular project meetings to discuss the project progress, pseudo-anonymisation and use of synthetic datasets, organisation of the remote meeting to discuss issues related to the secondments in Ukraine, continued monitoring of the secondment progress, use of the redundant communication links and others) are also listed in [4].

4.4 Intellectual Property Management

An important goal of our project is to bridge the gap between research and innovation. This gap is partially due to the different goals that often drive academic and commercial actors: researchers generally want to publish and publicise their work widely, while companies do not want to jeopardise potential IP applications. The SECURE-NET partners will be committed to the principles of intellectual property management as agreed in the consortium agreement and grant agreements [1] [6]. The SECURE-NET general approach is that all project activity and outputs will be considered open and shareable, unless explicitly decided otherwise.

5 Concluding Remarks

This deliverable outlines the plan for the SECURE-NET communication, dissemination, and exploitation. It defines the objectives, identifies target audiences, and provides an overview of the strategic activities and monitoring metrics. Table 17 summarises the specific activities for communication, dissemination, and exploitation, along with the monitoring approach.

Regarding communication, the SECURE-NET project partners will announce accepted and published papers and conference/workshop talks on social media (Facebook and LinkedIn) and on the SECURE-NET website. Partners will write newsletters about the organised events, publish on the SECURE-NET website (and partners' websites). SECURE-NET will invite regional and international partners to collaborate in the research activities. The partners will promote training events and seminars on the SECURE-NET website, social media, and partners' networks, highlighting the organised scientific and training workshops/seminars, as well as other events.

Regarding dissemination, the SECURE-NET partners will present research results at international conferences and workshops, as well as to companies in seminars, regional workshops, training schools, etc. They will publish in international venues– journals, conferences, workshops, and publish the scientific workshop proceedings with recognised publishers. Partners organise scientific workshops at international venues. Organise 4 training events for researchers and innovators, 4 training events for support staff, and seminars on practical aspects and challenges of implementing cybersecurity measures in times of war. The SECURE-NET partners will also organise seminars, regional workshops, and training schools for companies to present research results. The public project deliverables will be shared using the CHESS website.

Regarding exploitation, the SECURE-NET project will publish articles and papers in recognised venues using open-access principles. Project partners will share the conference presentations, training and seminar presentations, the SECURE-NET-related master thesis on the SECURE-NET website. SECURE-NET will transfer research results into practical use (e.g., creating prototypes, software, and demonstrations) and apply research outputs in companies. Partners encourage trained participants to apply their knowledge in their daily activities. The partners will submit research and cross-sectoral collaboration proposals.

The plan for dissemination, exploitation and communication will be updated by M36 in D4.3. M24, and the final report by M47 will produce the interim report on communication, dissemination, and exploitation.

Table 17: Strategic Activities to Achieve Objectives

Objectives	Communication	Dissemination	Exploitation
O1: Share research results	• Announce about accepted papers, conference/workshop talks on social media (Facebook, and LinkedIn). • Announce about published paper on SECURE-NET website. • Write newsletters about the organised events, publish on the SECURE-NET website (and partners' websites).	• Present at international conferences and workshops. • Publish in international venues– journals, conferences, workshops. • Publish scientific workshop proceeding with recognised publishers. • Present research results to companies in seminars, regional workshops, training schools etc.	• Share the conference presentations on SECURE-NET website. • Publish articles and papers using open access principles in the recognised venues. • Share supervised, defended SECURE-NET Master thesis.
O2: Invite to collaborate	• Invite regional and international partners to collaborate in the research activities. • Write newsletters about the organised events, publish on the SECURE-NET website (and partners' websites).	• Organise scientific workshops at international venues.	• Transfer research results to practical use (create prototypes, software, demonstrations). • Apply research outputs in companies.
O3: Provide training and awareness	• Promote training events, and seminars on SECURE-NET website and social media. • Promote training events, and seminars in SECURE-NET partners' networks • Write newsletters about the organised events, publish on the SECURE-NET website (and partners' websites).	• Organise four training events for researchers and innovators • Organise four training events for support staff • Organise seminars on practical aspects and challenges of implementing cybersecurity measures in times of war. • Organise seminars, regional workshops, training schools for companies to present research results.	• Share training and seminar presentations openly on the SECURE-NET website. • Encourage trained participants to apply the gained knowledge in their daily activities.
O4: Inform about achievements	• Write newsletters about the organised events, publish on the SECURE-NET website (and partners' websites).	• Share the public SECURE-NET deliverables using the SECURE-NET website.	
O5: Ensure sustainability			• Submit research and cross-sectoral collaboration proposals

References

[1] SECURE-NET Grant Agreement, Project 101217315, 2025, https://cordis.europa.eu/project/id/101217315

[2] SECURE-NET Deliverable D1.1, SECURE-NET Secondment Strategy, 2025

[3] SECURE-NET Deliverable D1.2, Personal Career Development Plan, v. 1, 2026

[4] SECURE-NET Deliverable D5.1, Project Management and Risk Management Plan, 2025.

[5] SECURE-NET Deliverable 5.2. – Data Management Plan, Project 101217315, 2025, https://cordis.europa.eu/project/id/101217315

[6] SECURE-NET Consortium Agreement, 2025.