CyberAgent

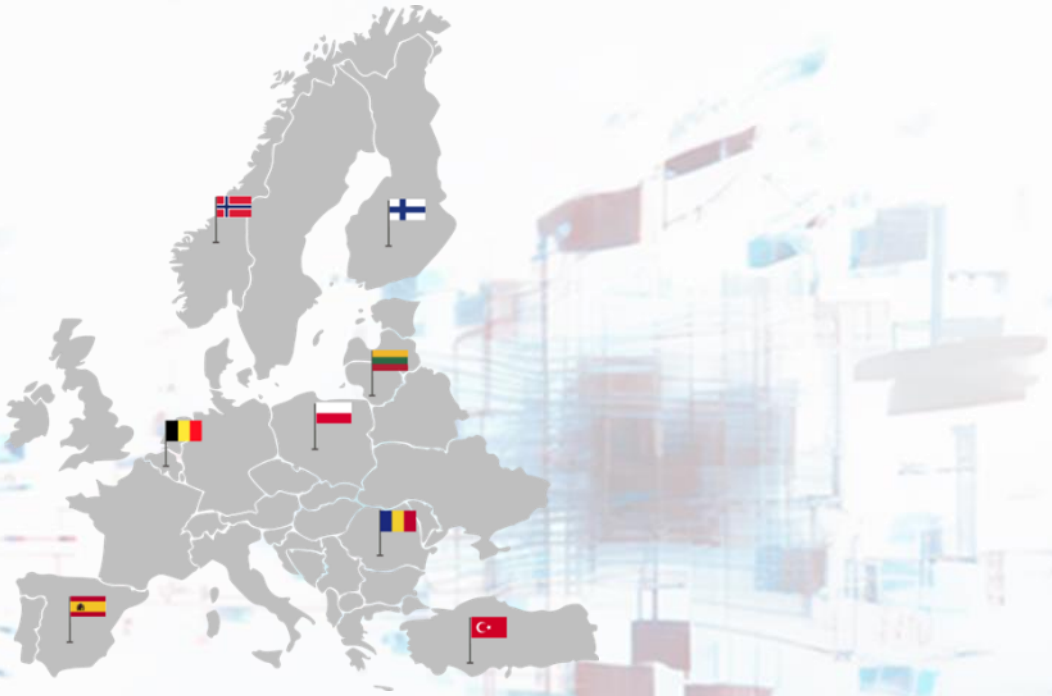
Co-funded by the European Union

DISSEMINATION & COMMUNICATION STRATEGY

CYBER AGENT 10.2023

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Work Package 6: Dissemination & Exploitation

Deliverable 6.1: Dissemination & communication strategy

Leader of WP6 and deliverable 6.1 – Women4Cyber

CONTENT

ABBREVIATIONS

CEN – The European Committee for Standardization

CENELEC – The European Committee for Electrotechnical Standardization

ECSO – The European Cyber Security Organisation

ENISA – The European Union Agency for Cybersecurity

EU – The European Union

HEI – Higher Education Institution

SME – Small and medium-sized enterprise

VET – Vocational education and training

WP – Work Package of the project

INTRODUCTION

This document describes the three-year plan for the dissemination and communication activities of the project, including: the visual identity, project website development, stakeholder map, strategy for dissemination, communication and engagement of project summary, guidelines publication and results exploitation, a schedule of dissemination, communication, and engagement activities, the medium that will be used to reach the stakeholders, schedule for producing internal newsletters, schedule of dissemination meetings including high level project end results presentation.

PROJECT DESCRIPTION

CyberAgent aims to create a platform that equips the target group with cybersecurity and entrepreneurial skills, fostering inspiration, empowerment, upskilling, reskilling, and engagement among SME employees. This initiative also seeks to **increase the participation of women in the IT sector** by taking the role of Cyber Security Change Agent.

The project will **facilitate collaboration between Higher Education Institutions (HEIs), Vocational Education and Training (VET) institutions, and SMEs,** promoting the exchange of best practices in cybersecurity and the job market. Moreover, it aims to enhance the employability of the target groups, support SMEs in building their cyber resilience, preserve their reputation and competitiveness, and raise organisational cybersecurity maturity and culture.

The primary beneficiaries of this project **are SME employees**, with a particular focus on women, who require upskilling to play the role of a Change Agent in cybersecurity SMEs. **Secondary target groups** encompass **HEIs and VETs**, who can incorporate the training content into their programs, benefiting students and trainees.

The project encompasses the development of **8 up-to-date training modules covering various aspects of cybersecurity**, including technical, analytical, risk management, and organisational skills. These modules will be accessible through an online platform and can be utilised for blended learning.

Project results will be piloted with at least 80 participants, including at least 30 women, from 8 countries. Additionally, it will involve 24 VET trainers and 10 HEI teachers.

The project's results will be available to the public throughout and beyond its duration. Within 3 years following the project's conclusion, the training courses will be extended to reach a minimum of 800 more SME employees in 100 SMEs within partner countries. English versions of the materials will be used for dissemination in other European countries to further expand the project's reach.

PARTNERS

The project consortium comprises eight partners, with Vilnius University serving as the coordinator, representing a wide range of European locations.

	Participating Organisation Legal Name	Country	Role
1	Vilniaus Universitetas	Lithuania	Coordinator
2	Liceul Tehnologic „Grigore C. Moisil" Buzau	Romania	Partner
3	Women4Cyber Mari Kert - Saint Aubyn Foundation	Belgium	Partner
4	Ecosistemas Virtuales Y Modulares SL	Spain	Partner
5	Prios Kompetanse AS	Norway	Partner
6	Teknopark Istanbul Mesleki Ve Teknik Anadolu Lisesi	Turkey	Partner
7	Hackeru Polska Spolka z Ograniczona Odpowiedzialnoscia	Poland	Partner
8	Olemisen Balanssia Ry	Finland	Partner

The consortium includes one higher education institution, two VET institutions (from Romania and Turkey), four organizations from the labor market, and one NGO.

See Annex 1 - Partners website and social medias.

AIM OF THIS DOCUMENT

The aim of this document is to cover both European and national dissemination activities. To guarantee an efficient implementation at local and EU level, all partners will turn the Dissemination Plan into national dissemination plans, adapted to the local context. Moreover, this document will focus on outlining the methods and strategies employed to effectively communicate both the project's outcomes and its ongoing progress to the primary target audiences and relevant stakeholders.

MAIN ACTIVITIES

To effectively disseminate the Cyber Agent project activities, we will employ a strategic and comprehensive approach. First, we will utilise our project platform and social media channels to broadcast updates, announcements, and highlights of these activities, making them accessible to our target audience. The use of engaging multimedia content, such as videos, photos, and infographics, will play a pivotal role in conveying the value and impact of these events. Additionally, we will leverage direct outreach through email newsletters and personalised invitations to ensure stakeholders are well-informed and encouraged to participate. Our strategy will also involve collaboration with partner organisations, encouraging a wider participation.

1) **The definition and creation of visual identity guidelines** that will ensure that the project will rely upon a recognized brand once disseminated. Specifically, the visual identity will be translated in the creation of the project's logo, tagline and documents' templates (see section 5.1).

2) **The production of the following offline and online communication materials:**

- **Project's website and digital platform** (embedded into the project's website) that will be developed in line with the latest design, mobile and user-friendly techniques and it will become the face of the project.
- **1 Poster/Leaflet and a roll-up** that will be used to promote the project during the international bootcamps, will be available for download and will be updated every 6 months with new content that will follow the project's progress and development.
- **Social media profiles** in the main channels (at least 1 project's profile on Facebook, Twitter, LinkedIn, YouTube and Instagram) that will help achieve better recognition of the project activities among the wider public, above all HEIs teachers, SME employees, VET providers and public and private agencies working on business support.
- **E-newsletters**, produced on a quarterly basis and aimed to disseminate the intermediate results on a large scale. The e-newsletter will be sent via email to all registered users (involved stakeholders and other interested audience) and through the partners' networks. E-newsletters will also be published on our project's and partners' websites.

3) **The production of the following audio-visual materials:**

- **4 Infographics** to be produced to promote project activities and results.
- **2 promotional videos**, the first one short (maximum 3 minutes) and the second one long (maximum 10 minutes), that will be used to promote the project and to stimulate debates during the planned dissemination events. The videos will be shot in the original languages of the participants, include English subtitles and be uploaded to the YouTube account of our project.

4) **The organisation of the following dissemination events**:

- **1 Final Conference** (to be held in Belgium on month 36 to present our project's activities and results to a bigger audience and launch the students' competition for the EU award.

DISSEMINATION RESPONSIBILITIES

Each partner will be responsible for dissemination activities within their own country and using their own networks, contacts and dissemination channels. All of the partners are already investing resources in educating SMEs on the need to improve cybersecurity skills.

As Dissemination WP leader Women4Cyber will coordinate the dissemination activities and will measure their impact across the consortium partners' channels. The WP leader has proven expertise in communication plans addressing business creation, support to SME staff, entrepreneurship students and career centers. Moreover, its position as dissemination leader in the project will ensure that the design and production of an effective dissemination strategy will promote the EU added value of the project.

Each partner will be responsible for planning their own dissemination activities and reporting back to the WP leader, which will design a dissemination plan template to be used for both planning and reporting purposes. The reports on dissemination activities will be filled out on a 6-months basis.

1. DISSEMINATION PLAN

1.1. OBJECTIVES

The success of the CyberAgent project relies significantly on how effectively we communicate and share our progress, results, and goals with our target audiences and stakeholders. In this Dissemination Plan, we outline a clear set of objectives to guide our efforts:

- To increase awareness of the project, its objectives and milestones reached.
- To make all the relevant project results public to target groups (dissemination).
- To engage with target audiences in a reciprocal exchange (communication), by using online channels for ongoing dialogue and feedback.
- To ensure effective collaboration between the partners for a coherent, joint dissemination and exploitation effort.
- To establish and maintain a positive and consistent project image.
- To identify and engage with key stakeholders in the project's field.
- To monitor and evaluate the effectiveness of dissemination strategies and adjust as needed.
- To involve local communities in project activities and encourage their active participation.

These objectives will contribute to a comprehensive and well-rounded Dissemination Plan for the CyberAgent project.

1.2. TARGET AUDIENCES

- SME employees
- Women in cybersecurity
- HEI teachers
- HEI entrepreneurship students
- VET providers
- VET trainees
- Students
- Unemployed people
- EU Policy makers
- National decision makers
- European Commission
- Labour market actors and other cybersecurity practitioners
- Broad public
- Media and secondary disseminators
- Research and Academic Communities
- Business associations
- IT Professionals and Women Associations

1.3. CRITERIA FOR SUCCESS

In our pursuit of disseminating the CyberAgent project effectively, it is crucial to outline the key principles and practices that will guide our communication efforts. This list encapsulates our approach to disseminating information about the project and engaging with our target groups and stakeholders:

- **Use clear language** which is suited to the target groups: in all our publications, partners will make sure to emphasize the main messages and benefits of the project for each specific group we are addressing.
- The aim of the dissemination is primarily to **distribute neutral information** about the project.
- **Prioritize quality interactions over the quantity** of emails sent. We aim to engage the right contacts within the relevant institutions in meaningful discussions about the project. Our hope is that these contacts will, in turn, use their own networks to spread the word about the CyberAgent project.
- The publications should be created and formatted to be **suitable for various national contexts**. If multiple publications are produced, it is essential for the partners to **adhere to a consistent graphic and text style**. Prior to releasing a campaign, the partners should decide on the responsible party for developing the unified design. It's important to mention that partners must incorporate the project logo, the EU flag, and the disclaimer in all their publications (see section 5.2).
- Make sure to **disseminate information in a timely manner**, aligning with project milestones and developments to keep stakeholders informed promptly.
- **Utilise a variety of communication channels**, such as social media, newsletters, press releases and events, to reach targeted audience.
- Ensure that all project materials are **accessible to individuals with disabilities**, complying with accessibility standards and guidelines (for instance, include captions and descriptive transcripts for social media posts).

1.4. ACTIVITIES

Dissemination of the project will be related to tangible project results.

Prior to the dissemination of each result or organised activity, **the lead organisation for dissemination (Women4Cyber) will prepare dissemination templates** and agree them with the coordinator and the quality management committee. The approved version will be presented to the partners so that **they can disseminate a unified message**. Partners will be able to adapt, localise and disseminate these templates to stakeholders through their own dissemination channels and contacts.

The following is a description of the activities and deliverables, and what impact is expected from the required dissemination of the project.

Train the trainer Bootcamp

It is a mobility activity involving trainers and trainees from partner countries. This intensive 3-day training course leverages resources developed in WP3, WP4, and WP5, offering participants the opportunity to engage in various learning activities. These activities will be broadcasted online, making them accessible to the wider Higher Education (HE) and Vocational Education and Training (VET) community across the EU. The bootcamp, unlike many cybersecurity events, takes a unique approach by focusing on SMEs and emphasizing problem-based learning and case studies. This physical event, with remote attendance options, stands out as a valuable initiative, inspiring similar events beyond the project's conclusion.

Stakeholder workshops

Six stakeholder workshops are scheduled at M6, M10, M14, M20, M26, and M32 to gather input from diverse stakeholder groups. These workshops, conducted online or in person, are essential for tailoring and scaling the SME Cyber Security Change Agent program effectively. They also serve to engage policy makers, raise cybersecurity awareness among SMEs, and provide valuable insights for policy development in education and cybersecurity. One of the workshops will take place in Brussels, organised by Women4Cyber, engaging EU policy makers directly.

Training programmes for HEI and VET students

The project will develop comprehensive training programs for Higher Education Institution (HEI) and Vocational Education and Training (VET) students, comprising 8 modules. These modules will be available in electronic format, accessible in both English and the languages of the project partners. The training materials, designed to meet micro-credential requirements for HE students, VET students, and SME employees, offer a diverse range of formats to accommodate various learning preferences. These resources encompass short presentations, videos, notes, best practice showcases, online resource libraries, concise toolkits for adapting innovative models and technology in agribusinesses, case studies, role-playing simulations, training activities, assignments, peer exercises, and assessment tasks.

Additionally, specific dissemination activities have been designed to foster the transfer of knowledge to our project's target groups and especially to the end-users responsible to implement the project. Tangible results to be included within the strategy will be:

- **Training Needs Mapping Reports**, used to inform stakeholders about the research carried out, the issues and challenges identified and recommendations to address these challenges.
- **Cybersecurity Curriculum**, providing the basis for a EU-wide program on cybersecurity.
- **Cybersecurity Training Programme** design and delivery, providing dedicated support to SME employees and other interested stakeholders (i.e., VET providers and startups).
- **Cybersecurity Training Toolkit**, summing up the knowledge transferred to trainees and available to all other stakeholders interested to develop a capacity building process on cybersecurity.
- **Digital Platform and International Bootcamps**, pairing HEIs students as future SME employees with SMEs all across the EU.
- **Best Practices**, including success stories on the deployment of cybersecurity campaigns and targeting any VET providers interested in replicating the cybersecurity training programme.

1.5. DISSEMINATION & EXPLOITATION DELIVERABLES

Consortium partners are committed to making various reports and guides publicly available to actively involve the academic community in the project's implementation and outcomes. Those include for WP 6 – Dissemination & Exploitation:

- Dissemination & communication strategy including progress reports at M12, M24, and M36 (Lead by Women4Cyber);
- Stakeholder engagement plan including the organisation of 6 workshops (exploitation);
- Policy recommendations (exploitation);
- Good practice guide for SMEs (exploitation).

In this section, we will detail the Stakeholder Engagement Plan, the policy recommendations and the good practice guide for SMEs.

Stakeholder engagement plan

This task will focus on engaging with stakeholders and communities relevant to the project objectives, namely the cybersecurity SME industry, HEI and VET providers, and women in cybersecurity. The task leaders will develop an engagement plan that will be used to identify and track the most suitable stakeholder avenues to disseminate, elicit requirements about, and exploit the project outcomes. The engagement plan will include an outreach strategy and the organisation of 6 stakeholder workshops at M6, M10, M14, M20, M26, and M32. An initial Stakeholder Engagement Plan will be delivered in M6 and subsequent reports summarising the progress on the stakeholder engagement and workshops will be released at M12, M24, and M36.

SME partners will help develop the network of SME stakeholders while Women4Cyber will provide the link to the women in cybersecurity community. Women4Cyber will help promote the project's contribution towards gender balance by engaging women in the SME Cyber Security Change Agent programme and showcasing best practices and success stories from women participants. The project will be able to benefit from ongoing actions and best practices from Women4Cyber on skills development and gender diversity in cybersecurity.

Policy recommendations

This task will focus on mapping, analysing and positioning CyberAgent vis à vis relevant existing policies and strategies at EU level. The project will cover existing policies and best practices to inform the project implementation and highlight its added value throughout the project (i.e. via newsletters, social media, blogs).

Consortium members will develop a policy brief summarising lessons learned and offering recommendations to support ongoing EU policies and enhance SME cybersecurity through the CyberAgent project's upskilling efforts. These recommendations, derived from project outcomes and identified needs, will be presented in a report at the project's conclusion (M36). Leveraging existing relationships with the European Commission, ENISA, CEN CENELEC, and ECSO, Women4Cyber will facilitate communication channels to share project insights, emphasising their relevance to the cybersecurity landscape and potential impact on policies and strategies.

Good Practice Guide for SMEs

To ensure enduring support for SMEs in adopting the programme, the consortium will develop a comprehensive Good Practice Guide tailored specifically for SMEs. This guide will draw upon the insights gained from the implementation and lessons learned during the SME Cyber Security Change Agent program. Its core objective is to equip SMEs with sustainable guidelines and a practical toolkit, facilitating the seamless integration and continuous operation of the Change Agent role within their organisations. Additionally, it will feature best practices for promoting gender balance and encouraging the participation of women and other underrepresented groups in the cybersecurity domain. To assist SMEs in self-assessment, a checklist will be included, allowing them to gauge the readiness of their processes and tools for successful Change Agent program implementation. The delivery of this guide is scheduled for the project's conclusion at month 36 (M36).

2. TIMELINE AND ACTION PLAN

This plan outlines the phases of dissemination for the Cyber Agent project, focusing on the key activities and using relevant communication channels to engage stakeholders, experts, and target audiences. Each phase is designed to maximize visibility and impact.

Phase 1: Project Introduction and Networking (M1-M6)

Core Objective: To establish a strong online presence and create awareness about the project. Networking and engagement with potential stakeholders are vital. The focus is on building a foundation for the project's success. This includes getting information about the project on the internet, communicating with stakeholders and building a framework for successful project implementation.

At this stage, it is important to introduce the project to the stakeholders, emphasize the transparency of the project and involve them in the project activities and dissemination: introduce the project, its objectives, the results we plan to produce, and highlight the importance and impact of the project. Emphasise the commitment of the project consortium to strengthen the cybersecurity knowledge of the stakeholders and to increase the resilience of the organisations to cyber-attacks.

Tasks:

- Design a comprehensive visual identity.
- Launch a project website as a central information platform.
- Launch project' social media accounts and prepare social media campaigns.
- Invite stakeholders to engage with the project through social media channels. Encourage them to follow, share, and participate in discussions related to cybersecurity.
- Announce project goals and partners on social media.
- Issue a press release to inform stakeholders and target audiences.
- Send out a project newsletter to introduce the project.
- Build an email list for future engagement.
- Develop presentation which partners will use during events, conferences, meetings when presenting their organisations etc.
- Produce and print roll-up that will be used to promote the project during the international bootcamps, will be available for download in every partner organisation.
- Organise workshops for stakeholders.
- Network with other projects, initiatives and organisations that promote women in IT.
- Ask the project consortium partners to announce the project through their own channels.
- Participate in EU events such as Safer Internet Week, European Cyber Security Month, All Digital Week, Girls in ICT, etc. and disseminate information about the project.
- Identify and engage potential stakeholders for collaboration.

This dissemination strategy foresees that preparatory activities should be performed to help launch the dissemination events later on during the project lifetime (*see Annex 1: Preparatory activities Gantt chart).*

Phase 2: Research and Curriculum Development (M7-M13)

Core Objective: The aim of this phase is to maintain contact with existing stakeholders, to broaden the network of contacts and to encourage exchanges and dialogue among external stakeholders to share challenges, solutions and practices, and to have a system-level impact, as tangible results will be felt to have been generated during this phase.

This phase involves engaging stakeholders in the research, informing stakeholders about the progress of the project, ensuring transparency, sharing up-to-date information on the development of curriculum, engaging experts, and promoting project activities and events.

Tasks:

- Update presentation with news which partners will use during events, conferences, meetings when presenting their organisations etc.
- Create engaging content for social media and promote upcoming events and milestones on social media.
- Regularly update the content (news, activities, interviews, reports, deliverables etc.) of the project website, partner websites and social media.
- Promote upcoming training modules.
- Host expert-led webinars and discussions.
- Organise workshops for stakeholders.
- Maintain contact with other projects, initiatives and organisations that promote women's involvement in IT, provide updates on project activities and results, and expand the contact list.
- Ask the project consortium partners to update you on the project through their own channels.
- Participate in EU events such as Safer Internet Week, European Cyber Security Month, All Digital Week, Girls in ICT, etc. and disseminate information about the project.
- Encourage contributions from experts, which can be shared on the website or social media.

Phase 3: Developing Training Material, Integration into Platform and Initial Testing (M14-M24)

Core Objective: This phase focuses on the dissemination of the developed curricula and training materials, as it will include the development and validation of the training materials in English and in the national languages of the partners, the development of the training platform, and the integration of the training materials into the platform.

In this phase, partners will continue to engage with stakeholders, expand the stakeholder network and gather feedback

Tasks:

- Update presentation with news which partners will use during events, conferences, meetings when presenting their organisations etc.
- Create engaging content for social media and promote upcoming events and milestones on social media.
- Maintain contact with other projects, initiatives and organisations that promote women's involvement in IT, provide updates on project activities and results, and expand the contact list.
- Regularly update the content (news, activities, interviews, reports, deliverables etc.) of the project website, partner websites and social media.
- Organise workshops for stakeholders.
- Ask the project consortium partners to update you on the project through their own channels.
- Participate in EU events such as Safer Internet Week, European Cyber Security Month, All Digital Week, Girls in ICT, etc. and disseminate information about the developed results.
- Encourage contributions from experts, which can be shared on the website or social media.
- Highlight the integration of training materials into the project platform.
- Emphasize the real-world relevance and accessibility of the materials.
- Promote the training activities emphasizing the unique approach.
- Start disseminating the planned pilot trainings.

Phase 4: Teacher/Mentor Training and Platform Pre-Piloting (M25-M30)

Core Objective: Share information on the completion of training programmes, involve stakeholders and collect feedback. This phase will include training for the mentors/teachers who will participate in the pilot trainings and pilot testing in preparation for the pilot trainings.

Tasks:

- Update presentation with news which partners will use during events, conferences, meetings when presenting their organisations etc.
- Regularly update the content (news, activities, interviews, reports, deliverables etc.) of the project website, partner websites and social media.
- Organise workshops for stakeholders.
- Ask the project consortium partners to update you on the project through their own channels.
- Maintain contact with other projects, initiatives and organisations that promote women's involvement in IT, provide updates on project activities and results, and expand the contact list.
- Prepare a dissemination to involve SMEs and women in the pilot training.

- Participate in EU events such as Safer Internet Week, European Cyber Security Month, All Digital Week, Girls in ICT, etc. and disseminate information about developed results.
- Involve politicians, IT and cybersecurity leaders in dissemination.
- Share updates on teacher and mentor training programs, testimonials and stories of success on the project website and social media.
- Pilot the platform with trained educators.
- Disseminate the pilot program to reach a wider audience.
- Collect feedback and make necessary improvements based on audience input, via surveys and social media interactions.

Phase 5: Methodological Guidelines and Ongoing Pilot (M31-M36)

Core Objective: In the final phase, pilot trainings are launched, a Good Practice Guide for SMEs, Policy recommendations are produced and participation in the pilot trainings is encouraged. This phase is very important as these recommendations will serve as a basis for highlighting the project's position and relevance at the European Union (EU) level in the context of existing policy and strategy frameworks.

The aim of this phase is to inform the wider community about the project's results, impact and best practices.

Tasks:

- Update presentation with news which partners will use during events, conferences, meetings when presenting their organisations etc.
- Regularly update the content (news, activities, interviews, reports, deliverables etc.) of the project website, partner websites, newsletters and social media.
- Organise workshops for stakeholders.
- Ask the project consortium partners to update you on the project through their own channels.
- Execute a dissemination to involve SMEs and women in the pilot training.
- Participate in EU events such as Girls in ICT, etc. and disseminate information about developed results.
- Involve politicians, IT and cybersecurity leaders in dissemination.
- Share updates on pilot testing, demonstrating the project's commitment to quality.
- Disseminate methodological guidelines for educators and stakeholders.
- Share policy recommendations derived from project outcomes.
- Promote the project's achievements and contributions.
- Conclude the dissemination phase and prepare for the project's evaluation and future steps.

3. DISSEMINATION PLANS OF PARTNERS

Our project is expected to improve the knowledge and skills of the target groups in the field of cybersecurity. This is achieved by raising awareness and capacity building among SMEs on skills training and retraining needs. Offering high-level learning programmes and tools that reinforce skills development will make this step achievable. HEIs students will be more receptive to the real needs of SMEs and VETs will be better able to provide training that is relevant to these needs. In addition, our project will provide access to cybersecurity materials adapted to the context and language of each participating country.

Impacts expected at regional/local level

- Experiential learning methodology and real-life tasks in the field of cyber security and cyber resilience for SMEs.
- Supporting the up-skilling and re-skilling of SME employees and bridging the gap between HEIs and VETs.
- Improve/update cybersecurity knowledge and skills of regional HEIs, students and SME communities.
- Increased involvement of local authorities and cooperation with HEIs and VETs to disseminate knowledge on cybersecurity, as well as on new career paths and opportunities for SMEs to support local economies.

Impacts expected at national/partner country level:

- Strengthening cooperation, alliances and synergies between national business support agencies, SMEs, VET providers and HEIs.
- Promote work-based learning by developing national policies that are more favourable to the sustainability of SMEs.
- Increase the employability of vulnerable workers, especially women, by harnessing technology and innovation in their industry.
- Promote sustainability and address the economic, social and environmental challenges facing each country.
- Help SMEs become more resilient in the face of cyber-attacks and embed a cyber culture in the company.

Not only will the participating countries be significantly impacted by our project's outcomes, but also their network of EU partners. As our project deliverables are not only in the languages of the partners, but also in English, the inherent transferability of each deliverable ensures that they are relevant at European level and increases the likelihood that they will be translated into other languages. The project will also provide recommendations and suggestions on cybersecurity paths for policy makers responsible for developing national strategies in the partner countries.

Impacts expected at international/European level:

- Policy makers will be informed about the progress and results of our project both at national and European level, which may be done through the National Digital Coalition (NDC) networks.
- Contribute to the cross-border dissemination of good practices on cybersecurity and cyber resilience of SMEs.
- Contribute to lifelong learning and support European policies in the field of cyber security education.
- Foster cooperation, synergies, and sharing of experience between a wide range of EU-related networks.
- Support the EU economy, which will benefit from the project results, learning resources and knowledge transfer.
- Support the EU in growing sustainable businesses and foster entrepreneurship.

In the partner countries, organisations and associations involved in digital and cybersecurity issues have been introduced to the idea of the project and are ready to support and contribute to its dissemination.

The dissemination strategy of each partner is outlined below and will be updated during the project through the dissemination progress reports (M12, M24, M36).

3.1. DISSEMINATION STRATEGY FOR LITHUANIA

Action	Details	Estimated Delivery Date(s)
Planned Public Events/Seminars	Stakeholders' events. Pilot testing CyberAgent course.	According to agreed schedule
Other Planned Dissemination Activities	Use social media channels. Use contacts with other HEIs, VETs and SMEs in Lithuania. Use of our own Webpages for dissemination. Use of Lithuanian partners webpages and social media pages for dissemination. Presentations about the project given in conferences and seminars organising by third parties.	Continuously

National Entities/Organisations being approached to assist in national dissemination activities i.e., Organisations that have close links to the project target groups that will benefit from using the CyberAgent results in particular the courseware and e-Learning content being developed.

Name of Entity	Web Page URL
Vilnius university Kaunas faculty	www.knf.vu.lt
National Digital Coalition of Lithuania	www.skaitmeninekoalicija.lt
National distance learning association	www.ndma.lt

3.2. DISSEMINATION STRATEGY FOR ROMANIA

Action	Details	Estimated Delivery Date(s)
Planned Public Events/Seminars	Stakeholders' events. Pilot testing Cyber Agent course.	According to agreed schedule
Other Planned Dissemination Activities	Distribution on social media and on our own weboage of images and details regarding the project: short description, results, events, activities, partners. Dissemination of the results of the project face-to-face meetings during different events such as Teacher's Council, County pedagogical meetings, Erasmus days, European Year of Competences, European Skills Week, European project writing workshops, our High School Day. Presentations, explanations, debates and round tables about the project given in conferences and seminars organised by third parties. Designing the Project Corner with information about the Alliances for Innovation Program in our school.	Continuously

National Entities/Organisations being approached to assist in national dissemination activities i.e., Organisations that have close links to the project target groups that will benefit from using the CyberAgent results in particular the courseware and e-Learning content being developed.

Name of Entity	Web Page URL
Technological Highschool «Grigore C. Moisil », Buzau	https://liceulmoisilbuzau.ro/Joomla341/index.php
Europe Direct Centre	https://europedirectbuzau.ro
National Cyber Security Directorate	https://dnsc.ro

3.3. DISSEMINATION STRATEGY FOR BELGIUM

Action	Details	Estimated Delivery Date(s)
Planned Public Events/Seminars	Stakeholders' events. Pilot testing CyberAgent course. Project Final Conference.	When such event is planned and also according to agreed schedule
Other Planned Dissemination Activities	Use W4C social media channels to share content about the project milestones. Use contacts of other HEIs, VETs and SMEs in Belgium. Use of W4C Website for dissemination of articles and press releases.	Continuously

National Entities/Organisations being approached to assist in national dissemination activities i.e., Organisations that have close links to the project target groups that will benefit from using the CyberAgent results in particular the courseware and e-Learning content being developed.

Name of Entity	Web Page URL
Women4Cyber Foundation	https://women4cyber.eu
Women4Cyber Belgium	https://www.linkedin.com/company/women4cyber-belgium?originalSubdomain=be
Global Cyber Alliance	https://www.globalcyberalliance.org

3.4. DISSEMINATION STRATEGY FOR SPAIN

Action	Details	Estimated Delivery Date(s)
Planned Public Events/Seminars	Stakeholders' events. Pilot testing CyberAgent course.	According to agreed schedule
Other Planned Dissemination Activities	Use social media channels. Use contacts with other HEIs, VETs and SMEs in Spain. Use of our own Webpages for dissemination. Use of Spain partners webpages and social media pages for dissemination. Presentations about the project given in conferences and seminars organising by third parties.	Continuously

National Entities/Organisations being approached to assist in national dissemination activities i.e., Organisations that have close links to the project target groups that will benefit from using the CyberAgent results in particular the courseware and e-Learning content being developed.

Name of Entity	Web Page URL
Ecosistemas Virtuales y Modulares SL	https://evm.net
EVM Consulting	www.evm.consulting
Fundación Imagine	https://imagine50.org
INCIBE – Instituto Nacional de ciberseguridad	www.incibe.es
ISMS forum	www.ismsforum.es

3.5. DISSEMINATION STRATEGY FOR NORWAY

Action	Details	Estimated Delivery Date(s)
Planned Public Events/Seminars	Stakeholders' events. Pilot testing CyberAgent course.	According to agreed schedule
Other Planned Dissemination Activities	Use social media channels. Use contacts with other HEIs, VETs and SMEs in Norway. Use of our own Webpages for dissemination. Use of Norway partners webpages and social media pages for dissemination. Presentations about the project given in conferences and seminars organising by third parties.	Continuously

National Entities/Organisations being approached to assist in national dissemination activities i.e., Organisations that have close links to the project target groups that will benefit from using the CyberAgent results in particular the courseware and e-Learning content being developed.

Name of Entity	Web Page URL
Steinkjer Næringsforum (Chember)	Steinkjer Næringsforum (steinkjernf.no)
Verdal videregående skole (VET school)	https://web.trondelagfylke.no/verdal-videregaende-skole/
Adcom (SME)	Adcom - Totalleverandør av IT og telefoni til din bedrift

3.6. DISSEMINATION STRATEGY FOR TURKEY

Action	Details	Estimated Delivery Date(s)
Planned Public Events/Seminars	Stakeholders' events. Pilot testing CyberAgent course.	According to agreed schedule
Other Planned Dissemination Activities	Posts on TIMTAL's website. Posts on TIMTAL's social media channels. Dissemination through our partners' network. Use contacts with other VETs, HEIs, and SMEs in Turkiye.	Continuously

National Entities/Organisations being approached to assist in national dissemination activities i.e., Organisations that have close links to the project target groups that will benefit from using the CyberAgent results in particular the courseware and e-Learning content being developed

Name of Entity	Web Page URL
Teknopark Istanbul VET School (TIMTAL)	https://pendikmtal.meb.k12.tr
Zonguldak Bulent Ecevit University	https://w3.beun.edu.tr
Istanbul Teknopark	www.teknoparkistanbul.com.tr
Siber Vatan	www.sibervatan.org

3.7. DISSEMINATION STRATEGY FOR POLAND

Action	Details	Estimated Delivery Date(s)
Planned Public Events/Seminars	Stakeholders' events. Pilot testing CyberAgent course.	According to agreed schedule
Other Planned Dissemination Activities	Use social media channels. Use contacts with other HEIs, VETs and SMEs in Poland. Use of our own Webpages for dissemination. Use of Polish partners webpages and social media pages for dissemination. Presentations about the project given in conferences and seminars organising by third parties.	Continuously

National Entities/Organisations being approached to assist in national dissemination activities i.e., Organisations that have close links to the project target groups that will benefit from using the CyberAgent results in particular the courseware and e-Learning content being developed

Name of Entity	Web Page URL
HackerU Poland	www.hackeru.pl
ThriveDX Group	www.thrivedx.com

3.8. DISSEMINATION STRATEGY FOR FINLAND

Action	Details	Estimated Delivery Date(s)
Planned Public Events/Seminars	Olemisen regular project conferences. Stakeholders events. WP5 Pilot testing phase.	When such event are planned and also according to agreed schedule
Other Planned Dissemination Activities	Posts on Olemisen's website. Posts on social media channels. Dissemination through our partners' network.	Continuously

National Entities/Organisations being approached to assist in national dissemination activities i.e., Organisations that have close links to the project target groups that will benefit from using the CyberAgent results in particular the courseware and e-Learning content being developed

Name of Entity	Web Page URL
Raseko	www.raseko.fi
Turku University of Applied Science	www.tuas.fi
The Association of Finnish eLearning Centre	https://eoppimiskeskus.fi

4. COMMUNICATION CHANNELS

In order to maintain a unified communication, partners will refer to this document and the templates that will be created and hosted in the project's MS Teams environment. Women4Cyber is responsible for creating and sharing these templates with the partners.

Graphic charter:

- Project and EU logo in most common formats;
- Unified presentations template;
- Unified MS Word template;
- Video conference backgrounds.

Presentation material:

- For each phase, presentations will be created with basic content that partners can adapt, localise and use for dissemination to different audiences (both internal and external communication).

Printed material

- Leaflets, posters, infographics;
- Roll-up banner.

Online material

Press releases, social media campaigns and newsletters will be released throughout the project. Templates for these publications will be created at the beginning of the project. At key stages, content will also be created, which the partners will be able to adapt, localise and publish on their own channels.

- Press release template;
- Social media campaigns template;
- Unified Newsletter template.

4.1. PROJECT WEBSITE AND COLLABORATIVE PLATFORM FOR SKILLS DEVELOPMENT

The SME Cyber Security Change Agent Collaboration Digital Platform is an integral part of the project's online presence. This platform is a dynamic hub that brings together various stakeholders, including higher education institutions, vocational training providers, labour market entities, technological institutions, and representatives from the cybersecurity industry. Within the CyberAgent project, this platform's primary purpose is to establish an interconnected collaboration space that enhances knowledge transfer among consortium partners, other training providers, and the broader public while maximising the added value for the EU.

This platform will align with the goals of supporting the "European Digital Innovation Hub" (EDIH), with a specific focus on fostering the widespread adoption of digital technologies, particularly among SMEs and midcaps, as well as public sector organisations across Europe.

The platform will serve as a comprehensive one-stop-shop for SME Cyber Security Change Agents and SME management. It will function as an interactive hub, offering a wide range of resources, including knowledge sharing, networking opportunities, workshops, webinars, matchmaking services, and the exchange of best practices. Additionally, selected stakeholders from each partner country will utilise the platform to provide targeted mentoring sessions and other soft skills workshops. The project website will be seamlessly integrated into this platform, enhancing its functionality and reach. To be developed by Prios.

Project's website, embedded into the project's digital platform, will be developed in line with the latest design, mobile and user-friendly techniques and it will become the face of the project. The primary aim of the website is to function as a central hub for disseminating project activities and outcomes. Specifically, it serves as an early-stage tool for sharing project-related information with both the consortium members and the public. This includes the distribution of project deliverables, the digital platform, and upcoming events relevant to Cyber Agent.

The sitemap of the website **www.cyberagents.eu** is:

- Home
- About
  - Objectives
  - Main goals
  - Expected results
- Partners
- News
- Events
- Resources & Results
- Contact
  - Newsletter (subscribe)

4.2. SOCIAL MEDIA

Social media profiles on key platforms, including Facebook, LinkedIn, YouTube, Twitter and Instagram, will be established during the project's initial phases. These channels aim to enhance the project's visibility and recognition among a broader audience, with a primary focus on Higher Education Institution (HEI) teachers, SME employees, Vocational Education and Training (VET) providers, and both public and private agencies dedicated to business support. Each partner will have the duty of sharing project updates and cybersecurity news on a weekly basis through social media platforms, adhering to the specified timetable. Furthermore, consortium partners will leverage their respective channels to ensure that dissemination efforts are effectively carried out in the national languages represented by the consortium members.

The content strategy for social media encompasses a variety of themes, including countdowns to major events, project news, achievements, progress updates, excerpts from educational materials and research results, motivational quotes, informative cybersecurity content, photos and videos from partner meetings and activities, and behind-the-scenes glimpses of project work. Additionally, researching and using relevant hashtags and keywords (like #CyberAgent #CyberSecurity #Erasmus+) will be essential for increasing the reach of our social media campaigns.

Project communication channels:

Facebook page: https://www.facebook.com/cyberagent.eu/about

User name : @cyberagent.eu
To share project news and events

Instagram page: https://www.instagram.com/cyber.agent.eu/

User name : @cyber.agent.eu
To share visual and graphic content like event photos, infographics and project highlights.

LinkedIn page: https://www.linkedin.com/company/cyber-agent-eu

User name : @cyber-agent-eu
To share professional content and message, and encourage networking.

YouTube page: https://www.youtube.com/channel/UCtROjchC8N7u7IdsmCpwapg

User name : @CyberAgentEU
To share video content, including project presentations and recordings.

Twitter page: https://twitter.com/CyberAgentEU

User name : @CyberAgentEU
To share brief news and real-time events updates.

4.3. NEWSLETTERS

W4C, the communication and dissemination WP lead will create newsletters, **on a quarterly basis** and aimed to disseminate the intermediate results on a large scale. The e-newsletter will be distributed via email to all registered users, encompassing involved stakeholders and an expanded audience of those interested. Additionally, they will be shared across the networks of project partners to maximise their reach. The newsletters will also be featured on both the project's official website and the websites of consortium partners. To ensure accessibility to a local audience, consortium partners will take the initiative to translate the newsletters into their respective national languages.

Newsletter schedule

- **Newsletter 1 – M5**
- General promotion of CyberAgent and its partners
- **Newsletter 2 – M8**
- Reference to the deliverables promoted in the previous newsletter
- **Newsletter 3 – M12**
- Reference to the deliverables promoted in the previous newsletter
- **Newsletter 4 – M16**
- Reference to the deliverables promoted in the previous newsletter
- **Newsletter 5 – M20**
- Promotion of MS4.1 SME Cyber security change agent platform
- Reference to the deliverables promoted in the previous newsletter
- **Newsletter 6 – M24**
- Promotion of D3.1 Training modules for HEI students
- Promotion of D3.2 Training modules for VET students
- Reference to the deliverables promoted in the previous newsletter
- **Newsletter 7 – M28**
- Reference to the deliverables promoted in the previous newsletter
- **Newsletter 8 – M32**
- Reference to the deliverables promoted in the previous newsletter
- Promotion of D4.2 Pilot platform
- Promotion of D6.5 Final conference
- **Newsletter 9 – M36**
- Promotion of all project deliverables
- Dissemination of D5.3 CyberAgent upskilling Training Program Evaluation
- Dissemination of D5.4 Teaching methodology for SMEs Cyber Security Change Agents
- Dissemination of D6.3 Policy recommendations
- Dissemination of D6.4 Good Practice guide for SMEs
- Promotion of sustainability efforts of the project

4.4. PRESS RELEASE

Identified results of special interest will trigger press releases to be published on the CyberAgent website and relevant cybersecurity platforms. Furthermore, they will be distributed to all partners' press departments to stimulate decentralised communication and broad utilisation of media outlets/journalists. A press release will therefore be issued for any major announcements and significant milestones related to the project, including the promotion of events such as workshops and training programmes in order to give them more visibility.

4.5. FINAL CONFERENCE

The final conference of the project will be a large-scale dissemination event in month 36 in Belgium. It has the primary objective of showcasing our project's activities and outcomes to a broader audience. Additionally, during this event, we will launch a student competition for the EU award, aiming to engage and inspire future talents. The conference anticipates the participation of 50 attendees and is set to be a significant dissemination event. Its main focus will revolve around sharing the insights, knowledge, and experiences gained throughout the CyberAgent project. This includes the presentation and promotion of the reports and training materials developed as part of our initiative.

4.6. PARTNERS NETWORK AND WEBSITE

Each partner is responsible for disseminating information about the project through its own contacts and networks. The project will also provide the consortium with the opportunity to make new contacts through meetings, workshops and conferences.

Information about the project, its activities and results will be published on the websites of all CyberAgent partners.

5. GRAPHIC GUIDELINES

5.1. VISUAL IDENTITY

The actions of the initial awareness phase start with the design of a CyberAgent logo and visual identity to ensure clear, consistent and recognisable brand for all communications and to underline the project's philosophy and objectives.

The purpose of a project's visual identity is to create an emotional impression that gives stakeholders a clear sense of the project and its nature. The project's visual identity comprises all the imagery and graphical content employed to identify and distinguish CyberAgent and its outputs within the principal domains in which the project operates and targets, namely cybersecurity and education.

The project visual identity includes the logo and its guidelines in terms of colours and graphical layout, which will be employed to unify all communication material of the project, including the template of the documents and the template of the slides (templates are available in MS Teams WP6-Dissemination & Exploitation > Template). The project logo to project partners is available in various formats (for publishing and electronic documents) in the project's MS Teams environment.

In CyberAgent, the following are the visual elements developed to provide the visual identity of the project:

Logo

Versions of the Logo

Font set

Headlines	Sub headlines	Body
Montserrat / SemiBold 600 / 64px	Open Sans / Regular 400 / 54px	Open Sans / Regular / 14px

Colour palette

Color 1	Color 2	Color 3	Color 4	Color 5
#273B6B	#9C2736	#8693AB	#BDD4E7	#AAB9CF
39,59,107	156,39,54	134,147,171	189,212,231	170,185,207

5.2. MANDATORY ATTRIBUTES

When disseminating, partners must include the project name/acronym, project number, project logo, EU emblem and disclaimer. This must be used in all communication materials and documents related to the Erasmus+ funded project, such as:

- Project documents, reports;
- Project website, partners websites, social media when disseminating about CyberAgent project;
- Press releases;
- Promotional items and materials (e.g., presentations, leaflets, posters, newsletters, websites);
- Any communication made by the partnership as a whole, or as an individual project partner;
- During events and on presentation slides.

All recipients of EU funding have a **general obligation** to acknowledge the origin and ensure the visibility of any EU funding received. All publications (for all project products and dissemination material) will follow the official requisites of the European Commission and contain:

- Project CyberAgent logo;
- European flag emblem.

Please use the following guide for more information: http://publications.europa.eu/code/en/en-5000100.htm

"Co-funded by the European Union" should always be spelled out in full and placed next to the emblem. **The emblem must remain distinct and separate and cannot be modified by adding other visual marks, brands or text**.

Logo download from website: https://www.eacea.ec.europa.eu/about-eacea/visual-identity/visual-identity-programming-period-2021-2027/european-flag-emblem-and-multilingual-disclaimer_en

The EU emblem is the single-most important visual brand used to acknowledge the origin and ensure the visibility of EU funding. Apart from the EU emblem, no other visual identity or logo may be used to highlight EU support. The EU emblem should not be modified or merged with any other graphic elements or texts.

When displayed in association with other logos (e.g. of beneficiaries or sponsors), the emblem must be displayed at least as prominently and visibly as the other logos. If other logos are displayed in addition to the Union emblem, the Union emblem should have at least the same size as the biggest of the other logos.

More information: https://commission.europa.eu/funding-tenders/managing-your-project/communicating-and-raising-eu-visibility_en

https://op.europa.eu/en/publication-detail/-/publication/d1d3df9b-03e9-11ed-acce-01aa75ed71a1/language-en

https://commission.europa.eu/system/files/2022-07/communicating_and_raising_eu_visibility_-_guidance_for_external_actions_-_july_2022.pdf

https://commission.europa.eu/system/files/2021-05/eu-emblem-rules_en.pdf

In addition, a disclaimer must be added to each publication:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The text can be found in all EU official languages here: https://www.eacea.ec.europa.eu/about-eacea/visual-identity/visual-identity-programming-period-2021-2027/european-flag-emblem-and-multilingual-disclaimer_en

5.3. COPYRIGHTS

Partners must respect copyright in their communication materials and not infringe copyright laws at organisational, local, national and EU level. Partners are recommended to use free graphic resources such as: https://pixabay.com, www.pexels.com, https://unsplash.com, www.iconfinder.com etc. in the development and dissemination of project products. If partners use graphics from these or similar websites, they must comply with the licences for the graphics used and, if the licence states so, must attribute authorship when using graphic elements as required by the specific licence.

5.4. PERSONAL DATA COLLECTION AND PROCESSING

The protection of privacy is very important to the CyberAgent Consortium, and all members of the Consortium must seek the consent of the people they wish to photograph at all times at all events during the project (for use at workshops, events, scientific conferences and other occasions). Partners must follow the General Data Protection Regulation (GDPR).

Each partner must use its own internal policies when collecting and processing personal data, and must not use personal accounts for storing and processing data collected during the project. Each partner takes responsibility for the processing and protection of personal data in accordance with the internal procedures in force within that partner's organisation.

Whenever collecting data (e.g. in surveys, workshops, where photographs are taken or signatures need to be collected, as proof of participation if required by the project, etc.), the partners must inform the participants about the fact that the data is being collected, the purpose of the data collection, the duration of the data collection, the time for which it will be stored, and the manner in which the data will be processed (in accordance with the partner's internal procedures), etc.

Partners must behave responsibly and not arbitrarily send information by e-tools (emails, social networking messages, etc.) without first obtaining the consent of the recipients, i.e. information about the project and its activities must be sent to those contacts whose consent is obtained.

6. DISSEMINATION TRACKING

Communication strategies will be discussed at the regular monthly online meetings of the consortium. The project partners are using Microsoft Teams and e-mails for internal communication and dissemination tracking.

Placed on the project MS Teams Share folder (WP6), consortium partners are required to provide data regularly on their dissemination activities in the dissemination tracker of the project.

6.1. MONITORING DISSEMINATION AND COLLECTING EVIDENCE

The task leader and partners have developed a communication strategy and will report on the progress and general dissemination activities at regular intervals (M12, M24, and M36).

Project partners have to report on dissemination events, activities (e.g., seminar, article, social media, publication, presentation, TV, etc.) **every 6 months to Women4Cyber:** Women4Cyber will develop a dissemination aggregation template and every 6 months partners shall submit a table in the WP6 folder of the MS Teams platform every 6 months and present it at the partner meetings. Each partner must keep a record of dissemination and provide evidence for inclusion in the interim and final reports

The project plans wide range of dissemination activities, which will be periodically summarized by Women4Cyber and discussed within the partnership meetings. These discussions will help the partnership to evaluate periodically the impact of the dissemination, to define the ways for improvements and to identify the activities which have the biggest impact on different target groups. It means that the dissemination plan will be periodically reviewed, extended, and improved to ensure the active involvement of all the partners.

The results of project dissemination will be summarized and included in the midterm and final reports.

In order to monitor and evaluate the success of dissemination, partners need to collect information about all dissemination events:

- Title of event,
- Fix when the event took place,
- Short description,
- When a publication was published or a presentation given,
- Who the target audience is,
- Provide evidence (a link and preferably a screenshot, as links stop working after a certain period of time; photos of the event, clearly showing the speaker, the audience and slides with the project's required attributes).

Indicators (qualitative or quantitative, e.g. number of people at the seminar, number of visitors to the website or reactions to a social post, shares).

Evidence of dissemination is gathered through:

- e-material;
- copies of printed reports, press releases, articles and materials;
- screenshots of websites and screenshots of social networking groups;
- photographs, photos and videos of events;
- copies of conference abstracts or journal articles;
- lists of participants, minutes of events, etc.

6.2. KEY PERFORMANCE INDICATORS

Statistical information on the dissemination of the project will be collected to assess the impact of dissemination. The dissemination of the project will be recorded in a uniform format provided by Women4Cyber. The dissemination will be recorded in terms of the target group reached by the project dissemination.

Result	Indicator
Project website	News, project results are regularly published on the partners' websites
	Visitors number, demographics statistics, new visitors, returning visitors, number of pages visited
Collaborative platform for skills development	Number of engagements, satisfaction
	Visitors number
Partners website	Project results are regularly published on the partners' websites
	Number of publications, if available, measure the number of users reached
Linkedin	Number of posts on project account, partners accounts
	Number of expressions, likes, shares of each post
Facebook	Number of posts on project account, partners accounts
	Number of expressions, likes, shares of each post
Instagram	Number of posts on project account, partners accounts
	Number of expressions, likes, shares of each post
Twitter	Number of posts on project account, partners accounts

	Number of expressions, likes, shares of each post
YouTube	Number of posts on project account, partners accounts
	Number of expressions, likes, shares of each post
Newsletters	Number of newsletters
	Number of emails sent / number of people reached
	Pages and number of pages, where the newsletter is published, number of visitors
	New subscribers, unsubscribing rate
Press releases	Number of press releases
	Number of publications, shares
	Number of visitors, when it is possible
Events, seminars, workshops, roundtables etc	Number of events
	Number of participants
Final Conference	Number of participants
	The satisfaction level of attendees.
	Post-conference surveys or feedback on the event
Posters	Number of posters produced
Infographics	Number of infographics
	Number of people reached, number of engagements (shares, likes, clicks, etc.)
Promotional videos	Number of videos
	Number of people reached, number of engagements (shares, likes, clicks, etc.)

Project results, deliverables	Number of publications
	Number of people reached, number of engagements (shares, likes, clicks, etc.)
Direct own contacts and contacts of associated partners	Number of contacts
People working or studying in the partner organisation	Number of people who learned about the project, number of people participating in the pilot training or other activities

Statistics will also be compiled on target groups as soon as they can be identified, like number of persons who found out about the project, who took part in the survey, who took part in the pilot trainings, satisfaction with attending the events; if these statistics can be calculated for any other dissemination.

- SME employees
- Women in cybersecurity
- HEI teachers
- HEI entrepreneurship students
- VET providers
- VET trainees
- Students
- Unemployed people
- EU Policy makers
- National decision makers
- European Commission
- Labour market actors and other cybersecurity practitioners
- Broad public
- Media and secondary disseminators
- Research and Academic Communities
- Business associations
- IT Professionals and Women Associations

7. EXPLOITATION OF PROJECT RESULTS

There are many different ways to disseminate and exploit results:

- The Erasmus+ Project Results Platform;
- Project or organisational websites;
- Meetings and visits to key stakeholders;
- Dedicated discussion opportunities such as information sessions, workshops, (online) seminars, training courses, exhibitions, demonstrations, or peer reviews;
- Targeted written material such as reports, articles in specialised press, newsletters, press releases, leaflets;
- Audiovisual media and products such as radio, TV, YouTube, Flickr, video clips, podcasts or apps;
- Social media;
- Public events;
- Project branding and logos;
- Existing contacts and networks.

8. CONCLUSION

As described in this report, this CyberAgent dissemination strategy is based on a number of preparatory activities in the first year that led to the phasing-in of a number of project events as from M1 till the end of the project. The strategy has been agreed and understood by all the partners, meaning that its implementation should be an effectively positive one. In addition, this report has generated a roadmap, on how certain project results can be exploited in the long term.

Also, it is expected that the positive impact the CyberAgent project will foster an interest in trying to seek to go forward with potentially a new proposal, such as an Erasmus+, Horizon.

ANNEXES

Annex 1. Partners website and social medias

Partners	Website	Social Medias
Vilniaus Universitetas	www.knf.vu.lt/en www.knf.vu.lt/en/smes-cyber-security-change-agents	Facebook Instagram LinkedIn YouTube
Liceul Tehnologic "Grigore C. Moisil" Buzau	https://liceulmoisilbuzau.ro/	Facebook
Women4Cyber Mari Kert - Saint Aubyn Foundation	https://women4cyber.eu/	X Instagram LinkedIn
Ecosistemas Virtuales Y Modulares SL	https://evm.net/	LinkedIn
Prios Kompetanse AS	https://www.prios.no/	Facebook LinkedIn YouTube
Teknopark Istanbul Mesleki Ve Teknik Anadolu Lisesi	https://teknoparkistanbul.meb.k12.tr/	Instagram
Hackeru Polska Spolka z Ograniczona Odpowiedzialnoscia	https://hackeru.pl/	Facebook Instagram LinkedIn YouTube
Olemisen Balanssia Ry	https://olemisen.fi/	Facebook Instagram

Annex 2. Dissemination strategy and goals overview

This tab outlines the target audience, goals, types of information, and communication tools for engaging project partners with stakeholders in the CyberAgent Project.

Target audience	Goals	Type of information	Communication means & tools
Project partners, Associated partners, affiliated entities **Members, other stakeholders in consortium countries**	• Raise awareness. • Strengthening cooperation, attracting new network members and sharing a common understanding. • Creating a sustainable skills development model for IT professionals and those wishing to change their job profile. • Establish links with other networks; increase cooperation and synergies.	• Exchange of good practices • Case studies • Insights from experts and stakeholders • Concluding remarks and recommendations • Experience reports • Training and skills development • Collaborative platform for skills development	• Project website, partners websites • Social media channels • Publications on the websites of associated partners • Publications and press releases • Workshops to boost trainers numbers • Events in 8 countries • Meetings and seminars in the countries of the consortium • Final conference in Belgium • Collaborative platform for skills development • Newsletters
Research and Academic communities, Business associations, VET communities, IT professionals and Women associations	• Raise awareness. • Better understanding and collaboration. • Increase interest from SMEs. • Better understanding of innovation, knowledge and research projects and initiatives. • Establish links with other networks. • Increase cooperation and synergies.	• Case studies and success stories • Experience reports • Exchange of good practice • Insights from experts and stakeholders • Opportunities to identify cybersecurity gaps and needs • Opportunities to use training and skills development	• Project website, partners websites • Social media channels • Publications on associated partners websites • Direct own contacts and contacts of associated partners • Publications and press releases • Conferences / events • Newsletters • Surveys
Policy makers, regulators and public bodies like European Commission. National decision makers, ministry representatives, national and regional funding agencies and international institutions	• Raise awareness. • Influence policy priorities. • Improve documents and strategies to enhance SMEs' cybersecurity resilience. • Draw attention to training and retraining opportunities in the field of cyber security. • Include more women in cybersecurity-related jobs. • Reduce unemployment and aim to reduce NEETs. • Widen access to public funding.	• Share lessons learned • Assessing the potential for up-skilling and re-skilling • Socio-economic analysis • Recommendations for policies and strategies related to cyber security resilience building, in particular for SMEs	• Project website, partners websites • Social media channels • Publications on associated partners websites • Direct own contacts and contacts of associated partners • Conferences/Events • Meetings and seminars in the countries of the consortium • Final conference in Belgium • Collaborative platform for skills development • Promotional video • Recommendations and reports on cybersecurity aspects • Papers and reports

Target audience	Goals	Type of information	Communication means & tools
Civil society at regional, national and European level like Students, HEI and VET teachers, Unemployed people, NEETs, women, citizen, consumer, NGOs organisations and specialised media	• Increase awareness of up-skilling and re-skilling opportunities, their impact on employment for SME employers, and the significance of boosting SMEs' cyber resilience. • Promote career opportunities for NEETs through SME cyber security qualification training. • Raise awareness of the role of public funding.	• Involvement of SMEs and higher education/vocational education and training institutions in addressing training needs and opportunities. • Specific examples of cybersecurity skills training. • SMEs' needs, cybersecurity trends, roadmaps and action plans to increase their resilience to cyber-attacks. • Requalification and job creation • Consultations to identify skills gaps and needs	• Collaborative platform for skills development • Project website, partners websites • Social media channels • Publications on associated partners websites • Dissemination material • Promotional videos • Publications and press releases • Events and seminars • Surveys

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau