Co-funded by the European Union

CYBERAGENT UPSKILLING TRAINING PROGRAM EVALUATION

CYBER AGENT 05.2026

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 5: Boost CyberAgent Upskilling at local and regional level

Deliverable 5.3: CyberAgent upskilling Training Program Evaluation

Leader of WP5 – EVM Grupo
Leader of deliverable 5.3 – ProxyLab ry

CONTENT

INTRODUCTION

The CyberAgent project aims to strengthen cybersecurity awareness, skills and readiness among SME employees, higher education and vocational education and training learners. As cybersecurity risks increasingly affect small and medium-sized enterprises, there is need for accessible, flexible and practical upskilling opportunities that can support both workplace-based learning and education-based training pathways.

This deliverable, D5.3 CyberAgent Upskilling Training Program Evaluation, presents the evaluation of the CyberAgent pilot implementation carried out under Work Package 5: Boost CyberAgent Upskilling at local and regional level. The report consolidates evidence from the national pilots implemented in Romania, Belgium, Norway, Spain, Türkiye, Poland, Lithuania and Finland. It examines how the training programme was prepared, promoted, delivered and evaluated across different national and organisational contexts.

The evaluation focuses on three main dimensions. First, it reviews the national piloting processes, including recruitment, participant engagement, stakeholder involvement, collaboration between educational institutions and SMEs, delivery formats, implementation challenges and lessons learned. Second, it analyses platform and training participation data to understand the reach and progression of learners across the CyberAgent modules. Third, it presents the results of the participant feedback survey, which provides evidence on the perceived quality, relevance, usefulness, platform experience, learning outcomes, impact and improvement needs of the programme.

The CyberAgent pilot was implemented through a flexible delivery model combining self-paced online learning with local onboarding, trainer support, face-to-face sessions, online meetings and follow-up activities where relevant. This approach allowed partners to adapt the training to the needs and realities of different target groups. SME employees often required flexibility due to work responsibilities, while VET and HEI learners benefited from structured guidance and integration into education settings.

1. TABLE OF FIGURES

2. TABLE OF ILLUSTRATION

3. METHODOLOGY

The methodology used for this deliverable combines qualitative and quantitative evidence collected during and after the CyberAgent piloting phase. The purpose was to evaluate both the implementation process and the learning experience of participants across the partner countries.

The evaluation was based on three main sources of evidence:

- National piloting reports submitted by the project partners after the implementation of the pilot activities.
- Platform analytics and participation data showing registrations, course starts, module completion and test results.
- Participant feedback survey data collected after the piloting activities.

The national piloting reports were reviewed and consolidated to identify common patterns, country-specific experiences, implementation challenges and lessons learned. The analysis covered recruitment and participant selection, stakeholder involvement, collaboration between SMEs and educational institutions, delivery formats, onboarding activities, support mechanisms, engagement levels and perceived skills development.

The platform analytics were used to assess the reach and engagement of the training programme. These data included the number of registered users, learners who started at least one course or module, and learners who passed at least one module test or completed the minimum pilot requirement. Module-level data were also reviewed to understand participation patterns across the nine CyberAgent modules. These figures were used to assess how participants moved from registration to active learning and completion.

The participant feedback survey provided the main quantitative evidence on learner experience and perceived impact. The dataset contained 272 survey responses. The survey included questions on respondent profile, delivery mode, trainer support, module quality, module relevance, module usefulness, digital platform experience, learning outcomes, satisfaction, barriers, impact and open-text improvement suggestions.

The methodology combines statistical analysis, qualitative synthesis and cross-country comparison to provide a balanced understanding of the CyberAgent pilot by showing not only what participants rated positively or negatively, but also why certain challenges occurred and how the programme can be improved for future use.

4. NATIONAL PILOTINGS

4.1. CONSOLIDATED REVIEW

4.1.1. GENERAL INFORMATION

This consolidated report brings together the national piloting reports submitted after the CyberAgent pilot implementation phase in Romania, Belgium, Norway, Spain, Türkiye, Poland, Lithuania and Finland. The report summarises the evidences into one structured overview covering preparation, stakeholder involvement, implementation, follow-up and support, participant engagement and skills and knowledge development.

Table 1 - Countries and participating organisations

Country	Partner organisation
Romania	GCM
Belgium	Women4Cyber Foundation
Norway	Prios Kompetanse AS
Spain	EVM Group
Türkiye	Teknopark Istanbul MTAL
Poland	IT AKADEMIJA
Lithuania	Vilnius University
Finland	ProxyLab

4.1.2. PREPARATION PHASE

Recruitment and participant selection

Across participating countries, recruitment targeted the three main CyberAgent profiles: SME employees and trainers, higher education students and lecturers, and VET students and teachers. The approaches differed by country depending on existing networks, national partner profiles, and access to education and business stakeholders.

In Romania, GCM used its existing stakeholder network and dissemination activities through institutional channels, partner networks and direct communication. SME employees were recruited through business networks and partner organisations, supported by earlier contact with the National Cyber Security Directorate and Europe Direct Center. HEI students were reached through university professors in Bucharest and Brașov who were members of the Romanian Knowledge Committee. VET students were recruited through in-person presentations by trainers at the GCM school, where the benefits of completing CyberAgent modules were explained.

In Belgium, Women4Cyber Foundation recruited participants through CyberAgent and Women4Cyber social media channels. A first recruitment round used a joint application form developed by EVM and generated almost 24 applications from Belgium. A second recruitment round used a separate LinkedIn form and generated more than 800 expressions of interest. After geographic and eligibility screening, 66 participants were selected.

In Norway, Prios Kompetanse AS recruited participants in three ways: advertising the courses, contacting schools to pilot formal courses, and using its own network. The school-level approach was rejected for HEI students and only partly accepted by VET schools through individual teachers. In total, interest was registered from 12 VET students, 17 HEI students and 18 SME employees.

In Spain, EVM Group promoted the training opportunity from November 2025 to the end of January 2026 through social media, professional networks, and direct email campaigns targeting SMEs in the Canary Islands, VET providers and HEIs across Spain. The campaign generated interest from 92 people by 21 January 2026. Of these, 20 were SME employees, 36 were HEI students, 2 were VET teachers and 34 were VET students.

In Türkiye, Teknopark Istanbul MTAL carried out a comprehensive announcement process for VET, HEI and SME target groups. Face-to-face initial training was organised for TIMTAL, while other stakeholders were involved through online information sessions. Active promotion generated interest from 135 people by 21 April 2026: 13 SME employees, 17 HEI students, 16 VET teachers, 88 VET students and 1 HEI trainer.

In Finland, ProxyLab organised the pilot through its existing networks in training and digital skills activities and education and cybersecurity-related project work. SME participants were recruited through direct communication with small companies, local business contacts and professional networks in Southwest Finland. HEI participants were reached through contacts in higher education and applied sciences networks particularly from Turku University of Applied Science and Metropolia University. VET participants were recruited through vocational education contacts and trainers. The Finnish pilot communication outreach used social media combined with a targeted recruitment approach. This was considered more suitable for reaching motivated learners and ensuring that participants understood the expectations of the pilot before joining.

In Poland, IT Akademija promoted the pilot from November 2025 until the end of February 2026 through Facebook and LinkedIn, paid Facebook advertising campaigns, stakeholder networks and direct communication. Three paid Facebook campaigns were conducted between January and April 2026. The campaigns reached 79,836, 127,214 and 228,493 Meta platform users respectively. Poland also presented the pilot during events and through business and professional networks, including IBWN, the International Policy Learning Event in Mazowsze, the Vilnius Chamber of Commerce, Industry and Crafts, the Business Women's Club, BPW networks, and the Polish and Lithuanian Chamber of Commerce. The activities attracted 79 participants.

In Lithuania, Vilnius University informed companies registered in the knowledge network and other listed stakeholders. Information was published on the VU Kaunas Faculty Facebook account and website, and students were informed through Moodle announcements and face-to-face lectures. Direct contact was the main recruitment method, especially for HEI students and SMEs. VET and higher education institutions were contacted by phone and through direct invitations. A total of 136 individuals participated in the Lithuanian pilot training.

4.1.3. MAIN PREPARATION CHALLENGES AND RESPONSES

Several common challenges were reported across countries. The first challenge was recruitment and engagement of SME employees, who often had limited availability due to work responsibilities. Romania addressed this through direct communication by email, phone and WhatsApp, supported by Knowledge Committee members who shared information in WhatsApp groups. Lithuania also found that SME representatives needed the most consultation, especially during platform registration and module selection. In Finland, the main preparation challenge was the limited time availability of SME employees. Many potential SME participants expressed interest but had difficulty committing to structured training during working hours. This was addressed by presenting the training as a flexible, self-paced opportunity that could be completed outside fixed schedules. Poland reported that paid advertising campaigns were particularly effective in attracting SME representatives.

The second challenge was securing formal institutional involvement from education providers. Norway and Finland reported that schools could not commit at institutional level because the academic year and studies had already been planned, leaving no time or space for extra teaching. The solution was to contact individual VET teachers and recruit HEI students who were studying or had recently completed studies. Poland addressed institutional participation by signing collaboration agreements with Zespół Szkół Ogólnokształcących w Sejnach and the University of Szczecin. Spain also reported official collaboration agreements with the Universidad de Santiago de Compostela and IES Villaverde.

The third challenge was participant follow-through after initial interest. Spain reported strong initial interest but low follow-through, requiring an intensive communication plan using individual and group emails. Türkiye also reported that follow-through decreased in later stages and responded with intensive communication, reminders, technical support and extra guidance for modules with lower exam completion rates. Belgium observed that some participants became unresponsive or dropped out due to competing professional or academic commitments.

The fourth challenge was digital onboarding and platform access. Romania reported minor difficulties in communication and onboarding and addressed them through step-by-step instructions and ongoing support. Poland and Lithuania both reported technical issues during registration, particularly confirmation emails not being received. Participants were advised to check Spam or Junk folders or register again with another email address.

The fifth challenge specific to the Polish context, was legal and administrative preparation for underage VET learners. Poland reported that some VET students were underage, requiring parental consent forms before access to the platform. This was handled through cooperation between the VET institution administration, teachers, parents and guardians.

4.1.4. STAKEHOLDER INVOLVEMENT

Table 2 - List of stakeholders involved in the piloting

Country	SME stakeholders	HEI stakeholders	VET stakeholders	Other or cross-target stakeholders
Romania	SC EVAL SAFETY SRL, LIAROM POWER INVEST SRL, TECNO EUROMAG SRL, DMC PRESTCOM LIMITED SRL, MONDO CONSULT SRL, TELESKOP, PURE AUDIT & CONSULTING, OLIMP NET	National University of Science and Technology POLITEHNICA Bucharest, Transilvania University of Brașov	Technological Highschool Grigore C. Moisil, Technological Highschool Henri Coanda	National Cyber Security Directorate and Europe Direct Center supported earlier networking, according to the preparation description
Belgium				Women4Cyber Belgium chapter supported promotion
Spain	Sociedad de Desarrollo de Santa Cruz de Tenerife S.A.U., WISE Canarias, Incolab Cluster, CEOE	Universitat de Girona, Universidad Rovira i Virgili, Universidad de Santiago de Compostela	IES Virgen de Gracia, I.E.S Arcipreste de Hita, IES Villaverde	
Türkiye	INNOMATE Ltd, Avcı Computer, Solcar Motor Vehicles, ALPDLP Software, Ozztech Technology, Technopark Cube Incubation	Istanbul University, Marmara University, Maltepe University, Istanbul Commerce University	Teknopark Istanbul MTAL, Zonguldak MTAL, Antalya Kepez Şehit Özcan Şenol MTAL	
Poland	Polish and Lithuanian Chamber of Commerce, IBWN International Women Business Network, Vilnius Chamber of Commerce, Industry and Crafts, Business Women's Club, BPW Vilnius Chamber Lithuania, INFOBALT Association	University of Szczecin	Zespół Szkół Ogólnokształcących, Technikum w Sejnach	International Policy Learning Event – Mazowsze, WOMEX, BPW network, direct partner networks
Lithuania	Vilnius Chamber of Commerce, Industry and Crafts, International Business Women Network	Vilnius University	Kauno Kolegija, SMK	Lithuanian Computer Society, National Digital Coalition, National Association of Distance Education
Finland	Polygonal North Oy, Ineo Oy, Avila Oy	Turku University of Applied Sciences - Turku UAS, Metropolia university, Aalto University, University of Turku	RASEKO, ProxyLab training center	Viro keskus

Norway	Steinkjer and Nmadal chamber of Comers		Levanger videregående skole, KBT Fagskole	EDIH Ocenaoplolis

4.1.5. COLLABORATION BETWEEN EDUCATIONAL INSTITUTIONS AND SMES

The collaboration between HEIs, VET providers and SMEs was organised through close coordination and continuous communication facilitated by project partners. Educational institutions recruited students and supported academic engagement, while SMEs involved employees and highlighted the relevance of cybersecurity skills in the workplace. Communication was maintained through meetings, emails and online platforms. Feedback from HEIs and SMEs was collected and shared to support evaluation of the platform and training content.

Romania reported that educational institutions contributed to the pedagogical approach, learning objectives and module structure, while SMEs provided input on real-world cybersecurity needs. During implementation, educational institutions recruited learners and supported platform engagement, while SMEs encouraged employee participation and practical application. In support activities, educational institutions offered academic guidance and mentoring, while SMEs enabled employees to participate and encouraged workplace application.

Other countries reported collaboration through stakeholder dissemination and implementation roles rather than a separate collaboration section. Spain described stakeholders distributing the call, signing collaboration agreements, and integrating platform content in VET classrooms. Türkiye described SME, HEI and VET stakeholders participating in the pilot process and applying training content. Poland described formal collaboration agreements with a VET institution and a university, as well as dissemination through SME and business networks. Lithuania described cooperation with business associations, universities, applied sciences institutions and national networks. In Finland, ProxyLab acted as the link between education-oriented participants and SME representatives. Educational contacts helped reach learners and frame the training as a competence development opportunity, while SMEs provided the workplace perspective by highlighting the need for practical cybersecurity awareness in daily operations. The Finnish collaboration focused on validating whether the CyberAgent modules could serve both educational and workplace learning needs. S

The main benefits of education-SME collaboration reported in the national reports were alignment between academic learning and labour market needs, broader access to participants, practical relevance of training, and exchange between education and industry. The main challenges were scheduling, availability of SME employees, differences between institutional calendars and workplace responsibilities, and the need for continuous communication. The main lessons learned were the importance of clear communication channels, flexible self-paced delivery, and involvement of both education and industry partners from planning to evaluation.

4.1.6. TRAINING PROGRAMME IMPLEMENTATION

Overall training delivery

The common delivery model across countries was based on the CyberAgent online platform, self-paced module completion and complementary support through online or face-to-face meetings. Most countries combined asynchronous platform learning with synchronous introductory, support or final sessions.

Romania implemented the pilot over February and March 2026 using synchronous and asynchronous self-paced formats. GCM organised separate kick-off meetings for VET students, SME employees and HEI students, followed by continuous support and final feedback meetings. Spain delivered the programme through individual self-paced learning plans and two online sessions: a kick-off session on 29 January 2026 and a closing session on 26 March 2026. Türkiye used a hybrid model, with physical initial training for TIMTAL students and teachers and online information sessions for other stakeholders. Finland implemented the training mainly as a self-paced online pilot supported by targeted onboarding and follow-up. Participants received instructions on how to register, select modules, complete the learning activities, take the module tests and submit feedback. Poland used different structures for target groups, including face-to-face VET sessions and online HEI and SME sessions. Lithuania integrated the pilot into HEI lectures and organised an online introductory lecture for SME participants on 13 March 2026. Belgium organised two online info-sessions: a kick-off and a wrap-up. Norway mainly used self-paced learning supported by email, chat and limited face-to-face support.

Table 3 - Pilot sessions organisation

Country	Main sessions reported	Format	Main topics covered
Romania	SME kick-off on 10 February 2026, VET kick-off on 11 February 2026, HEI kick-off on 17 February 2026, VET final meeting on 26 March 2026, HEI and SME final meeting on 31 March 2026	VET kick-off and final meeting face-to-face, SME and HEI meetings online	Platform introduction, eight modules, EQF5 and EQF6 levels, materials, pilot stages, responsibilities, credits, hours, registration, module selection, midterm and final assessments, pass requirements, feedback
Belgium	Kick-off and wrap-up sessions	Online	Pilot objectives, learning outcomes, completion goal, final consolidation
Norway	Self-paced implementation, one physical meeting with women VET participants	Mainly online, with some face-to-face support	Platform use, module choice, training completion, group engagement for women VET participants
Spain	Kick-off on 29 January 2026, closing session on 26 March 2026	Online	Platform functionality, module structure, learning objectives, contact methods, milestones, certification process, Piloting student CyberAgent Competition
Türkiye	Physical initial training for TIMTAL, online information sessions for VET schools in Zonguldak and Antalya, SMEs and university students	Hybrid	Platform operation, cybersecurity goals, module structures, learning objectives, critical stages of pilot training

Poland	VET kick-off on 26 February 2026, VET final session on 31 March 2026, HEI and SME kick-off on 10 March 2026, HEI and SME final session on 8 April 2026, Module M2 consultations by Šarūnas Končius	VET face-to-face, HEI and SME online, additional consultations online	Project introduction, objectives, platform, registration, module structure, training process, tests, feedback, module-specific technical support
Lithuania	HEI pilots during face-to-face lectures, SME introductory online lecture on 13 March 2026, active testing in March and April	Hybrid, HEI face-to-face, online and self paced	Registration, platform use, module choice, learning tasks, self-evaluation tests, knowledge assessment tests, feedback and technical issue reporting
Finland	Introductory guidance and individual onboarding during February 2026 Self-paced learning during March to April 2026 Follow-up and feedback collection during April 2026	Mainly online and self-paced, with individual support by email and online communication	Platform registration, module selection, learning pathway guidance, completion of at least one module, feedback collection and relevance of cybersecurity skills for SMEs

4.1.7. PARTICIPANT FIGURES AND ENGAGEMENT

Statistics from the platform analytics

The distribution of registered users shows that the CyberAgent pilot exceeded all project indicators and reached all target groups identified: HEI students, HEI trainers, SME representatives, VET students and VET trainers. The education sector represents the largest group was HEI students, with 226 registered users, followed by VET students with 174 registered users. SME participation was also significant, with 126 registered SME users. This is an important result because SME employees and representatives are a central target group of the CyberAgent project and are hard to engage due to the time constraints they are having. Their participation shows that the training content was not limited to educational use but also reached workplace-based learners who can apply cybersecurity knowledge directly in organisational contexts. The trainers and teachers were also involved as foreseen.

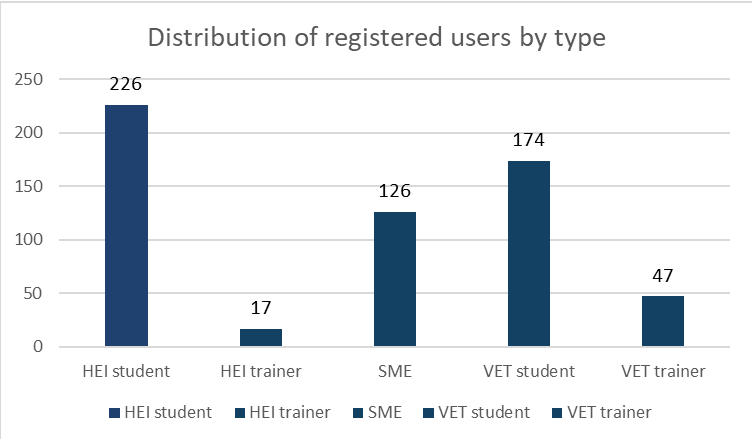

Figure 1 - Distribution of registered users

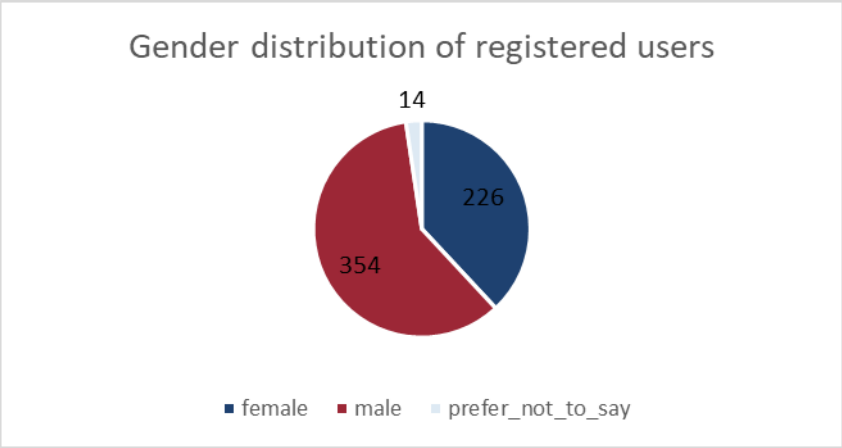

Figure 2 - Platform gender distribution

The gender distribution shows that the CyberAgent pilot reached 354 male participants, 226 female participants, and 14 participants who preferred not to disclose their gender. Male participants formed the largest group, which is not unexpected in cybersecurity-related training, where men are still often overrepresented in technical and digital fields. At the same time, the number of female registrations is important. With 226 women registered, the pilot shows that the programme was able to attract a substantial female audience, not only a small minority. This is a positive result for a project that aims to make cybersecurity skills more accessible and inclusive. It also suggests that the project's outreach, especially through education networks, women-focused networks and flexible online learning, helped reduce some barriers to participation.

The course progress data shows that the three main learner groups moved from registration to active participation at a strong rate. HEI students had the highest number of registrations, with 226 registered users. Of these, 194 started at least one course and 156 passed the test. This shows that HEI students were not only interested in the training but also actively engaged with the learning process. VET students also showed strong engagement. Out of 174 registered users, 162 started at least one course, which means that almost all registered VET students moved into active participation. 129 VET students passed the test, showing a solid completion outcome. This suggests that the training was accessible and relevant for vocational learners, especially when linked to practical learning or teacher-supported implementation. For SME participants, 126 registered, 111 started at least one course, and 90 passed the test. This is a positive result because SME employees often face time constraints due to work responsibilities. The fact that most SME users who registered also started the training suggests that the flexible online format helped them participate despite professional commitments.

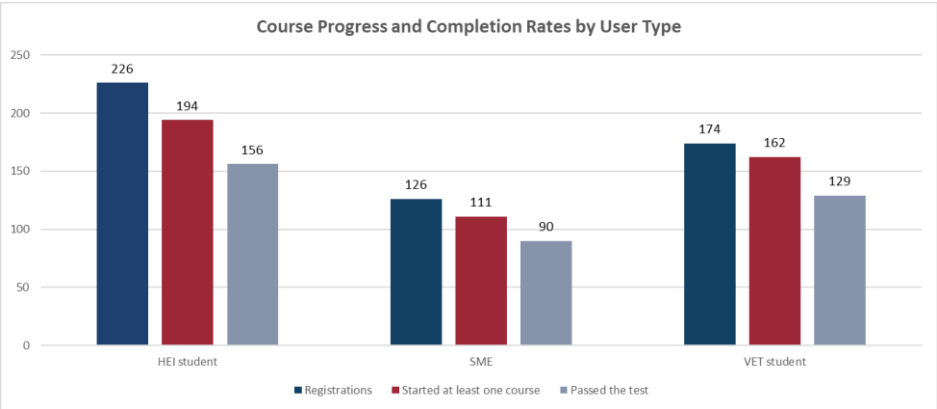

Figure 3 - Course progress and completion

The platform analytics show strong overall engagement with the CyberAgent training programme across the nine modules. The platform attracted broad interest and that a significant share of participants progressed from registration to active learning and successful test completion.

In total, the platform recorded 2,410 module registrations, 1,547 course starts, and 1,060 passed module tests. These figures indicate that the piloting phase reached a substantial number of learners and generated meaningful participation beyond simple registration. The difference between registrations and course starts is expected in an online and self-paced training environment, where some participants register for several modules but do not necessarily begin all of them.

Some drop-off between registration and completion is normal in self-paced online training, especially because learners can register for several modules and were asked to validate at least one module.

Table 4 - All modules' statistics

Module	Registrations	Started the course	Passed the test
M1	489	349	189
M2	352	247	176
M3	253	154	101
M4	259	203	154
M5	223	165	140
M6	208	117	94
M7	212	155	116
M8	226	118	90
M9	188	39	No test for this module
	2410	1547	1060

The module-level progress chart shows clear interest across the full CyberAgent training programme, with the strongest participation in the first modules. M1 had the highest number of registrations, with 489 users, and also the highest number of course starts, with 349 users. This suggests that many participants began their learning pathway with M1, probably because it was seen as an entry point into the programme. However, the number of passed tests dropped to 189, showing that not all learners who started the module completed the assessment. A similar pattern appears in M2, which had 352 registrations, 247 starts and 176 passed tests. This is a strong result and shows that many learners continued beyond the introductory stage. M4 and M5 also performed well, especially M5, where 140 out of 165 starters passed the test. This indicates that learners who started M5 were highly likely to complete it successfully.

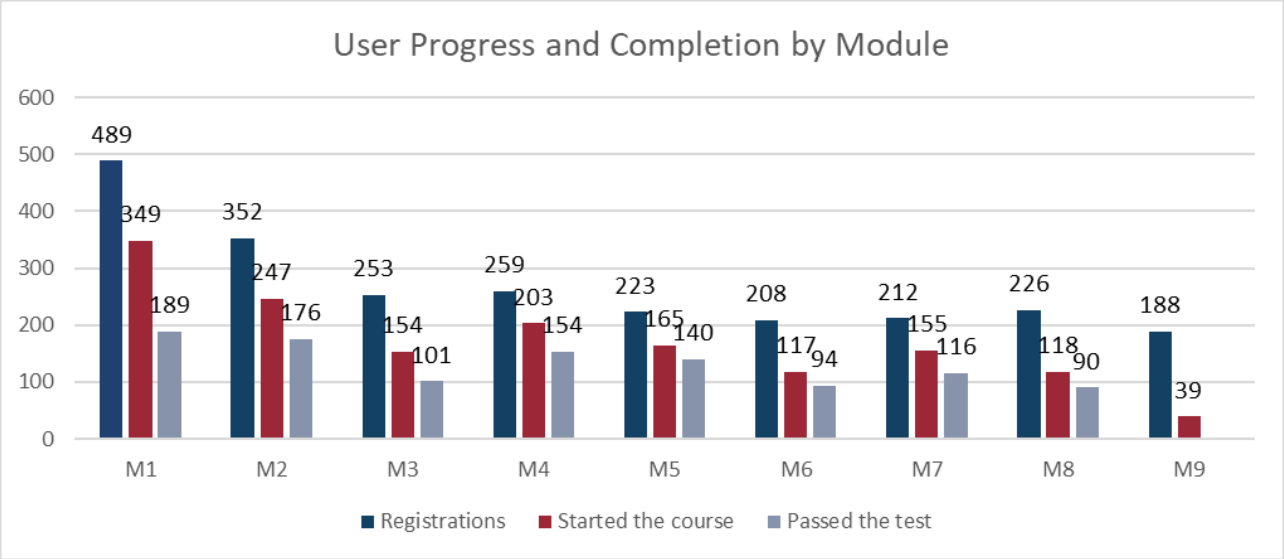

Figure 4 -Progress and completion numbers by module

The more technical or specialised modules show slightly lower engagement. M3, M6, M7 and M8 had fewer registrations and starts than M1 and M2 but still produced solid completion numbers. This suggests that participants were more selective when choosing these modules, possibly depending on their role, prior knowledge, or confidence with technical cybersecurity topics.

M9 stands out because it had 188 registrations but only 39 course starts. Since this module did not include a test, there is no passed-test figure. The lower start rate may mean that participants prioritised the assessed cybersecurity modules during the pilot period. It may also show that career-oriented content needs to be introduced more clearly as part of the learning pathway.

4.1.8. TARGET GROUP FIGURES BY COUNTRY

Table 5 - Summary of user data per country

Country	Platform registration / selection	Started / active participation	Passed / completed minimum requirement	Target-group profile reported	Trainers / teachers	Gender information reported
Romania	70 registered users: VET 29, HEI 32, SME 9	58 users spending more than 45 minutes: VET 28, HEI 22, SME 8	64 passed or completed minimum requirement: VET 28, HEI 28, SME 8	Piloting profile reported as VET 28, HEI 29, SME 9	11 trainers, 2 HEI teachers, 11 VET teachers	SME trainees: 7 women, 2 men, HEI trainees: 11 women, 18 men, VET trainees: 8 women, 20 men, HEI lecturers: 1 woman, 1 man, VET trainers: 10 women, 1 man
Belgium	66 selected participants	54 course users	32 completed the pilot minimum requirement	Profile reported as VET 3, HEI 23, SME 20	No formal HEI or VET teacher involvement reported	40 women, 5 men
Norway	HEI 15, SME 23, VET 17, =55	HEI student: 11 unique users, VET student: 14, SME: 15 and VET trainer: 2 unique users	SME: 8), VET student: 7 , HEI student	Profile reported as VET 14, HEI 11, SME 15	2 trainers	28 men and 14 women
Spain	59 registered platform users	49 course users	26 users passed at least one module test, 74 modules completed in total	Interest received from VET 34, HEI 36, SME 20. Registered profile reported as VET 11, HEI 26, SME 9. Passed profile reported as VET 5, HEI 16, SME 5	2 EVM trainers, 1 HEI trainer, 2 VET teachers	Overall gender repartition: 68.5% men, 29.3% women. Course users: 71.4% men, 26.5% women. SME registered users: 2 women, 7 men
Türkiye	136 registered users reported overall, role table reports 100 users: VET 77, HEI 10, SME 13	85 active participants	78 passed by role table: VET 65, HEI 5, SME 8	Interest received from VET 88, HEI 17, SME 13. Registered profile reported as VET 77, HEI 10, SME 13	4 INNOMATE trainers, 1 HEI trainer, 10 VET teachers	Gender repartition: 80% men, 19% women. SME employees: 3 women, 10 men
Poland	79 registered participants	69 started at least one module	52 passed at least one module test	Registered profile: VET 24, HEI 23, SME 20. Started profile: VET 21, HEI 20, SME 16. Passed profile: VET 17, HEI 14, SME 11	3 trainers, 2 HEI teachers, 10 VET teachers	44 men, 34 women and 1 undisclosed registered
Lithuania	136 registered participants	255 course/module starts across all modules	111 passed at least one module	Profile reported as HEI 89 registrations dropping to 78 course starts, SME 25 registered, all started, and 21 passed. VET student figure not reported	1 trainer, 10 HEI teachers, 4 VET teachers	49 women registered and 42 passed, 79 men registered and 63 passed, 8 undisclosed registered and 6 passed
Finland	34 registered participants	24 started at least one course or module	22 passed at least one module test	Registered profile: VET 8, HEI 9, SME 11. Passed profile: VET 6, HEI 8, SME 8	2 trainers	22 men and 12 women

4.1.9. SKILLS AND KNOWLEDGE DEVELOPMENT

All national reports reported positive development in cybersecurity awareness, knowledge, confidence or practical skills. Additional quantitative and qualitative assessments can be found in the feedback survey analysis in the section 3 of this report.

Romania reported that participants showed clear improvement in cybersecurity knowledge and skills. Feedback indicated increased awareness of online safety, data protection, cyber threats and secure digital practices. Participants stated that the course helped them understand real-life cybersecurity risks and how to respond to them. Final discussions confirmed increased confidence in identifying threats and applying preventive measures in personal and professional contexts.

Belgium reported moderate engagement overall, with time constraints affecting completion of more demanding modules. Participants who completed the training demonstrated noticeable improvements in cybersecurity knowledge and confidence. Survey feedback indicated satisfaction with the pilot, increased awareness of cybersecurity concepts and stronger readiness to apply these skills in professional or academic contexts.

Norway reported generally positive engagement, with variation due to the self-paced format. Most participants reported increased cybersecurity knowledge. Many indicated that they gained new practical skills and better understanding of cybersecurity challenges, especially in an SME context. Several participants reported greater confidence and a stronger ability to contribute to cybersecurity improvements in SME settings. Informal feedback suggested that SME employees found the training directly relevant to daily work, while some students were more critical because they lacked a clear context in which to apply the knowledge.

Spain reported a very positive overall perception of the course, highlighting comprehensive content and a learning method adapted to people balancing studies and work. Evaluation results showed that 85.71% agreed or strongly agreed that the training boosted confidence in cybersecurity topics, 82.85% reported acquiring new practical cybersecurity skills, knowledge and strategies, and 80% felt they understood their role's impact on SME cybersecurity practices. However, only slightly over half, 51.42%, felt capable of actively contributing to cybersecurity improvements within an SME.

Finland reported positive learner engagement among the participants who completed the pilot and evaluation. The was overall found useful for improving general cybersecurity awareness, understanding cyber risks, and recognising the importance of everyday secure digital practices. SME employees valued the topics connected to organisational security, risk awareness, data protection and secure online behaviour. All target groups valued the possibility to study independently and select modules according to their own interests. However, it was pointed out that some modules were lengthy.

Türkiye reported strong positive data. The general perception was positive, with participants highlighting comprehensive content and suitability for people balancing academic studies with professional life. High scores in Systems Administration and Security Operations indicated acquisition of practical cybersecurity skills and strategies. SME employees reported better understanding of their role's impact on SME cybersecurity practices. The report also noted that completion rates remained low in more technical modules such as Analytical Tools, indicating a need for practical mini-activities and technical guidance.

Poland reported high engagement across SME representatives, HEI students and lecturers, and VET students and teachers. Participants completed self-assessment activities, consultations and knowledge assessment tests. Feedback indicated improved cybersecurity awareness, digital safety understanding and practical cybersecurity skills. Participants reported gaining knowledge in cybersecurity risks, social engineering, data protection, risk management, cybersecurity governance and technical security measures.

Lithuania reported that informal feedback and module analysis showed different interests across target groups. Students tended to choose more technical subjects, while SMEs chose more analytical and risk management subjects. HEI students demonstrated a broad spectrum of technical and analytical skills. SMEs showed needs around governance and systems administration. The VET audience, although small, focused on technical and risk management fundamentals. At least one participant from each group tested and passed the final test for all modules from M1 to M9.

4.1.10. LESSONS LEARNED

The national piloting reports show that the CyberAgent training programme was implemented successfully across different educational, organisational and national contexts. The cross-country analysis points to three main conclusions: recruitment works best when it is targeted and relational, retention depends on structured follow-up and the future CyberAgent model should be differentiated for HEI, VET and SME workplace settings.

Recruitment approaches that worked best

The pilot shows that recruitment was most successful when partners used existing trusted networks, direct communication and clear explanations of the value of the training. Passive dissemination alone was not sufficient. Countries that combined institutional contacts, personal invitations, targeted online promotion and direct follow-up were better able to convert interest into actual participation.

For HEI and VET learners, recruitment worked best when the training was connected to existing educational structures. The strongest examples were those where teachers, lecturers or institutional contacts introduced the training directly to learners, explained its relevance, and supported access to the platform. Future HEI and VET implementation should not rely only on open calls, but should be embedded into courses, practical assignments or teacher-guided extracurricular activities.

For SME employees, recruitment required a different logic. SMEs were more difficult to reach and retain because employees had limited time and competing work responsibilities. The most effective SME recruitment approaches were those that presented the training as practical, flexible and directly useful for workplace cybersecurity. Direct contact through business networks, chambers, SME associations, professional contacts and project partners' own networks appears more suitable than general dissemination. Paid social media campaigns can increase visibility, but they should be combined with eligibility screening, onboarding and follow-up to avoid a gap between expressions of interest and actual participation.

Target groups that were hardest to retain

As foreseen by the partners at the beginning of the project, SME employees were the most challenging group not only to retain throughout the full learning process but also to engage. This was not because the content was irrelevant, but because workplace learners face time constraints, various schedules and limited availability for structured training. In several countries, SME participants showed interest but needed additional reminders, flexible deadlines, technical support or individual guidance to complete the training.

VET and HEI learners were easier to retain when the training was supported by teachers or linked to an educational activity. However, where participation depended fully on voluntary self-paced learning, follow-through also became more difficult. This means that the issue is not only target group motivation, but the level of structure around the learning process.

The key lesson is that self-paced learning increases access but does not automatically guarantee completion. The future implementation model should therefore combine flexibility with light structure. This could include a short onboarding session, suggested learning timetable, reminders, module completion milestones, and a final reflection or feedback activity. These elements do not need to reduce flexibility, but they help learners move from registration to active completion. Trainer support appears to be a strong factor for successful engagement.

Delivery models that appear strongest

The cross-country evidence supports a differentiated implementation model rather than one uniform training pathway for all learners. The strongest delivery model across the pilot was not a purely self-paced model, nor a fully classroom-based model. The most transferable model was a blended support model: online self-paced modules combined with introductory guidance, technical support, reminders and optional synchronous activities.

- For VET learners, face-to-face or teacher-supported delivery appears particularly effective. VET students benefit from clear instructions, classroom integration, practical examples and teacher encouragement. The training can be used as part of cybersecurity, digital skills, ICT, business or entrepreneurship-related learning.
- For HEI learners, the training works best when connected to academic or professional development objectives. HEI implementation can be more independent than VET, but students still benefit from a structured introduction, recommended module pathways and links to real-world cybersecurity roles.
- For SME employees, the strongest model is flexible workplace-based learning. SME learners need short, practical pathways that clearly answer: "What does this mean for my company, my role and my daily work?" For this target group, long academic framing should

be reduced and replaced with practical guidance, workplace examples, checklists and action-oriented tasks.

4.1.11. SUGGESTED IMPLEMENTATION MODELS FOR THE NEXT PHASE

Based on the piloting evidence, the CyberAgent programme confirmed the three differentiated models' approach: an HEI model, a VET model and an SME workplace model. These models should share the same core platform and learning content, but differ in recruitment, facilitation, learning pathway, support and expected follow-up.

HEI implementation model

The HEI model should position CyberAgent as a flexible academic and professional development resource for students in cybersecurity, ICT, business, management, engineering and related fields. The model should be semi-structured rather than fully informal.

Recommended implementation approach:

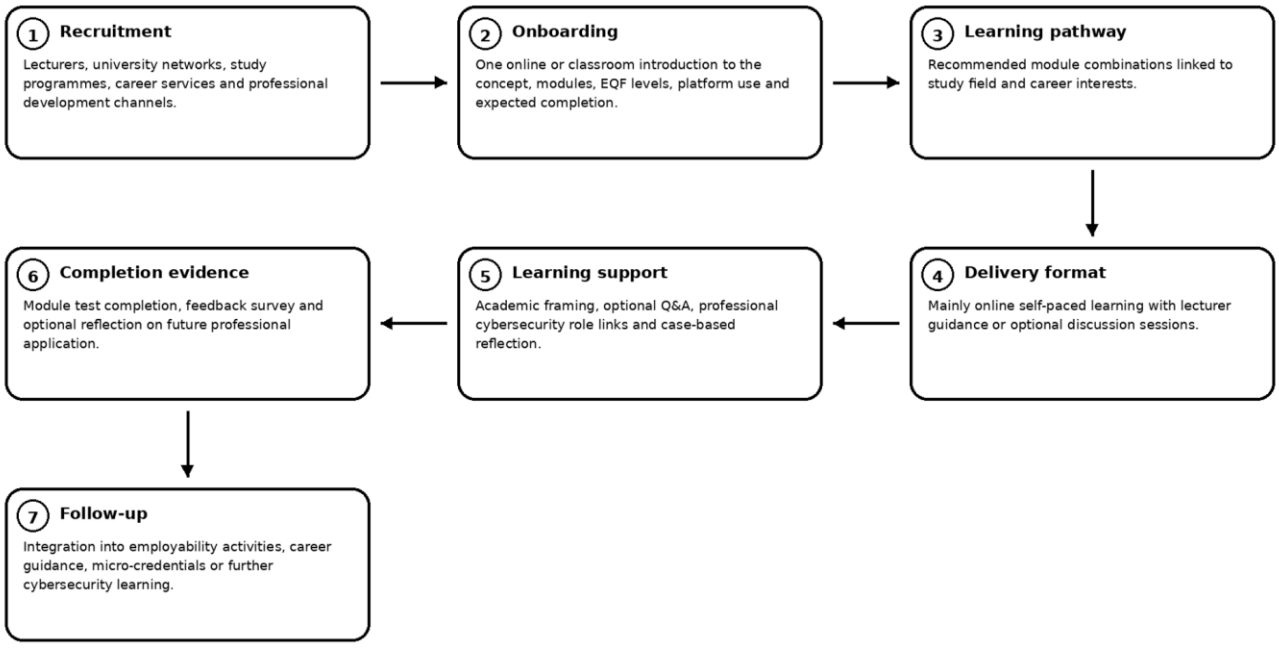

Figure 5 - HEI implementation model for CyberAgent training

The HEI model should emphasise employability, professional identity and progression into cybersecurity-related roles. Students can be encouraged to use CyberAgent as a bridge between academic knowledge and workplace cybersecurity practice.

VET implementation model

The VET model should be more structured and teacher supported. The piloting shows that VET learners benefit from clear guidance, practical examples and classroom or blended delivery. The training should therefore be integrated into existing digital skills, ICT, business, entrepreneurship or workplace digital safety where possible.

Recommended implementation approach:

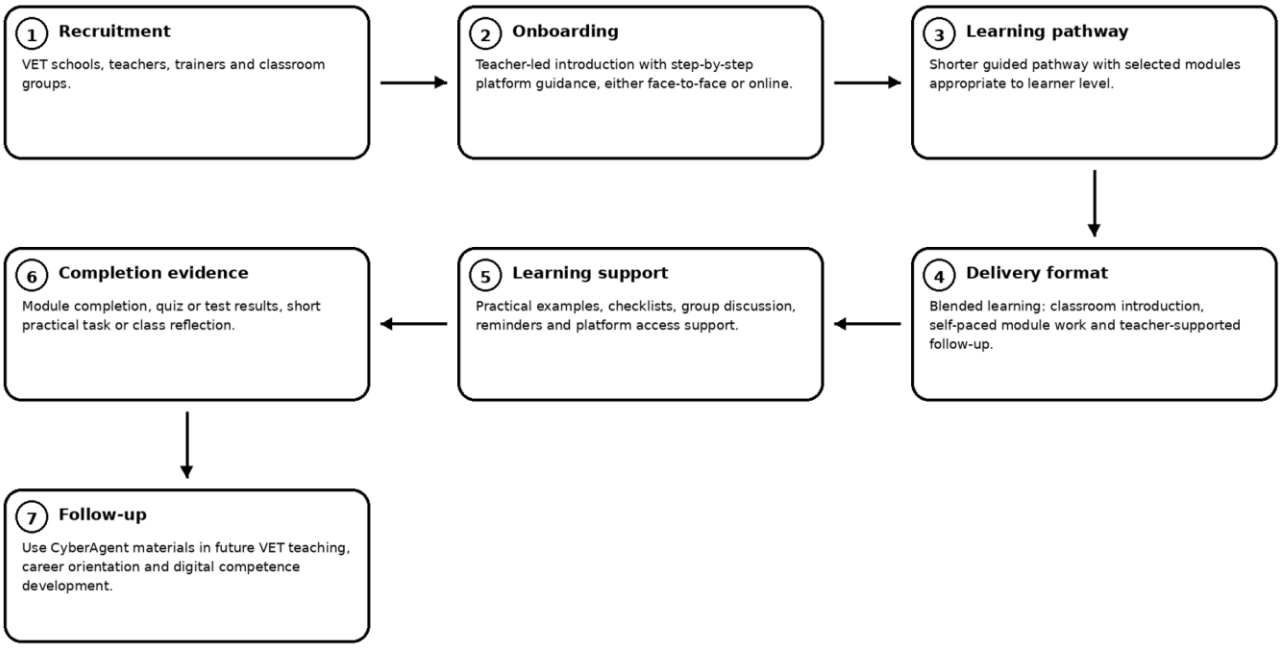

Figure 6 - VET implementation model for CyberAgent training

The VET model should focus on practical cybersecurity behaviour, employability and awareness of workplace risks. It should avoid presenting the programme as only technical cybersecurity training. Instead, it should show learners how cybersecurity relates to everyday work, communication, data protection and responsible digital behaviour.

SME workplace implementation model

The SME model should be the most flexible and practice oriented. SME employees are a central target group, but they are also the hardest to retain because of limited time and work responsibilities. The future SME model should therefore minimise unnecessary complexity and make the value of participation immediately clear. The SME model should not simply copy the education model. It should be built around workplace relevance. The language, examples and follow-up tasks should help employees transfer learning into daily routines, such as password practices, phishing awareness, safe data handling, incident reporting and basic risk recognition.

Recommended implementation approach:

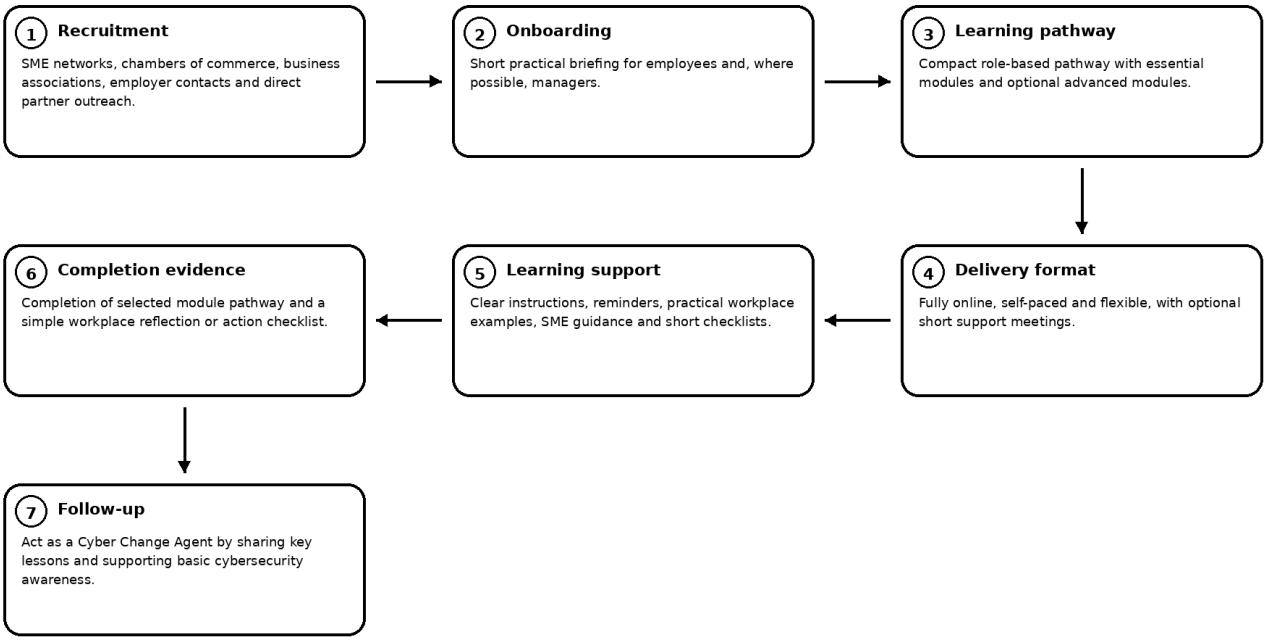

Figure 7 - SME workplace implementation model for CyberAgent training

THE CYBER CHANGE AGENT CONCEPT

The next phase should clarify how the CyberAgent training leads to the Cyber Change Agent concept. The piloting shows that the training can raise awareness and improve knowledge, but the post-piloting phase should define how trained participants can become local multipliers in education and SME settings.

A Cyber Change Agent should not be understood as a technical cybersecurity expert. Rather, the role should be defined as a person who can promote basic cybersecurity awareness, encourage safer digital behaviour, recognise common risks and guide peers or colleagues towards appropriate support.

One of possible Cyber Change Agent implementation pathway in SMEs could be:

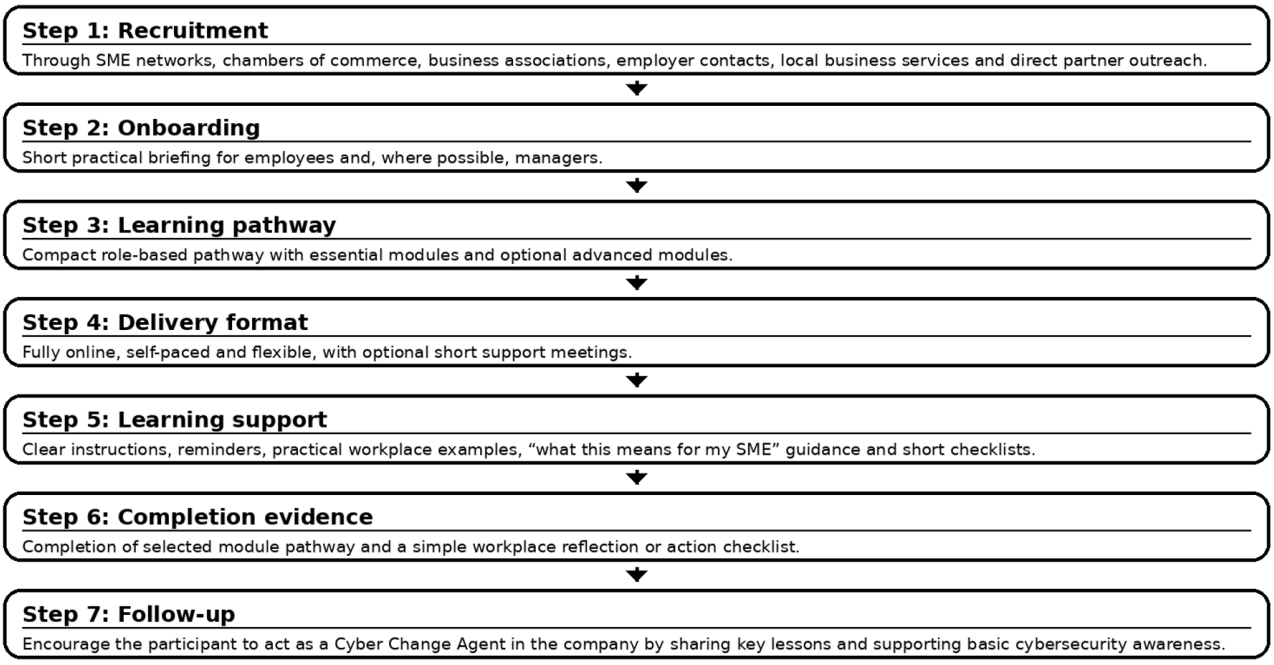

Figure 8 - Step-by-step SME workplace implementation model for CyberAgent training

5. PILOTING EVALUATION – FEEDBACK SURVEY ANALYSIS

5.1. METHODOLOGY

After the piloting session, a feedback survey was shared to all participants to gather feedback, measure qualitative and quantitative elements and highlight areas of improvement.

The analysis uses the data exported from this participant survey. The dataset contains 272 rows. The survey includes respondent profile questions, delivery-mode questions, trainer-support questions, module evaluation questions, platform-evaluation questions, impact questions, satisfaction questions, recommendation questions and open-text questions.

The dataset was checked and cleaned before analysis, and no personal identifiers were used in the analysis.

Closed Likert-type answers were converted to numerical scores to calculate averages. For quality ratings, Very poor = 1, Poor = 2, Average = 3, Good = 4 and Very good = 5. For agreement ratings, Strongly disagree = 1 through Strongly agree = 5. Positive responses are reported as Good/Very good, Satisfied/Very satisfied, or Agree/Strongly agree depending on the question type. "I did not follow this module" was excluded from module-quality averages but counted as non-followed for module reach.

Important note on satisfaction level: In the analysis, both the mean score and the positive rating percentage were used because they provide complementary information. The mean score reflects the overall average evaluation on a 1 to 5 scale, taking all response categories into account, including neutral and negative ratings. The positive rating percentage, on the other hand, shows the proportion of respondents who selected the two highest categories, such as Good/Very good or Satisfied/Very satisfied. For this reason, two indicators may have the same or very similar mean score but different positive percentages. This can happen when one item has more Very good ratings but also more Average or negative ratings, while another has a larger concentration of Good ratings. Therefore, the mean indicates the general strength of the ratings, while the positive percentage shows how widely positive perceptions were shared among participants. Using both measures gives a more balanced understanding of the survey results.

While some satisfaction levels can sometimes be below the 80% threshold, it is important to also consider the dissatisfaction level which is most of the time very low, i.e below 5%.

5.2. ANALYSIS

Respondent profile and coverage

The respondent distribution shows good coverage across the piloting countries.

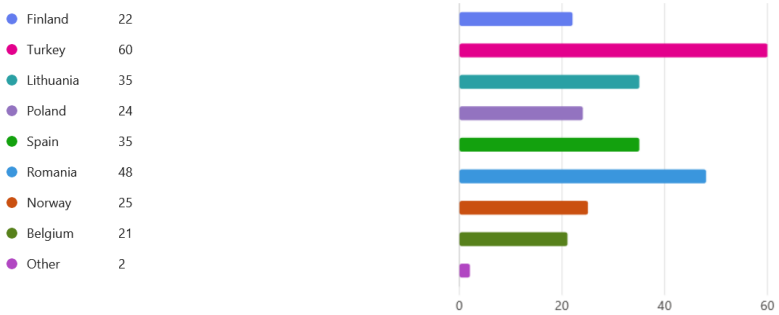

Figure 9 - Respondent distribution per country

The survey responses came mainly from learners in education. VET students formed the largest group, with 124 respondents, representing 46% of the sample. HEI students followed with 101 respondents, or 37%. SME employees represented 47 respondents, equal to 17% of the sample. Although this is the smallest group, their participation is important as they are hard to engage in piloting activities.

Figure 10 - Respondent groups

Evaluation of training delivery and trainer support

The training was mainly followed through two modes: 174 participants followed it fully online through the platform, while 98 used a hybrid mode with platform and trainer support. Trainer-support questions were answered by the hybrid participants.

Table 6 - Evaluation of delivery and trainer support

Trainer/delivery indicator	Number of answers	Mean /5	Good or very good
Trainer availability and support	98	4.81	96.9%
Clarity of trainer explanations	98	4.81	96.9%
Usefulness of off-platform sessions	98	4.80	99.0%
Feedback and follow-up during training	98	4.83	95.9%

The trainer-supported pathway performed very well. Trainer availability, clarity of explanations, usefulness of off-platform sessions and feedback/follow-up all scored highly. This suggests that the train-the-trainer and local delivery arrangements supported learner engagement where trainer support was available. The fully online route also performed positively in the overall outcome indicators, but few open comments show that some learners would benefit from clearer platform guidance, more practical examples and more interaction.

Evaluation of training modules

The module evaluation results are positive overall. Across all nine modules, the average satisfaction rate was 78.3%, with quality, relevance and usefulness all scoring close to 80% level. This shows that participants generally valued the CyberAgent training content and found the modules useful for building cybersecurity knowledge and awareness.

Table 7 - Training module evaluation

Module	Quality satisfaction %	Relevance satisfaction %	Usefulness satisfaction %	Average satisfaction %
M1 Security Program Management	83.7%	85.6%	81.4%	**83.6%**
M2 System Administration	79.6%	80.0%	81.3%	**80.3%**
M3 Analytical Tools	77.3%	79.1%	76.9%	**77.8%**
M4 Security Operations	81.7%	76.0%	77.5%	**78.4%**
M5 Security Governance & Policy	78.2%	78.5%	78.2%	**78.3%**
M6 Cybersecurity Planning	77.7%	73.2%	75.2%	**75.4%**
M7 Risk Management	79.7%	76.7%	76.5%	**77.6%**
M8 Business Continuity	81.6%	76.6%	73.0%	**77.1%**
M9 Empowering Careers in Cybersecurity	77.5%	70.9%	71.2%	**73.2%**
Overall	**79.9%**	**77.9%**	**77.1%**	**78.3%**

Comparative analysis of quality, usefulness and relevance satisfaction by module

The participant satisfaction was generally positive across all CyberAgent modules, but the pattern is not identical for quality, usefulness and relevance. Learners were asked not only to judge the modules only by how well they were prepared, but also by how clearly they could connect the content to their own learning, work or future role.

The quality satisfaction scores are the most stable across the modules. All modules scored between 77.3% and 83.7%, which suggests that participants generally saw the learning materials as well developed and acceptable in terms of structure, content and presentation. M1 Security Program Management received the highest quality score at 83.7%, followed by M4 Security Operations at 81.7% and M8 Business Continuity at 81.6%. Even the lowest quality score, 77.3% for M3 Analytical Tools, remains positive.

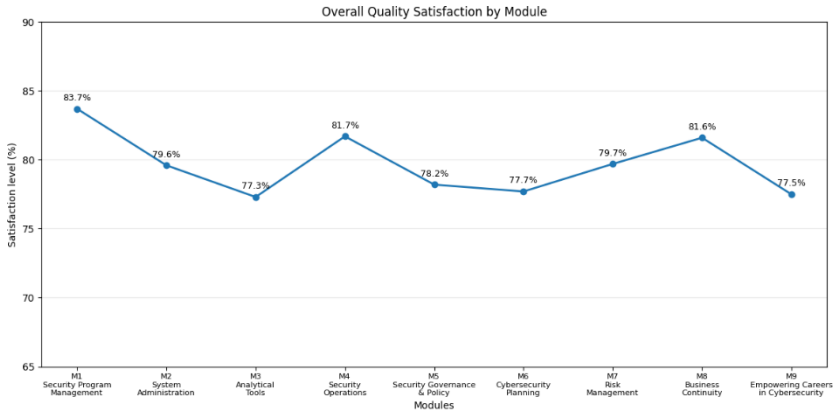

Figure 11 - Overall quality satisfaction by module

The usefulness satisfaction chart shows a downward movement across the programme. M1 and M2 received the strongest usefulness scores, with 81.4% and 81.3%. These modules were probably easier for participants to connect with practical learning needs, especially as entry-level or foundational topics. However, usefulness drops in later modules, especially M8 Business Continuity at 73.0% and M9 Empowering Careers in Cybersecurity at 71.2%. As most of participants are students, maybe some did not fully see how to apply them directly in their own context.

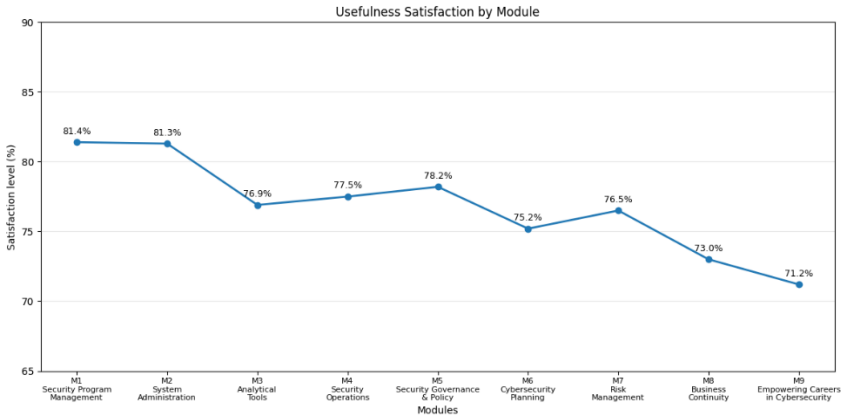

Figure 12 - Overall satisfaction by module

The relevance satisfaction chart shows the widest variation. M1 again stands out with the strongest result, 85.6%, which confirms that participants clearly recognised the importance of security programme management. M2 System Administration also performed well at 80.0%. By contrast, M6 Cybersecurity Planning scored 73.2% and M9 Empowering Careers in Cybersecurity scored 70.9%, the lowest relevance result. Same as the previous chart, since the respondents are mostly VET and HEI students, they may not immediately understand how planning or career-development content applies to them.

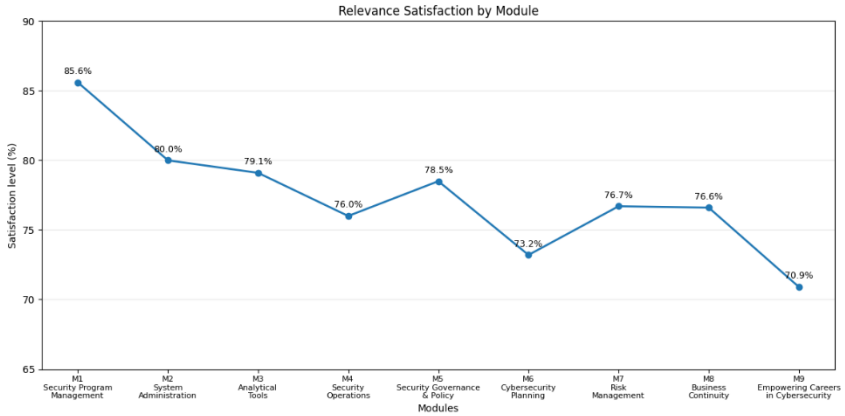

Figure 13 - Overall relevance evaluation by module

The comparison shows that the CyberAgent modules were positively received, especially in terms of quality. The main improvement need is to strengthen the perceived relevance and usefulness of some modules. This could be done by adding more real SME examples, short practical tasks, role-specific guidance, templates, simulations and clearer learning pathways for different groups of learners.

Evaluation and the 80% satisfaction indicator target: Some context

The training content targeted satisfaction rate was set at 80%. Looking at the overall satisfaction rate, this indicator was reached. However, when looking at some specific modules individually, the indicator was not fully reached. The main reason appears to be technical. The large-scale piloting phase was not only designed to test the quality and relevance of the training content, but also to assess the technical robustness of the platform under real implementation conditions. During this period, the platform was put under significant pressure, with a high number of users accessing the courses, completing activities, navigating between modules and submitting assessments within a limited timeframe. This intensive use revealed some temporary technical weaknesses, including login difficulties, navigation issues, progress tracking problems and exam submission errors. These issues, that were completely fixed during the piloting, affected the user experience and, in some cases, influenced participants' perception of the modules themselves, even when the content was relevant and useful. Therefore, the lower satisfaction rates observed in certain modules should be understood mainly as a consequence of temporary platform instability during the piloting phase, rather than as an indication of insufficient content quality. A chronological review of the survey timestamps shows that average evaluation scores declined noticeably during the period between 29 March and 10 April, when several users reported technical problems related to login, exam submission, answer confirmation and platform navigation. In total, 25% of respondents reported technical issues. A more detailed analysis of modules M3, M5, M6 and M9, whose quality ratings fell below the projected 80% threshold, supports this interpretation. The lowest evaluations were strongly concentrated within the technical instability period. For example, in M3, 7 out of the 8 lowest evaluations came from respondents who also reported technical problems during this period. A similar pattern was observed in M5 with 5 out of 7 low evaluations, M6 with 7 out of 10, and M9 with 4 out of 7. Once the technical issues had been resolved, the evaluation curve for these modules returned to a higher level.

For M9 "Empowering Careers in Cybersecurity" the lower scores in relevance and usefulness also appear to be linked to the structure of the module. M9 did not include a final knowledge assessment test, which may have reduced learner engagement and the perceived formal value of the module. Without an objective assessment mechanism, participants may have found it more difficult to recognise their learning progress or connect the module to measurable outcomes.

The profile of the respondents also helps explain the lower ratings for some strategically oriented modules. A large share of the survey respondents came from the academic community, particularly VET and HEI learners. These participants may not yet have direct work experience in SMEs or organisational cybersecurity planning. As a result, modules such as M6 "Cybersecurity Planning" and M8 "Business Continuity" which require a more strategic and organisational perspective, may have seemed less immediately relevant or useful to students. By contrast, more practical and introductory modules, such as M1 and M2, received stronger evaluations because their value was easier for learners to understand and apply in their current learning context.

Evaluation of the digital platform

The platform is the key component of the CyberAgent project which serve as a digital learning and collaboration ecosystem that can support knowledge exchange, training delivery and transfer to other countries. The survey results show that the platform worked positively overall. Some user comments identify concrete usability improvements that were considered by the consortium to enhance the user experience.

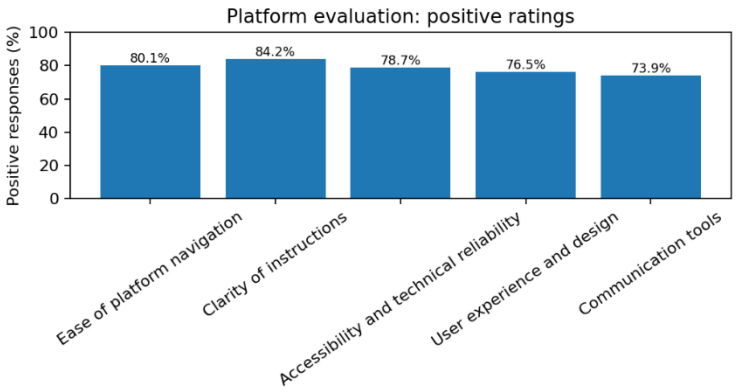

Figure 14 - Platform evaluation

Platform indicator	Mean /5	Good or very good
Ease of platform navigation	4.05	80.1%
Clarity of instructions	4.21	84.2%
Accessibility and technical reliability	4.06	78.7%
User experience and design	4.08	76.5%
Communication tools (trainer or peer interaction through the messaging feature)	4.06	73.9%

Clarity of instructions is the strongest platform indicator, with 84.2% positive ratings. Communication tools received the lowest positive share at 73.9%. This is still positive overall, but it suggests that peer interaction and trainer communication features could be improved or better explained to users.

Satisfaction item	n	Mean /5	Satisfied or very satisfied	Dissatisfied or very dissatisfied
The training content	272	4.22	84.9%	4.4%
The platform	272	4.03	77.2%	6.2%

Learning outcomes and impact

The results indicate that the training achieved its central upskilling purpose. The strongest result is transferability: respondents widely agreed that the training could be adapted in other countries. Knowledge improvement and understanding of SME cybersecurity challenges also reached high positive levels. The SME applicability scored lower. It can be explained by the fact that most respondents are students and they can't foresee yet how they would apply this knowledge.

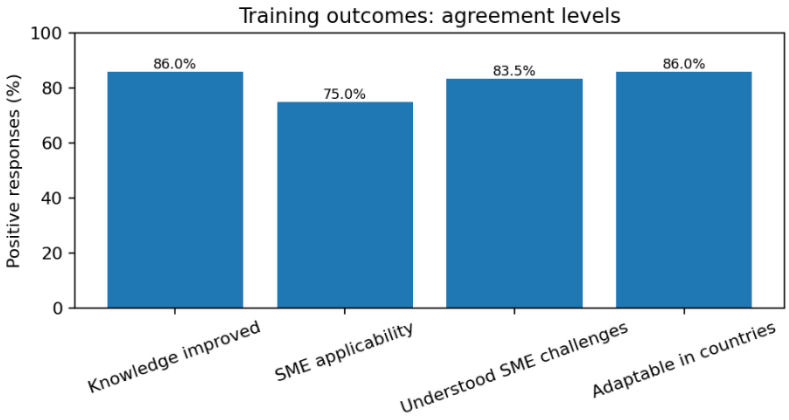

Figure 15 – Satisfaction of learning outcomes and impact

Table 8 - Detailed value of learning outcome and impact

Outcome indicator	Mean /5	Agree or strongly agree	Disagree or strongly disagree
The training improved my cybersecurity knowledge	4.23	86.0%	1.5%
The training is applicable in real SME contexts	4.06	75.0%	3.3%
The training helped me better understand cybersecurity challenges faced by SMEs	4.17	83.5%	2.2%
I believe that this training could be easily adapted in other countries	4.36	86.0%	1.1%

Prior to the programme, respondents assessed their real understanding of cybersecurity as mixed: 78 respondents reported low or very low prior understanding, 127 reported medium prior understanding, and 67 reported high or very high prior understanding. After the programme, 243 respondents reported that they had increased their cybersecurity knowledge, 23 were not sure, and 6 reported no increase.

The strongest impact indicators were flexibility of the format (86.0% positive) and increased confidence (82.7% positive). The lowest, although still positive, was feeling capable of contributing to cybersecurity improvements in an SME (71.7% positive). This suggests that future versions should add more workplace transfer tasks, examples and action-planning exercises to help learners convert knowledge into practical SME improvement actions.

The strongest impact indicators were flexibility of the format (86.0% positive) and increased confidence (82.7% positive). The lowest, although still positive, was feeling capable of contributing to cybersecurity improvements in an SME (71.7% positive). This suggests that future versions should add more workplace transfer tasks, examples and action-planning exercises to help learners convert knowledge into practical SME improvement actions.

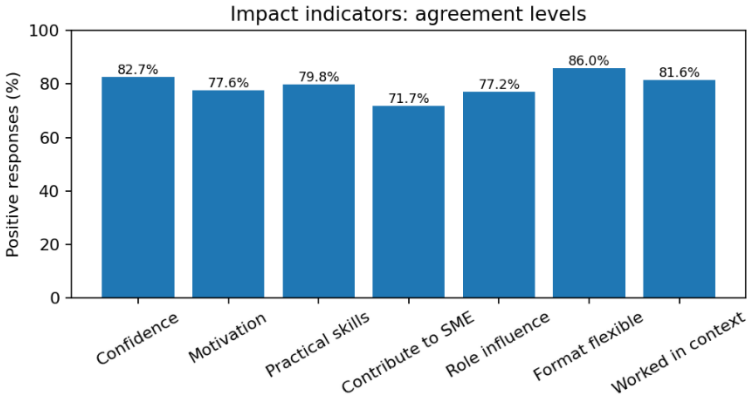

Figure 16 - Score of specific items impact evaluation

Table 9 - Detailed values of impact evaluation

Impact indicator	Mean /5	Agree or strongly agree	Disagree or strongly disagree
The training increased my confidence in cybersecurity topics	4.15	82.7%	1.5%
The training increased my motivation to engage with cybersecurity	4.12	77.6%	2.6%
I gained new practical cybersecurity skills, knowledge and strategies	4.14	79.8%	2.9%
I feel capable of contributing to cybersecurity improvements in an SME	3.93	71.7%	6.6%
I understand how my role can influence SME cybersecurity practices	4.05	77.2%	2.6%
The training format was flexible enough for my schedule (pace, timing, hybrid/online)	4.31	86.0%	3.3%
The training worked well in my learning/work context (student / SME employee).	4.21	81.6%	3.7%

Knowledge and competence development

Two questions give a useful before and after view of the training impact. The first question asked participants to reflect on their real level of cybersecurity understanding before starting the programme, while the second asked whether their cybersecurity knowledge increased after completing the training.

Before the training, most participants did not consider themselves highly knowledgeable in cybersecurity. The largest group selected Medium, with 126 respondents, equal to 46.3% of all participants. A further 57 respondents, or 21.0%, selected Low, and 22 respondents, or 8.1%, selected Very low. This means that 75.4% of participants placed themselves between very low and medium before the programme. Only 48 respondents, or 17.6%, selected High, and 19 respondents, or 7.0%, selected Very high.

15. Now that you have finished the training, what do you think was your real understanding of cybersecurity before starting the program?

Figure 17 - Self-understanding of cybersecurity before the training

After the training, the responses show a very strong perceived learning effect. 243 out of 272 participants, or 89.3%, answered that they had increased their cybersecurity knowledge. Only 6 respondents, or 2.2%, answered No, while 23 respondents, or 8.5%, were not sure.

16. After completing the training, have you increased your cybersecurity knowledge?

Figure 18 - Evaluation of knowledge gain after the training

The comparison suggests that the training was especially relevant because the participant group started from a mixed but mostly non-expert baseline. Since nearly half of the respondents rated their previous understanding as only Medium, and almost one third rated it as Low or Very low, the programme addressed a clear learning need. The high share of participants reporting increased knowledge shows that the training successfully reached not only beginners but also participants who already had some previous cybersecurity understanding.

A closer cross-comparison confirms this. Among participants who initially rated their understanding as Very low, 90.9% still reported an increase in knowledge. Among those who rated themselves as Low, 86.0% reported improvement. The result was also strong among those with a Medium starting level, where 89.7% reported increased knowledge. Even participants who started from High or Very high levels mostly reported improvement, with 91.7% and 89.5% answering Yes, respectively.

Table 10 - Comparative analysis between cybersecurity initial understanding level and knowledge gain perception

Initial understanding	Yes, knowledge increased	I'm not sure	No
Very low	90.9%	9.1%	0.0%
Low	86.0%	10.5%	3.5%
Medium	89.7%	8.7%	1.6%
High	91.7%	4.2%	4.2%
Very high	89.5%	10.5%	0.0%

The findings indicate a broad and positive learning impact. The training appears to have been accessible enough for participants with limited prior knowledge, while still offering added value to those who already had a stronger cybersecurity background. The very small share of negative responses suggests that the programme was effective in improving participants' perceived cybersecurity competence.

Barriers, qualitative feedback and improvement needs

The survey asked respondents whether they faced barriers and invited them to describe improvement needs. Quantitative barrier responses show that most participants did not report significant barriers, while technical issues and content complexity were the most common challenges among those who did.

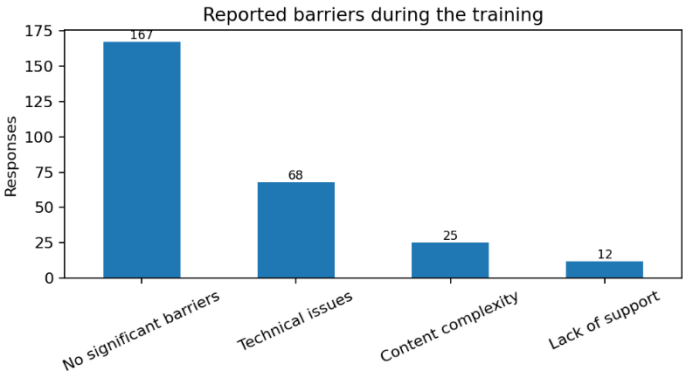

Figure 19 - Reported barriers during the training

Table 10 - Detailed barriers category

Barrier category	Responses	Share
No significant barriers	167	61.4%
Technical issues	68	25.0%
Content complexity	25	9.2%
Lack of support	12	4.4%

The open-text answers provided an indicative synthesis to guide the improvement strategy. The most repeated themes are presented below.

Table 11 - Improvement suggestions in open text answers

Qualitative theme	Indicative mentions
Platform usability, navigation or assessment flow	35
Technical access or reliability issues	29
Positive value: accessibility, flexibility and broad knowledge	24
More practical cases, hands-on labs or real SME examples	22
Content density, structure or learning-path differentiation	17
Voice, language or presentation style	11
Need for more interaction or peer learning	8

The qualitative feedback shows that participants were generally positive about the training, with many stating that no major improvements were needed. However, the comments also highlight several clear areas for improvement: the training content should be made less text-heavy, more dynamic, and more practical. Several participants noted that some modules were too fragmented across many PDFs or chapters, while others mentioned repetition or unclear structure. Assessment design also emerged as an important issue, with comments about repetitive questions, visible correct answers, unclear exam flow, and technical problems in submitting or completing tests. In addition, some learners felt that highly technical modules, especially those involving system administration or analytical tools, may be too advanced for average SME employees without prior IT experience.

Indicative improvement strategy based on the gathered feedback

Priority	Recommendations	Action/Response
High	Review all quiz and exam questions for correctness, clarity, repetition, and technical errors	A full pedagogical and technical review of all module quizzes and final exam questions was made and incorrect content was fixed.
High	Fix final exam interface issues, especially answer confirmation and submission logic	The final exam flow from the learner perspective was reviewed and all issues related to answer selection, confirmation, saving and final submission were corrected.
High	Consolidate fragmented PDFs and reduce unnecessary repetition	Some materials were merged to harmonise and avoid overlapping sections.
Medium	Improve platform navigation, login guidance, progress tracking, and PDF access	2 platform onboarding guides were developed, one for students and one for mentors, to facilitate platform use and onboarding
Low	Standardise terminology, spelling, translation, and wording consistency	A final language and consistency review across all platform pages, module materials, quizzes and instructions was performed to standardise cybersecurity terminology, module names, spelling, grammar, translations and formatting.

Better structure for dense modules: Several comments noted that modules are information rich. This is a quality strength, but the learning path should be more clearly structured for different audiences, especially SME employees with limited prior knowledge.

Platform and assessment flow: Comments mentioned navigation, login clarity, assessment flow, question design, "next" button placement and the need to avoid questions that appear to reveal answers.

More interactivity: Some respondents suggested more quizzes, peer activities, review tasks and interactive elements to make online learning more engaging.

Conclusions and recommendations

The piloting validates the CyberAgent training programme as a relevant and transferable upskilling programme for cybersecurity awareness, governance and practice in SME contexts. The evidence supports finalisation and wider use of the platform.

1. **The piloting achieved strong reach.** The piloting reached well above the application target of 80 attendees. The participants base covers the main target groups and includes many women.
2. **The training generated clear learning gains.** 89.3% of respondents stated that their cybersecurity knowledge increased. Confidence, motivation and practical skills indicators were also positive.
3. **The training content is strong.** 84.9% were satisfied or very satisfied with the content, and module ratings were consistently above 4/5 across the three rating thematics.
4. **The platform is functional but should be refined.** 77.2% were satisfied or very satisfied with the platform, but technical issues, navigation and assessment flow require targeted improvements.
5. **The programme has transfer potential.** 86.0% agreed or strongly agreed that the training could be adapted in other countries, supporting the project's European added-value logic.

Potential actions to be considered for the final exploitation

Recommendation	Possible action	Priority
Emphasise the differentiated learning paths	Provide clearer routes for SME employees, HEI students, VET students and managers. Keep the academic depth but add shorter "what this means for my SME" guidance.	High
Improve platform onboarding	Add a short start page explaining login, module selection, completion flow, communication tools and support options.	High
Strengthen interaction	If possible, add peer discussion prompts, optional peer review, short reflective activities and trainer follow-up guidance.	Medium

Improve accessibility and presentation	Review language consistency, subtitles, voiceovers and multilingual characters.	Medium
Monitor lower-scoring areas	Pay special attention to the indicator “I feel capable of contributing to cybersecurity improvements in an SME”, as these point to practical workplace transfer needs.	Medium

CONCLUSION

The CyberAgent piloting across Romania, Belgium, Norway, Spain, Türkiye, Poland, Lithuania and Finland showed that the platform and training materials were relevant for all three target groups: SME employees, HEI participants and VET participants. The strongest implementation results appeared where recruitment was supported by direct networks, where teachers or trainers actively guided participants, and where the platform was complemented by synchronous onboarding, consultation and follow-up.

The feedback survey results supports the conclusion that the CyberAgent upskilling training programme reached the foreseen indicators. It also provided concrete direction for fine-tuning the training modules, delivery approach and platform before wider exploitation.

The national pilots also confirmed the value of self-paced cybersecurity training, especially for learners balancing work, studies and other commitments. At the same time, the reports show that self-paced delivery requires structured support, regular reminders and clear onboarding to maintain engagement. The country reports also show that target groups use the platform differently: SME participants focus more on workplace relevance, governance and risk management, HEI students show interest in technical and analytical content and VET students benefit from practical, teacher-supported integration. This is one of the main lessons from the piloting. The programme should be strongly scaled with different training pathway. HEI, VET and SME contexts require different forms of recruitment, support and follow-up. HEI implementation should connect the modules to employability and professional development. VET implementation should use a more structured, teacher-supported and practical model. SME implementation should be shorter, more flexible and directly linked to workplace cybersecurity needs. These pathways should be connected through the Cyber Change Agent concept, where trained participants act as local multipliers of cybersecurity awareness in their study, training or workplace environments.

The reported learning outcomes were positive across the countries. Participants improved their cybersecurity awareness, confidence, practical knowledge and understanding of cybersecurity risks. Several reports also showed increased readiness to apply cybersecurity practices in academic, personal and workplace contexts.

The main improvement areas identified across the reports concern engagement continuity, workload of practical activities, clarity of technical requirements, platform onboarding, and additional support for more demanding modules. Shorter practical activities, clearer technical prerequisites and continued integration into HEI and VET teaching were identified as useful directions for future implementation. As well as reinforcing the importance of flexible learning pathways, clear module recommendations and practical SME-oriented examples for participants who do not have specialist cybersecurity roles.

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 Grupo

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

IT Akademija

ProxyLab

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau