Co-funded by the European Union

BOOST CAMP IN LITHUANIA FOR TRAINERS: CYBER SECURITY LECTURERS' WORKSHOP: 23-25 SEPTEMBER, 2025

CYBER AGENT 09.2025

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.

www.cyberagents.eu

Work Package 5:D: Boost CyberAgent Upskilling at local and regional level

Deliverable 5.2: Boost camp in Lithuania for trainers

Leader of WP5 – EVM, leader of deliverable 5.2 – IT Akademija

CONTENT

INTRODUCTION 2
1. BASIC INFORMATION FROM THE APPLICATION 2
2. RESPONSIBLE PARTNERS FOR THE BOOSTCAMP ACCORDING TO THE APPLICATION 3
3. AGENDA OF THE CYBERAGENT BOOSTCAMP 4
4. SUMMARIES OF PRESENTATIONS 14
5. EVALUATION OF RESULTS: 28
ANNEXES 33
ANNEX 1. EVALUATION TRAIN-THE-TRAINER FORM 33

INTRODUCTION

This document is designed to describe the training activities for train-the-trainer before the implementation of the CyberAgent pilot trainings:

- Description of the preparation stage for partners;
- Training implementation activities:
  - Training organization,
  - 3-day training program,
    - Skills and knowledge about cybersecurity and entrepreneurship,
    - Presentation of training materials,
    - Platform presentation and practical testing,
    - Pilot training organization strategy and evaluation (number and profile of participants; participants' selection process; tasks for participants),
    - Guidelines for trainers and participants,
    - Training impact measurement,
    - Submission of reports after the pilot training.

1. BASIC INFORMATION FROM THE APPLICATION

Details of the train-the-trainer bootcamp under the application, including what needs to be implemented.

The project application foresaw a 3-day "Train the Trainer Boostcamp" in Lithuania on September 23–25, which trained the trainers and piloted the final SME Cybersecurity Change Agents programme in collaboration with the developed local and regional networks. The event was organised in Kaunas and led by IT Akademija.

Three staff members from each partner organisation participated.

This Boostcamp resulted not only in a 3-day training but also in a Train the Trainer programme with an evaluation component. The training addressed the following areas: cybersecurity and entrepreneurship skills and knowledge, as well as guidance on how to organise pilot trainings.

The SME Cybersecurity Change Agents received updated and targeted training. To ensure a consistent training offer across all partner countries during the pilot, using all tools developed within the project, it was necessary to train the trainers. A Boostcamp for trainers was developed and conducted prior to the pilot. HEI and VET teachers, as well as other educators involved in the pilot, participated to become familiar with the training modules, enhance their motivation, and learn from each other.

Covered Topics:

- Presentation of HEI and VET curricula
- Overview of cybersecurity, including IT law and legal regulations on cybersecurity
- Case studies and practical examples
- Introduction to training modules and materials
- Use of the collaboration platform
- Digital pedagogical approaches
- Assessment methods, tools, and linking assessment to competences
- Customization of training based on participants' needs

CyberAgent Boostcamp Mobility Activity

The CyberAgent Boostcamp served as a mobility activity for trainers and trainees from all partner countries, consisting of an intensive 3-day training course. Participants had the opportunity to utilize the resources developed in WP3, WP4, and WP5, and engage in various learning activities broadcast through the platform, making them accessible to the HE and VET community across the EU. Participants from multiple European countries facilitated the transfer of skills and knowledge in cybersecurity through problem-based learning and case studies. Unlike many cybersecurity events in Europe, which typically adopt a technical focus and target larger enterprises with already educated staff, the Boostcamp addressed the needs of SMEs, providing practical skills and accessible solutions. The Boostcamp was a physical event with the option to attend remotely and represented a unique initiative, offering inspiration for similar events beyond the project's completion.

2. RESPONSIBLE PARTNERS FOR THE BOOSTCAMP ACCORDING TO THE APPLICATION

- D.5.2. Boostcamp in Lithuania for trainers. Partner IT Akademija. Organised a train-the-trainer boostcamp in Kaunas;
- D5.3. Olemisen. Performed CyberAgent upskilling training program evaluation;
- D5.4. EVM. Presented teaching methodology for SMEs Cyber Security Change Agents;
- T.5.3. EVM. Presented practical upskilling of SME Cyber Security Change Agents;
- All partners involved in training.

3. AGENDA OF THE CYBERAGENT BOOSTCAMP

Based on the information provided in the application, VU prepared a three-day training programme.

SMEs Cyber Security Change Agents / CyberAgent

Project number: 101111732

CYBERAGENT BOOSTCAMP AGENDA

23rd-25th of September 2025

23rd of September 2025

1st day, Meeting place V auditorium (II corpus), VU Kaunas faculty, Muitinės str. 8, Kaunas

MS Teams link: Boostcamp in Lithuania for trainers | „Microsoft Teams“

Time	Topic
10:00-10:30	**Welcome. Introduction to Cybersecurity and CyberAgent Project** ***Dr. Renata Danielienė**, Vilnius University, Lithuania*
10:30-11:00	**SME Cyber Security Change Agents Learning Pathways** *Vilnius University, Lithuania*
11:00-11:30	**HEI and VET Curriculum** ***Dr. Renata Danielienė**, Vilnius University, Lithuania*
11:30-11:45	**Coffee break in the basement (0 floor)**
11:45-12:45	**Dilemma of Cybersecurity Workforce: Models and Academia vs Industry and Real Needs and Expectations** ***Dr. Vilius Benetis**, Director at NRD Cyber Security, Lithuania (online)*
12:45-13:15	**Women Mentoring in the Tech Sector: Success Stories, Best Practices, and Experience** ***Tomas Lekavičius**, Partnerships Manager of WomenGoTech, Lithuania*
13:15-14:45	**Lunch**
14:45-15:15	**Digital Pedagogy in Adult Education** ***Assoc. Prof., Dr. Danguolė Rutkauskienė**, President of the National Association of Distance Education, Lithuania*
15:15-15:45	**Learning Across: Showcasing Our Journey and Best Practices for SMEs** ***Milda Savickaitė**, Infobalt, Innovation Policy Manager (online)*
15:45-16:15	**Academic Environment and Infrastructure** ***Dr. Renata Danielienė,** Vilnius University, Lithuania*
16:15-16:30	**Coffee break in the basement (0 floor)**
16:30-16:45	**Academic Environment and Infrastructure**

	Vilnius University, Lithuania
16:45-17:15	**Cybersecurity Challenges for VET Schools** *Liceul Tehnologic „Grigore C Moisil“, Romania*
17:15-18:00	**Follow-up, discussions, individual consultations** *All partners*
19:00	**Dinner**

CYBERAGENT BOOSTCAMP AGENDA

24th of September, 2025

2nd day, Meeting place V auditorium (II corpus), VU Kaunas faculty, Muitinės str. 8, Kaunas

MS Teams link: [Boostcamp in Lithuania for trainers | „Microsoft Teams“]

Time	Topic
10:00-10:30	**New Digital Tools with AI** *Liceul Tehnologic „Grigore C Moisil“, Romania*
10:30-11:00	**Legal Requirements for AI Cybersecurity** ***Assoc. Prof. Dr. Paulius Astromskis**, Vilnius University, Lithuania*
11:00-11:30	**M7. Risk Management and Mitigation** ***Assoc. Prof. Dr. Ilona Veitaitė**, Vilnius University, Lithuania*
11:30-11:45	**Coffee break in the basement (0 floor)**
11:45-13:15	**Introduction and Use of the Collaboration Platform** *Prios Kompetanse AS, Norway*
13:15-14:45	**Lunch**
14:45-15:15	**Practical sessions: Gamification Elements, Badges, and Certification. Assessment. Piloting One Module. Theory and Practice** *Prios Kompetanse AS, Norway*
15:15-15:30	**WP2 Training Needs Report Results** *ProxyLab Ry, Finland*
15:30-16:15	**The Strategy for Organising Pilot. Discussions, Feedback** *EVM Group SL, Spain*
16:15-16:30	**Coffee break in the basement (0 floor)**
16:30-17:00	**Measuring and Evaluating the Impact of Training Reporting After the Pilot Trainings** *ProxyLab Ry, Finland*
17:00-17:30	**M2. Systems Administration** ***Šarūnas Končius**, Lithuania*
17:45-18:00	**Follow-up. Discussions**
18:00-19:00	**Dinner**
19:15-21:00	**A Lithuanian Cultural Evening**

CYBERAGENT BOOSTCAMP AGENDA

25th of September, 2025

3rd day, Meeting place V auditorium (II corpus), VU Kaunas faculty, Muitinės str. 8, Kaunas

MS Teams link: [Boostcamp in Lithuania for trainers | „Microsoft Teams“]

Time	Topic
10:00-10:30	**M4. Security Operations** *ProxyLab Ry, Finland*
10:30-11:00	**M1. Security Program Management** *Ministry of National Education Milli Egitim Bakanligi, Turkey*
11:00-11:30	**M3. Analytical Tools** *Ministry of National Education Milli Egitim Bakanligi, Turkey*
11:30-11:45	**Coffee break in the basement (0 floor)**
11:45-12:15	**M5. Security Governance & Policy** *EVM Group SL, Spain*
12:15-12:45	**M6. Cybersecurity Planning** *Liceul Tehnologic „Grigore C Moisil“, Romania*
12:45-13:15	**M8. Business Continuity, Disaster Recovery, and Incident Management & Personnel Security** *Prios Kompetanse AS, Norway*
13:15-14:30	**Lunch**
14:30-15:00	**Additional Module** *Women4Cyber Mari Kert - Saint Aubyn Foundation Women4Cyber Foundation, Belgium*
15:00-15:15	**Active recruitment tactics for pilot training** *Women4Cyber Mari Kert - Saint Aubyn Foundation Women4Cyber Foundation, Belgium*
15:15-15:35	**Practical Workshop and Discussions “My First Pilot Training”** *Vilnius University, Lithuania* **With coffee in the basement (0 floor)**
15:35-17:25	**Exploring HEI: The Vilnius University Case** *Vilnius University, Lithuania*
17:25-17:40	**Certificates, Discussions, Follow-up.** *Vilnius University, Lithuania*
19:00	**Dinner**

The host of the meeting

Project Coordinator
Vilnius University Kaunas Faculty
Renata Danielienė
renata.danieliene@knf.vu.lt

Project administrator
Donatas Misiūnas,
donatas.misiunas@knf.vu.lt

SMEs Cyber Security Change Agents / CyberAgent. Project number: 101111732. www.cyberagents.eu
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.

OTHER USEFUL INFORMATION:

Lunch every day at the same time, 1:15-2:45 p.m., at the Daugirdas Hotel restaurant,
T. Daugirdo str. 4, Kaunas (based on your pre-selected meal).

Dinner:

23rd September at the restaurant "Medžiotojų užeiga" (Hunters' Inn).
Rotušės a. 10. Kaunas.

24th September at the Daugirdas Hotel restaurant,
T. Daugirdo str. 4, Kaunas (based on your pre-selected meal).

25th September at the Monte Pacis restaurant,
Tito Masiulio str. 31, T. Masiulio g. 31, Kaunas

More about guest speakers:

Information about lecturers:


CyberAgent
SPEAKERS OF CYBERAGENT BOOSTCAMP IN LITHUANIA
CYBER AGENT 2025
Call: ERASMUS-EDU-2022-PI-ALL-INNO
Programme: ERASMUS2027
Project ID. 101111732
Co-funded by the European Union
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.
www.cyberagent.eu

Guest Speakers of CyberAgent Boostcamp in Lithuania

Dr. Vilius Benetis, Director at NRD Cyber Security

The presentation would present the dilemma existing in cybersecurity skillsets - cybersecurity specialists on the market: what education organizations are delivering, and what are industry needs (and even if they do understand what they want?). In the presentation the roles and value from NIST NICE, FIRST CSIRT Competences and Skills model, as well as ENISA Cybersecurity Roles model will be referred and exemplified for practical situations from different European, USA and other countries contexts. Additionally, real examples of prominent cybersecurity company – NRD Cyber Security will be provided – whom we get to hire, and what we see in the market on reeducation efforts. Finally, presentation will include presentation of Lithuanian cybersecurity ecosystem – showing educational and community organisations, discussing their roles.

Dr. Vilius Benetis is cybersecurity capacity building expert, who leads a team of experts to consult, establish, and modernise CSIRT/SOCs for governments, organisations, and sectors in Africa, Asia, Europe, and Latin America.
He is an active contributor to the development of cybersecurity methodologies for ENISA, FIRST.org, GFCE and ITU. He is official global Ambassador of CIS Controls, and was Industry Cybersecurity Professor at KTU (2018-2023).

www.linkedin.com/in/viliusbenetis

CyberAgent Booscamp in Lithuania, 23-25 September 2025

Guest Speakers of CyberAgent Boostcamp in Lithuania

Tomas Lekavičius, Partnerships Manager of WomenGoTech

The Women Go Tech mission is to navigate women towards careers in tech. We're doing it by utilizing business professionals' mentoring sessions, providing tech content, events, and a multi-layer community. Started as a first mentorship program for women in Lithuania in 2017, we've expanded activities in the CEE region with a focus on Baltics, Poland, and Ukraine. Having positively impacted the lives of hundreds of women and cultivated a new generation of female role models in tech, our NGO has grown from a local project into a movement with significant influence across the region. We are also a long-term grantee of Google.org and winners at the "European Digital Skills Awards 2024".

www.linkedin.com/in/tomaslekavicius

Tomas Lekavičius dedicates part of his time to driving the partnerships and business development efforts in Women Go Tech, leading the NGO's collaboration with some of the biggest and fastest-growing companies in CEE. Shaping the Industry With Mentorship: Women Go Tech insights

- How Women Go Tech designed the mentorship program to accelerate women's careers in tech with expert guidance, career events, and a supportive community;
- Building the future power hub for women in tech: unlocking the potential of women in Central and Eastern Europe to bridge the tech skills gap and drive innovation. The findings reveal untapped potential to address Europe's ICT skills shortage, as the pandemic-driven digital transformation and advancements in generative AI create unprecedented opportunities for individuals without formal tech education;
- Tendencies, opportunities, and actions: from individual paths to ecosystem building.

CyberAgent Booscamp in Lithuania, 23-25 September 2025

Guest Speakers of CyberAgent Boostcamp in Lithuania

Milda Savickaitė, Infobalt, Innovation Policy Manager

This presentation introduces to the EDIH4LT and CyberHubs projects, highlighting effective practices, collaboration opportunities, and tailored support in the fields of digital innovation and cybersecurity.

www.linkedin.com/in/milda-savickaite

CyberAgent Booscamp in Lithuania, 23-25 September 2025

Guest Speakers of CyberAgent Boostcamp in Lithuania

Assoc. Prof., Dr. D. Rutkauskiene, President of the National Association of Distance Education

Dr. Danguolė Rutkauskienė serves as the President of the National Association of Distance Education. She is an expert in the field of digital education with a comprehensive research background.

Areas of Scientific Research

Dr. Rutkauskienė's primary research interests lie in the management of e-learning and Open and Distance Learning (ODL). Her work focuses on several key areas:

- She investigates the strategic implementation of e-learning methodologies and technologies to optimize educational outcomes.
- Her research includes the development of effective methodologies for creating computer-based learning modules.
- She also conducts sociological research to understand the social dynamics and effects of the computer-based learning process on students and educators.

www.linkedin.com/in/danguole-rutkauskiene-19185621/

CyberAgent Booscamp in Lithuania, 23-25 September 2025

Guest Speakers of CyberAgent Boostcamp in Lithuania

Šarūnas Končius

IT service management, IT strategy, and Microsoft technologies expert with more than 20 years of experience. Šarūnas Končius is an experienced IT consultant and lecturer with over two decades of expertise in Microsoft technologies and IT service management practices. He actively delivers training for various organizations, specializing in ITIL, Office 365, Microsoft Teams, and IT strategy, with the ability to effectively teach both IT professionals and business users.

Key Competencies

- Public speaking, presentations, and adult training
- IT service management based on ITIL and MOF practices
- IT strategy development, change management, communication
- Microsoft technologies implementation, support, and training

Work Experience

- Since 2018 – Independent IT Consultant (Microsoft solutions implementation, training, change management).
- Since 2008 – Independent ITIL Trainer (ITIL v3/2011 and ITIL 4 courses).
- 2008–2018 – IT Strategist, Microsoft Lithuania.
- 2003–2008 – IT Services and Consulting Specialist, Microsoft Baltics.
- 2001–2003 – Server Products Specialist, Microsoft Latvia.
- 1996–2001 – Lecturer and Deputy Director, Alna Training Center, Lithuania.

Education

- Kaunas University of Technology – Bachelor in Information Technology Engineering (1988–1993).

Certifications

- ITIL® 4 Specialist, ITIL Foundation
- Microsoft Certified Trainer, Microsoft Certified Systems Engineer
- Prosci® Change Management Practitioner
- CompTIA Certified Technical Trainer
- Multiple Microsoft technology certifications since 1995

www.linkedin.com/in/sarunask

CyberAgent Booscamp in Lithuania, 23-25 September 2025

4. SUMMARIES OF PRESENTATIONS

Welcome. Introduction to Cybersecurity and CyberAgent Project. Dr. Renata Danielienė

The CyberAgent project (Erasmus+ initiative, Project ID 101111732) is designed to build stronger cybersecurity capacity among small and medium-sized enterprises (SMEs) by training educators, lecturers, and business representatives to act as cybersecurity change agents. Funded by the European Union, the project brings together a wide consortium of partners, including business organizations, vocational education and training institutions, NGOs, and EU-level bodies.

During the Boost Camp in Lithuania (23–25 September 2025), trainers and lecturers gather to exchange best practices, strengthen their competencies, and explore innovative approaches for integrating cybersecurity knowledge into teaching and business training contexts. This workshop marks an important step in scaling up the project's impact by empowering multipliers who will pass on cybersecurity skills to wider communities.

So far, the project has:

- Reached over 160,000 people through awareness-raising and communication activities.
- Produced more than 10 official deliverables, openly available on the **project website**.
- Organized and participated in 30+ events across Europe to disseminate results and engage stakeholders.
- Attracted a growing online community with 680+ followers.

The presentation also outlines the project's work packages (WP1–WP6), covering areas such as needs analysis, training program design, pilot implementation, dissemination, and sustainability. The upcoming October 2025 workshop will continue this momentum, fostering collaboration between academia, industry, and policy actors.

In summary, the CyberAgent project is shaping a new generation of cybersecurity educators and practitioners, helping SMEs strengthen resilience against digital threats through knowledge, skills, and active change leadership.

SME Cyber Security Change Agents Learning Pathways, *Jorė Bendinskaitė*

The presentation introduces the CyberAgent learning and career pathways developed for cybersecurity education in both higher education (HEI) and vocational education and training (VET). The study pathway covers key modules such as risk management, security programme management, analytical tools, systems administration, security governance, business continuity, and security operations. While both HEI and VET address the same themes, they differ in depth and credit allocation.

The career pathway highlights four competence categories: technical skills, analytical skills, risk management, and organizational skills. To support these pathways, diverse teaching methods are applied, including lectures, practical hands-on training, collaborative and peer learning, technology-enhanced learning, and community engagement. Modules are delivered in various formats: remote, synchronous, asynchronous, blended, and self-learning.

Drawing on international projects (CyberPhish, FuseIT, dComFra) and commercial platforms (Udemy, Coursera), the CyberAgent project has designed a typical module structure applicable to both HEI and VET. This structure includes clear goals, outcomes, teaching methods, assessments, and resources, ensuring flexibility and relevance in cybersecurity education.

In summary, the CyberAgent pathways aim to equip learners at different levels with structured, adaptable, and career-oriented cybersecurity training, empowering them to become effective professionals and change agents in the digital security field.

HEI and VET Curriculum, *Dr. Renata Danielienė*

Dr. Renata Danielienė's presentation from Vilnius University details the "Cyber Agent" project's (funded by the European Union) Higher Education Institution (HEI) and Vocational Education and Training (VET) curriculum. The main goal of the project is to train SME employees, with the aim of turning them into Cyber Security Change Agents.

The program consists of 9 modules and is closely integrated with the European Qualifications Framework (EQF), offering two distinct learning pathways:

- EQF Level 4–5 (called the "Gateway Pathway"): This path is intended for SME employees without an HEI or VET background. It provides foundational cybersecurity skills with light specialization.
- EQF Level 5–6: This trajectory targets SME employees with adequate background and HEI students. It features advanced and complex training activities with deeper specialization.

The creation period for the training materials, which include presentations, Word documents, videos, and self-assessment and knowledge verification tests, runs from June 1, 2024, to September 30, 2025. All modules will be available and localized into 8 languages (EN, LT, PL, ES, NO, TR, FR, FI, RO).

Knowledge is assessed through a two-stage system that encourages deep learning:

- Self-Assessment Tests: 3–5 questions after each topic. Unlimited attempts are allowed, and immediate feedback reinforces learning.
- Knowledge Assessment Test: A comprehensive 36-question test, which is allotted 45 minutes and allows only one attempt. A minimum score of 75% of correct answers is required for certification.

The program's delivery is flexible, offering three main methods: Blended Learning (2–4 month programs combining face-to-face sessions with online consultations), Online Self-Paced Learning (with no set deadline, allowing professionals to balance it with work), and Corporate Training (customized programs for larger companies).

Dilemma of Cybersecurity Workforce: Models and Academia vs Industry and Real Needs and Expectations, *Dr. Vilius Benetis*

The presenter's message was that their presentation, "Dilemma of cybersecurity workforce: models and academia vs industry and real needs and expectations," was dedicated to the detailed analysis of the gap between formal cybersecurity specialist training and real industry expectations. The speaker aimed to emphasize that the company they represent specializes in cybersecurity operations build-out, incident detection, handling, and enhancing cyber capacity for organizations and nations. They stressed the necessity of establishing and modernizing Computer Security Incident Response Teams (CSIRTs) and Security Operation Centres (SOCs), advocating for the application of the SIM3 and SOC-CMM models for modernization, and the Oxford CMM model for national capacity building.

During the presentation, international frameworks dedicated to defining competencies and roles were thoroughly discussed, with the goal of aligning them with industry needs. Among these, the ENISA ECSF (European Cybersecurity Skills Framework) was mentioned, which classifies 12 core profiles and particularly details the mission of the Cyber Incident Responder (monitoring status, managing incidents, restoring systems according to the Incident Response Plan). Also discussed were the NIST NICE Framework, which categorizes functions into 7 areas (e.g., Oversight and Governance, Protection and Defense, Investigation), and the FIRST.org CSIRT Services Framework, which describes roles in Incident Management, Vulnerability Management, and Situational Awareness, specifying tasks such as root cause determination and artifact analysis.

In conclusion, the speaker raised essential questions reflecting the dilemma between academia and industry, such as: "What is the industry interested in getting from universities?", "Can Cybersecurity be a profession?", and "What certificates to choose for incident handling specialization?". The presentation also included and discussed a map of the Lithuanian cybersecurity ecosystem.

Women Mentoring in the Tech Sector: Success Stories, Best Practices, and Experience, *Tomas Lekavičius*

The presentation by Tomas Lekavičius discusses the mission of Women Go Tech: to guide women toward careers in the technology sector across the Central and Eastern European region, particularly the Baltics, Poland, and Ukraine. We accomplish this by utilizing mentorship sessions from business professionals, providing tech content, hosting events, and fostering a multi-layered community.

The organization started in 2017 as the first mentorship program for women in Lithuania and has now grown into a community of over 70,000 women and over 700 mentors. Our efforts have been highly recognized: we won the European Digital Skills Award 2024 in the "Women in ICT Careers" category and were the first NGO in the Baltics to receive significant funding from Google.org for expansion across Europe.

Our programs include the AI Foundations Program (with over 40,000 registered users) and our flagship, six-month Mentorship Program ("Acceleration"). This program helps women accelerate their careers in the IT sector by offering specialized tracks, including Software Development, Product Thinking, Data Science, and Cyber Security (covering Administrator and Analyst roles).

Research conducted in collaboration with Stanford University confirms the effectiveness of our programs: mentorship participants achieve an approximately 50% higher job placement rate in technology compared to control groups. Furthermore, we've identified that the main motivators for women choosing ICT are better pay (78%), career growth, and work-life balance. The biggest obstacles women face are ageism, stereotypes, rigid workplaces, and bias against alternative education pathways. Therefore, we urge policymakers to invest in reskilling programs and promote pay transparency, and businesses to implement structured mentorship and value alternative learning methods.

Learning Across: Showcasing Our Journey and Best Practices for SMEs, Milda Savickaitė

The presenter's message was that her presentation, titled "CyberHub Lithuania: Learning Opportunities," was dedicated to introducing the Lithuanian cybersecurity ecosystem and the opportunities it provides for education, collaboration, and professional development. The presenter presented that "CyberHub Lithuania" is a platform that connects academia, industry, and the public sector with the aim of strengthening the country's cybersecurity competencies. The platform offers various learning opportunities, including practical training, seminars, certification programs, and collaborative projects. The main focus of the presentation was to foster cooperation between universities, vocational training institutions, and companies to ensure that training content meets real industry needs and guarantees that specialists are prepared to tackle contemporary cybersecurity challenges.

Cybersecurity Challenges for VET Schools, *Adriana Iuliana Voicu*

The presentation addresses the critical need to integrate cybersecurity into Vocational Education and Training (VET) schools, emphasizing that education is the first line of defense against cybercrime, as over 60% of cyber attacks target poorly prepared educational institutions and individual users. VET schools, which train future professionals in key technical sectors (e.g., IT, mechanics, industry), must equip students not only with technical skills but also with fundamental knowledge of data protection and cyber risks, especially since students are exposed to cyber risks daily through technology and during company internships.

VET schools face major challenges grouped into several categories. These include a lack of cybersecurity culture (low awareness, security seen as solely an IT responsibility), incomplete or outdated curriculum (superficial treatment of digital security topics, lack of interactive resources), and outdated or vulnerable technical infrastructure (poorly secured networks, outdated devices, lack of control over access). Additional challenges stem from insufficient teacher training in IT security and the risky use of online media and social networks by students who lack good data protection practices. Student exposure during internships also poses a risk of security breaches due to a lack of clear protocols between the school and employers.

To address these issues, VET schools have several key needs: mandatory integration of cybersecurity into all specializations and alignment of curricula with European standards (like DigCompEdu); establishing partnerships with IT companies and specialized organizations for training and mentoring; providing practical and experiential activities for students, such as attack simulations and competitions; and maintaining secure and modernized digital infrastructure with updated equipment and clear user management policies.

The presentation recommends concrete actions, including using modern teaching methods like attack simulations and virtual laboratories, establishing continuous training of teachers (and creating digital security ambassador networks), developing clear Internal Regulations for technology use, and implementing a cyber incident response plan at the school level. Ultimately, the document calls for the development of a national strategy for digital security in vocational education in partnership with all stakeholders to transform VET schools into safe, modern environments.

Digital Pedagogy in Adult Education, Assoc. Prof., Dr. Danguolė Rutkauskienė

The presenter said that her presentation, "Digital Pedagogy," focused on the critical role of digital competence for educators in the evolving landscape of teaching and learning. The presenter stated that mastering digital pedagogy is essential for teachers to effectively use digital tools and resources to design engaging, innovative, and inclusive learning experiences. The presenter presented that this includes the need for educators to possess a strong synthesis of technological, pedagogical, and content knowledge (known as TPACK) so they can meaningfully integrate technology into their subjects.

The presenter emphasized that digital tools allow for a shift from traditional, passive learning models to more active, hands-on, and collaborative methods. The presenter also presented how technology supports flexible learning environments, such as blended and online learning, which enables personalized learning paths and continuous progress monitoring. Essentially, the presenter conveyed the message that digital pedagogy is the essential framework needed to guide teachers in transforming their teaching practices to meet the demands of the 21st-century digital society.

New Digital Tools with AI, *Carmen Daniela Macadon*

The presenter's message was that her presentation focused on integrating powerful AI-driven digital tools into content creation and educational workflows to enhance creativity, boost engagement, and streamline collaboration without requiring specialist technical skills. She highlighted four primary tools: Gamma AI, Invideo AI, Magic School AI Innovator, and Learning Apps.

The presenter introduced Gamma AI as an AI-powered platform designed for the instant creation of polished presentations, documents, and websites from basic ideas or existing text. She explained that it automatically generates visually balanced layouts and allows users to easily embed rich media, proving useful for educators to create engaging lessons rapidly and for businesses to produce materials with analytics. Invideo AI was presented as an intuitive platform for easy video creation, enabling users to quickly produce professional marketing and educational videos by converting text to video, adding voiceovers, and optimizing the output for various social media platforms.

Magic School AI Innovator was described as a comprehensive AI platform built specifically by and for educators, offering over 80 AI-powered tools to automate routine tasks and enable educators to "teach smarter, not harder." She noted that it supports key workflows, including Lesson Planning (creating rubrics and individualized education programs), Assessment (customizing quizzes and surveys), and Communication (generating professional emails and newsletters), all while ensuring safe AI experiences for students. Finally, Learning Apps (LearningApps.org) was highlighted as a tool for enhancing education through interactive learning and gamification, allowing for personalized experiences and providing progress tracking insights through custom educational activities accessible across multiple devices.

The presenter emphasized that integrating these tools offers significant practical benefits, including an average 70% time saved on content creation, a three-fold increase in engagement due to multimedia elements, and a reported 85% improvement in perceived output quality. Furthermore, these tools offer seamless integration with established educational ecosystems like Google Classroom, Canvas, Schoology, and Microsoft Office.

Legal Requirements for AI Cybersecurity, *Assoc. Prof. Dr. Paulius Astromskis*

The presentation addresses the legal requirements for AI cybersecurity, focusing on the EU AI Act and its risk management dimensions. The EU AI Act classifies AI systems based on risk, ranging from Unacceptable risk (e.g., AI employing subliminal techniques to distort behaviour) down to Minimal risk (e.g., spam filters and recommender systems). Systems classified as High-risk—such as those used in medical devices, education, immigration, and law—are subject to stringent compliance requirements, including mandatory conformity assessments, transparency, and post-market surveillance.

A central requirement for High-risk AI systems is ensuring accuracy, robustness, and cybersecurity throughout their lifecycle, as detailed in Article 15 of the AI Act. This requires technical solutions appropriate to the relevant circumstances and risks. Measures must be included to prevent, detect, respond to, and control attacks that try to manipulate the training data set (data poisoning), manipulate pre-trained components (model poisoning), or use adversarial examples to cause the AI model to make a mistake (model evasion). Securing these systems requires an integrated and continuous approach using proven practices and AI-specific controls, which necessitates a security risk assessment.

The presentation emphasizes the importance of a formalized Risk Management System for AI, referencing international standards like ISO 31000 (Risk management) and ISO/IEC 23894 (Guidance on risk management for AI). This process involves risk identification, which includes classifying assets into "Crown jewels" (critical business objectives) and "Stepping stones" (resources attackers leverage to pivot across networks). The document also outlines AI threat categories (including eavesdropping/hijacking, data poisoning, and physical attacks) and standard control families (such as Access Control, Incident Response, and System Security) from frameworks like NIST SP 800-53 Rev. 5 and ISO/IEC 27002. Finally, the presentation notes that High-risk AI systems certified under a cybersecurity scheme pursuant to the EU Cybersecurity Act (Regulation (EU) 2019/881) are presumed to comply with the cybersecurity requirements of the AI Act.

M7. Risk Management and Mitigation, *Assoc. Prof. Dr. Ilona Veitaitė*

The presenter's message was that their presentation, "Risk Management and Mitigation," focused on outlining a module designed to equip students with the necessary skills to continuously manage cybersecurity risks in ICT infrastructures, systems, and services. The core purpose is to enable students to effectively plan, apply, report, and communicate comprehensive risk analysis, assessment, estimation, and mitigation processes. Upon completion, students are expected to gain an advanced understanding of risk management, apply advanced methods and tools to assess risks, design management strategies, and ultimately develop and execute strategic cybersecurity policies tailored for SME workplaces in line with established standards.

The module content delves into key topics including Risk Assessment, Risk Identification, Insider Threats, Risk Measurement and Evaluation Models and Methodologies, and Risk Control. Risk Assessment differentiates between Quantitative assessments (focused on financial impacts) and Qualitative assessments (focused on human and productivity aspects). Risk Identification covers defining the scope, external and internal context, and analyzing both tangible and intangible sources of risk, including threats, opportunities, and vulnerabilities.

A significant portion of the module is dedicated to Insider Threats, covering their definition, types, costs, and the steps involved in building a mitigation program. Risk Measurement topics introduce the Capability Maturity Model Integration (CMMI) framework for risk management, which progresses through five maturity levels. Finally, Risk Control focuses on identifying and selecting risk treatment options, preparing and implementing plans, and assessing the effectiveness of these controls. Controls are categorized as people, physical, technological, or organisational.

Assessment for the module uses both Self-assessment tests and a final Knowledge assessment test. Required reading materials include resources on compliance standards and relevant directives such as the NIS 2 Directive.

Introduction and Use of the Collaboration Platform, *Jo Sakaraissen*

The intensive, hands-on workshop is designed to familiarize cyber security lecturers and trainers with the CyberAgent collaboration platform, which is dedicated to learning how to safeguard businesses against cyber threats. The core purpose of the session is for participants to collaboratively determine how the platform can be useful in their specific contexts and achieve the project's goal of making an impact.

The workshop uses a three-perspective approach, having participants experience the platform in rotating roles: as an Admin (managing users and platform configuration), a Content Contributor (creating blogs, organizing events, and sharing knowledge), and a Student (completing courses, earning badges, and exploring learning features). Participants work in country-based groups, with each group initially assigning these roles.

The workshop structure involves a Platform Walkthrough of admin and student views, followed by Group Work and Tool Exploration (using blogs, messages, and feedback systems). This is succeeded by a Reflect & Discuss session and Implementation Planning to develop strategies for using the tools with learners. The practical session includes specific tasks for each role: Admins set up accounts and courses and schedule events; Content Contributors publish blog posts and send event invitations; and Students complete self-assessment and knowledge assessment quizzes for a module. A rotation strategy is employed to ensure all participants gain a comprehensive understanding of the system's functionality from multiple user perspectives. The final debrief session focuses on documenting observations, comparing role experiences, collecting suggestions for improvement, and presenting findings on usability, functionality, and user experience.

WP2 Training Needs Report Results, *Karim Bechlem*

The presenter's message was that their presentation focused on the WP2 Training Needs Report, which analyzed and mapped the necessary competencies for an SME Cyber Security Change Agent. The core objective was to bridge the critical gap between current educational offerings and the practical cybersecurity skills required by small and medium-sized enterprises, driven by the increasing sophistication of cyber threats. The research utilized a mixed methodology, combining Desk Research (analyzing VET and HEI curricula) and Field Research (surveying over 360 educators and SME employees across eight EU countries).

A major finding highlighted was the significant Gender Gap Crisis, noting that only 18.5% of EU ICT specialists are women, with 87% of women reporting unconscious bias in the workplace. Regarding training, while current programs often cover Cybersecurity Fundamentals and Network Security, the primary identified skills deficits in the industry are Cloud Security expertise, threat detection and response, and incident response and recovery. Furthermore, the top gaps in the system are a low level of threat awareness and insufficient regular training, particularly concerning the top threats identified by SMEs: Phishing and social engineering, AI-driven attacks, and Ransomware. It was also noted that 66% of SMEs do not use external services for cybersecurity tasks.

The presenter concluded with Key Recommendations for Change, advocating for the development of tailored training that balances technical and human-centric aspects, the establishment of mentorship networks, the promotion of women into leadership positions to serve as role models, and the implementation of inclusive hiring practices. The resulting qualification profile for the change agent was defined at two levels: EQF 4/5 (focused on fundamentals and basic risk management) and EQF 6 (focused on advanced concepts, security architecture expertise, and strategic leadership).

The Strategy for Organising Pilot. Discussions, Feedback, *Adelina Luntraru Mihai*

The presenter's message was that her presentation, "EVM Piloting trainings," focused on the practical upskilling and piloting objectives for the SME Cyber Security Change Agents training. The primary goals the presenter highlighted were: to assess the effectiveness and quality of the CyberAgent cybersecurity modules and platform designed for specialists from SMEs and students from HEIs and VET providers. A second, equally important goal was to create SME Cyber Security Change Agents by upskilling at least 240 individuals (SME employees, HEI, and VET students) in cybersecurity across all partner countries during the first year. Ultimately, the presenter aimed to ensure a knowledgeable workforce prepared to address current and future cybersecurity challenges in the SME sector.

The presenter emphasized the preparation phase, which includes reviewing the piloting and evaluation plans, identifying stakeholders, and translating and validating project documents (like contracts and content). The concept of the project-formed "CyberAgent" SME network becoming a basis for future activities was raised, inviting members to participate in the curriculum piloting to strengthen their cybersecurity capacities. Maximizing the impact and reaching targets, particularly for women's upskilling, is crucial, so partners need to consider expanding the network to include female-employed SMEs, universities, and VET providers.

The schedule the presenter outlined projects that stakeholder identification and participant selection will occur from October to December 2025, and training material preparation in December 2025. The trainings, which include supervised consultation, will be implemented from January to April 2026. Expected outcomes involve 80 HEI students, 80 VET students, and 80 SME employees (with a minimum of 30 being women) participating across all 8 countries, completing at least 30 training hours per country, with a target of at least an 80% satisfaction level.

Measuring and Evaluating the Impact of Training, Reporting After the Pilot Trainings, *Karim Bechlem*

The presenter's message was that their presentation, "WP5 CyberAgent upskilling Training Program Evaluation," focused entirely on the detailed methodology for measuring and evaluating the impact of the pilot cybersecurity training. The evaluation, scheduled for April 2026, is designed to assess four main objectives: the quality of the developed training modules, the relevancy of the learning outcomes, the reliability of the training schemes and certification process, and the effectiveness of the collaboration between educational institutions and SMEs.

The presenter detailed the structure of the evaluation survey, which will be administered to VET students, HEI students, and SME employees. The survey is comprehensive, utilizing a Likert scale (1 to 5) and open-ended questions across multiple sections. Key areas of inquiry include: Training Modules (clarity, practicality, relevance to real needs), Learning Outcomes (achievement and skill improvement), Reliability (structure of the scheme, fairness of assessment, certification clarity), Collaboration (added value, integration of academic and practical needs), and Impact (increased confidence, ability to apply knowledge in daily work, and positive career impact).

All evaluation data will be collected through multi-language digital forms and stored on the project's central repository. Project success will be measured by various indicators, including the number of trained participants, platform interactions, and statistics on module completion. The final output will be a 20-page Evaluation Report with comparative analysis. Finally, the presenter raised a crucial question for the group: whether to go further for impact measurement by implementing pre- and post-training tests.

M2. Systems Administration, *Šarūnas Končius*

The presenter's message was that their presentation, "M2 Systems Administration: Training Overview," focused on outlining the structure, content, and recommended improvements for the Systems Administration training module within the CyberAgent program. The presenter detailed that the module requires no prerequisites and allocates 5 ECTS credits (with 48 contact hours and 77 individual work hours). Its main purpose is to enable students to continuously manage, analyze, assess, estimate, and mitigate cybersecurity-related risks in ICT infrastructures, systems, and services. Upon completion, students will know networking fundamentals, how to operate on and secure Linux and Windows servers, and how to utilize knowledge of Cloud and AI to speed up tasks and perform automations.

The presenter presented that the module's content is divided into seven topics, including Operating System Administration, Database System Administration, Network Administration, Cloud Administration, Cyber-physical System Administration, System Hardening, and Availability. The presenter analyzed that the content generally ranges from Beginner to Intermediate-Advanced and is largely beginner-friendly with adequate support. The current resources include over 1,200 slides across the seven parts.

The presenter noted several strengths, including the comprehensive and well-structured program, the professional tone, the planned use of virtual machines for practice, and the inclusion of self-assessment quizzes. However, the presenter highlighted key areas requiring additional attention, such as improving the objectives for some learning topics, correcting the order of some materials, and needing better step-by-step documentation for hands-on labs. The presenter also recommended correcting the title of the last part from "7. Availability" to "7. Security Operations and Incident Response" to better reflect the subject matter. Recommendations for improvement included creating additional English-only documentation, testing all hands-on labs before delivery, encouraging trainers to share tips, and providing a virtual machine to give a more realistic experience with SIEM, alerts, and incidents.

M4. Security Operations, *Karim Bechlem*

The presenter's message was that their presentation, "Module 4 – Security Operations," focused on outlining the structure and learning goals for the Security Operations training module. After completing the module, the presenter stated that students and trainees will be able to effectively manage security operations within ICT infrastructures, systems, and services. Furthermore, they will gain the skills to monitor, detect, and respond to cybersecurity incidents by applying best practices, tools, and relevant frameworks.

The presenter presented that the module content is broken down into four key units:

1. Security Operations Fundamentals: This unit covers the basics of Security Operations and the Security Operations Centre (SOC), including roles and responsibilities, and an explanation of key SOC tools such as SIEM, EDR, XDR, MDR, and SOAR.

2. Security Convergence: This section explores understanding security convergence, the fundamentals of physical security, and includes case studies highlighting convergence issues.
3. Security Information and Events Management (SIEM): This unit focuses on reviewing security monitoring principles, implementing SIEM solutions, and setting up logs and alerts.
4. Security Operations Practices: This final unit addresses identifying data sources and optimizing log collection, centralizing alerts with the SIEM, and testing the SIEM.

The presenter provided examples of practical lab work to be included, such as simulating an attack using a Living Off the Land Binary (LOLBIN) tool like MpCmdRun.exe to test a system's defense against disabling the antivirus, simulating a privilege escalation attack using Mimikatz to test for detection, and running a detection test on a Linux server to ensure SQL injection attempts reach the SIEM.

The presenter emphasized the context of why Security Operations are needed: the necessity for continuous, proactive defense, and the importance of business continuity, intellectual property, and reputational protection.

M1. Security Program Management. M3. Analytical Tools. *Cİhan Uysa*

The presenter's message was that their presentation, "M1: Security Program Management" and "M3: Analytical Tools," focused on outlining the structure and objectives of two integrated cybersecurity modules designed to equip trainees with management and data analysis skills.

The presenter stated that the Security Program Management (M1) module aims to teach participants how to design and manage cybersecurity programs, apply metrics, manage quality and resources, and assess and report threats correctly. The module content covers four core areas: Project Management (defining scope, scheduling, current threats, and incident response plans), Resource Management (human resources, inventory management, effective use of technological resources, and budget allocation), Security Metrics (measurement techniques, data collection with SIEM, project monitoring), and Quality Assurance and Control (quality standards, compliance audits, and testing techniques). This module includes over 10 scenario-based tasks and 18 self-assessment questions alongside 144 knowledge questions.

The presenter then introduced the Analytical Tools (M3) module, which focuses on teaching participants how to apply metrics and analytics to protect assets and identify risks. The content covers Performance Measurements (metrics), Data Analytics (data collection, cleaning, visualization, and application in cybersecurity), and Security Intelligence (sources, threat intelligence collection methods and frameworks, and AI-driven platforms). This module includes 8 scenario-based tasks and 18 self-assessment questions with 150 knowledge questions.

Overall, the modules emphasize the combined tactical and strategic knowledge required to manage modern cybersecurity programs effectively through measurement, planning, and intelligence.

M5. Security Governance & Policy, *Adelina Luntraru Mihai*

The presenter's message was that their presentation, "Security Governance & Policy," focused on outlining the objectives and comprehensive content of a training module designed to prepare learners to face cybersecurity challenges in SMEs. The presenter stated that the module's core objective is integrating security governance into business strategy and ensuring compliance with legal regulations, such as the GDPR. The module, which awards 3 ECTS credits and requires 75 hours of live training and 50 hours of individual study, is available in multiple languages.

The presenter presented that the module enhances skills in identifying threats, designing robust policies, managing incidents effectively, and developing governance structures that assign clear organizational roles. The content is broken down into five key chapters:

1. Organizational Context: This covers the evolution of cybersecurity in SMEs, major threats, and the specific challenges of SMEs versus large enterprises, such as limited budgets and staffing.
2. Privacy: This section addresses privacy principles in cybersecurity, Personal Data Protection and GDPR, and the impact of privacy on SME operations.
3. Laws, Ethics, and Compliance: This unit explores relevant national and international legislation, regulatory compliance in SMEs, cybersecurity ethics, and the legal consequences of non-compliance. It also analyzes how AI-based tools can strengthen governance through automated monitoring.
4. Security Governance: The content focuses on the governance structure, roles and responsibilities in security management, cybersecurity maturity models, and enhancing abilities in conducting risk assessments and strategic response plans under simulated crisis conditions.
5. Managerial Policy: This final chapter covers the development, implementation, monitoring, and continuous improvement of security policies, including adapting them to technological and regulatory changes.

The presenter noted that the module enhances skills in crisis management and decision-making in high-stress scenarios involving AI-driven attacks and ransomware.

M8. Business Continuity, Disaster Recovery, and Incident Management & Personnel Security, *Jo Sakaraissen*

The presenter's message was that their presentation, "Module 8: Business Continuity, Disaster Recovery, and Incident Management," focused on a highly practical training module designed to keep small and medium-sized enterprises (SMEs) operational even when facing unexpected events. The presenter emphasized that the goal is to equip learners with the skills and competences to protect organizational assets, reduce downtime, and limit crises by having clear procedures.

The presenter presented that the module is structured into eight essential subtopics:

1. Incident Response: This covers developing a plan, identifying roles, defining severity levels, and implementing steps for response and recovery.
2. Disaster Recovery: This focuses on understanding disaster recovery and developing a formal Disaster Recovery Plan (DRP), including recovery steps.
3. Business Continuity: This involves creating a Business Continuity Plan (BCP), assigning roles, and conducting a Business Impact Analysis (BIA) to prioritize critical functions.
4. Security Awareness and Training: This addresses developing effective training programs and measuring their impact.
5. Secure Hiring and Termination Practices: This covers defining security requirements for roles, conducting background checks, and ensuring immediate access revocation upon termination.
6. Third-Party Security: This unit addresses assessing vendor risk, due diligence in selection, and establishing contractual security requirements.
7. Security Audits and Reviews: This focuses on incorporating security into regular review processes, including audits and post-incident reviews.
8. Employee Data Privacy: This final topic covers data collection limitations, storage and access controls, and compliance with privacy regulations.

The presenter noted that each of the eight subtopics is designed with a consistent structure that ensures both theoretical knowledge and practical application, featuring explanatory text, presentations, and short, applied exercises.

5. EVALUATION OF RESULTS:

The International Boostcamp attracted significant interest and exceeded the planned number of participants. In total, 34 individuals attended the event.

The participant structure was as follows:

- 26 target group participants:
  - 9 Higher Education Institution (HEI) teachers;
  - 7 Vocational Education and Training (VET) teachers;
  - 10 Small and Medium-sized Enterprise (SME) representatives.
- 6 guest speakers who delivered presentations (3 attended in person, 3 joined online).
- 2 project administrators from the host organization.

Following the training, a participant survey was conducted to evaluate the program's effectiveness and impact. A total of 23 completed evaluation forms were collected. Guest speakers and a few target group participants did not complete the survey as they did not attend the entire three-day program. The 23 responses from the 26 core participants represent an 88% response rate, which is considered a very high result, indicating strong participant engagement and interest in the project's activities.

This evaluation was aimed at assessing the effectiveness and impact of the program, providing valuable insights into participant satisfaction, learning outcomes, and areas that could be improved. The feedback helps organizers better tailor the content and format of future events to meet real participant needs.

Most Useful Sessions and Topics

Participants found the greatest benefit in the following areas, which were mentioned most frequently:

- Artificial Intelligence (AI) and Cybersecurity: Sessions related to these topics were mentioned 5 times, including legal requirements and relevant, insightful content.
- Women in the Tech Sector (W4C): Sessions dedicated to women's inclusion and mentoring (e.g., "Women Mentoring in the Tech Sector by WomenGoTech," W4C module) received significant attention, mentioned 5 times in total. This content was rated as particularly relevant, expanding the partnership network, and providing examples of good practices.
- Practical Work and Platform: Aspects related to the project platform, such as platform testing, practical workshops, and piloting strategies, were mentioned 6 times. This indicates a high level of interest in the direct practical application of the project implementation and training materials.
- Specific Modules and Lecturers: M4 (Security Operations/SOC analysts) was mentioned 2 times as particularly useful. Participants also positively evaluated sessions by external lecturers and speakers, noting that they received many good ideas for new cooperation.

Least Useful Sessions and Reasons

Given that a large proportion of respondents indicated that all sessions were useful (or none were less useful), the total number of negative feedback comments is very low.

- General Overviews: One group of responses indicated that a general overview of all modules was less useful, especially if the participant was already familiar with them.
- Specific Mentions: Modules M3 and M6 were each mentioned 1 time as less useful. There was also feedback that the content of "Cybersecurity Challenges for VET Schools" was not engaging enough.

Suggestions for Future Seminars

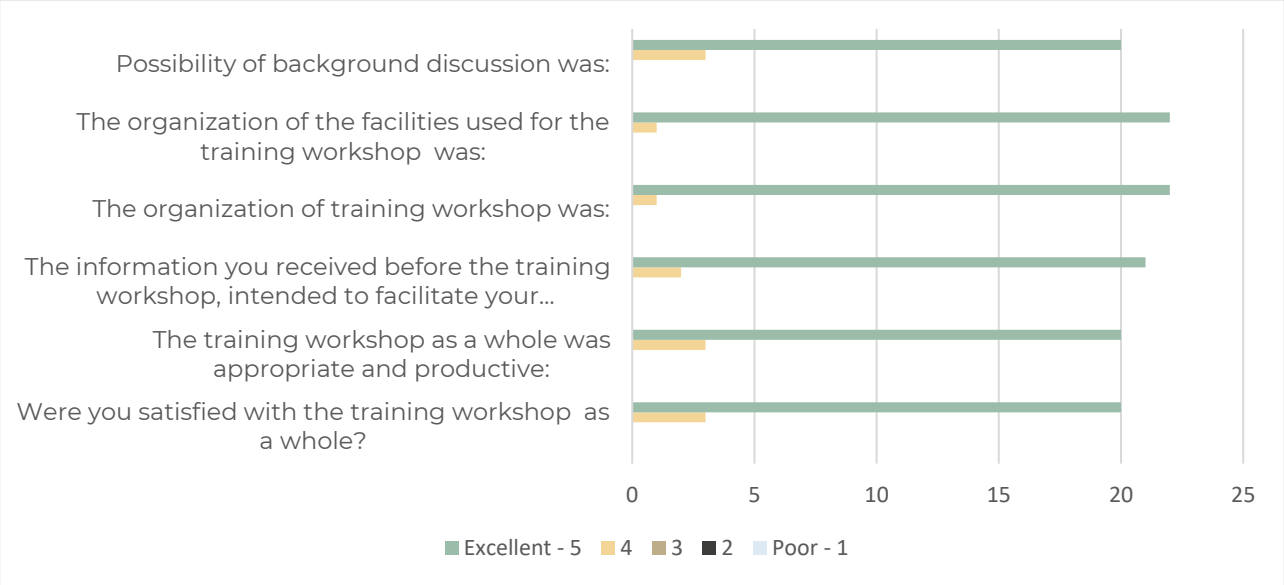
Although one participant emphasized that no changes were necessary ("No suggestion, just follow the Lithuanian example"), others provided constructive suggestions, dominated by requests for practical content:

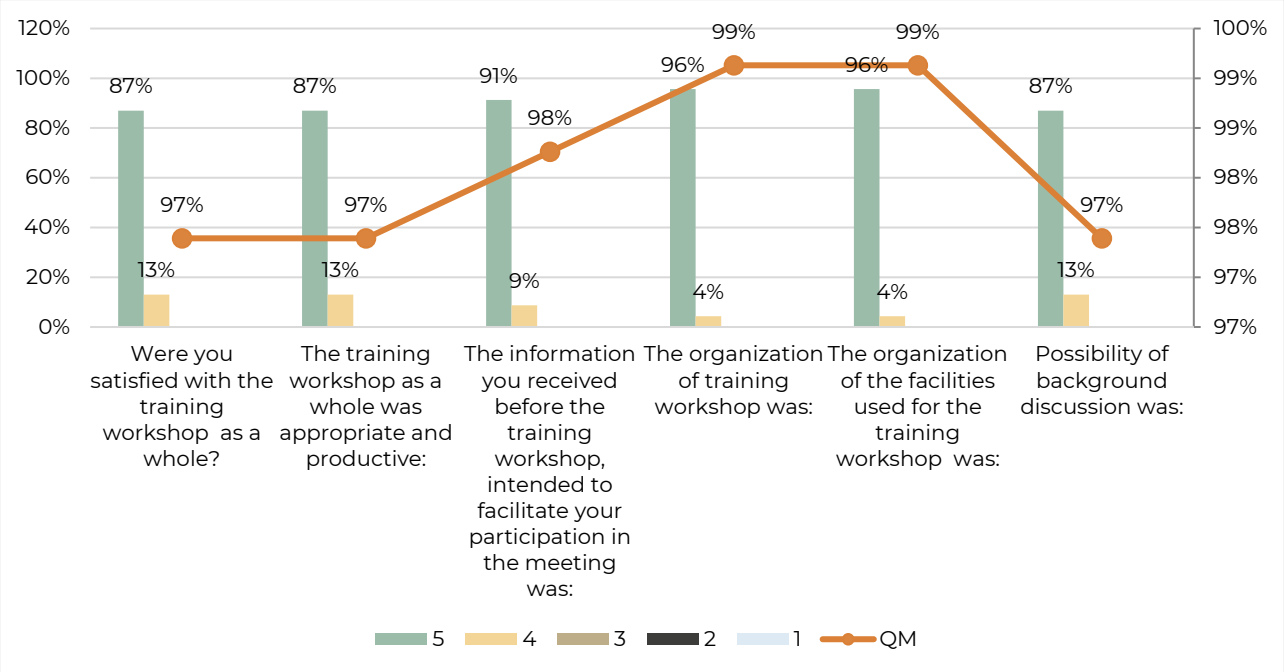
- More Practical Activities: The most frequently noted suggestion is the development of more original "hands-on" activities and practical exercises (mentioned 3 times). This indicates a need to increase practical experience and engagement to better prepare for the application of the training material.

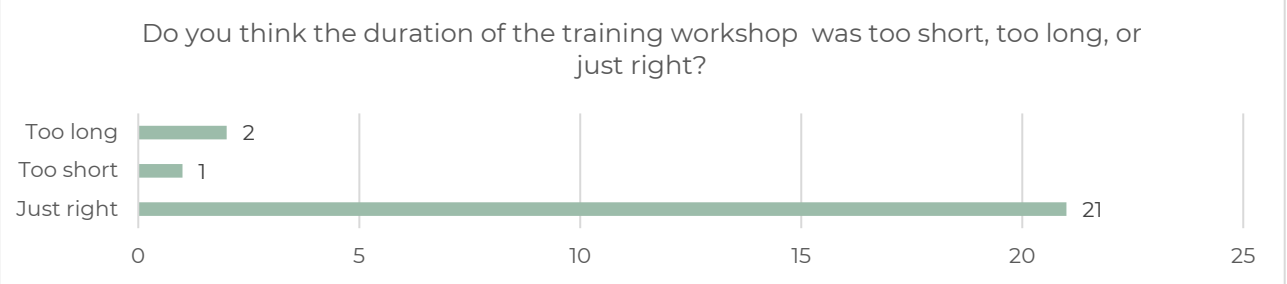
It is important to emphasize that the three-day Boostcamp program was highly intensive, covering a wide range of theoretical and strategic topics necessary for the successful implementation of the pilot trainings. Although time for additional practical tasks was limited, a significant focus was placed on hands-on work with the project's collaboration platform. More than two hours were dedicated to this activity, during which participants actively tested the platform's functionality, providing real-time comments and feedback. Therefore, the participants' suggestion for more practical activities is viewed not as a shortcoming of the program, but as a valuable insight for the upcoming national pilot trainings, whose longer format will allow for the integration of more practical content.

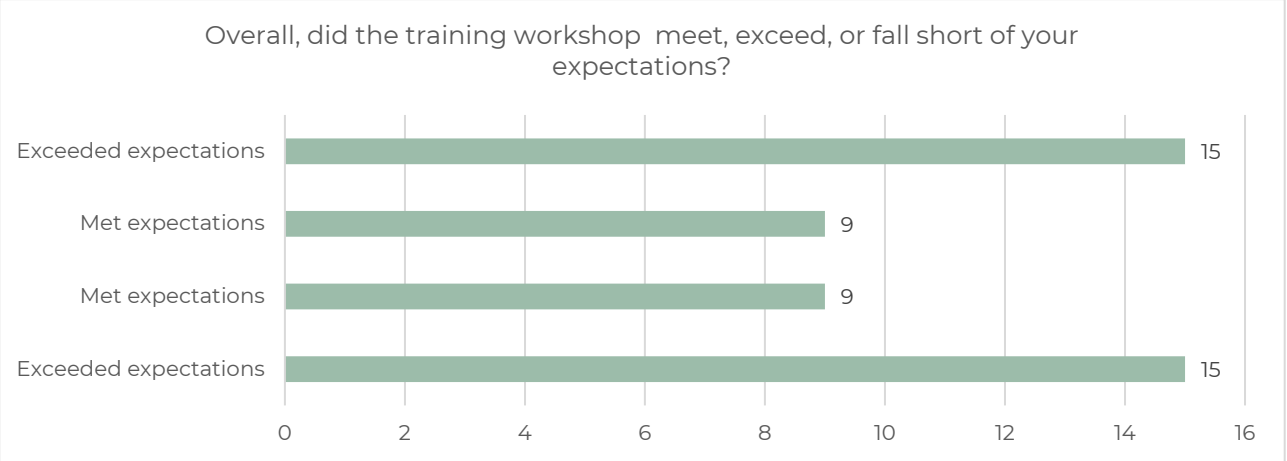
The survey results show that the training was valuable, and the content related to AI/Cybersecurity, W4C mentoring, and the practical application/testing of the project platform was recognized as the most useful. In summary, the feedback received from participants was positive and constructive, which confirms the high overall quality of the seminar. Participant insights affirmed the project's direction, with the main recurring suggestion for future workshops being the inclusion of even more original, hands-on content. This feedback is highly valuable and will be directly applied when planning the next project phase—the national pilot trainings.

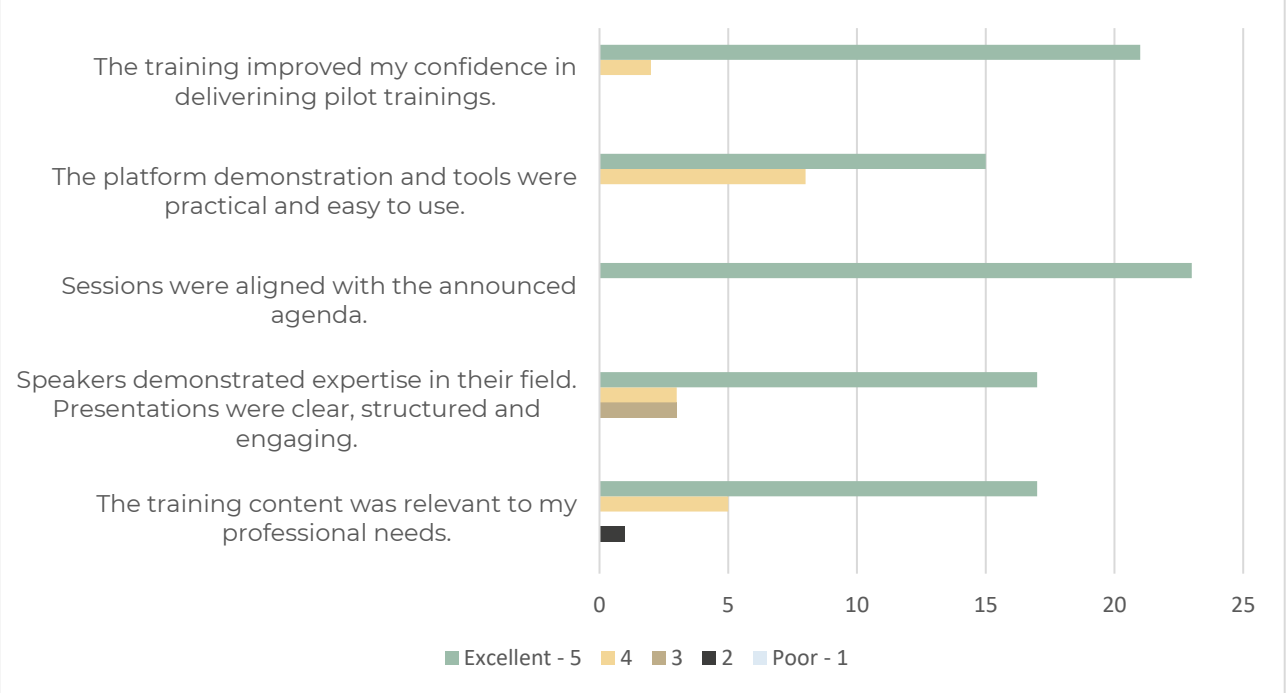
The survey data is presented in charts:

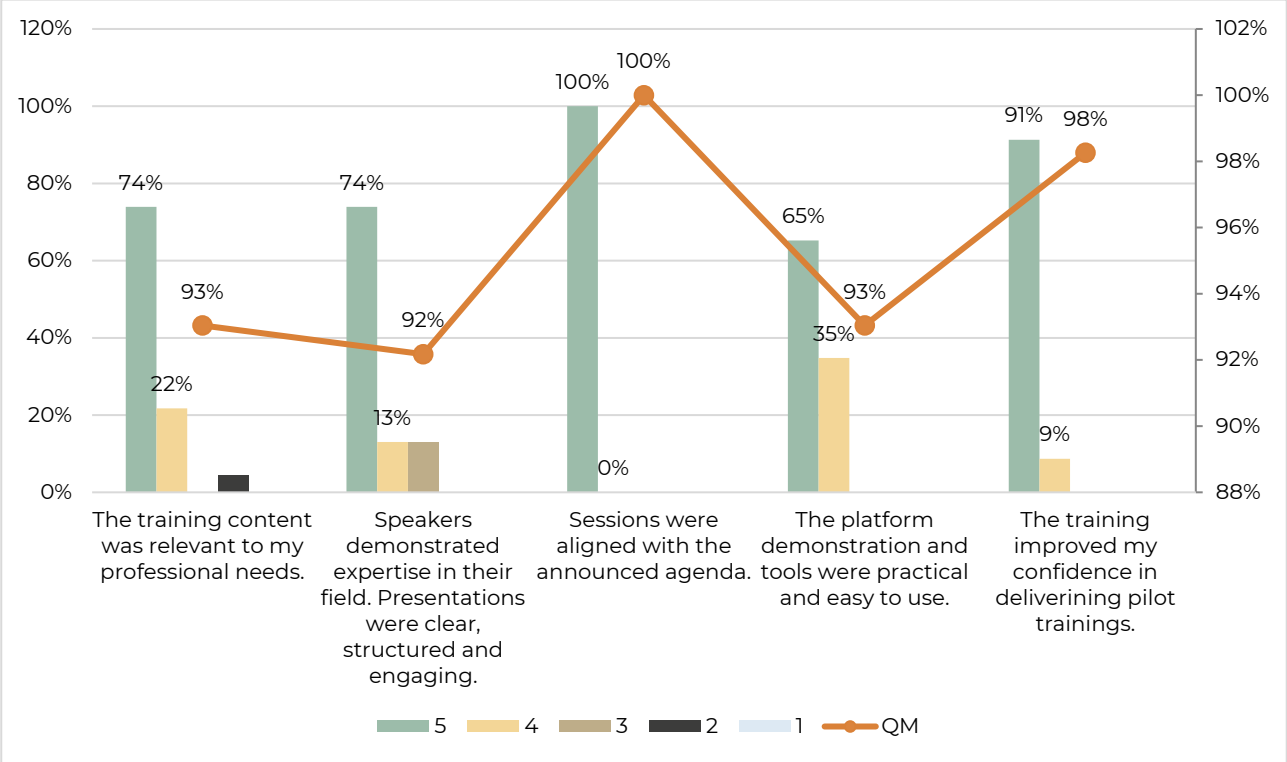


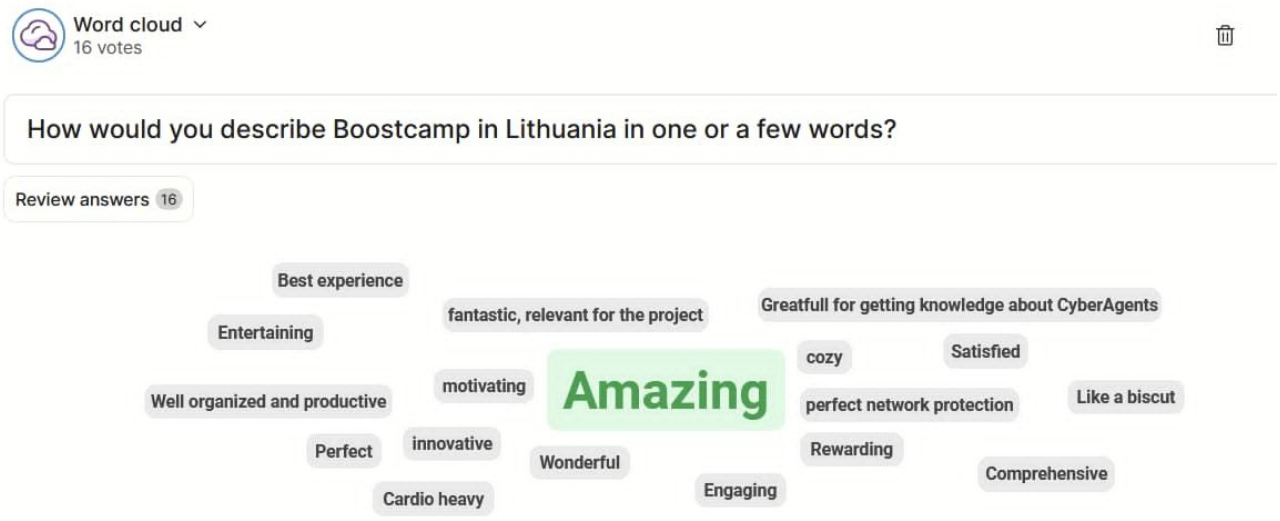



Do you think the duration of the training workshop was too short, too long, or just right?
Too long
Too short
Just right
2
1
21
0
5
10
15
20
25


Overall, did the training workshop meet, exceed, or fall short of your expectations?
Exceeded expectations
Met expectations
Met expectations
Exceeded expectations
15
9
9
15
0
2
4
6
8
10
12
14
16

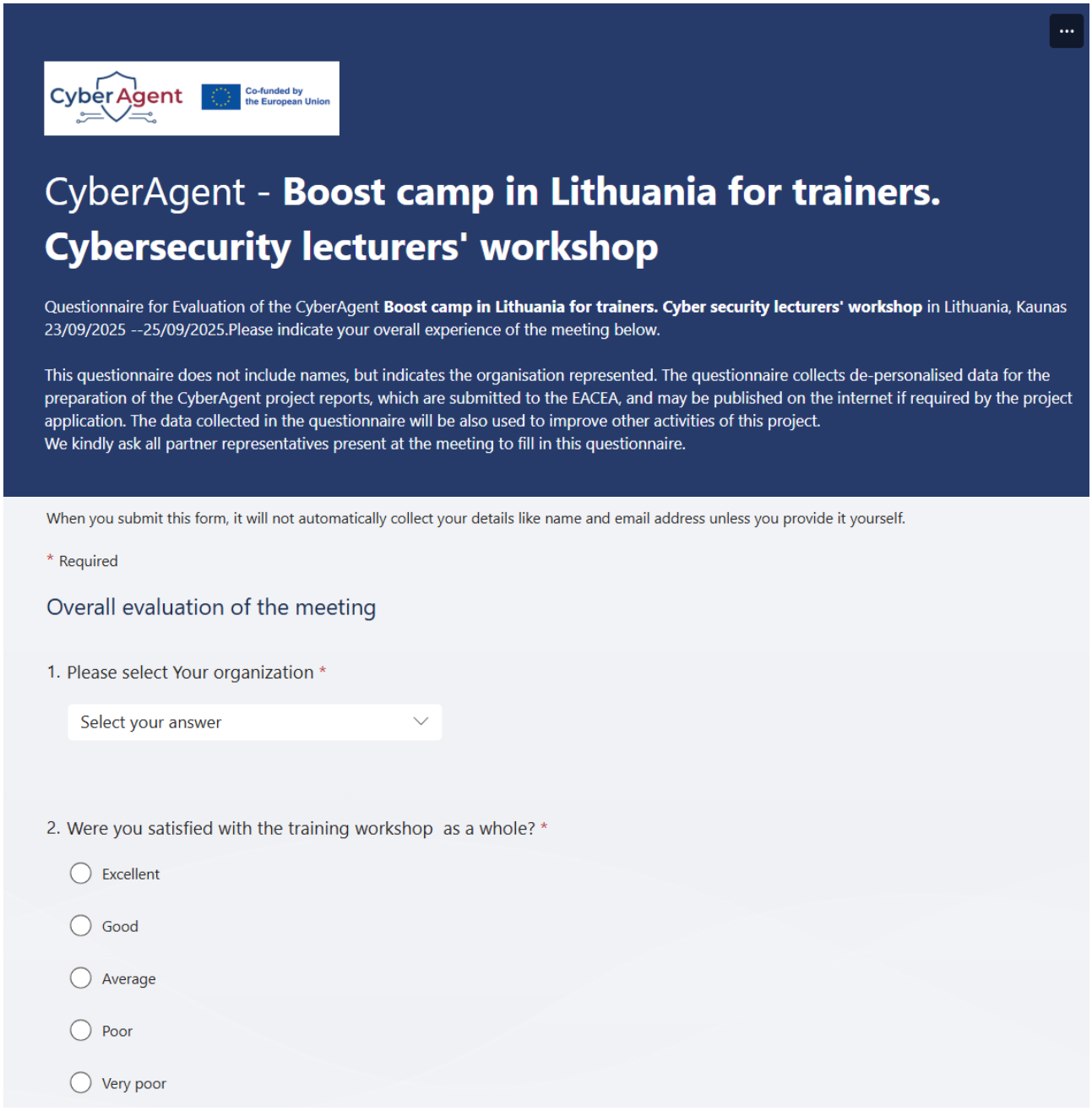

The training improved my confidence in deliverining pilot trainings.
The platform demonstration and tools were practical and easy to use.
Sessions were aligned with the announced agenda.
Speakers demonstrated expertise in their field. Presentations were clear, structured and engaging.
The training content was relevant to my professional needs.
0
5
10
15
20
25
Excellent - 5
4
3
2
Poor - 1


120%
100%
80%
60%
40%
20%
0%
102%
100%
98%
96%
94%
92%
90%
88%
74%
22%
93%
74%
13%
92%
100%
0%
100%
65%
35%
93%
91%
9%
98%
The training content was relevant to my professional needs.
Speakers demonstrated expertise in their field. Presentations were clear, structured and engaging.
Sessions were aligned with the announced agenda.
The platform demonstration and tools were practical and easy to use.
The training improved my confidence in deliverining pilot trainings.
5
4
3
2
1
QM


Word cloud
16 votes
How would you describe Boostcamp in Lithuania in one or a few words?
Review answers 16
Best experience
fantastic, relevant for the project
Greatfull for getting knowledge about CyberAgents
Entertaining
cozy
Satisfied
motivating
Amazing
Well organized and productive
perfect network protection
Like a biscut
Perfect
innovative
Rewarding
Wonderful
Comprehensive
Engaging
Cardio heavy

ANNEXES

ANNEX 1. EVALUATION TRAIN-THE-TRAINER FORM



CyberAgent - **Boost camp in Lithuania for trainers. Cybersecurity lecturers' workshop**

Questionnaire for Evaluation of the CyberAgent **Boost camp in Lithuania for trainers. Cyber security lecturers' workshop** in Lithuania, Kaunas 23/09/2025 --25/09/2025.Please indicate your overall experience of the meeting below.

This questionnaire does not include names, but indicates the organisation represented. The questionnaire collects de-personalised data for the preparation of the CyberAgent project reports, which are submitted to the EACEA, and may be published on the internet if required by the project application. The data collected in the questionnaire will be also used to improve other activities of this project.
We kindly ask all partner representatives present at the meeting to fill in this questionnaire.

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

Overall evaluation of the meeting

1. Please select Your organization *

Select your answer

2. Were you satisfied with the training workshop as a whole? *

- Excellent
- Good
- Average
- Poor
- Very poor

3. The training workshop as a whole was appropriate and productive: *

- ◯ Excellent
- ◯ Good
- ◯ Average
- ◯ Poor
- ◯ Very poor

4. The information you received before the training workshop, intended to facilitate your participation in the meeting was: *

- ◯ Excellent
- ◯ Good
- ◯ Average
- ◯ Poor
- ◯ Very poor

5. The organization of training workshop was: *

- ◯ Excellent
- ◯ Good
- ◯ Average
- ◯ Poor
- ◯ Very poor

6. The organization of the facilities used for the training workshop was: *

- ◯ Excellent
- ◯ Good
- ◯ Average
- ◯ Poor
- ◯ Very poor

7. Possibility of background discussion was: *

- ◯ Excellent
- ◯ Good
- ◯ Average
- ◯ Poor
- ◯ Very poor

8. Do you think the duration of the training workshop was too short, too long, or just right? *

- ◯ Too short
- ◯ Too long
- ◯ Just right

9. Overall, did the training workshop meet, exceed, or fall short of your expectations? *

- ◯ Exceeded expectations
- ◯ Met expectations
- ◯ Fell short of expectations

10. Do you have any general comments about the training workshop?

Enter your answer

Next

Page 1 of 2

Never give out your password. Report abuse

11. How much do you agree/disagree with the following statements (select a rating from 1 to 5, where 1 means strongly disagree and 5 means strongly agree) *

	5	4	3	2	1
The training content was relevant to my professional needs.	○	○	○	○	○
Speakers demonstrated expertise in their field. Presentations were clear, structured, and engaging.	○	○	○	○	○
Sessions were aligned with the announced agenda.	○	○	○	○	○
The platform demonstration and tools were practical and easy to use.	○	○	○	○	○
The training improved my confidence in delivering pilot trainings.	○	○	○	○	○

12. Which session(s) did you find most useful, and why? *

Enter your answer

13. Which session(s) did you find less useful, and why? *

Enter your answer

14. Do you have any comments on the topics mentioned above? (optional question)

Enter your answer

15. Suggestions for improvement of future training workshops. (optional question)

Enter your answer

Back Submit

Page 2 of 2

Never give out your password. Report abuse

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

Olemisen Balanssia ry

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau