



Co-funded by
the European Union

SUPPORTING DOCUMENT FOR THE D4.3 PLATFORM FINE- TUNED AND TRANSLATED

CYBER AGENT

06.2026

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 4: CyberAgent Collaboration Digital Platform
Deliverable 4.3: Platform fine-tuned and translated
Leader of WP4 – Prios



“SMEs Cyber Security Change Agents” by Erasmus+ Project “Platform fine-tuned and translated ” under the Creative Commons licence CC BY-NC-ND

CONTENT

INTRODUCTION.....	2
1. LEARNING AND TRAINING ENVIRONMENT	2
2. CENTRALISED KNOWLEDGE REPOSITORY	6
3. COMMUNITY AND COLLABORATION HUB.....	11
4. BLOG AND AWARENESS RISING CONTENT	12
5. EVENTS AND ENGAGEMENT SECTION	15
6. USER ACCOUNTS AND PERSONALISED ACCESS.....	16
7. MULTI-LINGUAL ACCESSIBILITY.....	19

INTRODUCTION

The SME Cyber Security Change Agent Collaboration Platform is a one-stop hub for cross-border collaboration in cybersecurity upskilling among European SMEs. Bringing together higher education institutions, vocational providers, labour market actors, and cybersecurity experts, the platform fosters knowledge exchange and best practices. It offers targeted resources, e-learning courses, and matchmaking tools to enhance cybersecurity skills, with a focus on empowering women in the field. By supporting EU-level policy dialogue, it promotes policies tailored to SMEs' cybersecurity needs, driving digital technology adoption within SMEs and the public sector and contributing to a resilient and secure digital Europe.

1. LEARNING AND TRAINING ENVIRONMENT

The platform provides a structured e-learning environment offering cybersecurity training modules tailored to different target groups. Dedicated learning environment is for:

- Higher education (HEI) learners and educators
- Vocational education and training (VET) learners and trainers
- SME learners

HIGHER EDUCATION (HEI) LEARNING TRACK

The **Higher Education (HEI) track** is designed for university students, academic staff, and educators seeking to strengthen their knowledge and teaching capacity in the field of cybersecurity. This learning pathway focuses on:

- Developing **theoretical understanding** of cybersecurity concepts, threats, and protection mechanisms;
- Strengthening **analytical and critical thinking skills** related to cyber risks, digital systems, and data protection;
- Supporting educators in integrating cybersecurity topics into **formal curricula and academic courses**.

HEI modules are structured to combine conceptual explanations with applied examples, enabling learners to connect cybersecurity theory with real-world scenarios. The content supports academic learning outcomes while remaining relevant to current labour market and research needs.

VOCATIONAL EDUCATION AND TRAINING (VET) LEARNING TRACK

The **Vocational Education and Training (VET) track** is tailored to VET learners, trainers, and practitioners, with a strong emphasis on **practical application and workplace relevance**. This pathway focuses on:

- Building **job-ready cybersecurity skills** applicable in SMEs and operational environments;
- Supporting trainers in delivering cybersecurity education aligned with **vocational standards and professional profiles**;
- Enabling learners to recognise, prevent, and respond to common cyber threats encountered in everyday work contexts.

VET modules prioritise hands-on learning, operational awareness, and actionable guidance, ensuring that learners can directly transfer acquired competences into professional practice.

MODULAR LEARNING DESIGN AND KEY TOPICS

Across both learning tracks, the platform delivers **modular cybersecurity training units** covering key topics such as:

- Cyber threats and vulnerabilities
- Digital safety and data protection
- Secure use of digital tools and systems
- Organisational cyber resilience and risk awareness

The modular structure allows learners to engage with content flexibly, selecting learning units according to their existing knowledge, professional needs, and learning goals.

SUPPORT FOR UPSKILLING AND RESKILLING

The learning modules are explicitly designed to support both **upskilling and reskilling processes**, enabling users to:

- Update existing digital competences in response to evolving cyber risks;
- Acquire new cybersecurity skills relevant to changing job roles and organisational demands;
- Strengthen transversal competences such as problem-solving, risk awareness, and responsible digital behaviour.

By focusing on **practice-oriented learning outcomes**, the platform ensures that users gain competences that are directly applicable in educational, vocational, and professional environments.

PRACTICE-ORIENTED AND LEARNER-CENTRED APPROACH

The e-learning environment follows a **learner-centred and practice-oriented pedagogical approach**, combining structured content with real-life examples and applied learning tasks. This approach supports:

- Active learner engagement;
- Improved knowledge retention;
- The development of confidence in applying cybersecurity principles in real-world contexts.

E-learning for higher education

Toggle the buttons to see the different views

Available courses

Module description

How it works

Find the Higher education learning module that suits your need.

Available content

Filter content



Module 1 - Security Program Management



Module 2 - Systems Administration



Module 3 - Analytical Tools



Module 4 - Security Operations



Module 5 - Security Governance & Policy



Module 6 - Cybersecurity Planning



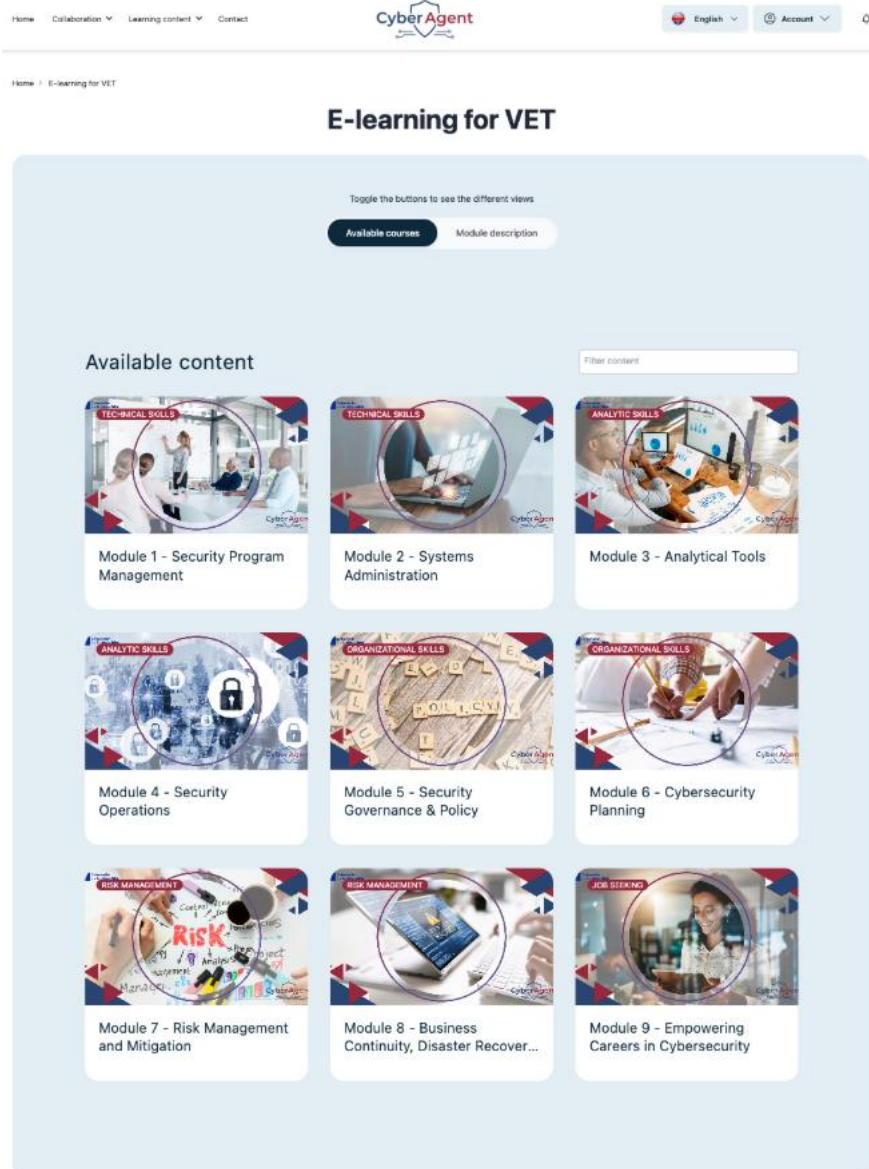
Module 7 - Risk Management and Mitigation



Module 8 - Business Continuity, Disaster Recovery and Incident...



Module 9 - Empowering Careers in Cybersecurity



The screenshot shows the 'E-learning for VET' section of the CyberAgent platform. At the top, there is a navigation bar with links for Home, Collaboration, Learning content, and Contact. Below this, a toggle switch allows users to view 'Available courses' (selected) or 'Module description'. The main content area, titled 'Available content', features a grid of nine course modules, each with a representative image and a title:

- Module 1 - Security Program Management (Technical Skills)
- Module 2 - Systems Administration (Technical Skills)
- Module 3 - Analytical Tools (Analytic Skills)
- Module 4 - Security Operations (Analytic Skills)
- Module 5 - Security Governance & Policy (Organizational Skills)
- Module 6 - Cybersecurity Planning (Organizational Skills)
- Module 7 - Risk Management and Mitigation (Risk Management)
- Module 8 - Business Continuity, Disaster Recover... (Risk Management)
- Module 9 - Empowering Careers in Cybersecurity (Job Seeking)

2. CENTRALISED KNOWLEDGE REPOSITORY

The CyberAgent platform hosts a **centralised knowledge repository** that aggregates a wide range of resources, supporting continuous learning, professional development, and informed decision-making across educational and organisational settings.

TYPES OF LEARNING RESOURCES

The repository includes diverse resource formats to address different learning preferences and use cases, such as:

- **Educational materials** explaining core cybersecurity concepts, terminology, and frameworks;
- **Practical guides and checklists** supporting secure digital practices in daily work and learning environments;
- **Reference documents** providing structured background information on cybersecurity risks, threats, and preventive measures;
- **Awareness-raising materials** aimed at improving digital safety culture and risk perception;
- **Best-practice examples and case-based insights** drawn from real-world organisational and educational contexts.

This diversity ensures that the platform supports both introductory learning and more advanced reference needs.

SUPPORT FOR CONTINUOUS AND SELF-DIRECTED LEARNING

The knowledge repository is designed to promote **continuous, self-directed learning** by allowing users to:

- Access resources on demand, independent of formal training schedules;
- Use materials for refresher learning or just-in-time problem solving;
- Explore topics at their own pace according to professional needs and personal learning objectives.

This approach enables users to maintain and update their cybersecurity knowledge in response to evolving digital threats and technological developments.

APPLICATION ACROSS EDUCATIONAL AND PROFESSIONAL CONTEXTS

The learning resources are structured to be **transferable and applicable** across multiple contexts, including:

- **Educational settings**, where teachers and trainers can use materials to support lesson preparation, classroom activities, and curriculum development;
- **Professional environments**, particularly SMEs, where employees and managers can apply guidance to improve everyday digital security practices;
- **Organisational contexts**, supporting internal awareness-raising, policy development, and cyber resilience strategies.

The repository therefore acts as a bridge between **theoretical knowledge and practical implementation**.

BEST-PRACTICE ORIENTATION AND KNOWLEDGE TRANSFER

A key feature of the repository is its emphasis on **best-practice insights**, enabling users to learn from proven approaches rather than abstract recommendations. These insights support:

- The adoption of effective cybersecurity behaviours;
- Organisational learning and improvement;
- The transfer of knowledge across sectors and countries.

By highlighting practical and replicable solutions, the platform strengthens users' capacity to respond to real cybersecurity challenges.

ACCESSIBILITY AND USER-FRIENDLY DESIGN

The knowledge repository is embedded within the platform's **user-friendly interface**, enabling easy navigation and discovery of relevant materials. Combined with the platform's multilingual functionality, this ensures that resources are **accessible to a broad European audience**, regardless of linguistic or professional background.

Learning resources

Welcome to the course resource library. Here you can easily access and download the accompanying materials from your lessons, designed to provide you with direct support for your learning.

Available resource

Available resource



versionFourKeys.learningResourceModuleO



versionFourKeys.learningResourceModuleTv



versionFourKeys.learningResourceModuleFi



versionFourKeys.learningResourceModuleSi



versionFourKeys.learningResourceModuleTt



versionFourKeys.learningResourceModuleFc



versionFourKeys.learningResourceModuleSi



versionFourKeys.learningResourceModuleEi

Business continuity

Filter levels

English

Filter content

Filter by type

Short videos

Interviewing for Security Components	Higher Education				
Third Party Security	Higher Education				
Incident Response and Communication	Higher Education				
Employee Data Privacy	Higher Education				
Compliance with privacy regulations	Higher Education				
Security Termination Practices	VET Higher Education				
Disaster Recovery	Higher Education				
Security in Review Process	Higher Education VET				
Information Security Awareness Employee Training	VET Higher Education				
Internal Audit vs External Audit	Higher Education VET				

Short presentations

Incident Response	Higher Education				
Disaster Recovery	Higher Education				
Business Continuity	Higher Education				
Security Awareness, Training and Education	Higher Education				
Security Hiring Practices	Higher Education				
Security Termination Practices	Higher Education VET				
WHY THIRD-PARTY SECURITY IS CRITICAL FOR SMES	Higher Education				
KEY SECURITY CONTENT IN THIRD-PARTY CONTRACTS	Higher Education				
DEFINING ROLES AND RESPONSIBILITIES IN VENDOR SECURITY	Higher Education				
AUTOMATED SECURITY MONITORING FOR YOUR BUSINESS	Higher Education				
Security assessments for SMEs: A practical journey	VET Higher Education				
INTERNAL VS. EXTERNAL SECURITY AUDITS	VET Higher Education				
UNDERSTANDING SECURITY TESTING FOR SMALL BUSINESSES	VET Higher Education				
SELECT APPROPRIATE SECURITY TOOLS	Higher Education				

3. COMMUNITY AND COLLABORATION HUB

The CyberAgent platform functions as a **collaborative digital space** designed to facilitate interaction, knowledge exchange, and peer learning among a diverse range of stakeholders involved in cybersecurity education and practice. By bringing together **SME employees, educators, trainers, learners, and cybersecurity experts**, the platform supports the creation of a **cross-sectoral community of practice** focused on strengthening cybersecurity awareness and organisational resilience.

MULTI-STAKEHOLDER ENGAGEMENT

The collaborative environment is structured to enable meaningful engagement between different user groups, including:

- SME staff and managers seeking practical cybersecurity solutions;
- Educators and trainers delivering cybersecurity-related learning in HEI and VET contexts;
- Learners developing cybersecurity competences for future employment;
- Cybersecurity stakeholders and practitioners contributing expert insights and experience.

This multi-stakeholder composition ensures that knowledge exchange is **practice-informed, education-oriented, and labour-market relevant**.

KNOWLEDGE EXCHANGE AND PEER LEARNING

The platform enables users to **share experiences, insights, and lessons learned** related to cybersecurity challenges and solutions. Through this peer-based interaction, users can:

- Discuss real-life cybersecurity issues encountered in educational or workplace settings;
- Exchange practical strategies for prevention, mitigation, and response to cyber risks;
- Learn from diverse perspectives across sectors, countries, and professional roles.

This peer learning approach supports the development of **collective intelligence** and reinforces learning beyond individual training modules.

COMMUNITY OF PRACTICE DEVELOPMENT

CyberAgent supports the establishment of a **sustainable community of practice**, where users actively contribute to and benefit from shared knowledge over time. This community-oriented model:

- Encourages continuous engagement rather than one-off participation;

- Fosters trust and mutual learning among participants;
- Enables the accumulation of shared expertise and practical know-how.

By connecting users around common cybersecurity challenges, the platform strengthens a culture of **collaboration, responsibility, and shared problem-solving**.

SUPPORT FOR CYBERSECURITY AWARENESS AND RESILIENCE

The collaborative features directly contribute to improved **cybersecurity awareness and resilience** by:

- Facilitating the dissemination of good practices and effective solutions;
- Supporting reflection on emerging threats and changing digital risks;
- Enabling users to adapt shared knowledge to their own organisational or educational contexts.

This collective learning process enhances users' capacity to anticipate, prevent, and respond to cybersecurity incidents.

CROSS-BORDER AND CROSS-SECTOR COOPERATION

As a European platform, CyberAgent enables **cross-border collaboration**, allowing users from different countries and systems to engage in dialogue and exchange. This contributes to:

- Increased understanding of cybersecurity challenges across contexts;
- Transferability of solutions and practices;
- Alignment with European priorities on digital skills, resilience, and cooperation.

4. BLOG AND AWARENESS RISING CONTENT

The CyberAgent platform includes a dedicated **blog section** that serves as an accessible and dynamic channel for **cybersecurity awareness-raising, knowledge dissemination, and reflection**. The blog complements the structured learning environment by providing regularly updated, easy-to-access content that supports informal and continuous learning.

THEMATIC FOCUS AND CONTENT SCOPE

Blog articles and contributions address a wide range of **cybersecurity-related themes**, including:

- Emerging cyber threats and evolving risk patterns;
- Current trends in digital security and cyber resilience;
- Good practices in cybersecurity prevention and response;
- Practical insights relevant to SMEs, educators, and training providers;
- Reflections on cybersecurity challenges in educational and organisational contexts.

This thematic diversity ensures that the blog remains relevant to multiple target groups and levels of expertise.

KNOWLEDGE DISSEMINATION AND TRANSLATION OF EXPERTISE

The blog plays a key role in **translating complex cybersecurity knowledge into accessible formats**, making expert insights understandable for non-specialist audiences. Content is presented in a way that:

- Reduces technical barriers to understanding cybersecurity issues;
- Highlights key messages and actionable takeaways;
- Encourages readers to apply insights in real-life situations.

By doing so, the blog supports broader outreach and impact beyond formal training participants.

SUPPORT FOR AWARENESS-RAISING AND PREVENTIVE CULTURE

The blog contributes to the development of a **preventive cybersecurity culture** by:

- Raising awareness of common digital risks and vulnerabilities;
- Encouraging proactive and responsible digital behaviour;
- Promoting reflection on the human and organisational dimensions of cybersecurity.

This awareness-raising function is particularly important for SMEs and educators, where prevention and early recognition of risks play a critical role in cyber resilience.

COMPLEMENTARITY WITH LEARNING MODULES AND RESOURCES

Blog content is designed to **complement and reinforce** the platform's structured learning modules and knowledge repository. It:

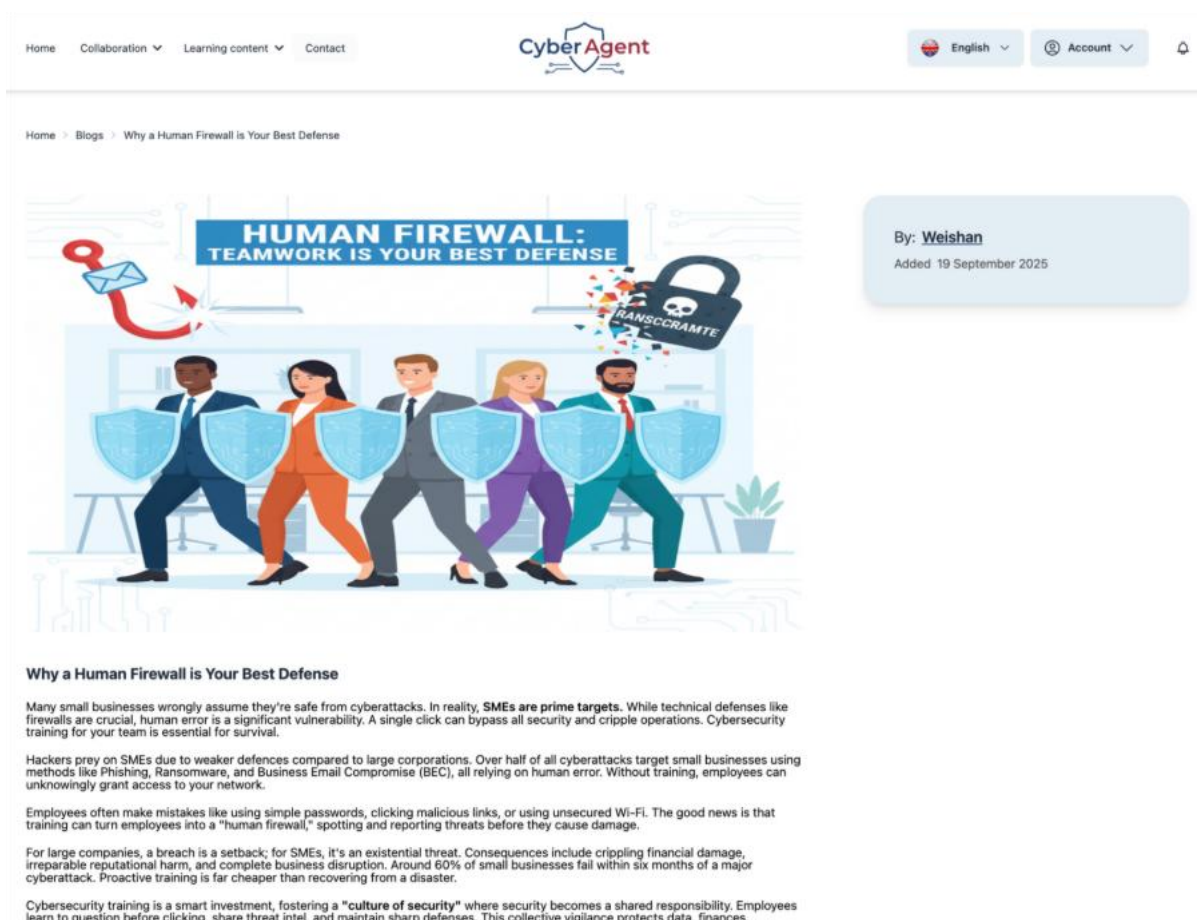
- Provides contextual background to formal training topics;
- Introduces new issues that may later be addressed through dedicated learning units;
- Encourages users to explore additional platform resources.

This integrated approach strengthens coherence across the platform's learning and dissemination components.

CONTINUOUS UPDATES AND ENGAGEMENT

As a regularly updated section, the blog helps ensure that the platform remains **current and responsive** to developments in the cybersecurity field. It encourages repeat visits and sustained user engagement by:

- Offering timely insights on relevant topics;
- Reflecting ongoing discussions and challenges in cybersecurity;
- Supporting continuous professional development.



Blogs

Create new blog →

Search blogs

All languages

Sort by date (Descending)



Why a Human Firewall is Your Best Defense

Cybersecurity training transforms an SME's weakest link—the human element—into its first and most solid line of defense...

By: [Weishan](#)

Actions



Training CyberAgents: Turning curious students into Cyber-Aware professionals

At TechEd VET College, we wanted to go beyond theory in our IT and business subjects.

By: [WiseTiger3451](#)

Actions



We thought we were too small to be targeted – We were wrong

Like many small businesses, we assumed cyberattacks were something only large corporations needed to worry about.

By: [WiseTiger3451](#)

Actions

5. EVENTS AND ENGAGEMENT SECTION

The CyberAgent platform includes an **integrated events section** that serves as a central point for disseminating information about **upcoming training activities, workshops, webinars, and project-related events**. This functionality enhances the platform's role as an active learning and engagement environment, extending participation beyond self-paced, asynchronous e-learning.

CENTRALISED ACCESS TO CAPACITY-BUILDING ACTIVITIES

The events section provides users with **clear and structured access** to information about planned activities, including:

- Training sessions and workshops linked to cybersecurity skills development;

- Online and hybrid events supporting professional learning and peer exchange;
- Project-related meetings, dissemination events, and stakeholder activities.

By centralising this information, the platform ensures transparency, visibility, and ease of access for all target groups.

BRIDGING ONLINE LEARNING AND REAL-WORLD PRACTICE

A key function of the events section is to **connect online learning with real-world capacity-building activities**. Events are designed to:

- Complement and reinforce content provided through e-learning modules;
- Offer opportunities for practical application, discussion, and clarification;
- Enable learners to interact directly with trainers, experts, and peers.

This blended approach strengthens learning outcomes by combining digital resources with experiential and interactive formats.

6. USER ACCOUNTS AND PERSONALISED ACCESS

The CyberAgent platform enables registered users to create **personal user accounts**, providing secure and personalised access to the platform's learning, collaboration, and engagement features. This functionality supports structured participation and enhances the overall learning experience by aligning platform content with individual user needs and roles.

ACCESS TO TAILORED LEARNING CONTENT

Through personal user accounts, users can access **learning content tailored to their profile and target group**, such as HEI learners, VET learners, educators, trainers, or SME professionals. This targeted access:

- Helps users identify relevant learning materials more efficiently;
- Supports differentiated learning pathways based on educational or professional context;
- Reduces information overload by prioritising applicable content.

PARTICIPATION IN PLATFORM ACTIVITIES

Registered users can actively **participate in platform-based activities**, including:

- Engaging with e-learning modules and training resources;
- Taking part in collaborative and community-oriented activities;
- Accessing event-related information and engagement opportunities.

This active participation strengthens user involvement and fosters a sense of belonging within the platform's learning community.

[Home](#)
[Collaboration](#)
[Learning content](#)
[Contact](#)



 English

 Account

Home > Profile

Profile

Information

No social links added

Username:

Organisation: Organisation not added

Gender: Female

Country: Norway

User type: SME

Account role:

[Change password](#)

EDIT INFORMATION

Skills

product comprehension [Delete](#)

project management principles [Delete](#)

JavaScript Framework [Delete](#)

ADD SKILL

My experiences

Project supervisor at Prios Kompetanse [Delete](#)

Full-time (Current)

01/07/2024 - Present

Steinkjer, Norway (Hybrid)

ADD EXPERIENCE

Interests

Cooking

Design

Writing

EDIT INTERESTS

My badges

Total points 50

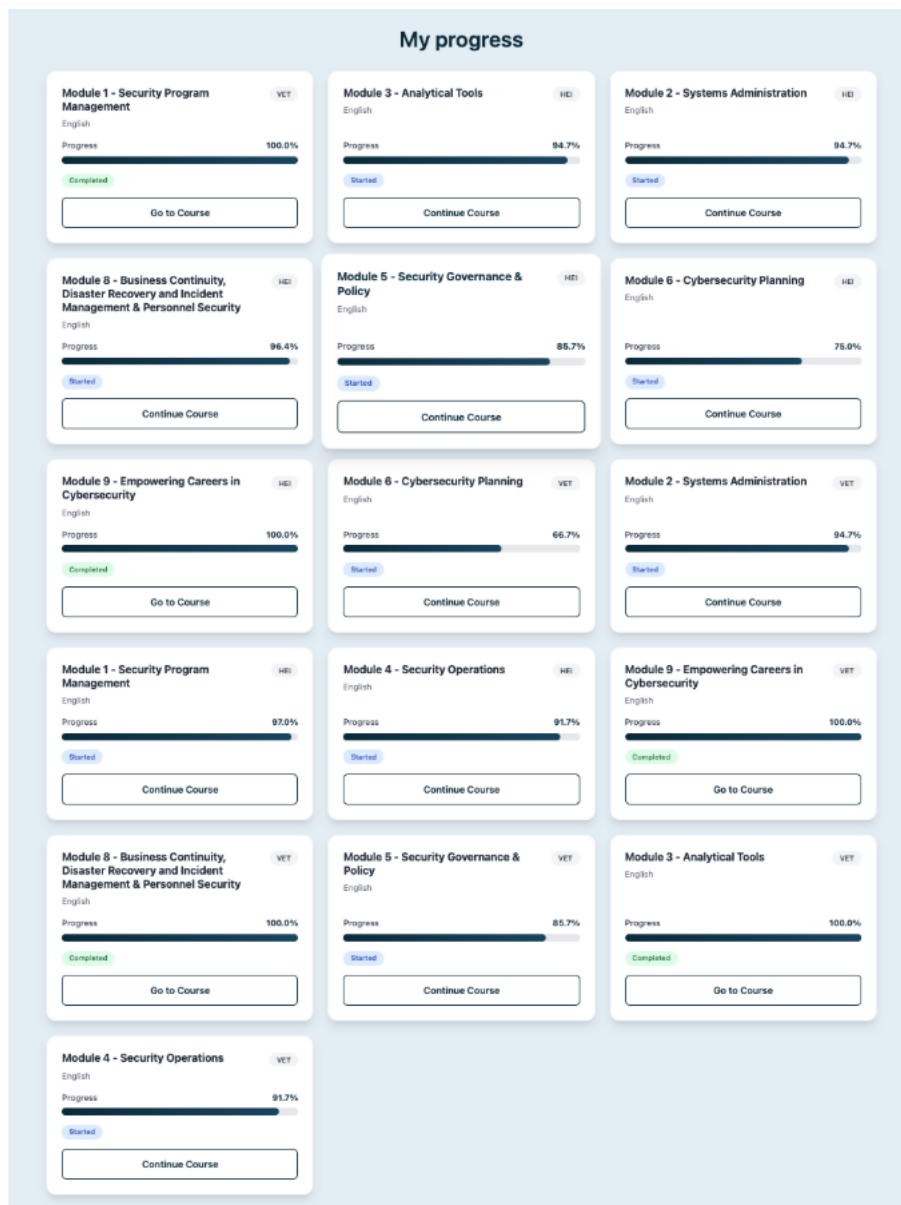
 Chapter expert 1

 Chapter expert 2

 Chapter expert 3

 Module 1 - VET

VIEW MILESTONES



7. MULTI-LINGUAL ACCESSIBILITY

To ensure **inclusiveness, accessibility, and broad European reach**, the CyberAgent platform is available in **multiple languages**, enabling users from diverse linguistic and cultural backgrounds to access content in their preferred language. This multilingual approach directly supports equal access to learning opportunities across countries and regions.

SUPPORT FOR LINGUISTIC DIVERSITY

The platform's multilingual functionality ensures that cybersecurity learning materials, resources, and informational content can be accessed by users who may otherwise face language barriers. This:

- Facilitates participation from users across different European countries;
- Enhances comprehension and learning effectiveness;
- Supports learners with varying levels of proficiency in English or other widely used languages.

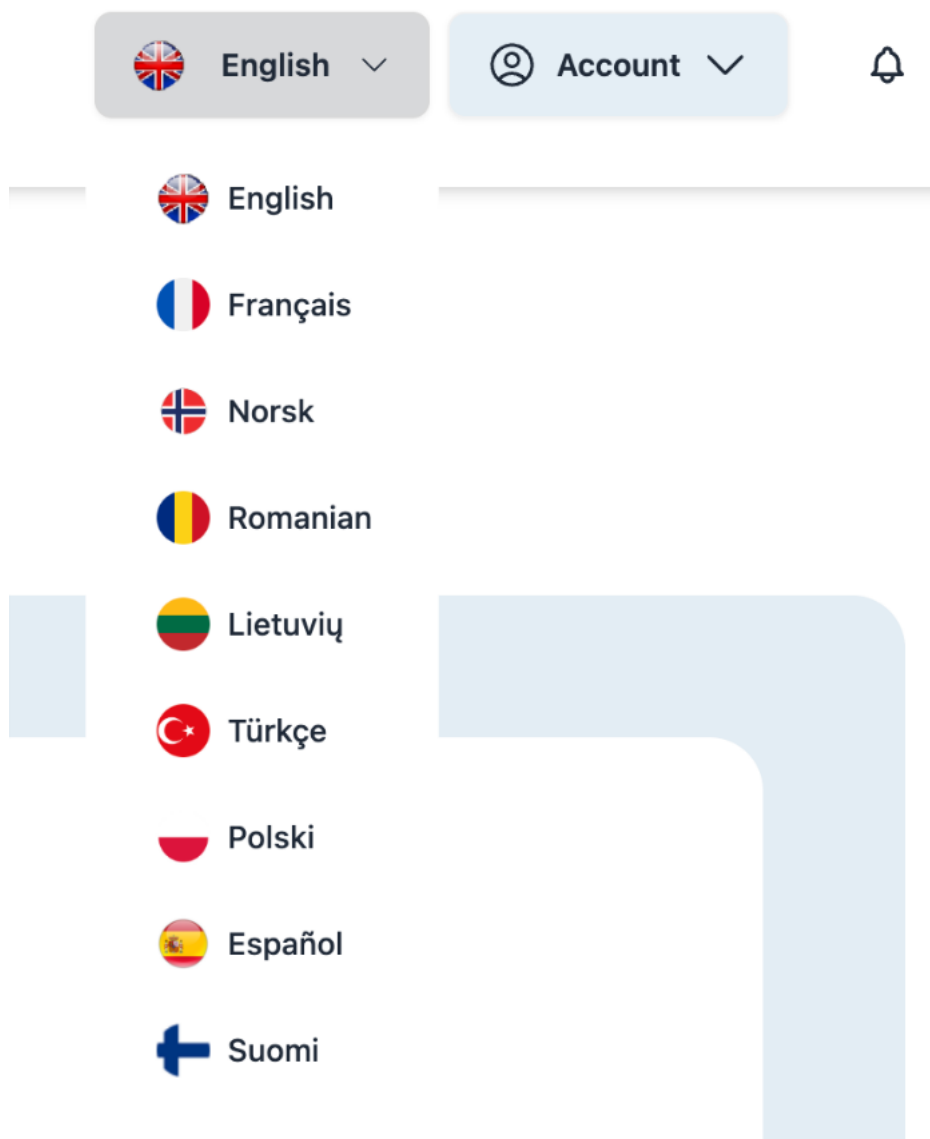
By recognising linguistic diversity, the platform promotes fairness and inclusivity in digital education.

ENHANCED USER ENGAGEMENT AND LEARNING OUTCOMES

Providing content in multiple languages contributes to **improved user engagement and learning outcomes**, as users are more likely to:

- Engage actively with content presented in their native or preferred language;
- Retain knowledge more effectively;
- Apply cybersecurity principles confidently in real-world contexts.

This is particularly relevant for VET learners and SME staff, where practical understanding is essential.



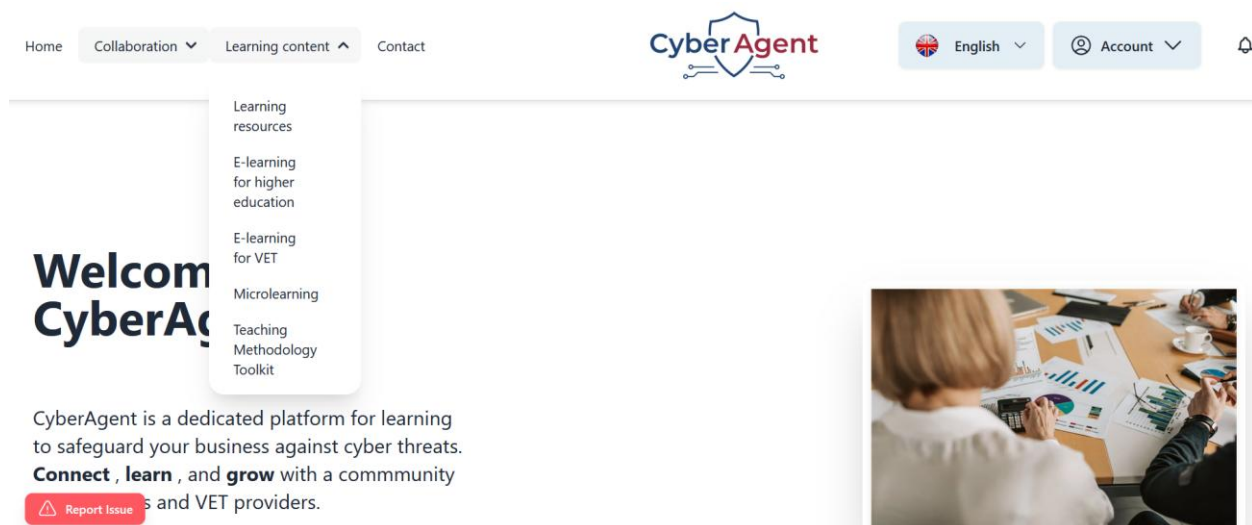
ANNEX

Appendix: Visual Evidence of Platform Fine-Tuning, Multilingual Localization, and User Engagement

This appendix provides visual evidence of the final, fine-tuned CyberAgent Collaboration Digital Platform, fulfilling the requirements for Deliverable 4.3. The platform serves as a comprehensive "one-stop-shop" for cybersecurity upskilling and cross-border collaboration.

Structured Learning and Collaboration

The platform features an intuitive navigation system tailored to the project's target groups. The "Learning content" section provides dedicated access to E-learning for Higher Education, E-learning for VET, Microlearning, and the newly integrated Teaching Methodology Toolkit. Crucially, this toolkit has been fully translated into all partner languages to equip educators and trainers across Europe with accessible, high-quality pedagogical resources.



Concurrently, the "Collaboration" menu integrates Blogs, Events, and user networking tools to foster an active Community of Practice.

Welcome to CyberAgent

CyberAgent is a dedicated platform for learning
to safeguard your business against cyber threats.

Connect, **learn**, and **grow** with a community

of experts and VET providers.

 Report Issue



Personalized User Profiles and Gamification

Registered users are provided with personalized dashboards. These profiles allow learners to track their specific module progress, manage their professional skills and experiences, and view earned badges as part of the platform's gamification strategy. Furthermore, users can instantly generate and download certificates upon the successful completion of module exams.

Comprehensive User Onboarding and Support: To ensure seamless navigation and effective utilization of the platform's features, detailed manuals have been developed and integrated directly into the platform. Fully aligning with the project's multilingual objectives, these manuals are available to all target groups in all partner languages:

Student Guides:

Kaip naudotis platforma esame parengę visomis partnerių kalbomis student vadovus, kurie yra pateikiami platformoje:

EN- <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/b8fab8f9-d72a-443e-a13f-3c22069d602a.pdf>

FR - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/2f17462d-0970-4fe9-ab8d-c13ced70f362.pdf>

NO - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/8c4bccc5-31c9-493e-b15e-b59167e4c614.pdf>

RO - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/f0369e0e-d7e4-436b-a584-273809072dae.pdf>

LT - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/b5337095-d38d-49d5-a0ba-98da54ee41ae.pdf>

TR - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/d3c11868-42da-4bcf-a42f-2911d3532eca.pdf>

PL - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/0c04b5ce-077c-4eba-b52c-13270eea6cb7.pdf>

ES - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/bb00dfe5-9a2e-428a-8e33-226ed3e52416.pdf>

FI - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/9d82aae8-1af9-4995-a6ad-9f180a273313.pdf>

Mentor Guides:

EN - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/06ee0f45-334f-487c-ae82-b7afde749321.pdf>

FR- <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/0c9a7488-adb7-4473-aa9b-02cbb19c0729.pdf>

NO- <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/1ad944ff-3306-4b00-9ec7-e3b1c9e33744.pdf>

RO - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/712d4bf2-2d0c-4354-924c-62361818c00f.pdf>

LT - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/d8a20778-11c9-42c3-a4d9-fa6dadd6fc04.pdf>

TR - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/5549dbd3-62de-49fc-bfbd-95480005bd5c.pdf>

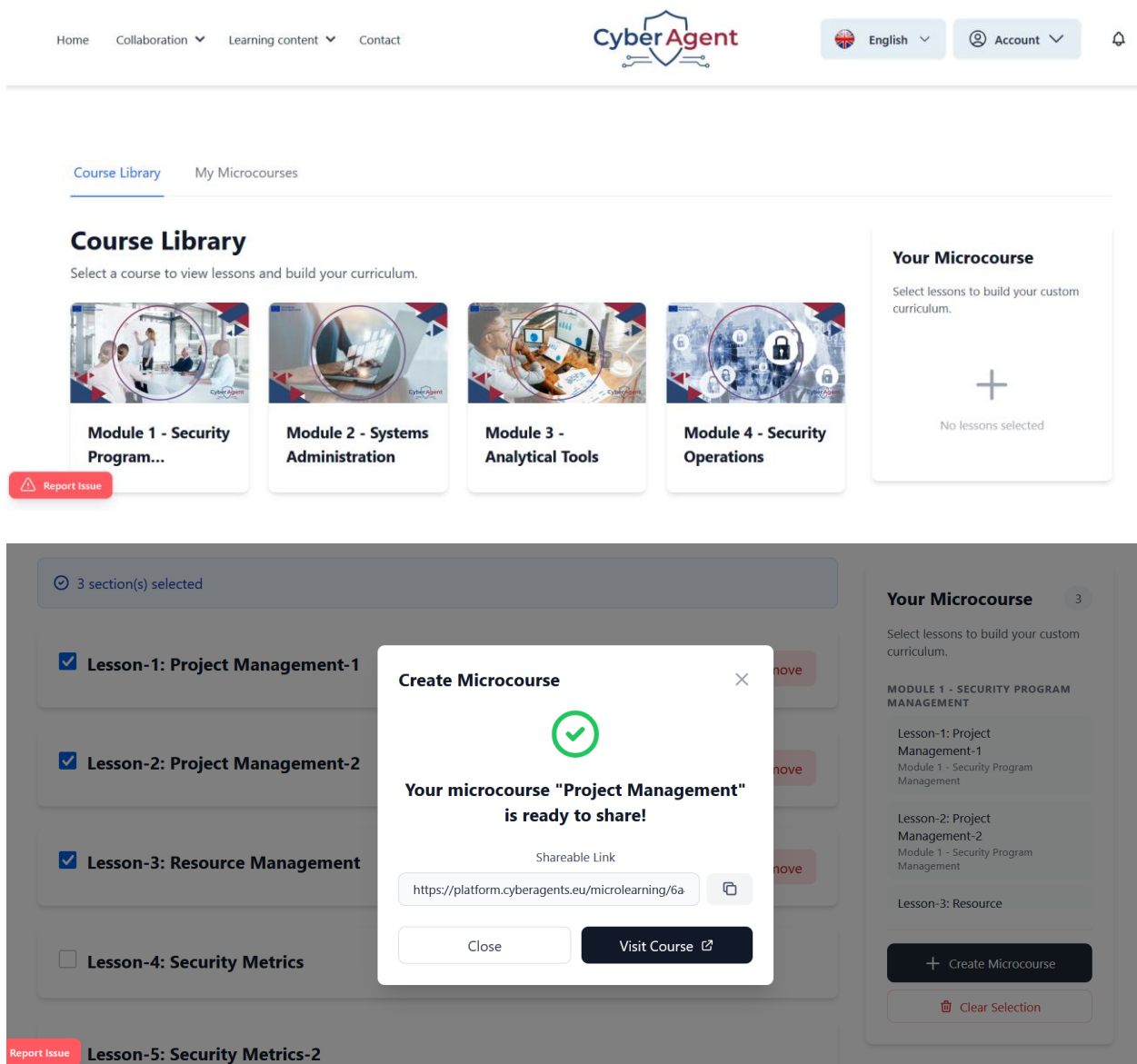
PL - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/0cbb4109-2102-46a1-9016-f6112192d423.pdf>

ES - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/9ff13799-ece3-40fe-bceb-b250be2a422d.pdf>

FI - <https://prioskompetanse.blob.core.windows.net/followupmedia/uploads/5bad9daa-2c05-4ab2-8f67-bb86c2a653af.pdf>

Custom Learning Paths and Micro-Module Personalization

An advanced new feature has been successfully integrated into the platform, enabling learners to construct customized micro-modules based on their personal or specific enterprise requirements. This functionality is fully embedded into the platform's digital infrastructure and functions in all partner languages. This ensures that users are not limited to the standardized module selection across the four predefined core categories (technical, analytical, risk management, and organizational skills). Instead, learners can flexibly combine specific topics from any available module to design a unique learning pathway, monitor their progress in real time, and study at their own pace. The screenshots below illustrate the visual implementation and functional operation of this feature.



The screenshot displays the CyberAgent platform interface. At the top, the navigation bar includes links for Home, Collaboration, Learning content, and Contact, along with the CyberAgent logo, a language selector (English), and an Account menu. Below the navigation bar, the 'Course Library' section is active, showing four modules: Module 1 - Security Program..., Module 2 - Systems Administration, Module 3 - Analytical Tools, and Module 4 - Security Operations. A 'Your Microcourse' section on the right allows users to select lessons to build a custom curriculum. A modal window titled 'Create Microcourse' is open, displaying a green checkmark and the message 'Your microcourse "Project Management" is ready to share!'. The modal provides a shareable link: <https://platform.cyberagents.eu/microlearning/6a>, and buttons for 'Close' and 'Visit Course'. The background shows a list of lessons selected for the microcourse: Lesson-1: Project Management-1, Lesson-2: Project Management-2, Lesson-3: Resource Management, and Lesson-5: Security Metrics-2.

Learning Goals:

After finishing this course, students will be equipped with the skills to effectively manage security programs in response to cybersecurity threats. They will develop defense strategies against current threats such as phishing, ransomware, and DDoS attacks within the frameworks of project and resource management. Additionally, students will learn to apply security metrics and quality assurance methods, gaining the ability to optimize security programs, manage resources efficiently, and enhance organizational security by utilizing appropriate tools against evolving threats. This course will also build their competence in threat assessment, reporting, and communication, enabling them to implement cybersecurity strategies effectively within their organizations.

Project Management

24 lessons selected

MODULE 1 - LESSON-1: PROJECT MANAGEMENT-1

Learning Goals

Lesson-1: Project Management-1

Project Planning

Lesson-1: Project Management-1

Cyber Attacks

Lesson-1: Project Management-1

DDOS Attack

Lesson-1: Project Management-1

As demonstrated in the visual evidence, the platform supports hierarchical access levels, including profiles with Admin and Superadmin privileges. These elevated roles ensure effective backend management, user support, and long-term platform sustainability. For all users, these profiles allow learners to track their specific module progress, manage their professional skills and experiences, and view earned badges as part of the platform's gamification strategy. Furthermore, users can instantly generate and download certificates upon the successful completion of module exams.

Advanced Analytics and Quality Monitoring

To support continuous quality assurance and long-term sustainability, the platform integrates a robust Admin Analytics Dashboard. This backend system tracks real-time quantitative metrics, confirming 820 registered users distributed across key target groups (including HEI students, VET students, and SMEs). The analytics module precisely monitors platform access trends, user interactions by language, and course-related performance data such as exam completion rates and average scores.

Welcome to CyberAgent

CyberAgent is a dedicated platform for learning to safeguard your business against cyber threats. **Connect**, **learn**, and **grow** with a community of SMEs, HEIs and VET providers.



Analytics

Users Information ↗

Platform Access ↗

User Interaction ↗

Course Related Data ↗

Exam Debug ↗

Analytics dashboard

×

Users Information

TOTAL USERS REGISTERED

820

TOTAL USERS CREATED LAST 30 DAYS

30

Type of users

HEI student	305 Users
VET student	215 Users
SME	164 Users
VET trainer	57 Users
User	52 Users
HEI trainer	27 Users

Gender Distribution

M Male	453 Users
F Female	293 Users
N Not Specified	57 Users
P Prefer_not_to_say	17 Users

Users by country

Select a country...

Export to Excel

Lithuania	167 Users	Turkey	137 Users	Romania	96 Users
Poland	83 Users	Spain	66 Users	Not specified	63 Users

Analytics dashboard

×

Platform Access

TOTAL PLATFORM VISITS

1 213



PLATFORM VISITS LAST 30 DAYS

66



PLATFORM VISITS LAST 7 DAYS

24



PLATFORM VISITS LAST 14 DAYS

38



Platform visits by country

Not specified

Total 521
30 days 30

Romania

Total 178
30 days 3

Spain

Total 115
30 days 8

Turkey

Total 92
30 days 2

Belgium

Total 70
30 days 5

Norway

Total 66
30 days 4

Lithuania

Total 60
30 days 10

Poland

Total 54
30 days 2

Finland

Total 23
30 days 1

Other

Total 17
30 days 0

Albania

Total 5
30 days 0

Latvia

Total 3
30 days 0

Analytics dashboard

×

User Interaction

Resource Interaction

* Total Users: The count of unique individuals who engaged with the content (e.g., downloads or external link clicks).

* Total Interactions: The cumulative number of times resources were used (counts every download and external redirect).

TOTAL USERS

128

USERS (30 DAYS)

6

TOTAL INTERACTIONS

595

INTERACTIONS (30 DAYS)

12

Interactions by language

EN English (en)

Total 271

30 days 7

RO Romanian (ro)

Total 198

30 days 2

PL Polish (pl)

Total 38

30 days 1

TR Turkish (tr)

Total 37

30 days 2

ES Spanish (es)

Total 32

30 days 0

NB Norwegian (nb)

Total 19

30 days 0

Interactions per module

Business continuity

Total 133

30 days 1

Security program management

Total 79

30 days 2

Gestionarea programelor de securitate

Total 59

30 days 0

Analytics dashboard

×

Course Related Data

Filter Course Data

Search courses by name...

Q

Course Language

All Languages

Difficulty Level

All Difficulty Levels

User Country

All User Countries

User Type

All User Types

Gender

All Genders

Gender Distribution

male: 383

Unknown: 2

female: 243

prefer_not_to_say: 15

Not specified: 7

User Type Distribution

SME: 129

Unknown: 2

VET trainer: 49

HEI student: 263

VET student: 178

HEI trainer: 22

User: 7

Course Overview

Course Details

User Progress

Course Name	Difficulty	Enrollments	Exam Completion Rate	Avg. Exam Score	Avg. Time (minutes)	Actions
Modul 1 - Zarządzanie programem bezpieczeństwa pl	EQF 5	26	61.54%	89.83%	858 min	View Details
Modül 1 – Güvenlik Programı Yönetimi tr	EQF 6	20	25%	79.5%	107 min	View Details
Modül 1 – Güvenlik Programı Yönetimi tr	EQF 5	86	0%	0%	204 min	View Details

Profile

Information

Username:

Gender:

Country of residence: Lithuania

User type:

Account role:

[Change password](#)

EDIT INFORMATION



First Name:

Last Name:

Skills

cyber security

Delete

computer science

Delete

risk management

Delete

ICT project management

Delete

project management

Delete

public relations

Delete

My experiences

Delete

Delete

Previous page

1 / 5

Next page

ADD EXPERIENCE

Interests

Compliance

AI tools

Ethical usage of AI

EDIT INTERESTS

My badges

Total points 120

Chapter expert 1
 Chapter expert 2
 Chapter expert 3
 Chapter expert 4
 Chapter expert 5

Chapter expert 6
 Module 7 - HEI
 Module 9 - HEI

VIEW MILESTONES

My progress

Modulis 6 - Kibernetinio saugumo planavimas

Lithuanian

Progress 100%

Completed

Exam: Passed
Score: 100%

Go to Course

Certificate

Modulis 4 - Saugumo operacijos

Lithuanian

Progress 8.3%

Started

Continue Course

Modulis 9 - Karjeros galimybių stiprinimas kibernetinio saugumo srityje

Lithuanian

Progress 100%

Completed

Go to Course

Certificate

Welcome to the course "Risk Management and Mitigation"

This module is one of the most important, as small and medium-sized enterprises often become targets of cyber-attacks due to limited resources, making the ability to identify and manage risks a necessity.

Module learning objective

In this module, you will gain knowledge about risk management processes (identification, assessment, and control), and about the measures needed to protect your organisation's assets, ensure business continuity, and implement effective security procedures.

After completing this module, you will be able to:

- Identify and assess risks arising from various sources, threats, and vulnerabilities, and understand their impact on business objectives.
- Apply quantitative and qualitative methods to assess the likelihood and potential consequences of risks.



Module 7 - Risk Management and Mitigation

Main Information about Module ✓

Main information about module ✓

Multilingual Localization

To ensure broad accessibility and inclusivity across Europe, the platform interface and its learning resources have been successfully localized. Visual evidence demonstrates the full translation of the learning environments into English, French, Norwegian, Romanian, Lithuanian, Turkish, Spanish, Finnish, and Polish. Screenshots provided below:



Learning resources

Welcome to the course resource library. Here you can easily access and download the accompanying materials from your lessons, designed to provide you with direct support for your learning.

Available resource

Available resource



Accueil > Ressources pédagogiques

Ressources pédagogiques

Bienvenue dans la bibliothèque de ressources du cours. Vous pouvez y accéder facilement et télécharger les documents d'accompagnement de vos leçons, conçus pour vous apporter un soutien direct dans votre apprentissage.

Ressources disponibles

Ressources disponibles



Læringsressurser

Velkommen til kursressursbiblioteket. Her kan du enkelt få tilgang til og laste ned tilhørende materiell fra leksjonene dine, utformet for å gi deg direkte støtte i læringen din.

Tilgjengelig ressurs

Tilgjengelig ressurs



Rapporter Problem

Resurse educaționale

Bine ați venit la biblioteca de resurse a cursului. Aici puteți accesa și descărca cu ușurință materialele atașate lecțiilor, concepute pentru a vă oferi sprijin direct în procesul de învățare.

Resurse disponibile

Resurse disponibile



Raportează Problema

Mokymosi ištekliai

Sveiki apsilekę kursų išteklų bibliotekoje. Čia galite surasti ir atsisiųsti kursams skirtą mokymosi medžiagą.

Galimas išteklis

Galimas išteklis



Öğrenme kaynakları

Ders kaynak kütüphanesine hoş geldiniz. Burada, derslerinize eşlik eden ve öğrenmenize doğrudan destek sağlamak üzere tasarlanmış materyallere kolayca erişebilirsiniz ve indirebilirsiniz.

Mevcut kaynak

Mevcut kaynak



Recursos didácticos

Bienvenido a la biblioteca de recursos del curso. Aquí podrás acceder fácilmente y descargar los materiales complementarios de tus lecciones, diseñados para proporcionar apoyo directo en su aprendizaje.

Recursos disponibles

Recursos disponibles



 Reportar Problema



Oppimateriaalit

Tervetuloa kurssimateriaalikirjastoon. Täällä voit helposti käyttää ja ladata oppituntiesi oheismateriaaleja, jotka on suunniteltu tukemaan oppimistasi suoraan.

Saatavilla oleva materiaali

Saatavilla oleva materiaali



 Ilmoita Ongelmasta



Materiały szkoleniowe

Witamy w bibliotece zasobów kursu. Tutaj można łatwo uzyskać dostęp i pobrać materiały towarzyszące lekcjom, które mają na celu zapewnienie bezpośredniego wsparcia w nauce.

Dostępne zasoby

Dostępne zasoby



 Zgłoś Problem

Please note: while this document validates the technical deployment, fine-tuning, and multilingual translation of the platform, the comprehensive pedagogical analysis of the pilot training phase—including user feedback and learning outcomes—is thoroughly documented in Deliverable 5.3: CyberAgent upskilling Training Program Evaluation.



Co-funded by
the European Union

Get social with the project!



www.cyberagents.eu



contact@cyberagents.eu



[@Cyber-Agent-EU](https://www.linkedin.com/company/Cyber-Agent-EU)



[@CyberAgent.EU](https://www.facebook.com/CyberAgent.EU)



[@CyberAgentEU](https://twitter.com/CyberAgentEU)



[@Cyber.Agent.EU](https://www.instagram.com/Cyber.Agent.EU)



[@CyberAgentEU](https://www.youtube.com/CyberAgentEU)

Project Partners



Kaunas
Faculty



**TEKNOPARK
İSTANBUL**
Mesleki ve Teknik
ANADOLU LİSESİ

