



Co-funded by
the European Union

SUPPORTING DOCUMENT FOR THE D4.2 OPERATIONAL PLATFORM CYBER AGENT 12.2025

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.



Work Package 4: CyberAgent Collaboration Digital Platform

Deliverable 4.2: Operational platform

Leader of WP2 – Prios



“SMEs Cyber Security Change Agents” by Erasmus+ Project
“Operational platform” under
the Creative Commons licence CC BY-NC-SA

CONTENT

INTRODUCTION	2
1. LEARNING AND TRAINING ENVIRONMENT	2
2. CENTRALISED KNOWLEDGE REPOSITORY	6
3. COMMUNITY AND COLLABORATION HUB	10
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 CyberAgent online platform serves as a comprehensive digital hub designed to support cybersecurity capacity building, learning, and collaboration across education, training, and the SME sector. The platform integrates learning, knowledge sharing, and community engagement functionalities, enabling users to develop practical cybersecurity skills and strengthen organisational cyber resilience.

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:

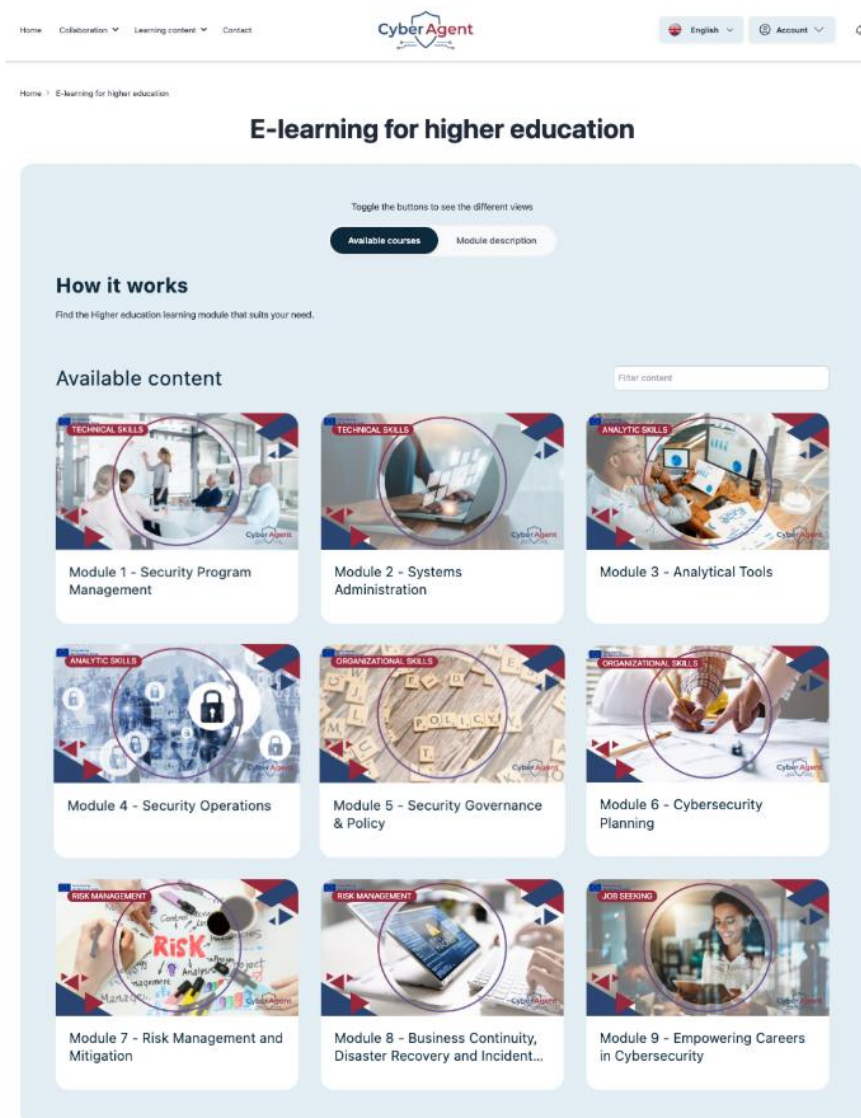
- Update existing digital competences in response to evolving cyber risks;
- Acquire new cybersecurity skills relevant to changing job roles and organisational demands;
- Strengthen transversal competences such as problem-solving, risk awareness, and responsible digital behaviour.

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 VET

Toggle the buttons to see the different views

Available courses

Module description

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 Recover...



Module 9 - Empowering Careers in Cybersecurity

2. CENTRALISED KNOWLEDGE REPOSITORY

The CyberAgent platform hosts a **centralised knowledge repository** that aggregates a wide range of **base**, 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				
SELECTING THE RIGHT SECURITY SOLUTIONS	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

Please do not change headers and footers: header must have two logos: Erasmus+ and CyberAgent logo; footer must have a ribbon and page number. Please include the delivery number and the name of the delivery in the footer. The text must be in capital letters.

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.


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



English

Account

[Home](#)
[Blogs](#)
[Why a Human Firewall is Your Best Defense](#)



By: [Weishan](#)

Added 19 September 2025

Why a Human Firewall is Your Best Defense

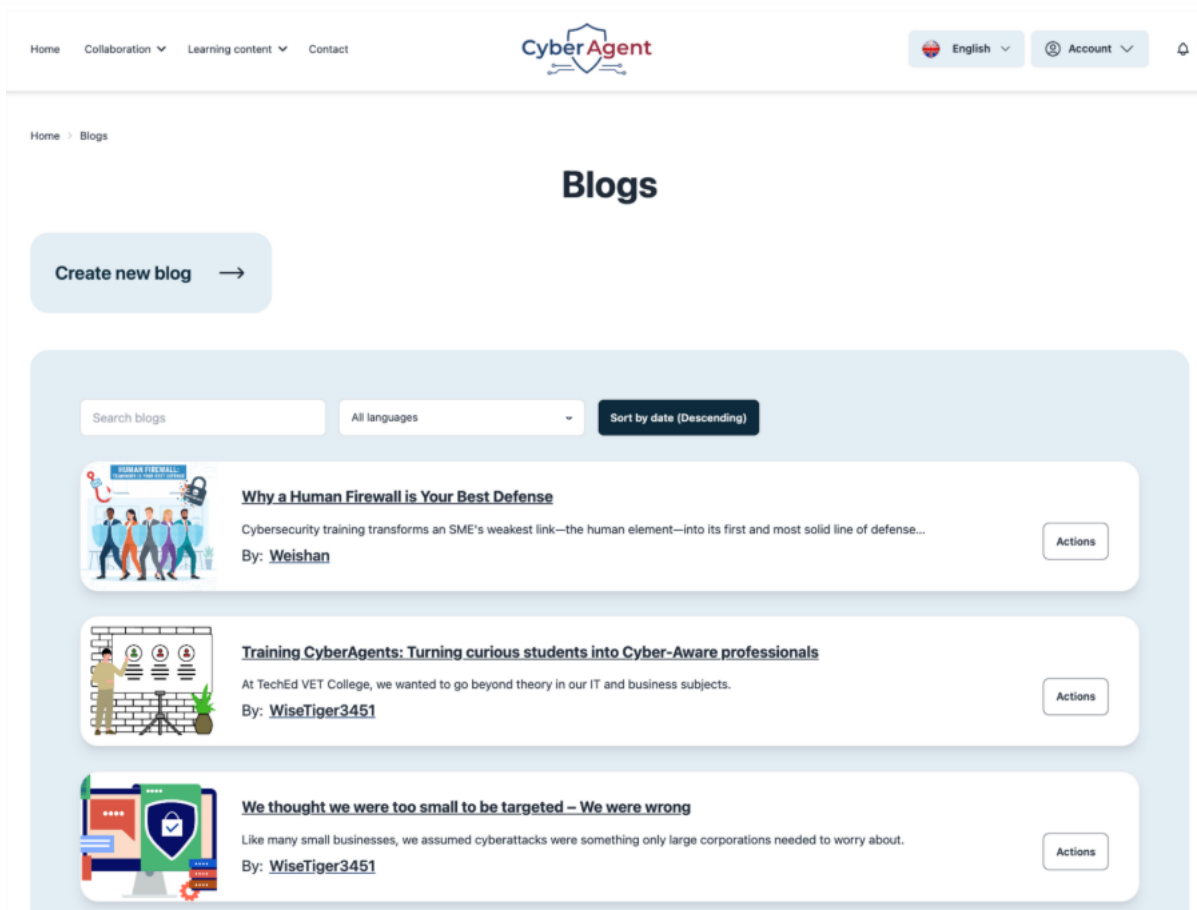
Many small businesses wrongly assume they're safe from cyberattacks. In reality, **SMEs are prime targets**. While technical defenses like firewalls are crucial, human error is a significant vulnerability. A single click can bypass all security and cripple operations. Cybersecurity training for your team is essential for survival.

Hackers prey on SMEs due to weaker defences compared to large corporations. Over half of all cyberattacks target small businesses using methods like Phishing, Ransomware, and Business Email Compromise (BEC), all relying on human error. Without training, employees can unknowingly grant access to your network.

Employees often make mistakes like using simple passwords, clicking malicious links, or using unsecured Wi-Fi. The good news is that training can turn employees into a "human firewall," spotting and reporting threats before they cause damage.

For large companies, a breach is a setback; for SMEs, it's an existential threat. Consequences include crippling financial damage, irreparable reputational harm, and complete business disruption. Around 60% of small businesses fail within six months of a major cyberattack. Proactive training is far cheaper than recovering from a disaster.

Cybersecurity training is a smart investment, fostering a **"culture of security"** where security becomes a shared responsibility. Employees learn to question before clicking, share threat intel, and maintain sharp defenses. This collective vigilance protects data, finances, and customer trust.



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

CyberAgent
English
Account

Home > Profile

Profile

Information

No social links added

Username: [redacted]

Organisation: Organisation not added

Gender: Female

Country: Norway

User type: SME

Account role: [redacted]

[Change password](#)

EDIT INFORMATION

Skills

product comprehension [Delete](#)

project management principles [Delete](#)

JavaScript Framework [Delete](#)

ADD SKILL

My experiences

[Delete](#)

Project supervisor at Prios Kompetanse

Full-time (Current)

01/07/2024 - Present

Steinkjer, Norway (Hybrid)

ADD EXPERIENCE

Interests

Cooking





Design

Writing

EDIT INTERESTS

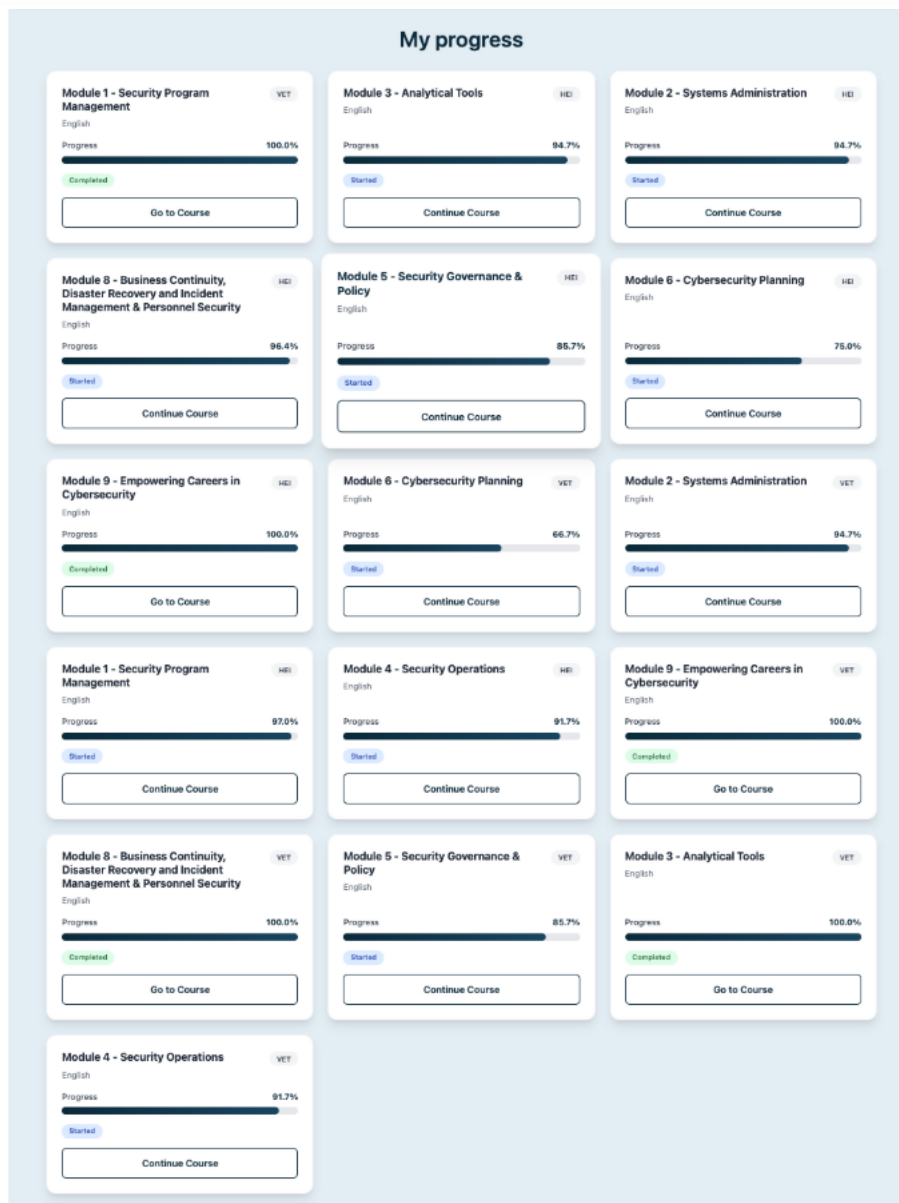
My badges

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.

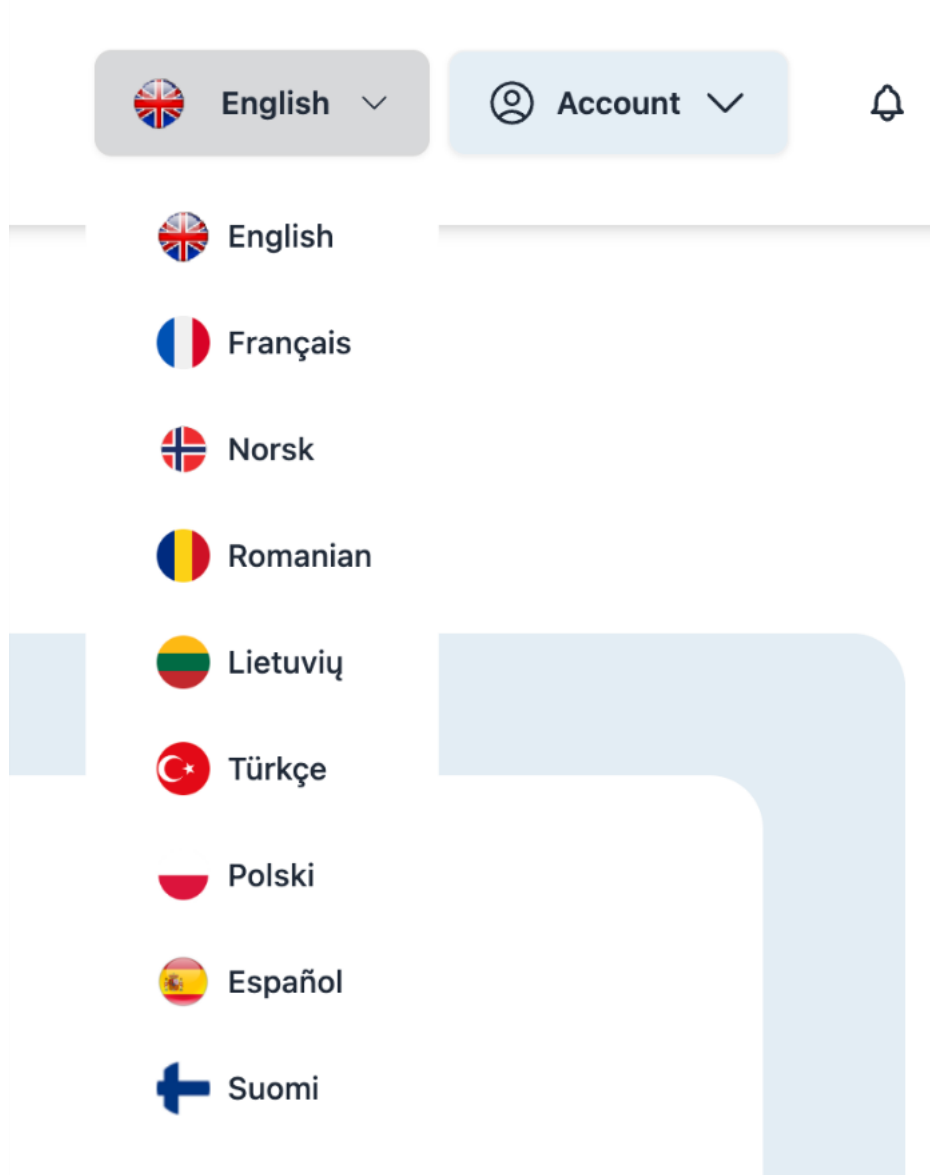
By recognising linguistic diversity, the platform promotes fairness and inclusivity in digital education.

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.





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

