Co-funded by the European Union

SME CYBER SECURITY CHANGE AGENTS LEARNING PATHWAY'S STRUCTURE

CYBER AGENT 06.2024

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 2: CyberAgent approach and structure design

Deliverable 2.3: SME Cyber Security Change Agents learning pathway's structure

Leader of WP2 – Olemisen Balanssia ry
Leader of deliverable 2.3 – Vilnius University

CONTENT

ABBREVIATIONS

CBL – Challenge-Based Learning Model

CL – Cooperative Learning Model

EC – European Commission

ECTS – European Credit Transfer and Accumulation System

EQF – European Qualifications Framework

GICL – Guided Inquiry Collaborative Learning Model

HEI – Higher Education Institutions

PBL – Project-Based Learning Model

POGIL – Process Oriented Guided Inquiry Learning Model

SME – Small and Medium Enterprises

VET – Vocational Education Institutions

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

The general aim of this report is to develop and describe new professional learning pathways for upskilling cybersecurity skills among European SME (Small and Medium Enterprises) employees.

Based on the findings from the mapping of the training needs for SME Cyber Security Change Agents, external resources analysis of the learning outcomes in terms of knowledge skills and competencies were identified. Following the analysis of the identified learning outcomes, this report provides guidance on two types of training curriculum from EQF (European Qualifications Framework) level 4 to 6 to cover the range of skills and knowledge required for the project target groups, SME employees and students, and adapt the training outcomes to the different backgrounds and profiles of the trainees.

- The EQF level 4-5 will be implemented for SME employees not having HEI background as well as VET (Vocational Education and Training) studies. This level will provide the cybersecurity foundational skills and knowledge with light specialisation in some modules.
- The EQF level 5-6 which will be an offer for SME employees who also have adequate background to follow it and HEI (Higher Education Institutions) students. At that level, more advanced and complex training activities will be performed.

It was decided to update the EQF levels to 4-6 not only to cover a broad range of learning outcomes as previously mentioned but also to enable a gateway between the training's curriculums as an upskilling pathway for VET students and employees at level 4 to reach the level 6.

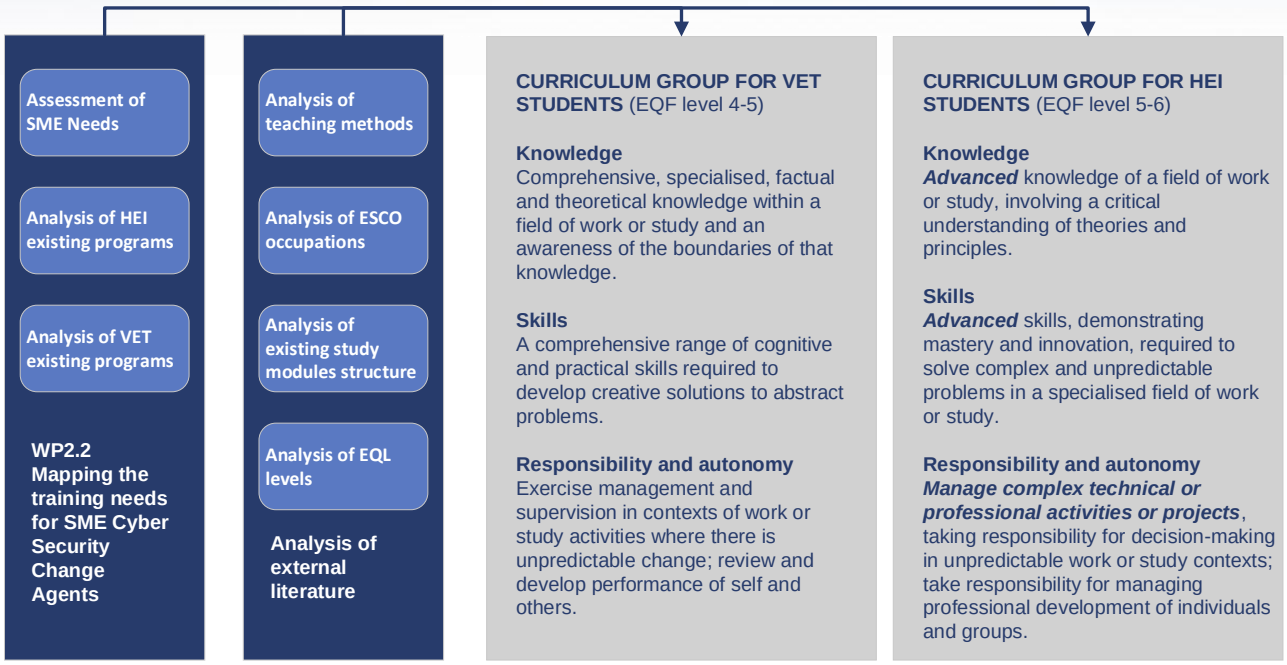

Figure 1. An illustrative diagram, adhering to EC guidelines, depicts the eight EQF levels, providing a visual representation of the education framework.[1]

The curriculum addresses the learning outcomes and the need for training SME Employees to upskill themselves to fill the role of SME Cyber Security Change Agents and educating HEI and VET students to fill the role after study. Each curriculum comprises eight modules covering four subtopics:

- Technical skills - Updated knowledge of cybersecurity threats and related legal issues - Practical knowledge of how to deal with cybersecurity threats.
- Analytic skills - Critical thinking mindset - Ability to analyse and understand local threats, how they happen, people at risk, etc.
- Risk management - Learn to provide and describe SME workplaces with cybersecurity routines - Create your own workplace SME handbook for cybersecurity and how to follow it up.
- Organisational skills - How to implement new routines and ways of working in cybersecurity at SME workplaces; Conducting leader support in cybersecurity.

In addition, a central part of creating the learning pathways for upskilling cybersecurity skills among European SMEs is how the micro-credentials will be implemented. They need to refer to learning outcomes (knowledge, skills, and competencies), course content, training (knowledge, skills, and competencies), gamification elements, duration, and number of ECTS (European Credit Transfer and Accumulation System). To fit the purpose, they need to be delivered through the establishment of partnerships between the HEIs with VET providers and private enterprises from the cybersecurity sector.

[1] https://europa.eu/europass/en/description-eight-eqf-levels

Micro-sections provide learners with more freedom to choose modules or parts of modules and to decide which level of certificate they need: certificates of participation or course completion certificate with certification test, i.e. proof that the course has been completed with the acquisition of a specific competence. Course completion certificates are issued for passing the final test with a score of at least 75%, and certificates of participation are issued for attending face-to-face, blended learning or online training in specific topics/modules. This practice not only increases the applicability and effectiveness of the training, but also stimulates motivation for learning, providing a clear value perspective for the participants' careers and further development.

Overall, this report outlines detailed guides for the development of CyberAgent modules, including the content outline of study and carrier pathways, the training and assessment methodologies, and the curriculum building roadmap.

1. STUDY PATHWAY

A learning pathway is an entire journey that participant takes from the moment he/she realises he/she needs to improve skills, start and complete training, to the moment he/she finishes learning and begin applying received knowledge. There are 3 stages in a learning pathway:

- Pre-learning,
- Learning,
- Post-learning.

The pre-learning stage is illustrated in the figure below.

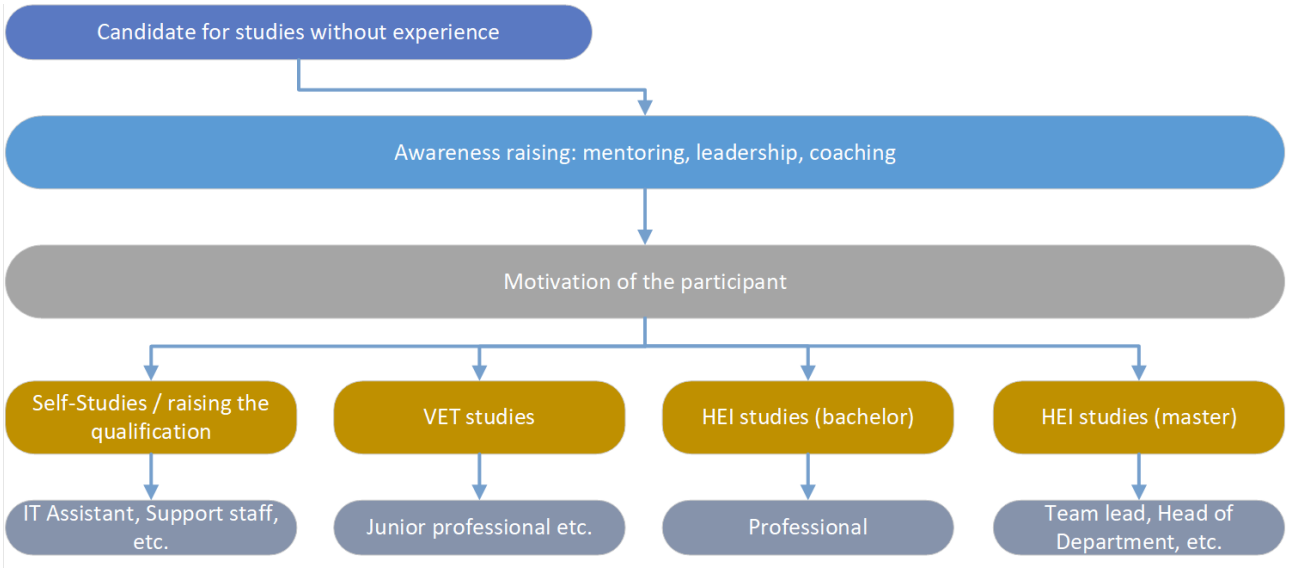

Figure 2. Learning pathway before studies start

In the context of SMEs, this learning/study pathway can be pursued. In the figure, the participant either decides to train himself or is influenced by an awareness-raising campaign and gains an understanding of the benefits of the training, the opportunities and the careers that can be acquired after the training.

Learning pathway as typical module via OLE (Online Learning Environment) structure has also been proposed. After a literature analysis and several projects applying the micro-credentials principle[2],[3],[4] each CyberAgent module is proposed to be 1-5 ECTS (each ECTS is 25-30 hours of workload) and starts with an introduction and is then divided into themes, which are sub-topics.

[2] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Moving Forward and Beyond in Education: Concept of FLEXIBLE LEARNING PATHWAYS. In KTU leidykla "Technologija" eBooks. https://doi.org/10.5755/e01.9786090218204

[3] https://arqus-alliance.eu/call/arqus-microcredential-development-f2f-workshop/

[4] https://www.youtube.com/watch?v=ECH0VvHIyRI, https://ndma.lt/alta2023/

At the end of the topics, a self-assessment test consisting of several questions is given. The training materials of the module should support the study of 6-8 topics, in each of which there are 4-6 subtopics. The course may conclude with a knowledge test, which is not compulsory. This gives SME employees and students of training institutions the possibility to acquire and demonstrate the competences learned in a specific module or part of the training.

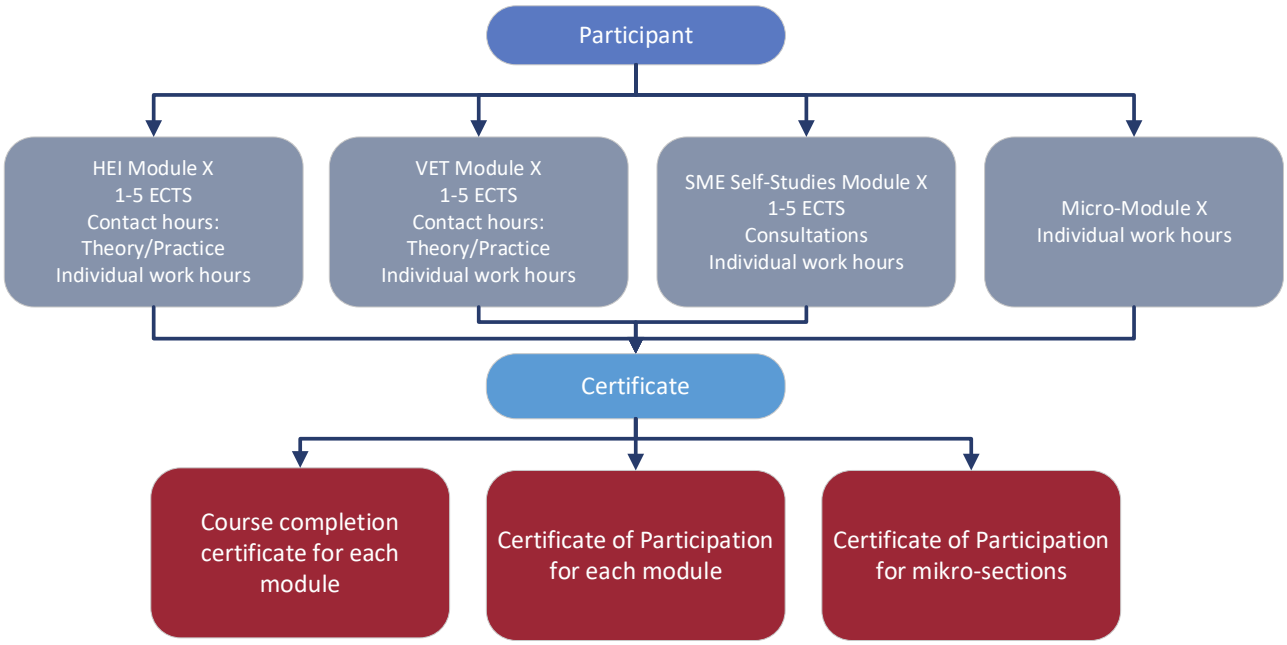

Figure 3. Studies structure

Micro-credentials are integrated into the learning process through the following key activities:

- Development of training modules: each module has to be carefully formulated taking into account the specific knowledge and skills required in the SME sector, with clear objectives, learning outcomes, teaching and learning methods, course duration.
- Practical tasks and projects: learners carry out practical tasks and develop projects which are assessed and provide clear evidence of the skills acquired.
- Clearly described knowledge assessment strategy and evaluation criteria: at the end of each module, a knowledge assessment is organised to determine whether the participant has achieved the required learning outcomes and whether they are eligible for a certificate to prove it.

As the target group of the project is SME employees, HEI and VET students, four types of studies are available, according to the learners' possibilities and needs:

- HEI studies: 8 modules, each 1-5 ECTS, where there are contact hours (theory and practice) and individual work hours;
- VET studies: 8 modules, each 1-5 ECTS, where there are contact hours (theory and practice) and individual work hours;

- Self-Studies (for SMEs): 8 modules, each 1-5 ECTS, where there are consultations (if needed) and individual work hours;
- Micro-modules: individual work hour depending on the number of chosen topics.

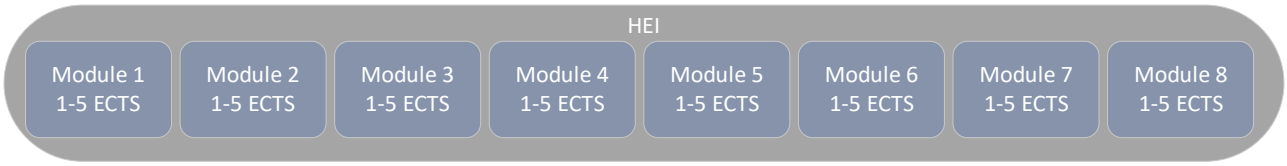

Figure 4. Studies structure for HEI

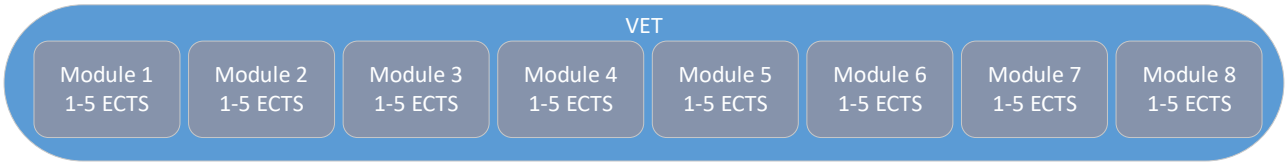

Figure 5. Studies structure for VET

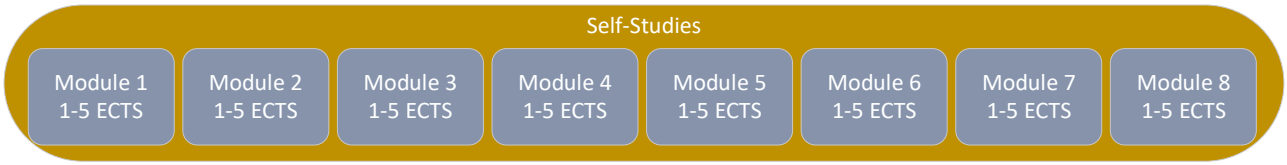

Figure 6. Studies structure for Self-studies

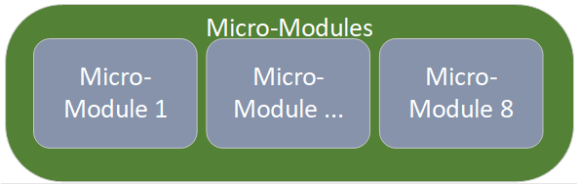

Figure 7. Studies structure of Micro-module

HEI and VET students will be able to study one module of 1-5 credits each. SMEs will be able to take one module at a time, or we may be able to offer microsections as part of the course.

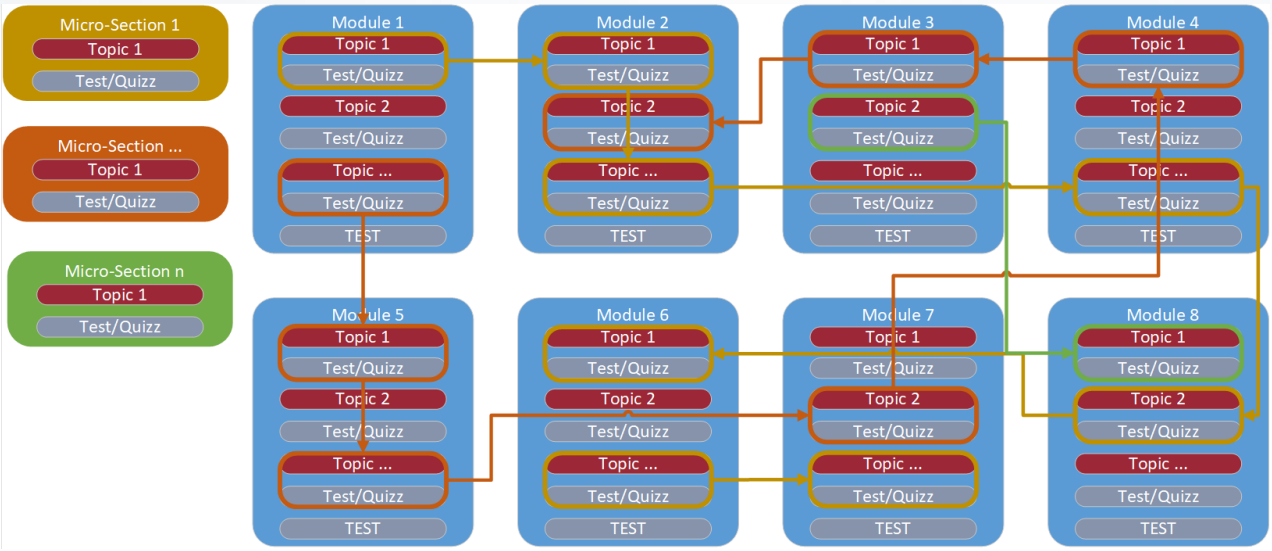

Figure 8. Learning pathways linkages

In all three (HEI, VET, SMEs) learning types, student studies 8 modules. In case Micro-modules, student choses modules by their own choice.

Micro-modules are short or long transparently assessed learning experiences. They are taken by the participant together with the challenge or separately. Each micro-module is valued with a different amount of learning workload measure (such as ECTS) and finishes with assessment. Successful completion of micro-module assessment rewards learners with micro-credentials.

Proposal is that each module from the HEI program can be modularized into one micro-module, each featuring specialized assignments and a detailed plan of implementation. Tests results can be assessed through badges, which are image-based and universally readable by computers. These images embed metadata detailing the competencies associated with each badge and information about the participant who holds it.

Micro-credential means the record of the learning outcomes that a participant has acquired following a small volume of learning. These learning outcomes will have been assessed against transparent and clearly defined criteria. Learning experiences leading to micro-credentials are designed to provide the participant with specific knowledge, skills and competencies that respond to societal, personal, cultural or labour market needs[5,6].

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Moving Forward and Beyond in Education: Concept of FLEXIBLE LEARNING PATHWAYS. In KTU leidykla "Technologija" eBooks. https://doi.org/10.5755/e01.9786090218204

[6] Council Recommendation of 16 June 2022 on a European Approach to Micro-Credentials for Lifelong Learning and Employability." Official Journal of the European Union, vol. 2022/C, 16 June 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=EN

2. CAREER PATHWAY

Post-learning pathway could be called carrier pathway. In the beginning of the project the research analysis of ESCO occupations (Described in the report: D2.2 - The SME Cyber Security Change Agents Training needs mapping report) was done. The analysis conducted in three phases aimed to investigate various cybersecurity occupations listed within the ESCO framework. In the first phase, occupations related to cybersecurity were identified and documented from the **ESCO portal**, highlighting their respective skills, competencies, and knowledge. These occupations included roles such as chief ICT security officer, digital forensics expert, embedded systems security engineer, ethical hacker, ICT resilience manager, ICT security administrator, ICT security engineer, ICT security manager, and knowledge engineer. Each occupation was defined by its specific responsibilities and focus areas within the field of cybersecurity, ranging from corporate security functions to digital forensics, ethical hacking, and resilience planning.

In the second phase, a table was filled out for each reviewed ESCO occupation, detailing its title and core responsibilities. These included tasks such as planning and implementing security measures, conducting vulnerability assessments, developing models for resilience and disaster recovery, and integrating knowledge into computer systems.

Additionally, the third phase involved mapping the ESCO occupations with associated learning outcomes, categorizing them into knowledge, skills, and competences. This process facilitated a comprehensive understanding of the educational requirements and expected proficiencies for each cybersecurity role, ensuring alignment with industry standards and best practices. Through these phases, the analysis provided valuable insights for the further research.

Figure 9. ESCO occupations defined in previous report

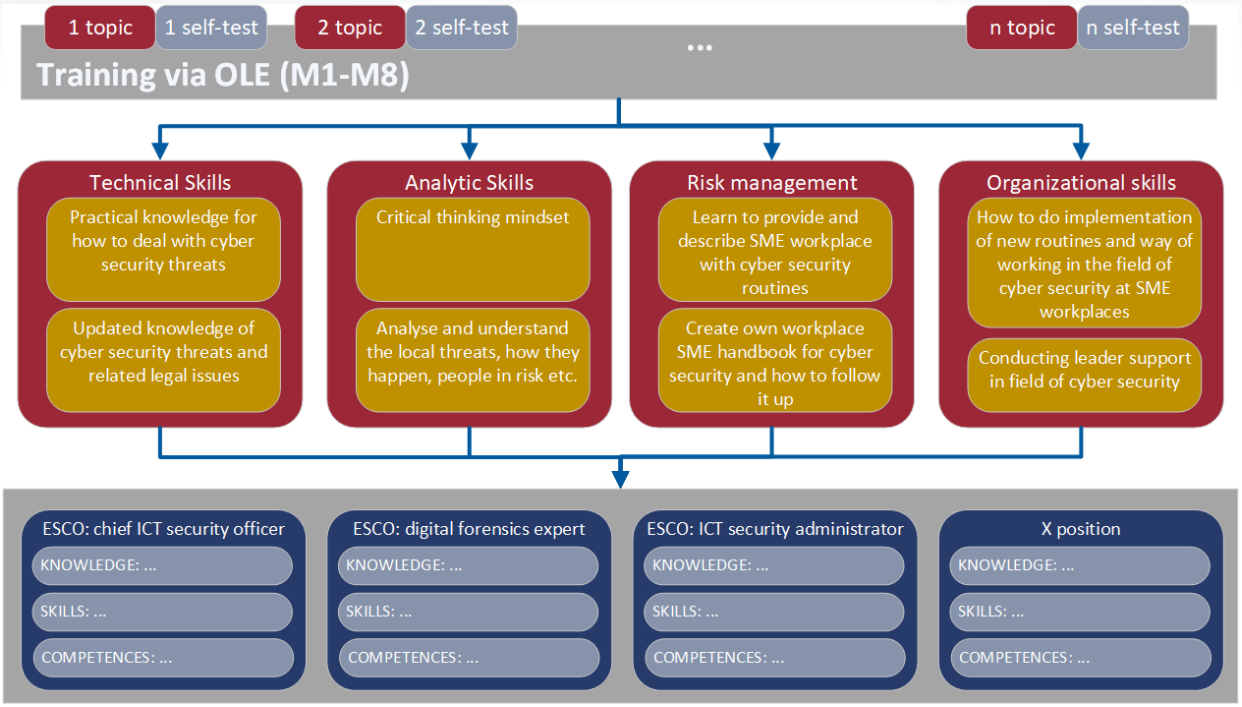

Figure 10. Possible post-Learnings pathways

Figure 10 illustrates potential career pathways that can be pursued after completing of studies via OLE (Online learning environment) (HEI, VET, SME) and acquisition of skills, as aligned with ESCO occupations.

With a clearer understanding of career opportunities, HEI and VET students studying cybersecurity will gain a clearer understanding of career options and be able to choose a further field of study or to work in companies in specific positions, while IT and other students will be able to choose CyberAgent modules as individual study modules, thus enhancing their field of study competences, such as organisational and risk management skills, etc.

SMEs staff will have the opportunity to upskill and develop their workplace competences. Based on the career path that has been developed and with clear career opportunities, other SME staff will be able to retrain in the field of cybersecurity.

Increased involvement of both students and SME staff is planned through the integration of mentoring schemes, the organisation of dissemination events, workshops (the project includes 6 joint workshops organised by all partners, as well as dissemination campaigns organised by each partner), inviting business and cybersecurity representatives, cooperation with social partners and the CyberAgent network, offering internships to students, etc. Furthermore, our diversity initiatives, including targeted outreach and support programs, aim to bolster the participation of women, fostering an inclusive cybersecurity workforce.

By comprehensively mapping ESCO occupations to our CyberAgent training modules, participants can seamlessly transition from learning environments to impactful roles in cybersecurity. In order to follow the career development of CyberAgent trainees, it is planned to organise pre-training, post-training and 3-month post-training surveys to find out how their skills

contribute to the cybersecurity of the organisations they work in. The surveys will be integrated into the training platform and will be offered automatically to the trainees before the beginning of the course, at the end of the course to measure progress and to evaluate the course and the quality of the training. A third survey will be used to find out if there have been any changes in the participants' careers.

3. TEACHING METHODS

The analysis of the pedagogical methods of the Information Systems and Cyber Security study programme of Vilnius University (VU), the Timtal and Moisil Buzau study programmes and external literature enables us to recommend several innovative combinations of teaching methods. These combinations could be included in the study modules, taking into account the structure of each module.[7]

Table 1. Recommended teaching methods

Category	Detailed information
Lecture and direct instruction	- **Theoretical lectures:** fundamental concepts and theories. - **Guest speakers** ((certified specialists in: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), CompTIA Security+, Certified Ethical Hacker (CEH), GIAC Security Essentials Certification (GSEC), Systems Security Certified Practitioner (SSCP), CompTIA Advanced Security Practitioner (CASP+), GIAC Certified Incident Handler (GCIH), Offensive Security Certified Professional (OSCP))).

Practical and hands-on learning	- **Practical Tasks/Labs:** hands-on experiments and practical exercises.
	- **Hands-On Activities**: real-world applications and interactive tasks.
	- **Technical Video Analysis:** analysis of video content for learning technical skills.
	- **Simulated Environments**:
	  o Hosted machines for cloud environment.
	  o Launch attacks on a target machine.
	  o Machine for planning and performing attacks – an attack box.

[7] Teaching Cybersecurity: A Project-Based Learning and Guided Inquiry Collaborative Learning Approach https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses

Category	Detailed information
Assessment and evaluation	- **Quizzes, Games, Dos and Don'ts**: Engaging and interactive assessments. - **Self-Assessment Tests**: For learner's self-evaluation at the end of topics.
Self-studies	- **Self-guided learning:** this method supports personalized learning paths and can be enhanced with digital resources and modular content that students can access as needed.
Collaborative and peer learning	- **Collaborative Learning, Teamwork**: group projects and collaborative tasks. - **Peer-to-Peer teaching and learning**: learners teach and learn from each other. - **Group mentoring and/or individual mentoring**: guidance provided by more experienced individuals.
Technology-enhanced learning	- **Usage of gamified cybersecurity learning platform**: engaging learners through game-like elements in learning platforms. - **Capture the flag competitions**: competitive events to enhance cybersecurity skills. - **Competitions**: competitions test students' skills and knowledge in a practical, applied setting and provide a measure of their competencies in a competitive format.
Community and public engagement	- **Educational events:** special events during initiatives like Cybersecurity Month. - **Public presentations**: seminars, conferences, and webinars. - **Social networking**: use of social media and networks for learning and engagement. - **Day Campus**: typically involves immersive, campus-based events that can include workshops, lectures, and networking opportunities

Category	Detailed information
Innovative learning models	- **BSCS 5E Instructional Model (5Es)** – the 5Es focuses on the following phases that consists of: Engagement, Exploration, Explanation, Elaboration, Evaluation. - **Challenge-Based Learning Model (CBL)** – an early implementation of CBL provides a framework that consist of six phases: Describe the challenge, Generation and brainstorming of ideas, review multiple perspectives that questions and support, Research and revise for best solutions, Test hypothesis, Share the findings and conclusions. - **Cooperative Learning Model (CL)** – similar to the 5Es and CBL models, Cooperative Learning promotes active learning in small groups and students receive a reward based on their performance that may include a grade, a tangible reward like a certificate or scholarship, or approval from a teacher. - **Project-Based Learning Model (PBL)** – project-Based Learning and Problem-Based Learning use the same abbreviation of PBL and are both focused on improving problem-solving, critical thinking, teamwork, communication, and creative skills; however, they consist of different phases., Independent and group research, Develop and present, Analyze and evaluate process. - **Process Oriented Guided Inquiry Learning Model (POGIL)** – this approach guides students through the exploration of a concept; followed by concept invention where students synthesize and explain the concept; and closes the learning cycle with the application of the theoretical concept. - **Guided Inquiry Collaborative Learning Model (GICL)** – this is a new approach largely based on the POGIL model.

In order to ensure that the various training strategies offered have the best possible impact, each approach will be selected and aligned with the specific learning objectives of the cybersecurity modules in the development of a comprehensive module syllabus and training materials.

Additional methods may also be chosen by the lecturers/mentors who will be delivering the CyberAgent training. During the development phase of the training materials, training will be provided to the instructors of the pilot trainings to inform them about the objectives, process and responsibilities of the training, and to prepare them to effectively teach the CyberAgent curriculum. The pilot training process also includes the collection of feedback from learners and trainers in order to monitor the effectiveness of the training methods used and to make adjustments where necessary.

Modules will be held in different teaching formats:

- in **remote format**,
- in **synchronous learning** (full support of teacher),
- and in **asynchronous learning** (support of teacher when needed), blended learning and self-learning.

As different ways of delivering the training are envisaged, the training methods are presented at this stage as guidelines.

4. MODULE STRUCTURE

The analysis of the module structure of the VU Cyber security study programme, the analysis of the module structure of international projects (**CyberPhish**, **FuseIT**, **dComFra**), and the analysis of the module structure of commercial platforms, such as **Udemy** and **Coursera**, has led to the creation of a typical module structure that could be applied to both HEI and VET modules.

Main goal is to develop 8 modules, where 8 modules would be for HEI students (EQF level 5--6), for VET students and SMEs (EQF level 4-5) and micro-modules for all type of students.

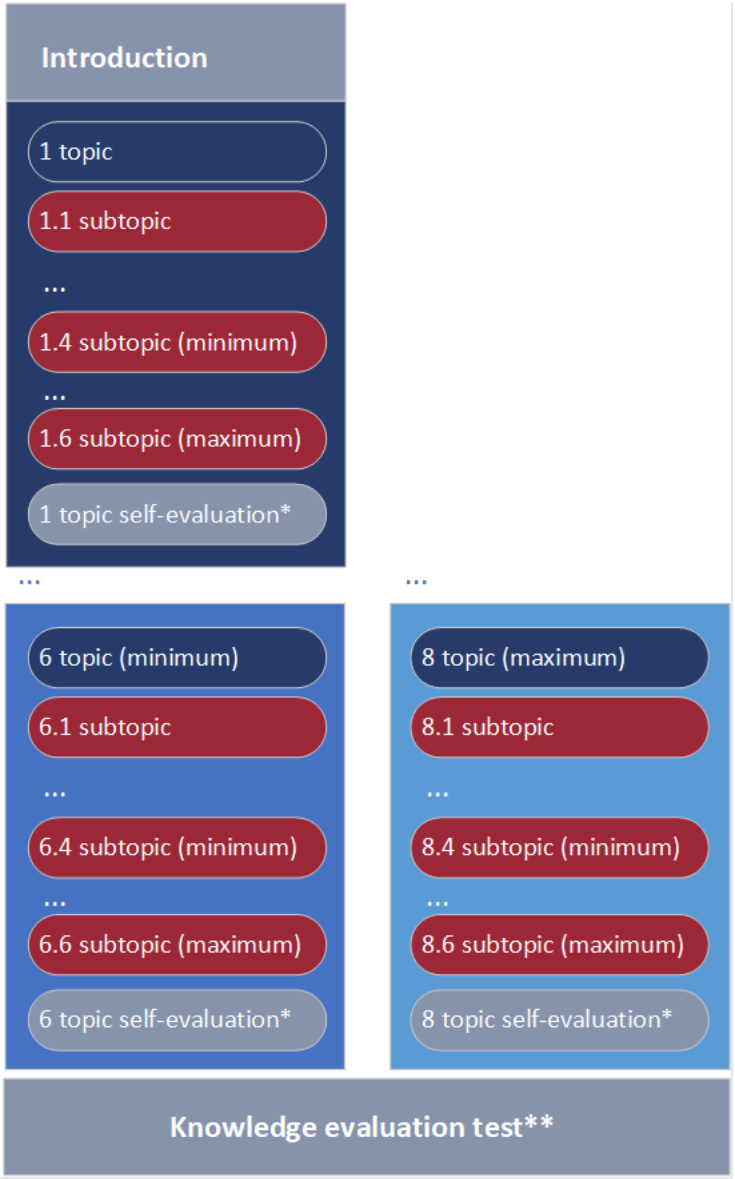

Figure 11. Module Structure

* It is recommended that each subtopic is followed by self-test (self-reflection) questions. However, at the module development stage, a different assessment method or option may be

chosen depending on the type of study chosen, e.g. students may be given practical exercises, simulations, etc., while self-test questions are offered to independent learners.

** A knowledge assessment test is optional. If the learner wishes to obtain a course completion certificate to verify the knowledge acquired, this test is compulsory. However, the learner has the option of obtaining a course completion certificate to prove that he/she has attended the training, in which case this test is optional.

To ensure that each training module is directly linked to practical applicability, the description of each module will provide clear examples of how the theory is applied in practice. This includes not only detailed scenarios for the applicability of the modules, but also specific tasks that students will undertake to consolidate the theoretical knowledge in real cybersecurity situations.

Each module should provide Technical skills, Analytic skills, Risk management skills, Organizational skills with different proportions. Self-assessment test is provided to test learners' knowledge at the end of any part of the module (topic). This not only allows for the assessment or evaluation of the knowledge acquired, but also the learner's progress is recorded and the participant collects points and badges, which allows the participant to be more involved in the learning process.

Following ECTS formalities where each ECTS is 25-30 hours of workload. According to this each module could be equal to 5 ECTS. Hours of workload could be distributed this way:

Table 2. Hours of workload

	Number of modules	Total of ECTS	Remote hours for theoretical skills	Remote hours for practical skills	Individual work hours	Total hours of workload
Modules for HEI students (EQF level 5-6)	8	8-40	20%	20%	60%	200-1200
Modules for VET Students (EQF level 4-5)	8	8-40	15%	25%	60%	200-1200
Self-studies (blended learning)	8	8-40	10%		90%	200-1080
Self-studies (online)	8	8-40				200-1200
Micro-modules	1-8	1-40				25-1200

Table 3. Recommended modules workload

Module	ECTS	Total hours	Contact hours	Contact hours (theory)	Contact hours (practice)	Individual work hours
HEI Module title	1-5	25-150	40%	20%	20%	60%
VET Module title	1-5	25-150	40%	15%	25%	60%
Self-studies (blended learning)	1-5	25-150	10%			90%
Self-studies (online)	1-5	25-150				100%
Micro-sections						10%-100%

Each module should have its own description. After analysis of the VU, Timtal and other programmes using micro-credentials, a typical module structure is proposed for each CyberAgent module (an example of a typical module structure is given in Annex 1).

Table 4. Typical structure for CyberAgent modules

Category	Detailed information
Module identification (basic information about module)	- Module title - Module code - Lecturer - Institution or department where module is delivered - Model of delivery - Language - Prerequisites
Module duration and workload (clearly time commitment and structure outline)	- Total duration (number of ECTS) - Student workload in hours - Contact work hours - Individual work hours

Educational goals and learning outcomes (details about what the module aims to achieve and what students will learn)	- Purpose and outcomes of the module
	- Learning outcomes
	  o Technical skills
	  o Analytic skills
	  o Risk skills
	  o Organization skills

Teaching and Learning Methods	- Teaching and learning methods
Assessment and Evaluation (explanation on how students will be assessed)	- Assessment methods - Tasks (labs, projects, presentations, reports, etc.) - Assessment strategy, assessment criteria
Facilitate resources	- Equipment, Software and Technology
Course content	- Module topics and subtopics
Resources	- List of sources - Additional sources

Each ECTS is considered 25-30 hours (contact or online hours + individual studying).

The module should have at least a two-level hierarchy:

- **The first level of the hierarchy** – topics. At this level, the main elements of the module could be introduction, entrance test, final test, and the base element – topic.
- **The second level of the hierarchy** – subtopics, the main educational elements of the module.

Each module at the first level of the hierarchy should include:

- **INTRODUCTION** to the module (textual description, video introducetion): relevance and benefits of module, base aims and outcomes of the module, required software and hardware, requirements for participants.
- **TOPICS** – main topics of the course, theoretical material and theoretical teaching methods.
- **SUBTOPIC** – subtopic of each topic, practical, analytical analysis and tasks, practical and analytical teaching methods. Topics and subtopics may include textual information, videos, audio clips, presentations, links to further reading.
- **MODULE Intro test** (if needed). The intro test on the intermediate and advanced levels should confirm that the applicant has mastered enough knowledge & skills at the previous levels.
- **MODULE acknowledgement tests**. Acknowledgement test should provide objective verification of a student's skills and demonstrate their competency to the module requirements.
- **GUIDELINES for mentors / teachers**. This document should contain methodological recommendations for mentors / teachers on the use of module educational elements.

Each TOPIC at the second level of the hierarchy should include:

- **INTRODUCTION** to the topic aims and outcomes, short content.
- **SUBTOPICS**: all the necessary educational elements to support the student to master the relevant skills.
- **TOPIC test**: brief recommendations for mentors / teachers on the module implementation and application. Each SUBTOPIC should consist of educational elements, whose contents correspond to the tasks of the module description. Each subtopic may (should) include a Subtopic TEST, confirming that the student has mastered the relevant skills on a high enough level.

The training materials of the module should support the study of 6-8 topics, in each of which there are 4-6 subtopics and, as minimum, one topic test. So, module should contain (approximately) 30-40 educational elements (methods described in section teaching methods) and 6-8 tests and one module final acknowledgment test.

5. CYBERAGENT CURRICULUM AND TRAINING PROGRAMME

Curriculum building roadmap

CyberAgent Curriculum and a Training Programme follows Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, developed by the joint task force of ACM, IEEE, AIS SIGSEC and IFIP (2017)[8] (hereinafter – **Guidelines**). More specifically, since the general focus of CyberAgent project is to increase inhouse cybersecurity competences of European SMEs, the curriculum follows framework of Organizational Security knowledge area, as recommendations by these Guidelines.

That said, the first step in curriculum building is to map pre-defined subtopics and modules in CyberAgent project with the knowledge units and key topics, recommended and described by the Guidelines (p. 59-70). The mapping is based on the logical correlation between these two pillars, as discussed and agreed by the project partners.

The second step is to assign specific learning outcomes, identified and described from the T2.2 "Mapping the training needs for SME Cyber Security Change Agents" with the knowledge unit and key topics, mapped above. It shall be noted herein that different occupation related to cybersecurity may have a variety of different knowledge, skills and competences, as eloquently mapped in abovementioned T2.2 deliverable. However, below provided proposal reflects the CyberAgent expected set of knowledge, skills, and competences, which may be adapted to the specific needs of specific occupations or trainee groups.

Having that said, the results of this curriculum building exercise are provided in Table 5 below.

[8] The Joint Task Force on Cybersecurity Education. (2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity: A Report in the Computing Curricula Series. Association for Computing Machinery, 31 December 2017. Available at: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf [Accessed 3 March 2024]

Table 5. Curriculum building roadmap

Subtopics and Modules	Knowledge Unit and Key Topics	Learning outcomes HEI	Learning outcomes VET
Technical skills			
- **Updated knowledge of cybersecurity threats and related legal issues**	**Security Program Management** - Project management - Resource management - Security metrics - Quality assurance and quality control	**Knowledge**: Learners will gain advance knowledge of advanced cybersecurity principles including sophisticated cyber threats and attack vectors, national and international cybersecurity legislation, standards, and compliance requirements relevant to their industry. **Skills**: Learners will be skilled to design and implement advanced risk assessment and management strategies to mitigate identified risks, using advanced methodologies and tools. **Competences**: Learners will be competent to lead and manage cybersecurity projects and teams implementing strategic cybersecurity policies and frameworks aligned with the organization's objectives and compliance obligations.	**Knowledge**: Learners will gain practical knowledge on the latest cybersecurity threats, including phishing, ransomware, and DDoS attacks, and how to manage these through effective project and resource management, and implementation of quality assurance and control measures. **Skills**: Learners will be skilled to utilize tools and software for protection against evolving cyber threats, and apply robust security practices in project and resource management to enhance the overall security metrics and quality control within their organizations. **Competences**: Learners will be competent in assessing and mitigating potential security threats, effectively communicating cybersecurity issues, and accurately reporting threats and breaches through the appropriate channels within their organization.

- **Practical knowledge for how to deal with cybersecurity threats**	**Systems Administration** - Operating system administration - Database system administration - Network administration - Cloud administration - Cyber-physical system administration - System hardening - Availability	**Knowledge**: Learners will gain advance knowledge in operating, database, network, cloud, and cyber-physical systems administration, and other areas, enabling them to effectively harden systems and ensure availability while applying the latest cybersecurity defense mechanisms. **Skills**: Learners will be skilled to use advanced methodologies and tools to design and implement secure system architectures—including operating systems, databases, networks, and cloud infrastructures **Competences**: Learners will be competent to develop and implement strategic cybersecurity frameworks for system administration, leading projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains.	**Knowledge**: Learners will gain practical knowledge on how to administer and secure operating systems, databases, networks, clouds, and cyber-physical systems against common cyber threats like phishing, ransomware, and DDoS attacks, while implementing effective risk management policies. **Skills**: Learners will be skilled to in identifying potential cybersecurity risks and vulnerabilities across various system platforms, using specialized tools and software to enhance system hardening and availability, and implementing basic cybersecurity practices such as secure password creation, safe browsing, and secure handling of sensitive data. **Competences**: Learners will be competent in assessing and mitigating security threats within system administration, effectively communicating cybersecurity issues, and promptly reporting any threats and breaches to the appropriate organizational channels.

Analytic skills			
- **Critical thinking mindset**	**Analytical Tools** - Performance measurements (metrics) - Data analytics - Security intelligence	**Knowledge**: Learners will gain advance knowledge of national and international cybersecurity legislation, standards, and compliance requirements, and others relevant to their specific industry. **Skills**: Learners will be skilled to use performance measurements, data analytics, and security intelligence to design and implement effective risk management strategies. **Competences**: Learners will be competent in using analytical tools to develop strategic cybersecurity policies with a critical thinking mindset, and make decisions in cybersecurity practices aligned with organizational objectives and compliance obligations.	**Knowledge**: Learners will gain practical knowledge in how to apply performance measurements, data analytics, and security intelligence to protect organizational assets. **Skills**: Learners will be skilled in using analytical tools to identify potential cybersecurity risks and vulnerabilities, apply data-driven insights to strengthen cybersecurity practices, and utilize performance metrics to evaluate and enhance the security of passwords, browsing, email, and data handling. **Competences**: Learners will be competent in assessing and mitigating potential security threats using analytical tools, accurately reporting threats and breaches to the appropriate channels within their organization.
- **Analyse and understand the local threats, how they happen, people in risk etc.**	**Security Operations** - Security convergence - Global security operations centers (GSOCs)	**Knowledge**: Learners will gain advance knowledge in local cyber threats, using insights from global security operations centers and current trends in cybersecurity defense strategies. **Skills**: Learners will be skilled to utilize advanced methodologies and tools within global security operations	**Knowledge**: Learners will gain practical knowledge of local cyber threats and their origins, assess how these threats impact organizational assets. **Skills**: Learners will be skilled to in identifying local cybersecurity risks and vulnerabilities, using tools and software such as secure password creation, safe

		centers to design effective risk management strategies, and develop plans to mitigate local cybersecurity threats effectively. **Competences**: Learners will be competent in developing and implementing strategic cybersecurity policies that address local threats through the use of global security operations centers.	browsing, and secure data handling tailored to their specific environments. **Competences**: Learners will be competent in assessing and mitigating local security threats using insights from global security operations centers, effectively communicating cybersecurity issues, and accurately reporting threats and breaches to the appropriate channels within their organization.
Risk management			
- **Learn to provide and describe SME workplace with cybersecurity routines**	**Risk Management** - Risk identification - Risk assessment and analysis - Insider threats - Risk measurement and evaluation models and methodologies - Risk control	**Knowledge**: Learners will gain advance knowledge of risk management processes, including risk identification, assessment, and control, enabling them to establish and describe effective cybersecurity routines tailored to the specific needs of SME workplaces in compliance with national and international standards. **Skills**: Learners will be skilled to apply advanced methodologies and tools to conduct comprehensive risk assessments, design and implement effective risk management strategies, and develop robust cybersecurity routines specifically tailored for SME workplaces.	**Knowledge**: Learners will gain practical knowledge in the processes of risk identification, assessment, and control, and risk management strategies to safeguard SME workplaces effectively. **Skills**: Learners will be skilled in identifying and analyzing potential cybersecurity risks within SME environments, using appropriate tools and software for threat mitigation, and promoting and implementing essential cybersecurity practices including secure password creation, secure browsing, and the safe handling of sensitive data. **Competences**: Learners will be competent assessing and mitigating security threats within SME workplaces,

		Competences: Learners will be competent in developing and implementing strategic cybersecurity policies for SME workplaces.	effectively communicating cybersecurity issues and procedures, and accurately reporting relevant threats and breaches to appropriate organizational channels.
- **Create own workplace SME handbook for cybersecurity and how to follow it up**	**Business Continuity, Disaster Recovery, and Incident Management & Personnel Security** - Incident response - Disaster recovery - Business continuity - Security awareness, training and education - Security hiring practices - Security termination practices - Third-party security - Security in review processes - Special issue in privacy of employee personal information	**Knowledge**: Learners will gain advance knowledge of how to create and implement a comprehensive SME workplace cybersecurity handbook, incorporating advanced cybersecurity principles, the latest defense mechanisms, and adherence to national and international legislation and standards in incident management, business continuity, and personnel security. **Skills**: Learners will be skilled to create and maintain an SME workplace cybersecurity handbook, using advanced methodologies to assess risks, design effective risk management and incident response strategies, and develop comprehensive business continuity plans tailored to their organization's needs. **Competences**: Learners will be competent in developing and implementing a cybersecurity handbook for SMEs, leading security projects and teams effectively, ensuring	**Knowledge**: Learners will gain practical knowledge in how to create a comprehensive SME workplace cybersecurity handbook that incorporates strategies for incident response, disaster recovery, business continuity, and personnel security, protecting organizational assets and sensitive data. **Skills**: Learners will be skilled to identify potential cybersecurity risks, utilizing tools and software to safeguard against threats, and applying best practices in cybersecurity to develop and maintain an SME handbook that addresses secure password creation, browsing, email security, and data protection. **Competences**: Learners will be competent in assessing and mitigating security threats, effectively communicating cybersecurity policies and practices, and systematically reporting security incidents within their SME, as outlined in their customized cybersecurity handbook.

		alignment with organizational objectives and compliance obligations.	
Organizational skills			
- **How to do implementation of new routines and way of working in the field of cybersecurity at SME workplaces**	**Security Governance & Policy** - Organizational context - Privacy - Laws, ethics, and compliance - Security governance - Executive and board level communication - Managerial policy	**Knowledge**: Learners will gain advance knowledge in how to implement new cybersecurity routines and workflows within SME workplaces, incorporating current cybersecurity principles, trends, and compliance with national and international legislation relevant to their industry. **Skills**: Learners will be skilled in using advanced methodologies to conduct risk assessments, design and implement new cybersecurity routines, and prepare response strategies, ensuring effective governance and compliance within SME workplaces. **Competences**: Learners will be competent in developing and implementing strategic cybersecurity policies, leading initiatives to establish new routines and workflows at SME workplaces, and making ethical decisions that align with organizational goals and compliance requirements.	**Knowledge**: Learners will gain practical knowledge in how to integrate new cybersecurity routines and practices within SME workplaces, in compliance with cybersecurity legislation, standards, strategies and policies for information security, risk management, and data protection. **Skills**: Learners will be skilled in applying cybersecurity tools and software to implement new security routines, identify and mitigate risks, and promote essential cybersecurity practices such as secure password creation, browsing, and data handling within the governance framework of SME workplaces. **Competences**: Learners will be competent in assessing and mitigating potential security threats, effectively communicating cybersecurity changes and policies, and accurately reporting security incidents within SMEs according to governance and compliance requirements.

- **Conducting leader support in field of cybersecurity.**	**Cybersecurity Planning** - Strategic planning - Operational and tactical management	**Knowledge**: Learners will gain advance knowledge in how to integrate advanced cybersecurity principles and current trends into strategic planning and operational management. **Skills**: Learners will be skilled in strategic planning and operational management, enabling them to effectively design and implement cybersecurity strategies that address emerging risks and ensure robust tactical responses. **Competences**: Learners will be competent in developing and implementing strategic cybersecurity frameworks, leading and managing cybersecurity initiatives.	**Knowledge**: Learners will gain practical knowledge in how to integrate strategic planning and operational management in cybersecurity to protect organizational assets, comply with relevant legislation and standards, and implement effective information security strategies and risk management policies. **Skills**: Learners will be skilled in identifying cybersecurity risks, using strategic planning and operational management tools to safeguard against threats, and promoting the implementation of fundamental cybersecurity practices within their leadership support roles. **Competences**: Learners will be competent in assessing and mitigating security threats, effectively communicating cybersecurity strategies and issues, and reliably reporting incidents and vulnerabilities to the appropriate channels within their organizations.

6. COURSE ASSESSMENT STRATEGY

Evaluation of knowledge is an integral part of the learning process and promotes deeper learning. This chapter describes the approach to course assessment that is needed to ensure that all participants in CyberAgent courses achieve the required learning outcomes and competences. The assessment process in the course is divided into two main parts: self-assessment and knowledge assessment tests, which are tailored to both Higher Education (HEI) and Vocational Education and Training (VET) students, taking into account their different needs and learning objectives.

As the topics of the modules could be the same for both HEIs and VET, some of the questions may be suitable for both HEI and VET courses. Thus, when designing the questions, it will be possible to specify whether the question is intended for VET or HEIs only or for both. This way of marking will only be used when designing the questions as it will facilitate the design of the questions. Once the questions have been imported into the platform, the databases will be different for VET and HEI.

Figure 12. Self-evaluation and knowledge evaluation data bases

1. Self-assessment tests: After the completion of each topic within the course, students will undertake self-assessment tests. These assessments are designed to provide immediate feedback, helping students to gauge their understanding of the recently covered material. This stage encourages self-reflection and aids in reinforcing the learning objectives of each topic. Additionally, it allows learners to identify areas where they might need further study or clarification, promoting a proactive approach to their learning journey.

By using self- assessment tests course participants could identify initial level of knowledge, and could check progress after each training topic.

A 3-5 question self-assessment quiz, with the mix of true/false, matching, and/or multiple choice questions is recommended. Another topic should be unlocked only after all questions are answered correctly. There should be no time limits or restrictions on attempts. Attempt should randomly select questions from according database.

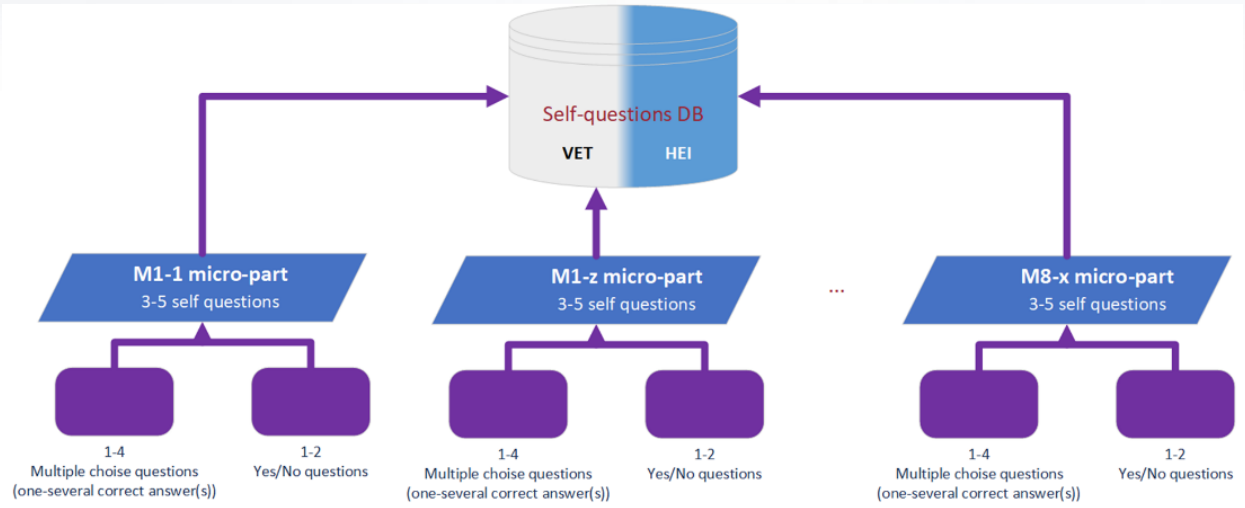

Figure 13. Self-evaluation data base structure

2. Knowledge assessment test*: Upon completing all topics in the course, students will be required to take a final test in order to get course completion certificate. This comprehensive assessment evaluates their overall understanding and mastery of the course content. The final test assesses students' retention of the material and identifies how well they can apply their knowledge in a broader context.

* During the development of the curriculum and materials, other methodologies for assessing the completion of the course and the assessment of knowledge will be considered, such as case studies, practical exercises and reflective reports, which will allow for a more comprehensive assessment of participants' analytical and critical thinking skills. This approach will also be available to lecturers for HEI and VET students in the course delivery.

By using knowledge assessment test course participants could identify their final level of knowledge, and if passed – receive a course completion badge (certificate).

A 36-question knowledge assessment test, with the mix of true/false, matching, and multiple-choice questions is recommended. There should be a 45 minute time limit, and only single attempt allowed. The test should be administered by randomly selecting questions from a database.

In addition, the assessment should also consider cheating prevention and therefore about four sets of questions should be developed. Some of the knowledge test questions for both VET and HEI may overlap, so we will have three attributes at the time of development: VET, HEI or VET and HEI.

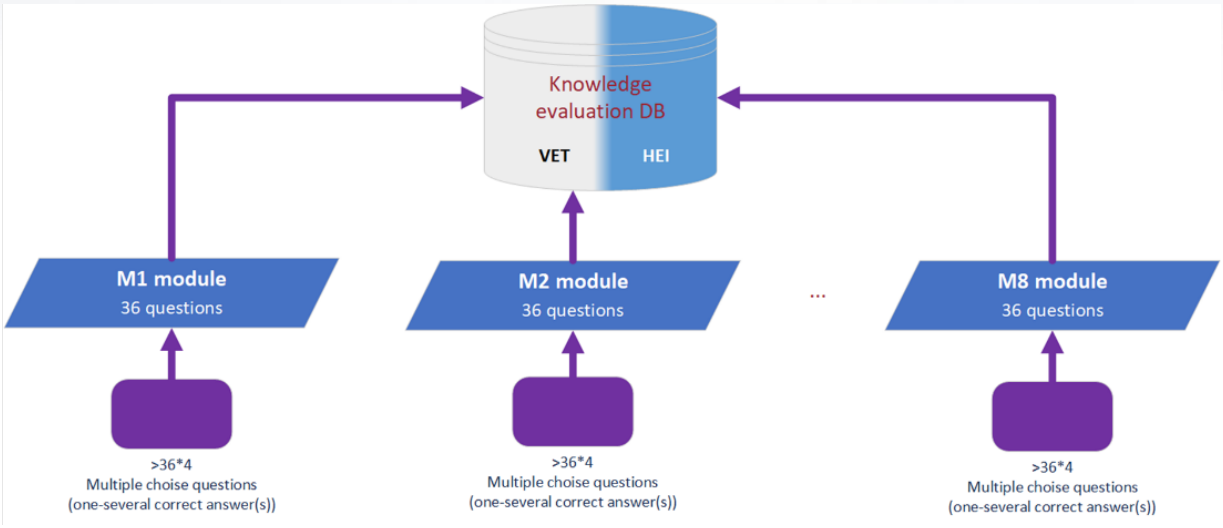

Figure 14. Knowledge evaluation data base structure

This two-stage assessment strategy not only supports effective learning by providing multiple feedback loops but also empowers learners to take an active role in their training.

Self-assessment tests and tests for knowledge assessment will be developed following syllabus of the courses and on the basis of results and recommendations developed in this project.

QUESTION DATABASE COMPOSITION

To ensure a sufficiently large and balanced question base, a at least 5 true/false or matching questions and 5 multiple choice questions will be created for each topic in the VET or HEI course.

Assuming, that there will be at least 10 topics in each course, overall base for each VET or HEI course should contain at least 10-20% true/false or matching, and 90-80% multiple choice questions. This is a general guideline, but the teacher will have the possibility to choose the structure of the questions according to the subject matter of the course.

Considering differences in VET / HEI learning goals and outcomes, the overall composition of question database for a single course should contain as it is shown in the table below.

Table 6. Questions' types

	True/false or matching questions	Multiple choice questions
General part of the course	20%	80%
VET specific part of the course	20%	80%
HEI specific part of the course	20%	80%
Total for a VET and HEI courses:	20%	80%

GUIDELINES FOR QUESTION CONSTRUCTION

Questions for self-assessment and knowledge assessment tests must be prepared in English and then localized to partner languages.

When developing test questions for both self-assessment and knowledge assessment within the course, it is essential to ensure that the questions are clear, concise, and accessible to all candidates, regardless of their backgrounds. This approach ensures that the assessments accurately reflect the learners' understanding of the course content and their ability to meet the stated skills and goals outlined in the course curricula.

General guidelines for question construction:

Clear guidelines will be applied in the development of the test questions: the questions must be comprehensible and directly related to the learning objectives of the course, without the use of complex terminology or confusing wording. Culturally specific or confusing questions will also be avoided to ensure fairness and accessibility for all course participants. Further guidance on the design of the questions is provided below.

Clarity and simplicity: questions must be straightforward, avoiding the use of complex language or jargon that could confuse or mislead the candidates. The goal is to assess the candidates' knowledge and understanding of the subject matter, not their ability to decipher complicated questions.

Directness and relevance: each question should directly relate to the key skills and goals of the course curricula. Irrelevant or tangential content should be avoided to maintain the focus on assessing the intended learning outcomes.

Cultural and background sensitivity: ensure that the questions do not assume specific cultural knowledge or experiences, making them accessible and fair to candidates from diverse backgrounds.

No tricky questions: the intent of each question should be clear, with no attempt to mislead or trick the candidates. Questions designed to catch candidates out or to test their ability to spot trickery do not effectively assess their understanding of the subject matter.

Unambiguous and concise presentation: questions should be phrased in a way that leaves no room for interpretation, ensuring that all candidates understand the question in the same way. Keep questions concise, avoiding unnecessary length that could obscure the main point.

Positive phrasing: avoid using negative phrasing in questions (e.g., "Which of the following is NOT..."). Negative phrasing can lead to confusion and misinterpretation, especially under exam conditions. Instead, frame all questions positively to promote clarity.

Specific guidelines for question construction:

Multiple-choice questions: ensure that all options are plausible and relevant to the question. The correct answer should be indisputably correct, while the distractors should be clearly incorrect to someone who understands the material.

True/False questions: present clear, factual statements that directly relate to the course content, ensuring there's no ambiguity about their truth value.

Matching questions: ensure both lists (e.g., terms on one side and definitions on the other) are clearly related and that there's a straightforward basis for making each match. Avoid uneven lists where the number of items doesn't align unless it's explicitly stated that some items will not be used or can be used multiple times.

The pilot training will analyse information on knowledge assessment methodologies and the assessment process by collecting feedback from both learners and trainers. This will allow to assess the appropriateness of the knowledge assessment methods and, if necessary, to complement or improve the assessment approach.

GAMIFICATION

This section introduces the description of the gamification elements implemented in CyberAgent courses. Gamification is the process of incorporating gamification principles into traditional learning activities in order to increase motivation and engagement of participants. These elements have been selected on the basis of the latest research on educational technology, which shows that gamification can significantly improve learning performance, increase students' motivation to learn and enhance their engagement in the learning process.

The gamification elements that will be integrated into the courses include badges, points, ranks and colour-coded nicknames that reflect the participant's experience and achievements.

- Badges will be awarded for:

- **Completion of the module**.
- **For passing a test based on the pass percentage**. For example, a participant will be awarded a bronze badge for a minimum passing score on the final test, a silver badge for a minimum passing score of 75%, a gold badge for a passing score of 76%-90% and a platinum badge for a passing score of 90%-100%. In this case, one participant may have 8 badges of this type.
- **Completing topic**.
- **Logging into the system every day for ten days**.
- **A special activity badge** for each topic will also be awarded by the course mentor/instructor.

- **Points and scores** calculated on the basis of self-assessment test scores + final test scores with multiplier.

CyberAgent course participants will not be able to see their progress individually, but will be able to compete with other participants in groups or teams (based on the highest number of points scored, but also based on the most badges). This encourages not only individual but also team competition and cooperation, which is important in developing cooperation skills.

Each participant will see his/her nickname when he/she logs in to the course, which will be colour-coded according to the course progress and the experience gathered (courses completed/recorded).

This will help course participants to better involve themselves in the training process. Course participants can repeat the same test several times to improve their score (points are awarded for the highest number of self-assessment tests taken correctly).

A special algorithm will calculate each participant's score taking into account the time taken to answer, the number of times the test is repeated and other parameters, thus minimising the possibility of cheating.

All gamification rules will be clearly described and communicated to the participants so that everyone can easily understand how the different gamification levels can be achieved and how they are calculated.

7. CYBERAGENT LEARNING/TEACHING PROCESS

This section summarises the information from all the chapters in this document and describes in detail the learning/teaching process, starting with enrolment in a CyberAgent course on the learning platform and ending with the completion of the course or the issuing of a certificate.

The CyberAgent courses are designed to cater to a diverse range of learners, including students from Higher Education Institutions (HEIs), Vocational Education and Training (VET) students, as well as employees from SMEs. We aim to give each participant the opportunity to choose the way of learning that suits them best, taking into account their personal circumstances and the organisational policies of the training institution.

Despite the learning/training method chosen, participants register on the CyberAgent platform and use the platform during the training.

Registration

Prospective participants interested in enrolling in the CyberAgent course must complete a registration form, selecting their desired modules and preferred method of learning. A conceptual diagram is provided to guide participants through the learning pathway from the first to the eighth CyberAgent module.

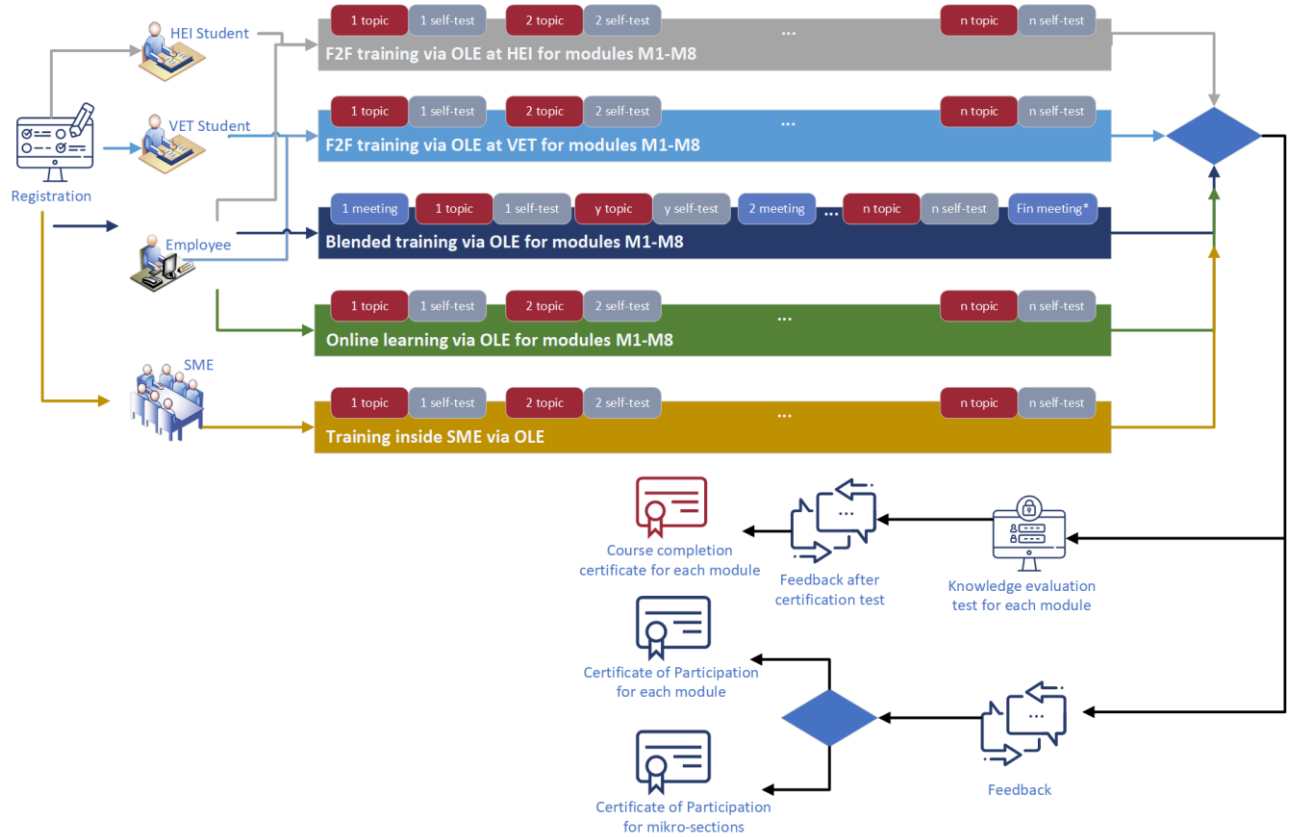

Figure 15. CyberAgent learning / teaching pathway

Confidentiality of participants' information will be ensured during the registration process, in particular with regard to GDPR requirements. During registration, participants will have the opportunity to familiarize themselves with the rules of the training platform, privacy and data protection rules.

Participant registration data is accessible only to designated individuals within the partners' organization, in compliance with internal policies of organisation. During pilot training sessions, participant data from project partners may be accessible to the CyberAgent coordinator, and the other partners are not allowed to see each other's participant data. Upon project completion, the coordinator may only access anonymized data of other partners for monitoring project outcomes, as specified in the project application, for up to 5 years post-project conclusion.

We offer tailored training options to meet the needs of our diverse target groups. HEI and VET students may engage with the training through university contact sessions. SME employees may choose the learning method that best suits their needs: blended learning, online-only, or, less commonly, joining HEI or VET lectures.

Training can also be offered to larger companies with multiple employees. In such cases, the training method will be customized to meet specific needs while still incorporating the CyberAgent module courses.

Upon registering on the platform, participants select their learning method and begin their studies. After completing a module or part of a module, they can qualify for a Certificate of Participation or a Course Completion Certificate, the latter of which is issued if a participant passes the module test with a score of at least 75%.

Finally, participants are required to complete a feedback form before receiving any certificate. This feedback is crucial for the continual improvement of our training offerings and ensuring participant satisfaction.

Learning/training ways

Employees have several options for engaging with the course content:

- If HEIs or VET institutions permit employees to attend as guest participant, the employee can participate in lectures alongside enrolled students. Such external participant sessions may be organized 1-2 times per year, based on the published lecture schedule.
- Employees can opt for a blended training approach, where training sessions are conducted on specific dates with a recommended duration of 2-4 months. Groups of at least 10 participants are advisable, with a maximum of 30 participants per group. Blended training includes both face-to-face and online consultations at the beginning, during, and at the end of the course to facilitate direct feedback and preparation for the final assessment.
- Employees may choose the online learning way for self-paced learning, with no set duration for course completion.
- Further details about CyberAgent modules are provided in Section 1. Study pathway.

Students involvement

Students enrolled in the cybersecurity study program may encounter different pathways based on their academic institution's regulations. They may either be required to complete some or all of the CyberAgent modules, or, depending on internal university policies, students who meet the criteria can choose to study one or multiple CyberAgent modules. HEI or VET students typically engage with the subjects through traditional classroom instruction as provided by their institution or may opt for self-study methods to prepare for the final knowledge assessment test.

SME involvement

In organisations where cybersecurity training is deemed necessary, a representative from the company may register the organisation for internal training sessions. In such cases, upon separate agreement with the university and/or instructors, the method of training, schedule, and issuance of certificates may be tailored to the organisation’s specific needs based on the existing modules.

Feedback Collection

Upon module completion, participants are required to fill out an anonymous feedback form accessible online. Feedback data is accessible only to authorized personnel within the partner‘s organization, with similar confidentiality measures applied during pilot training sessions and post-project data usage.

Feedback will mainly be collected from the course participants, but feedback from mentors/trainers will also be collected. The feedback collected will assess the organisational level of satisfaction of the participants, aspects of the course organisation, the learning process, the use of the acquired competences in practice, the content of the course, assessment strategies, the inclusion of gamification elements, areas for improvement, etc.

The results of the feedback will be regularly reviewed and presented to the project management team in order to react quickly and improve the training strategies according to real needs and market changes.

Only upon completing this form, participants are eligible to get a certificate of participation or to get course completion certificate or certificate of participation.

Course Completion Certificate

Successful completion of the assessment test results in the generation of a course completion certificate for the participant. There is one final test per module.

Certificate of participation

Participants who opt not to take the knowledge assessment test may receive a certificate of participation. This acknowledgment can be issued upon completion of a single module or several micro-parts within the course.

CONCLUSIONS AND SUMMARY

This report has successfully developed structured learning pathways for SME cybersecurity change agents tailored to address the specific needs at various educational and professional levels, from HEI to VET and direct SME employee training. The curriculum devised, comprising eight comprehensive modules, integrates technical, analytical, organizational, and risk management skills that are crucial for the effective empowerment of future cybersecurity professionals.

The structured approach to learning pathways ensures a comprehensive educational journey for SME employees. Through the stages of Pre-learning, Learning, and Post-learning, it supports knowledge retention and practical application. Micro-modules offer flexibility and adaptability to individual needs, enhancing learning with micro-credentials that provide recognized qualifications. This alignment with industry standards significantly contributes to fortifying cybersecurity capabilities within SMEs, preparing employees to meet current challenges and future advancements. The following Carrier Pathway analysis has mapped out the progression of cybersecurity roles as defined by the ESCO framework, facilitating a targeted educational approach that prepares individuals for effective integration into the cybersecurity workforce, ultimately enhancing their career prospects and professional development.

The explored diversity of pedagogical approaches within the cybersecurity curriculum should allow for a dynamic and flexible learning environment that accommodates different learning styles and needs. The incorporation of various teaching methods, including theoretical lectures, practical labs, gamification, and collaborative projects, ensures that students are not only recipients of knowledge but active participants in their learning journey. This comprehensive strategy should enhance engagement, understanding and better prepare students for real-world cybersecurity challenges. The adaptability of teaching methods to module-specific requirements should further personalize the learning experience, ensuring that educational outcomes are maximized for each student.

By systematically mapping the CyberAgent project's subtopics and modules to internationally recognized knowledge units, the curriculum not only meets but anticipates the dynamic requirements of the cybersecurity field. This methodical approach ensures that each learning outcome is strategically linked to real-world competencies that are crucial for the effective management of cybersecurity threats. The curriculum's adaptability allows it to serve various professional roles within the industry, preparing learners not just for immediate challenges but for long-term career development in cybersecurity.

The course assessment strategy outlined offers a framework for evaluating the proficiency and progress of students in cybersecurity programs. The two-stage approach, combining self-assessment tests and comprehensive knowledge evaluation tests, allows students to actively engage with the material, continuously evaluate their understanding, and adjust their learning strategies accordingly. By designing the assessment to accommodate both HEIs and VET students with tailored questions, the strategy ensures relevance and appropriateness for each

educational level, enhancing the learning experience. This method enables a clear measure of student mastery and readiness to apply their knowledge practically. Moreover, the introduction of gamification elements like badges and scoring systems not only motivates students but also fosters a competitive yet collaborative learning environment.

Finally, the CyberAgent learning and teaching process provides a comprehensive and adaptable educational framework suitable for a diverse range of learners from HEIs, VET institutions, and SMEs. This system allows for various participatory methods, including face-to-face, blended, and online learning, ensuring flexibility in how cybersecurity training is delivered and accessed. Registration on the CyberAgent platform initiates a pathway where participants select preferred modules and learning methods, culminating in the issuance of certificates upon successful completion and assessment. This structure not only supports personalized learning trajectories but also aligns with the rigorous privacy standards essential for maintaining participant confidentiality throughout the training process.

The recommendations and guidance provided in this document will be used in the next phase to develop CyberAgent's comprehensive training curricula, training materials, knowledge tests and assessments, practice exercises and other training content, which will be integrated into the CyberAgent training platform.

ANNEX 1. MODULE DESCRIPTION

MODULE DESCRIPTION

Module title	Module code
...	

Lecturer (s)	Institution or department where module is delivered
...	...

Mode of delivery	Language
Face-to-face, online, blended, consultations	*English, ...*

Prerequisites
...

Number of ECTS credits allocated	Student's workload	Contact work hours	Individual work hours
5	...	...	...

Purpose and outcomes of the module		
...		
Learning outcomes of the module	**Teaching and learning methods**	**Assessment methods**
Technical skills		
Analytic skills		
Risk skills		
Organization skills		

Facilitate resources (equipment, software, technology)
...

Module content: breakdown of the topics	Contact work hours					Individual work hours and tasks	
	Lectures (HEI/ VET)	Consultations (SMEs)	Practice (HEI/VET)	Tests	**All contact work**	**Individual work**	**Tasks**
1							
…							
n							
Total							

Assessment strategy	Comparative weight percentage	Assessment criteria
Self-test I		…
…		…
Self-test n		…
Knowledge evaluation test		…
HEI/VET certification -> Self-test I + …+ Self-test n + Knowledge evaluation test		
SMEs/Self-studies certification -> Self-test I + …+ Self-test n + Knowledge evaluation test		
Micro-modules, micro-section -> Self-test I (optional), Self-test n (optional)		

Studies material *(Last name, First Initial. (Year, Month Day). Article title. Magazine/Journal/Newspaper Title, Volume number (Issue number), Page numbers of the entire article, Publisher, URL)*
Required reading
…
Recommended reading
…

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau