



Kaunas Faculty





Co-funded by the European Union

SMEs Cyber Security Change Agents

Dr. Renata Danieliene
Vilnius University

CYBER AGENT 2025

Project ID. 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO Type of Action: ERASMUS-LS

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

Boost camp in Lithuania for trainers.

Cyber security lecturers' workshop:

23-25 September, 2025



Kaunas Faculty





Co-funded by the European Union

Project partners



Coordinator	 Kauno fakultetas
Vocational education and training institutions	 
Business organisations	   
EU-wide organisation	
Non-governmental organisation	



Kaunas Faculty





Co-funded by the European Union

CyberAgent the project we will work on

 Fostering Cooperation	Fostering cooperation between higher education institutions, vocational training institutions and small enterprises
 Sharing Best Practices	Sharing best cybersecurity practices and experiences
 Facilitating Employment	Enhancing employability, cyber resilience and an organisation's cybersecurity culture
 Creating CyberAgents	Empowering and upskilling participants to become Cybersecurity Change Agents
 Empower Women	Involving more women in the IT sector

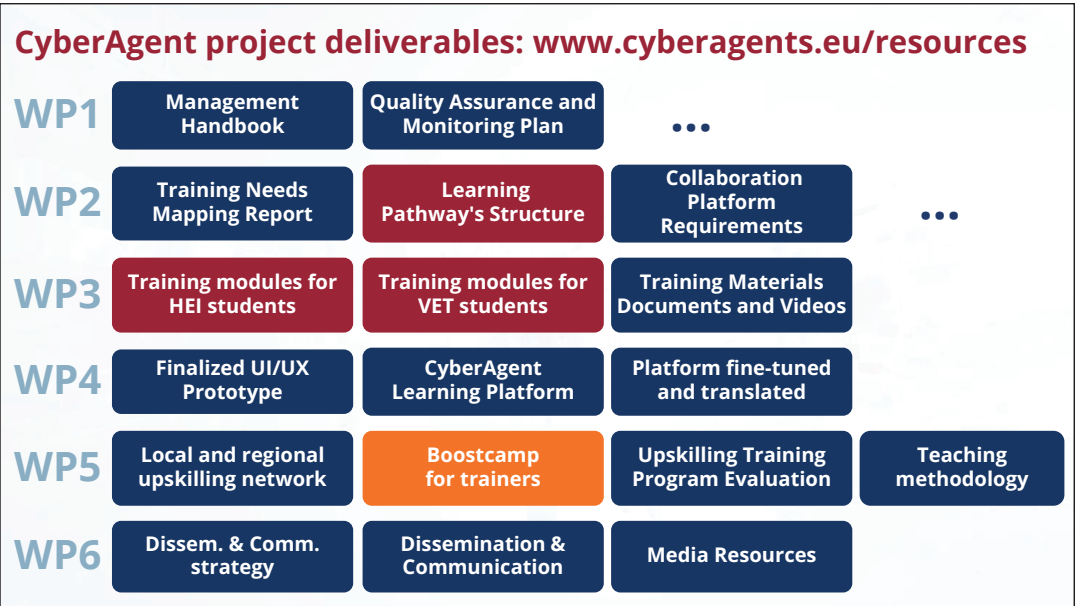
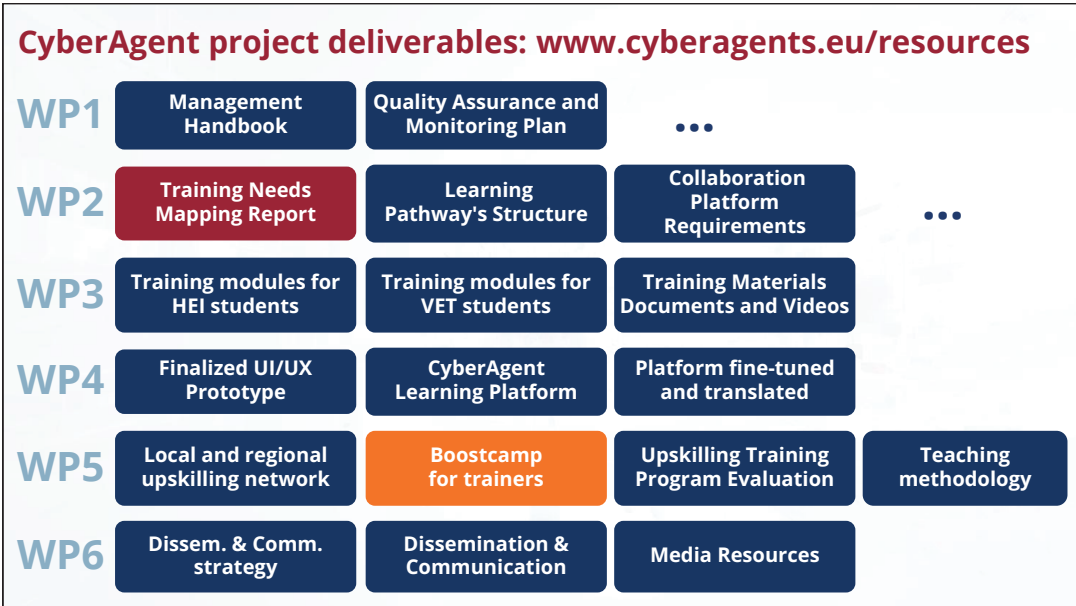
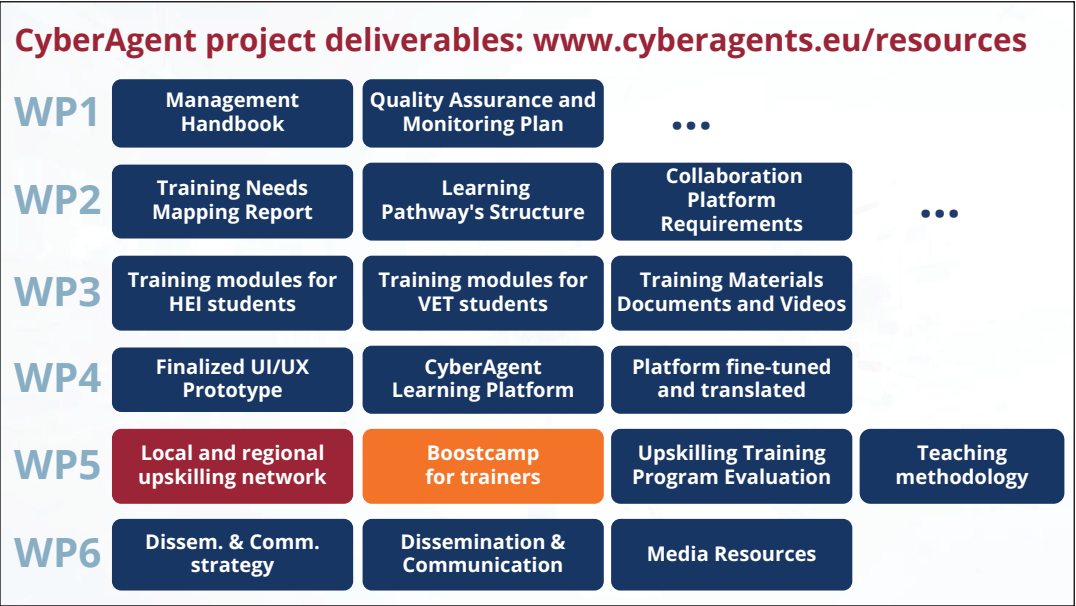
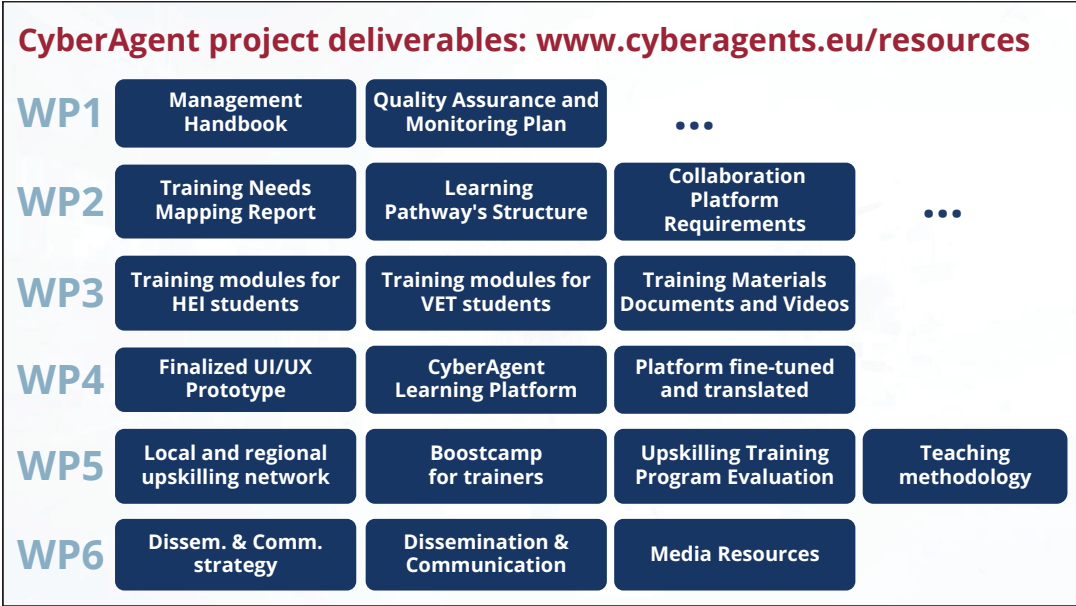


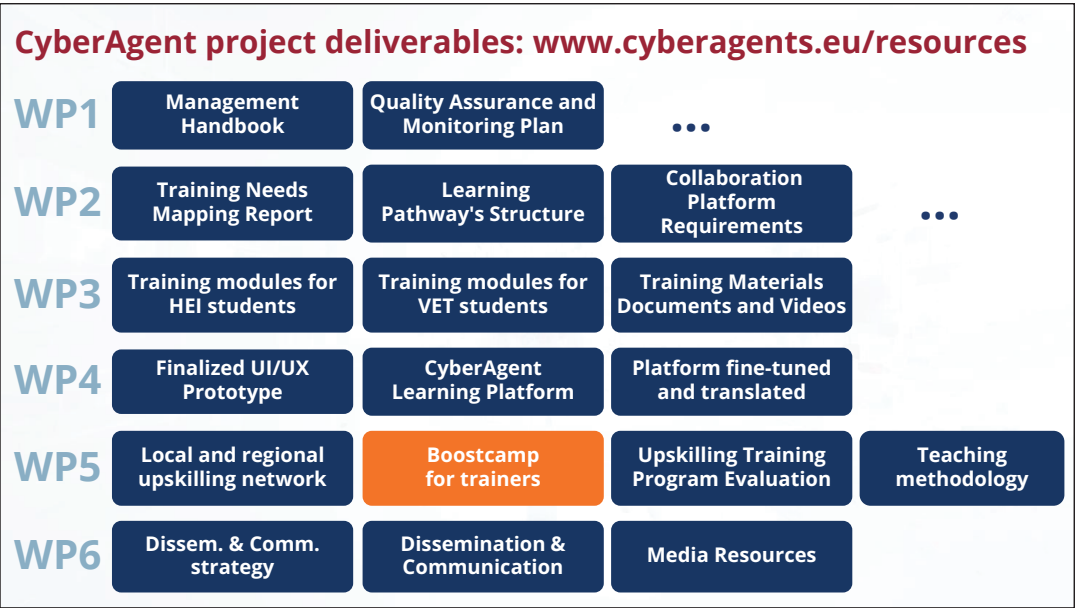
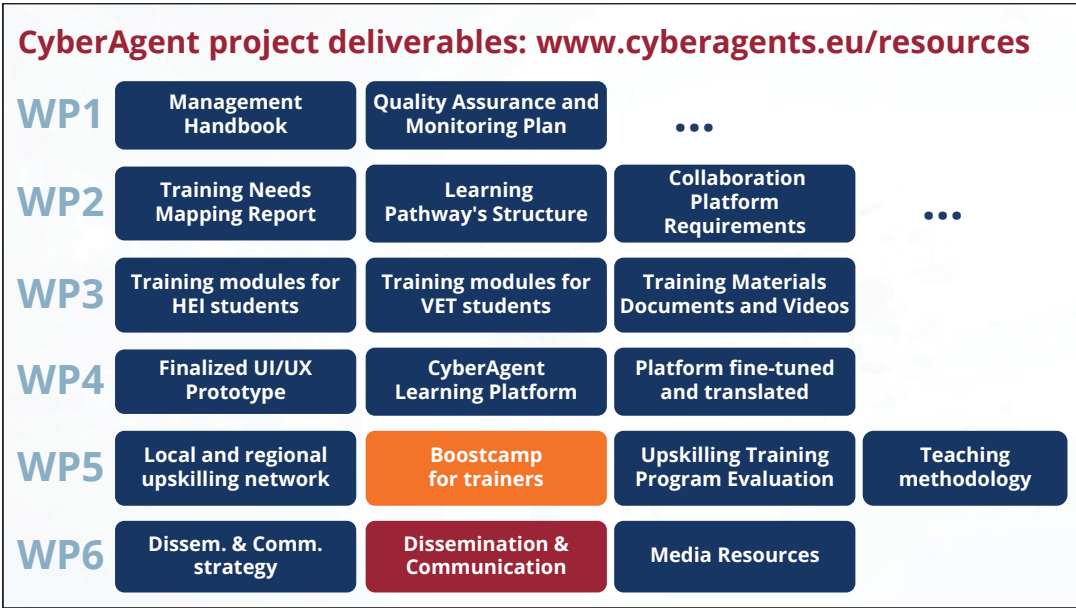
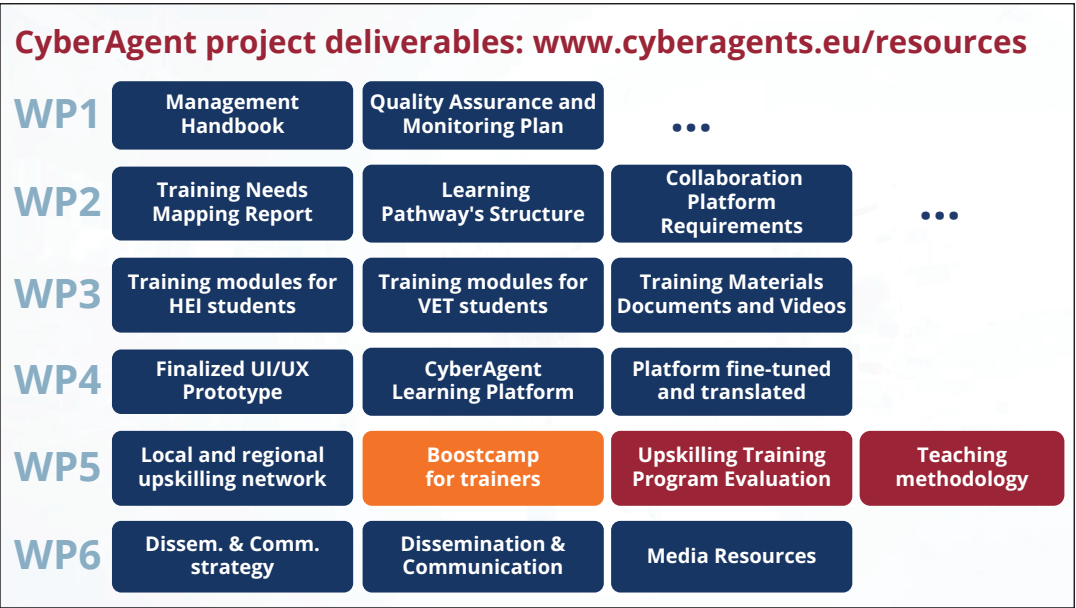
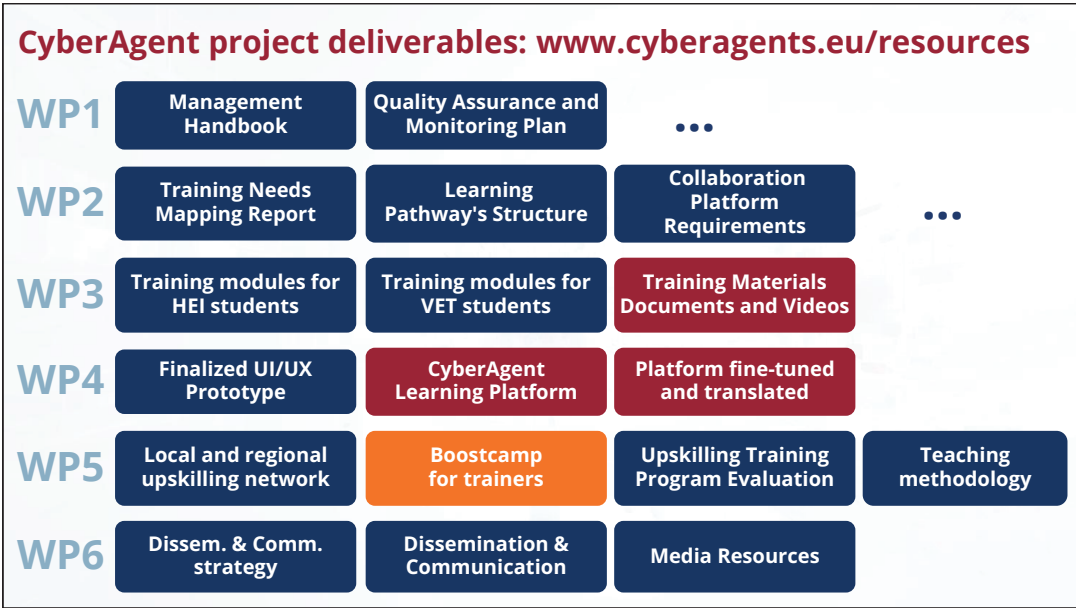
Kaunas Faculty





Co-funded by the European Union







MAIN RESULTS

>10 DELIVERABLES
Available on our website

>30 EVENTS
Attend by partners to spread the word about our project

160 000 PEOPLE REACHED

3^{596 participants} WORKSHOPS
On SMEs and Cybersecurity organised

6 NEWSLETTERS
Keeping up with CyberAgent news!

>680 FOLLOWERS



 Co-funded by the European Union

www.cyberagents.eu*More coming out soon!*

The next workshop is scheduled for the end of October.

 Kaunas Faculty



 Co-funded by the European Union

 Kaunas Faculty



 Co-funded by the European Union

Get social with the project!

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

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

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

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

 contact@cyberagents.eu

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

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

Project Partners

 Kaunas Faculty

 Prios

 AVM GRUPO

 TEKNOPARK ISTANBUL

 IT AKADEMİJA

 OLEMIŞEN İSTANBUL

 WOMEN 4 CYBER





Boost camp in Lithuania for trainers: cyber security lecturers' workshop: 23-25 September, 2025

LEARNING PATHWAY'S STRUCTURE

Jorė Bendinskaitė, VU

CYBER AGENT 2025

Project ID: 101111732

Call: ERASMUS-EDU-2022-PI-ALL-INNO

Type of Action: ERASMUS-LS

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



Co-funded by the European Union

STUDY PATHWAY

Assessment of SME Needs

Analysis of HEI existing programs

Analysis of VET existing programs

WP2.1 Mapping the training needs for SME Cyber Security Change Agents

Analysis of teaching methods

Analysis of ESCO occupations

Analysis of existing study modules structure

Analysis of EQL levels

Analysis of external literature

CURRICULUM GROUP FOR VET STUDENTS (EQF level 4-5)

Knowledge
Comprehensive, specialised, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge.

Skills
A comprehensive range of cognitive and practical skills required to develop creative solutions to abstract problems.

Responsibility and autonomy
Exercise management and supervision in contexts of work or study activities where there is unpredictable change; review and develop performance of self and others.

CURRICULUM GROUP FOR HEI STUDENTS (EQF level 5-6)

Knowledge
Advanced knowledge of a field of work or study, involving a critical understanding of theories and principles.

Skills
Advanced skills, demonstrating mastery and innovation, required to solve complex and unpredictable problems in a specialised field of work or study.

Responsibility and autonomy
Manage complex technical or professional activities or projects, taking responsibility for decision-making in unpredictable work or study contexts; take responsibility for managing professional development of individuals and groups.



Co-funded by the European Union

STUDY PATHWAY

Candidate for studies without experience

Awareness raising: mentoring, leadership, coaching

Motivation of the participant

Self-Studies / raising the qualification

VET studies

HEI studies (bachelor)

HEI studies (master)

IT Assistant, Support staff, etc.

Junior professional etc.

Professional

Team lead, Head of Department, etc.



Co-funded by the European Union

STUDY PATHWAY. MODULES

RISK MANAGEMENT

SECURITY PROGRAMME MANAGEMENT

ANALYTICAL TOOLS

SECURITY PLANNING

SYSTEMS ADMINISTRATION

SECURITY OPERATIONS

BUSINESS CONTINUITY

SECURITY GOVERNANCE

EMPOWERING CARRERS IN CYBERSECURITY



Co-funded by the European Union

STUDY PATHWAY

Both HEI and VET address the same themes, but the depth differs according to the EQF level.

Credits per modules:

HEI modules - 3 credits per module,

VET modules - 1 credit per module.

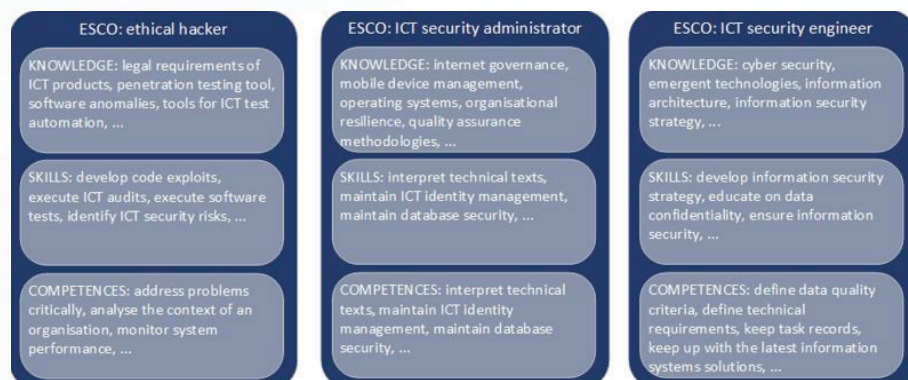


CARRIER PATHWAY

In the beginning of the project the research analysis of ESCO occupations 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.

Roles: 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.

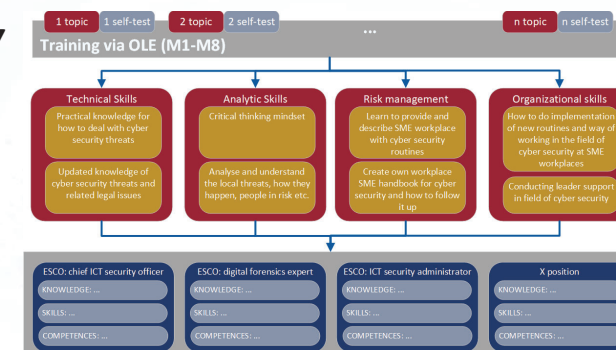
CARRIER PATHWAY. EXAMPLES



CARRIER PATHWAY

4 categories:

- technical skills,
- analytic skills,
- risk management
- organisational skills.



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.



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

TEACHING METHODS

Categories:

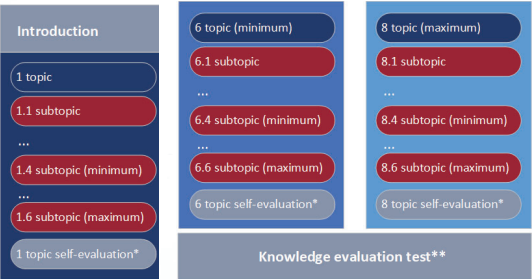
- *Lecture and direct instruction*
- *Practical and hands-on learning*
- *Assessment and evaluation*
- *Self-studies*
- *Collaborative and peer learning*
- *Technology-enhanced learning*
- *Community and public engagement*
- *Innovative learning models*

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.

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](#), [FuselT](#), [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.



WORKLOAD HOURS HEI

STUDY ACTIVITY	PERCENTAGE	HOURS (for 75 hors total)	Details
Lecture/Slides	30-35%	22,5 to 27	5-6 lectures (1,5 h each) 300-720 slides (20-40 alides/lecture) 30-60 pages of text explanation (2-4 for one lecture)
Video Materials	3-4%	2,25 to 3	40-60 min of video, 4-6 video (15 min each) 125 words per minute (5000-7500), if A4=2800 symbols, then 2-3 pages.
Self-study/Reading	40-45%	30 to 33	Independent reading, reviewing notes and research
Practical Tasks	25-30%	19,5 to 22,5	Assignments, exercises or case studies
	100%	100%	

3 ECTS = 75 hours of total study time, and the duration of each lecture is **1.5 hours**, we can divide this time across various study activities, including lectures (slides), video materials, self-study, and practical tasks. We can distribute the **75 hours** across different learning components based on common educational practice:
HEI: calculation for 3 ECTS

WORKLOAD HOURS VET

STUDY ACTIVITY	PERCENTAGE	HOURS (for 25 hors total)	Details
Lecture/Slides	30-35%	7,5 to 9	2-3 lectures (1,5 h each) 100-240 slides 10-20 pages of text explanation (2-4 for one lecture)
Video Materials	3-4%	0,75 to 1	13-20 min of video, 1-2 video (15 min each) 125 words per minute
Self-study/Reading	40-45%	10 to 10	Independent reading, reviewing notes and research
Practical Tasks	25-30%	6,5 to 7,5	Assignments, exercises or case studies
	100%	100%	

TYPICAL STRUCTURE FOR CYBERAGENT MODULES



1. Module identification
2. Module duration and workload
3. Educational goals and learning outcomes
4. Teaching and Learning Methods
5. Assessment and Evaluation
6. Facilitate resources
7. Course content
8. Resources

TYPICAL STRUCTURE

- Updated knowledge of cybersecurity threats and related legal issues	Security Program Management: Project management, Resource management, Security metrics, Quality assurance and quality control.	Knowledge... Skills... Competences...	Knowledge... Skills... Competences...
- 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... Skills... Competences...	Knowledge... Skills... Competences...

Get social with the project!

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 @CyberAgent-EU @Cyber-Agent-EU @CyberAgentEU
contact@cyberagents.eu @Cyber.Agent. EU @CyberAgentEU

Project Partners





Kaunas Faculty





Co-funded by
the European Union

HEI and VET Curriculum

Dr. Renata Danieliene

Vilnius University

CYBER AGENT

2025

Project ID: 101111732

Call: ERASMUS-EDU-2022-PI-ALL-INNO

Type of Action: ERASMUS-LS

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

D2.2 The SME Cyber Security Change Agents Training needs mapping report

Essential training content requirements

Identified training topics for target groups

Teaching methods

Gender inclusion

Main challenges

Cybersecurity situation for SMEs – most attacks target small businesses

D2.3 SME Cyber Security Change Agents learning pathway's structure

Learning pathway (EQF 4–6)

Study structure and micro-modules

Career path

Teaching methods

Recommended module structure

Evaluation system

Engagement and motivation



Kaunas Faculty





Co-funded by
the European Union

European Qualifications Framework Integration

VET, SME

EQF Level 4-5

Designed for SME employees without HEI background and VET studies. Provides foundational cybersecurity skills with light specialization in key modules.

HEI

EQF Level 5-6

Targeted at SME employees with adequate background and HEI students. Features advanced and complex training activities with deeper specialization.

Gateway Pathway

Enables upskilling progression from VET level 4 students and employees to reach advanced level 6 competencies.



Kaunas Faculty





Co-funded by
the European Union

DEVELOPMENT OF SYLLABUSES

2024

- Using D2.2 and D2.3 results VU prepared template for syllabuses
- Analysis of good practice examples
- Themes selection
- Adaptation of syllabuses

EVALUATION OF SYLLABUSES

- Internal and external evaluation

DEVELOPMENT OF TRAINING MATERIAL

2024-2025

- Presentations
- Word documents
- Videos
- Self and knowledge evaluation tests

EVALUATION OF TRAINING MATERIAL

- Internal and external evaluation

LOCALISATION OF TRAINING MATERIAL

2025

- All modules in EN, LT, PL, ES, NO, TR, FR, FI, RO

Correction

Correction

Developing syllabuses and training material:
01/06/2024 - 30/09/2025

[illegible]

Summary: 9 Modules

D3.3 Training Materials Documents and Videos
All modules in EN approved

Partn	ID	Name of module	No Slides	Pages of text files	No of pract. Tasks	Pract.exempl/ case studies	No of self - questions	No of knowledge questions	No of videos	Minute
VU	7	Risk Management and I	258	143	3	7	50	163	6	110
GCM	6	Cybersecurity Planning	437	99	16	16	64	165	5	65
TIMTAL	3	Analytical Tools	283	139	8	8	18	150	6	69
EVM	5	Security Governance & I	250	183	6	17	30	150	8	60
TIMTAL	1	Security Program Mana	312	151	12	12	18	144	6	53
PRIOS	8	Business Continuity, Dis	395	55	15	9	27	145	8	49
HackerU	2	Systems Administration	1275	0	111	0	21	144	1	55
Olemisen	4	Security Operations	481	61	12	2	55	165	3	55
Women4C	9	EMPOWERING CAREERS	78	0	1	0	0	0	3	180
			3769	831	184		283	1226	46	696

Suggestion for developing training material and indicating attributes and for the importing training material into the platform

MODULE ABC	ATTRIBUTE		...	ATTRIBUTE	
	HEI	VET/ SME		HEI	VET/ SME
Introduction					
1 topic	✓	✓	8 topic (maximum)	✓	✓
1.1 subtopic	✓	✓	8.1 subtopic	✓	
1.2 subtopic	✓		8.4 subtopic (minimum)	✓	✓
1.3 subtopic	✓	✓	...		
1.4 subtopic (min)	✓		8.6 subtopic (maximum)	✓	✓
1.5 subtopic	✓		8 topic self-evaluation HEI	✓	
1.6 subtopic (max)	✓		8 topic self-evaluation VET		✓
1 topic self-evaluation HEI	✓				
1 topic self-evaluation VET		✓			
Knowledge evaluation test HEI					
Knowledge evaluation test VET					
VET self-assessment and knowledge evaluation question could be part of HEI questions					

The scope of one module (VET, 1 ECTS)

Module-8: Business Continuity		HEI	VET
Submodule	Incident response	Topics: Definition and importance of incident response in cybersecurity	
		Key components of an effective incident response recovery	
		Overview of common cybersecurity threats (phishing, insider threats,)	
		Developing Incident Response Plan (IRP)	
		Roles and responsibilities in the Incident Response Team	
		Simulating the Incident: conducting a mock plan.	
Submodule	Disaster recovery	Topics: Understanding Disaster Recovery	
		Developing a Disaster Recovery Plan	
		Roles and responsibilities in Disaster Recovery	
		Recovery steps after disaster	
Submodule	Business continuity	Topics: Understanding business continuity	
		Developing Business Continuity Plan (BCP)	
		Roles and responsibilities in business continuity	
		Business Impact Analysis	
		Testing and improving BCP	
Submodule	Security awareness, training and education	Topics: Understanding security awareness	
		Developing security training program	
		Employee responsibilities in cybersecurity	
		Measuring the effectiveness of security awareness	

Assessment Strategy

Two-stage evaluation system promoting deeper learning through continuous feedback and comprehensive knowledge verification.

Self-Assessment Tests

3-5 questions after each topic completion with unlimited attempts and no time restrictions. Immediate feedback supports learning reinforcement.

- True/false questions
- Multiple choice options
- Matching exercises
- Progress tracking

Knowledge Assessment

36-question comprehensive test with 45-minute time limit and single attempt policy. Minimum 75% score required for certification.

- Random question selection
- Four question sets

One Pagers for dissemination



Training Delivery Methods

Blended Learning

2-4 month programs combining face-to-face sessions with online consultations. Groups of 10-30 participants with structured feedback sessions.

Online Self-Paced

Flexible individual learning with no set completion timeline, allowing professionals to balance training with work responsibilities.

Corporate Training

Customized organizational programs with tailored schedules and specialized certification processes for larger companies.

**Vilnius University
Kaunas Faculty**
Muitinės g. 8, Kaunas

renata.danieliene@knf.vu.lt

*Knowing where the trap is –
that's the first step in evading it.*
- Frank Herbert, Dune

Stay connected



Renata Danielienė
Lecturer and Researcher at Vilnius University



Get social with the project!

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 @CyberAgent-EU @Cyber-Agent-EU @CyberAgentEU
contact@cyberagents.eu @Cyber.Agent. EU @CyberAgentEU

Project Partners





Cybersecurity challenges for VET schools

CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS

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.

 Co-funded by the European Union

www.cyberagents.eu

CONTENT

1. Introduction
2. Profile of VET schools and the specifics of technical education
3. Major cybersecurity challenges for VET schools
4. Current needs of VET schools
5. Recommendations and directions for action
6. Conclusions



Source of image: generated by Chat GPT



2

1. Introduction

- Cybersecurity is the protection of information systems and personal data, along with digital infrastructure, from increasingly diverse and sophisticated threats in the online environment.
- Students in VET (**V**ocational **E**ducation and **T**raining) schools, through their daily access to technology, are exposed to a variety of cyber risks — from security breaches to phishing or malware attacks.

- The training of students in VET schools must include not only technical skills, but also fundamental knowledge about data protection, responsible use of digital platforms and understanding of cyber risks.
- According to an ENISA report (2023), over 60% of cyber attacks target individual users and poorly prepared educational institutions, making education a priority target.



Source of image: generated by Chat GPT



3



4

- “Education is the first line of defense against cybercrime,” says Ursula von der Leyen, President of the European Commission – emphasizing the importance of developing a culture of cybersecurity from an early age.
- The European project we are part of aims to identify the specific challenges of VET schools and propose practical and sustainable solutions for integrating cybersecurity into vocational education.

2. Profile of VET schools and the specifics of technical education

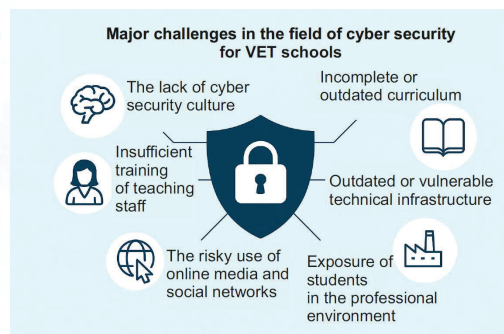
- VET (Vocational Education and Training) schools offer practical vocational training, focused on the needs of the labor market, in fields such as electronics, IT, electricity, mechanics, industry, agriculture, tourism and services.
- These institutions train future technicians, operators, installers, specialists and entrepreneurs in key economic sectors, contributing essentially to the socio-economic development of communities.

- The educational process is focused on acquiring applied technical skills, which involves the intensive use of digital equipment, software applications, online platforms and computer networks.
- In many VET schools, the level of digital literacy is uneven, with differences between students and even between teachers, depending on access to technology, previous training and available resources.
- The digital infrastructure varies considerably between schools: some have modern equipment and stable internet connections, while others use outdated networks, exposed to cyber risks.

- VET education frequently involves **internships in real companies**, where students have access to the companies' digital infrastructure, which poses an additional risk of vulnerability if they are not properly trained in IT security.
- By their very nature, VET schools have a **strategic role** in developing a generation of professionals who can work safely in a digitalized environment – but this requires a **systematic integration of cybersecurity into vocational training**.

3. Major cybersecurity challenges for VET schools

- Vocational education and training (VET) schools face a number of structural, pedagogical and technological challenges in trying to effectively integrate cybersecurity into the educational process. These challenges can be grouped as follows:



Source of image: generated by Chat GPT

- **Lack of cybersecurity culture**
 - ✓ Awareness of digital risks is low among students and teachers.
 - ✓ Security is often perceived as the exclusive responsibility of IT specialists, not all users.
 - ✓ Preventive educational initiatives or practical risk simulation workshops are lacking.
- **Incomplete or outdated curriculum**
 - ✓ Topics on digital security are treated superficially or are completely absent from the VET curriculum.
 - ✓ There is no integrated approach to basic digital and cyber-specific skills.
 - ✓ There is a lack of modern, interactive educational resources adapted to the level of students' preparation.

- **Outdated or vulnerable technical infrastructure**

- ✓ School networks are often poorly secured, without clear data management policies.
- ✓ Devices are rarely updated, exposing networks to viruses or attacks.
- ✓ Lack of control over internet and application access increases the risk of breaches.

- **Insufficient teacher training**

- ✓ Teachers do not receive ongoing training in IT security.
- ✓ There is a reluctance to adopt technology or an overreliance on automated protection solutions.
- ✓ Technical and pedagogical support is limited or non-existent in many schools.

- **Risky use of online environments and social networks**

- ✓ Students do not know good practices for protecting personal data.
- ✓ External platforms are used without checking their security.
- ✓ Phenomena such as cyberbullying, fake news or social engineering are little addressed in an educational way.

- **Student exposure to the professional environment**

- ✓ During internships, students may have access to company data or infrastructure without understanding the risks.
- ✓ The lack of clear protocols between school and employers can lead to accidentally caused security breaches.

4. Current needs of VET schools

- VET schools are at the heart of the process of training future specialists in technical and industrial fields. In the face of accelerated digitalization and increasing cyber risks, these educational institutions need to adapt their methods, resources and infrastructure. Current needs can be grouped into several key categories:

The current needs of VET schools



• Integrating cybersecurity into all specializations

- ✓ Introducing mandatory digital education modules covering essential security concepts: strong passwords, phishing, online identity protection, backup, etc.
- ✓ Adapting content according to the professional field (e.g. industrial network security, protecting customer data in tourism, protecting computerized systems in precision agriculture).
- ✓ Aligning VET curricula with European digital and cyber competence standards (e.g. DigCompEdu, DigComp 2.2).

• Partnerships with experts, companies and specialized organizations

- ✓ Collaboration with IT companies or cybersecurity competence centers for:
 - training sessions;
 - mentoring;
 - thematic visits;
 - participation in real projects.
- ✓ Involvement of authorities and NGOs that promote digital literacy and cybersecurity among young people.

• Practical and experiential activities for students

- ✓ Organization of:
 - interactive workshops on topics such as data protection, phishing attacks, basic cryptography;
 - computer attack simulations and rapid response scenarios;
 - thematic competitions (CyberChallenge, Capture the Flag, etc.).
- ✓ Use of free educational platforms (such as CyberRange or TryHackMe) for learning through games and simulation.

- **Secure and modernized digital infrastructure**

- ✓ Up-to-date equipment, secure Wi-Fi networks, effective antivirus and backup systems.
- ✓ Use of network and user management tools (e.g. access control, monitoring of student activity in the laboratory).
- ✓ Ensuring a clear system of roles and permissions for the use of IT equipment.

- **Clear internal policies and rules on the use of technology**

- ✓ Develop an internal digital regulation that defines:
 - what is acceptable and what is not in the use of technology in school;
 - the obligations of students and teachers in protecting data;
 - procedures in case of cyber incidents.
- ✓ Form an internal IT and digital security coordination team, with representatives of teachers, students and technical staff.

5. Recommendations and directions for action

In order to respond to the identified challenges and transform VET schools into safe, modern environments adapted to current digital requirements, concrete, coherent and sustainable measures are required:

- **Integrating cybersecurity into the VET curriculum**

- ✓ Introducing mandatory or optional modules dedicated to basic digital security in all qualifications.
- ✓ Adapting the content to the specifics of each specialization (e.g. industrial security for students in the field of automation).
- ✓ Using modern teaching methods: attack simulations, case studies, educational games, virtual laboratories.

- **Continuous training of teachers**

- ✓ Organizing courses, webinars and trainings in collaboration with IT experts or specialized institutions.
 - ✓ Creating networks of teacher ambassadors in digital security, who can support colleagues in their own institutions.
 - ✓ Ensuring formal recognition of skills acquired through digital micro-certifications.
- **Improving digital infrastructure and security policies**
 - ✓ Updating equipment and networks, implementing basic technical measures (firewall, 2-step authentication, back-up, etc.).
 - ✓ Developing an Internal Regulation for the use of technology (BYOD policy, internet access, passwords, etc.).
 - ✓ Establishing a cyber incident response plan at the level of each school

- **Involving students in training and prevention**

- ✓ Organizing an annual “Cybersecurity Week”: workshops, competitions, presentations by experts.
- ✓ Promoting collaborative learning through peer-learning – students can become digital ambassadors for their peers.
- ✓ Carrying out awareness campaigns: posters, podcasts, educational videos.

- **Strategic partnerships and outreach**

- ✓ Collaborating with local IT companies, universities and NGOs for mentoring, study visits and thematic internships.
- ✓ Participating in Erasmus+ projects or other European initiatives supporting cybersecurity in education.
- ✓ Creating a national or regional platform for the exchange of good practices between VET schools

- **Developing a national strategy for digital security in vocational education**

- ✓ In partnership with the ministries of education, IT and labor.
- ✓ Involving all educational stakeholders – students, teachers, parents, principals, local authorities.

6. Conclusions

- Cybersecurity must be treated as a priority in professional training.
- Challenges can be turned into opportunities through collaboration, education and tailored investments.
- The role of teachers is essential in shaping a culture of digital responsibility among students.

Bibliography

- **ENISA – European Union Agency for Cybersecurity**
 - Raportul ENISA Threat Landscape 2023
 - Website: <https://www.enisa.europa.eu>
 - <https://www.enisa.europa.eu/publications/>
- **Comisia Europeană – Discursuri și inițiative**
 - Ursula von der Leyen – Discurs privind „Starea Uniunii” 2022–2023
 - Discurs oficial (ec.europa.eu)
- **OECD – Digital Education Outlook**
 - <https://www.oecd.org/education/>
- **EU Cybersecurity Strategy for the Digital Decade (2020)**
 - <https://digital-strategy.ec.europa.eu>

- **CEDEFOP – European Centre for the Development of Vocational Training**
 - <https://www.cedefop.europa.eu>
- **European Commission – Digital Education Action Plan (2021–2027)**
 - <https://education.ec.europa.eu>
- **Raportul DESI (Digital Economy and Society Index)**
 - <https://digital-strategy.ec.europa.eu>
- S. Zeadally et al. (2022), *Cybersecurity education and training: Preparing the next generation workforce.*
- P. Mitropoulos et al. (2021), *Cybersecurity awareness in European schools: Challenges and recommendations.*



CyberAgent Co-funded by the European Union

Get social with the project!

www.cyberagents.eu @CyberAgent.EU @Cyber-Agent-EU @CyberAgentEU
contact@cyberagents.eu @Cyber.Agent. EU @CyberAgentEU

Project Partners

 Kaunas Faculty  Prios  AVM GROUP  TEKNOPARK ISTANBUL  IT AKADEMIJA  WOMEN 4 CYBER 



Boost camp in Lithuania for trainers: cyber security lecturers' workshop: 23-25 September, 2025

New digital tools with AI

Macadon Carmen Daniela, Technological High School Grigore C Moisil, Buzau, Romania

CYBER AGENT 2025

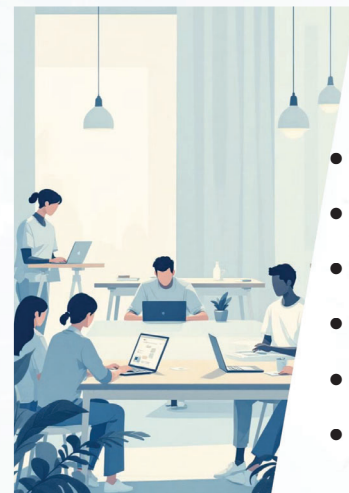
Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS

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.



Co-funded by the European Union

www.cyberagents.eu



Content

- Introduction
- Gamma AI
- Invideo AI
- Magic School AI Innovator
- Learning apps
- Benefits of Integrating These Tools



Co-funded by the European Union

2

Using Digital Tools

- Transform your content creation workflow with powerful AI-driven platforms that enhance creativity, boost engagement, and streamline collaboration—all without requiring specialist skills.



Co-funded by the European Union

3

Why Use Digital Tools?

- Time Efficiency**: Leverage AI automation and templates to complete tasks in minutes rather than hours
- Enhanced Creativity**: Produce professional-quality content without design or coding expertise
- Engagement Boost**: Capture attention through interactive multimedia experiences
- Seamless Collaboration**: Work together regardless of physical location or time zones



Co-funded by the European Union

4

1. Gamma AI

Gamma: AI-Powered Presentation & Content Creation

- Instant Creation
 - ❑ Transform ideas into polished presentations, documents, and websites within seconds using AI assistance
- No Skills Required
 - ❑ Create stunning visuals and coherent text without design or coding expertise through intuitive AI tools
- Rich Media Support
 - ❑ Enhance engagement with interactive galleries, embedded videos, dynamic charts, and interactive elements
- Versatile Output
 - ❑ Export to PDF and PowerPoint formats while maintaining mobile-friendly, easily shareable online versions

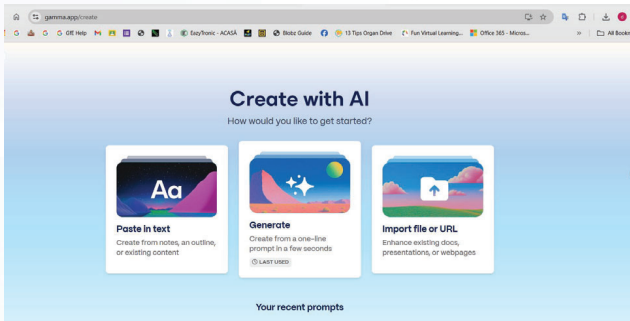
Gamma Features for Users

- AI-Powered Layouts
 - Automatically generates visually balanced slides with cohesive themes and professional aesthetics
- Quick-Start Import
 - Paste existing text or import documents to instantly transform content into structured presentations
- Real-Time AI Assistance
 - Get intelligent suggestions to rewrite, expand, or improve content as you work
- Integrated Media Library
 - Access Unsplash photos and Giphy animations without leaving the platform

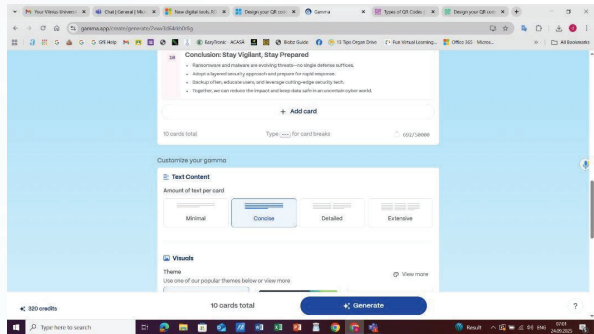
[gamma app](#)



gamma app



gamma app



Gamma in Education and Business



Education Applications

- Educators create engaging lessons in minutes, freeing time for personalised teaching whilst maintaining high-quality materials



Business Benefits

- From pitch decks to marketing materials, businesses leverage built-in analytics to track engagement and secure sensitive content with password protection

2. Invideo AI

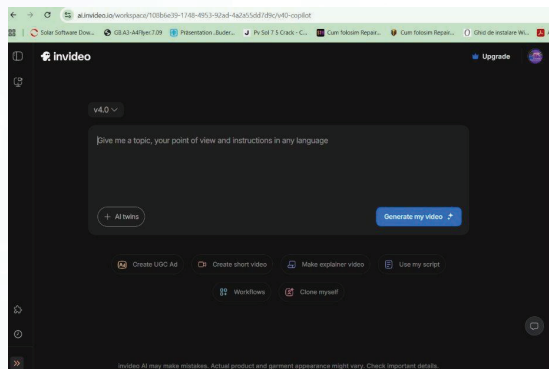
Invideo AI: Video Creation Made Easy

- Intuitive Video Platform
 - ✓ Create professional marketing and educational videos without video editing expertise
- Rich Content Library
 - ✓ Access templates, stock footage, and AI-powered editing tools for quick assembly
- Advanced Features
 - ✓ Convert text to video, add voiceovers, and customise branding elements easily
- Social Media Optimised
 - ✓ Quickly produce and adapt videos for various platforms and aspect ratios

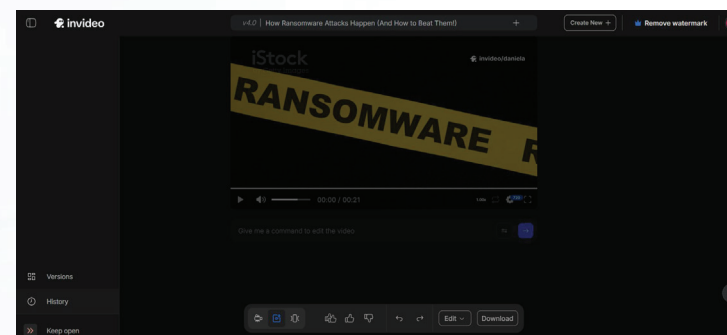
invideo.io/make/ai-video-generator_editor



Invideo AI



And...a video



3. Magic School AI Innovator

Transforming Education with Magic School AI

- **Teach smarter, not harder** by automating routine tasks and enhancing creativity
- **Safe AI experiences** for students with appropriate guardrails and oversight
- **Scalable for all schools** regardless of size, resources or technical expertise

Magic School AI Innovator: Empowering Education with Digital Tools

- Trusted by 13,000+ schools worldwide, used by over 5 million educators globally, Magic School AI is the award-winning AI platform specifically designed to increase educational experiences.

What is Magic School AI?

- **Built by educators, for educators**
 - Comprehensive AI platform that simplifies teaching workflows
 - Streamlines lesson planning, assessments and communication
 - Supports responsible AI integration in classroom settings
 - Personalises learning for every student's unique needs
 - Reclaim 7-10 hours of your week

Key Educator Tools Overview

- **Lesson Planning**
- 80+ AI-powered tools for creating engaging lesson plans, detailed rubrics, and tailored IEPs for all subjects and grade levels.
- **Communication**
- Generate professional emails, report card comments, newsletters and social media posts with consistent tone and quality.
- **Assessment**
- Create customised surveys, quizzes and formative assessments that adapt to student progress and curriculum requirements.



21

Explore magicschool.ai



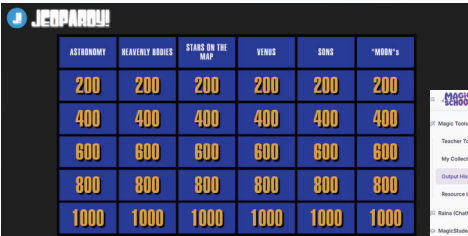
22

The screenshot displays the MagicSchool AI web application interface. On the left, there's a sidebar with navigation options: MagicTools, My Collections, Output History, Resource Library, Rains (Chatbot), MagicStudent, and MagicSchool Labs. The main area shows a grid of tool cards under the heading 'Filter by: Categories, Favourites, Custom, Create collection'. Tools include Rains (Have a question or request? Ask Rains, our trusted AI chatbot for educators), Image Generator (Generate and edit images with AI with Adobe Express), Lesson Plan (Generate a lesson plan based on a standard, topic, or objective), Multiple Choice Quiz / Assessment (Generate a multiple choice assessment, quiz, or test based on any topic, standard(s), or criteria), Writing Feedback (Generate feedback on student writing based on custom criteria or a rubric), Vocabulary List Generator (Generate a list of vocabulary words based on a subject, topic, or text), Math Story Word Problems (Write custom math word problems based on what you're teaching and any story topic), Standards Unpacker (Unpack any standard into component parts to understand what students need to learn), Choice Board (UDL) (Create a choice board for a student assignment based on the principles of UDL), Exemplar & Non-Exemplar (Generate exemplar & non-exemplar responses to specific assignments), Teacher Observations (Generate custom feedback for a teacher based on a classroom observation), Behaviour Intervention Suggestions (Generate suggestions for intervention based on the behaviours of a student that needs support), Tool Recommendations (Discover the best MagicSchool tools to use based on your specific needs), Worksheet Generator (Generate a worksheet based on any topic or text), Math Spiral Review (Generate a spiral review problem set for any maths standard(s) or topic(s)), Group Work Generator (Generate group work activity for students based on a topic, standard, or objective), Project Based Learning (PBL) (Generate a lesson plan based on the principles of Project Based Learning (PBL)), and Vocabulary Based Texts (Generate custom texts that include vocabulary words for your class to practice them in context).



23

Jeopardy Review Game - Output History



Output History				
Unlock all your resources when you upgrade to plus or enterprise				
Filter by: All resources, Paid, Star Date, End Date				
TS	Title	Tool	Shared	Created At
0	Cybersecurity quiz for 10th grade	Multiple Choice Quiz / Assessment	Private	2 Sept, 11:53
0		PD Planner	Private	2 Sept, 11:52
0	Cybersecurity for 10th grade	Jeopardy Review Game	Private	21 Jul, 15:13
0	10th Grade Cybersecurity and WWI Review Game	Survey Creator	Private	23 Apr, 16:12
0	10th Grade Cybersecurity Management Strategies	Jeopardy Review Game	Private	23 Apr, 16:07



24

4. Learning apps

Learning Apps: Enhancing Education Digitally

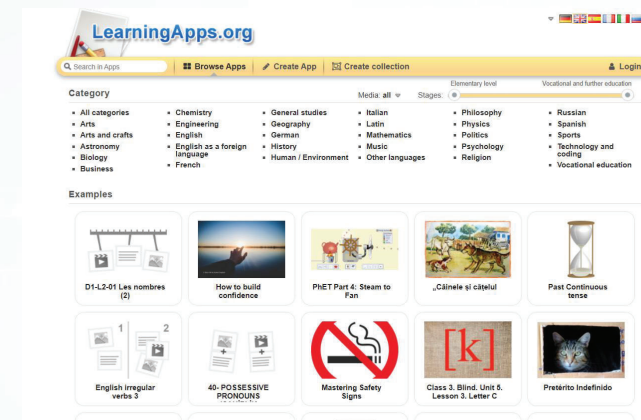
- Interactive Learning
 - Personalised experiences that adapt to individual learning styles and pace
- Gamification
 - Achievement systems that motivate continued engagement and skill building
- Progress Tracking
 - Data-driven insights into learning patterns and advancement
- Multi-Device Access
 - Learn anytime, anywhere across smartphones, tablets and computers

Learning Apps



Learning Apps

Browse Apps



Create App

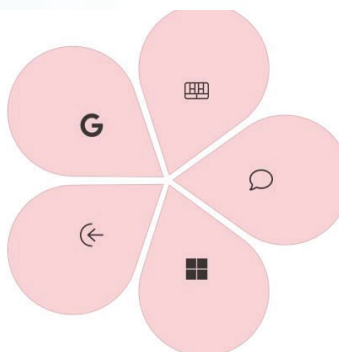
Short introduction to collections with pictures (English)

Example

Benefits of Integrating These Tools

Seamless Integration

- Google Classroom
 - Direct integration with Google's educational ecosystem.
 - Easy access through existing school login systems



- Canvas
 - Smooth workflow with popular higher education LMS.
- Schoology
 - Connects with K-12 favourite learning platform.
- Microsoft
 - One-click export to Word and other Office tools.

Benefits of Integrating These Tools

70% Time Saved

- Average reduction in content creation time compared to traditional methods

3X Engagement Increase

- Multimedia and interactive elements drive substantially higher audience engagement

85% Quality Improvement

- Users report significantly higher quality outputs with less effort

24/7 Accessibility

- Work across devices and collaborate remotely regardless of location

Bibliography

Made with GAMMA



Thank you for your attention!

Get social with the project!

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.



Project Partners



Legal Requirements for AI Cybersecurity

Dr. mult. Paulius ASTROMSKIS
2025-09-24 @ VU

CYBER AGENT

2025

Project ID: 10111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS

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.

Co-funded by the European Union

www.cyberagents.eu

AI & Risk Management Dimensions

Risk Management for AI

AI to Support Risk Management

Risky (Malicious) use of AI

Kaunas Faculty

Co-funded by the European Union

Unacceptable risk e.g. AI employing subliminal techniques to distort behaviour; AI manipulation systems; social scoring AI, real-time remote biometric identification e.g. facial recognition

High-risk e.g. medical devices, toys, radio equipment, education, immigration, law, employment etc.

Limited risk e.g. chat bots, deep fakes, emotion recognitions systems

Minimal risk e.g. spam filters, video games, recommender systems

Regulatory Requirements:

- Prohibition:** Violation of EU fundamental rights and values
- Conformity assessment, Transparency, Post-market surveillance etc.** (linked to High-risk)
- Transparency:** Risk of impersonation, manipulation, deception
- Codes of conduct:** Common AI systems

General purpose AI Model (GPAI): Transparency, Codes of Practice, Obligations (GPAI with systemic risk)

www.emergobyul.com/news/european-artificial-intelligence-act-impact-medical-devices

Figure 1: Risk classification of AI systems under the EU AI Act

Kaunas Faculty

Co-funded by the European Union

High Risk Artificial Intelligence Systems

Stringent compliance requirements

Risk Management System

Record Keeping

Robustness, Accuracy and Cybersecurity

Data and Data Governance

Technical Documentation

Transparency & Information

Human Oversight

Kaunas Faculty

Co-funded by the European Union

Guiding principles to address the cybersecurity requirement of the AI Act

- **Guiding principle 1:** The focus of the AI Act is on AI systems (not AI models or other components).
- **Guiding principle 2:** Compliance with the AI Act necessarily requires a security risk assessment.
- **Guiding principle 3:** Securing AI systems requires an integrated and continuous approach using proven practices and AI-specific controls
- **Guiding principle 4:** There are limits in the state of the art for securing AI models



ISSN 1831-9424

JRC SCIENCE FOR POLICY REPORT

Cybersecurity of Artificial Intelligence in the AI Act

Guiding principles to address the cybersecurity requirement for high-risk AI systems

Jurkiewicz, H., Harman, R., Jorras, A., Evans, T., Soler, Garmas, J., Sanchez Martin, J.

2023

CyberAgent

Kaunas Faculty

Co-funded by the European Union

Article 15: Accuracy, Robustness and Cybersecurity

- High-risk AI systems shall be designed and developed in such a way that they achieve **an appropriate level** of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects **throughout their lifecycle**.
- The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be **appropriate to** the relevant circumstances and the **risks**. <...> shall include, where appropriate, measures to **prevent, detect, respond to, resolve** and **control** for attacks trying to:
 - manipulate the training data set (**data poisoning**), or
 - pre-trained components used in training (**model poisoning**),
 - inputs designed to cause the AI model to make a mistake (**adversarial examples or model evasion**),
 - confidentiality attacks or model flaws.
- See also Recitals 76-78 (and others)



ISSN 1831-9424

JRC SCIENCE FOR POLICY REPORT

Cybersecurity of Artificial Intelligence in the AI Act

Guiding principles to address the cybersecurity requirement for high-risk AI systems

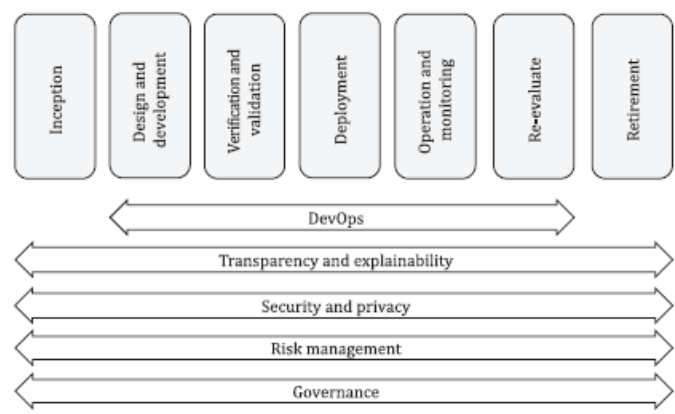
Jurkiewicz, H., Harman, R., Jorras, A., Evans, T., Soler, Garmas, J., Sanchez Martin, J.

2023

CyberAgent

Kaunas Faculty

Co-funded by the European Union



Inception

Design and development

Verification and validation

Deployment

Operation and monitoring

Re-evaluate

Retirement

DevOps

Transparency and explainability

Security and privacy

Risk management

Governance

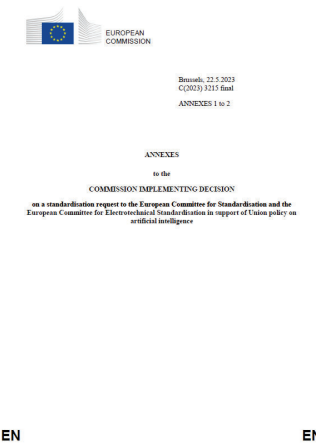
CyberAgent

Kaunas Faculty

Co-funded by the European Union

Article 40: Harmonised Standards and Standardisation Deliverables

- Commission shall issue, without undue delay, standardisation requests covering all requirements set out in Section 2 of this Chapter (incl. Article 15).
- Risk management system for AI systems:
 - This (these) European standard(s) or European standardisation deliverable(s) shall set up specifications for a risk management system for AI systems
 - The European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) are requested to draft the new European standards or European standardisation deliverables in support of Union policy on artificial intelligence by **30 April 2025**



EUROPEAN COMMISSION

Brussels, 22.5.2023
C(2023) 3215 final
ANNEXES 1 to 2

ANNEXES
to the
COMMISSION IMPLEMENTING DECISION
on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence

EN

EN

CyberAgent

Kaunas Faculty

Co-funded by the European Union

CEN/CLC/JTC 21 Published Standards

Reference	Date	Title
EN ISO/IEC 5259-1:2025	2025-05-21	Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 1: Overview, terminology, and examples (ISO/IEC 5259-1:2024)
EN ISO/IEC 5259-2:2025	2025-05-21	Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 2: Data quality measures (ISO/IEC 5259-2:2024)
EN ISO/IEC 5259-3:2025	2025-05-21	Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 3: Data quality management requirements and guidelines (ISO/IEC 5259-3:2024)
EN ISO/IEC 5259-4:2025	2025-05-21	Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 4: Data quality process framework (ISO/IEC 5259-4:2024)
CEN/CLC/TR 18145:2025	2025-02-26	Environmentally sustainable Artificial Intelligence
CEN/CLC/TR 17894:2024	2024-12-18	Artificial Intelligence - Artificial Intelligence Conformity Assessment
CEN/CLC ISO/IEC/TS 1279	2024-11-13	Information technology - Artificial intelligence - Treatment of unwanted bias in classification and regression machine learning tasks (ISO/IEC TS 12791:2024)
CEN/CLC/TR 18115:2024	2024-11-06	Data governance and quality for AI within the European context
EN ISO/IEC 25059:2024	2024-08-07	Software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Quality model for AI systems (ISO/IEC 25059:2023)
EN ISO/IEC 8183:2024	2024-06-12	Information technology - Artificial intelligence - Data life cycle framework (ISO/IEC 8183:2023)
EN ISO/IEC 23894:2024	2024-02-21	Information technology - Artificial intelligence - Guidance on risk management (ISO/IEC 23894:2023)
CEN/CLC ISO/IEC/TR 2402	2023-12-20	Artificial Intelligence (AI) - Assessment of the robustness of neural networks - Part 1: Overview (ISO/IEC TR 24029-1:2021)
CEN/CLC ISO/IEC/TR 2402	2023-12-20	Information technology - Artificial intelligence (AI) - Bias in AI systems and AI aided decision making (ISO/IEC TR 24027:2021)
EN ISO/IEC 23053:2023	2023-06-28	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (ISO/IEC 23053:2022)
EN ISO/IEC 22989:2023	2023-06-28	Information technology - Artificial intelligence - Artificial intelligence concepts and terminology (ISO/IEC 22989:2022)

https://standards.cencenelec.eu/dyn/www/f?p=205:32:0:::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D

CEN/CLC/JTC 21 Work programme

Project	Title	Status	Forecasted voting date
prCEN/CLC/TR XXX(WI=JT021009)	AI Risks - Check List for AI Risks Management	Preliminary	ND
prCEN/CLC/TR XXX(WI=JT021026)	Impact assessment in the context of the EU Fundamental Rights	Preliminary	ND
prEN ISO/IEC TR 23281(WI=JT021002)	Artificial Intelligence - Overview of AI tasks and functionalities related to natural language processing	Under Drafting	ND
(WI=JT021030)	Contributions towards ISO/IEC 27090	Preliminary	ND
prCEN/TS(WI=JT021033)	Guidance for upskilling organisations on AI ethics and social concerns	Preliminary	ND
prCEN/TS(WI=JT021034)	Guidelines on tools for handling ethical issues in AI system life cycle	Preliminary	ND
prCEN/TS(WI=JT021035)	Sustainable Artificial Intelligence – Guidelines and metrics for the environmental impact of artificial intelligence systems and services	Preliminary	ND
prEN ISO/IEC 23282(WI=JT021012)	Artificial Intelligence - Evaluation methods for accurate natural language processing systems	Under Drafting	2026-01-02
prEN XXX(WI=JT021029)	Artificial Intelligence - Cybersecurity specifications for AI Systems	Under Drafting	2026-07-15
EN ISO/IEC 23053:2023/prA1:2025(WI=JT021032)	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) - Amendment 1: Generative AI (ISO/IEC 23053:2022/Damd1:2025)	Under Enquiry	2026-07-17
EN ISO/IEC 23053:2023/prA1:2025(WI=JT021032)	Information technology - Artificial intelligence - Artificial intelligence concepts and terminology - Amendment 1: Generative AI (ISO/IEC 22989:2022/Damd1:2025)	Under Enquiry	2026-07-17
prEN XXX(WI=JT021038)	AI Conformity assessment framework	Under Drafting	2026-07-29
prEN XXX(WI=JT021039)	Artificial Intelligence - Quality management system for EU AI Act regulatory purposes	Under Drafting	2026-07-29
prEN XXX(WI=JT021025)	Artificial Intelligence - Evaluation methods for accurate computer vision systems	Under Drafting	2026-09-02
prEN XXX(WI=JT021044)	Artificial Intelligence - Taxonomy of AI tasks in computer vision	Under Drafting	2026-09-02
prEN ISO/IEC 25059 rev(WI=JT021027)	Software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Quality model for AI systems (ISO/IEC 25059:2023)	Under Drafting	2026-09-21
prEN ISO/IEC 24970(WI=JT021021)	Artificial intelligence – AI system logging	Under Drafting	2026-09-29
prEN 18228(WI=JT021024)	AI Risk Management	Under Drafting	2026-09-30
prEN ISO/IEC 24970(WI=JT021021)	AI trustworthiness framework – Part 1: Logging, transparency and human oversight	Under Drafting	2026-11-30
prEN ISO/IEC 42102(WI=JT021045)	Information technology - Artificial intelligence – Taxonomy of AI system methods and capabilities	Under Drafting	2026-12-07
prEN 18274(WI=JT021019)	Competence requirements for professional AI ethicists	Under Enquiry	2027-01-01
prEN ISO/IEC 25029(WI=JT021046)	Artificial intelligence - AI-enhanced nudging	Under Drafting	2027-01-14
prEN 18229-2(WI=JT021047)	AI trustworthiness framework – Part 2: Accuracy and robustness	Under Drafting	2027-02-25
prEN XXX(WI=JT021036)	Artificial Intelligence - Concepts, measures and requirements for managing bias in AI systems	Under Drafting	2027-03-03
prEN XXX(WI=JT021037)	Artificial Intelligence - Quality and governance of datasets in AI	Under Drafting	2027-03-18
prEN ISO/IEC 42001(WI=JT021048)	Information technology - Artificial intelligence - Management system	Under Approval	2027-06-08

https://standards.cencenelec.eu/dyn/www/f?p=205:22:0:::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1827B89DA69577BF3631EE2B6070F207D

INTERNATIONAL STANDARD

ISO 31000

Second edition 2018-02

INTERNATIONAL STANDARD

ISO/IEC 23894

First edition 2023-02

Risk management — Guidelines

Management du risque — Lignes directrices

Information technology — Artificial intelligence — Guidance on risk management

Technologies de l'information — Intelligence artificielle — Recommandations relatives au management du risque

CyberAgent

Kaunas Faculty

Co-funded by the European Union

IEC ISO

IEC 31010

Edition 2.0 2019-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Risk management – Risk assessment techniques

Management du risque – Techniques d'appréciation du risque

Construction and construction

Scope, Context, Criteria

Risk Assessment

Risk Identification

Risk Evaluation

Records and reporting

Monitoring and review

B.1 Techniques for eliciting views

B.2 Techniques for identifying risk

B.3 Determining sources, causes and drivers of risk

B.4 Techniques for understanding consequence and likelihood

B.5 Techniques for analysing dependencies and interactions

B.6 Techniques for analysing dependencies and interactions

B.7 Techniques that provide a measure of risk

B.8 Techniques for evaluating the significance of risk

B.9 Techniques for selecting between options

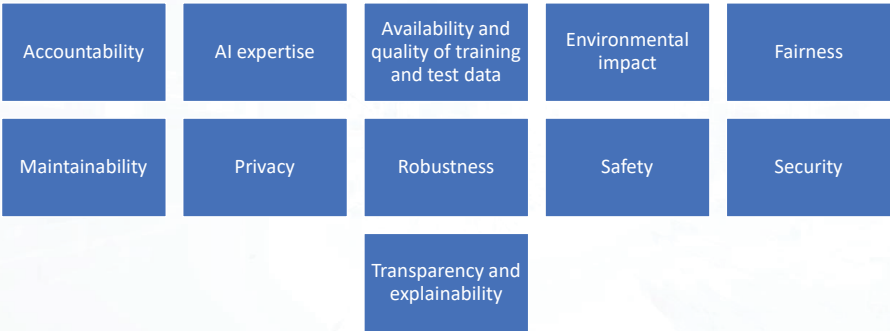
B.10 Techniques for recording and reporting

CyberAgent

Kaunas Faculty

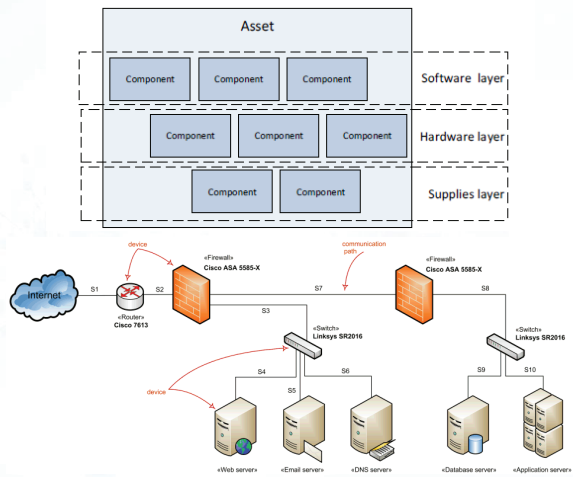
Co-funded by the European Union

Objectives (Annex A to ISO 23894:2023)



Risk Identification Identify Assets

- **“Crown jewels”** - These assets are critical to achieving the overall business objectives and are usually what the attackers would actively seek to exploit
- **“Stepping stones”** - These assets are resources that attackers would want to take control and leverage to pivot across network segments before reaching the crown jewels



AI Asset Taxonomy



- PROCESSES**
- Data Ingestion
 - Data Storage
 - Data Exploration/Pre-processing
 - Data Understanding
 - Data Labelling
 - Data Augmentation
 - Data Collection
 - Feature Selection
 - Reduction/Discretization technique
 - Model selection/building, training, and testing
 - Model Tuning
 - Model adaptation-transfer learning/Model deployment
 - Model Maintenance



- ENVIRONMENT/TOOLS**
- Communication Networks
 - Communication Protocols
 - Cloud
 - Data Ingestion Platforms
 - Data Exploration Platforms
 - Data Exploration Tools
 - DBMS
 - Distributed File System
 - Computational Platforms
 - Integrated Development Environment
 - Libraries (with algorithms for transformation, labelling, etc.)
 - Monitoring Tools
 - Operating System/Software
 - Optimization Techniques
 - Machine Learning Platforms
 - Processors
 - Visualization Tools



- ARTIFACTS**
- Access Control Lists
 - Use Case
 - Value Proposition and Business Model
 - Informal/Semi-formal AI Requirements, GQM (goal/Question/Metric) model
 - Data Governance Policies
 - Data display and plots
 - Descriptive statistical parameters
 - Model framework, software, firmware or hardware incarnations
 - Composition artefacts: AI models, composition builder
 - High-Level Test cases
 - Model Architecture
 - Model hardware design
 - Data and Metadata schemata
 - Data Indexes



- MODELS**
- Algorithms
 - Data Pre-processing Algorithms
 - Training Algorithms
 - Subspace (feature) Selection Algorithm
 - Model
 - Model parameters
 - Model Performance
 - Training Parameters
 - Hyper Parameters
 - Trained Models
 - Tuned Model



- ACTORS/STAKEHOLDERS**
- Data Owner
 - Data Scientists/AI developer
 - Data Engineers
 - End Users
 - Data Provider/Broker
 - Cloud Provider
 - Machine Provider
 - Service Consumers/Model Users



- DATA**
- Raw Data
 - Labeled Data Set
 - Public Data Set
 - Training Data
 - Augmented Data Set
 - Testing Data
 - Validation Data Set
 - Evaluation Data
 - Pre-processed Data Set

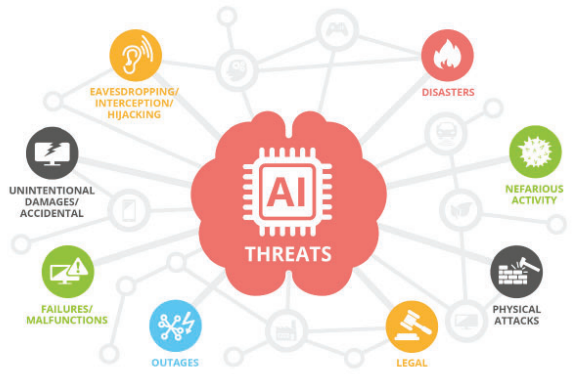
AI Threat taxonomy

ISO/IEC JTC 1/SC 42
Voting begins on: 2022-09-21
Secretariat: ANSI
Voting terminates on: 2022-06-15

Information technology — Artificial intelligence — Risk management

Risk sources (Annex B)

- Level of automation
- Lack of transparency and explainability
- Complexity of environment
- System life cycle issues
- System hardware issues
- Technology readiness
- Risk sources related to machine learning
- And others..



Types of Controls

Under ISO/IEC 27002:2022 controls are categorised as:

- **people**, if they concern individual people, particularly employees, which are a critical part of the information security equation; (8 controls)
- **physical**, if they concern physical objects, which are as important as the digital environment for ensuring information security; (14 controls)
- **technological**, if they concern technology; (24 controls)
- otherwise they are categorised as **organisational**, which focus on the policies, procedures, responsibilities and other organisational-level measures necessary for effective information security (37 controls)

in NIST SP 800-53, REV. 5 controls are organized into 20 families:

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Families of controls (NIST SP 800-53 Rev. 5)

INTERNATIONAL
STANDARD

ISO/IEC
27002

Third edition
2022-02

Information security, cybersecurity and privacy protection — Information security controls

Securité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Contents

1 Scope

2 Normative references

3 Terms, definitions and abbreviated terms

4 Structure of this document

5 Organizational controls

6 People controls

7 Physical controls

8 Technological controls

6.3 Information security awareness, education and training

6.4 Disciplinary process

6.5 Responsibilities after termination or change of employment

6.6 Confidentiality or non-disclosure agreements

6.7 Remote working

6.8 Information security event reporting

7.1 Physical security perimeter

7.2 Physical entry

7.3 Securing offices, rooms and facilities

7.4 Physical security monitoring

7.5 Protecting against physical and environmental threats

7.6 Working in secure areas

7.7 Clear desk and clear screen

7.8 Equipment siting and protection

7.9 Security of assets off-premises

7.10 Storage media

7.11 Supporting utilities

7.12 Cabling security

7.13 Equipment maintenance

7.14 Secure disposal or re-use of equipment

8.1 User endpoint devices

8.2 Privileged access rights

8.3 Information access restriction

8.4 Access to source code

8.5 Secure authentication

8.6 Capacity management

8.7 Protection against malware

8.8 Management of technical vulnerabilities

8.9 Configuration management

8.10 Information deletion

8.11 Data masking

8.12 Data backup prevention

8.13 Information backup

8.14 Redundancy of information processing facilities

8.15 Logging

8.16 Monitoring activities

8.17 Clock synchronization

8.18 Use of privileged utility programs

8.19 Installation of software on operational systems

8.20 Networks security

8.21 Security of network services

8.22 Segregation of networks

8.23 Web filtering

8.24 Use of cryptography

8.25 Secure development life cycle

8.26 Application security requirements

8.27 Secure system architecture and engineering principles

8.28 Secure coding

8.29 Security testing in development and acceptance

8.30 Outsourced development

8.31 Separation of development, test and production environments

8.32 Change management

8.33 Test information

8.34 Protection of information systems during audit testing

Annex A (Informative) Using attributes

ISO/IEC 27002:2022(E)

© ISO/IEC 2022 — All rights reserved

Article 42: Presumption of Conformity

- High-risk AI systems that have been certified or for which a statement of conformity has been issued under a **cybersecurity scheme pursuant to Regulation (EU) 2019/881** <...> shall be presumed to comply with the cybersecurity requirements set out in Article 15 <...>
- Regulation (EU) 2019/881 [Cybersecurity Act] Article 8: **ENISA** shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes <...>

Doc. dr. mult. Paulius Astromskis

Tel.: +370 601 04524

El. p.: paulius.astromskis@knf.vu.lt

Vilniaus universitetas Kauno fakultetas
Muitinės g. 8, Kaunas LT-44280





CyberAgent



Co-funded by
the European Union

Get social with the project!



www.cyberagents.eu



@CyberAgent.EU



@Cyber-Agent-EU



@CyberAgentEU



contact@cyberagents.eu



@Cyber.Agent.EU



@CyberAgentEU

Project Partners





Kaunas
Faculty



Prios



EVM
GRUP



TEKNOPARK
ISTANBUL
TEKNOLOJİLER
AKADEMİSİ



IT
AKADEMIJA



DIEHSEN
ISTANBUL



WOMEN
4CYBER



CYBERAGENT
EU



Boost camp in Lithuania for trainers: cyber security lecturers' workshop: 23-25 September, 2025

Risk Management and Mitigation

[Ilona Veitaitė, Vilnius University (VU)]

CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS

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.



Co-funded by the European Union

www.cyberagents.eu

Outline

- Purpose and Outcomes
- Teaching, Learning and Assessment Methods
- Module Content – Main Topics
- Assessment Strategy
- Studies Material



Co-funded by the European Union

2

Purpose

Enable students, upon completion of the course, to **continuously manage cybersecurity-related risks** in ICT infrastructures, systems, and services by effectively **planning, applying, reporting, and communicating** comprehensive risk analysis, assessment, estimation, and mitigation processes.

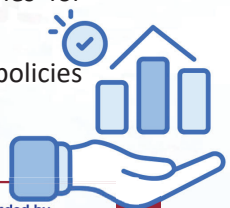


Co-funded by the European Union

3

Outcomes

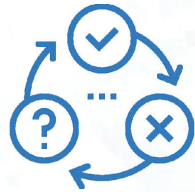
- **Knowledge:** Gain advanced understanding of risk management – identification, assessment, and control – to create cybersecurity routines for SME workplaces in line with standards.
- **Skills:** Apply advanced methods and tools to assess risks, design management strategies, and implement cybersecurity routines for SMEs.
- **Competences:** Develop and execute strategic cybersecurity policies tailored to SME workplaces.



Co-funded by the European Union

Teaching, Learning and Assessment Methods

- Teaching and learning methods will be selected by the lecturer, from Part 1.3. [Teaching Methods, e.g. practical tasks/labs, quizzes, games, technical video analysis, case studies, hands-on activities etc.] of D2.3 “SME Cyber Security Change Agents Learning Pathway’s Structure”
- Assessment methods:
 - Self-assessment tests
 - Knowledge assessment test



Module Content – Main Topics

- Risk Assessment
- Risk Identification
- Insider Threats
- Risk Measurement and Evaluation Models and Methodologies
- Risk Control



Risk Assessment

- Main definitions
- Importance
- General Risk Management Process
- General Risk Management Framework
- Risk Management Standards
- Practical Examples

IT risk assessment



Quantitative risk assessments, or assessments that focus on numbers and percentages, can help you determine the financial impacts of each risk.

Qualitative risk assessments help you assess a risk's human and productivity aspects.

Both categories have value and will allow you to communicate risk with different types of people. For example, your legal and financial teams will likely be most interested in the number. In contrast, your operations teams, such as sales and customer service, will be more concerned about how a security event would affect their operations and efficiency.

Source of image: <https://hyperproof.io/resource/it-risk-assessment/>

Risk Identification

- Leadership and commitment in risk management
- Defining the scope of risk management activities
- External and internal context of the risk management context
- Tangible and intangible sources of risk
- Threats and opportunities
- Vulnerabilities and capabilities

Stéphane Nappo

(Vice President Global Chief Information Security Officer 2018 Global CISO of the year)



Source of image: generated by Copilot, 15/01/2025.

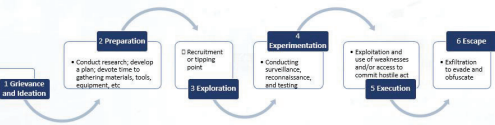
Quote

“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it”.

- Indicators of emerging risks
- The nature and value of assets and resources
- Consequences and their impact on objectives
- Limitations of knowledge and reliability of information
- Biases, assumptions and beliefs of those involved
- Practical examples and case studies

Insider Threats

The transformation of an insider threat into a malicious incident



Source: CISA, Insider Threat Mitigation Guide

CyberAgent

Co-funded by the European Union

- Definition and types of an insider threats
- The costs of insider threats
- Building an insider threat mitigation program
- Detecting and identifying insider threats
- Assessing insider threats
- Managing insider threats
- Practical examples and case studies

Expressions of Insider Threat



Source: CISA, Insider Threat Mitigation Guide

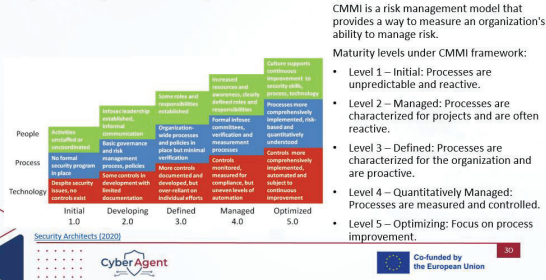
CyberAgent

Co-funded by the European Union

Risk Measurement and Evaluation Models and Methodologies

- Introductory Remarks
- Quantitative and Qualitative Risk Assessment Models and Methodologies
- The likelihood of events and consequences
- The nature and magnitude of consequences
- Complexity and connectivity
- Time-related factors and volatility
- Evaluation of the effectiveness of existing controls
- Sensitivity and confidence levels

Capability Maturity Model Integration



CyberAgent

Co-funded by the European Union

Risk Control

Types of Controls

Under ISO/IEC 27002:2022 controls are categorised as:

- **people**, if they concern individual people, particularly employees, which are a critical part of the information security equation;
- **physical**, if they concern physical objects, which are as important as the digital environment for ensuring information security;
- **technological**, if they concern technology;
- otherwise they are categorised as **organisational**, which focus on the policies, procedures, responsibilities and other organisational-level measures necessary for effective information security

In NIST SP 800-53, REV. 5 controls are organized into 20 families:

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AW	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	Privacy and Information Transparency
CP	Contingency Planning	RA	Risk Assessment
IR	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Families of controls (NIST SP 800-53 Rev. 5)

CyberAgent

Co-funded by the European Union

- Introductory Remarks
- Risk controls
- Identifying and selecting risk treatment options
- Preparing and Implementing risk treatment plans
- Assessing the effectiveness of risk controls
- Deciding whether the remaining risk is acceptable
- Recording and reporting

Assessment Strategy

- Self-assessment tests

Which of the following best describes indirect and intangible consequences of a cybersecurity incident?

- Immediate service disruptions and measurable financial costs.
- Secondary effects like loss of customer trust and long-term brand damage.
- Direct breach of regulatory requirements, leading to fines and legal actions.
- Direct data corruption caused by malware or unauthorized access.

- Knowledge assessment test

How do intangible assets, such as institutional knowledge, benefit a security organization?

- They can be easily replaced with new technologies
- They provide quick recovery and response after an incident
- They improve the speed of hardware upgrades
- They reduce the need for physical security systems

Is the following statement correct/true? Intangible assets are often less important than tangible assets in a security organization.

- False
- True

CyberAgent

Co-funded by the European Union

Studies Material

Required reading

1. Adarsh Nair and Greeshma M. R. (2023) Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing, Limited <https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&query=risk%20management>

2. Gregory J. Falco, Eric Rosenbach (2021) Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford university press, eBook

3. Kristina Narvaez, Betty Simkins, John Fraser (2014) Implementing Enterprise Risk Management: Case Studies and Best Practices. John Wiley & Sons

4. ENISA (2022) Risk Management Standards

5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

6. ISO 31000 Risk management — Guidelines

Recommended reading

1. Shobhit Mehta (2023) ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide. Packt Publishing, Limited <https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management>

2. Peter H. Gregory (2021) CISM Certified Information Security Manager All-in-One Exam Guide. McGraw-Hill

3. ISACA (2021) CRISC Review Manual 7th edition. ISACA

4. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011



13



Kaunas Faculty





Get social with the project!

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

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

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

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

contact@cyberagents.eu

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

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

Project Partners



Kaunas Faculty



AKADEMIJA



WOMEN 4 CYBER



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



Boost camp in Lithuania for trainers: cyber security lecturers' workshop: 23-25 September, 2025

Workshop – use of platform

[Jo Sakariassen, Prios Kompetanse]

CYBER AGENT 2025

Project ID. 10111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS

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.

**Co-funded by the European Union**

www.cyberagents.eu

11:45-13:15	Introduction and Use of the Collaboration Platform <i>Prios Kompetanse AS, Norway</i>
13:15-14:45	Lunch
14:45-15:15	Gamification Elements, Badges, and Certification. Assessment. Piloting One Module. Theory and Practice <i>Prios Kompetanse AS, Norway</i>



CyberAgent trainer workshop

Welcome to an intensive **hands-on** workshop designed to explore our platform from three distinct perspectives in this interactive, **laptop-required** session.



**Co-funded by the European Union**

2



Workshop intro



Purpose

You, not me, should figure out how to use the platform in your context. How can it be useful?



Three perspectives

We will experience the platform as admin, content contributor, and student



Hands-On learning

Don't leave Kaunas without have a clear idea on how the platform works!



**Co-funded by the European Union**

3

WHY WE'RE HERE



Our promise



Your delivery

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

Connect , learn , and grow with a community of SMEs, HEIs and VET providers.

How can you make the platform useful for your organization, how can you keep the promise and make the impact we like to achieve?



**Co-funded by the European Union**

4

WORKSHOP STRUCTURE

01

PLATFORM WALKTHROUGH

Explore admin and student views of the platform functions

02

GROUP WORK

Collaborate based on your assigned role within country groups

03

TOOL EXPLORATION

Use blogs, messages, feedback systems, and learning resources

04

REFLECT & DISCUSS

Share insights and experiences with your group

05

IMPLEMENTATION PLANNING

Develop strategies for using these tools with your learners





Co-funded by
the European Union

5

<https://platform.cyberagents.eu/en>

Home Collaboration Learning content

CyberAgent

English Login

Welcome to CyberAgent

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

CREATE AN ACCOUNT

ABOUT CYBERAGENT







Co-funded by
the European Union

6

GROUP SETUP

PARTNER BASED GROUPS

Form and work in groups

ROLE ASSIGNMENTS (WITHIN YOUR GROUP)

1 Admin per partner (at least)



ADMIN

Manages users, sets up learning content, and oversees platform configuration



CONTENT CONTRIBUTOR

Creates blogs, organises events, and shares knowledge with the community



STUDENT

Completes courses, earns badges, and explores all learning features



Collaborative product transformation
worldwide economy.



Seamless
collaboration,
worldwide impact.





Co-funded by
the European Union

7

This 45+ minute practical session allows each country group to explore the platform collaboratively whilst experiencing multiple user perspectives. Participants will rotate through different roles to gain comprehensive understanding of the system's functionality and user experience.

ADMINS SET UP

Ensure all group members have accounts and course enrolment. Send welcome messages via internal messaging system and schedule a "Lunch-and-Learn" event about phishing awareness.

CONTENT CREATORS SHARE

Publish a blog post on cyber-security topics relevant to training material. Use user search functionality to find another country's admin and send event invitations.

STUDENTS ENGAGE

Complete self-assessment quiz for one topic, then attempt knowledge assessment test. Read a group blog posts, rate usefulness, and connect with participants outside your group.





Co-funded by
the European Union

8

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

ROTATION STRATEGY

After approximately 20 minutes, rotate roles within your group if time permits. This ensures participants experience the platform from multiple perspectives - admin oversight, content creation responsibilities, and student learning journey.

The rotation approach encourages deeper understanding of user needs across different roles whilst maintaining collaborative momentum within country groups.



① Lunch will happen during the session.

Discussion & debrief session

The 45-minute debrief session captures valuable insights from the practical experience. Each group shares observations digitally through prepared forms, focusing on usability, functionality, and user experience across different roles.

O1

SHARE OBSERVATIONS

Groups document what was easy, confusing, or particularly liked using digital forms. Focus on specific features and functionality that stood out during the practical session.

O2

COMPARE ROLE EXPERIENCES

Discuss differences between admin, content creator, and student perspectives. Identify unique challenges and advantages each role encountered during platform interaction.

O3

COLLECT IMPROVEMENT SUGGESTIONS

Gather feedback on navigation, permissions, notifications, and other system elements. Note recurring themes and common pain points across groups.

O4

PRESENT FINDINGS

Each group presents key insights in 5-minute presentations, sharing discoveries and recommendations with all participants.



Let's Begin

1 FORM YOUR GROUP

Connect with colleagues from your country or region

2 ASSIGN ROLES

Distribute admin, content contributor, and student responsibilities

3 LOG IN AND PREPARE

Access the platform and get ready for hands-on exploration

CHECKLIST – EVERYONE!

- ✓ Make a post
- ✓ Sent a message to someone in the room
- ✓ Created an event
- ✓ Done module 8
- ✓ Look into resources for module 8
- ✓ Add some resources for your module
- ✓ Search and find a user
- ✓ Check your profile page and add something
- ✓ As Admin – administrate you users



**Kaunas Faculty**



**Co-funded by the European Union**

Get social with the project!

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

[@CyberAgent.EU](#)

[@Cyber-Agent-EU](#)

[@CyberAgentEU](#)

contact@cyberagents.eu

[@Cyber.Agent. EU](#)

[@CyberAgentEU](#)

Project Partners

**Kaunas Faculty**

**Prios**

**EVM GROUP**

**TEKNOPARK ISTANBUL**
TEKNOLOJİLER

**IT AKADEMIJA**



**WOMEN 4 CYBER**





CyberAgent

WP2 Training needs report

Boostcamp Kaunas

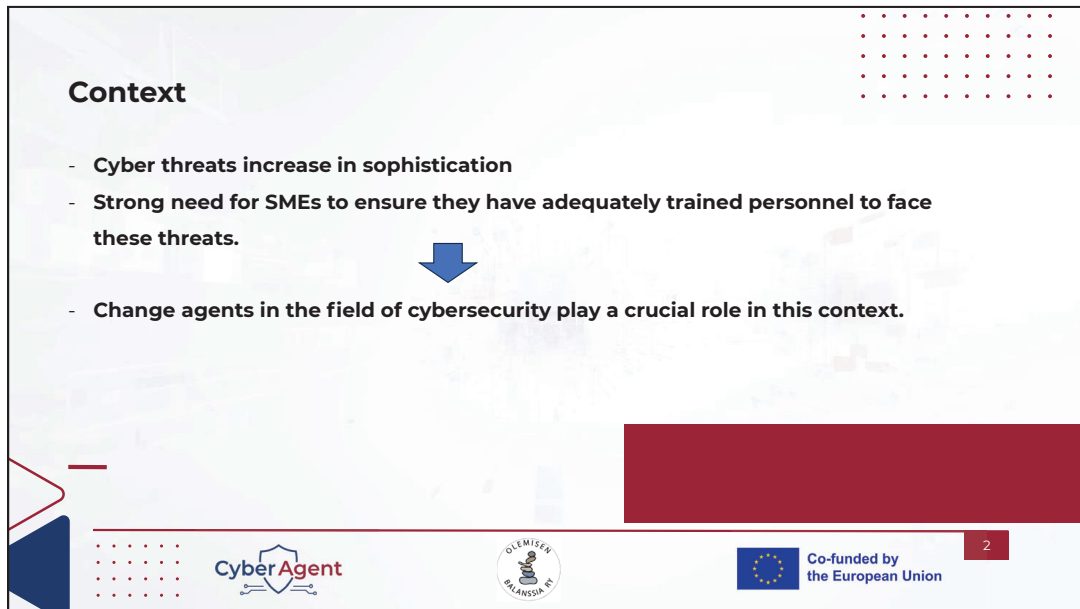
CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO Type of Action: ERASMUS-LS

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.

 Co-funded by the European Union

www.cyberagents.eu



Context

- Cyber threats increase in sophistication
- Strong need for SMEs to ensure they have adequately trained personnel to face these threats.

↓

- Change agents in the field of cybersecurity play a crucial role in this context.

CyberAgent

  Co-funded by the European Union

2



Objective

Analyse and map the training needs to identify the appropriate competences required for an SME Cyber Security Change Agent

- comprehensive review of current educational offerings
- understanding the preferences of the SMEs regarding cybersecurity issues

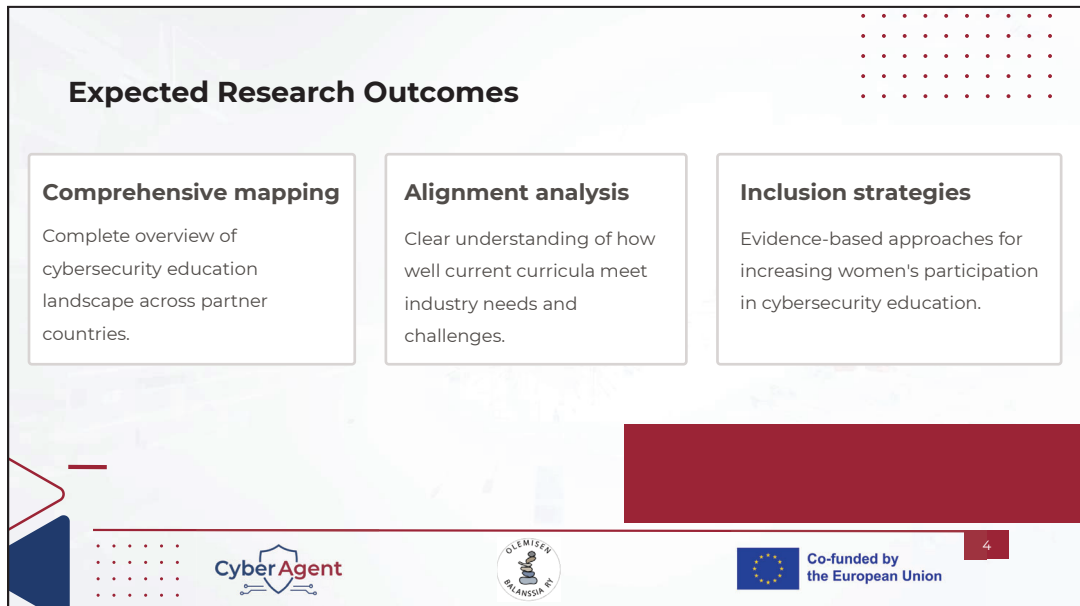
↓

Bridge the gap between current & required competencies and define the ideal skill set required.

CyberAgent

  Co-funded by the European Union

3



Expected Research Outcomes

Comprehensive mapping

Complete overview of cybersecurity education landscape across partner countries.

Alignment analysis

Clear understanding of how well current curricula meet industry needs and challenges.

Inclusion strategies

Evidence-based approaches for increasing women's participation in cybersecurity education.

CyberAgent

  Co-funded by the European Union

4



Methodology

Desk research + Field research



5

Desk research methodology

Literature review

Comprehensive analysis of existing and emerging educational provisions across partner countries.

Source compilation

Sourcing articles, white papers, research and reports on cybersecurity training content and needs.

Curriculum analysis

Examining VET and HE courses and their relevance to real-world challenges.



6

Desk research methodology

Studied educational levels

VET Level



Vocational Education & Training programmes focusing on practical cybersecurity skills and industry-ready competencies.

In 8 EU countries



Higher Education



University-level programmes emphasising theoretical foundations and advanced cybersecurity concepts.



8

Desk research methodology

Curriculum analysis framework

1

Current Components

Mapping existing curriculum elements across different educational institutions and countries.

2

Real-World Relevance

Evaluating alignment between academic content and industry cybersecurity challenges.

3

Gap Identification

Highlighting areas where educational provision may not meet current industry demands.



9



Field research methodology

Dual survey approach

Teachers & Trainers Survey

Designed for VET & HE educators from each country to understand current training provisions and identify gaps in cybersecurity education.

SME Employee Survey

Tailored to small and medium enterprises to assess employee engagement, challenges, and training needs in cybersecurity practices.

Special focus on determining characteristics, training needs, and learning preferences, particularly highlighting the needs of women in cybersecurity.



Co-funded by the European Union

10

Field research methodology

The research in numbers



8 countries covered



190 respondents from education institutions

 **HEI: 104**
VET: 86

176 employees surveyed





Co-funded by the European Union

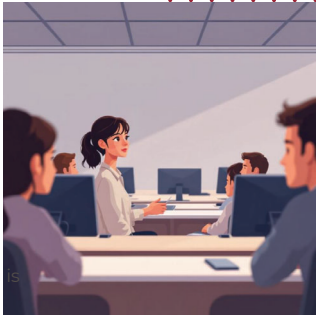
11

Field research methodology

Key Focus Areas

- Current training provisions in VET and Higher Education
- Gaps in cybersecurity curriculum
- Teaching methodologies and resources
- Gender representation challenges

The educator survey revealed insights into how cybersecurity training is currently delivered and where improvements are needed.





Co-funded by the European Union

12

Women in Cybersecurity

The Gender Gap Crisis

18.5%

Women ICT Specialists

Share of women among ICT specialists in EU27 in 2020

11%

Cybersecurity Women

Women working in cybersecurity globally

25%

Workforce Share

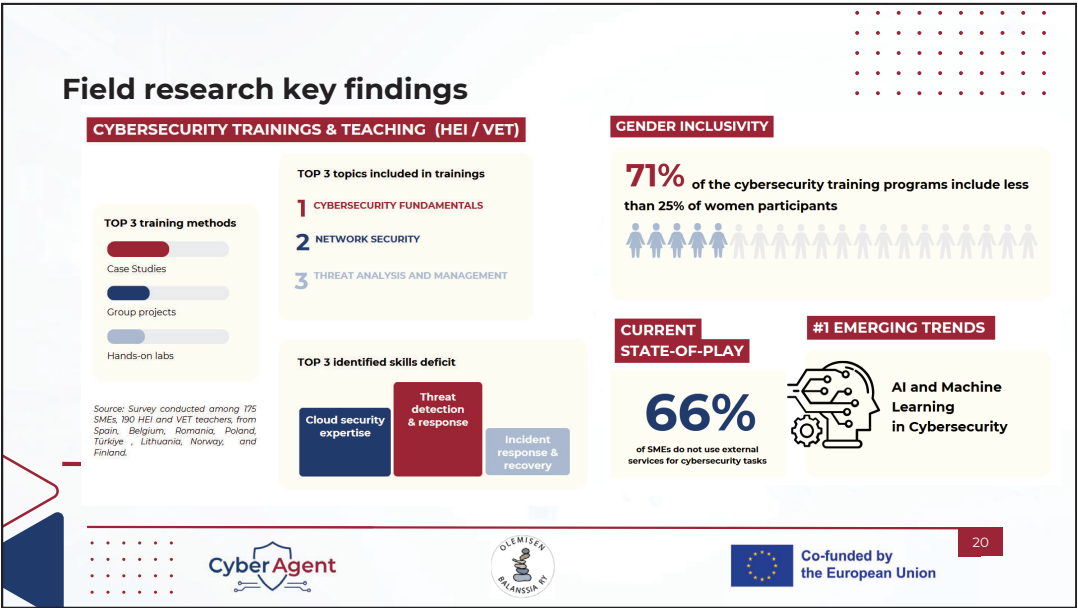
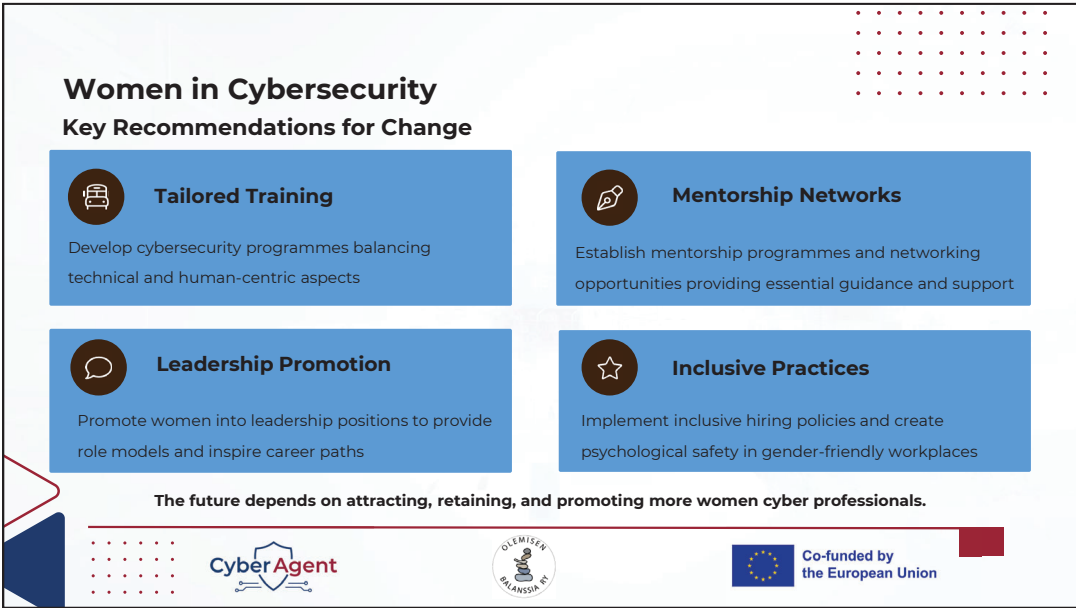
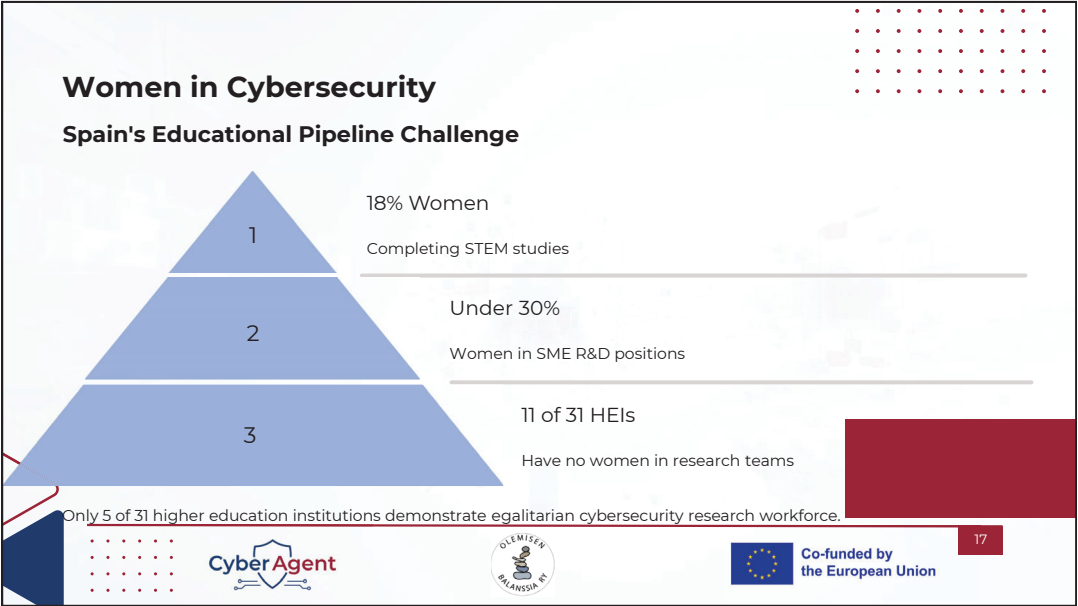
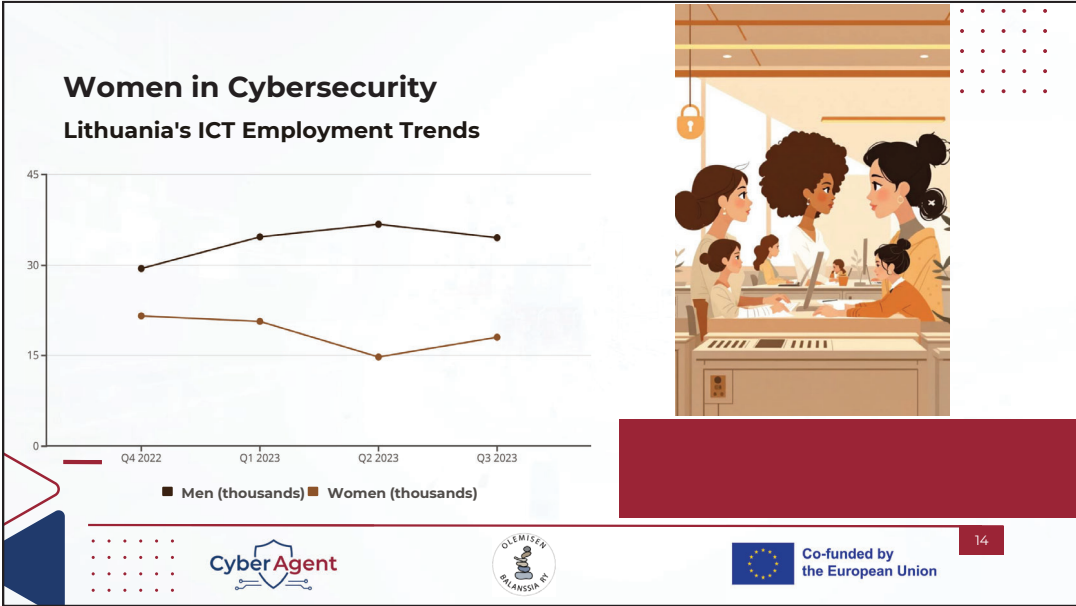
Women in cybersecurity vs 39% overall workforce

Microsoft's survey across 35 European countries found fewer than 1 in 5 computer science graduates were women.



Co-funded by the European Union

13



Field research key findings

TOP 3 competencies and knowledge area needs

Data Privacy and Protection

Risk Assessment & Management

Incident Response & Recovery

TOP 3 identified gaps

1 LOW LEVEL OF THREAT AWARENESS

2 LOW LEVEL OF CYBERSECURITY REGULAR TRAININGS

3 LOW LEVEL OF VULNERABILITY ASSESSMENT

Source: Survey conducted among 175 SMEs from Spain, Belgium, Romania, Poland, Türkiye, Lithuania, Norway, and Finland.

TOP 3 cybersecurity threats

Phishing & social engineering

AI-driven cyber-attacks

Ransomware attacks



Co-funded by the European Union

21

Training preferences and needs

Area 1 - Foundational Knowledge and Skills

Priority Areas

Cybersecurity fundamentals and network security are essential foundations requiring immediate attention.

Critical Gaps

Significant deficits in threat detection, cloud security, data privacy, and risk management.

SME Focus

Strong need for cybersecurity content specifically oriented towards small and medium enterprises.





Co-funded by the European Union

22

Training preferences and needs

Area 2 - Specialized Topics

Advanced Techniques

- Threat analysis and management
- Cryptography
- Advanced threat mitigation

Emerging Threats

- AI-driven cyber-attacks
- Ransomware attacks
- Phishing and social engineering
- Cloud security breaches
- IoT vulnerabilities





Co-funded by the European Union

23

Training preferences and needs

Area 3 - Practical Application

Hands-on Labs

Interactive laboratory sessions for practical experience in cybersecurity techniques and tools.

Case Studies

Real-world scenarios to bridge theory and practice, developing critical thinking skills.

Group Projects

Collaborative learning for problem-solving abilities and mirroring workplace dynamics.





Co-funded by the European Union

24

Qualification profile of a SME cyber security change agent

At EQF level 4/5 and at EQF level 6

Foundational knowledge and skills

Advanced and leadership-oriented abilities



25

Qualification profile of a SME cyber security change agent

At EQF level 4/5: Cybersecurity Foundations

Cybersecurity Fundamentals

Master basic concepts, understand protection importance and identify attack vectors.

Security Best Practices

Apply protection tools, identify risks, and implement security protocols effectively.

Risk Management

Assess potential threats and understand basic mitigation strategies.

Communication

Report security threats and issues clearly to appropriate stakeholders.



26

Qualification profile of a SME cyber security change agent

At EQF level 6: Advanced Cybersecurity Leadership

Advanced Concepts & Response

Master sophisticated cybersecurity principles and lead incident response and recovery operations.

Security Architecture Expertise

Design robust security frameworks and implement comprehensive network defence systems.

Strategic Leadership

Lead cybersecurity initiatives and make critical security decisions for organisations.

Advanced Risk Management

Design and implement comprehensive risk management strategies across enterprise systems.



27

Get social with the project!

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

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

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

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

contact@cyberagents.eu

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

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

Project Partners





Boost camp in Lithuania for trainers: cyber security lecturers' workshop: 23-25 September, 2025

Practical upskilling of SME Cyber Security Change Agents

[Adelina Luntraru, EVM Group]

CYBER AGENT

Project ID: 101111732

Call: ERASMUS-EDU-2022-PI-ALL-INNO

Type of Action: ERASMUS-LS

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.



Co-funded by the European Union

www.cyberagents.eu

2025

Objectives

- Evaluate the effectiveness and quality of CyberAgent cybersecurity modules and platform for professionals in SMEs and students from HEIs and VET institutions in partner countries.
- Establish SME Cyber Security Change Agents by upskilling at least **240 individuals** (SME employees, HEI, and VET students) in cybersecurity across all partner countries in the first year.
- Foster a knowledgeable workforce equipped to address present and future cybersecurity challenges within the SME sector.



2

Preparation

- Review of the pilot plan and assessment plan.
- Identification of stakeholders.
- Translation and validation of forms and additional documents. (agreements, contents)



3

CyberAgent network

The **CyberAgent network of SMEs**, formed during the project, will be the foundation for upcoming activities, inviting members to participate in training program testing and implementation to enhance their cybersecurity capabilities.

To maximize the impact and achieve the targeted outcomes—particularly in terms of upskilling women to become proficient cybersecurity agents within SMEs and training HEI and VET students—it is essential for project partners to consider **expanding the network further**.

- **SMEs that employ women**
- **Universities**
- **VET providers**



4

Formalize the collaboration of stakeholders with the project

- To ensure smooth collaboration, stakeholders should sign an agreement outlining roles and responsibilities.
- A standardized agreement template will be provided for partners to complete during participant selection.
- Partners are encouraged to recruit at least **10 enterprises, one university, and one VET provider** from their countries.



5

Participant profile

The pilot and training process is specifically designed to cater to diverse trainee profiles, including:

- **Higher Education Institution (HEI) students**
- **Vocational Education and Training (VET) students**
- **Current SME employees, with a particular focus on women**



6

Selection of participants - HEI and VET students

- Contact with educational institutions from each partner country that could be interested in the project and involve their teachers in the training program implementation (a collaboration agreement is recommended to be signed between the educational institution and the national project partner).
- It is vital to identify and involve teachers from the educational institutions in this activity as well, to help the students in the learning process and supervise the process together with the specialized trainers.
- Together with the educational centre and the teachers involved select the group of students (a class or course) that will have the interest, the time and the motivation to engage in this learning process. **Confirm the participation of minimum of 10 HEI students and 10 VET students from each country which will fill the commitment form and register on the platform.**



7

Selection of participants - SME employees

- Identify at least 15 potential candidates, employees of SMEs, from the local CyberAgent network or expand the reach.
- **Confirm the participation of minimum 10 participants (of which minimum 4 women) per country which will fill the commitment form and register on the platform.**



8

Implementation of the piloting and upskilling training program

- The training at the local level will be organized by each project partner in coordination with the specialists who participated in the international Train the Trainer Boostcamp organized in Lithuania between the 23rd and the 25th of September 2025.
- The training will have a hybrid format, with off the platform meetings between the trainers and the learners and the use of the platform as a learning space and for direct communication between the learners and with the trainers.
- The training program will begin with an introductory session involving all selected participants, during which trainers will introduce the platform and outline the available modules. A midterm session will be held to review progress, followed by a closing session to gather feedback, encourage ongoing engagement with the platform, and promote continued learning. Trainer support will be provided throughout the entire training period.
- The participants will start the training process according to their own needs and in their own rhythm, but ensuring that each module is being used by at least one participant to cover the piloting objectives of all the materials created.
- The participants must finish at least one module and receive the certification by the end of the piloting /training period.
- The participants must fully complete the assessment plan.

**for HEI and VET students, teachers from the local educational centers will work closely with the trainers*



9

Data collection - assessment plan

- An **initial evaluation** of participants' cybersecurity knowledge and learning needs will be conducted. Based on this assessment, trainers (in the case of students the collaboration of the teachers involved in the project will be required) will recommend a personalized learning path, highlighting the modules best suited to address the identified needs. Additionally, during the initial sessions with trainers, participants' motivation for undertaking the training course will be discussed in a group setting.
- A **mid-term follow-up** will be conducted to check progress and determine whether additional support or motivation is required to help participants achieve the established learning objectives.
- The **final evaluation** will be carried out through the platform to award the certificate, supported by a final assessment form that will evaluate the platform's effectiveness, the quality of the materials, and the overall training experience. Additionally, the closing sessions will provide an opportunity for participants to give more personalized, direct feedback.



10

Data collection - assessment plan

- All the evaluations included in the assessment plan will be collected through Multilanguage Microsoft digital forms, created by the Quality responsible of the project Olemisem
- The national partner ensures that they are completed by all the participants involved in the piloting in the project 's timeline for this activity and that all the quantitative indicators of participation are met.
- The forms will be stored as a database on the project 's Sharepoint repository and used for future reports.



11

Transnational synthesis

- Creation of national reports in English by all partners of the input collected through the assessment plan and the overall piloting activity to Olemisem within the established deadlines.
- Integration and comparative analysis, and preparation of the General Report of the CyberAgent Piloting activity with results and recommendations made by Olemisem (D5.3)



12

Timeline for the upskilling program



Expected results

- 80 HEI students who will pilot test the curriculum across 8 countries
 - 80 VET students trained
 - 80 SME employees, with minimum 30 women, from 8 countries, participating in the cybersecurity training programme as trainees, with attendance rate of at least 75%.
 - minimum 30 training hours per country
 - 10 self-evaluation sheets of the cybersecurity training programme by the participants per country
 - minimum level of satisfaction: 80%
 - 10 HEI teachers and 24 VET teachers involved in the piloting
- CyberAgent** Co-funded by the European Union 14

Get social with the project!

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.



Project Partners





WP5 CyberAgent upskilling Training Program Evaluation

Boostcamp Kaunas

CYBER AGENT 2025

Project ID: 101111732

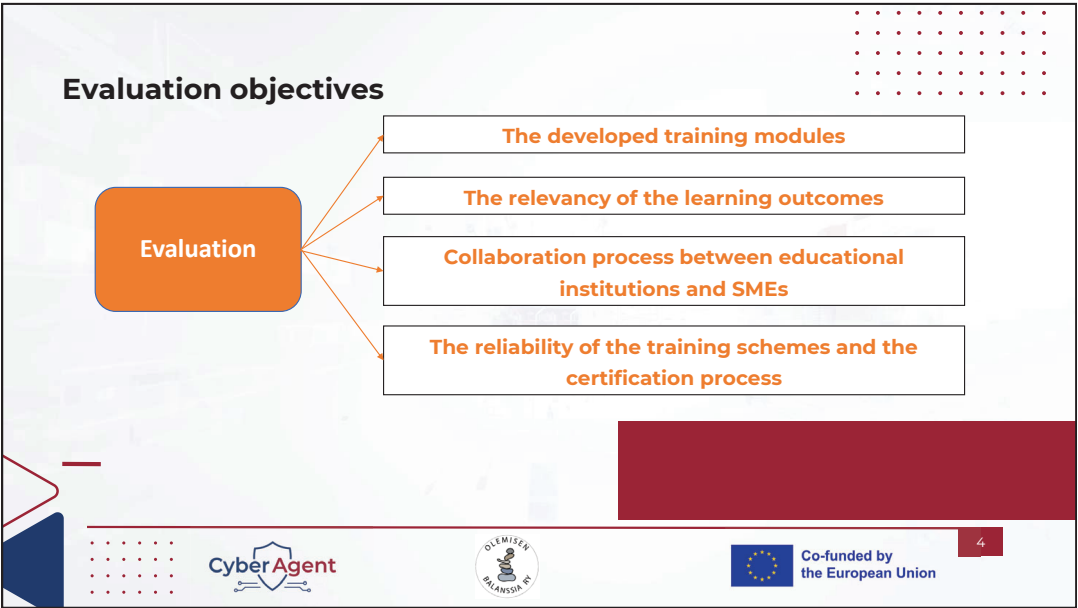
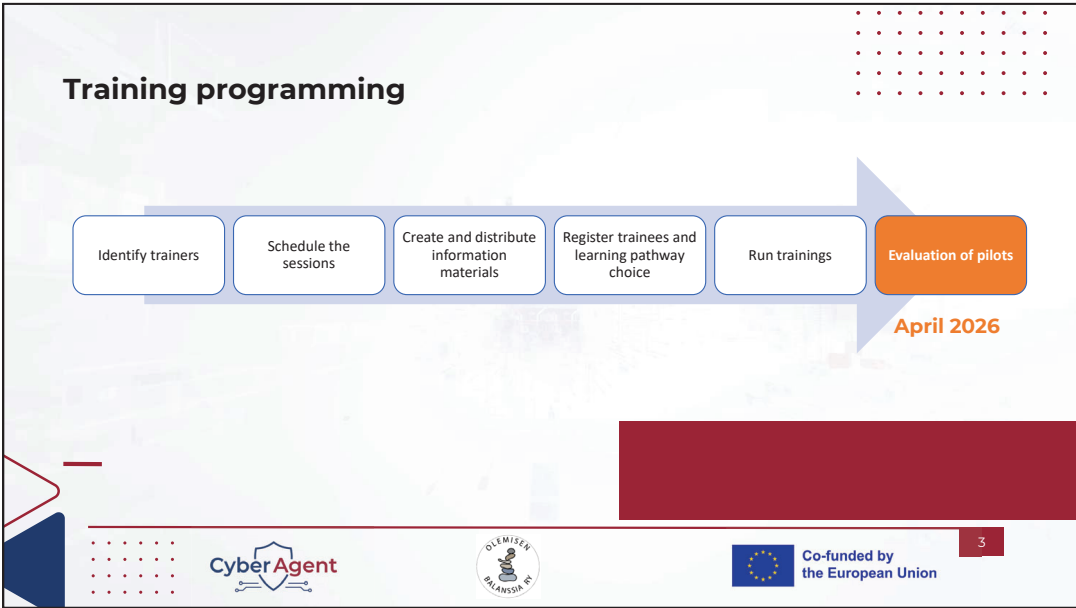
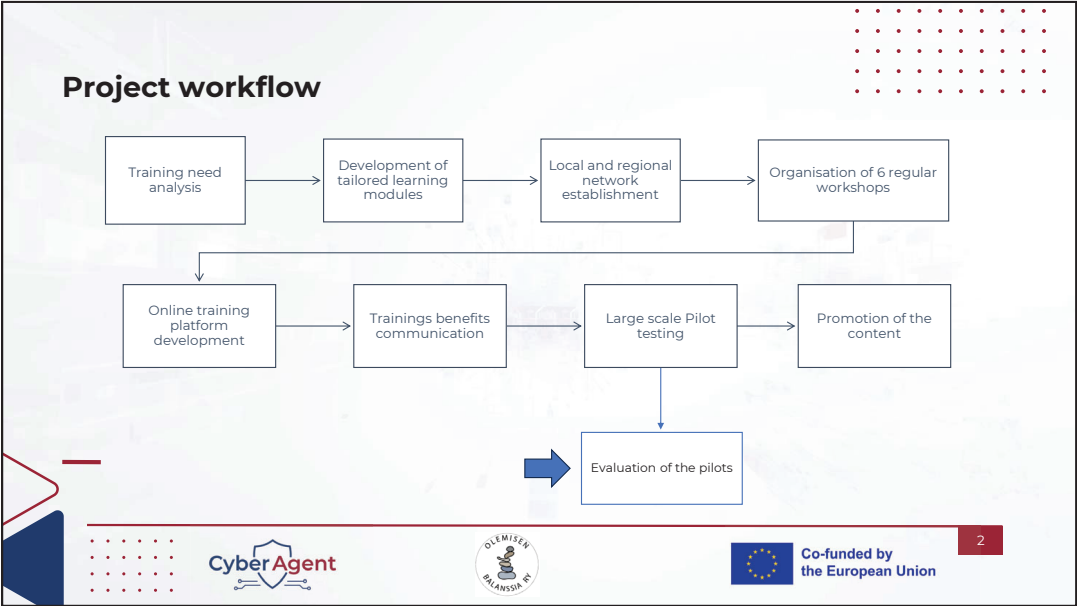
Call: ERASMUS-EDU-2022-PI-ALL-INNO

Type of Action: ERASMUS-LS

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.

 Co-funded by the European Union

www.cyberagents.eu



Evaluation survey

Section 1: General information

What is your role?

VET student

HEI student

SME Employee

Other (please specify): _____

Gender: M/F

How did you participate in the pilot training?

Online learning

In-person workshop

Blended (online & in-person)



5

Evaluation survey

Section 2: Training modules (clarify if 1 module per group to be pilot tested)

Please rate the following statements (1 = Strongly Disagree, 5 = Strongly Agree):

3. The training modules were clear and easy to follow.

4. The training materials (slides, exercises, examples) were practical and useful.

5. The modules addressed real cybersecurity needs relevant to my context (education/SMEs)

Open Question:

6. What part of the modules did you find most useful, and why?



6

Evaluation survey

Section 3: Learning outcomes

Likert Scale (1–5):

7. The learning outcomes of the training were relevant and clearly defined.

8. I was able to achieve the intended learning outcomes.

9. The training improved my skills and knowledge in cybersecurity.



7

Evaluation survey

Section 4: Reliability of training & certification

Likert Scale (1–5):

11. The training scheme was well-structured and reliable.

12. The assessment and evaluation methods were fair and transparent.

13. The certification process was clear and relevant. (ECTS delivery?)

Open Question:

14. Any comment about the certification process?



8

Evaluation survey

Section 5: Collaboration between educational institutions & SMEs (Depending on availability/use of collaboration features during piloting)
Likert Scale (1-5):
15. The collaboration between educational institutions and SMEs added value to the training.
16. The training reflected both academic and practical workplace needs.
17. Opportunities for networking and collaboration were provided.

Open Question:
18. Any comment on the collaboration features between SMEs and educational institutions?



9

Evaluation survey

Section 6: Training delivery (to be adjusted depending on how the piloting are implemented)
Likert Scale (1-5):
19. The teachers/trainers were knowledgeable and effective **OR** the learning pathway was relevant and effective.
20. The training methods (lectures, case studies, hands-on tasks) were engaging.
21. The time allocation and pacing of the training were appropriate.



10

Evaluation survey

Section 7: Impact
Likert Scale (1-5):
22. The training increased my confidence in applying cybersecurity skills.
23. I can apply the acquired knowledge in my daily work/studies.
23b. I feel competent to manage
24. The training will positively impact my career or my organization.



11

Evaluation survey

Section 8: Final feedback (if relevant)
What were the **strengths** of the training?
What were the **weaknesses** of the training?
Any other comments or suggestions?



12

Additional impact items

Project indicators during the piloting

- Number of trained students/employees,
- Number of interactions on the platform
- Number of registered users
- Any statistics from the platform (number of finished module, downloaded content, etc...)



13

Deliverable

- **Evaluation report after piloting.**
- **20 pages PDF in English.**



14

Do we go further for impact measurement?

- **Pre- & post-training test (test, quiz, practical exercise)**



15



Get social with the project!

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

[@CyberAgent.EU](#)

[@Cyber-Agent-EU](#)

[@CyberAgentEU](#)

contact@cyberagents.eu

[@Cyber.Agent. EU](#)

[@CyberAgentEU](#)

Project Partners





CyberAgent

Module 4 – Security operations

Boostcamp Kaunas

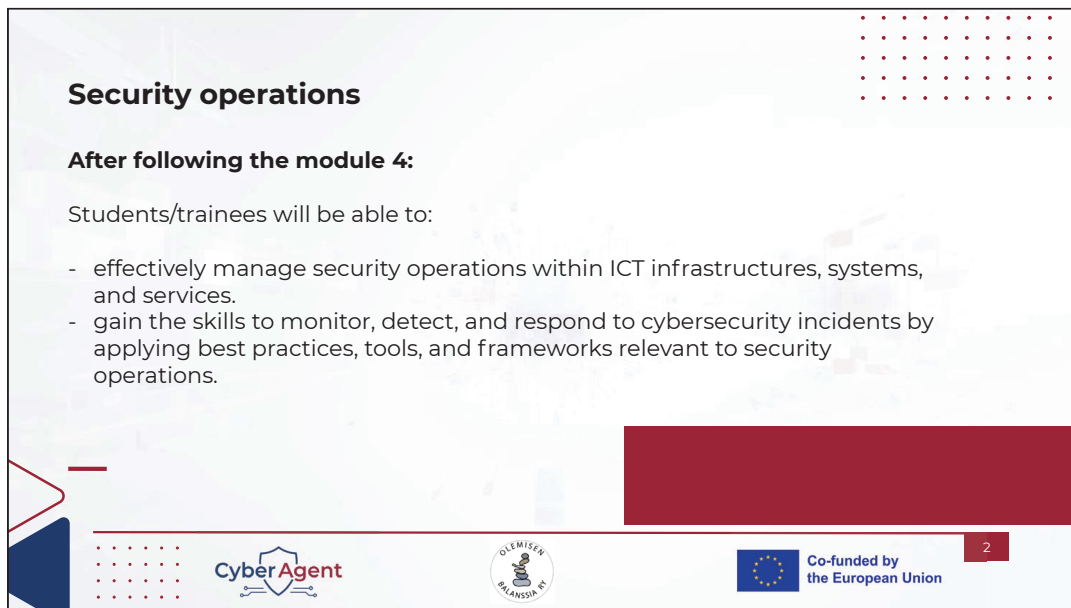
CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO Type of Action: ERASMUS-LS

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.

 Co-funded by the European Union

www.cyberagents.eu



Security operations

After following the module 4:

Students/trainees will be able to:

- effectively manage security operations within ICT infrastructures, systems, and services.
- gain the skills to monitor, detect, and respond to cybersecurity incidents by applying best practices, tools, and frameworks relevant to security operations.

   Co-funded by the European Union

2



Security operations

Module breakdown

Unit 1 - Security Operations fundamentals

- Understanding Security Operations and SOC (Security Operations Centre)
- Roles and responsibilities in Security Operations
- SOC Tools: SIEM, EDR, XDR, MDR and SOAR explained

   Co-funded by the European Union

3



Security operations

Module breakdown

Unit 2 - Security Convergence

- Understanding security convergence
- Fundamentals of physical security (physical security principles, protecting physical assets, policies)
- Case studies highlighting convergence issues

   Co-funded by the European Union

4

Security operations

Module breakdown

Unit 3 - Security Information and Events Management

- Review of security monitoring principles
- Implementing SIEM solutions
- Setting up logs and alerts



Co-funded by the European Union

5

Security operations

Module breakdown

Unit 4 - Security Operations Practices

- Identify data sources and optimize log collection
- Centralising alerts with the SIEM
- Testing your SIEM



Co-funded by the European Union

6

Context

Why are Security Operations needed?

- Need for continuous, proactive defense
- Business continuity, IP and reputational protection
- Evolving threats (ransomware, phishing, nation-state attacks)
- Increasing complexity in IT environments (cloud, IoT, remote work)



Co-funded by the European Union

7

Defining Security Operations

Security Operations are the continuous processes and tasks aimed at:

- Monitoring IT environments for anomalies
- Detecting and analyzing potential security events
- Coordinating a swift and effective response to incidents

Those processes allows to minimizes risk and impact of cyber threats



Co-funded by the European Union

8

Why setting-up a SOC?

24/7 Vigilance

Continuous monitoring of networks, endpoints, servers and databases ensures round-the-clock protection against threats.

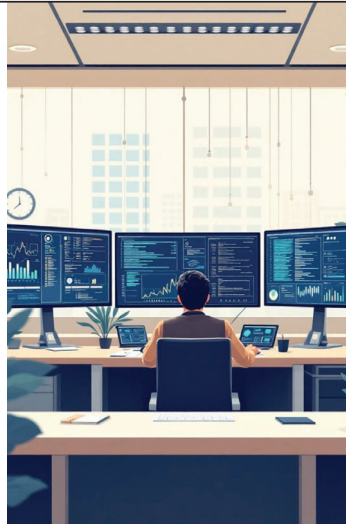
Rapid Detection

Bridge the critical gap between system compromise and threat detection, minimising potential damage.

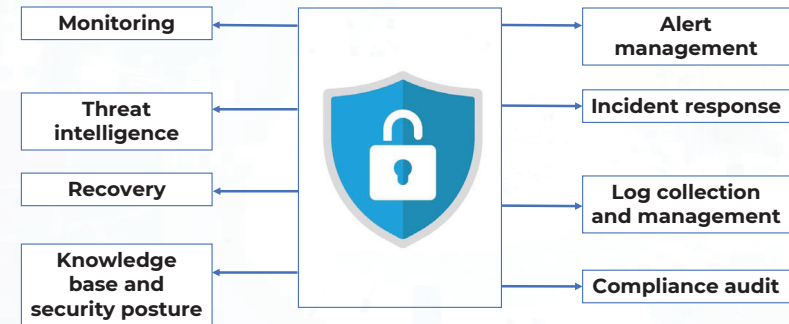
Comprehensive Defence

Stay ahead of evolving threats regardless of source, timing or attack methodology.

A SOC provides the advantage businesses need to defend against incidents and intrusions, maintaining security posture around the clock.



Key Security Operations Center principles



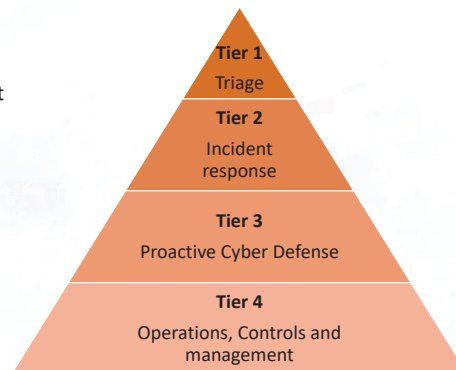
SOC Team structure

The SOC team roles and responsibilities:

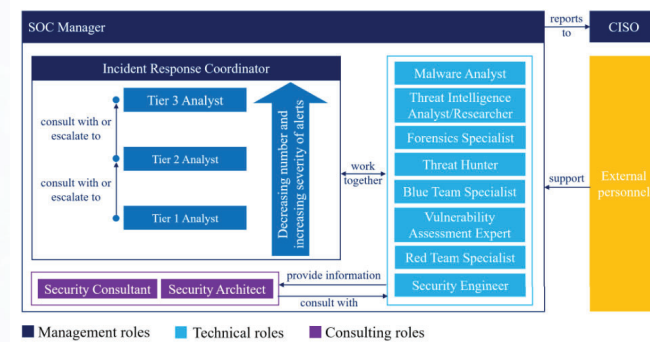
The structure of a SOC team consist of different tiers of SOC analysts and managers.

Tier 1-3 SOC focus on the tactical activities of managing a SOC either defensively (Tier 1-2) or proactively hunting threats (Tier 3).

Tier 4 SOC produce, report, and maintain performance metrics for optimal protection

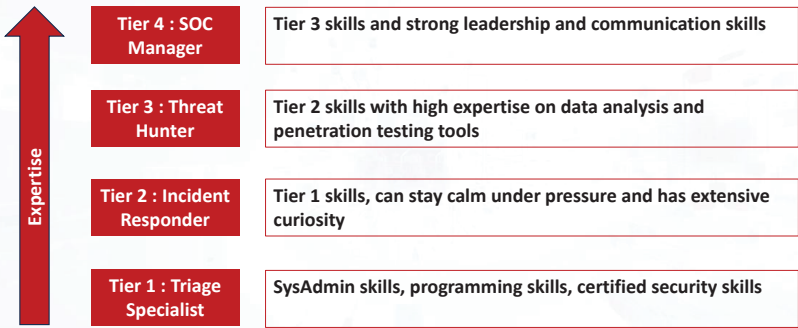


Overview of the SOC Team roles connections



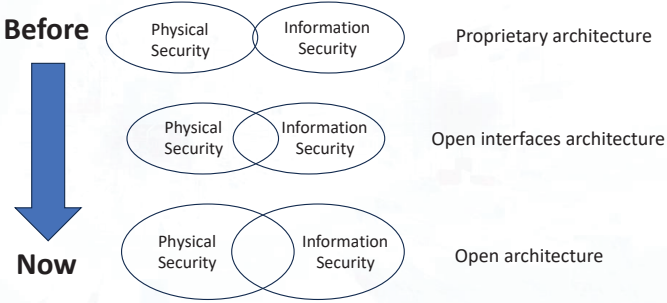
Source: M. Vielberth et al.: Security Operations Center: A Systematic Study and Open Challenges

SOC Team necessary skills



Unit 2 - Security Convergence

It refers to the integration of physical and information security strategies, technologies, and processes into a unified framework.



Training details

- In this training, we explore
- how integrating physical and cyber security systems, known as converged security, provides a more robust defense mechanism.
 - real-world implementations and explore a rule-based engine that links physical events, like door access, to information system event, like login attempts, from behind the scene.
 - how they are designed and how it is working at the back end.

main source of pictures and content: [A Case Study on Converged Security with Event Correlation of Physical and Information Security Article in International Journal of Security and Its Applications - September 2015](#)

Real-Time Alerts and Outputs

- Alerts include timestamp, user/device ID, rule triggered.
- Logs are available for auditing and analysis.
- System supports fast operator response.

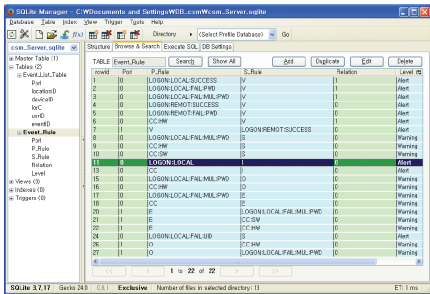


Figure 8. Event Rule Database Implemented with SQLite DBMS

Unit 3 - Security Monitoring

Security monitoring is the continuous process of collecting, analyzing, and responding to security events and incidents.

- **Purpose:** Ensures early detection of threats and minimizes the impact of cyberattacks.
- **Importance:** Forms the backbone of any modern cybersecurity program



Source: freepik

17

Keywords concept

- **Event:** Any observable occurrence in a system or network.
- **Alert:** Notification about a potential threat or anomaly.
- **Incident:** A confirmed breach or compromise that needs action.

18

Key Components of a Monitoring System

- **Log Sources:** Devices generating logs (servers, firewalls, endpoints).
- **Collection Mechanisms:** Agents or protocols (Syslog, Windows Event Forwarding).
- **Storage & Analysis Tools:** SIEM platforms or log aggregators.
- **Response Systems:** Tools that initiate alerts or automated responses.

19

Types of Monitoring

- **Network Monitoring:** Observing traffic patterns and protocols.
- **Endpoint Monitoring:** Tracking activities on end-user devices.
- **Cloud Monitoring:** Watching over cloud-based infrastructure and services.
- **Application Monitoring:** Ensuring application security and uptime.



Source: freepik

20

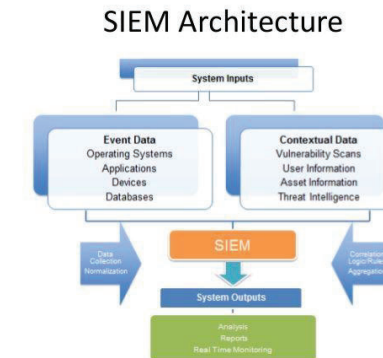
What is a SIEM?

SIEM (Security Information and Event Management) systems collect, normalize, correlate, and analyze security data from across an IT environment.

Function: Provides centralized visibility, alerts, and incident response capabilities.

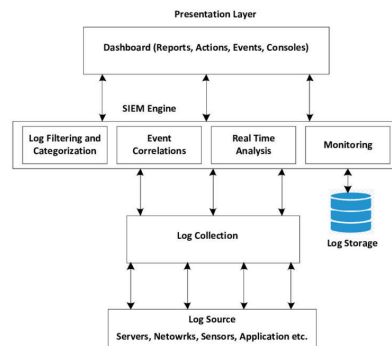
Benefit: Enables proactive threat detection and compliance management

SIEM architecture



SIEM Architecture Overview

- **Data Sources:** Firewalls, servers, endpoints, IDS/IPS.
- **Collectors/Agents:** Pull or receive log data.
- **Processing Engine:** Normalization, correlation, rule application.
- **Storage Layer:** Indexed or archived log data.
- **User Interface:** Dashboards, alerts, investigation panel.



Source: [ScienceDirect](#) (under CC licence)

Core Functions of SIEM

- **Log Collection:** Gather logs from diverse sources.
- **Normalization:** Convert logs to a consistent format.
- **Correlation:** Identify patterns or related events.
- **Alerting:** Generate real-time security notifications.
- **Dashboarding:** Visualize security status.
- **Reporting:** Support audits and compliance.

Installing and configuring SIEM

- **Select OS:** Linux is often preferred (e.g., Ubuntu).
- **Download & Install SIEM:** Use installation scripts or packages.
- **Configure Basic Settings:** Network, hostname, time sync.
- **Start Services:** Validate functionality.

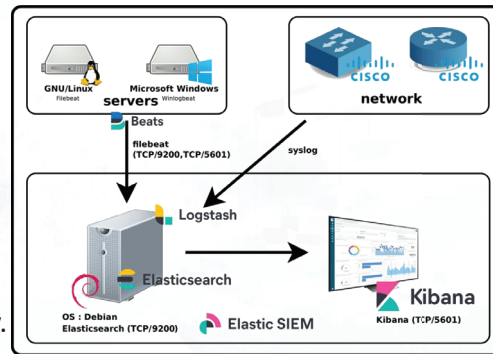
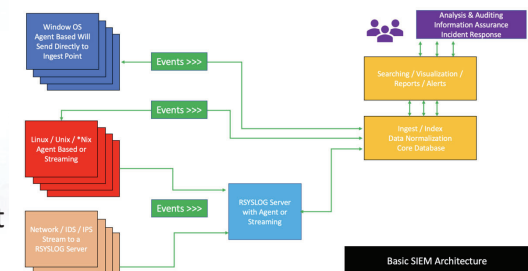


Illustration of Elastic SIEM installation, Source: Elastic

Configuring Log Collection

- **Syslog Integration:** For network devices and Linux.
- **Windows Event Forwarding:** Use Winlogbeat or agents.
- **Custom Logs:** Applications or audit logs.
- **Agent Deployment:** Install collectors on source machines.



Source: Under CC licence

Data Normalization

```
127.0.0.1 user-identifier andy [12/Nov/2021:20:25:11-0700] "GET /apache_pb.gif HTTP/1.0"
```

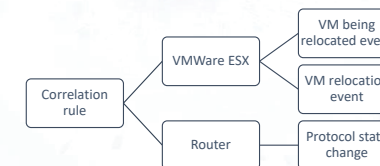
With

"127.0.0.1" refers to the client's IP address when a server request is made.
 "user-identifier" refers to the client's identification protocol.
 "andy" refers to the user ID.
 "[12/Nov/2021:20:25:11-0700]" refers to the date and time the request was made.
 "\"GET /apache_pb.gif HTTP/1.0\"" refers to the client's request.

- **Purpose:** Standardize logs from various systems.
- **Method:** Use parsers or templates.
- **Benefit:** Enables unified analysis and correlation.

Event Correlation Rules

- **Rule Engine:** Detects patterns like failed logins followed by access.
- **Thresholds:** Limit alerts to specific volume/time.
- **Boolean Logic:** Combine events using AND/OR/NOT.



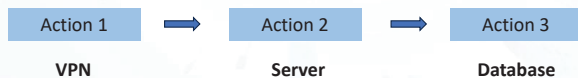
Creating Custom Correlation Rules

Scenario Example: If 5 failed logins + 1 successful login in 10 min.

Then Rule Elements: Source IP, user account, time window.

Action: Alert or automated script execution.

The correlation engine associates events from different log sources to identify security threats at an early stage



Dashboards and Visualization

- **Purpose:** Provide security overview at-a-glance.
- **Widgets:** Maps, graphs, timelines.
- **Customization:** Tailor by role (SOC, management, compliance).

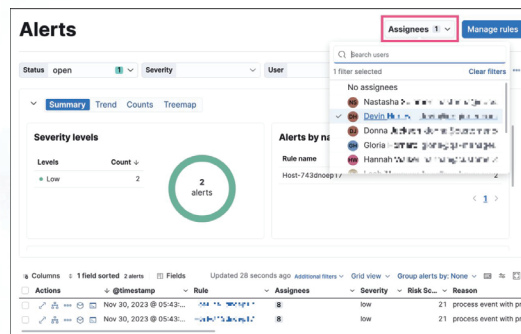


Source: Freepik

Alert Configuration

SIEM alert optimization is a crucial component of an effective security strategy, helping organizations to reduce false positives, prioritize critical incidents, and streamline incident response processes.

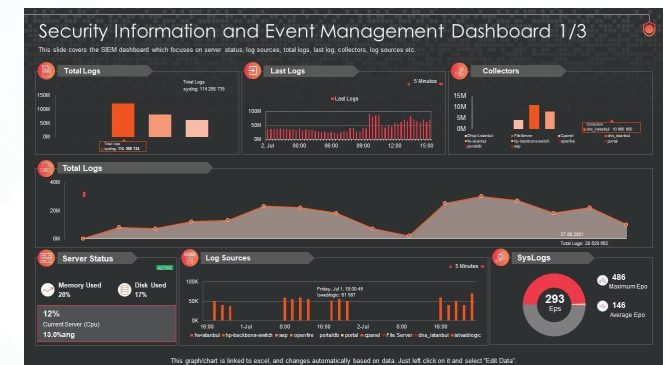
- **Static Alerts:** Trigger on specific events.
- **Threshold-Based Alerts:** Trigger on frequency patterns.
- **Behavioral Alerts:** Use baselines and anomalies.



Elastic SIEM alerts page Source: Elastic

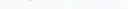
Common Tools in Monitoring

- **SIEM Platforms:** Elastic, Splunk, QRadar, Azure Sentinel
- **Log Management:** ELK Stack, Graylog
- **Network Sensors:** Zeek, Suricata



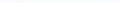
Source: LinkedIn

List of step by step practical activities

- 


 Co-funded by the European Union
 35

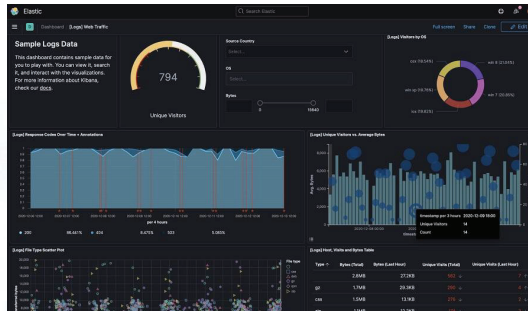
[illegible]



 Co-funded by the European Union

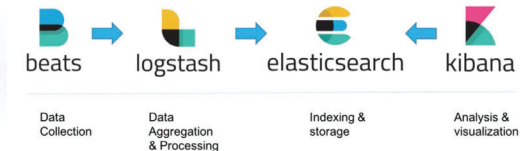
What is ELK?

- **ELK** is an open-source suite composed of three main components: **Elasticsearch**, **Logstash**, and **Kibana**. Later, **Beats** was added, forming the complete **ELK Stack**.
- The ELK Stack allows for **data indexing and analysis**. For instance, you can load different types of data — such as logs — and visualize them using **custom dashboards**, as shown in the screenshot.



Components of the ELK Stack:

- **Beats**: Installed as agents on the machines to be monitored, they forward logs.
- **Logstash**: Aggregates data and sends it to Elasticsearch.
- **Elasticsearch**: The core component that stores and accesses data via a RESTful API.
- **Kibana**: Enables dashboard creation and data visualization from Elasticsearch.



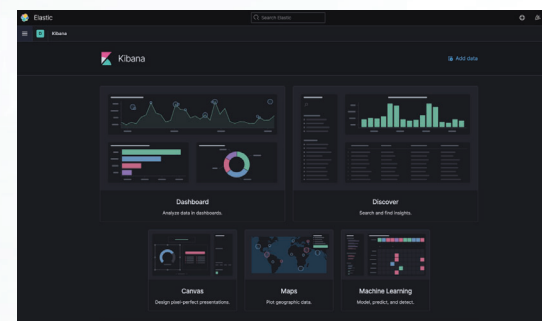
ELK Suite: the SIEM Solution

Practicing cyber security

- Installing elasticsearch and kibana
- Step by step full configuration
- Create detection rules etc...

```
{
  "name": "elkserver",
  "cluster_name": "elasticsearch",
  "cluster_uuid": "dFcm43uk3gE2SDH6743NCE9vQ",
  "version": {
    "number": "7.6.2",
    "build_flavor": "default",
    "build_type": "deb",
    "build_hash": "ef49eb3ee2rre676996e8aabd07ef6fb113f",
    "build_date": "2020-03-26T06:34:37.794943Z",
    "build_snapshot": false,
    "luene_version": "8.4.0",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}
```

Install Kibana



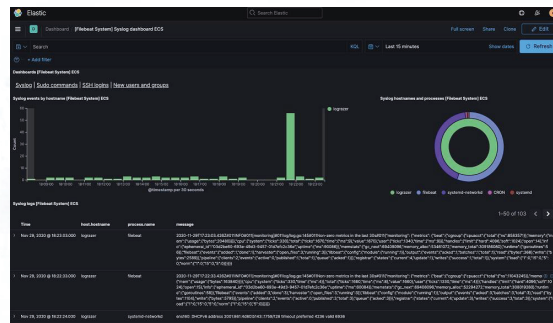
Your Kibana home interface will look like this

- You will see **preconfigured dashboards**, as well as the **Discover, Canvas, Maps, and Machine Learning** sections.
- Now let's configure the **security features** needed to use ELK as a SIEM.

Practicing cyber security

Step by step guide to

- Enable security features in ELK
- Send Syslog Logs to ELK
- Send Sysmon Logs to ELK
- Use Packetbeat for Network Monitoring



A default dashboard in ELK

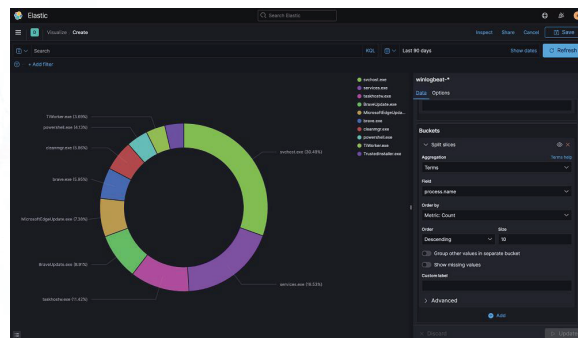
Create Detection Rules

Detection rules allow you to trigger an alert based on a defined event—for example, the execution of software detected by the antivirus, or the use of an admin account on a user workstation.

[Video tutorial](#)

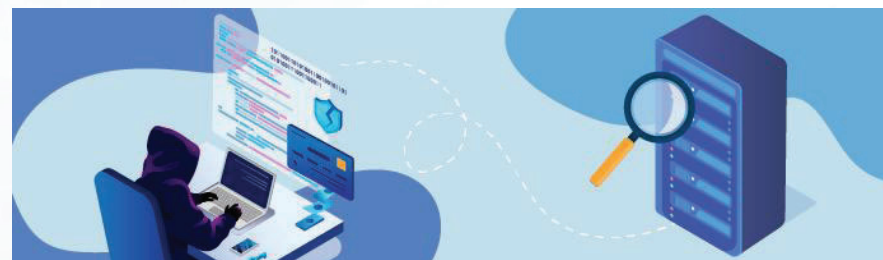
Dashboard configuration

Configuring dashboard to tailor data visualisation



Our chart properly configured to display the logs

Use the ATT&CK Matrix to Define Attack Scenarios to test your SIEM

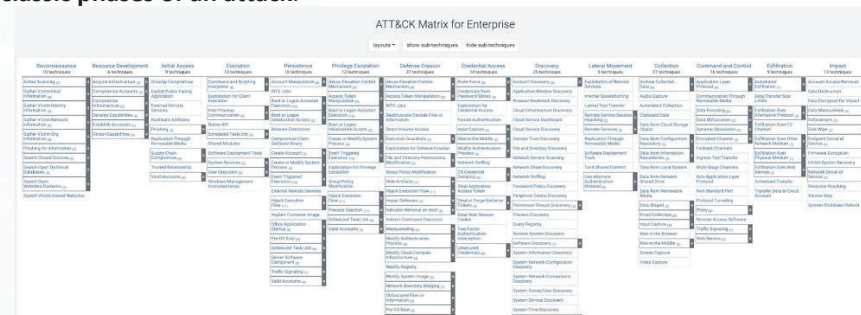


Use the ATT&CK Matrix to Define Attack Scenarios

Now that our SIEM is properly installed and configured, let's move on to **attack scenarios**. A cyberattack generally follows a pattern or modus operandi that we can model. The goal is to identify the **key stages of an attack**, as well as its progression.

Discover the ATT&CK Matrix

- It's composed of **12 tactics**, each containing multiple techniques and representing **classic phases of an attack**.



Structure of the ATT&CK Matrix

Simulate an attack on Windows

What is a LOLbin?

LOLbin (Living Off the Land Binary) is a term used to describe the use of **legitimate, built-in Windows tools**. While these tools are signed by Microsoft, they can still be misused to perform malicious actions on a system. You can find a list on the LOLBAS project.

- MpCmdRun.exe can also be misused to **disable the antivirus** on the target machine. This technique is listed in the ATT&CK matrix with ID **TA0011**.

Simulate Privilege Escalation on Windows

- Another common tactic in an attack is **privilege escalation** to enable **lateral movement**. One tool often used to gain administrative rights is **Mimikatz**, which extracts credentials from the compromised machine.
- This technique is listed in the [ATT&CK matrix as T1555](#).

Run a Detection Test on Linux

- In this third example, we'll run a **detection test on our Linux server**.
- We'll simulate an **SQL injection attack** and make sure the information reaches our SIEM.
- Start by adding **Apache logs**. For our test, we'll use the **DVWA application**, installed in the OpenClassrooms course on penetration testing.
- On your Linux server, enter the following commands:

```
sudo filebeat modules enable apache
sudo filebeat setup
sudo filebeat -e
```



49



Get social with the project!

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.



Project Partners





Boost camp in Lithuania for trainers: cyber security
lecturers' workshop: 23-25 September, 2025

M1 : Security Program Management

M3 : Analytical Tools

[Cihan UYSAL, Timta]

CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO Type of Action: ERASMUS-LS

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.



Co-funded by
the European Union

www.cyberagents.eu

Security Program Management

OBJECTIVES

- Design and manage cybersecurity programs
- Apply metrics, quality, and resources
- Assess threats and report correctly



2

Security Program Management

MODULE CONTENTS

Project management

- Project Planning
- Defining Project Objectives
- Defining Project Scope and Requirements
- Preparing the Project Schedule
- Project Management Tools
- Current Cybersecurity Threats (DDoS, Ransomware, Malware, Phishing, Zero-Day, IoT attacks, etc.)
- Threat Modelling and Vulnerability Analysis
- Emergency and Incident Response Plans
- Reporting Cybersecurity Threats and Incidents



3

Security Program Management

MODULE CONTENTS

Resource management

- Human Resources (Project Teams) Management
- Security Awareness and Team Training
- Hardware and Software Inventory Management
- Security Tools and Software
- Effective Use of Technological Resources
- Budget and Resource Allocation



4

Security Program Management

MODULE CONTENTS

Security metrics

- Security Metrics and Measurement Techniques
- Data Collection with SIEM
- Analysis of Security Metrics
- Project Monitoring and Performance Evaluation
- Review of Actions and Project Adaptation
- Reporting of Security Metrics



5

Security Program Management

MODULE CONTENTS

Quality assurance and quality control

- Quality Management
- Quality Standards in Cybersecurity
- Compliance and Quality Audits
- Testing and Validation Techniques
- Evaluation and Improvement Recommendations



6

Security Program Management

More than 10
scenario-based tasks



7

Security Program Management

ASSESSMENT

In this module, 18 self-assessment questions and 144 knowledge questions were prepared



8

Analytical Tools

OBJECTIVES

- Apply metrics and analytics to protect assets.
- Use analytics to identify risks and improve security.
- Evaluate, mitigate, and report security threats effectively.



9

Analytical Tools

MODULE CONTENTS

Performance measurements (metrics)

- Performance Metrics
- System and Network Monitoring
- Monitoring Performance Metrics
- Network Mapping
- Vulnerability Scanning
- Network Traffic Analysis



10

Analytical Tools

MODULE CONTENTS

Data analytics

- Data Collection
- Data Cleaning and Preprocessing
- Data Analysis
- Data Visualization
- Analytical Tools
- Applications of Data Analytics in Cybersecurity



11

Analytical Tools

MODULE CONTENTS

Security intelligence

- Understanding Security Intelligence
- Sources of Security Intelligence
- Threat Intelligence Collection Methods
- Threat Intelligence Frameworks
- AI-Driven Security Intelligence Platforms
- Case Studies on Security Intelligence Applications



12

Analytical Tools

Total 8 scenario-based tasks



13

Analytical Tools

ASSESSMENT

In this module, 18 self-assessment questions and 150 knowledge questions were prepared



14

Cihan Uysal

IT Teacher – Teknopark İstanbul Vocational and Technical High School

E-mail: cihanuysal85@gmail.com

WhatsApp: +90 554 697 60 69

LinkedIn: <https://www.linkedin.com/in/cihanuysal85/>

Thank you for your attention!



15

Get social with the project!

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



@CyberAgent.EU



@Cyber-Agent-EU



@CyberAgentEU



contact@cyberagents.eu



@Cyber.Agent. EU



@CyberAgentEU

Project Partners





Boost camp in Lithuania for trainers: cyber security lecturers' workshop: 23-25 September, 2025

Security Governance & Policy

[Adelina Luntraru, EVM Group]

CYBER AGENT

Project ID. 101111732

Call: ERASMUS-EDU-2022-PI-ALL-INNO

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

2025

Type of Action: ERASMUS-LS

Co-funded by the European Union

Security Governance & Policy

CHARACTERISTICS

Languages

Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish.

Duration & Workload

Live Training: 75 hours
Individual study: 50 hours



FULLY ONLINE
OR BLENDED



3 ECTS
CREDITS

Objective:

Prepare learners to face the challenges of cybersecurity in SMEs, **integrating security governance into the business strategy** and ensuring **compliance with legal regulations**, such as the GDPR.

The module covers aspects such as identifying threats and vulnerabilities, designing robust and adaptive security policies, and managing incidents effectively. In addition, it focuses on developing governance structures that assign clear roles in the organization, aligning cybersecurity with strategic objectives.



2

Chapters

Organizational context

Privacy

Laws, ethics, and compliance

Security governance

Executive and board level communication

Managerial policy



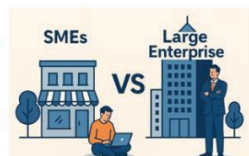
3

Organizational context

1. Evolution of cybersecurity in SMEs
2. Current major threats and vulnerabilities
3. Impact of cybersecurity on business strategy
4. Specific challenges of cybersecurity in SMEs versus large enterprises
5. Understand the regulatory implications of cybersecurity practices and how they align with governance structures.
6. Common cybersecurity challenges specific to SMEs, such as limited budgets, lack of dedicated security staff, and practical methods for prioritizing cybersecurity investments



Source: <https://cisomag.com/4-types-of-insiders-you-need-to-know/>



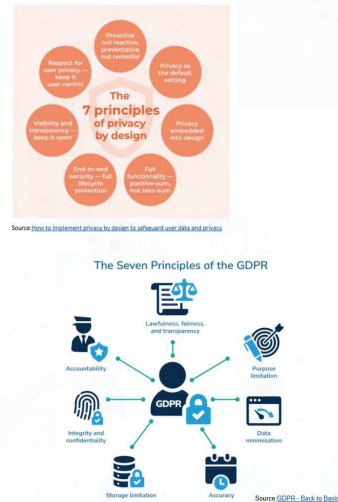
Source: Generated by chatgpt4, 2025



4

Privacy

1. Privacy principles in cybersecurity
2. Personal data protection and GDPR
3. Impact of privacy on SME operations
4. Tools and techniques for privacy protection



Laws, ethics, and compliance

1. Cybersecurity Organizations, Policies and Standards
2. Relevant national and international legislation
3. Regulatory compliance in SMEs
4. Ethics in Cybersecurity
5. Legal consequences of non-compliance in cybersecurity
6. Analysis of how AI-based tools can be utilized to strengthen cybersecurity governance and ensure compliance through continuous monitoring and automated threat response.



Source of image: generated by ChatGPT4, 2025.

Security governance

1. Cybersecurity governance structure
2. Roles and responsibilities in security management
3. Cybersecurity maturity models
4. Integration of cybersecurity into corporate governance
5. Enhance abilities in conducting risk assessments and formulating strategic response plans under simulated crisis conditions (Ransomware, phishing attack, ..)



Executive and board level communication

1. Cybersecurity communication strategies
2. Security reporting to senior management
3. Decision making based on security data
4. Crisis management and communication in cybersecurity
5. Master crisis management and decision-making skills in high-stress scenarios involving AI-driven attacks and ransomware.



Source: Canva, 2025

Managerial policy

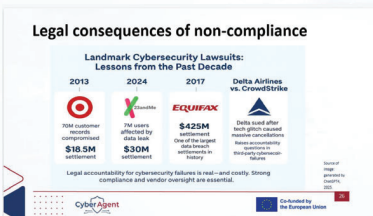
- 1. Security policy development
- 2. Policy implementation and monitoring
- 3. Evaluation and continuous improvement of policies
- 4. Adaptation of security policies to technological and regulatory changes
- 5. Exploration of how effective training and awareness policies can be a crucial component of regulatory compliance and risk mitigation.



9

Additional materials

- Videos created from the materials
- Case studies
- Links to other talks, interviews, webinars, articles, books



Source: Generated by chatgpt4, 2025

Effective Crisis Communication in The Age of AI (Webinar)

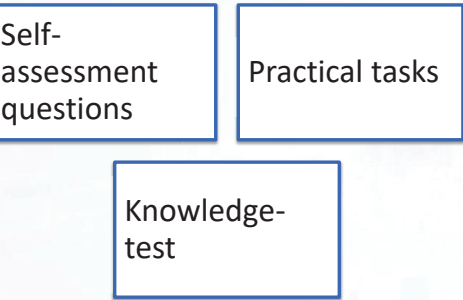


Check this webinar: [Effective Crisis Communication in The Age of AI](#)



10

Assessment



11

Get social with the project!

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.



Project Partners





Cybersecurity Planning

High School Grigore C Moisil, Buzău, Romania

CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO Type of Action: ERASMUS-LS

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.



Co-funded by the European Union

www.cyberagents.eu

SUBCHAPTERS

- #1 Introduction to Cybersecurity Planning: Data, human and societal security
- #2 Strategic Planning
- #3 Operational and Tactical Management



Co-funded by the European Union

#1 Introduction to Cybersecurity Planning: Data, human and societal security

Learning goals

- Define the legal aspects of data, human and societal security, laws and policies that govern data in SME's.
- Classify types of cyberattacks relevant to SME's
- Identify useful tools to prevent cyberattacks



Co-funded by the European Union

Content

- Data security: [Information Storage Security](#), [Investigatory process](#)
[Password attack techniques](#)
- [Human security](#): Awareness and Understanding
- [Societal security](#): what are [Cybercrime](#), [Cyber ethics](#), [Cyberlaw](#) -
[Digital evidence](#), [Digital contracts](#), [Multinational conventions](#)
- [Practical Examples](#)



Co-funded by the European Union

Security measures to protect stored data

- The document covers security measures to protect stored data, including data encryption, regular backups, access control, monitoring and detection systems, investigative processes, and defense strategies against password attacks

The investigative process- Analysis of a cyber attack

- Different types of malware are described, including spyware (designed to track and spy), adware (designed to deliver advertisements), worms (reproduce to spread), viruses (reproduce and attach to executable files), and ransomware (holds data captive until payment)

Infiltration methods

- It also details infiltration methods, focusing on social engineering techniques such as pretexting, tailgating, and quid pro quo, which manipulate people to divulge confidential information

Infiltration methods

- The document differentiates between DoS attacks, social engineering, and SEO poisoning. DoS disrupts network services, social engineering manipulates individuals, and SEO poisoning manipulates website rankings to distribute malicious code or gather confidential information

Cyberlaw

- A significant portion of the material addresses cyberlaw, emphasizing its role as the backbone of the fight against cybercrime. It provides a legal framework for investigating and punishing digital crimes, highlighting the importance of digital evidence, e-contracts, and international conventions

Practical exercises

- include implementing access keys and multi-factor authentication (Know+Have+Are)
- 1. [IMPLEMENTING ACCESS KEYS](#) Chrome for Developers
- 2. [Multifactor Authentication: Know+Have+Are](#) IBM Technologies
- 3. [Live Cyber Threat Map](#)



#2 Strategic Planning

Learning goals

- Define cybersecurity objectives relevant to SMEs using a SWOTanalysis
- Develop long-term strategies to address risks
- Allocate resources and budgets accordingly
- Establish KPIs to measure progress
- To regularly update the strategy based on new threats

Content

- Defining Cybersecurity Goals and Objectives
- SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats)
- Developing Long-Term Security Strategies
- Setting Key Performance Indicators (KPIs)
- Reviewing and Updating the Security Strategy

- This subchapter 2 covers cybersecurity planning and strategic approaches, emphasizing the importance of proactive measures and continuous improvement.
- It highlights various aspects of cybersecurity, from internal strengths to key performance indicators (KPIs).

Key Areas Covered

1. Internal Strengths:

The document identifies well-defined security policies and procedures, advanced protection solutions (like firewalls, antivirus, encryption, IDS/IPS, VPN, DLP, SIEM, AI, and cloud/IoT protection tools), qualified cybersecurity personnel, and regulatory compliance (GDPR, ISO 27001, etc.) as crucial internal advantages

2. Risk Management:

- It details risk management strategies including risk reduction (mitigation), risk transfer, risk acceptance, and risk avoidance. A Risk Analysis Matrix is noted as a primary tool for tracking risks based on probability and impact
- Risk, Interpretation, classification

		IMPACT		
		Low Insignificant just needs to be noted	Medium Reasonably requires monitoring	Big It will have a big impact
PROBA BILITY	Low (unlikely to happen)	E	D	C
	Medium (can be produced at some point)	D	C	B
	Big (probably will occur)	C	B	A

3. Key Performance Indicators (KPIs):

- The document emphasizes the importance of KPIs in achieving business goals, identifying areas for improvement, embedding core values, and informing future decisions. It outlines steps for setting target KPIs, including understanding business objectives, analyzing progress, setting goals, team review, checking progress, and aligning KPIs with company values

All in all, this subchapter underscores a comprehensive approach to cybersecurity, integrating strong internal controls, strategic risk management, performance measurement, and continuous improvement to safeguard against cyber threats.

#3 Operational and Tactical Management

Learning goals

- Implement access control measures to restrict unauthorized access
- Maintain systems through patch management
- Set up monitoring for unusual activities
- Provide employees with cybersecurity awareness training

Content

- [Implementing Access Controls](#)
- [Patch Management and Software Updates](#)
- [Continuous System Monitoring](#)
- [Employee Security Awareness Training](#)
- [Individual work](#)

- This subchapter covers a range of cybersecurity topics, from strategic planning to practical implementation, with a focus on protecting organizations from evolving threats.
- It emphasizes the importance of integrating strategy, operations, and tactics for a resilient digital environment

The role of artificial intelligence (AI) in monitoring

- The document highlights the role of AI in both monitoring and strengthening security measures, automating tasks like log analysis and vulnerability scanning, enabling real-time threat detection, and continuously learning to counter emerging threats
- It also addresses future cybersecurity trends, particularly how AI will change the threat landscape and potential solutions in 2025 and beyond

[Cybersecurity Trends for 2025 and Beyond](#) – IBM Technology

Quick Steps to Protect the Small Business



- The document provides quick steps for small businesses to enhance their security, including collecting only necessary data, locking down accounts, vetting AI providers, and training their teams Effective.
- **Cybersecurity Glossary for Small Businesses** - to understanding and safeguarding digital world, bridging the gap between technical jargon and real-world understanding.

Source: Gamma ai, 2025

Additional material

- Videos
- Case studies
- Individual work
- Practical exercises
- Test




Co-funded by
the European Union

Get social with the project!



www.cyberagents.eu



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



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



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



contact@cyberagents.eu



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



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

Project Partners



Kaunas
Faculty



Prios



EVM
GROUP



TEKNOPARK
ISTANBUL
TECHNOLOGY
INCUBATOR



IT
AKADEMIJA



DIEMEN
MILANOVA ET



WOMEN
4 CYBER



CYBERAGENT
EU



Boost camp in Lithuania for trainers: cyber security lecturers' workshop:
23-25 September, 2025

Cybersecurity for SMEs: Business Continuity, Disaster Recovery, and Incident Management

(Neda Mađarac, PRIOS Norway)

CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO Type of Action: ERASMUS-LS

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.



Co-funded by the European Union

INTRODUCTION



Based on the syllabus, we created **Module8 in 8 subtopics**. We focused on one of the most practical and important areas of cybersecurity: how to keep **the business running even when something goes wrong**.



Co-funded by the European Union

2

NEEDS ANALYSIS



Every organization, no matter how big or small, can face unexpected events—cyberattacks, system failures, human mistakes, or even natural disasters. The goal of this module is to help to prepare for these situations so that, at the end of the module, learner will have skills and competences to:

- Protect the organisation assets** (data, systems, people),
- Reduce downtime** and keep business operations going even when something happened,
- Avoid or limit crises** with clear procedures and response strategies.



Co-funded by the European Union

3

MODULE OVERVIEW



Main topics:

1. Incident Response
2. Disaster Recovery
3. Business Continuity
4. Security Awareness and Training
5. Secure Hiring and Termination Practices
6. Third-Party Security
7. Security Audits and Reviews
8. Employee Data Privacy



Co-funded by the European Union

4

MODULE DESIGN:



Each of the eight subtopics are designed with consistent structure which ensures both knowledge and practical application:

- a) **Explanatory text** (theoretical background, written in clear, practical language)
- b) **Presentations** (ppt's)
- c) **Practical tasks** (short, applied exercises where learners create, design, or simulate real-world cybersecurity solutions)
- d) **Self- assessment questions** (integrated at the end of each subtopic)
- e) **Videos** (short video materials that illustrate key points, best practices, or case studies)
- f) **Final assessment** At the end of the module, learners complete a comprehensive assessment)



5

MODULE DESIGN (EXTRA):



Self-study assignments- Independent research tasks (e.g., analyse a real-world cyber incident and write a case study).
Strengthens analytical skills and connects theory with practice.

Learning resources on the Platform- Recommended readings, frameworks, video materials, external resources links, and reports. Provides deeper insights and professional tools for further learning/ reading.



6

METHODOLOGY



This module combines **knowledge** (what learner needs to know), **skills** (what learner will be able to do), and **competences** (how learner will apply both in real-life situations).

To support their learning, we prepared **self-assessment tasks, knowledge tests, and practical exercises. Module also consists of learning resources which can be used to deepen the knowledge of learners.**

In simple terms: **this module will give learners the confidence and tools to make sure their organization can survive and recover from any cyber incident.**



7

PRACTICAL GOAL OF THE MODULE:



Learners will understand how to write and maintain a practical **cybersecurity handbook** for SMEs—one that follows advanced cybersecurity principles, uses the latest defense tools, and respects both national and international standards.



8

PRACTICAL GOAL OF THE MODULE:



By the end of the module, learners will be able to design and implement a complete **Business Continuity and Disaster Recovery (BC/DR) plan**, build a solid **incident management program**, and develop strong **personnel security policies** for their organization.



9

MAIN BENEFITS & EXPECTED OUTCOMES



This module prepares learners to understand how to protect (their) organizations against cyber threats and disruptions in the following way:

Preparing for incidents before they happen
Responding effectively to minimize damage
Ensuring that critical services stay operational
Building strong **personnel security policies**

Goal:

Empower learners with practical strategies for resilience and compliance regarding the cybersecurity threats.



10

ASSESSMENT STRATEGY

25% Self-assessment tests
75% Final knowledge evaluation



11

TEACHING/ASSESSMENT METHODOLOGY

In addition to lectures and theoretical input, Module 8 is structured around **active learning methods** that ensure students can apply knowledge in real-life SME contexts.

Self-assessment

Throughout the module, learners are guided to reflect on key concepts such as incident response, business continuity, and disaster recovery. Short self-assessment checkpoints are built in after each main topic to help learners to monitor their understanding and progress.



12

TEACHING/ASSESSMENT METHODOLOGY

Self-study

Learners complete an independent assignment where they research a major cybersecurity incident and prepare a short case study report. This exercise strengthens analytical skills, connects theory with real-world practice, and allows students to extract lessons relevant for SMEs.

TEACHING/ASSESSMENT METHODOLOGY

We tried to use engaging learning content with different teaching methods, e.g. videos, practical tasks, self-study, quizzes.

EXAMPLE OF THE VIDEO:



SKILLS AND COMPETENCES

By the end of Module 8, learner will:

- Be able to **develop and implement Business Continuity and Disaster Recovery plans**.
- Know how to **design and lead incident response programs**.
- Build strong **personnel security policies**.
- Be competent to **create and maintain a cybersecurity handbook for SMEs** aligned with international standards.

MODULE 8 CONTENT:

Incident Response

Definition & importance in cybersecurity
Key components of effective response & recovery
Common threats (phishing, insider threats, etc.)
Developing an **Incident Response Plan (IRP)**
Roles & responsibilities of the **Incident Response Team**
Simulation: **conducting a mock plan**

MODULE 8 CONTENT:

Disaster Recovery

- Understanding disaster recovery
- Developing a **Disaster Recovery Plan**
- Roles & responsibilities in recovery
- Recovery steps after a disaster



17

MODULE 8 CONTENT:

Business Continuity

- Understanding business continuity
- Developing a **Business Continuity Plan (BCP)**
- Roles & responsibilities in continuity management
- **Business Impact Analysis (BIA)**
- Testing and improving the BCP



18

MODULE 8 CONTENT:

Security Awareness & Training

- Understanding security awareness
- Developing training programs
- Employee responsibilities
- Measuring effectiveness



19

MODULE 8 CONTENT:

Security Hiring Practices

- Defining security role requirements
- Background checks & interviews
- Ongoing evaluation & development



20

MODULE 8 CONTENT:

Security Termination Practices

- Revoking access immediately
- Retrieving data & devices
- Exit interviews for security insights
- Legal & compliance considerations



21

MODULE 8 CONTENT:

Third-Party Security

- **Assessing vendor risk**
- Due diligence in selection
- Contracts & security requirements
- Ongoing monitoring & auditing
- Incident response & communication



22

MODULE 8 CONTENT:

Security in Review Processes

- Incorporating security into regular reviews
- Security audits & vulnerability testing
- Post-incident reviews



23

MODULE 8 CONTENT:

Privacy of employee information

- Data collection limitations
- Storage & access controls
- Compliance with privacy regulations
- Data sharing with third parties
- Employee consent & rights



24

CyberAgent Boostcamp in Lithuania 23rd-25th of September, 2025



Co-funded by
the European Union



Get social with the project!



www.cyberagents.eu



@CyberAgentEU



@Cyber-Agent-EU



@CyberAgentEU



contact@cyberagents.eu



@Cyber.Agent. EU



@CyberAgentEU

Project Partners





Prios



EVM
GRUPO



**TEKNOPARK
ISTANBUL**
TEKNOLOJİ VE
İNNOVASYON



IT
AKADEMIJA



**DIPLOMSKI
CENTAR
BEOGRAD**



**WOMEN
4CYBER**





Boost camp in Lithuania for trainers and
cyber security lecturers' workshop: 23-25 September, 2025

M+ - EMPOWERING CAREERS IN CYBER

CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS

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.



Co-funded by
the European Union



Co-funded by
the European Union

Cybersecurity is about people as much as technology

2

Our perspective

On the ground, we observe:

- **Barriers women face:** redirected to less technical roles, confidence gaps, workplace exclusion
- **Lack of support for companies** to build inclusive hiring practices
- **For newcomers, the field feels overwhelming:** unclear pathways, difficulty securing first jobs

This lived expertise shaped the pedagogy: case studies, testimonials, and strategies to navigate career progression.



Co-funded by
the European Union

3

Module content

The training is **self-paced**, **interactive**, and **highly practical**.

1	2	3
Career Pathways	Job-Seeking Strategies	Diversity & Inclusion
16 roles across managerial, analytical, and technical paths, linked to EU frameworks (ECSF, ESCO)	CV templates, LinkedIn guide, interview prep, and personal branding	Scenarios, myths vs. realities, and activities to confront bias and foster inclusion



Co-funded by
the European Union

4

Interactive approach

- Interactive quizzes
- 3 Webinars with field expert
- Action plans (week-by-week job hunt strategies)
- Templates & ready-to-use tools (resume, cover letter, LinkedIn checklist and guide)
- 16 cyber roles mapped to EU frameworks (ECSF, ESCO)



Co-funded by the European Union

5

B. CAREER PATHS OVERVIEW

Managerial roles in cybersecurity

Managerial cybersecurity roles sit at the intersection of **strategy, governance, and operational oversight**. These professionals are responsible for defining security policies, ensuring regulatory compliance, mitigating organisational risk, and leading security teams. They must blend a **strong technical foundation with strategic thinking**, leadership, and communication skills.

These roles are crucial in shaping the security culture and response readiness of an organisation: making high-level decisions that impact not only technical teams but also executive leadership, legal, compliance, and risk departments.

Click to discover each role profile in this category

[Chief Information Security Officer \(CISO\)](#) [Cybersecurity Risk Manager](#)

[ICT Security Manager](#) [ICT Resilience Manager](#) [Data Protection Officer](#)



Co-funded by the European Union

11

ICT RESILIENCE MANAGER

Or IT Resilience Manager, Disaster Recovery Manager
ESCO: ICT Resilience Manager

JOB OVERVIEW
The ICT resilience manager is responsible for ensuring that an organisation's information and communication technology (ICT) systems can withstand and recover from disruptions, maintaining business continuity. This role involves developing and implementing strategies to enhance cyber resilience and disaster recovery. Main responsibilities include:

- Developing and maintaining business continuity and disaster recovery (BC/DR) plans
- Performing risk assessments and business impact analyses
- Leading testing and simulation exercises for incident response and recovery
- Coordinating across departments during actual incidents
- Aligning resilience strategy with cybersecurity and business goals

CORE SKILLS

- KNOWLEDGE OF DISASTER RECOVERY TOOLS and techniques
- Familiarity with ISO 22301 (Business Continuity) and ISO 27001 (Information Security)
- Strong understanding of infrastructure, cloud systems, and operational dependencies
- Risk management and impact assessment
- Ability to lead cross-functional response teams during incidents

SOFT SKILLS

- Calm under pressure, especially during real disruptions
- Strong communicator, able to coordinate multiple teams and update leadership
- Proactive and methodical, plans ahead for worst-case scenarios
- Reliable and organised, managing regular testing, documentation, and reviews
- Resilient mindset, focused on minimising downtime and business impact

A DAY IN THE LIFE
An ICT resilience manager leads a quarterly disaster recovery test for an airline simulating a data center outage. They coordinate with IT and business teams to switch operations to a backup environment and evaluate how systems perform under failover conditions. After identifying a 7-minute delay in restoring booking systems, they update the recovery plan and schedule technical improvements.

WORK ENVIRONMENT

- Common in sectors with critical operations, airlines, healthcare, finance, utilities, telecom
- Typically hybrid or office-based, but may need to be on-call for crisis response
- Works with IT, cybersecurity, legal, compliance, and executive teams
- May manage internal resilience teams or coordinate external providers

CAREER GROWTH & SALARY EXPECTATIONS (2025 ESTIMATES IN EUROPE)
Entry-Level (BC/DR Analyst, Continuity Planner):
~€40,000 – €60,000/year
Mid-Career (ICT Resilience Manager, Disaster Recovery Lead):
~€60,000 – €90,000/year
Senior-Level (Head of Resilience, Director of Continuity or Risk):
~€90,000 – €120,000+/year

→ Critical sectors or regulated industries often pay higher due to risk exposure

CERTIFICATIONS & EDUCATION PATHWAYS
Education
Bachelor's degree in Information Technology, Cybersecurity, or Engineering
Master's degree in Business Continuity, Crisis Management, or Risk Governance

Certifications

- CBCP – Certified Business Continuity Professional
- ISO 22301 Lead Implementer – Business Continuity Management Systems
- CISM – Certified Information Security Manager
- ITIL – especially for understanding operational service continuity



Co-funded by the European Union

9

FIND YOUR PATH

Do you enjoy solving puzzles and investigating threats?

Do you love building secure systems from the ground up?

Do you like breaking things to see how they work?

Are you passionate about teaching or raising awareness?

Do you care about privacy, ethics, and protecting people's rights?

Are you a strategic thinker who enjoys planning and organising?



Co-funded by the European Union

9

A. MASTERING THE CYBERSECURITY JOB HUNT

What cybersecurity hiring managers are looking for?

Transferable skills are very important in cybersecurity and recruiters love to hear someone linking their skills from a different situation, job or context to a new role:

*"There is a need to find people who can cover multiple roles and fill the gaps, which can be hard to find in the competitive market [...] In addition to existing technical skills, cybersecurity professionals that have a learning mindset and an ability to adapt are critical in the field."*³

DID YOU KNOW?

- Hiring managers scan resumes in **6-7 seconds** before deciding to read further.⁴
- 70%** of resumes get rejected by ATS (Applicant Tracking System) due to poor keyword optimisation.⁵
- 72%** of recruiters use LinkedIn to source talent, with strong hiring trends in sectors like AI and cybersecurity.⁶

Co-funded by the European Union

17

WHAT WOULD YOU ASSUME?

Who would most people guess is more "professional" or "expert" at a glance?

- A) The man
- B) The woman
- C) Too close to call
- D) It depends on the viewer's own gender

Co-funded by the European Union

39

WEBINAR

Curious about what it really takes to build inclusive teams? Irasara and Steffen share practical insights on creating truly diverse and equitable workplaces. Coming from their corporate experience, they will share honest reflections, from shifting hiring mindsets to fostering psychological safety.

[WATCH WEBINAR](#)

Co-funded by the European Union

52

Conclusion

Module open to all: VET, HEI, SME employees, men and women!

Next step
→ Ensuring completion: exploring incentives & engagement strategies

Co-funded by the European Union

12



Boost camp in Lithuania for trainers and cyber security lecturers' workshop: 23-25 September, 2025

ENGAGEMENT STRATEGY FOR PILOTING

CYBER AGENT 2025

Project ID: 101111732
Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS

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.

Co-funded by the European Union

www.cyberagents.eu

Dissemination Timeline & Plan

PHASE 1	June 2025	PHASE 2	July - August 2025	PHASE 3	September 2025	PHASE 4	October 2025 - April 2026	PHASE 5	June 2026
Behind the scenes - Tease development progress & content sneak peak		Launch preparation - Build anticipation & warm up audiences for registration		Bootcamp - Show training in action		Pilot Trainings - Drive registrations, support pilot testers, promote training		Final Push - Celebrate success, share results	
- Start using #CyberAgentTraining hashtag - Share Module Spotlight post on social media (1 or 2 per week), to present each module - Blog post on the website - Teaser in Newsletter #6		- Share 3 dedicated Why It Matters post on social media for each audience (VETs, SMEs, HEIs) - Press release + Blog post		- Pictures of the Bootcamp on social media - Share video Interviews from trainers and partners - Start a social media Countdown before launch of pilot training - Create a landing page for people to pre-register with a "Notify Me" ? - Promo in Newsletter #7		- Press release + Blog post - Share Inside the Module post on social media monthly (October M1; November M2; December M3 & M4; January M5 & M6, February W4C; March M7; April M8) - Promo in Newsletters #8 & #9 - Share Testimonials on social media with feedback from the trainees and trainers - Provide a Digital Badge to all trainees for them to share their progress on LinkedIn - Organise a Live Demo with Q&A and publish the recording on YouTube		- Publish By the Numbers infographic (# registrations, completions, women participants, etc.) - Share results in newsletter #10 - Final Conference	

Co-funded by the European Union14

Pilot Outreach Strategy

RECOMMENDATIONS

- Peer-to-peer referrals:** SMEs in the network as ambassadors
- Map SMEs** via chambers of commerce, business associations, women-in-tech networks, key sectors...
- Incentives for SMEs:** visibility, recognition, certificate, early acces
- Outreach kits** prepared by W4C(emails, one-pagers, visuals)
- Joint social media campaign** across project & partner channels
- Amplify** through universities and VET providers
- Use storytelling**, milestones, and role models to make it engaging

Co-funded by the European Union15

Co-funded by the European Union

Get social with the project!



www.cyberagents.eu[@CyberAgentEU](https://www.facebook.com/CyberAgentEU)[@Cyber-Agent-EU](https://www.linkedin.com/company/Cyber-Agent-EU)[@CyberAgentEU](https://twitter.com/CyberAgentEU)

contact@cyberagents.eu[@Cyber.Agent.EU](https://www.instagram.com/Cyber.Agent.EU)[@CyberAgentEU](https://www.youtube.com/CyberAgentEU)

Project Partners

