



Kaunas
Faculty

SMEs Cyber Security Change Agents

Dr. Renata Danieliene
Vilnius University

Project ID. 101111732

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

Type of Action: ERASMUS-LS

Coordinator: Vilnius university

2025

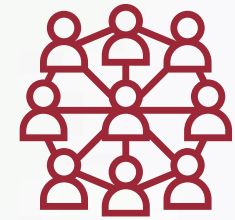


**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

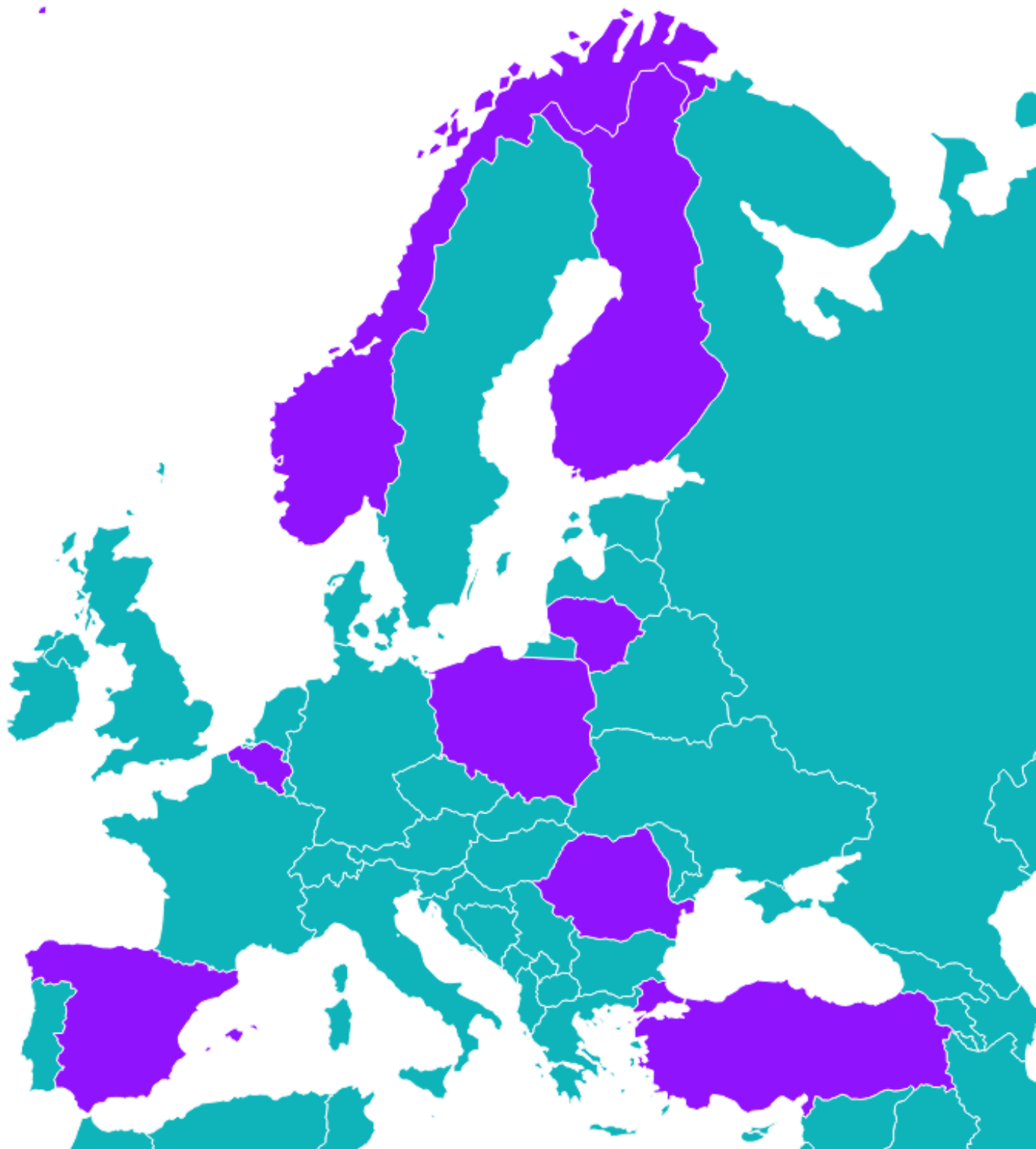


Kaunas
Faculty



Co-funded by
the European Union

Project partners



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



Kaunas Faculty



Kaunas Faculty



Co-funded by the European Union

A row of black dominoes on a light gray surface. The domino on the right is falling, and the letters "SME" are printed in white on its top face.

SME

One weak link can disrupt the entire chain.

SMEs are an essential part of Europe's critical infrastructure.

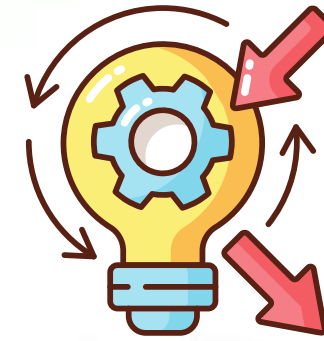
Developed training material for HEI, VET, SME:

Designed for technical and non-technical learners



Technical skills

Security Program Management
Systems Administration



Analytical skills

Analytical Tools
Security Operations



Organisational skills

Security Governance & Policy
Cybersecurity Planning



Risk Management skills

Risk Management
Business Continuity, Disaster
Recovery, and Incident
Management & Personnel Security

5

Result: Slides, videos, exercises, tests



Kaunas
Faculty



Co-funded by
the European Union



Additional module for ALL

EMPOWERING CAREERS IN CYBERSECURITY

Introduction to career paths
and opportunities

Focus on diversity and inclusion
Real-life examples and stories



Syllabuses of training material HEI & VET



EN, LT, PL, ES, NO, TR, FR, FI, RO



OBJECTIVES	WHAT YOU WILL LEARN
• Apply metrics and analytics to protect assets. • Use analytics to identify risks and improve security. • Evaluate, mitigate, and report security threats effectively.	• Manage, identify, analyse, assess, estimate, investigate the cybersecurity-related risks of ICT infrastructures, systems and service projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.
CHARACTERISTICS	TRAINING CONTENT
Languages Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish. Duration & Workload Live Training: 25 hours Individual study: 55 hours FULLY ONLINE OR BLENDED 3 ECTS CREDITS	Project management 1. Understand key concepts of project management, plan cybersecurity projects with clear objectives and scope, identify and analyse current cybersecurity threats, design incident response and emergency plans, report cybersecurity threats and incidents accurately. 2. Resource management 3. Security metrics 4. Quality assurance and quality control Assessment Self-assessment: 40% Final knowledge test: 60%
POWERED BY	Co-funded by the European Union Powered by: Priors, EWA, WISE, HackerU



OBJECTIVES	WHAT YOU WILL LEARN
• Apply metrics and analytics to protect assets. • Use analytics to identify risks and improve security. • Evaluate, mitigate, and report security threats effectively.	• Manage, identify, analyse, assess, estimate, investigate the cybersecurity-related risks of ICT infrastructures, systems and service projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.
CHARACTERISTICS	TRAINING CONTENT
Languages Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish. Duration & Workload Live Training: 48 hours Individual study: 77 hours FULLY ONLINE OR BLENDED 5 ECTS CREDITS	Operating system administration 1. Comprehensive coverage of fundamental system administration concepts across Windows and Linux environments. 2. Database system administration 3. Network administration 4. Cloud administration 5. Security-physical system administration Assessment Self-assessment: 40% Final knowledge test: 60%
POWERED BY	Co-funded by the European Union Powered by: Priors, EWA, WISE, HackerU



OBJECTIVES	WHAT YOU WILL LEARN
• Apply metrics and analytics to protect assets. • Use analytics to identify risks and improve security. • Evaluate, mitigate, and report security threats effectively.	• Manage, identify, analyse, assess, estimate, investigate the cybersecurity-related risks of ICT infrastructures, systems and service projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.
CHARACTERISTICS	TRAINING CONTENT
Languages Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish. Duration & Workload Live Training: 25 hours Individual study: 55 hours FULLY ONLINE OR BLENDED 3 ECTS CREDITS	Performance measurements (metrics) 1. Understand key performance metrics, monitor systems and networks effectively, track and analyze performance metrics, create and interpret network maps, conduct vulnerability scanning, analyze network traffic for security insights. 2. Data analytics 3. Security intelligence 4. Assessment Assessment Self-assessment: 40% Final knowledge test: 60%
POWERED BY	Co-funded by the European Union Powered by: Priors, EWA, WISE, HackerU



OBJECTIVES	WHAT YOU WILL LEARN
• Manage cybersecurity operations confidently. • Efficiently monitor, detect, respond to and recover from cybersecurity incidents. • Apply industry-standard tools and best practices specifically tailored for SMEs.	• Manage, identify, analyse, assess, estimate, investigate the cybersecurity-related risks of ICT infrastructures, systems and service projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.
CHARACTERISTICS	TRAINING CONTENT
Languages Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish. Duration & Workload Live Training: 30 hours Individual study: 60 hours FULLY ONLINE OR BLENDED 3 ECTS CREDITS	Security Operations Fundamentals 1. Learn the essentials of Security Operations Centres (SOC), understand key roles and responsibilities, gain insights into tools and technologies through practical examples. 2. Security Convergence 3. Security information and Events Management (SIEM) 4. Security Operations practices Assessment Self-assessment: 40% (four tests) Final knowledge test: 60%
POWERED BY	Co-funded by the European Union Powered by: Priors, EWA, WISE, HackerU



OBJECTIVES	WHAT YOU WILL LEARN
• Apply security governance frameworks aligned with business goals and regulations. • Create and communicate security policies, including threat and incident management. • Communicate cybersecurity needs to executives to support decisions, compliance, and ethics.	• Manage, identify, analyse, assess, estimate, investigate the cybersecurity-related risks of ICT infrastructures, systems and service projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.
CHARACTERISTICS	TRAINING CONTENT
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	Organizational context 1. Understand the evolution, major threats, and unique cybersecurity challenges faced by SMEs, and assess how cybersecurity impacts business strategy and regulatory compliance. 2. Privacy 3. Laws, ethics, and compliance 4. Security governance 5. Executive and board level communication Assessment Self-assessment: 40% Final knowledge test: 60%
POWERED BY	Co-funded by the European Union Powered by: Priors, EWA, WISE, HackerU



OBJECTIVES	WHAT YOU WILL LEARN
• Apply security governance frameworks aligned with business goals and regulations. • Create and communicate security policies, including threat and incident management. • Communicate cybersecurity needs to executives to support decisions, compliance, and ethics.	• Manage, identify, analyse, assess, estimate, investigate the cybersecurity-related risks of ICT infrastructures, systems and service projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.
CHARACTERISTICS	TRAINING CONTENT
Languages Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish. Duration & Workload Live Training: 30 hours Individual study: 60 hours FULLY ONLINE OR BLENDED 3 ECTS CREDITS	Introduction to Cybersecurity Planning 1. Defining the legal aspects of data, human and societal security laws and policies that govern SMEs, classifying types of cyberattacks relevant to SMEs, identifying useful tools to prevent cyberattacks. 2. Strategic Planning 3. Operational and Tactical Management 4. Assessment Assessment Self-assessment: 40% (three tests) Final knowledge test: 60%
POWERED BY	Co-funded by the European Union Powered by: Priors, EWA, WISE, HackerU



OBJECTIVES	WHAT YOU WILL LEARN
• Identify and assess risks from various sources, threats, and vulnerabilities to gauge impact on objectives. • Use quantitative and qualitative methods to evaluate risk likelihood and consequences. • Plan, implement, and review risk treatments, and assess residual risk acceptability.	• Manage, identify, analyse, assess, estimate, investigate the cybersecurity-related risks of ICT infrastructures, systems and service projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.
CHARACTERISTICS	TRAINING CONTENT
Languages Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish. Duration & Workload Live Training: 30 hours Individual study: 25 hours FULLY ONLINE OR BLENDED 3 ECTS CREDITS	Risk assessment 1. General risk management process, general risk management framework, principles of risk management, risk management standards. 2. Risk identification 3. Insider Threats 4. Risk measurement, evaluation models and methodologies Assessment Self-assessment: 40% Final knowledge test: 60%
POWERED BY	Co-funded by the European Union Powered by: Priors, EWA, WISE, HackerU



OBJECTIVES	WHAT YOU WILL LEARN
• Equip learners to design and implement Business Continuity (BC), Disaster Recovery (DR), and Incident Response Plans for SMEs. • Monitor, detect, respond to, and recover from cybersecurity incidents efficiently. • Apply industry-standard tools and best practices tailored for SMEs.	• Manage, identify, analyse, assess, estimate, investigate the cybersecurity-related risks of ICT infrastructures, systems and service projects and teams to enhance system hardening and availability, and making ethical decisions in maintaining robust cybersecurity practices across various administrative domains for SME workplaces.
CHARACTERISTICS	TRAINING CONTENT
Languages Available in English, Finnish, Turkish, Norwegian, Lithuanian, Romanian, French, Polish, Spanish. Duration & Workload Live Training: 30 hours Individual study: 40-50 hours FULLY ONLINE OR BLENDED 5 ECTS CREDITS	Incident Response 1. Understanding the importance and key components of incident responses, threat identification, phishing, insider threats, developing and simulate an Incident Response Plan (IRP), role assignment and team drills. 2. Disaster Recovery 3. Business Continuity 4. Security Awareness, Training, and Education 5. Security Auditing Practices Assessment Self-assessment: 40% Final knowledge test: 60%
POWERED BY	Co-funded by the European Union Powered by: Priors, EWA, WISE, HackerU

www.cyberagents.eu



Kaunas Faculty



Co-funded by the European Union

Implementation – From Content to Action



Bootcamp **Sep 2025, Lithuania**

- 26 lecturers · 7 countries
- 6 guest speakers
- 3 days of training
- Hands-on platform testing

8



Platform **In progress**

- EN content uploaded
- Multilingual access
- Testing phase underway



Kaunas
Faculty



Co-funded by
the European Union

7

January 2026 – Pilot Training Begins



Pilot training January 2026



Start: January 2026



Target group:
SME employees



Also includes:
HEI & VET students (future
cybersecurity specialists)



How will it work?



Open-access ·
Multilingual platform



Everyone can join and
choose modules



Learn **one, several or**
all modules

9

www.cyberagents.eu



Kaunas
Faculty



Co-funded by
the European Union



CyberAgent in Numbers

>10 DELIVERABLES
Available on our website

3⁵⁹⁶ participants
WORKSHOPS
On SMEs and Cybersecurity organised

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

7 NEWSLETTERS
Keeping up with CyberAgent news!

160 000 PEOPLE REACHED

>700 FOLLOWERS



**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



Kaunas
Faculty



Co-funded by
the European Union



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

12

Project Partners



Kaunas
Faculty

