Co-funded by the European Union

EQF LEVEL 4-5

TRAINING MODULES FOR VET STUDENTS

CYBER AGENT 01.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

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

www.cyberagents.eu

Work Package 3: Cyber Security Change Agents Learning Resource Development

Deliverable 3.2: Training modules for VET students
Leader of 3.2 – TIMTAL (TR)

CONTENT

LIST OF TABLES

INTRODUCTION

The rapid changes in science and technology, the changing needs of individuals and society, innovations and developments in learning and teaching theories and approaches have directly affected the roles expected from individuals. This change defines an individual who produces knowledge, can use it functionally in life, can solve problems, think critically, is enterprising, determined, has communication skills, can empathize, contributes to society and culture, etc.

The dizzying speed brought by the information age brings with it the ever-changing needs of individuals and societies. Innovations in learning and teaching theories are radically changing the roles expected from individuals. Now, it is not just having knowledge, but also skills such as being able to use that knowledge functionally in life, being able to produce solutions to complex problems, being able to think critically, being able to act with an entrepreneurial spirit, being able to communicate effectively, being able to show empathy and adding value to society that come to the fore. This transformation encourages individuals to constantly learn, adapt and improve themselves.

In this context, vocational training is also undergoing a major transformation. Traditional professions are being replaced by new, technology-focused and constantly developing professions. Cybersecurity is of critical importance in this change. Because in the digitalizing world, cybersecurity risks are increasing in every sector and every profession. Cybersecurity plays a vital role in many areas, from personal data to the protection of corporate secrets, from the security of critical infrastructures to the security of financial transactions.

The importance of cybersecurity training in vocational education is not limited to technical skills. It also includes raising individuals who have ethical values, a high sense of responsibility, are familiar with legal regulations and are open to continuous learning. Because cybersecurity is not only a technical problem, but also a social responsibility. Therefore, giving the necessary importance to cybersecurity training in vocational education is a critical step for the future of both individuals and society.

Vocational education includes the planning, research, development, organization and coordinated management, supervision and teaching activities of all vocational and technical education services together with agriculture, industry and service sectors within the integrity of the education system. The aim of these educational activities is to train expert individuals who will ensure the continuity of society and qualified personnel needed at every stage of production, and to emphasize vocational training.

The Cyber Agent vocational education program (EQF4-5) is designed to prepare individuals for cybersecurity life and is based on the labour market needs and job analysis approach. The Cyber Agent curriculum aims to provide the knowledge, skills, attitudes and behaviours that must be possessed to perform the relevant work and transactions through lessons and achievements, while on the other hand, educational activities are planned in a way that will prepare individuals for business life in accordance with this framework.

1. OBJECTIVES OF THE CYBERAGENT EQF LEVEL 4-5 PROGRAM

The need for cybersecurity has become quite important, especially in EU countries, as well as all over the world, and has increased rapidly in recent years. Simultaneously with technological developments, cyber risks and threats have also changed at the same speed and become complex. Cyber risks and threats have reached a potential that will cause much more comprehensive and negative results than physical attacks. With sectors such as finance, electronic communication, energy, transportation and aviation providing services in a secure digital environment, ensuring national cybersecurity has become one of the top priorities for our country. In this context, it is aimed to disseminate cybersecurity education in formal and informal education, and to develop and enrich educational content.

2. THE EUROPEAN QUALIFICATIONS FRAMEWORK

The EU developed the European Qualifications Framework (EQF) as a translation tool to make national qualifications easier to understand and more comparable. The EQF seeks to support cross-border mobility of learners and workers, promote lifelong learning and professional development across Europe.

The EQF is an 8-level, learning outcomes-based framework for all types of qualifications that serves as a translation tool between different national qualifications frameworks. This framework helps improve transparency, comparability and portability of people's qualifications and makes it possible to compare qualifications from different countries and institutions.

The EQF covers all types and all levels of qualifications and the use of learning outcomes makes it clear what a person knows, understands and is able to do. The level increases according to the level of proficiency, level 1 is the lowest and 8 the highest level. Most importantly the EQF is closely linked to national qualifications frameworks, this way it can provide a comprehensive map of all types and levels of qualifications in Europe, which are increasingly accessible through qualification databases.

The EQF was set up in 2008 and later revised in 2017. Its revision has kept the core objectives of creating transparency and mutual trust in the landscape of qualifications in Europe. Member States committed themselves to further develop the EQF and make it more effective in facilitating the understanding of national, international and third-country qualifications by employers, workers and learners.

Each of the 8 levels of the EQF is defined by a set of descriptors indicating the learning outcomes relevant to qualifications at that level in any qualifications system. The learning outcomes are defined in terms of:

- Knowledge: in the context of EQF, knowledge is described as theoretical and/or factual.
- Skills: In the context of EQF, skills are described as cognitive (involving the use of logical, intuitive and creative thinking) and practical (involving manual dexterity and the use of methods, materials, tools and instruments).
- Responsibility and autonomy: In the context of the EQF responsibility and autonomy is described as the ability of the learner to apply knowledge and skills autonomously and with responsibility.

Table 1-EQF Level-4 Learning Outcomes

Knowledge	Ability	Responsibility and autonomy
Factual and theoretical knowledge in broad contexts within a field of study or learning	A set of cognitive and practical skills required to produce solutions to specific problems in a field of work or education	Apply self-management within the guidelines of work or learning contexts that are generally predictable but subject to change; supervise the routine work of others, take some responsibility for the evaluation and improvement of work or learning activities

3. CYBER SECURITY VET STUDENTS (EQF LEVEL 4-5)

Cyber Security employee (Level 4-5) is a qualified professional who works in the field of information systems in the workplace, participates in cyber security preventive activity studies within the scope of vulnerability tracking and cyber security awareness raising processes, follows up on actions, monitors the operation and sustainability of systems used in cyber security analyses, determines the requirements of simple networks, sets up physical networks, performs simple level configurations related to network hardware, ensures network security, maintenance and improvements, provides technical support to users and carries out professional development studies in order to protect workplace IT infrastructures against cyber threats within the framework of quality requirements by implementing occupational health and safety and environmental protection measures.

3.1. CYBERAGENT LEARNING PROGRAM FOR EQF-4-5

The VET curriculum (EQF 4-5) was developed by strategically adapting the comprehensive HEI curriculum (EQF 5-6). The adaptation process involved concentrating the material to align with the 1 ECTS scope and focusing on the learning outcomes most relevant to the VET audience and immediate SME needs. Priority was given to topics that emphasize practical application and foundational cybersecurity skills, while more in-depth theoretical concepts were streamlined to fit the VET learning pathway.

Table 2-Module: 1

Units	**Topics**
Project management	Project Planning Defining Project Objectives Current Cybersecurity Threats (DDoS, Ransomware, Malware, Phishing, Zero-Day, IoT attacks, etc.) Threat Modeling and Vulnerability Analysis Reporting Cybersecurity Threats and Incidents
Learning outcomes: • Learners will be able to define project management phases and create a basic project plan. (Application) • Learners will articulate clear, measurable, and attainable project objectives. (Analysis) • Learners will identify, classify, and evaluate various cybersecurity threats. (Analysis) • Learners will develop threat models and perform vulnerability analyses for specific scenarios. (Application) • Learners will prepare incident reports following established protocols. (Application)	
Resource management	Security Tools and Software Effective Use of Technological Resources
Learning outcomes: • Learners will demonstrate effective use of cybersecurity tools and software for threat detection and response. (Application) • Learners will optimize technological resources for enhanced security and efficiency. (Application)	
Security metrics	Security Metrics and Measurement Techniques Data Collection with SIEM Analysis of Security Metrics Project Monitoring and Performance Evaluation Reporting of Security Metrics
Learning outcomes: • Learners will identify and apply relevant security metrics and measurement techniques. (Application) • Learners will configure and utilize SIEM tools for data collection and security monitoring. (Application) • Learners will interpret and analyze security metrics to assess security posture. (Analysis)	

• Learners will monitor and evaluate project performance using security metrics. (Evaluation) • Learners will compile and present reports based on security metric analysis. (Application)	
Quality assurance and quality control	Quality Management Quality Standards in Cybersecurity Testing and Validation Techniques
Learner outcomes: • Learners will implement quality management practices in cybersecurity projects. (Application) • Learners will identify and apply relevant cybersecurity quality standards. (Application) • Learners will develop and execute testing and validation procedures for cybersecurity solutions. (Application)	

Table 3-Module: 2

Units	**Topics**
Operating system administration	Operating Systems Relationship Between Hardware and Software Binaries, Hexadecimal Counting Bits & Bytes Command Line in OS Windows & Linux Commands Windows Client & Server Applications, Processes, and Services in Windows File Extensions & Types Registry Keys and Values Control Panel Settings Users and Groups Domain Structure & Server Manager AD & GPO Linux Interfaces & Kernel Processes in Linux File & Directory Naming Conventions Linux Shells & Command Syntax Manipulating Files & Folders Working with Pipe & System Monitoring Commands Process Management & Job Control Service Management
Learner outcomes:	

• Learners will compare and contrast different operating systems and their architectures. • Learners will explain the interaction between hardware and software in an OS environment. • Learners will perform binary and hexadecimal conversions and understand data representation. • Learners will execute fundamental commands in Windows and Linux environments. • Learners will manage applications, services, and processes using system tools. • Learners will configure and manage Active Directory and GPOs. • Learners will interact with Linux interfaces and perform kernel-level operations. • Learners will manage services and system processes using Linux commands.	
Database system administration	Repositories & Source Lists Managing a Web Server System Logs & Log Monitoring Scheduling Tasks in Linux Server & Network Troubleshooting Backup & Recovery Securing the GRUB Firewalls Active Directory Objects & GPO Management DNS & DHCP PowerShell Fundamentals Microsoft BitLocker, AppLocker & Firewall LDAP & Kerberos NTLM Password & Lockout Policies Authentication & Access Control Internet Control Message Protocol (ICMP) TCP vs UDP NetBIOS & SMB SSL & TLS Certificates Telnet and Secure Shell (SSH) Protocols HTTP & HTTPS Mail Systems Protocols Domain Name System Protocol (DNS) FTP & RDP Encapsulation Vs. Decapsulation Network Sniffers & Wireshark TCP/UDP DHCP, DNS
Learning outcomes: • Learners will configure repositories and manage source lists. • Learners will analyze and monitor logs for troubleshooting and security. • Learners will perform backup and recovery operations to ensure data integrity. • Learners will implement security measures including firewalls, BitLocker, and AppLocker.	
Network administration	Network Types & Wireless Networks Networks & Topologies

	Devices Identity & Access Devices Infrastructure & Security Devices Specialized Devices & Network Architecture Virtual Networks Physical and Logical Addresses OSI & Network Models Data Encapsulation and Decapsulation Network Protocols and Port Numbers Network Media and Cables Wireless Technologies Network Administration Tools Cisco Packet Tracer Network Classes & Subnetting Address Resolution Protocol (ARP) Static vs. Dynamic IP Addressing Network Address Translation (NAT) Switches & Cisco IOS Switch Port Security & Router Interfaces Configuring VLANs & DTP Inter-VLAN Routing Introduction to ACLs Network Troubleshooting
Learning outcomes: • Learners will design and manage networks, understanding protocols and topologies. • Learners will configure VLANs, ACLs, and manage IP addressing schemes. • Learners will use tools like Wireshark and Cisco Packet Tracer for monitoring and troubleshooting.	
Cloud administration	Hypervisors & Virtual Machines Containers Securing Virtual Environments Backup & Recovery Cloud Computing & CSPs What Are Cloud Service Models Cloud Deployment Types Virtual Networks AWS Compute Services Amazon Elastic Compute Cloud (EC2) Cloud Monitoring Tools Automation and Orchestration Tools Cloud Security Threats and Vulnerabilities Identity and Access Management (IAM) Role-Based Access Control (RBAC) Multi-Factor Authentication (MFA) Cloud Data Encryption Virtual Private Cloud (VPC) Docker & Kubernetes
Learning outcomes: • Learners will manage virtual environments using AWS, Docker, and Kubernetes.	

• Learners will implement cloud security controls and identity management.	
Cyber-physical system administration	Security & Access Controls Authentication Types TACACS+ and RADIUS AAA Configuration Risk Management Goals Encryption & Decryption Hashing & Rainbow Tables MAC Spoofing & ARP Poisoning VLAN Hopping & Rogue DHCP ICMP Flood TCP & UDP Flood Session Hijacking DNS Spoofing Defense in Depth (DID) & Zero Trust Demilitarized Zones (DMZs) Honeypots & Network Hardening Best Practices for a Secure Network VPNs SSH & VNC Stateful vs. Stateless Firewalls Host-Based vs. Network-Based Hardware vs. Software Firewalls Web Application Firewall (WAF) AI in Firewalls IDS & IPS NIDS & HIDS Snort tcpdump
Learning outcomes: • Learners will secure networks using firewalls, IDS/IPS, and threat detection tools. • Learners will apply encryption techniques and manage security protocols.	
System hardening	GenAI Techniques Code Generation User Account Management and Access Control Anomaly Detection and Troubleshooting Resolving Apache2 Service Errors Patch Management & Updates Automated Backup & Recovery Recovering Deleted Files with GenAI Cybersecurity Procedures Threat Detection & Analysis Threat Response & Remediation Leveraging AI for Real-Time Threat Detection Validating and Testing GenAI Models DNS Configuration & Security DHCP Configuration & Security PowerShell Fundamentals

	Switch Port Security Network Basic Input/Output System (NetBIOS) Server Message Block Protocol (SMB) Secure Sockets Layer (SSL) & Transport Layer Security (TLS) Security Certificates Mail Systems Protocols Domain Name System Protocol (DNS) File Transfer Protocol (FTP) Remote Desktop Protocol (RDP) Scheduling Tasks in Linux Server Troubleshooting Network Troubleshooting Backup & Recovery Securing the GRUB Setting Up & Securing Firewalls
Learning outcomes: • Learners will apply hardening techniques to enhance system security. • Learners will leverage AI for threat detection and system monitoring.	
System hardening	IR vs. SOC Events and Incidents Alert Detection & Alert Triage Documentation and Reporting What Are Web Attacks? DoS and DDoS SQL Injection & XSS Command Injection & Local File Inclusion (LFI) Cross-Site Request Forgery (CSRF) Brute-Force & Credential Stuffing Pass the Hash & Pass the Ticket Broken Access Control Ransomware Computer Virus & Worm Trojan Horse & Adware Keylogger & Cryptojacking Fileless Malware Understanding the Spread of Malware Managing IOCs & Password Policies Acceptable Use Policies (AUP) Bring Your Own Device (BYOD) Policies Remote Access Policies
Learning outcomes: • Distinguish the key roles and collaboration of R and SOC. • Define the difference between security incidents and breaches. • Explain the sources of security alerts and triage processes. • Provide effective documentation and reporting for security incidents. • Outline common types of web attacks (DoS/DDoS, SQL Injection, XSS, Command Injection, LFI, CSRF). • Explain brute force and credential stuffing attacks and outline their countermeasures.	

• Understand the basic principles of "pass the hash" and "pass the ticket" attacks. • Explain how broken access control vulnerabilities can be exploited. • Explain different types of malware (Ransomware, Virus, Worm, Trojan, Adware, Keylogger, Cryptojacking, Fileless Malware) and their propagation methods. • Explain the importance of managing threat intelligence indicators (IOCs). • Outline the key elements of strong password policies and acceptable use policies (AUPs). • Evaluate the security impacts of BYOD and remote access policies.

Table 4-Module: 3

Units	**Topics**
Performance measurements (metrics)	Performance Metrics System and Network Monitoring Monitoring Performance Metrics Network Mapping Vulnerability Scanning Network Traffic Analysis
Learning outcomes: • Learners will define performance metrics and explain their significance in evaluating system and network performance. • Learners will demonstrate the setup and use of monitoring tools for continuous assessment of system and network performance. • Learners will analyze and interpret performance metrics to assess system health and identify optimization opportunities. • Learners will create network maps to visualize, monitor, and optimize network structures. • Learners will conduct vulnerability scans, identify security risks, and recommend remediation steps. • Learners will perform network traffic analysis to detect and respond to potential threats.	
Data analytics	Data Collection Data Cleaning and Preprocessing Data Analysis Data Visualization Analytical Tools Applications of Data Analytics in Cybersecurity
Learning outcomes: • Learners will gather relevant data from systems, networks, and security logs for analysis. • Learners will clean and preprocess raw data to ensure accuracy and consistency. • Learners will apply statistical and analytical techniques to extract meaningful insights from data. • Learners will create data visualizations to effectively communicate analysis results.	

• Learners will utilize tools such as Python, R, and Power BI for comprehensive data analysis. • Learners will apply data analytics techniques to detect, analyze, and mitigate cybersecurity threats.	
Security intelligence	Understanding Security Intelligence Sources of Security Intelligence Threat Intelligence Collection Methods Case Studies on Security Intelligence Applications
Learning outcomes: • Learners will explain the importance of security intelligence in proactive threat management. • Learners will evaluate sources of security intelligence, including threat feeds, reports, and open-source tools. • Learners will describe methods for collecting and analyzing threat intelligence. • Learners will examine real-world cases to understand the application of security intelligence in preventing cyber threats.	

Table 5-Module: 4

Units	**Topics**
Security Operations fundamentals	Understanding Security Operations and SOC (Security Operations Centre) Roles and responsibilities in Security Operations Overview of security operations tools and technologies Practical examples and case studies
Learning outcomes: • Learners will explain the purpose and structure of a Security Operations Centre and its role in cybersecurity. • Learners will describe the roles and responsibilities of security operations personnel, including incident response, threat hunting, and monitoring. • Learners will identify and demonstrate the use of common security operations tools and technologies. • Learners will analyze real-world examples and case studies to understand security operations in practice.	
Security Convergence	Understanding security convergence Fundamentals of physical security (physical security principles, protecting physical assets, policies) Common threats faced by SMEs Case studies highlighting convergence issues
Learning outcomes: • Learners will define security convergence and explain its importance in integrating physical and cybersecurity measures. • Learners will apply principles of physical security to protect assets, facilities, and personnel. • Learners will identify and evaluate security threats commonly faced by small and medium-sized enterprises (SMEs).	

• Learners will examine case studies to understand the impact of convergence challenges. • Learners will review security information and event management processes.	
Security Information and Events Management	Review of security monitoring principles (based on other partners module) Implementing SIEM solutions Setting up logs and alerts Review of threat intelligence and detection methodologies (based on other partners module)
Learning outcomes: • Learners will explain security monitoring principles and their application in SIEM solutions. • Learners will configure and operate SIEM solutions for effective threat detection and response. • Learners will set up logging and alerting mechanisms in SIEM tools to monitor security events. • Learners will assess threat intelligence and detection methodologies for effective security operations.	
Security Operations Practices	Compliance and regulation Continuous improvement strategies in security operations Automation and orchestration Metrics and reporting
Learning outcomes: • Learners will explain the importance of compliance and regulation in security operations. • Learners will design and implement continuous improvement strategies for security operations. • Learners will leverage automation and orchestration to enhance security operations efficiency. • Learners will develop and use security metrics and reporting techniques to communicate security posture.	

Table 6-Module: 5

Units	**Topics**
Organizational context	Evolution of cybersecurity in SMEs Current major threats and vulnerabilities Impact of cybersecurity on business strategy Specific challenges of cybersecurity in SMEs versus large enterprises Understand the regulatory implications of cybersecurity practices and how they align with governance structures. Commmon cybersecurity challenges specific to SMEs, such as limited budgets, lack of dedicated security staff, and practical methods for prioritizing cybersecurity investments.
Learning outcomes:	

<table>
<tr><td colspan="2">

Learners will trace the development of cybersecurity practices within small and medium-sized enterprises.
Learners will identify and evaluate the most critical current threats and vulnerabilities affecting SMEs.
Learners will analyze how cybersecurity influences business strategy and operational decision-making.
Learners will compare the cybersecurity challenges faced by SMEs with those encountered by larger organizations.
Learners will interpret the regulatory requirements for cybersecurity and assess how they integrate with organizational governance.
Learners will describe practical solutions for common SME cybersecurity challenges, such as budget constraints and limited personnel.

</td></tr>
<tr><td>Privacy</td><td>Privacy principles in cybersecurity
Personal data protection and GDPR
Impact of privacy on SME operations
Tools and techniques for privacy protection</td></tr>
<tr><td colspan="2">Learning outcomes:

Learners will explain the core privacy principles in the context of cybersecurity.
Learners will apply GDPR requirements and evaluate their impact on personal data protection.
Learners will assess how privacy regulations affect daily operations and business models of SMEs.
Learners will use tools and implement techniques for maintaining privacy and protecting sensitive data.

</td></tr>
<tr><td>Laws, ethics, and compliance</td><td>Cybersecurity Organizations, Policies and Standards
Relevant national and international legislation
Regulatory compliance in SMEs
Ethics in Cybersecurity
Legal consequences of non-compliance in cybersecurity
Analysis of how AI-based tools can be utilized to strengthen cybersecurity governance and ensure compliance through continuous monitoring and automated threat response.</td></tr>
<tr><td colspan="2">Learning outcomes:

Learners will identify key cybersecurity organizations and assess relevant policy and standards frameworks.
Learners will summarize key laws affecting cybersecurity on national and international levels.
Learners will design strategies to achieve and maintain regulatory compliance in SME contexts.
Learners will examine ethical considerations in cybersecurity decision-making and behavior.
Learners will evaluate the legal ramifications of failing to comply with cybersecurity laws.
Learners will explore how AI tools can improve governance, automate monitoring, and enhance compliance.

</td></tr>
<tr><td>Security governance</td><td>Cybersecurity governance structure
Roles and responsibilities in security management</td></tr>
</table>

	Cybersecurity maturity models Enhance abilities in conducting risk assessments and formulating strategic response plans under simulated crisis conditions (Ransomware, phishing attack, ..) Executive and board level communication Cybersecurity communication strategies Security reporting to senior management Crisis management and communication in cybersecurity Master crisis management and decision-making skills in high-stress scenarios involving AI-driven attacks and ransomware.
Learning outcomes: • Learners will design and evaluate governance structures that support effective cybersecurity management. • Learners will assign and clarify responsibilities in organizational security frameworks. • Learners will assess cybersecurity maturity using established models. • Learners will conduct risk assessments and develop response strategies for scenarios like ransomware or phishing. • Learners will develop communication plans for conveying cybersecurity insights to senior executives and board members. • Learners will formulate effective communication strategies for internal and external cybersecurity stakeholders. • Learners will generate reports that inform senior management about cybersecurity performance and risks. • Learners will practice managing and communicating during cybersecurity crises, including those involving AI-driven attacks	
Managerial policy	Policy implementation and monitoring
Learning outcomes: • Learners will implement cybersecurity policies and establish procedures for their ongoing monitoring and enforcement.	

Table 7-Module: 6

Units	**Topics**
Introduction to Cybersecurity Planning: Data, human and societal security	Data security - Information Storage Security, Investigatory process Data security - Password attack techniques Human security -Awareness and Understanding Societal security – what are Cybercrime, Cyber ethics Societal security - Cyberlaw- Digital evidence, Digital contracts, Multinational conventions (accords)
Learning outcomes: • Learners will implement strategies to secure stored information and support investigatory processes. • Learners will identify and analyze common password attack techniques and develop appropriate countermeasures.	

<table>
<tr><td colspan="2">

Learners will promote cybersecurity awareness and foster understanding among employees and stakeholders.
Learners will explain the societal implications of cybercrime and evaluate ethical considerations in digital environments.
Learners will interpret key cyberlaw concepts, including digital evidence, contracts, and international accords.

</td></tr>
<tr><td>Operational and Tactical Management</td><td>Implementing Access Controls
Patch Management and Software Updates
Continuous System Monitoring
Employee Security Awareness Training</td></tr>
<tr><td colspan="2">Learning outcomes:

Learners will design and implement effective access control mechanisms to protect systems and data.
Learners will establish procedures for timely patch management and software updates to reduce vulnerabilities.
Learners will conduct continuous monitoring of systems to detect and respond to security events.
Learners will develop and deliver security awareness training programs to enhance employee engagement and reduce human risk.

</td></tr>
</table>

Table 8-Module: 7

Units	Topics
Risk assessment	General risk management framework and process Principles of risk management Risk management standards Practical examples and case studies
Learning outcomes: • Learners will describe and apply the general framework and process of risk management in cybersecurity. • Learners will explain the core principles that guide effective cybersecurity risk management. • Learners will identify and interpret widely accepted risk management standards. • Learners will evaluate risk scenarios through real-world examples and case studies	
Risk identification	Tangible and intangible sources of risk Causes and events Threats and opportunities Vulnerabilities and capabilities Changes in the external and internal context 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.
Learning outcomes: • Learners will distinguish between tangible and intangible sources of risk in cybersecurity environments. • Learners will identify risk causes and triggering events. • Learners will analyze cybersecurity threats and assess potential opportunities for improvement. • Learners will evaluate vulnerabilities and organizational capabilities in managing risks. • Learners will assess how contextual changes influence cybersecurity risks. • Learners will identify indicators signaling the emergence of new cybersecurity threats. • Learners will assess asset value and resource criticality in relation to risk. • Learners will estimate the potential consequences and their impact on strategic goals. • Learners will recognize the limitations of information and knowledge in the risk identification process. • Learners will reflect on how human factors affect risk perception and identification. • Learners will apply identification techniques through real-world scenarios.	
Insider threats	Definition and types of an insider threats Detecting and identifying insider threats Practical examples and case studies
Learning outcomes: • Learners will define insider threats and classify the various types. • Learners will develop skills to detect and respond to insider threat indicators.	

• Learners will analyze case studies of real-life insider threat incidents.	
Risk measurement and evaluation models and methodologies	Quantitative and qualitative risk assessment models and methodologies The likelihood of events and consequences The nature and magnitude of consequences Sensitivity and confidence levels. Practical examples and case studies
Learning outcomes: • Learners will compare and apply both quantitative and qualitative models in cybersecurity risk assessments. • Learners will evaluate the likelihood and potential outcomes of identified risks. • Learners will assess the severity and extent of consequences associated with cybersecurity risks. • Learners will determine levels of uncertainty and confidence in risk assessments. • Learners will implement risk evaluation models in practical scenarios.	
Risk control	Monitoring and review Recording and reporting Practical examples and case studies
Learning outcomes: • Learners will conduct regular risk monitoring and review processes. • Learners will document and report risk control measures effectively. • Learners will examine real-world examples to understand effective risk control implementation.	

Table 9-Module: 8

Units	Topics
Incident response	Definition and Importance of Incident Response Key Components of an Effective Incident Response Recovery Plan Common Cybersecurity Threats
Learning outcomes: • Learners will define incident response and explain its significance in cybersecurity management. • Learners will identify and implement key elements of a structured incident response recovery plan. • Learners will recognize and respond to common cybersecurity threats encountered during incident handling.	
Disaster recovery	Understanding Disaster Recovery Roles and responsibilities in Disaster Recovery Recovery steps after disaster
Learning outcomes: • Learners will explain the principles and goals of disaster recovery in the context of cybersecurity. • Learners will describe the roles and responsibilities of team members involved in disaster recovery.	

• Learners will develop a step-by-step plan to restore systems and operations after a cyber disaster.	
Business continuity	Understanding business continuity Roles and responsibilities in business continuity Business Impact Analysis
Learning outcomes: • Learners will explain the concept and importance of business continuity planning. • Learners will identify the roles and responsibilities related to ensuring business continuity. • Learners will conduct a business impact analysis to assess critical functions and dependencies.	
Security awareness, training and education	Understanding security awareness Employee responsibilities in cybersecurity
Learning outcomes: • Learners will explain the role of security awareness in reducing human-related cybersecurity risks. • Learners will recognize employee responsibilities in upholding cybersecurity protocols and best practices.	
Security hiring practices	Defining security roles requirements Conducting throughout background checks
Learning outcomes: • Learners will define cybersecurity job roles and formulate appropriate requirements. • Learners will apply best practices in conducting background checks for security-sensitive roles.	
Security termination practices	Revoking access immediately Notifying relevant teams Legal and compliance considerations
Learning outcomes: • Learners will implement procedures for promptly revoking access upon employee termination. • Learners will coordinate communication with relevant departments during the offboarding process. • Learners will examine legal and compliance requirements related to employment termination in cybersecurity.	
Third-party security	Assessing third-party risk Implementing contrasts and security requirements Ongoing monitoring and auditing Incident response and communication
Learning outcomes: • Learners will assess security risks associated with third-party vendors and partners. • Learners will design and apply contractual clauses to ensure third-party security compliance. • Learners will establish continuous monitoring and auditing practices for third-party security. • Learners will coordinate with third parties during incident response activities.	
Security in review processes	Incorporating security into reviews Vulnerability assessment and penetration testing

	Post-incident reviews
Learning outcomes: • Learners will integrate security considerations into organizational review processes. • Learners will conduct vulnerability assessments and penetration tests as part of review activities. • Learners will conduct post-incident reviews to evaluate effectiveness and improve future responses.	
Special issue in privacy of employee personal information	Data collection limitations Storage and access control Compliance with privacy regulations Data sharing and third parties Employee consent and rights
Learning outcomes: • Learners will identify appropriate boundaries for collecting employee personal data. • Learners will apply secure storage and access control measures for sensitive employee data. • Learners will ensure compliance with relevant privacy regulations such as GDPR. • Learners will evaluate risks and rules surrounding employee data sharing with third parties. • Learners will understand employee rights and the importance of obtaining informed consent.	

CONCLUSION

This report presents the curriculum appropriate to the vocational education level that should be taken into account for the successful implementation of CyberAgent training. Following the research conducted since the beginning of the project to identify the training needs, this document describes the needs of vocational education students for their participation.

The curriculum prepared for CyberAgent project EQF Level 5-6 was taken as a reference during the preparation of the program. From this level curriculum, topics suitable for EQF Level 4-5 were selected.

Finally, in order to ensure that the training is of the highest quality in terms of content, organization and skill development, questions related to topics not transferred from EQF Level 5-6.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau