DEFENSIVE CYBERSECURITY (EMaCS-03-02)				
DEGREE PROGRAM:	Master in Computer Science for the Human-Centric and Sustainable Industry			
SEMESTER: Third	**TYPE:** Basic	**CREDITS:** 5 ECTS	**WORKLOAD:** 125 hours	**MENTORING:** 0,5 hours/week
LANGUAGE: English				

OBJECTIVES	
General	Student can protect ICT systems against intrusions by utilizing technical solutions and is able to make informed decisions when procuring solutions.
Specific	• Develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products.

SUSTAINABILITY

The Defensive Cybersecurity course contributes significantly to sustainability by empowering students to protect ICT systems against intrusions through informed decision-making and the utilization of technical solutions. Sustainability, in the context of cybersecurity, involves ensuring the longevity and resilience of digital infrastructures. Students gain knowledge about secure development lifecycle models, operating systems security, and information systems hardening, aligning with sustainable practices. The emphasis on cybersecurity controls and solutions fosters an understanding of defensive security practices, contributing to the sustainability of digital environments. Additionally, the course promotes ethical outcomes by instilling an awareness of the importance of communication, coordination, and cooperation with internal and external stakeholders. Collaborative teamwork is encouraged, emphasizing the collective responsibility for sustaining secure digital ecosystems.

RESILIENCE AND HUMAN-CENTRIC DEVELOPMENT

The Defensive Cybersecurity course actively contributes to resilience and human-centric development by equipping students with the skills to develop, deploy, and operate cybersecurity solutions on infrastructures and products. The technical focus on security controls, secure development lifecycle models, and information system hardening enhances the resilience of digital systems against potential threats. Students learn to configure solutions according to the organization's security policy, fostering adaptability and responsiveness in the face of evolving cyber threats. The emphasis on defensive security practices aligns with a human-centric approach, ensuring that cybersecurity measures prioritize the protection of individuals and organizations. The course promotes collaborative works and effective communication, reinforcing the importance of teamwork and collective efforts in building resilient cybersecurity strategies.

SUBJECT MATTER

- Technical security controls.
- Software development lifecycle security models.
- Information system hardening.
- Network security.

COMPETENCES

C1. AQUIRING DATA, INFORMATION AND DIGITAL CONTENT
C5. PROGRAMMING
C7. PROTECTING PERSONAL DATA AND PRIVACY
C8. PROTECTING HEALTH AND WELL-BEING
C9. REFLECTING ON ETHICAL OUTCOMES
C10. EXPLORATORY AND CRITICAL THINKING
C11. PROBLEM FRAMING
C12. IDENTIFYING NEEDS AND TECHNOLOGICAL RESPONSES
C14. SOLVING TECHNICAL PROBLEMS
C18. COLLABORATING THROUGH DIGITAL TECHNOLOGIES

LEARNING OUTCOMES

Knowledge	Know about: • Secure development lifecycle. • Operating systems security. • Computer networks security. • Information systems hardening. • Cybersecurity controls and solutions. • Offensive and defensive security practices. • Secure coding recommendations and best practices. • Cybersecurity recommendations and best practices. • Cybersecurity-related technologies.
Skills	• Integrate cybersecurity solutions to the organisation’s infrastructure • Acquire the ability to configure solutions according to the organisation’s security policy. • Be able to identify and solve cybersecurity-related issues.
Attitudes/values	• Become aware of the relevance to communicate, coordinate and cooperate with internal and external stakeholders correctly. • Promote collaborative works with other team members and colleagues.

TEACHING METHODS

Method	**Class Workload**	**Individual Workload**	**Total**
Theoretical Sessions	4	50	54
Laboratory Sessions	16	55	71
TOTAL	**20 hours**	**105 hours**	**125 hours**

EVALUATION

Evaluation Procedure	**Percentage on the subject grade**
Laboratory Assignments	50%
Homework Assignments	50%
TOTAL	**100%**

PRECONDITIONS

Basics of programming (Python), Linux operating system, Virtualization

DEPARTMENT	School of ICT
LECTURERS	Jani Ekqvist
LITERATURE	To be defined later.