OPERATIONAL CYBERSECURITY (EMaCS-03-06)

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	Students are expected to extend their knowledge of security operations centre's concept and activities, to trial, compare and promote technical solutions suitable for SOC operation, and to implement threat hunting and monitoring controls and tools as part of security operations centre's tasks and processes. After completing the course, the students are expected to plan, implement and conduct different cybersecurity incident handling and threat hunting activities to enhance the overall security posture of computer systems and the network infrastructure.
Specific	• List the relevant standards overarching information security management. • Perform structures for various data types. • Build capabilities for visualising and monitoring anomalies and correlated threats in computer networks. • Plan and document cybersecurity incident handling processes and workflows for various SOC tiers and operators. • Utilise threat intelligence information in threat hunting.

SUSTAINABILITY

The course significantly contributes to sustainability by addressing cybersecurity within the framework of Cybersecurity Policies and Recommendations. By instilling knowledge about best practices and policies, students learn to approach operational cybersecurity with a sustainable and standardized mindset. The emphasis on Resilience and Readiness to Restore Vital Functionalities highlights the importance of cybersecurity measures in maintaining the stability and functionality of computer systems. By understanding and implementing incident handling processes, students contribute to the overall sustainability of organizational operations in the face of cyber threats.

RESILIENCE AND HUMAN-CENTRIC DEVELOPMENT

In the context of resilience and human-centric development, the program equips students with a range of skills in Threat Hunting, Incident Handling, and Response. This empowers them to actively engage in monitoring anomalies, identifying threats, and responding effectively to cybersecurity incidents. The emphasis on Collaboration through Digital Technologies underscores the human-centric aspect, encouraging teamwork and cooperation in dealing with cybersecurity challenges. Moreover, the focus on Applying Principles of Social Safety and Security reflects the commitment to ensuring not only technological resilience but also the well-being of individuals and communities affected by cybersecurity incidents. Through these aspects, the course promotes a holistic and human-centric approach to operational cybersecurity.

SUBJECT MATTER

This study focuses on the networked infrastructure monitoring as part of organisations' operational activities with emphasis on reactive actions in anomaly detection and respective control processes, and also in the resilience and readiness to restore vital functionalities.

COMPETENCES

C3. MANAGING AND EVALUATING DATA, INFORMATION AND DIGITAL CONTENT
C4. INTEGRATING AND RE-ELABORATING INFORMATION and DIGITAL CONTENT
C5. PROGRAMMING
C6. USING MACHINE LEARNING AND A.I. TECHNIQUES
C11. PROBLEM FRAMING
C13. CREATIVELY USING DIGITAL TECHNOLOGIES
C16. WORKING WITH OTHERS

C18. COLLABORATING THROUGH DIGITAL TECHNOLOGIES

LEARNING OUTCOMES

Knowledge	• Know about: ○ Cybersecurity policies. ○ Cybersecurity recommendations and best practices. ○ Incident handling standards, methodologies and frameworks. ○ Incident handling tools. ○ Incident handling communication procedures. ○ Security Operation Centres (SOC) operation. ○ Computer Security Incident Response Teams (CSIRTs) operation. ○ Cybersecurity-related technologies. ○ Computer system vulnerabilities.
Skills	• Practice technical, functional and operational aspects of cybersecurity incident handling and response. • Utilise cyber threat information in threat hunting activities. • Work on operating systems and relevant infrastructures. • Model & identify threat actors' TTPs and campaigns. • Analyse network traffic semantics. • Integrate cybersecurity solutions to the organisation's infrastructure. • Configure solutions according to the organisation's security policy. • Use XDR platform. • Perform threat hunting to detect attacks hidden from conventional defensive systems.
Attitudes/values	• Apply principles of social safety and security.

TEACHING METHODS

Method	**Class Workload**	**Individual Workload**	**Total**
Instructor-led laboratory sessions	17	0	17
Applied laboratory assignments	0	88	88
Research project	0	30	30
TOTAL	**17 hours**	**118 hours**	**135 hours**

EVALUATION

Area	**Corresponding weightage**
Laboratory/Home Assignments	50 %
Applied Project	30 %
Written group assignments and presentations	20 %
TOTAL	**100 %**

PRECONDITIONS

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

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