CYBER THREAT INTELLIGENCE (EMaCS-03-01)				
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 broaden their knowledge of different ways to utilise cyber threat intelligence information, especially from the defenders' viewpoint. Students conduct and perform data analysis on various cyber threat intel datasets gathered from different sources. Students will also design and implement customised dataset and information models for more efficient cyber threat contextualization in various sectors. The course is intended to stimulate the students' creativity, critical thinking and threat assessment by engaging in the analysis of short-term and long-term, real-life cyber threats.
Specific	• Use cyber threat intelligence and information in cyber defence. • Identify and mitigate various risks in specialized network infrastructure such as industrial networks. • Conduct and perform data analysis on various cyber threat intel datasets gathered from different sources. • Design and implement your own customised set of data and information models for more efficient cyber threat conceptualisation.

SUSTAINABILITY

The course on Cyber Threat Intelligence plays a pivotal role in promoting sustainability by equipping students with the knowledge and skills to assess and enhance an organization's cybersecurity posture. In the realm of cybersecurity, sustainability encompasses the ability to maintain robust defences against evolving threats. Students gain insights into cyber threat intelligence sharing standards, methodologies, and frameworks, fostering a collective and collaborative approach to cybersecurity. Understanding advanced and persistent cyber threats prepares students to contribute proactively to the sustainability of digital ecosystems. Additionally, the emphasis on ethical and responsible information sharing procedures underscores the importance of maintaining a secure and trustworthy digital environment, aligning with sustainability principles.

RESILIENCE AND HUMAN-CENTRIC DEVELOPMENT

The Cyber Threat Intelligence course significantly contributes to resilience and human-centric development by emphasizing proactive preparedness for potential threats. Students develop skills to identify, mitigate, and analyse risks in specialized network infrastructures, including industrial networks. The course stimulates creativity, critical thinking, and threat assessment, fostering a resilient mindset among students. The ability to design and implement customized data and information models enhances the adaptability of cybersecurity strategies, aligning with the principles of resilience. Furthermore, the course encourages effective communication, coordination, and cooperation with internal and external stakeholders, acknowledging the human-centric aspect of cybersecurity and promoting a collaborative approach to building resilience in the face of cyber threats.

SUBJECT MATTER

This course focuses on the correlation of information regarding threat-related data and metadata to assist in decision making. The emphasis will be on proactive preparedness for and anticipation of potential threats for the organisation.

COMPETENCES

C2. BROWSING, SEARCHING AND FILTERING DATA, INFORMATION AND DIGITAL CONTENT
C3. MANAGING AND EVALUATING DATA, INFORMATION AND DIGITAL CONTENT
C5. PROGRAMMING
C7. PROTECTING PERSONAL DATA AND PRIVACY

C8. PROTECTING HEALTH AND WELL-BEING
C9. REFLECTING ON ETHICAL OUTCOMES
C15. MANAGING SYSTEMS and/or PROJECTS
C17. COMMUNICATING EFFECTIVELY

LEARNING OUTCOMES

Knowledge	• Know about cyber threat intelligence sharing standards, methodologies, frameworks and threat actors. • Know how to develop cyber threat intelligence contexts. • Know about threat actors' tactics, techniques and procedures (TTPs). • Know about cyberattack procedures. • Know about advanced and persistent cyber threats.
Skills	• Be able to assess and enhance an organisation's cybersecurity posture. • Acquire the capacity to collect, analyse, correlate and enrich cyber threat information originating from multiple sources. • Be able to model & identify threat actors' TTPs and campaigns. • Be able to automate threat intelligence management procedures. • Acquire the ability to conduct technical analysis and reporting. • Be able to use CTI platform and to extend CTI platform's utilisation through integrations.
Attitudes/values	• Become aware of the relevance to communicate, coordinate and cooperate with internal and external stakeholders correctly. • Apply principles of social safety and security. • Accept the need applying ethical & responsible information sharing procedures.

TEACHING METHODS

Method	**Class Workload**	**Individual Workload**	**Total**
Instructor-led laboratory sessions	17	0	17
Applied laboratory assignments	0	98	98
Research project	0	20	20
TOTAL	**17 hours**	**118 hours**	**135 hours**

EVALUATION

Area	**Corresponding weightage**
Laboratory/Home Assignments	60 %
Applied Project	20 %
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.