COURSE SYLLABUS

Cybersecurity Operations and Incident Response, 7.5 credits

Cybersecurity operations och incidenthantering, 7,5 högskolepoäng

Course Code:	TCOS25	**Education Cycle:**	Second-cycle level
Confirmed by:	Dean Mar 1, 2024	**Disciplinary domain:**	Technology
Valid From:	Jan 1, 2025	**Subject group:**	DT1
Version:	1	**Specialised in:**	A1F
		Main field of study:	Computer Science

Intended Learning Outcomes (ILO)

After a successful course, the student shall:

Knowledge and understanding
- display knowledge of key standards and frameworks for cybersecurity operations and incident response
- display knowledge of key concepts and technologies for network security and intrusion detection
- display knowledge of different tools and applications for security monitoring, digital forensics, and evidence collection

Skills and abilities
- demonstrate skills in using tools for security monitoring, digital forensics, intrusion detection, and log management
- demonstrate skills in creating and using an incident response plan

Judgement and approach
- demonstrate an insight into the different phases of a cyberattack and suggest how an organisation can protect itself against cyberattacks during the different phases
- demonstrate an insight into the societal, legal, and ethical aspects of cybersecurity operations and incident response

Contents

Cybersecurity operations are crucial to protecting an organisation's assets' confidentiality, integrity, and availability. The course starts with discussing key standards and frameworks for cybersecurity operations and incident response. The course includes technical concepts of network security, intrusion detection, as well as security monitoring, and digital forensics. During the course, students will gain hands-on experience of common tools and applications used for security monitoring, digital forensics, and intrusion detection.

The course includes the following elements:
- Key standards and frameworks for cybersecurity operations, Security Operations Centre (SOC) concepts, blue teaming, etc.
- Key standards and frameworks for incident response (e.g., NIST SP800-61), different phases in the incident response plan, and handling of cybersecurity incidents
- Different phases of a cyberattack (e.g., Cyber Kill Chain, MITRE ATT&CK, attack trees, threat intelligence, etc.)
- Network security concepts including intrusion detection/prevention, firewalls, network admission control, virtual private networks, etc.
- Digital forensics and digital evidence, including computer and network forensics
- Security monitoring, intrusion data analysis, security information, and event management (SIEM)

Type of instruction

The course consists of lectures, laboratory work, and project work.

The teaching is conducted in English.

Prerequisites

Passed courses at least 90 credits within the major subject in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent, and taken course Ethical Hacking and Penetration Testing, 7,5 credits or the equivalent. Proof of English proficiency is required.

Examination and grades

The course is graded 5,4,3 or Fail.

Registration of examination:

Name of the Test	Value	Grading
Project[I]	4 credits	5/4/3/U
Laboratory	2 credits	U/G
Seminar	1.5 credits	U/G

[I] Determines the final grade of the course, which is issued only when all course units have been passed.

Course literature

The literature list for the course will be provided eight weeks before the course starts.