Tallinn University of Technology
School of Information Technologies

ITC8270 Cyber Incident Handling

Extended syllabus
Fall 2024

Course aims/objectives:	The student has the foundational knowledge required to work in a security operation center (SOC) and is able to participate in cyber incident response.
Learning outcomes:	The student: - knows how to establish incident handling team and typical team designs. - can manage cyber incidents, preserving needed evidence and chain of evidence. - can build incident management system and manage cooperation between law enforcement and incident handlers. - can establish procedures for evidence and incident management.
Brief description of the course (topics):	Triage and basic incident handling Creating incident handling procedures and testing Large scale incident handling Cooperation with Law Enforcement agencies Identifying and handling cyber-crime traces Incident handling and cooperation during phishing campaign Law enforcement view of computer security incidents Law enforcement needs for evidence analysis Role of (tabletop) exercises in developing incident handling capability
Language of the course:	English
ECTS credits:	6 ECTS
Students:	This is a compulsory course for students studying on the Cyber Security MSc (IVCM) programme's Cyber Security and Digital Forensics specializations.
Special needs:	Persons with disabilities can participate in this course. Please inform the professor(s) in the beginning of the course of any special instruction, or assessments of this course that may be necessary to enable you to fully participate in this course.
Registration:	Students who would like to take the course should declare the course in the ÕIS (Student Information System) by deadlines set in the academic calendar.
Prerequisite courses and/or knowledge:	N/A
Prerequisite resources:	Internet access, webcam with microphone
Professor(s):	Rain Ottis, rain.ottis@taltech.ee Andrew James Roberts, andrew.roberts@taltech.ee
Contacting Professor(s):	Preferred means of contact is using e-mail or Teams.
Schedule for classes:	Online sessions on Thursdays at 1800.
Study process description:	The course will be held on-line. Materials are accessible via Moodle. Lectures will be on BBB (via Moodle) or Teams.

Course's e-support: Course materials can be accessed via the e-learning environment Moodle under the course title ITC8270 Cyber Incident Handling (Fall 2024): https://moodle.taltech.ee/enrol/index.php?id=33802. If you are not a Cyber Security MSc student, please contact the professor for the password.

Study literature: Provided via the e-learning environment

Assessment: The students will have a number of individual and group tasks for a total of 100 points:

1. Individual tasks – 60% of the grade
    a. 6x Quiz/reflection [10 points each]

2. Group tasks – 40% of the grade
    a. Incident Management Plan or Red Team Campaign Plan for a given fictional entity [20 points]
    b. After Action Report for the tabletop exercises [20 points]

In order to pass the course, the student will have to earn at least 30 points for individual tasks and 21 points for group tasks, as well as participate in the tabletop exercises.

Detailed requirements and evaluation criteria for each task are described in the course Moodle page.

The sum of points for each item is converted into a grade using the following principles:
"5" excellent 91-100
"4" very good 81-90
"3" good 71-80
"2" satisfactory 61-70
"1" poor 51-60
"0" fail less than 51

Academic integrity: As a student at Tallinn University of Technology, you have an obligation to conduct your academic work with honesty and integrity according to University standards. It is expected that all work that you submit will be your own, and that you have actually done the work that you are submitting. Plagiarism and cheating will not be tolerated. While use of AI tools for graded assignments is allowed, any such use must be properly documented.

Failure to abide by the rules above will be followed with grade "0" for the course and a notice to the Program Manager and the School's Committee for Handling Violations of Academic Practice and Contemptible Behaviour. Depending on the Committee's proposal, it may lead to Dean issuing a letter of reprimand or in case of repeated or very severe misconduct, exmatriculation from the University.

Detailed schedule and topics

The semester plan is preliminary and might be changed in case of guest lecturer cancellations, changes in available reading material, etc. Up-to date instructions and links to weekly on-line sessions will be provided through the course Moodle page.

The course spans 16 weeks. Every week there is one on-line session, containing (guest) lectures, student presentations, discussion and/or tabletop exercises. The students also have various written assignments and additional reading.

Detailed schedule is provided in the course Moodle page.