EP279V Cyber Security Analysis 3.0 credits

Cybersäkerhetsanalys

This is a translation of the Swedish, legally binding, course syllabus.

Establishment

The official course syllabus is valid from the autumn semester 2026 according to the decision by director of first and second cycle education. Decision date: 2026-03-04

Grading scale

P, F

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Knowledge and skills in basic programming, 5 credits.

At least one of the following three:

- Knowledge and skills in ethical hacking, 3.5 credits, equivalent to completed course EP274V.
- Knowledge in IT security, 6 credits, equivalent to completed course in cybersecurity, data security, information security, network security or similar.

- At least 3 years of professional experience in a technical role in one of the following areas: system development, system administration, system architecture, IT architecture, IT security. This must be verified, for example with a certificate from the employer.

English skills equivalent to the upper secondary school course English B/English 6.

Intended learning outcomes

After passing the course, the student should be able to

- model threats in large-scale computer systems (including software, networks, etc.)
- describe and evaluate threats and attacks in large-scale computer systems
- describe defence mechanisms for computer system and how they relate to vulnerabilities and attacks
- carry out risk analysis based on a model
- report and present models, a cybersecurity risk analysis, and defense strategies for a computer system

in order to

- understand and explain which threats a specific system can have
- understand and explain how attacks work and propagate through a system architecture
- argue why certain risks should be prioritised
- choose an effective defense to decrease risk.

Course contents

This course teaches a threat modeling-based method for analyzing cybersecurity risks for systems-of-systems. It includes developing and combining models for computer system resilience, threat actor capabilities, and business impacts of realized threats into an overall cyber risk assessment. Moreover the course addresses how cyber risk analysis is used for identifying and arguing for cost efficient defense mechanism selection for protecting the analyzed system-of-systems.

Examination

- PRO1 - Project assignment, 3.0 credits, grading scale: P, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

If the course is discontinued, students may request to be examined during the following two academic years.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.