Module Description, available in: EN

Cyber Security

General Information

Number of ECTS Credits

3

Module code

TSM_CyberSec

Valid for academic year

2026-27

Last modification

2025-10-14

Coordinator of the module

Michael Mäder (HES-SO, michael.maeder@hefr.ch)

Explanations regarding the language definitions for each location:

- Instruction is given in the language specified for each location and module execution.
- Documentation is available in the language(s) listed for each location and module execution. If the documentation is in multiple languages, the percentage distributed is indicated (100% = all documentation provided).
- The examination, including both questions and answers, is provided entirely (100%) in the language(s) specified for each location and module execution. The exams are on-site.

	Lausanne			Lugano	Zurich		
Instruction	**X** E 100%						
Documentation	**X** E 100%						
Examination	**X** E 100%						

Module Category

TSM Technical scientific module

Profile Recommendations

This module is recommended for the following profiles:

	Lausanne
Profile	CS, ICS

Lessons

2 lecture periods and 1 tutorial period per week

Entry level competences

Prerequisites, previous knowledge

- Basic concepts of cryptography
- Knowledge of at least one programming language, such as Python

Brief course description of module objectives and content

The course will first cover the basic knowledge required in the field of computer security, such as the CIA principles (confidentiality, integrity, availability), as well as data security and safety.

The module will build on this foundation to provide students with a comprehensive overview of how to identify and assess threats and risks. Students will then be able to propose and implement a set of mitigation measures. This course will be applied to three areas of security: secure software development, software security, and tool-based web security.

The course covers the following main topics:

- Review of basic security concepts.
- Secure development (DevSecOps)
- Software security
- Web security
- Cyber Threat Intelligence
- Deception techniques
- Social engineering

Aims, content, methods

Learning objectives and competencies to be acquired

- Understand and be able to select the appropriate cryptographic primitives.
- Identify and document the threats and risks to a system and propose various types of mitigation mechanisms.
- Understand, apply, and use processes and tools for secure development.
- Understand and identify vulnerabilities in software and web applications, and propose mitigation measures.

Module content with weighting of different components

Basics (20%) :

- Confidentiality, integrity, availability, authenticity, authorization, accountability.
- Threat models, malware, etc.
- Data protection under the GDPR/nLPD
- Data protection and data obfuscation techniques (pseudonymization, anonymization) in relation to the GDPR/nLPD
- Intrusion Detection and SIEM (Security Information & Event Management)
- Risk and threat analysis and standards

Secure development (40 %) :

- SDLC: DevOps fundamentals and how DevOps teams can build and deliver secure software.
- DevSecOps: how to integrate security into continuous delivery and deployment.
- Security automation tools, patterns, and techniques in DevOps.

Software Security (20 %) :

- Identifying software vulnerabilities (SANS Top 25)
- Software exploitation techniques and tools
- Software protections and mitigations

Web Application Security (20%) :

- Web Vulnerabilities (OWASP Top 10)
- Web Exploitation Techniques and Tools
- Web Security Measures and Mitigation Strategies

Teaching and learning methods

This course includes theoretical presentations and practical exercises (labs).

Literature

Course slides, references to online resources, and book references are mentioned in the module introduction and throughout the semester.

Assessment

Additional performance assessment during the semester

The module contains additional performance assessment(s) during the semester. The achieved mark of the additional performance assessment(s) applies to both the regular and the resit exam.

Description of additional performance assessment during the semester

Practical assignments (labs) will be carried out throughout the semester. These will be assessed and will account for 30% of the final grade.

Basic principle for exams

As a rule, all standard final exams are conducted in written form. For resit exams, lecturers will communicate the exam format (written/oral)

together with the exam schedule.

Standard final exam for a module and written resit exam

Kind of exam

Written exam

Duration of exam

120 minutes

Permissible aids

Aids permitted as specified below:

Permissible electronic aids

- Personal summary (limited number of pages)
- No computer
- No internet access

Other permissible aids

No other aids permitted

Exception: In case of an electronic Moodle exam, adjustments to the permissible aids may occur. Lecturers will announce the final permissible aids prior to the exam session.

Special case: Resit exam as oral exam

Kind of exam

Oral exam

Duration of exam

30 minutes

Permissible aids

No aids permitted