MASTER OF SCIENCE IN ENGINEERING

Module Description, available in: EN

Cyber Security Operations

General Information

Number of ECTS Credits

3

Module code

TSM_CyberSecOp

Valid for academic year

2024-25

Last modification

2023-07-03

Coordinator of the module

Bruce Nikkel (BFH, bruce.nikkel@bfh.ch)

Explanations regarding the language definitions for each location:

- Instruction is given in the language defined below for each location/each time the module is held.
- Documentation is available in the languages defined below. Where documents are in several languages, the percentage distribution is shown (100% = all the documentation).
- The examination is available 100% in the languages shown for each location/each time it is held.

	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:

	Zurich
Profile	ICS

Lessons

2 lecture periods and 1 tutorial period per week

Entry level competences

Prerequisites, previous knowledge

Students should have a basic understanding of the fundamentals of cybersecurity, including network security, system security, and cryptography. Additionally, they should have a good understanding of operating systems, and network architecture. Basic knowledge of OSINT would also be beneficial.

Brief course description of module objectives and content

This module is designed to provide a practical introduction to Cyber Security Operations. Students will learn about different operational security functions like SOCs, CERTs, DFIR teams, CTI and Hunt teams, Red and Blue teams, and the tools they use to detect and respond to cyber criminal activity. The module provides in depth coverage of digital forensics.

Aims, content, methods

Learning objectives and competencies to be acquired

Upon completion of the module, students should be able to:

- Understand operational cyber security roles and responsibilities within an organization,
- Explain basic concepts of detection, incident response, threat intelligence, and security testing.
- Perform digital evidence preservation and forensic analysis, conduct investigations
- Write forensic/incident reports for different recipients (police, regulators, management, technical peers)
- Restore an organization to a safe and operational state
- Understand how ethical hacking can be used to improve the security of systems

Module content with weighting of different components

DFIR: Digital Forensics and Incident Response (DFIR) is the main focus of the module. This includes securing and preserving digital evidence, forensic analysis, reconstructing past events, creating timelines, and performing investigations.

Detection: students will be introduced to logging and monitoring systems, intrusion and anomaly detection systems (HIDS and NIDS), and Security Information and Event Management (SIEM) systems, and other operational aspects of detection.

CTI: students will be introduced to Cyber Threat Intelligence (CTI), the intelligence process and lifecycle, intel sharing communities, intel / IOC exchange platforms (like MISP), and OSINT.

Security testing: The testing component covers a high level overview of penetration/Red-Team testing, security reviews, cyber excercises, and ethical hacking. The use of Bug-Bounty programs to improve security is also explained

Teaching and learning methods

Lectures with a mix of practical and theoretical exercises.

Literature

The following material is provided:

- Teacher's slides and notes
- Selected publications (papers, books)
- Relevant videos

Assessment

Certification requirements

Module does not use certification requirements

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

Will be communicated to students at the beginning of the module.

Other permissible aids

Will be communicated to students at the beginning of the module.

Special case: Resit exam as oral exam

Kind of exam

Oral exam

Duration of exam

30 minutes

Permissible aids

Aids permitted as specified below:

Permissible electronic aids

Will be communicated to students at the beginning of the module.

Other permissible aids

Will be communicated to students at the beginning of the module.