inholland
university of applied sciences

Security

Course guide 2024-2025

Semester	Spring (semester 2)
Inholland location(s)	Haarlem
Inholland faculty	Engineering, Design and Computing
Language of instruction	English
Cycle	Bachelor level
Number of ECTS	30

Subjects

Subject title	ECTS	Course code
Governance, Risk & Compliance	3	
Secure Software Development	4	
Cryptography	2	
Network Security	3	
Research Security	2	
System Hardening and Secure Virtual Systems	3	
Cyber Incident Response and Investigation	3	
The Human Factor	2	
Ethical Hacking & Tools	3	
Final Project Security	4	

Content subjects

The digital landscape is changing at a rapid pace. Now more than ever news about cyber security reaches us on an almost daily basis. New technologies are shifting the attack opportunities available for attackers, increasing the need for a new generation of cyber security specialists.

In 2023 an ISC2 study estimated the global security workforce gap to be four million people. This minor aims to offer students with the needed knowledge for the working field as well as preparing them for problems they will encounter in the field.

This minor focuses not only on gaining technical cyber security knowledge but also on bridging the gap between technical personnel and management. The minor covers a broad range of subjects to facilitate this particular goal.

This program is based on gaining an in-depth understanding of the five core functions of the NIST CSF 2.0 framework. The five core functions of this circular framework are: Identify, Protect, Detect, Respond & Recover, all driven by the core function Govern.

Most courses are assessed by working on real cases provided by partner companies. Students need to combine their research with the knowledge gained from the lectures to help define a solution for these problems.

These activities will contribute to gaining a breadth of experience, knowledge & skills over the broad spectrum of cyber security. Next to that, students are encouraged to gain high-level expertise in their Final Project. Here students have the opportunity to excel and grow in an expertise that best fits their interests.

Learning outcomes

At the end of this minor the student:
- Has an understanding of the complexities and dependencies in cyberspace;
- Can contribute to solving risks in cyberspace from both technical, policy, and managerial approaches;

- Has an understanding of the ethical responsibilities related to securing cyberspace.
- Can manage cyber threats to acceptable risks;
- Can manage the impact of a cyber incident to acceptable levels;
- Can bridge the gap between technical and more policy-oriented professionals within the organizations;
- Can translate tactical and operational cyber-related issues into a strategy for an organization;
- Can critically reflect on new developments and results within the field of cyber security;
- Has an understanding of laws and regulations related to IT security.

Mode of delivery, planned activities and teaching methods

Strategies and teaching activities
- Workshops / living labs by experts;
- Theoretical classes with practical exercises;
- Working on solving security problems of real companies;
- Researching security problems.

Prerequisites and co-requisites

Audience:
- Bachelor Information Technology 3rd & 4th year;
- Bachelor Business IT Management 3rd & 4th year;
- Bachelor Computer Science 3rd & 4th year.

Do keep in mind there are a lot of technical courses in this course. It is recommended that students have experience/knowledge of networking and programming.

Recommended or required reading and/or other learning recourses/tools

-

Assessment methods and criteria

- Final Project Assessment;
- Code assessment;
- Individual (written) exams;
- Case studies;
- Contributing to discussion forums.

Lecturer(s)

Teachers of the Information Technology program in Haarlem and various guest lectures & workshops by specialists from the field of Cyber Security.

One of the partners in this minor we work closely with is the Eurofins company, which specializes in IT Security.

Contact persons: Petra Folkertsma - Petra.Folkertsma@inholland.nl and Wiley Finch - Wiley.Finch@inholland.nl