Kristiania

Program description

Master in Cyber Security

120 ECTS

2023-2025

Studiet er akkreditert av Styret: 18.10.2022
Studiet er godkjent i Utdanningsutvalget: 30.09.2022 (UU/EIT-sak 121/22)
Programbeskrivelsen er godkjent i Utdanningsutvalget: 30.09.2022 (UU/EIT-sak 121/22)

Table of contents

1. Introduction

The main goal of the master program is to train future cyber security professionals knowledgeable in areas of secure software development, IT governance, audit, and management, where it is necessary to protect critical systems and national infrastructure from versatile cyber threats. Upon completion, students will be able to undertake the leadership role in managing the organization's cyber security strategy and architect complex and secure DevOps processes with cloud integration.

The study program will cover the following directions of professional development, that students will be able to focus on the following areas from information security:

- DevSecOps: integration of a security culture into the software development process and products deployment automation in the cloud
- Zero Trust Architecture: perimeter less security involving social-technical aspects of security
- Advanced Data Analytics: deployment of intelligent mechanisms to analyse enormous quantities of data and being able to find indicators of compromise

Moreover, the students will be able to work in the following domains connected to information security such that:

- Information Security Risk Management and IT governance
- Quantum Computing Security and Cryptography
- IoT (Internet of Things) security and security Cloud Orchestration
- Incident Readiness and Business Continuity
- Protection against ransomware and reverse engineering

Upon completion of the master's program, the following job opportunities will be available to students, however not limited to:

- Cyber security consultant
- Security Engineer
- DevSecOps engineer
- Chief Information Security Officer
- Chief Information Officer

Kristiania University College has the necessary competence and staff members with relevant qualifications and research portfolios to teach and supervise students in cyber security. A particular emphasis is put on qualification development through training and certifications in the field of information security to deliver the most relevant and up-to-date knowledge to our students. The study will be intricately connected to the cyber security laboratory (SmartSecLab) and all research groups at the School of Economics, Innovation and Technology working in the corresponding domain (MOTEL, AISE and others). It is a well-recognized national and international environment with an extensive network of cooperation partners and funded projects in cyber security.

The career development opportunities that are available to students after finishing the master's program:

- PhD program in Applied Information Technologies at Kristiania University College
- Professional certifications (CISSP, CISA, ISO27001, etc.) as the program structure is coherent with major professional development courses and programs

1.1 Formal requirements

To be qualified for enrolment in the Master in Cyber Security program, applicants must meet the following requirements:

- The target group of candidates must hold a bachelor's degree in Software Engineering, Information Security, Computer Science, Information Technology, Information Systems, Human Computer Interaction, or related disciplines with an average grade of minimum C equals minimum 2.7 ECTS. Relevant practices, or other special considerations, may, in some cases, weigh up for non-compliant grade requirements.
- The applicants must also write a motivational letter of 400-500 words in English describing their motivation to study at the master's program with insight into cyber security's role in modern society with its challenges and opportunities.
- The candidates must have programming knowledge (at least 7.5 ECTS of relevant courses with a minimum grade C), e.g., Python, Java, C/C++
- The candidates must have knowledge about cyber security principles (at least 7.5 ECTS of relevant courses), e.g. Confidentiality, Integrity, and Availability as well as relevant frameworks such as NIST cyber security framework.

2. Learning Outcomes

All study programs at Kristiania University College have established an overall learning outcome that every student is expected to achieve after completing the study. Learning outcomes describe what the student is expected to know, be able to and be able to do because of the learning processes associated with the study. Learning outcomes are described in the category's knowledge, skills, and general competence.

Knowledge

The candidate…

- has advanced knowledge in the main fields of cyber security, understands modern toolkit and technologies used to protect information and infrastructure
- can analyse modern computer systems and evaluate the level of implemented security controls
- has in-depth knowledge of theoretical approaches and corresponding practical methods

Skills

The candidate …

- can analyse the current state of the art in cyber security and develop own research projects
- can critically analyze available cyber security solutions and refine their knowledge based on the existing theoretical frameworks and tools
- can independently develop a project following NIST cyber security framework and relevant industrial standards

General competence

The candidate …

- can analyze problems related to ethics and legality of the application of cyber security tools
- can initiate and lead the innovation work in the field of cyber security practice and implementation
- can communicate terminology and problem areas from the domains in cyber security both in technical and non-technical terms

3. Structure of the program

Master in Cyber Security is two-year program that is a two-year program at Kristiania University College that covers 120 ECTS points, where 27.5 ECTS are cyber security-dedicated courses and 22.5 ECTS are a common set of courses offered at master level at the School of Economics, Innovation and Technology. Further, a student has an opportunity to spend a semester (30 ECTS) abroad as a part of the exchange program or to focus on building competence in the following recommended areas: (i) Zero Trust Architecture, (ii) Advanced Data Analytics or (iii) DevSecOps; or select elective courses from other relevant master's programs. The master's program concludes with dedicated work on a master's thesis project.

The study is offered across four semesters and has the following specific components:

<table>
<tr><th>Semester</th><th colspan="4">Master in Cyber Security</th></tr>
<tr><td>1. semester</td><td>Secure Software Development
7,5 ECTS</td><td>End-point and Cloud Security
7,5 ECTS</td><td>Cyber Threat Intelligence
7,5 ECTS</td><td>Ethics, sustainability, and society
7,5 ECTS</td></tr>
<tr><td>2. semester</td><td>Cryptography and Blockchain
7,5 ECTS</td><td>AI for Cyber Security
7,5 ECTS</td><td>Research Methods
7,5 ECTS</td><td>Proposal Development
7,5 ECTS</td></tr>
<tr><td rowspan="3">3. semester</td><td colspan="4">Recommended focus areas (Zero Trust Architecture, (ii) Advanced Data Analytics or (iii) DevSecOps)
30 ECTS</td></tr>
<tr><td colspan="4">Electives from the relevant area of study
30 ECTS</td></tr>
<tr><td colspan="4">Alternatively: Exchange semester abroad
30 ECTS</td></tr>
<tr><td>4. semester</td><td colspan="4">Master Thesis
30 ECTS</td></tr>
</table>

Table 1. Courses matrix

Specialization course	Elective courses

3.1 Academic progression

Master in Cyber Security is a complete second-degree master's program built on Kristiania University College's own Bachelor's program in Information Technology – cyber security specialization. During the first and second semesters, students will develop skills and competence in cyber security while building and managing versatile software products across a full range of network solutions. They will master knowledge in applying artificial

intelligence and open-source intelligence for extensive data analysis while looking for traces of incidents. In the third semester, students will have three opportunities to master their skills: (i) they can follow one of three recommended focus areas (reflecting different career opportunities for students in future that will be regularly updated), (ii) select relevant electives from other master's programs within SEIT portfolio or (iii) perform exchange semester abroad in partner universities. Finally, the master project will be executed in cooperation with industrial partners in the fourth semester.

3.2 Courses

Courses	ECTS	Description
Secure Software Development	7,5	Modern software is an overly complex system performing various tasks such as data analysis in healthcare systems, analyzing camera images in self-driving cars and even controlling gates in water damns. With increasing complexity, it is imperative to understand and integrate cyber security in every aspect of the software development lifecycle. The objective of the course is to give students an understanding of the core cyber security principles in CD/CI as well as DevSecOps to plan, develop and manage agile software products.
End-point and Cloud Security	7,5	The course aims to give students an understanding of the fundamental methods and tools to be used in the security of an entire range of solutions, from smaller Internet of Things applications to large-scale cloud systems. It is no longer a simple one-dimensional approach to deploying intrusion detection or anti-virus programs yet an orchestration of multiple tools. The students will learn how to navigate, deploy, manage, and monitor networks using conventional and cloud solutions with defence-in-depth principles and share responsibilities.
Cyber Threat Intelligence	7,5	Information has extreme value when collected and applied in a relevant and timely manner. The students will learn how to operate with the threat's information, open-source intelligence, social network intelligence, and forensics analysis of the artefacts and log files. They will also master skills in applying the attribution and basic triage based on internationally recognized frameworks, such as MITRE ATT&CK.
Ethics, sustainability, and society (common)	7,5	The main aim of this course is to provide students with the fundamental knowledge of ethics and sustainability necessary for responsible innovation and the development of modern technologies in modern society. The central topics include the role of ethics in responsible innovation and the development of information technology (IT); social, economic, and environmental impacts of innovations and modern technologies; and how IT development and innovation can contribute to achieving the UN Sustainable Development Goals. In covering ethical and sustainability issues, the course addresses the perspectives of various stakeholders at the individual level (IT developers, innovators, consumers,

		investors), the organizational level (commercial, public, and non-governmental organizations), and the societal level (local and regional communities, nations, international society). Group work on viable solutions to real-life ethical and sustainability challenges constitutes an essential part of the course.
Cryptography and Blockchain	7,5	Cryptography-enabled blockchain has become a revolutionary technology that changed many aspects of everyday life, from the economy to healthcare. While there are many benefits for the general social good, it is imperative to understand how to navigate cryptographic solutions to ensure systems security and everyone's privacy. Students will learn data-in-transit and data-at-rest encryption aspects, how to analyze bitcoin transactions and perform secure integration of common blockchain solutions.
AI (Artificial Intelligence) for Cyber security	7,5	The value of modern Information Technology systems lies in the information highlighted by the Big Data paradigm. With a growing amount of information, it becomes challenging to perform manual analysis of the log files, for example, for traces of attacks or system compromise. Artificial Intelligence has proven effective and time-efficient in performing cyber security-related data analysis tasks. The students will learn advanced data analytics, machine learning methods and how to perform the entire range of functions from data pre-processing to intelligent decision-making.
Research methods (common)	7,5	Research is a cyclical process where new and carefully planned investigations build and extend on established work. The aim is to provide students with a fundamental understanding of research as a conceptual, empirical, and practical approach to gathering new insight and knowledge. The content provides a broad overview of how researchers work in the economy, innovation, and technology. It presents students with relevant methods from these domains, along with their possibilities and limitations. Students will learn a systematic approach to empirical investigation, including literature search, research design and methodology, qualitative and quantitative analyses, and the presentation and evaluation of results. After the course, students can study and interpret existing research on a topic and suggest approaches to broaden or deepen knowledge within a given topic.
Proposal development (common)	7,5	This course's main objective is to help students conceptualize and prepare a research proposal in their area of interest and to nurture a sense of curiosity and active participation in research. The course has an applied approach that involves collaborative and reciprocal partnerships between the university (faculty, staff, and/or students) and external communities for the mutually beneficial exchange of knowledge and resources.

Table 2. Compulsory courses

3.3 Electives

The third semester in the Master in Cyber Security will give students flexibility in specializing in topics they want, either in cyber security, aligned master programs, or spending one semester abroad at the partner university. There is an ongoing process with the development of the courses on the master level depending on the current needs in the industry. Therefore, the students have access to the most up-to-date topics in the information technologies and cyber security through the following courses. The list of the elective courses to be offered at Kristiania University College in the Table 3 is subject to changes considering the modern technologies' development and cyber security trends. To facilitate the selection of the electives, the students will be offered a set of three recommended focus areas identified in the program's structure above to focus on building a corresponding career path.

Courses	**ECTS**
MS120 IT Governance	7,5
MA211 Mobile Computing and Internet of Things	7,5
Security Team Lead and Project Management	7,5
Viruses Reverse Engineering and Triage	7,5
Financial Fraud and Computer Audit	7,5
Data Privacy and Legal Aspects	7,5
Incident Response and Investigations	7,5
Critical Infrastructure and Operational Security	7,5
e-Health and Smart Environments Security	7,5
Digital Forensics	7,5
Intrusion Anomaly Detection and Prevention	7,5

Table 3. Elective courses and practice

3.4 Master Thesis (30 ECTS)

Course 30 ECTS	**Description**
Master thesis	The master thesis is a research project in which students will apply the knowledge acquired during their studies. It is a crafted scholarly document presenting research questions and original arguments based on scientific methods under the guidance of an advisor. The thesis gives the student the opportunity to demonstrate expertise in their chosen research area. Students will acquire specialized problem-solving skills, being able to plan and conduct the steps in the research and/or development process at a high methodological standard. They shall take responsibility to conduct a well planned and executed project.

Table 4. Master thesis

4. Teaching methods

Master in Cyber Security is designed so that the sum of the topics and study work with these will lead the students towards the intended learning outcomes described in chapter 2 in the program description. The pedagogical platform's goal is to facilitate and encourage learning.

The individual courses are put together to show a breadth of knowledge, skills and general competence that reflects the field of practice. Some courses are more oriented towards knowledge exchange, others more oriented towards building specific skills, while others include more skills in links between theory and practice. The master's program in cyber security is created as a continuation of the bachelor's in cyber security at Kristiania University College, and the comprehensive education can be later continued as a PhD in applied information technology.

Cyber Security is a rapidly developing area that requires considerable practice and exercises to align with the theoretical foundations. Therefore, forms of work, teaching and assessment in the individual courses have been chosen to provide a good and meaningful correspondence between the learning outcome that is desired to be achieved, the teaching methods used, and the exam that concludes the course.

The methodological choices also reflect the course's contribution to the study program. The students, therefore, encounter a varied set of learning activities throughout the study period, a variation that, in total, should reflect the field of practice the student is studying for. Moreover, students will enhance their learning through a combination of both individual and group assignments to highlight the importance of teamwork in the cyber security domain.

The *Master in Cyber Security* emphasizes that students learn to use relevant methods from research and professional development work / artistic development work. This will contribute to the students, through their master's studies being able to complete an independent, limited research or development project or artistic work under supervision and in line with current academic and ethical norms. To take care of this, the teaching will include emphasis commenting on, illustrating, and elaborating material from teaching materials, as well as providing guidance and additional material that is not available in printed form. Finally, the students will apply learnt material on a variety of problems and tasks in cyber security.

As with all higher education, Kristiania University College also sets requirements for students' independent learning work. Kristiania University sees it as a task to facilitate the students' work through good learning designs. At the same time, we emphasize that a teacher can only communicate and facilitate. The actual learning takes place with the individual student because of the student's work. In connection with the teaching, the student must therefore expect a significant personal effort both in acquiring theoretical knowledge as well as practising and exercising cyber security tools and technologies.

While attending the master program in cyber security, the educational model might include the following components to facilitate learning and skills enhancement:

- Lectures to introduce the theoretical concepts and frameworks
- Seminars, oral presentations, and group works give students an opportunity to present, discuss and argue upon topics and achieve results
- Supervision and assessment to guide the learning process
- Digital follow-up through acceptable platforms
- Use cases work and project execution
- Attendance of the specialized workshop offered by the research environment
- Independent practice, lab work and exercises
- Participation in the collaboration projects through the cyber security lab – both internally and externally
- Industry consultations and coordination for better alignment with industry needs

For students who need tutoring beyond scheduled teaching, Kristiania University College has available subject resources, including administrative staff, librarians, digital learning resources (e.g., online movies) and student tutors. These can be contacted by the individual student if needed. In addition to literature and help with literature searches, the library also offers varied training in academic writing.

During the study process, there will be organized course-specific academic and industry events will be held, where guest lecturers, external organizations and business actors can participate. The corresponding cooperation projects can be managed by the course coordinator and/or students and supported by administrative resources. For a master's in cyber security, this is relevant for all the mandatory courses in the courses list. See the course description for more information. Moreover, the students will be encouraged to attend cyber security-related events whenever possible through special arrangements and agreements to broaden their understanding of the field and job opportunities.

4.1 Forms of assessment

Assessment is a situation where a submitted or presented work is assessed against a set of criteria. Criteria are given by the learning outcome that are defined for the individual subject. The assessment can be made by fellow students, teachers, or examiners. These will also be happy to give feedback, either as guiding feedback or as a grade (exam) with a thorough explanation.

At Kristiania University College, we distinguish between assessment as learning, assessment for learning and assessment of learning. The form of the work being assessed (the assessment form) can be the same in all three of these assessment situations, while the purpose varies.

In assessment as learning (fellow student assessment) and for learning (feedback from the teacher), the purpose is to shape a learning process to help the student to achieve the best possible learning outcome. We perceive this assessment as part of the teaching methods, which can be found in Chapter 4.1 above.

Learning assessment is a final assessment where the achieved learning results are assessed - in other words, the exam. The exam at Kristiania University College is defined as "An exam is a final assignment within a course or a limited sub-course". The submitted or presented work is assessed through an examination, and the result of the assessment must appear on the diploma.

Master in cyber security is a study program with extensive range of topics and involved technologies. Therefore, students will be exposed to either of the following exam formats, which offer the best way of assessment and evaluating of the student's performance:

- Supervised examination
- Multiple choice questions
- Home exam
- Oral presentation
- Portfolio assessment
- Assignments through semester
- Master thesis project
- Project-based practical exams

Some of the courses might include compulsory assignments (one or more). A compulsory activity, if included in the course, is a requirement that must be approved to be eligible for the exam. The activity can either be a requirement that one or more reports or practical works must be submitted (work requirements) and/or a requirement for participation in defined activities and/or lectures and/or compulsory practice.

A compulsory activity is assessed as Approved / Not Approved and gives the right to sit for an examination in a course with compulsory activity requirement when such an activity is assessed as Passed. Furthermore, students will be eligible for feedback on the performance in the compulsory assignment. Otherwise, the student loses the right to an examination in the course until the activity (ies) has been assessed as Approved.

The assessment of the various exam forms will follow the Norwegian grading system with the scale A - F, where A is the best grade, E is the lowest pass grade and F is fail. Or the exam also may use a Pass / Fail evaluation, which will be decided for each course.

For additional information about the exam and compulsory activity, see Kristiania University College's website.

5. Internationalization and international student exchange

The course has schemes for internationalisation and international student exchanges, according to the Regulations on the Supervision and Control of the Quality of Norwegian Higher Education (Studietilsynsforskriften) of February 2017 (§ 2-2, sections 7 and 8)

The schemes for internationalisation are adapted to the level, scope and uniqueness of the course. The content of schemes for international student exchanges is academically relevant.

As regards to arrangements for international student exchange, Kristiania University College has the following mobility program:

- Nordplus in the Nordic region or the Baltic States
- ERASMUS + in Europe
- "Study Abroad", for students in and outside Europe

Kristiania University College has agreements on student exchanges and academic relevance secured by the academic field of study. Exchange courses from partners are approved by academic supervisors, for admission to the program, with an equivalent of 30 credits.

For nominations for student exchange, requirements are set for grades and motivation applications.

For students at Master in Cyber Security, student exchange is possible during the third semester. For outgoing students, Kristiania University College, has established student exchange agreements with the following institutions:

- Kingston University, UK
- Arcada University of Applied Sciences, Finland
- Seoul National University of Science and Technology, South Korea
- University of Hertfordshire, UK
- Assumption University, Thailand

Changes to approved universities may occur. Information about exchange stays for the relevant year is therefore published online and on the learning platform.

5.1 Internationalization

In this context, internationalization is understood as placing Master in Cyber Security in an international context and that the students are exposed to a multitude of perspectives. All the reading

materials and lectures are given in English, and the study uses both Norwegian and international cases. The students shall write their Master Thesis in English. The program uses international lectures and guest lecturers. Our lectures also conduct research with international co-authors and play an active role in both national and international conferences.

The study offer is set in an international context and exposes students to a varied perspective on brand building. This is achieved through extensive use of international literature and cases in teaching. The courses will be offered in English with the involvement of lecturers having internationally recognized research and industry experience in the field of cyber security. Selected topics will be presented by guest lecturer from abroad or by companies with relevant use-cases and focus.

For the specific internationalization schemes, please consult the corresponding subject descriptions.

5.2 International student exchange

When it comes to the international student's exchange, Kristiania University College participates in the following mobility programs:

- Nordplus in the Nordic and Baltic countries
- ERASMUS+ i Europa
- «Study Abroad», for studenter i og utenfor Europa

In the program Master in Cyber Security, there has been allocated third semester for the international student exchange with 30 ECTS credits. The list of partner university accepting students from Kristiania University College:

- Kingston University, UK
- University of Hertfordshire, UK
- Assumption University, Thailand
- Arcada University of Applied Sciences, Finland
- Seoul National University of Science and Technology, South Korea

Kristiania University College reserves the right to make changes to relevant study places and updated information is published on the university college's web. There are also a limited number of study places at the corresponding partner university available for the exchange. For nomination to exchange program, there are usually requirements for grades and motivation application. Requirements can also be set for documentation of creative work / portfolios and Kristiania University College can conduct interviews of applicants for exchange. Kristiania University College aims to send well-qualified and motivated students to reputable foreign institutions. For both on-site and online studies, the exchange is only site-based.

Exchange schemes apply to students who have an agreement on degree awarding studies and who have obtained a minimum of 60 credits at Kristiania University College.

In addition to established international exchange programs, mentioned above, the students will be exposed to a range of opportunities through the cyber security research laboratory and corresponding environment at the faculty. The activities will include participation in the cyber security conferences on the national and international level, summer and winter school attendance, Capture The Flag (CTF) competitions and relevant cyber security events.