UNIVERSITY WEST

Programme Description

Master in Cybersecurity

TACYB – Autumn 24

Decision taken by	Department board.
Document contact	Fatiha Djebbar, Head of Program
Version	1
Adopted	2022-09-21.

This template for program descriptions was adopted by the Research and Education Board, HV 2022/508, 21 September 2022, editorial change 25 October 2022. Program description is a supplement to the program syllabus which is the legally binding document.

Basic data

Department	Institutionen för Ingenjörsvetenskap
Division	Avdelningen för matematik, data och lantmäteri
Name of Programme, Swedish	Magister i cybersäkerhet
Name of Programme, English	Master in Cybersecurity
HE credits (number of credits)	60
Level (1st Cycle, 2nd Cycle)	2nd Cycle
Entry requirements, Swedish	Kandidatexamen om 180 högskolepoäng i datavetenskap, informatik, datateknik, informationsteknologi, eller motsvarande. Dessutom, kunskaper motsvarande Engelska 6 krävs för behörighet.
Entry requirements, English	Bachelor of Science in Computer Science, Informatics, Computer Engineering, Information Technology, or equivalent. Additionally, verified knowledge of English corresponding to the course English 6 in the Swedish Upper Secondary School (high school) or equivalent.
Main field of study, Swedish	Datavetenskap
Main field of study, English	Computer Science
Degree, Swedish	Filosofie magisterexamen i datavetenskap med inriktning mot cybersäkerhet
Degree, English	Degree of Master of Science in Computer Science with specialization in Cybersecurity
Rate of study (full-time, part-time)	Full-time
Type of instruction (on campus, distance teaching)	Campus
Language of instruction (Sw, En)	English

General programme information

The Master of Science in computer science with a specialization in cybersecurity is a one-year program that takes place on campus and is taught in English. It is designed to give you the knowledge and skills you need to succeed in the fast-growing field of cybersecurity in government and corporate organizations. You will learn about topics such as cybersecurity standards and regulations, securing cyber physical systems, risk assessment and management, cyber forensics, cloud security, and penetration testing. The program offers hands-on experience and opportunities to connect with the cybersecurity industry, and you will also receive training to earn a CCNA cybersecurity "CyberOps" certification.

At University West, you'll get the chance to be part of a leading work-integrated learning (WIL) University in Sweden. As a student in this program, you'll focus on problem-based learning for industry and work on real projects from partner companies. Your specialization in cybersecurity was created in partnership with industry experts and focuses on the pressing needs of governments and industry. You'll learn from professionals in the field and get introduced to the latest best practices in cybersecurity. Through guest lectures, company visits, and company-proposed degree projects, you'll gain hands-on experience to design real-world security solutions. You'll have the opportunity to discuss your understanding, ask questions, and propose ideas to experts and potential employers. This program will help you build a strong foundation in cybersecurity and prepare you to pursue a Ph.D. in computer science with a focus on areas like cybersecurity, cyber law, network security, and more. After graduation, you'll be able to continue your studies at University West or other universities in Sweden and around the world.

Programme contents, structure, and progression

The Master of Science in Computer Science with a specialization in Cybersecurity includes 6 mandatory courses and a thesis project. The courses selection and content are designed to meet the objectives of the Higher Education regulation and meet the industry's need for cybersecurity workforce. The proposed program includes the main functions of cybersecurity from risk management, compliance, law, regulations, security, hacking, to digital forensics. The broad knowledge nature of the curriculum allows you to assume cybersecurity activities within an organization and prepares you to design strategies that integrate best security practices and solutions following the appropriate cybersecurity standards and regulations.

Program content and structure

The total program consists of 60 credits in accordance with the European Credit Transfer and Accumulation System (ECTS). The program curriculum and content are described as follow:

–PFC610 Principles of Cybersecurity, 7.5 credits

This course will give the students a broad overview of the subject of cybersecurity, and how it relates to other parts of the IT security area. The course attempts to answer the following questions:

- The threats - who, where why?
- Systems and their weaknesses
- Preventive defenses - cryptography, AAA, network security, firewalls
- Organisational defenses - policies, training
- Monitoring, patching.

Part of the course is based on the Cisco Network Academy Program course Cyberops Associate. It focuses mostly on network and end point devices security.

–SCS600 Security of Cyber-Physical Systems, 7.5

The course focuses on the cybersecurity aspects of systems such as:

- Internet of Things (IoT)
- Industrial Internet
- Smart Cities
- Smart Grid and "Smart" Anything (e.g., Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances).

As a student, you are introduced to the concepts of general security architecture, network security, and cyber physical security. Importance of continuous assessment of security threats and the countermeasures is emphasized. The notion of physical, logical, and organizational security is provided. Leading industrial communication standards are covered both theoretically and practically.

–SIM600 Security in Cloud Services, 7.5 credits

The course covers cybersecurity in cloud services and systems. The course is based on lectures and hands-on experience of cloud security in a live cloud environment. The course also contains an introduction to research methodology, which is applied in an academic study of a cloud security topic. Main topics included in the course:

- introduction to cloud security
- managing user identities and access in the cloud
- Cloud Infrastructure Security
- Cloud Network Security
- data security in the cloud
- Cloud Security Management and Governance

- Operations Best Practices
- scientific methodology

–SLP600 Cyber Security Privacy, Law, Policy, and Compliance, 7.5credits
This course provides an overview of laws and ethical issues related to cybersecurity. The course also identifies policies, rules, and procedures that ensure connected devices and networks meet an acceptable level of security based on emerging frameworks for cybersecurity.

–AIR600 AI-based Risk Assessment and Management, 7.5 credits
This course introduces cybersecurity risk analysis and related AI-driven management concepts, as a foundation for cybersecurity protective mechanisms. AI-based principles and processes used for risk management methodologies are introduced. Comprehensive cybersecurity controls are practiced to learn about means to protect industrial infrastructure assets. The implication of AI methodologies in cybersecurity management is emphasized through machine learning tasks used to assess vulnerabilities and to prioritize remedial actions to reduce cyber risk.

–EHP600 Ethical Hacking, Penetration Testing, and IT Forensics, 7.5credits
In this course, several tools, and methods to improve cyber security are studied. Some of the methods are preventive and used to improve protection, and some are reactive and are used to handle suspected attacks. Preventive methods are ethical hacking and penetration testing. Ethical hacking uses methods like vulnerability research, threat analysis, and vulnerability reporting. The market for vulnerabilities is also discussed. Penetration testing uses methods like reconnaissance, scanning for vulnerabilities, exploitation of vulnerabilities, and credentials cracking. Reactive methods are log handling, IT incident handling, and IT forensics. Subjects in log handling are secure logging and log analysis. Subjects in IT incident handling are the different phases of incident handling, preparation, identification, containment, eradication, and recovery. Subjects in IT forensics are acquisition and preservation of digital evidence.

– EXD600 Degree Project in Computer Science, 15 credits
In this course, the knowledge from previous studies in computer science must be applied. This usually takes the form of development work, an investigation, a comparative study, or some other type of study. The work must be carried out independently by the students, documented in the form of a project report, presented orally at a degree project seminar.

Program progression

The program objectives are based on the national objectives for the master's degree described in the Higher Education Ordinance. You obtain the master's degree after completing the requirements of 60 higher education credits with your specialization, of

which at least 30 higher education credits with specialization in the main area of education. The proposed program fulfills these criteria by requiring a bachelor's degree in computer science, computer engineering, information technology, electrical engineering, or a related subject, offering:

1. 15 credits on advanced level (SCS600 and PFC610), requiring courses at the undergraduate level as prerequisites. These courses are offered at the 1st period (LP1) as described in Figure 1.
2. 30 credits offered in LP2 and LP3 are on advanced level including SIM600, SLP600, EHP600 and AIR600 which require previous advanced level courses, SCS600 and PFC610, as prerequisites, and
3. 15 credits on advanced level, consisting of the degree project for master's degree EXD600 and offered at the last period of the program LP4.

A summary of program dependencies among courses and the path for progression are described in the following Figure.

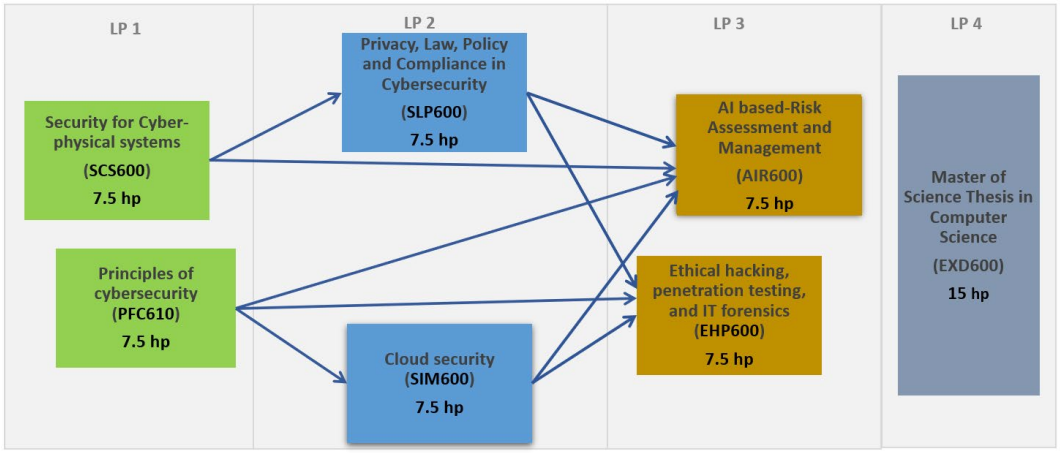

Figure 1: Courses Progression Plan, showing course dependencies.

The courses progression plan and the courses dependencies can be summarized as follow:

- As a student in the Master's in Cybersecurity program, you'll start with a solid foundation in the basics of cybersecurity. The courses "Security for Cyberphysical Systems" and "Principles of Cybersecurity" introduce fundamental concepts and terminologies related to cyberphysical systems (CPSs) and IT systems. The "Principles of Cybersecurity" course covers basic networking and provides an overview of defensive and offensive security techniques applied to IT systems. Meanwhile, the "Security for Cyberphysical Systems" course focuses on the

security of IoT and industrial systems. By completing these courses, you'll have the needed foundation for the rest of the program's courses.

- The "Privacy, Law, Policy and Compliance in Cybersecurity" course serves as a crucial link between the field of cybersecurity and its legal, ethical, and regulatory framework. This course helps you to examine laws related to privacy issues and the standards and regulations in cloud security, network security and risk assessment. The courses " Cloud security", "AI-based Risk Assessment and Management", and "Ethical Hacking, Penetration Testing and IT Forensics" build upon the knowledge gained in the "Privacy, Law, Policy and Compliance in Cybersecurity" course. In "Cloud security" course, you will learn how to identify internal and external threats to the operation of the cloud, network, and attached devices. You will then apply this knowledge in the " Ethical Hacking, Penetration Testing and IT Forensics" course, where you'll build and test security controls using industry-standard tools. After gaining an overall understanding of threats and vulnerabilities related to a given system, you will use the "AI-based Risk Assessment and Management" course to assess the risk and manage it based on the organization's risk tolerance strategy.

- The "Degree project" comes as an opportunity for students who gained a broad background in cybersecurity from prior courses in the program to deepen their expertise in a specific selected topic in one of the contemporary cybersecurity trends. Knowing that cybersecurity is circumstantial, students will need to adapt their security design and implementation to the topic environment. They will work individually on their project with the support of faculties within the department and industry partners. A summary of program dependencies among courses and path for progression is described in Figure.1.

DEGREE

Upon completion of this master's programme, you will receive a Master of Computer Science (MSc, 60 credits) with a specialisation in Cybersecurity.

The research basis for the programme

The Engineering Science department at University West offers two undergraduate programs and about 3 graduate programs. These programs include challenging courses and opportunities for research projects. The projects can be supervised by University West

senior lecturers who specialize in cybersecurity research or by industry collaborators, where you will have the opportunity to learn from experts in the field.

The department also provides opportunities for Ph.D. students. Graduates of these programs who choose not to immediately work in industry will be well-prepared to continue their studies and earn a Ph.D. in computer science-related fields like cybersecurity, cyber law, and network security anywhere in the world. The doctoral enrollments also mean that we establish a more far-reaching collaboration with other institutions in both the development of education and research that also will ensure that the doctoral students enter a larger environment meeting other doctoral students within the field and where a larger range of courses can be obtained. The doctorial students will also be involved in teaching activities (20% each).

The department has plans to grow by bringing in new experts, such as guest professors and senior lecturers who have the level of competence of full or associate professors. This will lead to the integration of the department into the Primus research environment, which will create opportunities for internal research collaborations and an increase in external funding for industrial IT security projects.

The labour market, collaboration, and work-integrated learning[1]

It is widely acknowledged that there is a significant demand for cybersecurity professionals and a shortage of skilled workers in the field. According to global market statistics, the following trends are apparent:

- The U.S. Bureau of Labor Statistics, employment of information security analysts is projected to grow 32% from 2019 to 2029, much faster than the average for all occupations.

- Cybersecurity Ventures, a market research firm, predicts that the global cybersecurity workforce will face a shortage of 3.5 million professionals by 2021, and this shortage is expected to grow to 6 million by 2025 (see Figure 2).

Recent legal regulations, including the EU Cybersecurity Act (CSA), are advocating for the development and adoption of security requirements to assure safety for organisations,

[1] Work-integrated learning is a pedagogical practice in which students' learning takes place through the integration of theoretical and practical knowledge and experience, derived from an educational context within the framework of both higher education as a work environment and civil society.

critical infrastructures, and consumer products. Furthermore, all manufacturing companies will need to comply to ensure consumer products safety, data privacy, etc. In summary, the employment figures for cybersecurity are high and are expected to grow significantly in the coming years due to the increasing demand for cybersecurity professionals and the shortage of skilled workers in the field.

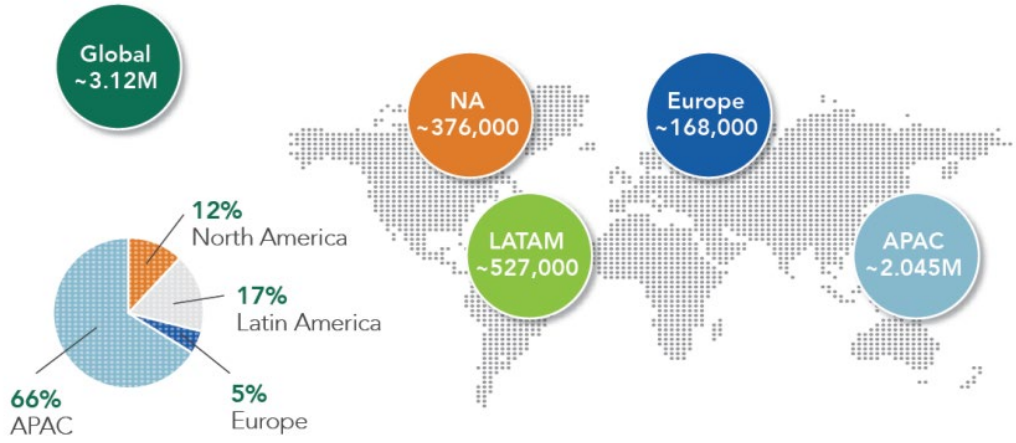

Figure 2: The global gap in the cybersecurity workforce

On graduation, you will be highly competitive for positions within the private and public sectors or for further PhD studies – anywhere in the world. You will be qualified to hold positions such as:

- Cybersecurity engineer
- Cybersecurity architect
- Cybersecurity consultant/analyst
- Cybersecurity specialist
- Penetration tester
- Forensic investigator
- Incident responder
- Audit/compliance consultant

In the Trollhättan and Gothenburg region alone, where University West is located, there are promising opportunities in multinational companies such as:

- Volvo Car
- NEVS
- GKN
- Husqvarna AB
- Combitech.

As these companies increase their development of connected and autonomous products, they must hire cybersecurity experts to address potential cyber risks.

Sustainable development

As a student in the Master's in Cybersecurity program at University West, it's important to understand how technology and security practices impact the environment, economy, and society. Sustainability is seen as a key aspect in all three dimensions, and University West places a strong emphasis on promoting sustainability in all its forms. Additionally, the university values diversity, gender equality, and inclusiveness, are strong basis that are reflected in its policies and programs.

Through industry collaboration, which is a key part of the academic complete environment at University West, you will have the opportunity to learn from experts in the field to develop sustainable best practices and standards. This will help you not only gain a deeper understanding of sustainability in cybersecurity, but also contribute to a more sustainable future. Sustainability is integrated into several courses in the Master's in Cybersecurity program, including:

- AI-based cyber–Risk Assessment and Management (AIR600): Implementing a comprehensive risk management plan that addresses cybersecurity threats and vulnerabilities can help organizations achieve sustainability by reducing the likelihood of data breaches and other security incidents. This can include measures such as encryption, firewalls, and intrusion detection systems.

- Cyber Security Privacy, Law, Policy, and Compliance (SLP600): Governments and organizations can work together to establish policies and regulations that encourage sustainability in cybersecurity. For example, there may be tax incentives for organizations that implement green cybersecurity practices, or regulations that require organizations to disclose any cyber breach against private data.

- Cloud security (SIM600): This includes in part using cloud computing and other technologies that reduce the energy consumption of IT systems and networks.

- The Degree Project course (EXD600) requires that students incorporate a focus on sustainability in their thesis work. This means that students will design, evaluate, or analyze systems, standards, and policies regarding economic, social, and environmental sustainability.

In addition to the above, you also could take a free course given by one of our collaborators. The course focuses specifically on the topic and will allow you to receive a certificate that you can include in your CV and show your future employer that you are aware of your impact on society.

Internationalisation

Internationalization is an important experiential learning component in higher education. It increases the quality of your education and positively impacts your social and cultural experience. You could be in contact with an international environment including teachers and students, and gain the soft skills usually connected to an international exchange. As University West is hosting several international master programs, cultural diversity is becoming a prominent façade to University West.

You will be studying with students from China, India, Vietnam, Turkey, Uganda, Kenya, Nigeria, South America, and EU-students to broaden your international experience. You will also be studying with Swedish students recruited from our own bachelor programs (for instance the Bachelor of Science in Programming and Networking students) and this will give the possibility to international students to integrate with the Swedish society. I addition, university West is working to strengthen existing collaborations and to develop new ones with other European universities. Visits to partner universities (for instance with the UC3M, Spain, TU Dortmund, Germany) are planned for the next two years with the aim of discussing collaboration. Brand new collaborations are also planned with the universities SUES in China, HZ in the Netherlands, and Wroclaw University of Science and Technology in Poland. Guest lecturers from abroad will also be invited in some of the courses to add to your international experience in the program.

Other information

As a student in the Master's in Cybersecurity program, you'll have access to various IT resources and support services provided by University West. These resources include basic services such as email, support from the university library and working rooms with desktops. You can expect these resources to work effectively and efficiently, so you can focus on your studies.

For the technical courses in the program, you'll need access to:

- Networking and security lab equipment. University West has a Cisco networking lab that partially meets these requirements. This lab, located on the ground floor of building B, features professional networking equipment, firewalls for isolating networks for cybersecurity experiments,
- A virtualization environment for cloud security experiments, and IoT lab equipment for cyber-physical systems security experiments.

With these resources at your disposal, you'll have the tools and equipment you need to successfully complete your coursework and advance your skills in cybersecurity.