Noroff
University
College

DIPLOMA

Tamas Szmandra
born 27 December 1980

on the 21 August 2024 was awarded the degree

Bachelor in Cyber Security

Programme of study: Bachelor in Cyber Security

The diploma is issued 27 September 2024.

The document is electronically signed by Sikt - Norwegian Agency for Shared Services
in Education and Research. The document is only valid in its original electronic form
with the accompanying electronic signature. Time for signing document 2024-09-27 13:02

General information about the degree

Bachelor in Cyber Security is awarded in accordance with the Regulations on Degrees and Titles Protected by Law of 16 December 2005 (No. 1574). The length of study for the degree is 3 years and it comprises 180 ECTS credits. One year of study comprises 60 ECTS credits.Bachelor in Cyber Security is a qualification that is part of first cycle/level 6 in the Norwegian Qualifications Framework for Lifelong Learning, approved by the Ministry of Education and Research on 8.11.2017.{VTM-MRK-SIDE3}

The student to successfully complete the course has achieved the following Learning Outcomes:

Knowledge

An understanding of theories, facts, principles, procedures in the subject area of Cyber Security

K1 Has a broad knowledge of cyber defence and attack techniques, technologies and tools in order to implement appropriate technical and non-technical solutions to prepare for, defend against, and recover from cyber intrusion

K2 Is familiar with appropriate and current procedures and standards for managing cyber risks and threats, undertaking penetration testing and ensuring network security

K3 Has knowledge of the legal and ethical issues and responsibilities pertaining to cyber security activities with regard to the impact of the cyber intrusion on society, industry, national infrastructure and national security

K4 Is familiar with current and emerging research and development in the field of cyber security and related disciplines

K5 Is able to update their knowledge in the area of cyber security through academic study, research and professional development

K6 Is familiar with the current and developing state of cyber criminality and cyber warfare threats, vulnerabilities and defensive tools and techniques

K7 Has knowledge of the history and development of cyber security, cybercrime and cyber warfare, its impact on safety and security of digital environments and infrastructures, alongside the resulting effects on society

K8 Is familiar with various computational tools, techniques and practices that underpin secure computing

Skills

The ability to utilise knowledge to solve problems or tasks (cognitive, practical, creative and communication skills)

S1 Is able to critically assess the threat level to a digital environment and select and apply appropriate computer system security and penetration tools and techniques in order to secure a computer network

S2 Can critically select and apply a range of analytical and methodological problem solving and investigative techniques including system profiling and vulnerability analysis, based on research and to be able to interpret the solutions and present results appropriately

S3 Is able to reflect on their own academic practice and development as a security professional, identify areas for improvement and adapt to future cyber security tools, techniques, technology and threats

S4 Is able to find, distil and evaluate relevant academic, commercial and non-commercial information assets then apply this information in resolving digital security problems

S5 Is able to identify stakeholders of cyber security and defence-related issues and communicate, network and collaborate with these stakeholders according to their individual requirements

S6 Can apply mathematical and software development theories, tools and techniques to computational challenges

General Competence

The ability to utilise knowledge and skills in an independent manner in different situations

G1 Is able to identify and appropriately act on complex ethical and social issues arising within academic and professional practice as a cyber security professional, whilst being aware of the greater implications of their actions and decisions

G2 Is able to plan, execute and manage a variety of activities and cyber security-related projects over time, alone or as part of a collaborative team to successful conclusion and in accordance with relevant legal and ethical requirements and principles

G3 Can distil and communicate cyber security-related theories, concepts, problems and solutions, with a variety of relevant stakeholders, through the selection and application of appropriate methods of communication

G4 Can exchange opinions, experiences and ideas with others with background and/or experience in cyber security and defence, through the selection and application of appropriate methods of communication, thereby contributing to the development of good practice within the cyber security community of practice

G5 Is familiar with, and can critically evaluate, current and evolving processes and disruptive technologies within the field of cyber security

G6 Is able to identify appropriate stakeholders and communicate, network and collaborate with these stakeholders at an appropriate level while considering security and confidentiality

G7 Is able to engage in critical self-reflection, and reflect upon relevant ethical and professional issues, as part of the lifelong learning strategy required of a cyber security professional

Noroff School of Technology and Digital Media

Transcript of Records

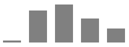
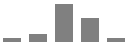
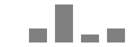
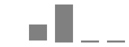
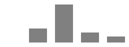
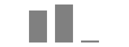
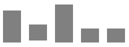
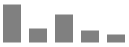
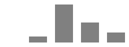
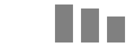
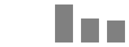
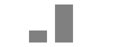
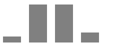
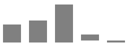
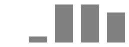
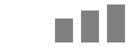
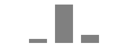
Name: **Szmandra, Tamas**

Date of birth: 1980-12-27

Degree: Bachelor in Cyber Security

Received: 2024-08-21

Study programme: Bachelor in Cyber Security

Course		Semester	Credits	Grade	Grade[1] distribution A B C D E
Compulsary Courses					
	Network and IT Security (Noroff School of technology and digital media)	2021 spring	25	Recognized	
UC3BCS20	Bachelor Project	2023 autumn	20	D	
	- Thesis and Artefact	2023 autumn		D	
Electives					
UC3IRF05	Incident Response Fundamentals	2024 spring	5	E	
UC3OIN05	Open-Source Intelligence	2024 spring	5	D	
UC3RMA05	Risk Management	2024 spring	5	C	
UC1DMA10	Discrete Mathematics	2021 autumn	10	C	
UC1PBL05	Problem Based Learning and Research Methodologies	2021 autumn	5	B	
UC1PR110	Programming 1-Introduction to Programming	2021 autumn	10	E	
UC1PR210	Programming 2-Programming and Databases	2022 spring	10	A	
UC2NSE10	Network Security	2022 autumn	10	E	
UC2OPS10	Operating Systems	2022 autumn	10	C	
UC2PEN10	Penetration Testing Practice and Procedure	2022 autumn	10	C	
UC2ISM10	Information Security Management	2023 spring	10	C	
UC2ST210	Studio 2	2023 spring	10	B	
UC2WAR10	Criminality and Warfare in the Digitial Domain	2023 spring	10	D	
UC3CNA10	Computer Network Attack	2023 autumn	10	E	
UC3CND10	Computer Network Defence	2023 autumn	10	D	
UC3VUL05	Vulnerabilities	2024 spring	5	C	
			Total: 180.0		

[1] For an explanation of the grade distribution, see the last page.

Noroff School of Technology and Digital Media

Transcript of Records

Name: **Szmandra, Tamas**
Date of birth: 1980-12-27
Degree: Bachelor in Cyber Security
Received: 2024-08-21
Study programme: Bachelor in Cyber Security

Credit system and grading

The academic year normally runs from mid-August to mid-June and lasts for 10 months. Courses are measured in "studiepoeng", considered equivalent to the European Credit Transfer System standard (ECTS credits). The full-time workload for one academic year is 1500 - 1800 hours of study / 60 "studiepoeng".

The Norwegian grading system consists of two grading scales: one scale with the grades pass or fail and one graded scale from A to E for pass and F for fail. The graded scale has the following qualitative descriptions:

A	Excellent	An excellent performance, clearly outstanding. The candidate demonstrates excellent judgement and a very high degree of independent thinking.
B	Very good	A very good performance. The candidate demonstrates sound judgement and a high degree of independent thinking.
C	Good	A good performance in most areas. The candidate demonstrates a reasonable degree of judgement and independent thinking in the most important areas.
D	Satisfactory	A satisfactory performance, but with significant shortcomings. The candidate demonstrates a limited degree of judgement and independent thinking.
E	Sufficient	A performance that meets the minimum criteria, but no more. The candidate demonstrates a very limited degree of judgement and independent thinking.
F	Fail	A performance that does not meet the minimum academic criteria. The candidate demonstrates an absence of both judgement and independent thinking.

The assessment is criterion referenced.

Grade distribution

The distribution of grades is shown by the percentage for courses using the graded scale A – F. Fail (F) is not included in the distribution. All results from the last five years are included in the calculation. The distribution is also shown for courses that have been active for less than five years. There has to be at least 10 approved results during the period.