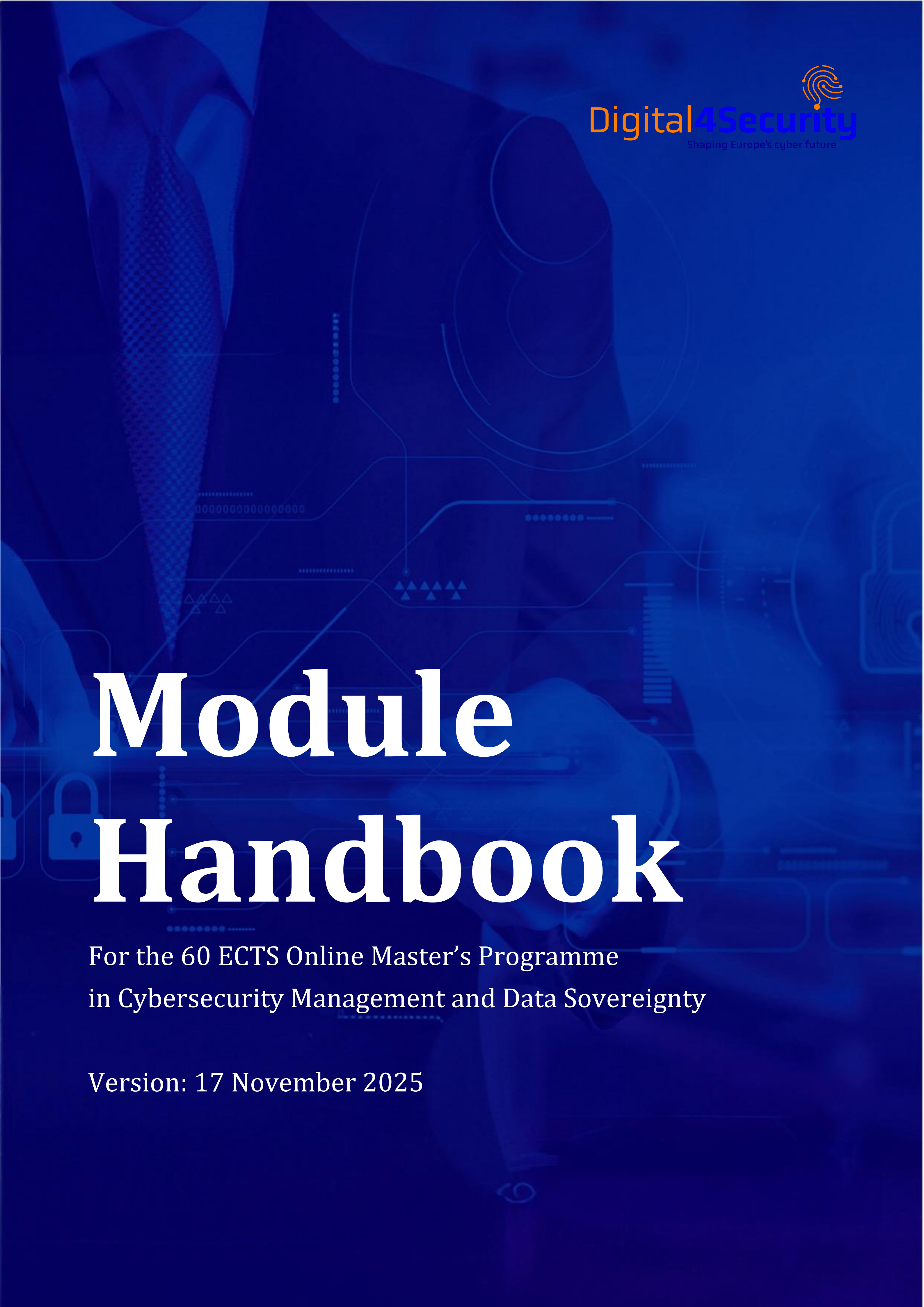


Digital4Security

Shaping Europe's cyber future

Module Handbook

For the 60 ECTS Online Master's Programme
in Cybersecurity Management and Data Sovereignty

Version: 17 November 2025

Table of Contents

Overview and Introduction to Digital4Security

Welcome to the Module Handbook for the 60 ECTS Online Master's Programme in Cybersecurity Management and Data Sovereignty, with the joint degree awarded by the German University of Digital Science (UDS, Germany), Munster Technological University (MTU, Ireland), and Universidad Internacional de La Rioja (UNIR, Spain).

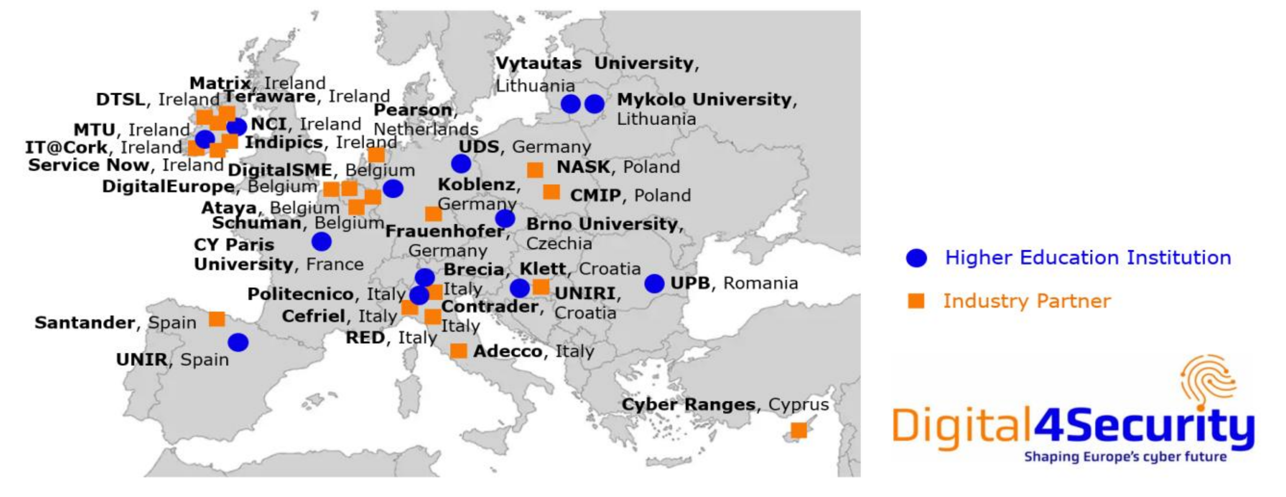
Beyond the academic environment provided by the three degree-awarding institutions, students also benefit from access to a broad European network of cybersecurity excellence established through the EU co-funded **Digital4Security** initiative. While the awarding institutions are responsible for overseeing teaching, assessing the attainment of learning outcomes, and conferring degrees, the master's programme is firmly embedded within a wider ecosystem of universities and industry stakeholders dedicated to advancing cybersecurity education and workforce development across Europe.

This 60 ECTS Online Master's Programme builds on extensive groundwork, vision, and cross-sectoral cooperation in the Digital4Security project. The initiative brings together academic and industry partners to deliver innovative, effective, and sustainable education aimed at developing high-level cybersecurity talent, particularly at the master's level, to meet the pressing needs of European Small and Medium-sized Enterprises (SMEs) and other organizations. The shared goal is to strengthen Europe's cyber resilience and safeguard economic stability in the digital age.

As part of this mission, Digital4Security has developed and continues to share a suite of resources with project partners, including insights into European business needs in cybersecurity, train-the-trainer materials for state-of-the-art course delivery, shared D4S branding, internship opportunities for students, access to industry certification, weekend-lectures and events, as well as a European staff network of cybersecurity experts.

Figure 1 illustrates the partners involved in the Digital4Security project. Students gain access to this network of cybersecurity excellence upon enrolling in the master's programme.

Figure 1: Digital4Security Partner Network.



A systematic overview of the Digital4Security partners is provided in Table 1.

Table 1: The Digital4Security Network – Higher Education Institutions (HEIs) and Associate Partners (Listed Alphabetically)

No.	Partner	Abbreviation	Country	Role
1	Adecco Formazione SRL	ADECCO TRAINING	Italy	Associate partner
2	Adecco Italia Holding di Partecipazione e Servizi SPA	ADECCO GROUP	Italy	Associate partner
3	Adecco Italia	ADECCO ITALIA	Italy	Associate partner
4	Ataya & Partners	ATAYA	Belgium	Associate partner
5	Banco Santander SA	BANCO SANTANDER	Spain	Associate partner
6	Brno University of Technology	BRNO	Czech Republic	HEI partner

No.	Partner	Abbreviation	Country	Role
7	Cefriel Società Consortile a Responsabilità Limitata Società Benefit	CEFRIEL	Italy	Associate partner
8	CMIP (Polski Klaster Cyberbezpieczenstwa CyberMadeInPoland Sp. z o. o.)	CMIP	Poland	Associate partner
9	Contrader SRL	CONTRADER	Italy	Associate partner
10	CY Cergy Paris Université	CY	France	HEI partner
11	Cyber Ranges Ltd	CYBER RANGES	Cyprus	Associate partner
12	DigitalEurope AISBL	DIGITALEUROPE	Belgium	Associate partner
13	Digital Technology Skills Limited	DTSL	Ireland	Associate partner
14	European Digital SME Alliance	DIGITAL SME	Belgium	Associate partner
15	Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung EV	FHG	Germany	Associate partner
16	German University of Digital Science	UDS	Germany	HEI partner
17	Independent Pictures Limited	INDIEPICS	Ireland	Associate partner
18	IT@Cork Association Limited LBG	IT@CORK	Ireland	Associate partner
19	Matrix Internet Applications Limited	MATRIX	Ireland	Associate partner
20	Munster Technological University	MTU	Ireland	HEI partner
21	Mykolo Romerio Universitetas	MRU	Lithuania	HEI partner
22	National College of Ireland	NCI	Ireland	HEI partner
23	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	NASK	Poland	Associate partner
24	Pearson Benelux	PEARSON B.	Netherlands	Associate partner
25	Politecnico di Milano	POLIMI	Italy	HEI partner
26	Profil Klett d.o.o.	PROFIL KLETT	Croatia	Associate partner
27	Red Open S.R.L.	RED OPEN S.R.L.	Italy	Associate partner
28	Schuman Associates SCRL	SA	Belgium	Associate partner

No.	Partner	Abbreviation	Country	Role
29	ServiceNow Ireland Limited	ServiceNow	Ireland	Associate partner
30	Skillnet Ireland Company Limited By Guarantee	SKILLNET	Ireland	Associate partner
31	Terawe Technologies Limited	TERAWE	Ireland	Associate partner
32	Universidad Internacional de La Rioja	UNIR	Spain	HEI partner
33	Università degli Studi di Brescia	UNIBS	Italy	HEI partner
34	Universitatea Națională de Știință și Tehnologie Politehnica București	UPB	Romania	HEI partner
35	Universität Koblenz	UNI KO	Germany	HEI partner
36	University of Rijeka	UNIRI	Croatia	HEI partner
37	Vytautas Magnus University	VMU	Lithuania	HEI partner

Educational Philosophy and Design

At the core of the Master's Programme in Cybersecurity Management and Data Sovereignty lies a competency-based educational model that integrates high academic standards with practical, industry-relevant skills. The programme is built on a comprehensive needs analysis reflecting the evolving demands of the European cybersecurity landscape and is designed to equip graduates with both a strong theoretical foundation and the job-ready competencies required to excel in applied fields.

Emphasising real-world applicability, the curriculum combines academic insight with contributions from industry to accelerate graduate employability and professional impact. The programme also embodies a spirit of pan-European collaboration, bringing together leading cybersecurity expertise from across the European continent. By actively engaging with diverse academic institutions and industry partners, it creates a rich and diverse learning environment, empowering students to thrive both intellectually and professionally.

Diversity and Inclusivity

Recognising the diverse needs of our student community, the 60 ECTS online master's programme has been carefully designed to provide a flexible, modular learning experience that is accessible to individuals from a wide range of sectors and professional backgrounds. This commitment to inclusivity is evident in the delivery model, which combines fully online modules with a varied set of complementary activities, including hybrid weekend workshops, networking opportunities, and options for on-site engagement across key European cybersecurity hubs.

The programme seeks to make advanced digital education both accessible and affordable to the widest possible audience. It actively promotes gender equality, ethnic diversity, and participation of underrepresented groups. At the same time, it also supports professionals who are already well established – for example, business leaders – who now wish to enhance their expertise in cybersecurity.

Programme Structure

The master's programme comprises **60 ECTS** in total, combining core study, elective opportunities, and a final thesis project. This structure provides both academic rigour and flexibility, enabling students to pursue individual interests and professional goals.

Mandatory Taught Modules (15 ECTS)

All students complete three mandatory taught modules (5 ECTS each), with one delivered by each of the degree-awarding universities. This ensures that every student benefits from the distinctive expertise of the partner institutions, and that all graduates will have studied at each university co-signing the joint degree.

- Communication Design for Cybersecurity – UDS
- Business Resilience, Incident Management, and Threat Response – MTU

- Ethical Hacking and Penetration Testing – UNIR

Together, these modules cover the programme's three overarching content areas: management, business resilience, and cybersecurity technology. They provide a common foundation that underpins further study and specialisation within the master's programme.

Elective Modules (30 ECTS)

Students tailor their learning through elective modules, selecting a total of 30 ECTS.

- **Profile-specific electives (20 ECTS):** Students may choose modules aligned with a professional profile. Completing at least 20 ECTS from the recommended modules within a profile is required for a formal recognition of that specialisation in the Diploma Supplement.
- **Free electives (10 ECTS):** Students may choose any available modules.

Choosing a professional profile is optional; students may instead combine electives freely across the 30 ECTS. However, selecting a profile is strongly recommended, as it facilitates tailored career preparation.

Procedures for selecting or changing professional profiles are outlined in the *Student Handbook* (Annex 8).

Additionally, micro-credentials may be recognised in place of elective modules within the programme. In practice, students may replace one 5 ECTS elective module through micro-credential recognition. This is governed by the *Study and Examination Regulations* (Annex 2), with further procedural guidance offered in the *Student Handbook* (Annex 8).

Master's Thesis (15 ECTS)

The programme concludes with the Master's thesis, an independent research or applied project through which students demonstrate their ability to integrate knowledge, address complex challenges, and contribute original insights to the field of cybersecurity management and data sovereignty.

For students who focus on a particular professional profile, completing the thesis on a topic aligned with that profile forms an integral part of their professional preparation.

The Master's thesis is a mandatory component of the programme. Its procedures are set out in detail in the *Study and Examination Regulations* (Annex 2).

Professional Profiles

Designed to equip students with the professional skills needed to fill critical roles in cybersecurity management and data sovereignty, this master's programme offers six distinct professional profiles, each featuring a curated selection of recommended modules.

- **Chief Information Security Officer (CISO)** – Focused on strategic leadership and management of an organisation's cybersecurity approach (curated by UDS).
- **Cybersecurity Educator** – Teaching and promoting cybersecurity awareness and best practices within organisations (curated by UDS).
- **Cyber Legal, Policy, and Compliance Officer** – Concentrating on the legal and regulatory aspects of cybersecurity, ensuring compliance with relevant laws and policies (curated by MTU).
- **Cybersecurity Risk Manager** – Dedicated to identifying, assessing, and mitigating risks to information security (curated by MTU).

- **Cyber Threat Intelligence Specialist** – Gathering and analysing threat intelligence to inform defensive strategies (curated by UNIR).
- **Cybersecurity Auditor** – Focused on evaluating and improving an organisation's cybersecurity policies, practices, and controls (curated by UNIR).

Each professional profile is linked to a set of recommended modules. Students who complete at least 20 ECTS from these recommendations, and write their thesis on a profile-aligned topic, will receive formal recognition of their profile preparation in the Diploma Supplement.

The profiles are aligned with the European Cybersecurity Skills Framework (ECSF), which defines typical cybersecurity professional roles, including their titles, missions, tasks, skills, knowledge, and competencies. More information about these profiles is available on the **ECSF** website.

An overview of the modules recommended per profile is provided in Table 2.

Table 2: Recommended Elective Modules per Professional Profile

Module	CISO	Educator	Cyber Legal	Risk Manager	Threat Intellig.	Auditor
AI & Emerging Topics in Cybersecurity	X	X	X	X		
Malware Analysis					X	
Cybersecurity Culture, Strategy & Leadership	X	X				
Enterprise Architecture, Infrastructure Design and Cloud Computing					X	
Law, Compliance, Governance, Policy, and Ethics	X	X	X	X		X
Research Methods		X				
Security Operations				X	X	X
Technological Foundations for CS & Security Controls				X	X	
Automation of Security Tasks and Data Analytics					X	
CISO and Crisis Communication	X					
Risk Management of Cyber-Physical Systems	X			X		X
Cybersecurity Auditing			X			X
Cybersecurity Economics & Supply Chain	X			X		
Cybersecurity Education & Training Delivery I		X				
Cybersecurity Education & Training Delivery II		X				
Cybersecurity in Industry - Security of OT & CPS						
Cybersecurity Law & Data Sovereignty			X			X
Machine and Deep Learning in Cybersecurity						
Digital Forensics, Chain of Custody and eDiscovery			X			X
Threat Intelligence					X	

Module Descriptors

The *Study and Examination Regulations* (Annex 2) specify the module descriptors, which are key elements of information required for each module. Typically, this information is provided for every module individually. However, for aspects that are uniform across the programme, a central specification is provided:

- **Language of Instruction:** English;
- **Examination Requirements:** To pass a module, students must achieve at least 60% of the total available points.

The interpretation of performance, including grade classification, is set out in the *Study and Examination Regulations* (Annex 2) and applies uniformly across all modules, and for overall programme performance.

Furthermore, the Module Handbook specifies the **Term of Delivery** for mandatory modules only, as these are scheduled consistently to ensure a coherent learning progression across cohorts. For elective modules, the term of delivery is not fixed in the Handbook. Instead, the Master's Board determines which elective options are offered when, providing students with due advance notice of typically one year. The overall availability of modules and professional profiles is governed by the *Study and Examination Regulations* (Annex 2).

For all modules, contact details are provided for the responsible individuals – where appropriate, covering both the delivering partner and the Module Guarantor separately. These details are included in the *Section "Contacts"* and are made available internally for enrolled students and staff only.

Module Guarantor Accountability

In recognition of their overall accountability for the master's programme, one of the degree-awarding partner universities assumes responsibility for each module.

This applies also to modules delivered by supporting partner institutions, particularly from the Digital4Security academic network.

The responsibilities of the Module Guarantor institution include:

- Ensuring the module aligns with the overall Programme's learning outcomes;
- Ensuring that module content and planned assessments are appropriate for delivering and evaluating the module's learning outcomes;
- Reviewing and approving learning materials and assessments;
- Monitoring instructional quality and delivery;
- Serving as an additional point of contact for academic and administrative matters related to the module;
- Providing backup teaching capacity in case the delivering partner becomes unavailable or cannot fulfil their responsibilities.

Table 3 provides an overview of the modules included in this Handbook. Partner abbreviations are explained in Table 1. In addition, the table indicates professional profiles, showing which elective modules are recommended for particular career pathways, using the following abbreviations:

- Chief Information Security Officer: CISO
- Cybersecurity Educator: Educator
- Cyber Legal, Policy, and Compliance Officer: Cyber Legal
- Cybersecurity Risk Manager: Risk Manager
- Cyber Threat Intelligence Specialist: Threat Intelligence
- Cybersecurity Auditor: Auditor.

Table 3: Overview of Modules Included in this Handbook, along with Programme Relation and Partners Involved

No.	Module	ECTS	Programme Relation	Delivering Partner	Module Guarantor
1	Communication Design for Cybersecurity	5	Mandatory	UDS	UDS
2	Business Resilience, Incident Management & Threat Response	5	Mandatory	MTU	MTU
3	Ethical Hacking & Penetration Testing	5	Mandatory	UNIR	UNIR
4	AI & Emerging Topics in Cybersecurity	5	Elective - recommended for CISO, Educator, Cyber Legal, Risk Manager	UDS	UDS
5	Malware Analysis	5	Elective - recommended for Threat Intelligence	UNIR	UNIR
6	Cybersecurity Culture, Strategy & Leadership	5	Elective - recommended for CISO, Educator	VMU/ ATAYA	UDS
7	Enterprise Architecture, Infrastructure Design and Cloud Computing	5	Elective - recommended for Threat Intelligence	UPB	MTU
8	Law, Compliance, Governance, Policy, and Ethics	5	Elective - recommended for CISO, Educator, Cyber Legal, Risk Manager, Auditor	UNIBS	MTU
9	Research Methods	5	Elective - recommended for Educator	UNI KO	UDS
10	Security Operations	5	Elective - recommended for Risk Manager, Threat Intelligence, Auditor	CY CERGY	UNIR
11	Technological Foundations for CS & Security Controls	5	Elective - recommended for Risk Manager, Threat Intelligence	UPB	UNIR
12	Automation of Security Tasks and Data Analytics	5	Elective - recommended for Threat Intelligence	UNIRI	UNIR
13	CISO and Crisis Communication	5	Elective - recommended for CISO	VMU/ ATAYA	UDS

No.	Module	ECTS	Programme Relation	Delivering Partner	Module Guarantor
14	Risk Management of Cyber-Physical Systems	5	Elective - recommended for CISO, Risk Manager, Auditor	POLIMI/ CEFRIEL	MTU
15	Cybersecurity Auditing	5	Elective - recommended for Cyber Legal, Auditor	VMU/ ATAYA	UNIR
16	Cybersecurity Economics & Supply Chain	5	Elective - recommended for CISO, Risk Manager	MRU	UDS
17	Cybersecurity Education & Training Delivery I	5	Elective - recommended for Educator	BUT	UDS
18	Cybersecurity Education & Training Delivery II	5	Elective - recommended for Educator	UPB	UDS
19	Cybersecurity in Industry - Security of OT & CPS	5	Free Elective	POLIMI	MTU
20	Cybersecurity Law & Data Sovereignty	5	Elective - recommended for Cyber Legal, Auditor	BUT	MTU
21	Machine and Deep Learning in Cybersecurity	5	Free Elective	UNIRI	UNIR
22	Digital Forensics, Chain of Custody and eDiscovery	5	Elective - recommended for Cyber Legal, Auditor	UPB	UNIR
23	Threat Intelligence	5	Elective - recommended for Threat Intelligence	UPB	UNIR
24	Thesis	15	Mandatory	UNI KO	UDS

Fixed and Adjustable Elements in the Modules

The central element of each module description is the list of *learning outcomes*. Regardless of who teaches the module, or in which term it is delivered, students can consistently expect to develop the defined areas of knowledge, skills, and competencies.

Moreover, the ECTS assigned to each module and the corresponding workload expectations are fixed. One ECTS credit corresponds to approximately 25 hours of work, encompassing live participation in sessions, individual study (including lecture viewing, reading, and assignments), group projects, and exam preparation. Further guidance on ECTS and workload is provided in the *Student Handbook* (Annex 8).

Each module is structured as a 12-week plan, providing a general overview of the topics covered and their approximate timing. Lecturers may make limited updates to the content – for example, by incorporating emerging developments in cybersecurity that take precedence over previously planned deep-dives in a given week. However, such changes must remain proportionate and, importantly, continue to support students in achieving the module's intended learning outcomes as defined in this handbook.

More systematic changes are governed by the *Internal Quality Handbook* (Annex 4), with final decisions on updates to the Module Handbook made by the Master's Board. All adjustments occur within carefully defined bounds: always respecting the learning outcomes, ECTS, and assessment requirements of each module, while continually seeking to enhance the teaching provision, so as to support students in achieving the intended learning outcomes. The rationale for this approach – recognising that core elements of the curriculum are fixed and can only be altered through programme re-accreditation – is explained in detail in the *Student Handbook* (Annex 8).

Course lecturers may change over time, provided that the required standards of teaching excellence are maintained. Lecturer requirements are defined in the *Study and Examination Regulations* (Annex 2), including subject-matter expertise, professional rank, English proficiency, and pedagogical standards.

Changes to the accountable institution for a module (the Module Guarantor) may only be made through formal updates to the *Module Handbook*, as approved by the Master's Board of Directors.

Microcredentials

Modules that form part of this Master's programme may also be offered and certified as microcredentials. This means that the participant group in a module may be mixed, comprising students already enrolled in the full Master's programme and learners admitted only to a single module as a microcredential. Microcredentials allow prospective students to test the programme prior to full enrolment. They also provide working professionals with targeted upskilling opportunities without committing to a full Master's. Where a learner subsequently applies for admission to the Master's programme, one module successfully completed as a microcredential can be recognised as prior learning, in accordance with the *Study and Examination Regulations* (Annex 2).

Modules

Communication Design for Cybersecurity

Module designation	*Communication Design for Cybersecurity*
Term(s) in which the module is taught	Spring, Autumn
Institution(s) involved	UDS
Relation to curriculum	Mandatory
Teaching methods	The teaching and learning strategy for this module will consist of interactive classes and structured online activities, including videos, tutorials, case studies, and discussions. Each week, learners will engage with 2 hours of directed online activities, introducing key concepts related to the weekly topic. Further activities will focus on concise, engaging content such as explanatory videos, case illustrations, readings, and guided tutorials. Learners will work on tasks and exercises related to the weekly content, ensuring they can apply theoretical principles to real-world cybersecurity challenges. Live sessions will emphasize hands-on learning, integrating students' interests - such as specific scenarios or business cases - with the instructor's expertise through interactive discussions, practical demonstrations, and collaborative problem-solving. To support independent learning, lecture and tutorial materials will be provided, supplemented with links to external resources such as cybersecurity communication frameworks, documentation, case studies, and industry-relevant tools. Learners will also receive mentoring and formative feedback on their completed activities to refine their understanding and improve practical skills.
Workload (incl. contact hours, self-study hours)	• *Approximate Total workload: 125 hours* • *Contact hours / Directed e-Learning Activities: 24 hours* • *Project Work: 48 hours* • *Private study including examination preparation: 53 hours*

Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*N/A*
Module summary	Effective cybersecurity is not just about technology – it's about communication. This module equips learners with the knowledge, skills, and competencies to bridge the gap between technology and human behaviour. Integrating insights from psychology, communication theory, design, and cybersecurity, students learn to translate complex security concepts for diverse audiences, while countering manipulation tactics used by attackers. The course covers communication frameworks, cognitive biases, design methodologies, and stakeholder engagement techniques, alongside case studies on phishing, social engineering, and crisis response. Participants refine their ability to craft clear and actionable security messages using approaches such as legal design thinking, multimodal communication, and real-time security monitoring. Hands-on exercises include presenting cybersecurity strategies to executives, honing both presentation skills and the ability to argue effectively in complex leadership and management debates. Advanced techniques such as motivational interviewing, cognitive reframing and design thinking help participants not only convey their messages effectively, but also extract key insights from stakeholders to improve security practices. Additionally, the course explores how communication strategies can drive cybersecurity innovation in an organization, and participants examine the role of design in fostering cybersecurity awareness. By the end of the module, participants will be able to design impactful cybersecurity communication, combat misinformation, and cultivate a security-conscious culture within and beyond their organizations.
Module objectives/intended learning outcomes	This module conveys key knowledge, skills, and competencies in cybersecurity communication, at EQF Level 7 (master's). **Knowledge:** Demonstrate specialised knowledge of cybersecurity communication strategies, integrating insights from psychology, communication theory, design, and cybersecurity for enhanced cybersecurity solutions. **Skills:** Design and implement advanced cybersecurity communication strategies, effectively translating complex security concepts for

	diverse stakeholders, while mitigating attackers' manipulation tactics. **Competence:** Manage and transform organisational cybersecurity communication practices, taking responsibility for strategic improvements and professional knowledge development. In further detail, the course covers the following Learning Outcomes. ***LO1: Specialized Knowledge in Cybersecurity Communication:*** *Demonstrate well-developed knowledge of communication theories, frameworks, and design techniques to effectively address cybersecurity challenges and enhance stakeholder engagement.* ***LO2: Designing Advanced Communication Strategies:*** *Develop and implement advanced communication strategies that bridge the gap between technical cybersecurity concepts and human behaviour.* ***LO3: Critical Analysis of, and Response to, Cybersecurity Communication Barriers:*** *Critically evaluate the reasons for cybersecurity reluctance in an organization; analyse psychological tactics used by cyber attackers to manipulate behaviour; devise organizational counter-strategies to strengthen cybersecurity resilience.* ***LO4: Strategic Leadership in Cybersecurity Communication:*** *Demonstrate leadership and manage organizational cybersecurity communication, prioritizing critical messages, aligning with business objectives, and developing strategies to engage employees, executives, and external stakeholders.* ***LO5: Innovation in Cybersecurity Communication:*** *Develop novel cybersecurity communication solutions by identifying needs and opportunities at the intersection of technology and psychology; explore a broad range of possibilities, including innovative approaches such as implication design methods and multimodal cybersecurity data displays.* ***LO6: Communication for Cybersecurity Innovation*** *Leverage communication strategies, such as those from design thinking, to facilitate and drive cybersecurity innovation within organizations; support the community in understanding security challenges and developing effective solutions through clear, strategic, and collaborative communication.*
Content	**Week 1: Introduction to Implication Design**

	• **Overview:** Communication in cybersecurity goes beyond just text messages. This week explores the broad scope of cybersecurity communication, emphasizing the crucial role that communication *design* plays in crafting effective messages. • **Definition** of Communication • **Implication Design Concept:** Using design elements to raise awareness and foster intuitive user behaviour that is security-aware. • **Case Studies:** ○ Eyecam and its implications on privacy perception. ○ Alias for enhanced control over smart assistants. • **Ethics in Cybersecurity Communication:** Prioritizing security empowerment rather than manipulation, fostering trust, responsible behaviour, and compliance. • **Preparation:** Understanding the course structure and grading; comprehension of implication design principles. **Week 2: Anticipation & Implication Design Workshop** • **Overview:** Building on the previous introduction to implication design, this week introduces tools for anticipating future risks and benefits in cybersecurity. Focus is placed on proactive approaches to risk mitigation through implication design. • **Anticipation Tools** ○ Future Cone ○ Needs-Based Outcome Assessment (NOA) ○ Tarot Cards of Tech (TCT) • **Workshop:** Using forecasting tools (TCT, NOA) to identify likely cybersecurity pitfalls in an organisation and create proactive redesigns using implication design methods. **Week 3: Communication Frameworks** • **Overview:** Why communication is crucial in cybersecurity leadership. • **Case Example:** Colonial Pipeline Cyberattack • **Stakeholder Mapping:** Identifying different cybersecurity audiences (including executives, IT teams, employees, regulators, customers, business partners). • **Communication Models and their Application in Cybersecurity Communications:** Shannon & Weaver's Transmission Model, Schulz von Thun's Quadrat-Modell, Reeves & Nass's Media Equation, McKim's Perceive-Imagine-Express Model and Internal vs. External Communication, Grice's Maxims of Communication, Watzlawick's Pragmatics of Communication,

Lazarus' Protection Motivation Theory, Sweller's Cognitive Load Theory, Cialdini's Principles of Persuasion.

- **Hands-On:** Stakeholder-specific communication exercises using different models.

Week 4: Malicious Cybersecurity Communication

- **Overview:** How attackers use communication maliciously to exploit human psychology and system vulnerabilities.
- **Communication Barriers & Cognitive Biases:** Why and when people ignore security risks; strategies for raising awareness and prompting action.
- **Identifying Malicious Communication Techniques that Exploit Human Biases:** Authority Bias, Bandwagon Effect, Scarcity & Urgency Bias, Reciprocity Bias, Cognitive Load / Decision Fatigue, Default / Status Quo Bias, Overconfidence Bias, Consistency Bias, Dunning-Kruger Effect, Availability Heuristic, Halo Effect, Unfinished Task Bias.
- **Hands-On:** Analysing phishing attempts, social engineering attacks, and deepfake scams; crafting counter-strategies.

Week 5: Media in Cybersecurity Communication

- **Overview:** This week explores cybersecurity communication across diverse media – from language to visuals, sounds, and other sensory channels.
- **Semantic Domain:**
  - Using *Legal Design Thinking* to inspire clear, user-friendly communication
  - Applying *Argumentation Techniques* to craft logically structured and strategically persuasive messages, identify common fallacies, and engage in cybersecurity debates.
- **Multimodal Design:**
  - *Artistic & Functional Data Displays*
  - *Sonification:* Using sound to signal real-time cybersecurity states and anomalies.
  - *Data Visualization:* Creating artistic 2D/3D displays that reflect live security metrics.
  - *Pioneering Data Displays:* Exploring smell and taste for cybersecurity communication.
- **Hands-On:** Design and test various communication assets – from simple alerts to structured arguments – and evaluate their impact.

Week 6: Advanced Communication for Cybersecurity Professionals

- **Overview:** Cybersecurity leaders need to communicate with impact – especially when facing skepticism or resistance. This week focuses on persuasive, psychologically attuned strategies for engaging executives and employees alike.
- **Psychological Techniques:**
  - *Validation:* Acknowledge concerns (cost, friction) to reduce defensiveness.
  - *Motivational Interviewing:* Use open-ended questions and reflective listening to foster change.
  - *Cognitive Reframing:* Shift security from a burden to a value-add.
  - *Storytelling & Narrative Framing:* Make cybersecurity relatable and identity-driven.
- **Case Study:** Overcoming the "We've Never Had a Breach" mindset.
- **Hands-On:** Practice live interactions using validation, reframing, and conflict de-escalation techniques; develop and deliver a board-level cybersecurity strategy presentation.

Week 7: Communication Strategies for Navigating Problem Spaces

- **Overview:** Problem solving involves two phases: (1) exploring problem spaces and (2) exploring solution spaces. The first focuses on identifying key problems and defining criteria for good solutions; the second on finding and evaluating solutions. This week covers approaches for navigating problem spaces, highlighting the critical role of communication.
- **Key Concepts:**
  - *Problem-Solving Process:* From Problem to Solution Space
  - *Question Taxonomy*
  - *Mastering Abstraction*
  - *Problem Statements,* including Personas, Point-of-View Madlibs, Want Ads and How Might We (HMW) Questions – Focussing problem solving efforts and inspiring solutions.
- **Tools for Problem Definition & Mapping:**
  - Five Whys & Root Cause Analysis – Identifying the core issue behind security vulnerabilities.
  - JEA's Random Attack and Problem Restatement Framework – Reframing security challenges to map out the problem space and explore hidden opportunities
- **Hands-On:**

	○ *Laddering in Abstraction on Problem Statements:* Moving between broad and specific problem scopes to explore innovative cybersecurity solutions. ○ *Crafting 'How Might We' Questions:* Transforming initial cybersecurity problem statements into more generative and actionable innovation prompts. ○ *Cybersecurity Challenge Reframing:* Participants work in teams to reformulate a given cybersecurity challenge of an organization using problem-reframing techniques. **Week 8: Communication Strategies for Navigating Solution Spaces** • **Overview:** Communication is essential in navigating both problem and solution spaces in innovation processes, though the tools and approaches differ. In solution spaces, the toolkit and mindset shift depending on whether teams are exploring opportunities and producing solutions, or evaluating them. • **Communication Strategy Shifts:** During idea generation, open and inclusive communication encourages all suggestions without judgment, fostering creativity and diverse ideas. Only afterward does the team transition to rigorous evaluation, aiming to identify the most promising options. • **Methodologies:** ○ *Alex Osborn's Brainstorming:* Core principles that guide communication during brainstorming include "defer judgment," "encourage wild ideas," and "aim for quantity." ○ *William Gordon's Method of Operational Creativity:* The session leader introduces the cybersecurity challenge in abstract terms, allowing teams to generate a broad set of solution approaches without knowing the specifics. Later, teams narrow down to address the concrete problem to be solved. • **Hands-on:** ○ Yes-And Exercise ○ Problem Solving Session using Alex Osborn's Brainstorming: Teams tackle a cybersecurity issue following Osborn's communication mottos. ○ Problem Solving Session using William Gordon's Operational Creativity: Teams approach a cybersecurity challenge by first exploring general options before focusing on the specific issue to be addressed.

	Week 9: Design Thinking for User-Centred Cybersecurity Innovation: From Problem to Solution Spaces - **Overview:** Cybersecurity measures often fail when they overlook real user experiences. Effective communication with stakeholders is crucial to identify pain points and gather insights that drive improvements. This week applies Design Thinking to explore how cybersecurity solutions can be crafted through user-cantered communication, helping to craft measures that are user-friendly, efficient, and aligned with organizational needs. - **The Design Thinking Process:** ○ *Empathize:* Conduct stakeholder interviews to uncover pain points around cybersecurity implementation; observe workflows to identify compliance barriers. ○ *Define:* Synthesize findings into key security challenges (e.g., “Employees bypass security due to time constraints”). ○ *Ideate:* Brainstorm security solutions that accommodate stakeholder needs. ○ *Prototype:* Rapidly create low-fidelity security solution mockups. ○ *Test:* Gather user feedback, and iterate solutions. - **Hands-On:** Rapid Design Thinking Sprint, with teams tackling a cybersecurity issue using the design thinking process. **Week 10-12: Project and Exam** **Overview:** This final phase focuses on consolidating key concepts from earlier weeks. Participants will apply their knowledge in a final *Communication Design* project based on a self-chosen real-world case. Both asynchronous and synchronous formats will support feedback, questions, and collaborative problem-solving.
Exams and assessment formats	**Grading Breakdown:** - **40% Weekly Submissions**: Hands-on exercises that apply key concepts from the weekly topics. - **60% Proctored Examination**: A comprehensive evaluation consisting of: ○ **30% Written Examination**: Covering core topics from all input weeks, testing knowledge and application. ○ **30% Communication Design**: A detailed communication strategy and design for a cybersecurity business

	case, chosen by the participant, developed in partnership with an organization that verifies the student's identity. **Reassessment Strategy:** The reassessment for this module will be designed to evaluate all Learning Outcomes, ensuring that students can demonstrate a thorough understanding and application of the course material.
Reading list	The recommended reading list of this course includes publications and further resources such as: Bünzli, F., & Eppler, M. J. (2024). Spotlight on a thought leader - How to become an effective communicator: Schulz von Thun's contribution to Business Communication. *International Journal of Business Communication*, *61*(2), 484-491. Cialdini, R. B. (2009). *Influence: Science and practice* (Vol. 4, pp. 51-96). Boston: Pearson Education. Dorasamy, M., Joanis, G. C., Jiun, L. W., Jambulingam, M., Samsudin, R., & Cheng, N. J. (2019, December). Cybersecurity issues among working youths in an IoT environment: A design thinking process for solution. In *6th International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE. d.school. (2010). *Bootcamp Bootleg*. Introduction to Design Thinking Methods, Stanford University. Fogg, B. J. (1999). Persuasive technologies. *Communications of the ACM*, *42*(5), 26-29. Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018, April). "A stalker's paradise." In *Proceedings of the 2018 CHI conference on human factors in computing systems* (pp. 1-13). Grice, H. P. (1975). Logic and conversation. In Cole and Morgan (Eds.), Syntax and Semantics, Volume 3: Speech atcs (pp. 41-58). Elsevier. Lazarus, R. S. (1991). *Emotion and adaptation*. Oxford University Press.

	McKim, R. H. (1972). *Experiences in visual thinking*. Belmont, CA: Wadsworth Publishing. Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021, June). Human factors in cybersecurity: A scoping review. In *Proceedings of the 12th International Conference on Advances in Information Technology* (pp. 1-11). Reeves, B., & Nass, C. (1996). *The media equation: How people treat computers, television, and new media like real people and places*. Cambridge University Press. Shannon, C. E., & Weaver, W. (1964). *The mathematical theory of communication*. University of Illinois Press. Snow, S., Happa, J., Horrocks, N., & Glencross, M. (2020). Using design thinking to understand cyber attack surfaces of future smart grids. *Frontiers in Energy Research*, *8*, 591999. Sweller, J. (1988). Cognitive load during problem solving. *Cognitive science*, *12*(2), 257-285. Teyssier, M., Koelle, M., Strohmeier, P., Fruchard, B., & Steimle, J. (2021, May). Eyecam: Revealing relations between humans and sensing devices through an anthropomorphic webcam. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-13). Tversky, A., & Kahneman, D. (1990). Judgment under uncertainty: Heuristics and biases. Watzlawick, P., Bavelas, J. B., & Jackson, D. D. (2011). *Pragmatics of human communication: A study of interactional patterns, pathologies and paradoxes*. WW Norton & Company. Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, *32*(3), 215-257.

Business Resilience, Threat Response, and Incident Management

Module designation	*Business Resilience, Threat Response, and Incident Management*
Term(s) in which the module is taught	Winter, Autumn
Institution(s) involved	MTU
Relation to curriculum	Mandatory
Teaching methods	*The teaching and learning strategy for the Business Resilience, Threat Response, and Incident Management module will consist of classes and directed activities such as videos, tutorials, case studies and discussions on the programme's Learning Management System (LMS). Each week learners will begin by engaging with 2 hours of directed online activities aimed at introducing threshold concepts for that week's topic. Directed activities consist of short digestible pieces of content, such as explanatory videos, reading, guided tutorials, etc. Learners will then attend a live 1-hour lecture and a 1-hour tutorial session. Learners will be assigned tasks and exercises related to the directed content so that they can connect the theory to practice. Live sessions will mostly be practically based so as to make best use of the lecturer's expertise in the classroom. Learners will benefit from mentoring and formative feedback on completed directed activities during classes.* *The learning and assessment materials will be made available to learners through the programme's LMS. To support learners' independent learning the lecture notes and lab materials will be complemented by links to additional resources available on the Internet (e.g., documentation/framework tools, tutorials/videos, etc.).*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125 hours* *Directed e-Learning Activities: 24 hours* *Synchronous Lectures: 12 hours* *Tutorial Sessions: 12 hours* *Private study including examination preparation, specified in hours: 77 hours*
Credit points	*5 ECTS*

Required and recommended prerequisites for joining the module	*N/A*
Module summary	*This module aims to provide learners with knowledge on documentation, strategies, and technologies that support the processes of business resilience, threat response, and incident management. The module will examine how an organisation can prepare for business disruption and what actions can be taken to prevent and contain an incident, reduce the impact to organisational systems and get the business operational as quickly as possible after an incident occurs. Learners will acquire the necessary incident management skills required to develop contextual plans, run books and the associated processes and tools to enable effective business resilience capabilities. Furthermore, learners will be able to identify and illustrate the challenges associated with developing risk-based business resilience, threat response, and incident management processes. Learners will gain practical experience in aligning an organisation to industry standards and best practices that are commonly used for business resilience, threat response, and incident management tasks incorporating several stages, including preparation for incidents, detection and analysis of a security incident, containment, eradication, and full recovery, and post-incident analysis and learning.*
Module objectives/intended learning outcomes	*The Business Resilience, Threat Response, and Incident Management module is focussed on enabling learners to build, operate and critically assess an organisation's incident response capabilities and the resilience of their current critical processes and services, including the systems underpinning them. This module will appraise the key technical controls required in addition to the people and process elements required to build and operate a resilient organisation. In addition to evaluating the risk profile of an organisation, the module will enable learners to understand the requirements for directing operations during an incident with next gen-technology mind-set.* *On successful completion of this module the learner will be able to:* *LO1: Evaluate incident response plans, their effectiveness and their alignment to industry leading standards and appropriate incident response principles and methodologies.* *LO2: Critically appraise response activities for incident management from initial compromise to recovery and make recommendations for improvement.* *LO3: Contrast methods to assess the maturity of an organisation's incident response capabilities.*

<table>
<tr>
<td>Content</td>
<td>
<em>Business Resilience, Threat Response, and Incident Management is a 5 ECTS module delivered over 2 hours per week for 12 weeks. An indicative schedule of topics to be addressed each week is outlined below:</em>
<table>
<tr><th></th><th>Lecture Topic</th><th>Detail</th></tr>
<tr><td>1</td><td>Introduction</td><td>A background on the industry leading best practices (Including NIST Cybersecurity Framework for Incident Response). Understanding what risk means for an organisation and how an event ties into risk management processes. Providing an overview of where IR impacts governance, risk and compliance. Legal and regulatory compliance requirements for cyber incidents. Resilience standards (ISO 22301). Principles of incident management (ISO/IEC 27035).</td></tr>
<tr><td>2</td><td>Assessing Impact of Cyber Attacks</td><td>Understanding the threat landscape, recent incidents and developments in IR tools and processes. Overview of business resilience with business continuity and the IR focus on availability, while managing disruption. Cloud platform considerations and challenges.</td></tr>
<tr><td>3</td><td>System Security Concepts</td><td>How Blue teams evaluate and defend systems and environments. Understanding blue team activities during an incident.</td></tr>
<tr><td>4</td><td>Scaling Incident Response</td><td>Shaping and improving your IR posture. Focus on Red teams and how they play the role of attackers by identifying security vulnerabilities and launching attacks within a controlled environment. Understanding when and how to use a red team during an incident.</td></tr>
<tr><td>5</td><td>IR Roles and Responsibilities</td><td>Computer Incident Response Teams (CIRTs) operation. A mapping of IR roles to activities. How to prioritise these when directing incident response activi-</td></tr>
</table>
</td>
</tr>
</table>

		ties. Incident Management, Crisis Management and Business Continuity. Executive level stakeholders.
6	Incident Response Process	IR activities and processes to gain Business input for IR. Incident Response Plan. Detection, Investigation, Analysis and Activation. Cross-domain and border-domain knowledge related to cybersecurity.
7	Business Processes	The business perspective on regulation and operational resilience. Business Impact Analysis. The importance of process and service mapping to systems. Organisational and governance impact.
8	System Forensics and Tools	The role of Incident Response, Forensics and E-discovery and the intersection. Focus on system forensics and tools from an IR perspective.
9	Threat Intelligence & Threat Response	Threat intelligence processes. Importance of SIEM from threat hunting to performance monitoring.
10	Security operations for IR	Secure Operation Centres (SOCs) operation. Approaches, processes and roles within Sec Ops for monitoring, the three-tiered model for SOC. Threat intelligence processes and tooling.
11	IR Improvement process	How to evaluate your organisation's posture for IR. IR Reporting. IR Measurement. IR Auditing. IR Testing. Post incident activities supporting continuous improvement.
12	Summary	Re-cap on core domains and takeaways.

Exams and assessment formats	*The summative assessment strategy for this module is shown in the table below.*

Assessment Type	Assessment Description	Outcome addressed	%	Assessment Date
Continuous Assessment 1	For this proctored assessment learners will have to evaluate real-world incidents and critique the incident response process. The CA is based on course content covered up to the date of assessment. Critical appraisal and evaluation required.	LO1, LO2	40	Week 5
Continuous Assessment 2	Terminal proctored assessment based on 5 varied themes covered during the course requiring critical evaluation and demonstration of conceptual learning based on scenarios, research and critical appraisal.	LO1, LO2, LO3	60	Week 11

Reassessment strategy:

The reassessment strategy for this module will consist of an assessment that will evaluate all learning outcomes.

Reading list	*Recommended Book Reading* • *Anson, S. (2020). Applied Incident Response. 1st edition. John Wiley & Sons. [ISBN: 978-1119560265]* • *Diogenes, Y., & Ozkaya, E. (2022). Cybersecurity–Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system. 3rd Edition. Packt Publishing Ltd. [ISBN: 978-1803248776]* • *Crask, J. (2024). Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301. 2nd edition. Kogan Page [ISBN: 978-1398614871]*

Supplementary Book Reading

- *Thomas, A.E. (2018). Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence. [ISBN: 978-1643169705]*
- *Thompson, E. C. (2018). Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. 1st Edition. Apress. [ISBN: 978-1484238691]*
- *Bautista, W. (2018), Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents [ISBN: 978-1788625562]*

Other Resources

Description	**URL**
Verizon Breach Report	https://www.verizon.com/business/resources/reports/dbir/
Sans Reading Room	https://www.sans.org/reading-room/
Incident Handler's Handbook	https://www.sans.org/white-papers/33901/

Ethical Hacking & Penetration Testing

Module designation	*Ethical Hacking & Penetration Testing*
Term(s) in which the module is taught	Spring, Autumn
Institution(s) involved	UNIR
Relation to curriculum	Mandatory
Teaching methods	*Lab works, virtual lessons, audiovisual resources, collaborative work, mentorship, technical material, self-evaluation.*
Workload (incl. contact hours, self-study hours)	*Total workload: ca. 125 hours* *Contact hours:* – *Virtual lessons: 15 h.* – *Audiovisual teaching resources: 6 h.* – *Mentorship: 16 h.* – *Collaborative work: 7 h.* – *Case studies: 17 h.* *Self-study:* – *Study of the basic material: 30 h.* – *Reading the supplementary material: 20h.* – *Lab works: 10 h.* – *Self-evaluation test: 4 h.*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Management & analytical skills, basic knowledge of auditing processes (e.g., DEMING cycle), teamwork skills, planning and leadership skills. Fundamental theorical knowledge of operating systems, computer networking, and programming tools and systems.*
Module summary	*This module will allow the student to understand, analyze and manage the ethical hacking process by learning the concepts, techniques and processes through videos, practical exercises and laboratories. Obtaining the ability to use the results of an audit for management and decision making.*

Module objectives/intended learning outcomes	On successful completion of this module, the learner will be able to: 1. Demonstrate knowledge of the basic principles and importance of ethical hacking and system auditing, including methodologies, techniques, and the laws, policies, and legal aspects involved in the ethical hacking process. 2. Analyse and manage the methodologies and techniques used in ethical hacking. 3. Recognise how the tools used in ethical hacking audits function and interpret their results. 4. Explain the importance of ethical hacking practices and describe the methodologies used for penetration testing in various environments. 5. Demonstrate skills in analysing, identifying, and mitigating vulnerabilities in computer systems. 6. Identify threats and attack methodologies during the development of an ethical hacking audit. 7. Analyse the security posture of systems by identifying vulnerabilities and distinguishing between different types of cyberattacks. 8. Manage technical and executive reports to support decision-making. Skills: • Manage ethical hacking audit processes by selecting specific attacks according to the results required. • Plan and manage the ethical hacking process. • Prepare results reports after the ethical hacking process to support decision-making.
Content	*1. Ethical hacking fundamentals (history & main concepts)* • *Description: Description of the History and fundamentals of the Ethical Hacking process, and its evolution, regulations and policies.* • *Level of difficulty: medium* *2. Operating systems vulnerabilities & attack vectors* • *Description: Description of the OS vulnerabilities and attack vectors, methodology of identification, detection, and neutralization. (Methods, tools, and procedures)* • *Level of difficulty: medium*

	3. Network vulnerabilities & attack vectors (IT, IoT, OT) • *Description: Description of the network vulnerabilities and attack vectors, methodology of identification, detection, and neutralization. (Methods, tools, and procedures)* • *Level of difficulty: medium* *4. Web vulnerabilities & attack vectors* • *Description: Description of the Web vulnerabilities and attack vectors, methodology of identification, detection, and neutralization. (Methods, tools, and procedures)* • *Level of difficulty: medium* *5. Cloud vulnerabilities & attack vectors* • *Description: Description of the Cloud vulnerabilities and attack vectors, methodology of identification, detection, and neutralization. (Methods, tools, and procedures)* • *Level of difficulty: medium* *6. Pentesting methodologies* • *Description: Theorical description of the types of different methodologies to develop a pentesting, the stages and requirements for it, and the generation and interpretation of executive and technical reports.* • *Level of difficulty: low* *7. Footprinting and reconnaissance* • *Description: Fundamental description of the process for reconnaissance and footprinting stage, the tools used and the concepts to apply in an ethical hacking audit.* • *Level of difficulty: medium* *8. Vulnerability analysis and exploitation tools* • *Description: Description and explanation of the vulnerability analysis, the tools used for analysis, and*

	- *the tools for exploitation. Interpretation of the analysis.* - *Level of difficulty: low* *9. Ethics and legislation in ethical hacking* - *Description: Definition and explanation of the laws, regulations, and policies for an ethical hacking process. (national and International)* - *Level of difficulty: low* *10. Ethical Hacking certification roadmap:* - *Description: Introduction to the certification in Ethical Haking (study preparation, in technical and theorical aspects)* - *Level of difficulty: low* *11.-12. Module Wrap-Up and Practical Insights*
Exams and assessment formats	*Self-evaluation test: 4 h. (10%)* *Lab Works: 10 h. (15%)* *Collaborative work: 7 h. (15%)* *Final proctored exam: 2 h. (60%)*
Reading list	*EC-Council. (2016). Certified Ethical Hacker (CEH) V9: Ethical Hacking and Countermeasures. EC-Council.* *Palmer, C. (2015). Ethical Hacking and Penetration Testing Guide. McGraw-Hill Education.* *Engebretson, P. (2014). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress.* *Simpson, K., & Peck, M. (2019). Ethical Hacking for Beginners: Learn the Basics of Security, Hacking, and Penetration Testing. Independently published.*

	Oriyano, S. (2019). Ethical Hacking: A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking. Independently published. *Anand, N. (2020). Ethical Hacking: Ethical Hacking and Penetration Testing Guide. Independently published.* *Han, D., & Singh, A. K. (2021). Ethical Hacking: Learn the Fundamentals of Web Security, Network Security, and Ethical Hacking. Independently published.* *Brown, J. M. (2018). Ethical Hacking: A Hands-On Introduction to Breaking In. Addison-Wesley Professional.* *Dieterle, D. A. (2018). Ethical Hacking and Penetration Testing: A Hands-On Introduction to Hacking. Packt Publishing.* *Smith, S. (2017). Ethical Hacking: The Ultimate Beginner's Guide to Using Penetration Testing to Audit and Improve the Cyber Security of Computer Networks, Including Tips on Social Engineering. CreateSpace Independent Publishing Platform.*

A.I. & Emerging Topics in CyberSecurity

Module designation	*A.I. & Emerging Topics in CyberSecurity*
Institution(s) involved	UDS
Relation to curriculum	*Elective; recommended module for: CISO, Educator, Cyber Legal, Risk Manager*
Teaching methods	*Lecture, self-organized learning (flipped classroom), tutorial, hand-on, seminar/discussions, case study, guest lectures.*
Workload (incl. contact hours, self-study hours)	*Total workload: 125 h* • *Contact hours: 24 h* o *Lecture: 12 h* o *Hands-on/Tutorials: 6 h* o *Seminar/discussion & guest-lecture: 2 h* o *Flipped classroom: 4 h* • *Group Project: 40* • *Private study: 61 h*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Recommended, not required:* • *Security Operations* • *Machine Learning and Deep Learning in Cybersecurity* • *Ethical Hacking & Penetration Testing* *- or equivalent knowledge, skills and competencies acquired through prior study or professional experience.*
Module summary	*The module delves into AI and its impact on cybersecurity, highlighting its offensive and defensive applications. Using both lectures and flipped classroom sessions, students will learn key AI concepts and their applications in today's Security Operations Centers (SOCs). Finally, they will apply their learning in a group project, developing AI-powered cyber defense or attack scenarios.*
Module objectives/intended learning outcomes	On successful completion of this module, the learner will be able to: **LO1:** Demonstrate well-developed knowledge of core AI concepts, including generative AI and large language models, and explain their relevance to cybersecurity operations.

	LO2: Critically analyse the opportunities and limitations of AI in offensive and defensive cybersecurity applications, including within Security Operations Centers (SOCs). **LO3:** Identify and assess vulnerabilities, adversarial threats, and ethical risks associated with the use of AI in cybersecurity. **LO4:** Apply AI methods and tools to design and prototype solutions addressing real-world cybersecurity challenges in both defensive and offensive contexts. **LO5:** Collaborate effectively in teams to develop and present AI-driven scenarios, integrating technical, organisational, and regulatory considerations. **LO6:** Evaluate emerging trends and regulatory developments in AI for cybersecurity, anticipating their impact on professional practice and policy.
Content	*--Prerequisites & recap of required knowledge--* **Week 1: Security Operations & Cybersecurity Foundations** *Summary*: Recap the essentials of cybersecurity, focusing on SOC operations and using the NIST Cybersecurity Framework as a reference. Bring students up to speed on fundamental concepts and ensure consistent prerequisite knowledge. *Lecture Content:* • NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover, Govern) • Key SOC operations: vulnerability management, threat detection, incident response, red teaming, ... • SOC tools/technologies: SIEM, SOAR, IDS/IPS, EDR/NDR/XDR, TIP, ... • Standards and frameworks: NIST CSF, MITRE ATT&CK, CIS • Data in SOC: Types, Values, and Significance • Key SOC challenges: alert fatigue, evolving threats, APTs, ... **Week 2: Data Science/Engineering Foundations** *Summary:*

	Recap foundational concepts in data science and engineering with a focus on AI/ML. *Lecture Content:* • Data science/analytics concepts: statistical analysis. unsupervised and supervised ML, anomaly detection, neural networks, deep learning, reinforcement learning, CNN, RNNs, LSTM, ... • Data engineering concepts: data cleaning, normalization, enrichment, ETL, distributed data processing and big data architectures., ... **Week 3: Rise of AI – Generative Models & LLMs** *Summary:* Introduction to modern AI with a focus on generative models and LLMs. Bridge the gap between traditional data analytics and advanced AI concepts. *Lecture Content:* • Modern AI: Generative models and transformers. • LLMs and their architecture. *--Applications of AI in Cybersecurity--* ***Week 4: AI-powered Cyber Attack (Part 1)*** *Summary:* Explore how AI can be leveraged to automate and enhance cyber-attacks, guided by the MITRE ATT&CK framework. *Lecture Content:* • Introduction to cyber threat landscape: attackers TTPS • AI-powered social engineering and phishing attacks (initial access). • AI-generated malware (execution)

Week 5: AI-powered Cyber Defense (Part 1)

Summary:

Explore how AI strengthens cyber defense and improves SOC operations, guided by NIST Cybersecurity framework.

Lecture Content:

- AI for advanced threat detection and hunting.
- AI to enhance monitoring and reduce alert fatigue
- AI for automated incident response

Week 6: AI-powered Cyber Attack/Defense (Part 2) – *Flipped Classroom*

Summary:

A flipped classroom approach where students present on topics exploring AI applications in cyberattacks or defenses.

Lecture Content: (Potential Topics)

- AI-Driven Threat Intelligence
- AI for Secure Coding
- AI in Forensic Analysis and Incident Investigation
- AI for Adoptive Honeypots and Sandboxes
- AI-Powered Security Training and Awareness Programs
- AI for Penetration Testing and Red Team Operations
- AI for Vulnerability Management (Identification, Prioritization, and Patching)
- AI for Reporting and Summarization
- AI in Automated Reconnaissance
- AI for Automated Exploit Generation...

Week 7: AI-powered Cyber Attack/Defense (Part 3)

Summary:

Continuing the lecture series on AI for defensive and offensive security.

Lecture Content:

- The missing topics from week 6.

--Concerns & Considerations of AI in Cybersecurity--

	Week 8: Security Concerns in AI-driven Cybersecurity *Summary:* Addressing the security concerns and risks associated to AI systems and their usage in cybersecurity. *Lecture Content:* • AI-powered applications weaknesses & vulnerabilities. • Adversarial Machine Learning (weaknesses & vulnerabilities of AI models). • Related Frameworks: OWASP Machine Learning Security Top Ten, OWASP Top 10 for LLM Applications MITRE ATLAS, AIID, ADML. ***Week 9: Reliability in AI-driven Cybersecurity*** *Summary:* Focusing on key considerations when applying AI systems in cybersecurity. *Lecture Content:* • Importance of explainability and interpretability in AI (Explainable AI - XAI). • Building trust and ensuring accountability in AI-driven systems. • Domain-specific AI models (RAG systems) and the importance of fine-tuning. • Metrics and KPIs for benchmarking AI systems in cybersecurity (robustness, accuracy, security, etc.). ***Week 10: Responsible AI-driven Cybersecurity*** *Summary:* Examine the ethical, legal, and regulatory concerns associated with AI, particularly in cybersecurity. *Lecture Content:* • Ethical considerations of AI systems: fairness, bias, and transparency. • Privacy concerns with AI systems

	- Legal and regulatory requirements for AI systems, e.g., GDPR, AI Act, etc. *--Emerging Cross-cutting Topics—* ***Week 11: Future Trends in AI & Cybersecurity*** *Flipped classroom + (optional) guest lecture* *Summary:* Engage students (in form of flipped classroom) in exploring cutting-edge trends and controversial topics in AI and cybersecurity. Guest lecture (if available) to provide industry insight. *Lecture Content: (potential topics)* - Post-quantum cryptography and AI's role in post-quantum security - AI in zero trust architecture - Privacy-preserving AI & federated learning - AI and its impact on cyber warfare - AI in zero-day exploit discovery - AI at the edge (from cloud computing to edge computing) - Trust in the era of AI generated data - Human-AI Collaboration - AI-generated vulnerable codes ***Week 12: Wrap-up*** - *Overview of the course.* - *Final project presentations by students.* - *Discussions.* - *Guest lecture (from industry).*
Exams and assessment formats	- *Mid-term assessment (proctored quiz) end of W5 (15%)* - *Flipped classroom in W6 & W11 (10%)* - *Group project from W6 to W12 (30%)* o *Intermediate presentation (a pitch) in W8 (5%)*

	o *Final presentation in W12 (12.5%)* o *Technical report / scientific paper by W12 (12.5%)* • *Final proctored exam (45%)*
Reading list	***Recommended Reading Material:*** 1. *Muniz, Joseph. The modern security operations center. Addison-Wesley Professional, 2021.* *>>LINK<<* 2. *Abbas, R., Michael, K., Pitt, J., Vogel, K. M., & Zafeirakopoulos, M. (2023). Artificial Intelligence (AI) in Cybersecurity: A Socio-Technical Research Roadmap. The Alan Turing Institute.* *>> LINK <<* 3. *European Union Agency for Cybersecurity. (2022). Artificial intelligence and cybersecurity research.* *>> LINK <<* 4. *Sharma, R., Kalita, J., & Sharma, R. (2024). Artificial Intelligence in Cyber Security. ResearchGate.* *>> LINK <<* 5. *Kott, A. (2023). AI in Cybersecurity: The Paradox. IEEE Security & Privacy, 21(4), 94-98.* *>> LINK <<* 6. *Armando, A., Basile, C., Biondi, F., Botta, A., Carbone, R., Catania, V., Chessa, S., Ferretti, S., Marotta, A., & Mazzeo, G. (2024). AI in Cybersecurity: Activities of the CINI-AIIS Lab at University of Genoa. ITAL-IA 2024.* *>> LINK <<* 7. *Choo, K. K. R., Dehghantanha, A., & Parizi, R. M. (2023). Artificial Intelligence in Cyber Security. Pearson.* 8. *Sikos, L. F., Stumptner, M., Mayer, W., Howard, C., Voigt, S., & Philp, W. (2023). AI in Cybersecurity. 2023 Intermountain Engineering, Technology and Computing (IETC), 1-6.* *>> LINK <<* 9. *Liu, Y., Zhao, X., & Sun, Y. (2023). Adversarial machine learning in cybersecurity: Challenges and opportunities. IEEE Transactions on Information Forensics and Security, 18, 2614-2629.* *>> LINK <<* 10. *Patel, A., & Johnson, M. (2024). Securing the Internet of Things: AI-driven approaches and challenges. IEEE Internet of Things Journal, 11(3), 1852-1867.* *>> LINK <<* 11. *Nguyen, T., & Anderson, K. (2023). Ethical considerations in AI-driven cybersecurity: A framework for responsible implementation. AI and Ethics, 3(4), 401-418.* *>> LINK <<*

Malware Analysis

Module designation	*Malware Analysis*
Institution(s) involved	*UNIR*
Relation to curriculum	*Elective; recommended module for: Threat Intelligence*
Teaching methods	*Lab works, virtual lessons, audiovisual resources, collaborative work, mentorship, technical material, self-evaluation.*
Workload (incl. contact hours, self-study hours)	*<u>Total workload</u>: 125 hours* *<u>Contact hours:</u>* – *Virtual lessons: 15 h* – *Audiovisual teaching resources: 6 h.* – *Mentorship: 16 h.* – *Collaborative work: 7 h.* – *Case studies: 17 h.* *Self-study:* – *Study of the basic material: 30 h.* – *Reading the supplementary material: 22 h.* – *Lab works: 8 h.* – *Self-evaluation test: 4 h.*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Management & analytical skills, basic knowledge of auditing processes (e.g., DEMING cycle), teamwork skills, planning and leadership skills. Fundamental theorical knowledge of operating systems, computer networking, and programming tools and systems.*
Module summary	*This module will allow the student to understand, analyze and manage the malware analysis process by learning the methods, techniques and tools used. With exercises, videos and laboratories the student will learn the importance and how to use the results for auditing and other cybersecurity processes.*

Module objectives/intended learning outcomes	On successful completion of this module, the learner will be able to: 1. Demonstrate knowledge of the history of malware and its evolution, including relevant regulations and policies, and define key concepts such as types of malware, malware lifecycles, and common infection methods. 2. Comprehend the malware analysis process. 3. Classify different types of malware according to defined criteria. 4. Recognise how the tools used in the malware analysis process work and interpret their results. 5. Identify the methods, tools, and programs used in the malware analysis process. 6. Plan and execute the malware analysis process. 7. Analyse the structure and functionality of malware by dissecting code, identifying malicious behaviours, and determining potential damage or security risks. 8. Prepare reports with the results of malware analysis for organisational use. Skills • Evaluate and analyse types of anti-malware solutions according to their performance, and recognise major malware campaigns to inform preventive measures. • Manage the malware analysis process during critical situations, supporting the business resilience plan. • Develop results reports after malware analysis to support managerial decision-making.
Content	*1. Malware analysis introduction and fundamentals:* • *Description: Introduction to the context of malware analysis. Understanding the structure, operation, and interaction of malware, the importance of the process for malware analysis, to provides valuable information not only for the design and development of effective countermeasures, but also for understanding the origin of an attack and the ability to assess whether an organization's security systems can detect it and therefore analyse and take the necessary and appropriate response actions.*

	Level of difficulty: low *2. <u>Malware analysis methodologies:</u>* • *Description: This topic focuses on the study of a "Malware Analysis and Reverse Engineering" methodology using malware analysis and reengineering techniques and methods whose main objective is to acquire knowledge and gain a complete understanding of a particular malware, its operation, identification and ways to remove it.* *Level of difficulty: medium* *3. <u>Malware analysis tools:</u>* • *Description: fundamental explanation and description of the different tools used for developing the malware analysis process.* *Level of difficulty: medium* *4. <u>Anti-Malware tools:</u>* • *Description: Fundamental explanation and description of the actual anti-malware tools.* *Level of difficulty: medium* *5. <u>Case studies: Malware scenarios</u>* • *Description: Simulate malware to learn how it works under controlled conditions.* *Level of difficulty: low* *6. <u>Malware crisis management:</u>* • *Description: Methodological description of the process and procedures for the malware analysis process (preparation, action, execution, dissemination and feedback) communication for resilience business plan.* *Level of difficulty: medium*

	7. Malware analyst certification roadmap: • *Description: Introduction to the certification in malware analysis. (study preparation, in technical and theorical aspects)* *Level of difficulty: low* *8.-12. Consolidation and real-world integration*
Exams and assessment formats	*Self-evaluation test: 4 h. (10%)* *Lab Works: 10 h. (15%)* *Collaborative work: 7 h. (15%)* *Final exam: 2 h. (60%)*
Reading list	*Bermejo, J., Abad, C., Bermejo, J. R., Sicilia, M. A., y Sicilia, J. A. (2020). Systematic Approach to Malware Analysis (SAMA). Appl. Sci., 10(4), 1360. https://doi.org/10.3390/app10041360* *Monnappa, K. A. (2018). Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing Ltd.* *de Vicente Mohino, J. J., Bermejo-Higuera, J., Bermejo Higuera, J. R., Sicilia, J. A., Sánchez Rubio, M., & Martínez Herraiz, J. J. (2021). MMALE a methodology for malware analysis in linux environments. Computers, Materials & Continua, 67(2), 1447-1469.* *Masid, A. G., Higuera, J. B., Higuera, J. R. B., & Montalvo, J. A. S. (2023). Application of the SAMA methodology to Ryuk malware. Journal of Computer Virology and Hacking Techniques, 19(2), 165-198.* *Gregg, M. (2008). Build Your Own Security Lab: A Field Guide for Network Testing. Wiley Publishing.* *Hale Ligh, M., Adair, S., Hartstein, B., and Richard, M. (2011). Malware Analyst's Cookbook and DVD. Tools and Techniques for Fighting Malicious Code. Wiley Publishing, Inc.*

	Sikorki, M., and Honing, A. (2012). Practical Malware Analysis. The hans-on guide dissecting malicious software. No Starch Press. Casey, E. (2013). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press. Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2018). Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley. Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press. Mandiant. (2014). M-Trends: The Advanced Persistent Threat. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-m-trends-2014.pdf Dhar, P., & Mohanta, B. K. (Eds.). (2019). Malware Forensics: Investigating and Analyzing Malicious Code. CRC Press. Russinovich, M. E., & Solomon, D. A. (2012). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (6th ed.). Microsoft Press. Rouse, M. (2018). Malware (malicious software). Retrieved from https://searchsecurity.techtarget.com/definition/malware-malicious-software Rogers, M., & Gregg, N. (2012). Practical Mobile Forensics (1st ed.). Packt Publishing. IEEE Computer Society. (2015). Malware Analyst's Guide to Network Analysis. IEEE Computer Society Press.

	Harris, S. (2019). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory (2nd ed.). Wiley.

Cybersecurity Culture, Strategy & Leadership

Module designation	*Cybersecurity Culture, Strategy & Leadership* *(The CISO Fundamentals)*
Institution(s) involved	*VMU/Ataya, UDS*
Relation to curriculum	*Elective; recommended module for: CISO, Educator*
Teaching methods	Pre reading, Lectures, Case studies
Workload (incl. contact hours, self-study hours)	*125 hours in total* • Readings: 12 hours before the module + 12 hours during delivery (24 hours) • Lectures: 12 sessions × 2 hours each (24 hours) • Case studies and workshops / Lab work: 6 hours × 12 weeks (72 hours) • Project-specific self-study: 3 hours • Module exam: Multiple-choice, proctored: 2 hours
Credit points	*5 ECTS*
5Required and recommended prerequisites for joining the module	No additional requirements specific for this module.
Module summary	Management practices for Chief Information Security officers and those reporting to this function include various management practices, involve specific culture and involves developing adequate strategy. This module addresses those management practices and train students on understanding and applying those practices. It includes implementing those processes and practices including the seven maturity components to ensure resilient operations.
Module objectives/intended learning outcomes	Upon completion of this module, the learner will gain a thorough understanding of the role of the CISO and the key cultural and governance practices required to achieve protection objectives. They will also develop the skills necessary to effectively assume leadership responsibilities in planning, construction, operation, and monitoring activities. Learning outcomes that students should attain in the module: • **LO1. Knowledge:** Demonstrate understanding of the role of the CISO and the cultural and governance practices essential for

	achieving protection objectives, as well as a fundamental understanding of threats, vulnerabilities, and the protection controls required. • **LO2. Skills:** Demonstrate skills in performing various CISO roles, with the ability to complete leadership tasks across the "plan, build, run, and monitor" domains of activity. • **LO3. Competences:** Design a functional CISO organisation and define relevant activities aligned with business objectives.
Content	1. The cybersecurity landscape including review of some narrated incidents. Overview of potential business impacts. 2. Overview of cybersecurity threats 3. Overview of cybersecurity vulnerabilities 4. Overview of controls as structured following major categorisations (four ISO 27001 domains, Five NIST domains, etc.) 5. Review of major cybersecurity related frameworks and regulations 6. The governance activities and the PLAN domains of governance. 7. Case Discussion: Building a CISO culture, a function and align with the organisation 8. The Risk Management process: Business and technology risks 9. The protection roadmap The BUILD domains of governance to implement relevant transformation actions 10. Incident management, CERT and the RUN domains of governance 11. The MONITOR domain including the seven components of maturity and the definition of security Dashboards (technical and managerial). 12. Understand the various cybersecurity roles and the development of a CISO organisation
Exams and assessment formats	*One short computer-based quizz after the sessions 5 and 10. (10% each)* *One written assignment related to the development of a CISO organisation in a specific industry with specific technology and business requirements. (10%)* *In-class participation (10%)* *Proctored exam (60%)*
Reading list	*The virtual CISO article* *NIST CSF 2.0* *ENISA CSF* *CISM BOK (ISACA.org) - description videos*

	https://www.bing.com/ck/a?!&&p=cf68174b44ef6b6bJmltdHM9MTcyNTIzNTIwMCZpZ3VpZD0xYWUyY2FhNS03OTg5LTY1NjktMGQ0MS1kZTI4Nzg4ZjY0ZjcmaW5zaWQ9NTE1NQ&ptn=3&ver=2&hsh=3&fclid=1ae2caa5-7989-6569-0d41-de28788f64f7&u=a1L3ZpZGVvcy9zZWFyY2g_cT1jaXNtK2RvbWFpbnMmcXB2dD1jaXNtK2RvbWFpbnMmRk9STT1WRFJF&ntb=1 (PDF) Challenges and Solutions for Cybersecurity and Information Security Management in Organizations (researchgate.net) Challenges and Solutions for Cybersecurity and Information Security Management in Organizations March 2024 Vladimer Svanadze Sergiy Gnatyuk Cybersecurity and Strategic Management | Request PDF (researchgate.net) Cybersecurity and Strategic Management September 2023 DOI: 10.17323/2500-2597.2023.3.88.97 Budi Budi Gunawan Barito Mulyo Ratmono Ade Gafar Abdullah

Enterprise Architecture, Infrastructure Design and Cloud Computing

Module designation	*Enterprise Architecture, Infrastructure Design and Cloud Computing*
Institution(s) involved	UPB, MTU
Relation to curriculum	*Elective; recommended module for: Threat Intelligence*
Teaching methods	Lectures & Independent Study
Workload (incl. contact hours, self-study hours)	Total workload: ***125 hours (30 Contact + 95 Independent Learning)*** Contact hours: **Lectures: 6 x 2 hours = 12 hours** **Labs: 6 x 2 hours = 12 hours** **Tutorial: 6 x 1 hour = 6 hours** Private study including examination preparation, specified in hours[1]: **Independent Learning: 95 hours**
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*N/A*
Module summary	*The module aims to provide learners with the knowledge and skills to make informed, risk-aware decisions about enterprise architecture, infrastructure design, and cloud computing. It focuses on understanding how digital infrastructure choices impact business strategy, resilience, compliance, and trust. Learners will critically examine security strategies, assess the risks and opportunities of digital transformation, and develop governance-aligned recommendations that support sustainable and secure organisational growth*
Module objectives/intended learning outcomes	*On successful completion of this module the learner will be able to:* *LO1: Critically evaluate enterprise security architectures and cybersecurity frameworks to support defence-in-*

	depth strategies that protect the confidentiality, integrity, and availability of enterprise systems and data. *LO2: Assess the unique challenges and requirements of cloud security compared to traditional IT security, with emphasis on virtualised architectures, service models, and data protection strategies.* *LO3: Recommend secure-by-design approaches to secure enterprise architectures by integrating cybersecurity controls, governance principles, and regulatory considerations to support risk-informed business decisions*
Content	*Week 1: Introduction to EA, Infrastructure & Cloud* Defining EA, infrastructure, and cloud in a digital enterprise; differences from traditional IT; intro to CIA triad within architectural thinking; positioning security as a design concern not an afterthought; relationship to business goals, *Week 2: Enterprise Architecture Frameworks* TOGAF, SABSA, Zachman overview; layering business/app/infra/security domains; mapping SABSA layers to CIA triad; architectural roles in cybersecurity governance. *Week 3: Modelling and Architecture Tooling* ArchiMate, UML for infrastructure and security zoning; visualising defence in depth as architectural layers; mapping firewalls, DMZs, and zoning into infrastructure diagrams. *Week 4: Infrastructure Design Principles* Redundancy, segmentation, zoning, microsegmentation, Zero Trust embedded in infrastructure; secure-by-design principles; aligning infrastructure to security controls. Architectural validation via pen testing and red/blue team simulations. *Week 5: Cloud Architecture & Design* Infrastructure-as-Code (IaC), containers, microservices, orchestration, shared responsibility model, securing cloud-native patterns (serverless, PaaS, SaaS); threat modelling in cloud environments. Using threat intelligence to inform cloud threat models and architecture decisions. *Week 6: Security by Design in EA*

	Embedding security principles in EA layers; CIA triad revisited in enterprise security strategy; aligning SABSA objectives to business risk; continuity and disaster recovery as architectural functions. Integrating vulnerability management and CVE tracking into architectural governance processes. *Week 7: Identity, Access & Governance in Cloud* IAM architecture; Authentication vs Authorisation, MFA, federation, least privilege, RBAC/ABAC models; governance as risk control; audit trails and trust zones. *Week 8: Cloud Infrastructure: Secure Design Patterns* Virtualisation, Kubernetes, service meshes, API gateways; DevSecOps, container hardening, secrets management; network and endpoint security by design (not bolt-on). Integrating static/dynamic security testing tools into CI/CD pipelines (e.g., SonarQube, ZAP). Container security lifecycle including image scanning (e.g., Trivy) and runtime protection (e.g., Falco). *Week 9: Cloud Deployment Models & Security Impact* IaaS, PaaS, SaaS models through an architectural lens; public/private/hybrid/multi-cloud; how deployment model affects attack surface, data flow, and control layers. *Week 10: Data Security and Sovereignty* Data lifecycle design (at rest/in transit); encryption models; privacy by design, data residency, compliance (e.g., GDPR, ISO27001), cloud security policies. *Week 11: Governance, Risk & Budget in EA* Strategic risk frameworks (e.g., NIST CSF); cost of poor security design; cloud cost management (FinOps); business continuity; risk appetite mapped to infrastructure priorities. *Week 12: Course Wrap-Up & Presentations* Peer presentations of “secure digital transformation” case studies; reflect on architecture–business alignment; link back to learning outcomes and real-world application.
Exams and assessment formats	*Continuous Assessment 1 (40%) —Case Study Presentation: for this assessment learners will have to analyse and present a case study of enterprise/cloud adoption, evaluating security strategies, governance implications,*

	and business alignment. The CA is based on course content covered up to the date of assessment. Critical appraisal and evaluation required. Learning Outcome addressed LO1 and LO3. *Assessment 2, proctored (60%) – Policy Brief / Strategy Recommendation Report/Project: for this assessment learners will have to write and present (with identity verification) a policy brief or executive strategy recommendation to a relevant stakeholder based on a given scenario (e.g., hybrid cloud adoption, data sovereignty compliance, etc/). The report must identify risks/opportunities, propose governance-aligned security strategies, and recommend decision pathways that enhance resilience and trust. The CA is based on the varied themes covered during the course requiring critical evaluation and demonstration of conceptual learning based on scenarios, research and critical appraisal. Learning Outcome addressed LO1, LO2 and LO3.* *Reassessment strategy:* *The reassessment strategy for this module will consist of an assessment that will evaluate all learning outcomes.*
Reading list	*Recommended Book Resources:* • Jackson, K.L. and Goessling, S. (2018). Architecting Cloud Computing Solutions: Build cloud strategies that align technology and economics while effectively managing risk. Packt Publishing. [ISBN: 978-1788472425] • Mather, T., Kumaraswamy, S. and Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly. [ISBN: 978-0596802769] • Sherwood, J., Clark, A. and Lynas, D. (2005). Enterprise Security Architecture: A Business-Driven Approach. CRC Press. [ISBN: 978-1578203185] • Comer, D.E. (2023) The cloud computing book: the future of computing explained. FL: Chapman and Hall/CRC. [ISBN 978-0367706807] *Supplementary Book Resources:*

	• The Open Group (2022). The TOGAF® Standard, 10th Edition. Van Haren Publishing. [ISBN 978-9401808620] • Ross, J.W., Weill, P. and Robertson, D. (2006). Enterprise Architecture as Strategy: Creating a Foundation for Business Execution. Harvard Business Review Press. [ISBN 978-1591398394] • Singer, P.W. and Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. [ISBN 978-0199918119] • Gilman, E. and Barth, D., 2017. Zero Trust Networks: Building Secure Systems in Untrusted Networks. O'Reilly. [ISBN 978-1491962190] • Dotson, C. (2023). Practical cloud security: a guide for secure design and deployment. O'Reilly Media. [ISBN: 978-1098148171] • Faynberg, I., Lu, H.-L. and Skuler, D. (2016). Cloud computing: business trends and technologies. Wiley. [ISBN: 978-1118501214] • Bodmer, S.M., Kilger, M., Carpenter, G. and Jones, J. (2012). Reverse deception: organized cyber threat counter-exploitation. McGraw-Hill. [ISBN: 978-0071772495]. • M Stallings, W. (2019. Information privacy engineering and privacy by design: understanding privacy threats, technology, and regulations based on standards and best practices: Addison-Wesley Professional. [ISBN: 978-0135302156]. • Mihir. Shah. (2023), Cloud Native Software Security Handbook, Packt Publishing, p.372, [ISBN: 978-1837636983]. • Tim Mather, Subra Kumaraswamy, Shahed Latif. (2009), Cloud Security and Privacy, "O'Reilly Media, Inc.", p.338, [ISBN: 9781449379513]. *Other Resources* • European Union Agency for Cybersecurity (ENISA), Threat Landscape Report. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends • Information Systems Security Association. ISSA Code of Ethics. Information Systems Security Association. https://www.issa.org/issa-code-of-ethics/ • NIST. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

	• IBM, 2025. *Cost of a Data Breach Report 2025.* https://www.ibm.com/reports/data-breach • Cloud Security Alliance (CSA), 2021. *Cloud Controls Matrix (CCM).* https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix • Verizon Breach Report. https://www.verizon.com/business/resources/reports/dbir/ • Sans Reading Room. https://www.sans.org/reading-room/

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Law, Compliance, Governance, Policy, and Ethics

Module designation	*Law, Compliance, Governance, Policy, and Ethics*
Institution(s) involved	*UNIBS, MTU*
Relation to curriculum	*Elective; recommended module for: CISO, Educator, Cyber Legal, Risk Manager, Auditor*
Teaching methods	*lesson, case studies.*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125 hrs* *Contact hours: 20 hours e-learning, 10 hours asynch.* *Private study including examination preparation, specified in hours: 95 hours (75 self-reading / 20 hours exams preparation)*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Basic understanding of cybersecurity principles, computer networks, and foundational knowledge of legal frameworks.*
Module summary	*The "Law, Compliance, Governance, Policy, and Ethics" module focuses on equipping students with an in-depth understanding of the legal, ethical, and governance frameworks that shape cybersecurity practices. It provides comprehensive insights into data protection laws, governance structures, and the intersection of legal and ethical standards in organizational cybersecurity strategies. Students will engage with real-world applications of laws such as the GDPR, NIS2, and the Cyber Resilience Act learning how to implement compliance measures and ethical practices in diverse cybersecurity environments. Through case studies, discussions, and practical exercises, students will develop the skills needed to craft and assess policies, promote ethical cybersecurity practices, and lead with integrity in professional settings.*
Module objectives/intended learning outcomes	*Upon successful completion of this module, students will be able to:* ***Analyze Legal and Ethical Frameworks**: Analyze and critically evaluate legal frameworks and ethical standards in cybersecurity, including the overlap and differences between cybersecurity, data protection, and privacy.*

	***Interpret and Apply Cybersecurity Laws and Regulations**: Interpret and apply legal requirements to protect information assets, ensuring compliance with international regulations and internal governance tools such as policies or standards.* ***Craft and Evaluate Policies**: Craft and assess policies that address ethical, legal, and practical aspects of cybersecurity operations while promoting organizational integrity.* ***Integrate Ethical Cybersecurity Practices**: Integrate and promote ethical considerations in decision-making and conduct across all levels of the organization, enhancing organizational integrity through privacy, confidentiality, and accountability.*
Content	***Week 1: Legal Foundations of Cybersecurity*** *An introduction to key legal instruments, foundational concepts, and essential terminology in cybersecurity law.* ***Week 2: Regulatory and Legal Aspects of Cybersecurity Strategy and Operations (I)*** *An overview of relevant laws, acts, and regulations at the EU level, including NIS2, DORA, and the Cyber Resilience Act.* ***Week 3: Regulatory and Legal Aspects of Cybersecurity Strategy and Operations (II)*** *Examination of the European regulatory landscape for the Digital Decade, with a focus on cybersecurity-related laws such as the AI Act, Data Act, DSA, and DMA.* ***Week 4: Data Protection and Privacy*** *In-depth analysis of GDPR principles, key concepts, and the roles and responsibilities of various stakeholders.* ***Week 5: Cross-Border Data Protection*** *Exploration of the Law Enforcement Directive, ePrivacy Directive, and regulations governing cookies, as well as issues surrounding international data flows.* ***Week 6: Accountability and Compliance Management*** *Discussion of accountability mechanisms and compliance management strategies within organizations, with a focus on specific sectors.* ***Week 7: Legal Frameworks and Compliance*** *A detailed study of how legislation underpins cybersecurity and data protection, emphasizing EU laws and corporate compliance mechanisms.*

	Week 8: Standards and Certifications *Analysis of prominent EU cybersecurity standards and certifications, their enforceability, and the consequences of non-compliance.* ***Week 9: Governance in Cybersecurity*** *Examination of the integration of cybersecurity within broader IT governance frameworks and the role of policies in shaping organizational strategies.* ***Week 10: Ethical Considerations and Policy-Making*** *Exploration of the ethical dimensions of cybersecurity decisions and policy-making, with attention to the impact of emerging technologies like AI.* ***Week 11: Workplace Surveillance and Cybersecurity*** *A study of the balance between surveillance for security monitoring and the protection of employee privacy, analyzing surveillance technologies, legal frameworks, and ethical considerations to inform policy development.* ***Week 12: Diversity and Inclusion in Cybersecurity*** *Evaluation of the role of inclusive practices in enhancing cybersecurity efforts, and the impact of cyber-attacks on personnel, including psychological effects on response teams.*
Exams and assessment formats	Part 1: **Final Written Exam (Proctored Multiple-Choice Questionnaire, 60%)** – 60 minutes. This exam will cover key concepts, legal frameworks, and technical aspects of cybersecurity. Part 2: **Case Study Analysis or Presentation (40%)**– Students may alternatively choose to select a relevant case study related to workplace surveillance, cybersecurity strategy, or data protection laws. They will submit a detailed written analysis or deliver a presentation, demonstrating their ability to apply theoretical knowledge to practical scenarios.
Reading list	Understanding Cybersecurity Law in Data Sovereignty and Digital Governance An Overview from a Legal Perspective [2022] Melissa Lukings , Arash Habibi Lashkari https://link.springer.com/book/10.1007/978-3-031-14264-2 Handbook on European data protection law [2018] https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition# Guide to the General Data Protection Regulation (GDPR) https://ico.org.uk/media/for-organisations/guide-to-data-

	protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

Research Methods

Module designation	Research Methods
Institution(s) involved	UNI KO, UDS
Relation to curriculum	*Elective; recommended module for: Educator*
Teaching methods	The teaching and learning strategy for the Research Methods module will consist of classes and directed activities such as videos, tutorials, case studies and discussions on the programme's Learning Management System (LMS). Each week learners will begin by engaging with 2 hours of directed online activities aimed at introducing threshold concepts for that week's topic. Directed activities consist of short digestible pieces of content, such as explanatory videos, reading, guided tutorials, etc. Learners will then attend a live 2-hour discussion and tutorial session. Learners will be assigned tasks and exercises related to the directed content so that they can connect the theory to practice. Live sessions will mostly be practically based so as to make best use of the lecturer's expertise in the classroom. Learners will benefit from mentoring and formative feedback on completed directed activities during classes. The learning and assessment materials will be made available to learners through the programme's LMS. To support learners' independent learning the lecture notes and lab materials will be complemented by links to additional resources available on the Internet (e.g., documentation/framework tools, tutorials/videos, etc.).
Workload (incl. contact hours, self-study hours)	(Estimated) Total workload: 125 hours Directed e-Learning Activities: 12 hours Synchronous Tutorial Sessions: 12 hours Private study including examination preparation: 101 hours
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*N/A*
Module summary	After taking this module, you will be able to fully understand the range of research approaches, methodologies and strategies used in research within Cyber Security.

	You will have the tools and knowledge by which you can design a research proposal in Cyber Security applying relevant research strategies to collect and test data. You will know the evaluation methods in Cyber Security for qualitative and quantitative data. You are able to carry out appropriate research in Cyber Security ensuring an ethical research methodology is employed.
Module objectives/intended learning outcomes	LOs (according to Bloom's taxonomy): On successful completion of this module the learner will be able to: • LO1 (Knowledge): know the range of research approaches, methodologies and strategies used in research within Cyber Security • LO2 (Comprehension): comprehend the tools or knowledge by which they can design a research proposal in Cyber Security applying relevant research strategies to collect and test data; • LO3 (Application): apply evaluation methods in Cyber Security for qualitative and quantitative data; • LO4 (Analysis): carry out appropriate research analysis in Cyber Security ensuring an ethical research methodology is employed; • LO5 (Synthesis): develop capacity for analysis and synthesis of data instances in Cyber Security • LO6 (Evaluation): develop research skills on exploring real-world issues in Cyber Security
Content	Module content 1. Introduction to Research 2. Theoretical foundations of Research Methods; Ethical Concerns (including wrt. the use of Generative AI) 3. Qualitative Research Methods 4. Quantitative Research Methods 5. Other Research Methods, in particular use of Generative AI 6. Different Research strategies 7. Research Design and Process 8. Data Collection Techniques 9. Interview Design and Analysis 10. Statistical Data Analysis (incl. Statistical tests) 11. Research Data Presentation 12. Cyber Security Miniproject Presentations

Exams and assessment formats	Cyber Security Miniproject presentation (100%)
Reading list	• Creswell, J. W. (2022). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 6th ed. Thousand Oaks, SAGE Publications: California. • Tang, H. (2020). Engineering Research: Design, Methods, and Publication. London: Wiley. ISBN: 978-1-119-62453-0 • Sönke Ahrens: How To Take Smart Notes, 2017 • Schmidt, J. F. K. (2016). Niklas Luhmann's Card Index: Thinking Tool, Communication Partner, Publication Machine. In A. Cevolini (Ed.), Forgetting Machines: Knowledge Management Evolution in Early Modern Europe (pp. 289-311). Brill. • Forte, T. (2022). Building a Second Brain: A Proven Method to Organize Your Digital Life and Unlock Your Creative Potential. Atria Books.

Security Operations

Module designation	*Security Operations*
Institution(s) involved	CY, UNIR
Relation to curriculum	*Elective; recommended module for: Risk Manager, Threat Intelligence, Auditor*
Teaching methods	Lectures, tutorials, practical sessions (hands-on labs)
Workload (incl. contact hours, self-study hours)	Total workload: 125 hrs Contact hours: 20 hours lectures, 10 hours practical labs Private study including examination preparation: 95 hours (75 self-reading / 20 hours exams preparation)
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	Basic understanding of networking and operating systems (Windows & Linux), familiarity with cybersecurity principles, and knowledge of IT infrastructure. Programming/scripting skills (Python, Bash, PowerShell) are beneficial.
Module summary	The "Security Operations" module provides students with a comprehensive understanding of cybersecurity operations in a Security Operations Center (SOC). It covers essential topics such as threat detection, network security monitoring, incident response, and SOC workflow automation. The module includes both theoretical and practical components, enabling students to develop hands-on skills in cybersecurity analysis and defense.
Module objectives/intended learning outcomes	Upon successful completion of this module, students will be able to: • Understand the role and responsibilities of a SOC analyst. • Utilize network security monitoring tools to detect and respond to cyber threats. • Investigate and analyze security incidents using threat intelligence and data correlation techniques. • Develop SOC workflows and implement automation strategies to enhance cybersecurity operations.
Content	**Week 1:** Introduction to SOC and its role in cybersecurity. **Week 2:** Network security monitoring and tools.

	Week 3: Fundamentals of cryptography in cybersecurity. **Week 4:** Common TCP/IP attacks and mitigation techniques. **Week 5:** Endpoint security technologies and best practices. **Week 6:** Incident analysis and response strategies. **Week 7:** Cyber threat hunting methodologies. **Week 8:** Event correlation and SIEM (Security Information and Event Management) systems. **Week 9:** Investigation of security incidents using forensic techniques. **Week 10:** SOC workflow automation and optimization. **Week 11:** Compliance, governance, and ethical considerations in cybersecurity. **Week 12:** Emerging cybersecurity challenges and future trends.
Exams and assessment formats	**Part 1**: Final Written Exam (Proctored Multiple-Choice Questionnaire, 60%) – 60 minutes. This exam will test knowledge of security operations concepts, network security, and incident response methodologies. **Part 2** (40%): Case Study Analysis or Practical Lab Report – Students may alternatively select a real-world cybersecurity incident for analysis, demonstrating their ability to apply SOC techniques to investigate and mitigate threats.
Reading list	- **"The Practice of Network Security Monitoring"** by Richard Bejtlich - **"Cybersecurity Operations Handbook"** by John Rittinghouse & William Hancock - **"Blue Team Handbook: Incident Response Edition"** by Don Murdoch - **"Security Operations Center: Building, Operating, and Maintaining Your SOC"** by Joseph Muniz, Gary McIntyre, & Nadhem AlFardan - NIST Special Publications on Cybersecurity (NIST SP 800-61, NIST SP 800-92) - MITRE ATT&CK Framework (https://attack.mitre.org/) - CIS Critical Security Controls (https://www.cisecurity.org/controls)

Technological Foundations in Computer Science and Security Controls

Module designation	*Technological Foundations in Computer Science and Security Controls*
Institution(s) involved	*UPB, UNIR*
Relation to curriculum	*Elective; recommended module for: Risk Manager, Threat Intelligence*
Teaching methods	*Lecture, lab*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125* *Contact hours:* • *Lecture (a lot of demos): 24 hours,* • *Practice / laboratory session: 24 hours* o *Preset environments (local or remote virtual machines* *Private study including examination preparation, specified in hours[1]: 59 hours - used for preparing sessions, solving assignments, preparing for examination, self-study* *Team project: 18 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Basic programming skills and knowledge: functions, structures, classes, recursion, programmer's toolchain* *Basic understanding and use of computing systems* *Comfort in using common applications in computing systems: web browsers, file browsers, Office suite, management of media files, email clients*
Module summary	*The "Technological Foundations in Computer Science and Security Controls" aims to create the fundamental set of skills and knowledge in computing systems and security. Students will gain understanding and competences expected for a system power user: investigate, update, configure, assess, monitor a computing system and its components, with particular focus on security.*
Module objectives/intended learning outcomes	*On successful completion of this module the learner will be able to:* *LO1: Outline the hardware-software stack in modern computer systems* *LO2: Define and explain fundamental security concepts*

	LO3: Use applications to configure, secure, troubleshoot issues with data, applications and networking *LO4: Develop basic scripts using Python* *LO5: Examine, evaluate and revise security properties of data and applications: confidentiality, integrity, reliability* *LO6: Identify fundamental security requirements in existing applications and setups*
Content	*1. Computer Systems: Hardware, Software, Users* *a. Overview of computing systems, models* *b. Hardware, computer system types* *c. Software, applications the software stack* *d. (Security) Issues with computer systems* *e. Investigate the software and hardware information of a computing system* *f. Install and uninstall new applications* *2. Tools and Common Applications of Computer Systems* *a. Applications and application types (for different system types)* *b. Local and web apps* *c. Using, configuring and customizing common applications* *d. Online and offline office suite software* *e. Synchronizing local, online and mobile apps and data* *3. Data and Files* *a. Data storage and representation: bits, bytes, ASCII, UTF-8, binary, text* *b. Files and filesystems* *c. Working with data* *d. Finding data and files* *4. File Management and Access Control* *a. Users and access* *b. Filesystem permissions and access control* *c. Configuring filesystem permissions* *5. Storing and Versioning Data* *a. Requirements for versioning and history* *b. Versioning and history in common applications (Office Suites, storing applications)* *c. Multi-versioning, version control systems* *6. Data Processing and Visualisation* *a. Processing data, results of processing* *b. Viewing data, types of plots* *c. Visualization software* *7. Secure Programming* *a. Common code weaknesses and vulnerabilities* *b. Best practices in programming* *c. Secure coding guidelines* *d. Defensive programming*

	8. Secure Code Operations *a. Secure Software Development Lifecycle* *b. Code Auditing* *c. Static and Dynamic Analys* *d. Software supply chain: building, packaging, delivery* *e. Continuous Integration & Continuous Delivery* *9. Networking and Connected Systems* *a. Networking Concepts: Addressing, Communcation Media, Protocols* *b. Network Parameters and Configuration (addressing, gateway, DNS)* *c. Network applications and services* *10. Fundamental Security Topics* *a. Security principles and concepts: threat model, subject-object model, access control, reference monitor, bug / vulnerability / exploits* *b. Security goals: integrity, confidentiality, reliability, availability, privacy* *c. Security in modern computer systems* *d. Data security, network security, web security, application security* *11. Integrity and Confidentiality* *a. Requirements for integrity and confidentiality* *b. Encryption, encryption algorithms and tools* *c. Digital certificates, TLS, connection security* *d. Validating integrity and confidentiality* *12. Authentication, Authorization and Access Control* *a. Authentication: Passwords, tokens, user IDs, two-factor* *b. Password best practices, password management, password leaks* *c. Authorization, permissions, roles* *d. Access control, ACLs* *e. Authentication, Authorization and Access Control databases* *f. A, A, AC in modern systems*
Exams and assessment formats	*Assignments (20%)* - *Practice exercises working with applications and files – 10%* - *Practice exercises on a networked system – 10%* *Team Project (20%)* - *Set up a (set of) secure, functional virtual machine(s) – 20%* *Digitally proctored exam (60%)* - *Quiz (multiple answer questions) - 45 minutes: 30%* - *Practical exam: - 120 minutes: 30%*

Reading list	*Computer Systems: A Programmer's Perspective, 3rd Edition (https://csapp.cs.cmu.edu/)* *The Missing Semester of Your CS Education (https://missing.csail.mit.edu/)* *Security Essentials: https://github.com/open-education-hub/essentials-security* *Common Weakness Enumeration: https://cwe.mitre.org/* *SEI CERT Coding Standards: https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards*

Automation of Security Tasks and Data Analytics

Module designation	*Automation of Security Tasks and Data Analytics*
Institution(s) involved	*UNIRI, UNIR*
Relation to curriculum	*Elective; recommended module for: Threat Intelligence*
Teaching methods	*Lesson, lab works, project*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125 hours* *Contact hours:* *Synchronous Lectures: 12 hours* *Tutorial Sessions: 12 hours* *Directed e-Learning Activities: 24 hours* *Independent learning and work on project: 77 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*None*
Module summary	This course provides a comprehensive introduction to using Python for automating cybersecurity tasks, including threat detection, intelligence gathering, vulnerability assessment, and incident response. Students will learn to write scripts, analyze data and integrate various tools, while adhering to ethical and legal guidelines in cybersecurity automation.
Module objectives/intended learning outcomes	On successful completion of this module the learner will be able to: *LO1: Utilize Python to implement advanced cybersecurity tasks, including configuring environments, writing scripts for network scanning, log analysis, vulnerability assessment, and ensuring secure coding practices..* *LO2: Design and implement automated processes for threat detection, threat intelligence gathering, and incident response using Python, integrating various cybersecurity tools.*

	LO3: Use Python to manipulate, analyze, and visualize data related to cybersecurity, enhancing threat intelligence through data analysis. *LO4: Apply ethical and legal standards in the automation of cybersecurity tasks, including web scraping and threat intelligence gathering, ensuring compliance with industry regulations and ethical principles.* *LO5: Independently create and refine automated solutions for cybersecurity challenges and communicate the importance and impact of automation in cybersecurity.*
Content	**12-Week Program: Automation of Security Tasks** **Week 1: Introduction to Python and Cybersecurity** • **Classes:** ○ Focus Areas: Introduction to Python programming language, Overview of Python in cybersecurity, Basic programming concepts. ○ Level of Difficulty: Introductory • **Labs:** ○ Focus Areas: Setting up Python environment, Writing and running basic Python scripts using Jupyter Notebook and/or Anaconda. ○ Level of Difficulty: Introductory **Week 2: Automating Reconnaissance** • **Classes:** ○ Focus Areas: Reconnaissance techniques in cybersecurity, Importance of reconnaissance in cyber threat intelligence, Tools and methods for reconnaissance. ○ Level of Difficulty: Introductory to Intermediate • **Labs:** ○ Focus Areas: Writing Python scripts to perform active scanning and search open technical databases using libraries for network interaction such as scapy and HTTP requests with requests. ○ Level of Difficulty: Introductory to Intermediate **Week 3: Threat Intelligence Fundamentals** • **Classes:** ○ Focus Areas: Introduction to threat intelligence, Sources of threat intelligence, Types

	of threat intelligence (strategic, operational, tactical, technical). ○ Level of Difficulty: Intermediate • **Labs:** ○ Focus Areas: Gathering threat intelligence using Python from OSINT feeds, social media, and forums using parsing tools such as BeautifulSoup and HTTP requests with requests ○ Level of Difficulty: Intermediate **Week 4: Data Analysis and Visualization for Threat Intelligence** • **Classes:** ○ Focus Areas: Importance of data analysis in threat intelligence, Techniques for data cleaning, transformation, and visualization. ○ Level of Difficulty: Intermediate • **Labs:** ○ Focus Areas: Using Python libraries such as Pandas for data manipulation and Matplotlib for visualization of threat intelligence data ○ Level of Difficulty: Intermediate **Week 5: Automating Log Analysis and Monitoring** • **Classes:** ○ Focus Areas: Importance of log analysis in cybersecurity, Techniques for parsing and analyzing log files. ○ Level of Difficulty: Intermediate • **Labs:** ○ Focus Areas: Writing Python scripts to automate log analysis and monitoring using logging libraries such as the built-in logging module and Loguru. ○ Level of Difficulty: Intermediate **Week 6: Network Traffic Analysis** • **Classes:** ○ Focus Areas: Introduction to network traffic analysis, Importance in threat intelligence, Tools and techniques for analyzing network traffic. ○ Level of Difficulty: Intermediate to Advanced • **Labs:**

- Focus Areas: Writing Python scripts to capture and analyze network traffic using libraries for network analysis such as scapy.
- Level of Difficulty: Intermediate to Advanced

Week 7: Incident Detection and Response Automation

- **Classes:**
  - Focus Areas: Incident detection and response processes in threat intelligence, Automating detection of suspicious activities, Tools for incident response automation.
  - Level of Difficulty: Intermediate to Advanced
- **Labs:**
  - Focus Areas: Developing Python scripts to automate incident detection and response workflows using system monitoring libraries such as psutil for system resource monitoring and subprocess for executing system commands
  - Level of Difficulty: Intermediate to Advanced

Week 8: Threat Hunting Automation

- **Classes:**
  - Focus Areas: Introduction to threat hunting, Techniques and tools for threat hunting, Automating threat hunting tasks.
  - Level of Difficulty: Advanced
- **Labs:**
  - Focus Areas: Writing Python scripts to automate threat hunting activities using threat intelligence data and query libraries such as elasticsearch .
  - Level of Difficulty: Advanced

Week 9: Vulnerability Management and Exploitation

- **Classes:**
  - Focus Areas: Common vulnerabilities and exploitation methods, Automating vulnerability assessments.
  - Level of Difficulty: Intermediate to Advanced
- **Labs:**

- Focus Areas: Conducting automated vulnerability assessments and exploiting vulnerabilities using Python and tools for vulnerability scanning and exploitation such as nmap and metasploit.
- Level of Difficulty: Intermediate to Advanced

Week 10: Advanced Web Scraping for Threat Intelligence

- **Classes:**
  - Focus Areas: Advanced techniques for web scraping, Legal and ethical considerations in web scraping.
  - Level of Difficulty: Intermediate to Advanced
- **Labs:**
  - Focus Areas: Writing Python scripts for advanced web scraping and data extraction using web scraping tools such as BeautifulSoup, Scrapy, and browser automation tools such as Selenium.
  - Level of Difficulty: Intermediate to Advanced

Week 11: Automating AI Models for Threat Intelligence

- **Classes:**
  - Focus Areas: Introduction to AI in cybersecurity, Using pre-trained AI models for threat intelligence, Methods for integrating AI into threat intelligence workflows.
  - Level of Difficulty: Advanced
- **Labs:**
  - Focus Areas: Writing Python scripts to forward data to free AI models (e.g., OpenAI, Hugging Face) and processing responses for threat intelligence.
  - Level of Difficulty: Advanced

Week 12: Integrating and Automating Security Tools

- **Classes:**
  - Focus Areas: Integration of various security tools, Building automated workflows, Best practices for automation in security.
  - Level of Difficulty: Advanced
- **Labs:**
  - Focus Areas: Creating and deploying integrated automation solutions for security

	tasks using Python and orchestration tools such as Docker and Ansible. ○ Level of Difficulty: Advanced
Exams and assessment formats	*Two proctored midterm assessments (20%)* *take-home lab assignments (40%)* *Proctored Finals (40%)*
Reading list	Mandatory Reading: • "Python for Cybersecurity: Using Python for Cyber Offense and Defense" by Howard E. Poston III • Python Documentation • Pandas Documentation • MITRE ATT&CK Framework • ENISA Threat Intelligence Sharing Guidelines (2020) Elective Reading (For Deeper Understanding and Additional Practice): • "Automate the Boring Stuff with Python: Practical Programming for Total Beginners" by Al Sweigart (2nd Edition, 2019) • "Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents" by Wilson Bautista (2020)

CISO and Crisis Communication

Module designation	*CISO and Crisis Communication*
Institution(s) involved	*VMU/Ataya, UDS*
Relation to curriculum	*Elective; recommended module for: CISO*
Teaching methods	Pre reading, lectures, case study, workshop and Coaching hours
Workload (incl. contact hours, self-study hours)	*125 hours in total* • Readings: 12 hours before the module + 12 hours during delivery (24 hours) • Lectures: 12 sessions × 2 hours each (24 hours) • Case studies and workshops / Lab work: 6 hours × 12 weeks (72 hours) • Project-specific self-study: 3 hours • Module exam: Multiple-choice, proctored: 2 hours
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	No additional requirements specific for this module.
Module summary	Cybersecurity Communication activities are essential in crisis situations and as regular communication of the CISO to stakeholders. Crisis communication is required for three specific focuses that are: Communicate to resolve the incident and the crisis; Communicate as a compliance notification required by law and regulators; and finally communicate to improve the reputation as a follow-up on an incident/crisis. Mastering communication activities is a must skill for cybersecurity leaders.
Module objectives/intended learning outcomes	Learning outcomes that students should attain in the module: **A. Knowledge:** Familiarity with the major communication requirements in cybersecurity, including: 1. Regular leadership communication activities with various stakeholders, including senior management, users, and regulators. 2. Crisis communication serving three purposes: containing the incident or crisis, meeting regulatory

	notification requirements, and preserving organisational reputation. 3. Regular awareness activities as an essential control for improving the preparedness of the human factor. **B. Skills:** Possess the skills necessary to plan, develop, and conduct effective communication actions. **C. Competences:** Be able to create a comprehensive communication plan, including the design, timeline, identification of target audiences, definition of communication channels, formulation of messages, evaluation of impact, and recommendations for future improvement.
Content	1. *The purpose of the communication activities in terms of Audience and business results. The impact of communication on the protection, detection, response and recovery activities related to cybersecurity.* 2. *Communication elements including the objective, the expected impact, the target audience, the communication channel, and the timing. How to build a communication plan.* 3. *Building a dashboard as a baseline for communication to key stakeholders. Contents of a dashboard and alignment with the four Dimensions of the Balanced Scorecard model.* 4. *The crisis communication – Part 1: Principles of Incident/Crisis management* 5. *The crisis communication – Part 1: Communicate to resolve the incident/Crisis* 6. *The crisis communication – Part 2: Cybersecurity related regulations and their notification requirements (NIS2, DORA, GDPR, etc.)* 7. *The crisis communication – Part 2: Conduct regulatory communication requirements* 8. *The crisis communication – Part 3: Business needs for preserving reputation. Build reputation requirements in line with business objectives.* 9. *The crisis communication – Part 3: Validate cybersecurity and communication activities in line with not-accepted reputational risks. Develop actions along with management and business leaders.* 10. *Awareness program objectives, audience and plans* 11. *Cybersecurity awareness tools: Phishing and user reflexes exercises, alignment with key threats and*

	vulnerabilities; awareness as a full protection mechanism. 12. *Putting it all together: case studies on major communication actions and campaigns before and after an incident.*
Exams and assessment formats	*Three written assignments after sessions 5, 7, and 9 related to the development of relevant communication plans (40%). One final proctored exam (60%).*
Reading list	Best Practices for Cyber Crisis Management — ENISA (europa.eu) cybersecurity-incident-management-guide-EN.pdf (cybersecuritycoalition.be) Chapter 6. Communications to Promote Interest | Section 1. Developing a Plan for Communication | Main Section | Community Tool Box (ku.edu) 10 Crisis Communication Plan Examples (and How to Write Your Own) (hubspot.com) FIRSTCON23-TLPCLEAR-Benetis-ISO-27035-practical-value-for-CSIRTs-and-SOCs.pdf (PDF) Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach (researchgate.net) Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach July 2024 Rūta Pirta-Dreimane Agnė Brilingaitė Evita Roponena

Risk Management of Cyber-Physical Systems

Module designation	*Risk Management of Cyber-Physical Systems*
Institution(s) involved	POLIMI, MTU
Relation to curriculum	*Elective; recommended module for: CISO, Risk Manager, Auditor*
Teaching methods	Lectures, Exercises, Assignments, Experiential learning (serious game)
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125* *Contact hours: 50* *Private study, including examination preparation, specified in hours[1]: 75*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*None*
Module summary	*The* ***Risk Management of Cyber-Physical Systems*** *module aims to equip students with the skills to analyse, assess, and manage risks associated with socio-cyber-physical systems. It provides a comprehensive understanding of complexities and practices in technology risk governance (in the different stages of the system life cycle), and in operational resilience, through practical applications of industry-recognized methods, tools and processes. Students will analyse case studies and engage with a serious game to gain practical insights into the interplay between cybersecurity and business continuity. The module includes three core instructors and features guest lectures from industry professionals, offering valuable practitioner perspectives.*
Module objectives/intended learning outcomes	After successful completion of this course, students will be able to: • Identify and categorise technology risks of operating and digital technologies • Describe and prioritise risk and resilience features of socio-cyber-physical systems exposed to a variety of threats

	• Distinguish and compare approaches to and methods for technology risk governance at different system life cycle stages (from deign, to project management, to operations) • Select and apply the most appropriate risk assessment approach and methods given the features of the socio-cyber-physical system under analysis • Examine and evaluate the suitability of an organisation's technology risk governance model • Prepare a strategic report on technology risk assessment • Describe the concepts and principles related to the Business Continuity Management (BCM), conduct Business Impact Analysis (BIA), identify and evaluate recovery strategies, develop Business Continuity Plans
Content	**Week 1** • Course introduction. • Risk management concept and process. • Risk-based technology selection and adoption. **Week 2** • System safety engineering of cyber-physical systems. • Risk engineering methods: ○ Failure Mode Effects and Criticality Analysis (FMECA) ○ Fault Tree Analysis (FTA) ○ Event Tree Analysis (ETA) ○ Probabilistic Risk Analysis (PRA) **Week 3** • Risk analysis of socio-technical systems: ○ Human and organisational risk factors ○ Risk management of organisational accidents ○ High Reliability Organization theory ○ Critical incident analysis

	Week 4 • Cyber risk modelling: ○ Types of risks (humans, IT, OT) ○ Cyber risk models and principles ○ Cascading effects ○ Correlation among risks ○ Risks of intangible assets **Week 5** • Challenges and advances in industrial cyber risk assessment: ○ Information security today ○ Challenges in modern security governance ○ Continuous risk assessment ○ Principles of social engineering **Week 6** • Cyber risk maturity models and management: ○ CMMs ○ DevSecOps drill down (SCA, SBOM, best practices) ○ EU legislation framework ○ US legislation framework and comparison **Week 7** • Case study by practitioners: *Cybersecurity Threats, Strategy and Management at Intesa SanPaolo* **Week 8** • Case study by practitioners: *Cyber and Physical Risk Management at SNAM spa* **Week 9** • Business Continuity Management: ○ BCM fundamentals and business cases ○ Business Impact Analysis

	○ Recovery strategies ○ Collaborative BCM and supply chain resilience **Week 10** • Business Continuity Management – Serious Game (Session 1) **Week 11** • Business Continuity Management – Serious Game (Session 2) **Week 12** • Cybersecurity for Critical Infrastructure: ○ Importance of CIP-R ○ Critical infrastructure resilience ○ Interdependencies and cascading events ○ Modelling and analysis of interdependent systems ○ Cyber threats to CI • Best practices and frameworks for CIP-R
Exams and assessment formats	• A group written assignment: prepare either an essay on the state of art review of a relevant topic/challenge in the industrial cybersecurity risk management domain, or a Technology Risk Assessment report on an advanced digital technology. (40%) • Final proctored written test, comprising exercises and theoretical questions *(60%)*
Reading list	• Bedford, Tim & Cooke, Roger M., “Probabilistic risk analysis: foundations and methods”, Cambridge University Press, 2001. • Reason J., “Managing the risks of organisational accidents”, Ashgate, 1997. • Hubbard, D. W., & Seiersen, R. (2023). How to measure anything in Cybersecurity Risk. *John Wiley & Sons, Inc*. • Course material: case texts, teaching notes and exercises, slides. • Suggested readings by the instructors.

Cybersecurity Auditing

Module designation	*Cybersecurity Auditing*
Institution(s) involved	*VMU/Ataya, UNIR*
Relation to curriculum	*Elective; recommended module for: Cyber Legal, Auditor*
Teaching methods	Pre reading, Lectures, Case study and workshop, Coaching hours
Workload (incl. contact hours, self-study hours)	*125 hours in total* • Readings: 12 hours before the module + 12 hours during delivery (24 hours) • Lectures: 12 sessions × 2 hours each (24 hours) • Case studies and workshops / Lab work: 6 hours × 12 weeks (72 hours) • Project-specific self-study: 3 hours • Module exam: Multiple-choice, proctored: 2 hours
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	No additional requirements specific for this module.
Module summary	Auditing is a third line of defence that aims at giving assurance to decision makers in relation to the existence and the efficiency of controls. Auditing involves validating the activities already performed by the second line of defence (for example risk managers, Chief information security officers, IT operations team, Devops teams) and the first line of defence (Business operations and managers). Building an annual audit programme, developing an audit plan for specific audit assignments, and finally conducting the assignment and producing the resulting report. Auditing produce a statement of findings and recommendations aimed at improving the governance and operations of the cybersecurity activities.
Module objectives/intended learning outcomes	Upon completion of this module, the learner will be able to demonstrate an understanding of audit activities as an integral part of the assurance process. They will be able to plan, develop, and conduct comprehensive cybersecurity audit assignments, and design audit plans tailored to the needs of stakeholders.

	Learning outcomes that students should attain in the module: **LO1. Knowledge:** Demonstrate familiarity with audit activities as part of the assurance process, including scoping, selection of suitable criteria, the audit process, and audit reporting. **LO2. Skills:** Plan, develop, and conduct a full cybersecurity audit assignment, producing outputs that inform stakeholders on the maturity, effectiveness, and outcomes of audit activities in alignment with business requirements and best auditing practices. **LO3. Competences:** Analyse business and technical requirements to create and adjust audit plans, select suitable criteria, and align audit activities with standard practices, including IT auditing certification frameworks. **LO4. Competences:** Execute audit fieldwork and produce a report with findings and actionable recommendations.
Content	1. *The purpose of audit activities and the need for a third line of defence and relation with Internal auditing (e.g. external/internal auditing for certification), and relation with monitoring activities* 2. *The business and technical need of an audit assignment.* 3. *The scoping of the assignment and the selection of suitable criteria and a framework, a method or a baseline. Assess the possible use of automated tools.* 4. *The development of an audit plan including various phases and a description of various fieldwork activities.* 5. *The management of audit work includes the validation of the existence of controls, the validation of the effectiveness of controls, substantive testing and conducting interviews.* 6. *The development of an audit report aligning the findings, the recommendations and the opinion statement to respond to audit request and business needs. The method to produce SMART recommendations that aim at bringing optimal, most suitable and effective mitigations.* 7. *The presentation of audit findings to the audit requestor highlighting the impact and severity of the*

	findings and the return on investment of proposed recommendations. 8. *The development of a yearly audit program based on the understanding of an audit universe, an assessment of business needs from the assurance and audit activity and the best use of available audit resources.* 9. *Understand of the specificities of cybersecurity auditing with the aim at giving assurance of protection controls, the maturity of the organisation, and the efficiency of the second lines of defence (Risk management; project management Office; Compliance management; CISO office; DPO office) as well as governance practices (Senior management role and involvement in cybersecurity governance; the cybersecurity spending effectiveness and justification).* 10. *A business case with a real-life audit request to be developed in groups in various environment (Auditing the supply chain, the cybersecurity project implementation; the effectiveness of performance indicators and veracity of management reporting on cybersecurity posture; The effectiveness of intrusion detection activities; the effectiveness of awareness activities, etc.).* 11. *Presentation of the business case in groups benefiting the whole class.* 12. *A business case with a real-life need for developing a yearly audit program based on a given risk assessment and a typical audit universe)*
Exams and assessment formats	*Evaluation of both business cases in sessions 10 and 12. (20%)* *Take-home assignments (10%)* *In-class participation (10%)* *Proctored exam: Evaluation of a "bad" audit report (60%)*
Reading list	ITAF - IT Audit Framework from ISACA Store - An ITAF Approach to IT Audit Advisory Services | Digital | English - ISACA Portal- Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One)

	Author: Osman Azab, CISA, CISM, CRISC, CGEIT, CSAC Date Published: 16 January 2024 Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One) (isaca.org) IS Audit Basics: Auditing Cybersecurity Author: Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt, and R. V. Raghu, CISA, CRISC Date Published: 1 March 2019 IS Audit Basics: Auditing Cybersecurity (isaca.org) A Client-Centered Information Security and Cybersecurity Auditing Framework, Mario Antunes, Marisa Maximiano, Ricardo Gomes (PDF) A Client-Centered Information Security and Cybersecurity Auditing Framework (researchgate.net) Integrated framework for cybersecurity auditing October 2020 Information Security Journal A Global Perspective 30(2) DOI: 10.1080/19393555.2020.1834649 Iman M. A. Helal, Osamah Almatari, Sherif Mazen, Sherif Elhennawy Integrated framework for cybersecurity auditing | Request PDF (researchgate.net)

Cybersecurity Economics & Supply Chain

Module designation	*Cybersecurity Economics & Supply Chain*
Institution(s) involved	*MRU, UDS*
Relation to curriculum	*Elective; recommended module for: CISO, Risk Manager*
Teaching methods	The teaching methods include interactive lectures that provide theoretical foundations, supplemented by hands-on practical exercises to apply the concepts in real-world scenarios. Students are encouraged to engage in discussions and group work to foster collaboration and deepen their understanding. Additionally, case studies and scenario-based learning are utilized to analyze real cybersecurity incidents, enabling students to develop critical thinking and problem-solving skills. Presentations allow students to articulate their findings and demonstrate their understanding of key concepts, fostering a comprehensive learning experience that blends theory with practical application.
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125 hours* *Contact hours: 30 hours - lesson* *Private study including examination preparation, specified in hours: 95 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Basic understanding of cybersecurity.*
Module summary	The *Cybersecurity Economics & Supply Chain* module aims to equip students with comprehensive knowledge of the economic aspects of information security and supply chain cybersecurity. It covers key concepts such as the direct and indirect costs of cyber incidents, the economic impact of various cyber threats on organizations, and the strategic role of cybersecurity in business planning. Students will explore frameworks, budget allocation for cybersecurity, and methods for managing third-party risks in supply chains. Through interactive lectures, practical exercises, and case studies, students will learn to conduct qualified investment analyses, understand technical incident reports, and apply economic models in security. Graduates will be able to strategically plan cybersecurity processes

	and evaluate the economic efficiency of security solutions within organizations and supply chains.
Module objectives/intended learning outcomes	*Upon successful completion of this module, students will be able to:* 1. **Understand Cybersecurity Economics.** Students will be able to analyze the economic implications of cybersecurity within organizations and incorporate cybersecurity considerations into business strategies. 2. **Assess the Costs of Cyber Incidents.** Students will develop skills to identify and evaluate the direct and indirect costs of cyber incidents, using case studies on data breaches, ransomware attacks, and other cybersecurity events. 3. **Analyze the Economic Impact of Cyber Threats.** Students will be equipped to evaluate how different types of cyber threats affect an organization's financial stability, reputation, and long-term growth prospects. 4. **Strategically Plan Cybersecurity Investments.** Students will learn to perform qualified investment analyses, make informed decisions about cybersecurity budgets, and determine the appropriate level of investment in prevention, detection, response, and recovery efforts. 5. **Apply Cybersecurity Frameworks and Standards.** Students will be able to utilize and critically assess various cybersecurity frameworks and standards. 6. **Manage Cybersecurity in Supply Chains.** Students will understand and manage the financial and strategic impact of cybersecurity risks across supply chains, particularly focusing on third-party risks and economic consequences. 7. **Anticipate Future Trends in Cybersecurity Economics.** Students will be prepared to explore and analyze emerging trends, technologies, and threats that shape the future of cybersecurity investments and the economic considerations within organizations. 8. **Effectively Communicate Findings.** Students will be capable of conducting comprehensive case analyses, preparing structured reports, and presenting their findings in a logical and sequential manner.
Content	This course provides knowledge on the economic aspects of information security, helping students understand and manage the financial implications associated with cyber threats and incidents. It aids in making informed investment decisions in security solutions and delving into descriptions of cyber threats and technical analyses of incidents. 1. Introduction to Cybersecurity Economics: Understanding the economic implications of cybersecurity within organizations.

	Overview of key concepts and the role of cybersecurity in business strategy. 2. Cost of Cyber Incidents: direct and indirect costs of cyber incidents. Case studies on data breaches, ransomware attacks, and other cybersecurity events. 3. Economic Impact of Cyber Threats on Organizations: Exploring how different types of cyber threats (e.g., phishing, DDoS, malware) affect an organization's financial stability, reputation, and long-term growth. 4. Investment in Cybersecurity. How Much is Enough? Discussion on budget allocation for prevention, detection, response, and recovery. **5. Economics of Cybersecurity Frameworks and Standards.** 6. Supply Chain Cybersecurity Risks and Vulnerabilities. 7. Cybersecurity in the Supply Chain. Economic Implications. Understanding the financial and strategic impact of cybersecurity across supply chains. How to manage third-party risk and its economic consequences. 8. **Future Trends in Cybersecurity Economics**: Exploring emerging trends, technologies, and threats that will shape the future of cybersecurity investments and economic considerations in organizations. 9.-12. **Review, Reflection, and Integration**
Exams and assessment formats	*Final proctored exam (60 minutes) (60%)* *Research paper (20%)* *Report (20%)*
Reading list	• ENISA Reports: Various resources on the economics of security and risk management. • Academic Papers: Including works by Anderson on the economic perspective of information security and Su's overview of economic approaches to information security management. • Practical Models: Such as the Return on Security Investment (ROSI) and other improvement models in IT security management. • Cybersecurity Frameworks: Including the Cyber Kill Chain and MITRE ATT&CK matrix. 1. Economics of Security: Facing the Challenges, ENISA, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/Experts_Contributions_2. 2. Economics of Security: Facing the Challenges, ENISA, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/EoS%20Final%20report/ 3. Security

	3. Economics and the Internal Market, ENISA, https://www.enisa.europa.eu/publications/archive/economics-sec/ 4. 4. Anderson, R. (2001): Why Information Security is Hard - An Economic Perspective. In: ACSAC 2001: Proc. 17th Annual Computer Security Applications Conference, pages. 358–365. IEEE Press, Los Alamitos. Downloadable from: http://www.acsac.org/2001/papers/110.pdf 5. 5. Su, X. (2006). An overview of economic approaches to information security management. http://eprints.eemcs.utwente.nl/5693/01/00000177.pdf 6. Sonnenreich, W., Albanese, J., and Stout, B. (2006). Return on security investment (ROSI)-A practical quantitative model. Journal of Research and Practice in Information Technology, 38(1), pages 45-56. Downloadable from: http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf 7.Cavusoglu, H., 7. Cavusoglu, H. and Raghunathan, S. (2004): Economics of IT Security Management: Four Improvement 8. 8. Cyber kill chain, https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain 9. 9. MITRE ATT&CK matrix, https://attack.mitre.org/

Cybersecurity Education and Training Delivery I

Module designation	*Cybersecurity Education and Training Delivery I*
Institution(s) involved	*BRNO/VUT, UDS*
Relation to curriculum	*Elective; recommended module for: Educator*
Teaching methods	*lecture, lab, seminar*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125* *Contact hours: lecture:* • *12 hours, seminar* • *discussions: 12 hours,* • *practice / laboratory session: 24 hours (each session consists of 1 hour lecture / demo, 1 hour seminar / discussion and 2 hours of assisted lab / practice session* *Private study including examination preparation, specified in hours: 77 hours - used for preparing for sessions, solving assignments, preparing for examination, self-study*
Credit points	*5 ECTS*
Recommended prerequisites for joining the module	*Technological Foundations for CS & Security Controls - or equivalent knowledge, skills and competencies acquired through prior study or professional experience*
Module summary	*The Cybersecurity Education and Training Delivery module aims to prepare students to identify weaknesses, raise awareness and develop training programs in the realm of cybersecurity education. It presents an array of technical tools and modern methodology to teach cybersecurity related content while combining it with fundamental pedagogical principles. Students will be able to plan and carry out cybersecurity trainings, which will further be developed in the second module of this kind.*
Module objectives	*Knowledge* - *Understanding of different materials, delivery methods and infrastructure components used in cybersecurity education* - *Mapping trainee groups requirements with specific types of materials and delivery methods* *Skills*

	- *Developing materials for cybersecurity classes* - *Deploying the infrastructure for delivery of training materials* - *Using Git, GitHub to develop content* - *Using cyber range technologies for trainings* - *Creating interactive media content for cybersecurity topics* *Competences* - *Organizing a cybersecurity training content repository* - *Communicating relevance of topics part of a training / course* - *Assessing individual and group characteristics with respect to cybersecurity knowledge and skills* - *Providing personalized support to trainees*
intended learning outcomes	**General Learning Outcomes:** (G1) Critically evaluate methodologies and materials for cybersecurity education (G2) Appraise students' needs to plan and carry out training (G3) Create new teaching material reflecting the relevance of emerging trends in cybersecurity and use modern technologies **Detailed Learning Outcomes:** (LO1) Analyse adult learners' needs and design lesson plans (LO2) Evaluate education methods and develop teaching strategies (LO3) Create interactivity and engagement (LO4) Design multimedia content for cybersecurity education (LO5) Propose training around cybersecurity incidents for SMEs (LO6) Support SMEs in live incident communication (LO7) Design and implement awareness training using tools (L08) Critically evaluate the effectiveness of gamification and scenario-based instructional strategies (LO9) Design and create interactive cybersecurity learning environments

Content	1. **Adult Learning Principles and Effective Methods for Cybersecurity Educators** a. core principles of pedagogy and adult learning, b. learner motivation, lesson planning and learner types 2. **Cybersecurity training and evaluation methods for students** a. interactive cybersecurity education methods, (board games, simulations) b. Types of materials, infrastructure and methods for teaching and training, c. student evaluation and assessment tools. 3. **Innovative Content Creation with AI and Multimedia Tools for engaged learning** a. tools for image, audio and video editing b. creation of interactive and asynchronous content c. use of AI to create customized learning material. 4. **Understanding the Needs of SMEs – Crisis Communications on a Shoestring** a. Introduction to SMEs and Their Unique Cybersecurity Challenges, b. Crisis Communications on a Budget: Key Principles, Internal & External Stakeholder Communications 5. **Collaborative tools and interactive presenting** a. various interactive cybersecurity education methods b. live polling and Q&A tools, Visual Collaborative Platforms, Game-based Learning Platforms, video conferencing tools . 6. **Practical Cybersecurity Considerations for SMEs** a. online tools to uncover high-level issues on web-facing software, b. how to develop short in-person or hybrid/synchronous courses you can deliver internally or via an intranet

	c. Engaging continuous assessment for asynchronous courses and online commercial resources for phishing simulations. 7. **Gamified Cyber Security Training** a. introduction to gamification in cyber security training, basic cybersecurity training providers e.g., b. basic terms such as InfoSEC color wheel, bug bounty, CTFs and cyber ranges. c. ethics in cybersecurity training (responsible disclosure, simulation realism, and unintended harm.) 8. **Cybersecurity Fundamentals** a. basic cybersecurity vulnerabilities and attack vectors. b. hands-on experience working with core cybersecurity tools such as Kali Linux, Metasploit, Splunk, ELK Stack, Wireshark, Snort, and Suricata. With MITRE ATT&CK 9. **Methodology and Trends in Scenario Design** a. Overview of scenario design for cyber exercises, b. integrating technical, operational, and strategic dimensions to prepare teams for complex cyber challenges. c. understanding trends, addressing target audience maturity, realism, gamification and evaluation aspects. 10. **Introduction to cyber range BUTCA** a. introducing students to the Brno University of Technology Cyber Arena (BUTCA) platform. b. technological architecture of the BUTCA platform, its functioning, requirements and deployment options. 11. **Scenario Design in BUTCA** a. Creation of own scenarios for teaching purposes b. user graphical interface, the principle of operation of game scenarios, and how to incorporate real-time student analytics. 12. **Classroom communication and presentation skills for cybersecurity educators** a. Assessment methods b. peer feedback, reflective discussion, and evaluation

Exams and assessment formats	*40% in class engagement: 20% for a project and 20% for quizzes* *Final proctored exam (60 minutes) (60%)*
Reading list	*Harris, J.M. (2012): Presentation skills for teachers. Routledge.* *Hattie, J & Timperley, H, 2007, 'The Power of Feedback', Review of educational Research vol. 77, no. 1, pp 81-112.* *van Rooij, E.C.M., Jansen, E.P.W.A. & van de Grift, W.J.C.M. First-year university students' academic success: the importance of academic adjustment. Eur J Psychol Educ 33, 749–767 (2018). https://doi.org/10.1007/s10212-017-0347-8*

Cybersecurity Education and Training Delivery II

Module designation	*Cybersecurity Education and Training Delivery II*
Institution(s) involved	*UPB, UDS*
Relation to curriculum	*Elective; recommended module for: Educator*
Teaching methods	*Lecture, lab, seminar*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125h* *Contact hours: lecture: 12 hours, practice / laboratory session: 36 hours – each session consists of 1 hour lecture (mostly practical interactive demos) and 3 hours of assisted lab / practice session* *Private study including examination preparation, specified in hours: 77 hours - used for preparing for sessions, solving assignments, preparing for examination, self-study*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Technological Foundations for CS & Security Controls* *Cybersecurity Education and Training Delivery I* *- or equivalent knowledge, skills and competencies acquired through prior study or professional experience*
Module summary	*The "Cybsersecurity Education and Training Delivery II" module aims to build the required skills for students to be creators of practical cybsersecurity contests and use competition-based learning in their educator role. Students will learn how to design, implement, deploy and grade challenges as part of cybsersecurity contests (e.g. CTF – Capture the Flag). These are to be used as part of training and teaching activities that students will conduct themselves.*
Module objectives/intended learning outcomes	*On successful completion of this module the learner will be able to:* *LO1: Design practical cybersecurity exercises that serve as both a learning and a (self)assessment platform for participants* *LO2: Outline common patterns in cybersecurity attack and defense activities that can be replicated and integrated in cybersecurity exercises* *LO3: Develop, employ and asses practical cybersecurity exercises, both as single-topic challenges and as vulnerable*

	boxes that feature complex interconnected topics closer to a real-world setup *LO4: Combine patterns from existing cybersecurity exercises into new customized deployments* *LO5: Assess student practical cybsersecurity knowledge and skills and revise exercises according to their current level* *LO6: Design and set up cyber range-environments and CTF (Capture the Flag)-like contests, including setting up the platform, selecting challenges, grading, providing support* *LO7: Summarize and interpret results and feedback of practice activities*
Content	*1. Overview of cybersecurity practice activities: wargames, CTF contests & challenges, vulnerable boxes* *a. Typical structure of a practice activity: root account, the flag* *b. Types of challenges and structure: box, jeopardy, attack-defense (red team-blue team)* *c. Sample challenges, sample sites, walkthroughs* *2. Pedagogical Considerations Related to Practical Activities* *a. Practical exercises: definitions and roles* *b. Structuring practical exercises* *c. Four-step approach to teaching practical exercises* *3. Cybersecurity Practice Arsenal* *a. Web challenges arsenal* *b. Binary files arsenal* *c. Crypto arsenal* *d. Forensics arsenal* *4. CTF Cybersecurity Challenges* *a. Contents of a cybersecurity challenge* *b. Lifetime of a cybersecurity challenge* *c. Use cases for challenges as services* *d. Tips and tricks for reliable challenges as services* *e. Aftermath of a contest including a CTF cybersecurity challenges* *5. Deployment of CTF Challenges* *a. Scripting the deployment of challenges* *b. Deploying challenges on a remote system* *c. Using containers for deployment* *6. CTF Engines – CTFd.io* *a. CTF engines for contests* *b. Features of CTFd*

	c. Sample deployment of CTF challenges *7. Pedagogical Aspects of Contests and Competitions* *a. Contests, Competitions, Gamification, role in learning* *b. Competition-based learning* *c. Designing a competition for learning* *d. Assessing results* *8. Organizing and Deploying a CTF Contest* *a. Setting up a contest: dates, accounts, challenge selection, storyline, announcements* *b. Deploying challenges* *c. Providing support, hints, maintaining active communication* *d. Presenting results, awards* *9. Using Virtual Machines* *a. Virtual machines, benefits of virtual machines* *b. Automating work with virtual machines* *c. Using virtual machines as vulnerable boxes* *d. Validating a challenge inside the virtual machine* *10. Designing a Vulnerable Box Challenge* *a. Identifying vulnerabilities for challenge* *b. Designing the challenge* *c. Validating a challenge* *d. Packing a challenge for deployment* *11. Deploying Vulnerable Boxes* *a. Using a vulnerable box to set up the challenge* *b. Packing a virtual machine* *c. Publishing a virtual machine* *12. Assessment of Results of Cybersecurity Practice Activities* *a. Scoreboards for results* *b. Statistics of results: times, challenges solved, hints* *c. Adjustments to difficulty (points, rating)*
Exams and assessment formats	*Two take-home assignments (20% each)* - *Team projects* - *First assignment: Create and deploy 3 CTF challenges, review / solve other 3 CTF challenges (from other teams) - peer-review* - *Second assignment: Create and deploy a vulnerable virtual machine (vulnerable box); solve / review the deployment of another vulnerable box (from another team)*

	Final digitally proctored exam: 60% - practical exam (3 hours): setting up the infrastructure for a CTF-like contest and a vulnerable virtual machine
Reading list	*Cybersecurity Educational Resources: https://github.com/CSIRT-MU/edu-resources* *CTFd.io: https://ctfd.io/* *VulnHub (Vulnerable Virtual Machines): https://vulnhub.com/* *TryHackMe: https://tryhackme.com/* *Running practical exercises: https://facultyfocus.aoeducation.org/2018-03/assets/aof_booklet_running_a_practical_exercise.pdf* *Practical Pedagogy: 40 New Ways to Teach and Learn: https://www.routledge.com/Practical-Pedagogy-40-New-Ways-to-Teach-and-Learn/Sharples/p/book/9781138599819*

Cybersecurity in Industry – Security of OT and Cyber-Physical Systems

Module designation	*Cybersecurity in Industry – Security of OT and Cyber-Physical Systems*
Institution(s) involved	POLIMI/Cefriel, MTU
Relation to curriculum	*Free Elective*
Teaching methods	Expert lectures, lessons, audiovisual resources, collaborative work, technical materials, seminars, case study discussions, and flipped classrooms. Virtual lessons 18h; Audiovisual teaching resources 4h; Mentorship 2h; Collaborative work 9h; Case studies 15h; Study of the basic material 36h; Flipped classroom (preparation) 50h; Reading the supplementary material 10h; Final Examination 3h; Flipped classroom (presentation) 3h
Workload (incl. contact hours, self-study hours)	(Estimated) Total workload: *125hours* Contact Hours: *48 hours* Self-study: *71 hours* Examination: *6 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• Management & analytical skills, teamwork skills. • Fundamental theoretical knowledge of operating systems, computer networking, programming tools, and systems. • Basic understanding of the techniques for reverse code engineering, malware analysis and cyber risk modelling. • Basic understanding of the industrial control systems.
Module summary	This module aims to equip learners with comprehensive knowledge and practical skills in OT (Operational Technology) security, highlighting the differences and overlaps with IT (Information Technology) security. The focus will be on understanding key principles, risk modelling, and the legal and regulatory landscape, alongside developing skills to analyse, evaluate, and implement effective security measures in industrial environments.

<table>
<tr><td></td><td><strong>Learning Objectives</strong>:

This module provides a comprehensive overview of the essential knowledge, skills, and competencies necessary for addressing cybersecurity in Operational Technology (OT) environments, highlighting the unique challenges compared to IT security. It covers key concepts such as risk modeling specific to OT, legal and regulatory frameworks, and emerging technologies like AI, 5G, and IIoT. The ability to analyze OT's evolving threat landscape, assess industrial cyber risks, and evaluate real-world attack cases is emphasized, along with the need to apply relevant standards and best practices. Competencies include identifying vulnerabilities, synthesizing remediation measures, and managing continuous risk assessments, all while navigating the complexities of modern OT security governance and human-related threats.</td></tr>
<tr><td>Module objectives/intended learning outcomes</td><td><strong>Learning Outcomes</strong>: On successful completion of this module, the learner will be able to:<ul><li>LO1: Evaluate the principles and challenges of OT security, differentiate them from IT security, and align security strategies with industry standards and best practices.</li><li>LO2: Critically assess and compare the OT threat landscape with IT, including analysing specific tactics, techniques, and procedures used in OT-focused cyber-attacks.</li><li>LO3: Examine and evaluate recent case studies of cyber incidents in OT environments, drawing lessons on risk assessment and security countermeasures.</li><li>LO4: Analyse and apply relevant laws, regulations, and standards to develop robust OT security frameworks, incorporating the latest technological advancements such as AI, 5G, and IIoT.</li><li>LO5: Develop comprehensive risk models and security measures tailored to OT environments, ensuring effective governance and continuous risk assessment.</li><li>LO6: Assess the impact of human factors on OT security, identifying key vulnerabilities and synthesising remediation measures to strengthen the overall security posture.</li></ul></td></tr>
<tr><td>Content</td><td><table><tr><th></th><th>Lecture</th><th>Content</th></tr></table></td></tr>
</table>

	1	The overlapping and differences between IT and OT security 1/2	The module introduces the basic concepts of OT security. Gartner defines Operational Technology (OT) as “hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events”. OT differs from IT in terms of functionalities, the culture of operators, and threats. OT is a novel and rapidly expanding area for cybercrime and industry. The number of attacks against OT infrastructures is increasing; the pandemic and the geopolitical crisis played a considerable role because of the acceleration of digital transformation. For example, the reduction of on-site staff put a strain on OT systems and the already limited resources and required increased external connectivity. However, from a cybersecurity point of view, IT and OT need specific competence and sensibility. The primary need is an integrated approach that includes cybersecurity, physical and cyber-physical security, integrated cyber-risk estimation, and governance models spanning IT and OT domains.
	2	The overlapping and differences between IT and OT security 2/2	
	3	OT Threat Landscape	This module aims to increase comprehension of the OT threat landscape and its differences from the IT world. OT security is not an extension of IT security and requires a unique set of competencies. Nonetheless, threat actors use different Tactics and Procedures. Background knowledge, such as the

			ATT&CK framework, is presented.
	4	Tactics, techniques and procedures of the cybercrime and their evolutions ½	In the deep analysis of the tactics, techniques and procedures used by threat actors in the context of attacks against OT and cyber-physical systems. The specialised framework for industrial systems of the ATT&CK framework is used. The module also aims to perform reverse code engineering of the most prominent cases. According to the attendance, basic elements of reverse code engineering will be presented as a prerequisite to the malware analysis module. This module is intended for managerial profiles and not for technical profiles.
	5	Tactics, techniques and procedures of the cybercrime and their evolutions 2/2	
	6	Analysis of recent and paradigmatic attack cases and lessons learnt – flipped classroom 1/2	In this module, we'll look at different real-life examples, some of which come from students' homework. Students must study a piece of harmful software or a cyber-attack related to OT security. Then, students will share what they have learned with the rest of the class and the teachers in a flipped classroom approach.
	7	Analysis of recent and paradigmatic attack cases and lessons learnt – flipped classroom 2/2	
	8		This course is pivotal for understanding how to mitigate risks in integrated systems and protect against cyber and man-made threats. Even from a cyber risk modelling point of view, OT security is not an extension of IT security and re-

			quires a unique set of competencies. The module will analyse the differences among classic cyber risk modelling techniques and theory and modelling of cyber-physical systems, with particular attention to correlation among different types of risk and the cascading effects on non-cyber systems (e.g., risks of explosion, etc). The module also discussed the role of humans in human-related threats.
	9	Standards, best practices and EU laws for cybersecurity in the context of OT cybersecurity 1/2	Having a comprehensive view of the EU cybersecurity law framework specifically applicable to industry, the student will be able to determine if their industry and activities are subject to a particular piece of cybersecurity legislation, assess the extent of this applicability, and understand the key concepts and requirements necessary for achieving compliance and demonstrating accountability. EU laws that could specifically impact the industry in the Cybersecurity domain, such as the NIS 2 Directive, the Cybersecurity Act, the Cyber Resilience Act, the Medical Device Regulation(s), the EU Machinery Directive, and ISO reference standards such as ISO-62443.
	10	Standards, best practices and EU laws for cybersecurity in the context of OT cybersecurity 2/2	

<table>
<tr><td></td><td><table>
<tr><td>11</td><td>The impact of the new technologies 1/2</td><td rowspan="2">The field of OT is undergoing a phase of evolution where new solutions (e.g., AI, 5G, IIoT, Quantum Computing, Quantum Cryptography) are being developed. These new technologies particularly impact integrated IT and OT systems, where cyber risks could have cascading effects on non-cyber risks. The existing literature recognises the critical need for robust cybersecurity measures to safeguard against intentional threats and hybrid attacks. Traditional approaches often involve individually securing data flows, network layers, and software components, emphasising preventing unauthorised access and ensuring data integrity. The module will analyse and discuss the impact of these new technologies and present foreseen coming threats.</td></tr>
<tr><td>12</td><td>The impact of the new technologies 2/2</td></tr>
</table></td></tr>
<tr><td>Exams and assessment formats</td><td>• Flipped classroom Works: 50h preparation + 3h presentation (30%)
• Collaborative work: 9h (10%)
• Final proctored exam: 3h (60%)</td></tr>
<tr><td>Reading list</td><td>• Douglas W. Hubbard, Richard Seiersen, “How to Measure Anything in Cybersecurity Risk”, Wiley Press (2023)
• Smita Jain, Vasantha Lakshmi, “IoT and OT Security Handbook: Assess risks, manage vulnerabilities, and monitor threats with Microsoft Defender for IoT”, Packt Publishing (2023)
• Otis Alexander, Misha Belisle, Jacob Steele, “MITRE ATT&CK for Industrial Control Systems: Design and Philosophy”, MITRE (2020)
• Course material: case texts, teaching notes and exercises, slides.
• Suggested readings by the instructors.</td></tr>
</table>

Cybersecurity Law & Data Sovereignty (BUT)

Module designation	*Cybersecurity Law & Data Sovereignty (BUT)*
Institution(s) involved	*BUT, MTU*
Relation to curriculum	*Elective; recommended module for: Cyber Legal, Auditor*
Teaching methods	*Lesson*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125 hours* *Contact hours: 24 hours - lesson* *Private study including examination preparation: 101 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Basic understanding of cybersecurity principles, computer networks, and foundational knowledge of legal frameworks.*
Module objectives/intended learning outcomes	This course provides students with a comprehensive understanding of cybersecurity measures and related cybercrime aspects with a focus on EU regulation and international tools. Additionally, it covers data sovereignty, teaching students the regulations surrounding data handling, digital identity, and maintaining integrity in electronic document management. On successful completion of this module the learner will be able to: LO1: Understand and apply cybersecurity measures: Students will be able to understand and implement preventive and regulative measures in cybersecurity, particularly within the frameworks especially of the NIS 2 Directive, Cyber Resilience Act, Cyber Solidarity Act, and Cybersecurity Act. Students will also be able to work with and asses the regulatory framework based on particular case studies. LO2: Assess cybersecurity legal frameworks: Students will critically assess the links between national legal regulatory frameworks and international harmonization instruments in cybersecurity.

	LO3: Deploy legal tools for cybersecurity incidents: Students will be able to use legal tools and processes for handling and reporting cybersecurity incidents, especially in collaboration with cybersecurity incident response teams. LO4: Understand cybercrime investigation and prosecution: Students will comprehend the legal tools and processes for investigating and prosecuting cybercrime, particularly through international instruments like the Budapest Convention. LO5: Handle and transfer electronic evidence: Students will gain the ability to navigate European rules and procedures regarding the production and transfer of electronic evidence and understand its relevance in legal cases including relevant case law. LO6: Understand data sovereignty regulations: Students will be familiar with various legal regimes for data handling, including personal data transfer, electronic document management, and digital identity, with a focus on retaining integrity through the chain of custody.
Content	***Cybersecurity and Cybercrime*** *The content of this part of the module will cover the main concepts and structure of the cybersecurity law and criminal law applicable to cybercrime. The first area will include the theory and practice of cybersecurity obligations based on category of the regulated subject; liability for cybersecurity incidents; relevant case law; and tools for coordination and standardisation of cybersecurity compliance, such as cybersecurity certification. In the second area, we will cover relevant legal provisions of substantive and procedural criminal law; categorisation of cybercrimes; as well as European and international procedural tools used in investigation and prosecution of cybercrime.* ***Data Sovereignty*** *This part of the module is aimed at an in-depth exploration of the legal dimensions of specific aspects of data sovereignty and specific regimes applicable under the EU law. It prepares students to navigate the complex legal landscape in specific areas connected to various forms of data flows, in order to be able to ensure compliance in their professional practices within the EU. Apart from the regulatory regimes for processing personal data, participating in data spaces or doing business through online platforms, the content will include rules and requirements applicable to handling of electronic documents, including the relevance for constituting electronic evidence, and to the use of electronic identification and digital identity in particular in its application in the public law processes.*
Exams and assessment formats	*Final 2-hour proctored open book exam (60%)* *Class assignments (2x 10%)*

	In-class participation (20%)
Reading list	DAIMI, K., ALSADOON, A., PEOPLES, C., EL MADHOUN, N. Emerging Trends in Cybersecurity Applications. Springer. 2023. Available online for free: https://link.springer.com/book/10.1007/978-3-031-09640-2 LEHTO, M., NEITTAANMÄKI, P. Cyber Security. Critical Infrastructure Protection. Springer. 2022. Available online for free: https://link.springer.com/book/10.1007/978-3-030-91293-2#bibliographic-information NIST. National Checklist Program (NCP), 2022. (https://ncp.nist.gov/repository) FIRST CSIRT Services Framework. 2019. (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Machine and Deep Learning in Cybersecurity

Module designation	*Machine and Deep Learning in Cybersecurity*
Institution(s) involved	*UNIRI, UNIR*
Relation to curriculum	*Free Elective*
Teaching methods	*The teaching and learning strategy will consist of lectures, exercises, and focused activities such as videos, tutorials, case studies, practical assignments, and project work.* *Each week, students will attend a one-hour live lecture and a one-hour tutorial session with a hands-on demonstration of the practical part of the lecture. During the class, participants will be given tasks and exercises related to the covered content to be able to connect theory with practice. The live sessions will mainly involve explaining theoretical concepts with an emphasis on practical application to best use the lecturer's expertise in the classroom. Students will additionally have 2 hours of online activities every week aimed at mastering the concepts covered in the weekly topics. Directed activities consist of reading selected chapters from the book, listening to parts of the content in the form of videos, solving practical tasks, and solving homework that will be given in the exercises.* *Students will benefit from mentoring and formative feedback on completed activities and projects during class. All module resources will be available to students in a structured format through the LMS.*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125 hours* *Contact hours* • *Synchronous Lectures: 12 hours* • *Tutorial Sessions: 12 hours* • *Directed e-Learning Activities: 24 hours* *Independent learning and work on project: 77 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Automation of Security Tasks and Data Analytics - or equivalent knowledge, skills and competencies acquired through prior study or professional experience*
Module summary	This module focuses on applying machine learning and deep learning techniques to cybersecurity challenges such

	as anomaly and malware detection, fraud detection, and spam classification. Students will explore various machine learning algorithms, analyze their performance, and design appropriate models for specific cybersecurity tasks. The course also covers explainability issues in AI-driven cybersecurity, alongside hands-on labs using Python and popular libraries like Scikit-learn, TensorFlow, and PyTorch.
Module objectives/intended learning outcomes	*It is expected that after successfully completion of this module and fulfilling all the prescribed obligations, the student will be able to:* *LO1. Compare the advantages and disadvantages of basic machine learning algorithms, especially those related to classification, clustering, and time series analysis.* *LO2. Analyse and apply appropriate machine learning methods when solving specific problems such as anomaly or malware detection.* *LO3. Analyse and select deep learning methods that are suitable for the given task in the field of cybersecurity, such as spam detection, and credit card fraud detection.* *LO4. Evaluate the performance of the model and, based on that, choose the best machine or deep learning model for a given problem in the field of cybersecurity.* *LO5. Design and apply a machine or deep learning model for a self-defined problem in the field of cybersecurity.* *LO6. Discuss the possibility of applying machine or deep learning in cybersecurity and explain related problems such as explainability, interpretability, transparency, personal data protection, and legal and ethical challenges.*
Content	**Week 1: Introduction to Data Analytics and Machine Learning in Cybersecurity** • **Lecture:** Overview of ML in cybersecurity, Benefits, and challenges, use of cloud cases, mobile applications, and IoT. Anomaly detection, Malware detection, Ethical and legal aspects of AI • **Tutorial/ Lab:** Introduction to Python for machine learning: Scikit-learn, PyOD (Python Outlier Detection), Matplotlib, XGBoost, Prophet, **Week 2**: **Unsupervised machine learning: Clustering**

	• **Lecture:** K-means, distance measures, Hierarchical clustering, elbow method, dimensionality reduction, PCA, t-SNE • **Tutorial/ Lab:** Apply K-means clustering, and identify outliers based on the distance from the cluster centroids. Visualize the clusters and anomalies using scatter plots. Compare different distance measures. Apply hierarchical clustering (agglomerative). Visualize the dendrogram to identify clusters. Calculate the within-cluster sum of squares (WCSS) for each K, plot the WCSS values against the number of clusters to create the elbow plot. Apply PCA to reduce the dimensionality of features. Apply t-sne. **Week 3: Supervised machine learning: Classification** • **Lecture:** Decision trees, features, Partitioning train-test set. Cross-validation. Evaluation: accuracy, precision, recall, F-score, AUROC, Confusion matrix. Naïve Bayes, k-nearest neighbours • **Tutorial/ Lab:** Build a decision tree classifier using Scikit-learn. Visualize the decision tree to interpret the rules and splits. Partition dataset for the training-testing. Perform k-fold cross-validation. Evaluate the model. Calculate accuracy, precision, recall, and F-score, AUROC. Visualize the confusion matrix using a heatmap. Apply Naïve Bayes, k-nearest neighbours evaluate and compare results. **Week 4: Supervised machine learning: Classification** • **Lecture:** Support Vector Machines (SVM). Ensembles, Bagging. Boosting, Random Forest (RF). Feature importance. XGBoost • **Tutorial/ Lab:** Build SVM and random forest classifier using Scikit-learn. Feature importance Train XGBoost model. Tune the hyperparameters (e.g., learning rate, number of boosting rounds). Visualize classes. Unbalanced classes. **Week 5: Time series analysis** • **Lecture:** Trends, Seasons, Cycles. Smoothing, moving average (MA), Autoregressive Integrated Moving Average (ARIMA), Seasonal ARIMA (SARIMA). Evaluation: Mean Absolute Error (MAE): Mean Squared Error (MSE): Root Mean Squared Error (RMSE), R-squared (R^2), • **Tutorial/ Lab:** Fit time series model with Prophet. Fine-tune Prophet model parameters and evaluate performance

	MAE. MSE, RMSE, R2. Visualize. Apply seasonality and holidays. **Week 6: Anomaly detection** • **Lecture:** Unbalanced classes, fraud detection, intrusion detection, false positives vs. false negatives, feature engineering, time series detection, goodness of fit, and density-based methods. Isolation forest. • **Tutorial/ Lab:** Anomaly detection applications in Cybersecurity: Network Intrusion Detection, Fraud Detection, and System Monitoring. Apply Z-score normalization. Apply Isolation Forest and One-Class SVM for anomaly detection. Use prophet for time series analysis of anomalies. **Week 7: Neural networks** • **Lecture:** Artificial Neural Networks (neurons, layers, hidden layers, activation functions). Perceptron. A Multi-layer Perceptron. Feed-forward network. Detecting spam emails using MLP. Backpropagation. Evaluation metrics. • **Tutorial/ Lab:** Perceptron. Multi-layer perceptron. Testing the influence of different network structure and different activation functions to network performances on spam detection. **Week 8**: **Introduction to Deep Neural Networks** • **Lecture:** Basic architecture of Deep Neural Network. Network hyperparameters. Training of neural network. Epochs. Loss function. Analysing Results. Credit Card Fraud detection using deep neural network. • **Tutorial/ Lab:** Using environments and services to define deep neural network architecture (e.g. TensorFlow, Keras, PyTorch, Google Colab). Training of neural network for credit card fraud detection. Analysing Results. **Week 9: Biometric authentication** • **Lecture:** Convolutional neural networks (CNN). Biometric authentication using CNN. Data augmentation. Transfer learning. Optimization algorithms. Parameter regularization. Overfitting and generalization. • **Tutorial/ Lab:** Creating a simple deep convolutional neural network for biometric authentication, training the model

	and testing the influence of various hyper parameters and learning parameters to network performances. Evaluate performance using standard metrics. **Week 10: Adversarial Machine Learning** • **Lecture:** Adversarial attacks (Poisoning attacks, Evasion attacks, Model extraction attacks). Adversarial Machine Learning Examples. Popular Adversarial Attack Methods. Generative Adversarial networks (GAN). Deep fake. • **Tutorial/ Lab:** Using Deep fake and different GAN models for adversarial attacks on image classification. **Week 11: Transformers and emerging topics** • **Lecture:** Typical deep learning architectures and appropriate tasks (Recurrent neural network (RNN). Long Short-Term Memory (LSTM). Autoencoders. Attention. Transformers. Large language models. Using transformers for different cybersecurity tasks. • **Tutorial/ Lab:** Using different transformer networks and testing them on user behaviour analytic and biometric authentication tasks. **Week 12: Overview of Course Material, Class Discussion & Guest Lecture (optional)**
Exams and assessment formats	***Two midterm assessments*** • 1. proctored online quiz ML in week 7 (LO1, LO2, LO4, LO6) (25%) • 2. proctored online quiz DL in week 12 (LO3, LO4, LO5, LO6) (35%) ***Weekly (1,2,3,4,5,6,8,9,10,11) short computer-based quizzes*** (LO1 - LO6) (15%) ***Project assignment*** on selected ML topic in cybersecurity (e.g. anomaly detection, credit card fraud detection, (image) malware detection, biometric authentication, adversarial attack,...) with technical report and oral presentation (LO1 - LO6) (25%)
Reading list	***Recommended books.***

	Clarence Chio, David Freeman: Machine Learning and Security: Protecting Systems with Data and Algorithms, O'Riley, 2018. *Marwan Omar, Machine Learning for Cybersecurity, Springer, 2022.* *Ian Goodfellow, Yoshua Bengio, Aaron Courville Deep Learning (Adaptive Computation and Machine Learning series), The MIT Press, 2016.* *Emmanuel Tsukerman, Machine Learning for Cybersecurity Cookbook. Over 80 recipes on how to implement machine learning algorithms for building security systems using Python;Packt 2019.* ***Supplementary Books*** *Soma Halder and Sinan Ozdemir. Hands-On Machine Learning for Cybersecurity, Packt, 2018.* *Rajvardhan Oak, 10 Machine Learning Blueprints You Should Know for Cybersecurity, Packt 2023.* *Francois Chollet, Deep Learning with Python, Second Edition 2nd Edition, Manning, 2021.* ***LAB resources:*** *scikit-learn - Machine Learning in Python https://scikit-learn.org/stable/* *PyOD documentation! https://pyod.readthedocs.io/en/latest/* *XGBoost Documentation https://xgboost.readthedocs.io/en/stable/* *Prophet forecasting https://facebook.github.io/prophet/* TensorFlow https://www.tensorflow.org/ Keras https://keras.io/ PyTorch https://pytorch.org/ Google Colab https://colab.google/

Digital Forensics, Chain of Custody and eDiscovery

Module designation	*Digital Forensics, Chain of Custody and eDiscovery*
Institution(s) involved	UPB, UNIR
Relation to curriculum	*Elective; recommended module for: Cyber Legal, Auditor*
Teaching methods	*The teaching and learning strategy will consist of classes and directed activities such as videos, tutorials, case studies and discussions on the programme's Learning Management System (LMS). Each week students will begin by engaging with 1 hour of directed online activities aimed at introducing threshold concepts for that week's topic. Directed activities consist of short digestible pieces of content, such as explanatory videos, reading, guided tutorials, etc. Learners will then attend a live 1-hour lecture and a 1-hour tutorial session. Learners will be assigned tasks and exercises related to the directed content so that they can connect the theory to practice. Live sessions will mostly be practically based so as to make best use of the lecturer's expertise in the classroom. Learners will benefit from mentoring and formative feedback on completed directed activities during classes. All module resources are made available to learners in a structured format via the LMS.*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125 hours* *Directed e-Learning Activities: 12 hours* *Synchronous Lectures: 12 hours* *Tutorial Sessions: 12 hours* *Private study including examination preparation: 89 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Law, Compliance, Governance, Policy, and Ethics - or equivalent knowledge, skills and competencies acquired through prior study or professional experience*
Module summary	*This module aims to enable learners to develop a knowledge, skills and competence to approach a Digital Forensics investigation whilst safe-guarding the chain of custody of acquired digital forensic evidence. This module also aims to develop skills associated with eDiscovery. Learners will gain practical experience in using various tools used in Windows forensics, Linux forensics, mobile forensics, network forensics and eDiscovery. This module provides an in-depth*

<table>
<tr><td></td><td><i>coverage of various sub-domains of digital forensics and how it is related to eDiscovery.</i></td></tr>
<tr><td>Module objectives/intended learning outcomes</td><td><i>The Digital Forensics, Chain of Custody and eDiscovery module is intended to enable learners to develop knowledge, skills, and competences in digital forensics, as well as eDiscovery. From a practical perspective, learners develop expertise on a range of tools associated with mobile, network and the digital forensics of various operating systems. Furthermore, learners investigate and assess digital forensic case studies.</i>
<i>On successful completion of this module the learner will be able to:</i>
<i>LO1: Demonstrate in-depth critical awareness and interpretation of laws, compliance requirements, methods and procedures used in digital forensics investigations.</i>
<i>LO2: Carry out a forensic investigation of operating systems, mobile devices and networks, critically analyse the evidence and document the findings in a report.</i>
<i>LO3: Compare, evaluate and use forensic tools to forensically analyse digital devices.</i>
<i>LO4: Carry out an eDiscovery engagement across multiple platforms making use of various electronic discovery tools.</i>
<i>LO5: Critically analyse the results of an eDiscovery review, prepare production sets, write reports, and appraise the concepts for information retrieval and enterprise search technologies.</i></td></tr>
<tr><td>Content</td><td>
<table>
<tr><th></th><th>Lecture Topic</th><th>Detail</th></tr>
<tr><td>1</td><td>Introduction</td><td>Introduction to the module.
Principles of forensics, need of digital forensics, background to digital forensics, Computer crime.
Categories of incidents.
Cybercrime investigation.
Scenarios of eDiscovery and digital forensics investigations.</td></tr>
<tr><td>2</td><td>Digital forensics models and methodologies.</td><td>Digital evidence.
Direct and circumstantial evidence.
Types of data (content and non-content).
The digital forensics process.
Exemplar models and methodologies.</td></tr>
</table>
</td></tr>
</table>

			Standards and best practices.
	3	Digital Evidence	Sources of digital evidence and the investigation process. Evidence handling rules. ACPO principles of computer related evidence. Legal and ethical obligations. Handling digital evidence (Identification, Collection, Acquisition, Preservation) Triage and anti-forensics. Chain of custody. Need to maintain extensive documentation. Digital evidence admissibility (Assessment, Consideration, and Determination) Digital forensics report writing, typical parts, letter of findings, affidavits.
	4	Forensic Tools	Types of computer forensic tools, various tasks performed by forensic tools and its details. Drive imaging. Password cracking tools. Forensic workstation, choosing the forensic toolkit. Validating and testing forensic software, using NIST tools. Cloud platform challenges and considerations.
	5	Windows Forensics	Importance of operating system forensics. Relevant windows data structures. History of the windows registry, registry editor key, registry information.

			Tracking user activity by analysing shellbags and quick access/Recent Files Review bitlocker encryption and location of recovery keys.
	6	Network Forensics	Basics of network forensics When to apply network forensics. Key elements in communication. Network trace. Key concepts to interpret a network trace. IP and MAC addresses and networking infrastructure. Show how session keys (perfect forward secrecy) encryption/decryption works with RSA .Public Key encryption. Explain the role of deep packet inspection and web application firewalls in a network.
	7	Mobile Device Forensics	Mobile devices, mobile phones in crime, collecting a phone for analysis, data recovered from a mobile phone. Components of mobile phone. Accessing the data from a mobile phone. Tools used for mobile forensic analysis.
	8	Linux Forensics	Linux shell, linux boot sequence. Filesystems and disk/directory Encryption techniques. Important directories and sub-directories. File deletion in linux. Find Recently accesses/modified/changed files Log analysis /var/log/*
	9	Introduction to Electronic Discovery & Enterprise Search	What is discovery, how is conventional discovery different to eDiscovery. What is electronic discovery.

		Common challenges of electronic discovery. Examine Microsoft Purview or Gcloud Vault , eDiscovery platforms. Discuss Full-text search, Faceting, Nearest-Neighbour/Clustering. Highlighting of hits. Rich document handling. Document fields and schema design.
10	Electronic Discovery Reference Model	Discussing various phases of Electronic discovery reference model in detail. Information governance. Deduplication, keyword searching, technology assisted review (TAR), email threading, textual near duplicate identification.
11	Electronic Discovery Processes	Approaches to eDiscovery. Forms of electronically stored information. What constitutes evidence and what is metadata. Selecting an eDiscovery tool. Significance of quality assurance in eDiscovery practices. Email archiving/journaling.
12	Revision, catch-up and formative feedback	

Exams and assessment formats

Assessment Type	***Assessment Description***	***Outcome addressed***	***%***	***Assessment Date***
Continuous Assessment 1	*This assessment will consist of practical tasks in the form of a*	*LO1, LO2, LO3*	*40*	*Week 6*

<table>
<tr><td></td><td>
<table>
<tr><td></td><td><em>homework. This will assess learners' knowledge and competences on digital forensic processes, concepts and various tools used in digital investigations.</em></td><td></td><td></td><td></td></tr>
<tr><td><em>Continuous Assessment 2</em></td><td><em>A proctored assessment that will assess learner's knowledge and analytical skills regarding enterprise search and eDiscovery rules, processes, and platforms. Learners will conduct practical activities using various tools and write a report on their work.</em></td><td><em>LO4, LO5</em></td><td><em>60</em></td><td><em>Week 11</em></td></tr>
</table>
<p><em>Reassessment strategy:</em></p>
<p><em>The reassessment strategy for this module will consist of an assessment that will evaluate all learning outcomes.</em></p>
</td></tr>
<tr><td>Reading list</td><td>
<p><em>Recommended Book Reading</em></p>
<ul>
<li><em>G. Johansen, 2020, Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd edition, Packt Publishing [ISBN: 978-1838649005]</em></li>
<li><em>J. Seitz, T. Arnold (2021) Black Hat Python, 2nd Edition: Python Programming for Hackers and Pentesters, No Starch Press, [ISBN: 978-1718501126]</em></li>
</ul>
</td></tr>
</table>

Supplementary Book Reading

- *H. Carvey. (2016), Windows Registry Forensics, 2nd Edition, Syngress. [ISBN: 978-0128032916]*
- *N. Jaswal (2019), Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Packt Publishing, [ISBN: 978-1789344523]*

Other Resources

- *[website], CD-ROM: Live CD for Forensics, http://www.caine-live.net/*
- *[website], Forensic articles, http://www.forensickb.com/*
- *[website], COMPUTER FORENSIC RESOURCES, http://www.evestigate.com/COMPUTER%20FOR ENSIC%20RESOURCES.htm*
- *[website], Security Journals/Whitepapers https://securityjournaluk.com/*
- *[website], Forensic Focus, http://www.forensicfocus.com*
- *[website], Sans, http://www.sans.org*
- *[website] AI Powered Search. https://livebook.manning.com/book/ai-powered-search/about-this-meap/v-9/*
- *[website], Guide: Good Practice Discovery Guide - CLAI, https://clai.ie/wp-content/uploads/2021/10/CLAI-Good-Practice-Discovery-Guide-v2_0.pdf*
- *[website], Relativity One Discovery User Guide. https://help.relativity.com/RelativityOne/Content/index.htm*
- *[website], Microsoft Purview, Microsoft365 eDiscovery. https://learn.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide*
- *[website] Apache Lucene Solr https://github.com/mike-royal/Apache-Lucene-Solr-Guide*
- *[website], Autopsy Sleuth Kit. https://www.sleuthkit.org/autopsy/*
- *[website], Nist forensic sample images. https://cfreds.nist.gov/*
- *[website] Linux forensics cheatsheet http://www.security-hive.com/post/linux-forensics-the-complete-cheatsheet*

Threat Intelligence

Module designation	*Threat Intelligence*
Institution(s) involved	*UPB, UNIR*
Relation to curriculum	*Elective; recommended module for: Threat Intelligence*
Teaching methods	*Lesson, lab works, assignments*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* ***125h*** *Contact hours:* • ***lesson=10h,*** • ***lab=20h,*** • ***assignments=20h*** *Private study including examination preparation:* ***75h***
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Familiarity with Linux distributions, Python scripting* *Knowledge of C/C++, OS design is desirable*
Module summary	This module aims to introduce the fundamentals of Cyber Threat Intelligence (CTI). The lectures will present the CTI lifecycle, highlight strategic integration and discuss emerging trends in this field. The students will learn how to identify threat intelligence data streams, apply the extracted information for vulnerability assessment and threat mitigation, and disseminate newly acquired knowledge into public databases.
Module objectives/intended learning outcomes	**Learning Outcomes**: On successful completion of this module, the learner will be able to: • **LO1:** Recognize different types of cyber threats and apply analytical techniques to assess their potential impact. • **LO2:** Gather threat data from open-source and proprietary sources, as well as structure it according to their needs. • **LO3:** Incorporate threat intelligence into (automated) incident response processes, improving the detection, investigation, and mitigation of attacks. • **LO4:** Use specialized platforms and tools to analyze threat data and share relevant information.

	• **LO5:** Utilize the acquired intelligence to guide proactive threat hunting efforts with the goal of identifying potential compromises and indicators of attack.
Content	***Week 1:*** *Introduction to Cyber Threat Intelligence (CTI)* - ***Lecture:*** *Overview of CTI and its role in a modern security strategy. Present open-source / commercial threat intelligence feeds.* - ***Lab:*** *Deploy aggregators for threat intelligence data streams. Probe for emerging threats based on geolocation and other factors.* - ***Difficulty:*** *Introductory* ***Week 2:*** *CTI lifecycle and cybersecurity frameworks* - ***Lecture:*** *Present the phases of CTI and best practices to be applied at each stage. Discuss how CTI fits into frameworks such as MITRE ATT&CK and its integration with other areas in cybersecurity.* - ***Lab:*** *Become familiar with popular formats / schemas used in specifying Indicators of Compromise (IOC).* - ***Difficulty****: Introductory* ***Week 3:*** *Strategic planning* - ***Lecture:*** *Describe how to align CTI with the security goals and policies of an organization. Explain how to present security-related findings to non-technical stakeholders.* - ***Lab:*** *Automate information extraction from public databases and use OSS to generate reports.* - ***Difficulty****: Introductory* ***Week 4:*** *Vulnerability management* - ***Lecture:*** *Correlate threat intelligence with vulnerability detection to prioritize patching and mitigation. Present CVE databases.* - ***Lab:*** *Perform static, targeted malware detection based on publicly available signatures. Extend verification to an entire system.* - ***Difficulty:*** *Introductory* ***Week 5:*** *Advanced threat actor profiling* - ***Lecture:*** *Explain the notion of Threat Actors and how to build Adversary Profiles using historical data and behavioural patterns.*

	- ***Lab:*** *Generate rotating network captures for arbitrary time frames. Investigate user activity and automatically extract identifying features. Discuss honeypots.* - ***Difficulty:*** *Intermediate* ***Week 6:*** *Incident Response* - ***Lecture:*** *Present how CTI is used to guide Incident Response efforts. Discuss Intrusion Detection and Prevention Systems (IDP / IPS).* - ***Lab:*** *Configure an IDS / IPS to generate events or actively block traffic. Discuss its integration with the Linux network stack & the Netfilter Framework while considering the performance impact.* - ***Difficulty:*** *Advanced* ***Week 7:*** *The role of auditing in CTI* - ***Lecture:*** *Discuss the importance of data collection during the CTI lifecycle, as well as its analysis and dissemination. Present new approaches in this field, such as Data Provenance.* - ***Lab:*** *Introduction to the Linux audit system and its configuration for detecting anomalous behaviour.* - ***Difficulty:*** *Intermediate* ***Week 8:*** *Automation using Elastic Stack* - ***Lecture****: Introduction to Elastic Stack.* - ***Focus:*** *Configure the Logstash pipeline to collect and parse log entries from different sources. Pass the processed log data to an Elasticsearch cluster and visualise it via Kibana.* - ***Difficulty:*** *Advanced* ***Week 9:*** *Emerging trends and the future of CTI* - ***Lecture:*** *Present challenges facing CTI today. Discuss methods of applying Machine Learning techniques for the purpose of achieving predictive threat intelligence.* - ***Lab:*** *Introduction to containers and microservice environments. Present technical challenges created by namespaces and how to overcome them. Discuss methods of applying these solutions to Virtual Machine images.* - ***Difficulty:*** *Advanced* ***Week 10:*** *Review* - ***Lecture:*** *(optional) Guest speaker. Exam prep.* - ***Lab:*** *Review of previous activities.*

	- ***Difficulty:*** *N\A* ***Week 11-12:*** *Consolidation and Future Directions*
Exams and assessment formats	*60%: Digitally proctored Exam* *40%: Continuous Evaluation (e.g., weekly assignments, presentations, quizzes, practical exercises)*
Reading list	***Mandatory Reading:*** - *“The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence”* - *“The Diamond Model of Intrusion Analysis”* - *“Intelligence-Driven Incident Response: Outwitting the Adversary”*

Thesis

Module designation	*Thesis*
Institution(s) involved	UNI KO, UDS
Relation to curriculum	*Mandatory*
Teaching methods	Thesis
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 375 hours* *Contact hours: 24 hours (2 hours per week) in group sessions with all participants* *Self-study: 351 hours, including 1:1 meetings with the assigned thesis supervisor/topic expert*
Credit points	*15 ECTS*
Required and recommended prerequisites for joining the module	In order to enroll, students must have completed at least two mandatory taught modules and a minimum of 30 ECTS total. Completion of the "Research Methods" module is recommended, but not mandatory.
Module summary	After taking this module, you will have knowledge of research in your specialisation area. You will have an understanding of academic theory and the preparation of research pertinent to your field of study. You will be able to select appropriate research methods and techniques suitable for your research field. You will understand the current state of the art in your research area, and be able to appropriately employ methods and existing research results in the development of new knowledge, theories and presentation of research in your research area.
Module objectives/intended learning outcomes	By completing their thesis, students are expected to demonstrate advanced knowledge, skills, and competences across the full range of programme learning outcomes. As module-specific learning outcomes, students are expected to:

	LO1: Identify, formulate, and investigate a complex problem in the field of Cybersecurity Management and/or Data Sovereignty. **LO2**: Critically evaluate and synthesise relevant academic and professional literature. **LO3**: Apply appropriate design and research methods to develop, implement, and critically assess an innovative solution. **LO4**: Communicate findings and their implications clearly, both in written and oral form. **LO5**: Plan, manage, and complete an independent research or applied project responsibly, ethically, and within defined timeframes.
Content	**Week 1:** Introduction to the thesis template and structure; overview of learning outcomes; time-management tips. **Week 2:** Requirements for abstracts and problem statements; defining scope and objectives. **Week 3:** Literature review guidance; strategies for sourcing and evaluating references. **Week 4:** Research methodology: selecting suitable qualitative, quantitative, and/or design methods. **Week 5:** Data collection and analysis approaches; ethical and legal considerations. **Week 6:** Writing the methodology section; discussion of work-integrated projects if applicable. **Week 7:** Drafting results / solution sections; peer review of initial findings. **Week 8:** Discussion and conclusion sections - linking back to objectives; handling limitations; peer review of drafts. **Week 9:** Preparing references, appendices, and formatting; citation consistency. **Week 10:** Thesis integration workshop I; cross-review of drafts. **Week 11:** Thesis integration workshop II; cross-review of near-final drafts. **Week 12:** Oral defence preparation, presentation techniques, and feedback from peers.
Exams and assessment formats	Thesis assessment is regulated in the *Study and Examination Regulations* (Annex 2).

Reading list	The reading list depends on the individual thesis.

Onboarding: A Programme-Wide Resource Module

In addition to the standard modules outlined above – which carry ECTS credits and are classified as mandatory, profile-specific recommended, or pure electives – there is one special module dedicated to onboarding and continuous support.

Although the *Welcome Module* does not carry ECTS credits, it plays an essential role in helping students begin their academic journey with confidence and direction. It provides a structured and supportive introduction to the 60 ECTS Online Master's Programme in **Cybersecurity Management and Data Sovereignty**, the digital tools used, and the wider Digital4Security community. Students are strongly encouraged to engage with this module at the start of their studies and to revisit its resources throughout their learning journey.

Welcome Module

Module designation	*Welcome Module*
Term(s) in which the module is taught	Available continuously. It is recommended at the start of the programme, and for ongoing reference to access resources and stay updated with programme notifications.
Institution responsible for the module	UDS, with contributions by all partners
Relation to curriculum	Orientation and support module (non-credit bearing)
Teaching methods	Self-paced online module with video guides, readings, interactive tools, and optional forum participation
Workload (incl. contact hours, self-study hours)	Student-chosen (self-paced, asynchronous)
Credit points	0 ECTS
Required and recommended prerequisites for joining the module	None. Open to all students and staff

Module summary	This self-paced module provides a supportive introduction to the 60 ECTS Online Master's Programme in Cybersecurity Management and Data Sovereignty. It helps students familiarise themselves with the online learning environment, understand key academic resources and procedures, and develop effective habits for sustainable, self-directed learning. The module also provides access to comprehensive programme documentation, including the Study and Examination Regulations, Student Handbook, and related materials.
Module objectives / intended learning outcomes	By engaging with this module, students will be able to: • Navigate the Digital4Security platform and associated tools (e.g., Moodle, Full Fabric). • Become familiar with the programme's institutional partners, academic regulations, and student support services. • Know and apply best practices in online learning, self-organisation, and time management. • Evaluate and reference sources appropriately, including AI-generated content. • Know and utilise available tools to support well-being, creativity, and motivation in a remote learning environment. • Locate and navigate key programme documentation. • Stay informed about programme news, updates, and upcoming events. • Know whom to contact for questions or support.

Content	• Introduction to the programme, degree-awarding universities, and Digital4Security partners. • Orientation to digital tools and the online learning environment. • Guide to essential programme documents and academic regulations. • Overview of student services and points of contact. • Guidance on maintaining academic integrity and ethical research practices. • *Mindfulness for Online Learning:* ○ Tips for designing and choosing effective learning spaces. ○ Developing effective online study habits. ○ Resources and strategies to support continuous well-being. • *Brief Training in Academic Writing and Research:* ○ Draft structuring. ○ Finding and evaluating sources. ○ Ethical source use, and formal referencing. ○ Basic research methods. • Community-building activities and opportunities for engagement. • D4S resources including thesis and slide templates. • Event calendar. • Forum.
Exams and assessment formats	This module contains self-test materials, but no ECTS-relevant assessments. The module is neither mandatory nor elective, but contains training and support materials.
Reading list	Recommended Reading Material: – Student Handbook – Study and Examination Regulations – Module Handbook – Academic Staff CVs – Internal Quality Handbook – Industry Advisory Board Manual

Document Governance

Amendments to this **Module Handbook** are subject to consideration and approval by the Master's Board of Directors. Suggestions for refinement can be made by instructors, the Quality Service Committee, and other programme boards or individuals as appropriate.

Any proposed changes shall be collected and compiled by the Secretariat and prepared for inclusion in the official meeting invitations of the Master's Board, which are distributed at least two weeks prior to the meeting. Proposed changes shall be indicated using track changes in the document. Information on the proposer and the rationale for the change may optionally be included using the comment function.

Correspondence regarding proposed changes shall be addressed to **secretariat@digital4security.eu**, with **masters.board@digital4security.eu** copied in Cc. The Secretariat also supports the Master's Board in monitoring the full set of programme documents to ensure that any substantive changes, i.e. those not of an editorial nature, are duly reflected across all affected documents.

Those who wish to propose changes shall do so with consideration, taking into account the *"Fixed and Adjustable Elements in the Modules"* as outlined above.

Changes to the delivering institution or the accountable university for a module (the Module Guarantor) may only be made through formal programme updates, including the official re-versioning of the Module Handbook, and must be approved by the Master's Board of Directors.

The current document is designated as *Module Handbook, Version 1 (V1)*. Editorial changes, such as spelling corrections or updates to figures that do not alter their meaning, do not affect the version number. Version numbering remains unchanged until student agreements have been signed. Upon official publication, each version shall be dated; the version history shall be accessible to students, staff, and other relevant programme stakeholders from the initiation of version numbering, typically through a version history table.

Document Context and Publication

This **Module Handbook** forms part of a comprehensive set of materials that introduce, govern, and support the **60 ECTS Online Master's in Cybersecurity Management and Data Sovereignty**, a fully online joint programme coordinated and delivered by the following three higher education institutions:

- German University of Digital Science (UDS) – Coordinator
  Marlene-Dietrich-Allee 14, 14482 Potsdam, Germany
- Munster Technological University (MTU)
  Rossa Avenue, Bishopstown, Cork T12 P928, Ireland
- Universidad Internacional de La Rioja (UNIR)
  Avenida de la Paz 137, 26006 Logroño, Spain

The programme's structure, academic standards, quality assurance mechanisms, and operational procedures are described across the following documentation package:

Self-Assessment Report - a reference document for external evaluation and accreditation under the European Approach for Quality Assurance of Joint Programmes

I. Governance and Quality Assurance

- Annex 1. Cooperation Agreement
- Annex 2. Study and Examination Regulations
- Annex 3. Rules of Procedure for the Master's Board
- Annex 4. Internal Quality Handbook
- Annex 5. Programme Survey Scales
- Annex 6. Industry Advisory Board Manual

II. Curriculum, Learning and Teaching Staff

- **Annex 7. Module Handbook**
- Annex 8. Student Handbook

- Annex 9. Teaching Staff CVs
- Annex 10. Practical Guide for Lecturers

III. Certification and Recognition

- Annex 11. Sample Degree Certificate
- Annex 12. Sample Diploma Supplement

IV. Administrative and Operational Documents

- Annex 13. Sample Student Agreement
- Annex 14. Sample Supporting Partner Contract
- Annex 15. Sample Remuneration Manual

The programme documentation is maintained as follows:

- **SharePoint** serves as the repository for all programme documents.
- The **Welcome Module** publishes most programme documents (except those requiring protection against forgery or containing confidential information), ensuring transparency for enrolled students and staff.
- The **Digital4Security website** provides open access to selected information for prospective students and other interested parties, including admission requirements and procedures, the course catalogue, examination and assessment regulations, and other key programme details.

No.	Document	SharePoint	Welcome Module	Website
0	Self-Assessment Report	✓	✓	
1	Cooperation Agreement	✓	✓	
2	Study and Examination Regulations	✓	✓	✓
3	Rules of Procedure for the Master's Board	✓	✓	
4	Internal Quality Handbook	✓	✓	✓
5	Programme Survey Scales	✓	✓	

No.	Document	SharePoint	Welcome Module	Website
6	Industry Advisory Board Manual	✓	✓	(✓)
7	Module Handbook	✓	✓	(✓)
8	Student Handbook	✓	✓	✓
9	Teaching Staff CVs	✓	✓	
10	Practical Guide for Lecturers	✓	✓	
11	Sample Degree Certificate	✓		
12	Sample Diploma Supplement	✓		
13	Sample Student Agreement	✓	✓	
14	Sample Supporting Partner Contract	✓		
15	Sample Remuneration Manual	✓		

In the event of inconsistencies or conflicting interpretations among these documents, the following **order of precedence** applies:

1. Cooperation Agreement
2. Study and Examination Regulations
3. Rules of Procedure for the Master's Board
4. Internal Quality Handbook
5. Module Handbook
6. Student Handbook
7. Student Agreement
7. Programme Survey Scales
8. Supporting Partner Contracts
9. Other supporting documents

This hierarchy, as officially defined in the *Cooperation Agreement*, serves to ensure that foundational arrangements and formally adopted regulations take precedence over illustrative or operational materials.

Should the reader become aware of, or suspect, any inconsistency or misalignment between the documents, please contact Secretariat@digital4security.eu.

Together, these materials form the backbone of a transformative joint programme that seeks to integrate academic excellence, industry relevance, and social responsibility. It reflects the shared commitment of academic leaders, instructors, students, industry experts, and partner institutions, to shaping a student-centred, accessible, and future-oriented study environment.

This collective effort supports:

- **Empowering cybersecurity leaders** with the capacity to anticipate and manage risks, while collaborating effectively across stakeholders;
- **Delivering high-quality, flexible online learning** grounded in real-world application;
- **Supporting lifelong learning and workforce adaptability** in a rapidly evolving digital landscape;
- **Aligning education with industry and market needs** to ensure professional relevance;
- **Facilitating European strategic autonomy** through digital sovereignty and resilient infrastructure;
- **Advancing inclusion, accessibility, and gender equality** in the cybersecurity field; and
- **Promoting responsible innovation, ethics, and regulatory compliance** in all aspects of digital security.

We thank all contributors for their continued collaboration in advancing the Digital4Security vision: to empower learners, institutions, and societies in shaping a more secure, inclusive, and sovereign digital future.

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA). Neither the European Union nor the granting authority can be held responsible for them.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Digital4Security

Shaping Europe's cyber future

ADVANCED
DIGITAL SKILLS
DIGITAL EUROPE PROGRAMME

Co-funded by
the European Union