COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
Hack the Hackers: Detection and Defense Against Cyber Attacks	

Academic staff	Core academic unit(s)
Coordinating: Industrial Partnership Professor Dr. Stephen Fedtke **Other:** Assoc. Prof. Dr. Ilona Veitaitė	Kaunas Faculty Institute of Language, Literature and Translation Studies ☐ Institute of Social Sciences and Applied Informatics ☒

Study cycle	Type of the course unit
First ☒ Second ☐	Compulsory Course ☐ Optional Couse ☐ Course Unit (Module) of the General University Studies ☐ Course Unit (Module) of Individual Studies ☒ Interdisciplinary Studies Course Unit (Module) ☐

Mode of delivery	Semester or period when it is delivered	Language of instruction
Auditorium and self-work	Spring semester	English

Requisites	
Prerequisites: Fundamentals of Information System Security, Introduction to Programming, Information Systems and Databases, Computer Networks and their Security, WWW Development Technologies, Operational Systems and their Security, Legal Regulations for Cyber Security	**Co-requisites (if relevant):** Computer Architecture, Experience with virtual machines

Number of ECTS credits allocated	Student's workload (total)	Contact hours	Individual work
5	130	48	82

Purpose of the course unit
In this hands-on course students dive into the realities of modern cyber defense and related technologies. They will learn how monitoring and defense technologies capture events and detect threats in real time, and how security operations centers (SOCs) work with their security information and event management (SIEM) system. Thanks to a 360-scope of the lecture's content the students get in contact with both the defender's as well as the attacker's perspective, i.e., with the goals of both Red and Blue Team. Last but not least, they learn how leading organizations across Europe currently build resilient, compliant and state-of-the-art cyber defense infrastructures and which tools they use. The course gives the students opportunity to: • Understand how cyber attacks are detected in real time – and how professionals respond • Learn also the perspective of attackers to evade or bypass • Explore interdisciplinary aspects – from sensors, logs and connection with legal compliance • Gain hands-on experience with SIEM tools, including leading platforms like Splunk

• Develop skills relevant to careers in security operations, compliance, forensics, cyber insurance, auditing and more
• Investigate how AI is boosting both sides attackers and defenders
• Transfer the knowledge to other areas that are more specific and individual and which also demand security monitoring

Learning outcomes of the course unit	Teaching and learning methods	Assessment methods
Knowledge and its application: Understand the purposes, concept and goals of security monitoring capabilities, starting with intrusion detection & prevention up to XDR solutions	Active lectures; weekly assignments; guided and independent laboratory tasks; project-based individual and pair work; problem solving and debugging; peer presentations and feedback; roadmap-based self-evaluation; analysis of standards and official technical documentation. The live-insights are provided by inviting external parties, such as companies running active SOCs or providing corresponding services, or by external specialists in the field of cybersecurity.	Formative roadmap self-evaluations; most assignments request a video-based presentation of the work (length varies between 4 to approx. 8 minutes); all assignments are mandatory, the mean grade is taken as IPW (see below); laboratory checkpoints; one independent work presentation based on a selected assignment in front of the class to document, demonstrate and defend the work; written examination with applied examples at the end.
Knowledge and its application: Understand the purpose of a SIEM and become able to implement and operate an own SIEM for corresponding detections, sensors and dashboards		
Knowledge and its application: Understand the synergy among different standards and systematizations focusing on risks, vulnerabilities and more, such as MITRE-ATTCK, CVE, CWE, etc.		
Specialized skills: Understand the technical and organizational structure of a SOC and related workflows, including their limitations, such as due to legal regulations like GDPR		
Research skills: Lean how machine learning algorithms or even more powerful AI concepts and algorithms get part of cyber defense		

Content	Contact hours							Individual work: time and assignments	
	Lectures	Tutorials	Seminars	Workshops	Laboratory work	Internship	**Contact hours, total**	**Individual work**	**Tasks for individual work**
1. Basics related to cyber attack patterns and detection strategies	2				2		**4**	**7**	Investigation of log files and other event sources for evidences, definition of „catching“ patterns within the own SIEM, and more
2. Security and compliance monitoring essentials – from event data collection up via tools, watchers and other agents up to the auditor's perspective	2				2		**4**	**7**	Applying different watcher and agent technologies for capturing standard events like file tracking, and more
3. How regulations/standards like NIS-2, DORA, ISO-27001 demand monitoring and boost their importance	2				2		**4**	**7**	Determining the relevant sections and paragraphs asking for specific monitoring activities, and more
4. Hands-on lab-based implementation of SIEM, XDR (eXtended Detection and	2				4		**6**	**9**	Installing an open-source SIEM on a

Response), SOAR (Security Orchestration, Automation and Response) and related solutions and technologies									VM system, installing a SOAR solution on-top, later using the commercial Splunk SIEM solution, and more
5. Conceptual and operational challenges of running a SIEM or SOC	2				2		**4**	**7**	Running the own SIEM to monitor the „own IT empire“, and more
6. Real-world experience with SIEM technology & custom detections	2				2		**4**	**7**	Running the own SIEM to monitor the „own IT empire“, and more
7. Evaluation of detection and correlation algorithms	2				2		**4**	**7**	Implementing detections ranging from simple to complex, and more
8. Development of own sensor prototypes and connecting them to the SIEM	2				4		**6**	**10**	Developing an own basic sensor as a source of events, forwarding these events to the own SIEM, and more
9. Getting in contact with standards and organizations that comprehensively identify and systematize vulnerabilities and attack vectors	2				2		**4**	**7**	Examining MITRE, CVE and CWE based on sample risks, and more
10. Experiencing with best practice problems related to incident analysis	2				2		**4**	**7**	Creating own malicious code and corresponding detection patterns, and more
11. Exploiting AI to improve monitoring capabilities	2				2		**4**	**7**	Using ML/AI projects from Github and integrate them to the own SIEM, and more
Total	**22**				**26**		**48**	**82**	
Note: Up to 2 contact hours may be replaced by guest lectures given by social partners or educational visits to social partner organisations.									

Assessment strategy	Weight %	Deadline	Assessment criteria
Independent practical work based on assignments	30% (IPW)	During semester	The student has to process all assignments. For most assignments the student has to present the results in a corresponding video with a length from 4 to 8 minutes. Assessment considers the justification of the presented solution, its structure, usability and quality and the credibility of research, attribution of sources and media, accuracy and depth of the security explanation, real examples, original demonstration or tutorial, use of current evidence, audience engagement, peer feedback, presentation quality, and timely completion. Detailed criteria are provided in the assignment description. The assessment of assignments happens on the 10-point scale according to the assessment criteria of the VU. The **IPW** grade is determined as the mean value of all assignments. For up to 3 assignments, students may work in groups with maximum 2 members; the segregation of duties and split of work needs to be clearly determinable. Both need to appear

			in 1 common video, or both create individual videos. Any such collaboration needs to be announced in advance.
Life presentation & defense	30% (LPD)	During semester	Each student picks one assignment and presents his or her work in front of the class within 10 to 15 minutes, followed by a 5-minute discussion. Due to required coordination, presentations, and thus the selected topic, need to be announced and confirmed in advanc. The assessment of the life presentation happens on the 10-point scale according to the assessment criteria of the VU.
Exam	40% (E)	Exam session	The examination may be taken only after all mandatory assessed work has been completed. It covers the integrated theoretical and practical course material. Students answer written questions, explain technical decisions, interpret examples or code, and apply course concepts to practical web-development situations. The assessment of the exam happens on the 10-point scale according to the assessment criteria of the VU.
Final Grade = IPW*0,3+LPD*0,3+E*0,4			**Exam grade must be ≥**

REGARDING THE EXTERNAL EXAMINATION OF THE COURSE UNIT

Mark ☒					**If permitted, please provide the conditions**
Not permitted	☒	**Permitted**	☐		

REGARDING THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE (GenAI) TOOLS (SUCH AS "CHATGPT", ETC.) WHEN STUDYING THE COURSE UNIT

Mark ☒				**If permitted, please provide the conditions**
Not permitted	☒	**Permitted**	☒	The use of an Artificial Intelligence (AI) generative model is allowed but must be disclosed, so if an AI generative model has been used in a text, paper, program code, report or other work, this must be clearly stated (with appropriate citations and/or a declaration of the use of an AI generative model). Failure to disclose the use of an AI generative model in an academic work is considered academic dishonesty. In order to ensure that generative AI tools (ChatGPT, etc.) have not been used in the preparation of the essay (i. e. the content of the essay has not been generated by the AI tools), if not disclosed, the lecturer has the right to ask follow-up questions, to use the AI detection tools and, if necessary, to modify or cancel the grade of the assignment.

REGARDING ACADEMIC PROGRESS

A student who (1) **throughout the semester consistently** fails to demonstrate **progress in achieving the expected learning outcomes of a subject (module)** during the practical classes (seminars, exercises, laboratory work, etc.) and (2) fails to complete all interim assessment requirements and tasks within the time specified in the course description, is not allowed to participate in the examination session.

Author (-s)	**Publishing year**	**Title**	**Issue of a periodical or volume of a publication**	**Publishing house or web link**
Required reading				
Stallings, W., & Brown, L.	2018	Computer security: Principles and practice (4th ed.)		Pearson.
Anderson, R.	2020	Security engineering: A guide to building dependable distributed systems (3rd ed.)		John Wiley & Sons.
Seshagirirao Lekkala , Priyanka Gurijala	2024	Security and privacy for modern networks: Strategies and insights for safeguarding digital infrastructures		Apress (Springer Nature).
Recommended reading				

None				

NOTE: *Including Open Educational Resources in the reading list is recommended*