INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «16» iyul

INTERNATIONAL QUALIFICATIONS AND ASSESSMENT CENTRE
XALQARO MALAKALAR VA BAHOLASH MARKAZI
IQAC

Programme	**CYBER SECURITY DIPLOMA - LEVEL 7**		
Unit Number/ Unit Title	**UNIT 6 RESEARCH PROJECT / MASTER'S THESIS IN CYBER SECURITY**		
Cohort Code:	L07RPMC-U6		
Unit Level	Level 7		
Total GLH	Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110		
Credits	20 CATS/ 10 ECTS		
Lecturer			
Start Date		**End Date**	

Unit Aims	This capstone unit provides learners with the opportunity to undertake a major research or applied project in an area of their choice within cyber security. The focus is on contributing to academic, industry, or policy knowledge through original inquiry, practical innovation, or critical investigation.
Differentiation Strategies *(e.g. planned activities or support for individual learners according to their needs)*	The total number of students to be in the lesson is approximately 20. This is a multicultural group of students predominantly between the ages of 24 – 45, with numerous ethnic, gender, and creed background. These are UK academic level 5 students; hence it is assumed that they have practical, theoretical, or technological knowledge and understanding of a subject or field of work to find ways forward in broadly defined, complex contexts. These students must be able to generate information, evaluate, synthesise the use information from a variety of sources. Various approaches to addressing the various identified students needs will be adopted throughout the lesson. Such will include:- 1. Progressive tasks 2. Digital resources 3. Verbal support

	4. Variable outcomes 5. Collaborative learning 6. Ongoing assessment 7. Flexible-pace learning
Equality & Diversity	Variety of teaching techniques will be employed to ensure that the needs of each individual learner are met.
Safeguarding & Prevent	Safeguarding policies and the Prevent duty are strictly observed to ensure the safety, well-being, and inclusivity of all students and staff.
Health & Safety	SIRM H&S policies will be maintained.
Learning Resources	**Teaching and Learning Materials**
	• Oates, B. J. (2006). Researching Information Systems and Computing. • Saunders, M. et al. (2019). Research Methods for Business Students. • Runeson, P. & Höst, M. (2009). "Guidelines for Conducting and Reporting Case Study Research in Software Engineering." • IEEE Cybersecurity Research Publications. • ACM Digital Library Cybersecurity Proceedings.

Learning Outcome	Assessment Criteria
LO1. 1. Define and scope a research problem or applied challenge.	1.1 Formulate research questions or project objectives. 1.2 Conduct a literature review to identify research gaps.
LO2. 2. Design an appropriate methodology or implementation strategy.	2.1 Select qualitative, quantitative, or mixed methods. 2.2 Justify ethical, legal, and technical considerations.
LO3. 3. Collect, analyze, and interpret data.	3.1 Apply tools (e.g., SPSS, Python, Wireshark) as relevant. 3.2 Interpret findings in relation to existing knowledge.
LO4. **4. Present research or solution in academic and professional formats.**	4.1 Write a comprehensive dissertation/report. 4.2 Deliver an oral defense or solution demonstration.
LO5. 5. Reflect on project outcomes and personal learning.	5.1 Evaluate strengths, limitations, and implications of the work. 5.2 Reflect on skills gained and areas for development.

Week	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Research Problem Identification**	**Research Problem Identification** – Aligning with industry gaps or academic voids	LO1: Define and Scope a Research Problem	
2	**Formulating Research Questions/Hypotheses**	**Formulating Research Questions/Hypotheses** – SMART criteria for cybersecurity topics	LO1: Define and Scope a Research Problem	
3	**Literature Review Strategies**	**Literature Review Strategies** – Systematic reviews vs. meta-analyses	LO1: Define and Scope a Research Problem	
4	**Tools for Scholarly Research**	**Tools for Scholarly Research** – Google Scholar, IEEE Xplore, Scopus, Snowballing	LO1: Define and Scope a Research Problem	
5	**Workshop: Annotated Bibliography**	**Workshop: Annotated Bibliography** – Critical analysis of 10+ key papers	LO1: Define and Scope a Research Problem	
6	**Research Proposal Drafting**	**Research Proposal Drafting** – Title, objectives, significance, and scope	LO1: Define and Scope a Research Problem	
7	**Research Methodologies**	**Research Methodologies** – Qualitative (case studies), quantitative (surveys), mixed methods	LO2: Design Methodology/Implementation Strategy	
8	Review	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Experimental Design**	**Experimental Design** – Lab setups, simulations, or real-world deployments	LO2: Design Methodology/Implementation Strategy	

10	**Ethical & Legal Compliance**)	**Ethical & Legal Compliance** – IRB approval, data privacy (GDPR/HIPAA considerations)	LO2: Design Methodology/Implementation Strategy	
11	**Technical Feasibility Assessment**	**Technical Feasibility Assessment** – Tools, datasets, and resource requirements	LO2: Design Methodology/Implementation Strategy	
12	**Workshop: Methodology Justification**	**Workshop: Methodology Justification** – Defending choices for peer review	LO2: Design Methodology/Implementation Strategy	
13	**Risk Mitigation Planning**	**Risk Mitigation Planning** – Addressing bias, data limitations, and validity threats	LO2: Design Methodology/Implementation Strategy	
14	Review	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics		
15	Midterm	- **Midterm assessment** covering all learning outcomes (theory and practical elements)		
16	Feedback & Reflection	- Review - Individual feedback on performance - Reflective discussion on key learning points		
17	**Data Collection Techniques**	**Data Collection Techniques** – Surveys, honeypots, logs, or attack simulations	LO3: Data Collection, Analysis, and Interpretation	
18	**Quantitative Tools**	**Quantitative Tools** – SPSS, R, or Python (Pandas, SciPy) for statistical analysis	LO3: Data Collection, Analysis, and Interpretation	
19	**Qualitative Tools**	**Qualitative Tools** – NVivo, thematic coding for interview/observational data	LO3: Data Collection, Analysis, and Interpretation	

20	**Network/Threat Analysis**	**Network/Threat Analysis** – Wireshark, Suricata, or malware sandboxing	LO3: Data Collection, Analysis, and Interpretation	
21	**Workshop: Data Visualization**	**Workshop: Data Visualization** – Tableau, Matplotlib for impactful findings	LO3: Data Collection, Analysis, and Interpretation	
22	**Triangulation & Validation**	**Triangulation & Validation** – Cross-verifying results with multiple methods	LO3: Data Collection, Analysis, and Interpretation	
23	Review	**Thesis Structure & Academic Writing** – IMRAD format, citation styles (APA/IEEE)	LO4: Academic/Professional Presentation	
24	**Technical Report Writing**	**Technical Report Writing** – Executive summaries, glossaries, and appendices	LO4: Academic/Professional Presentation	
25	**Conference Paper Submission**	**Conference Paper Submission** – Abstract, keywords, and peer-review simulation	LO4: Academic/Professional Presentation	
26	**Oral Defense Preparation**	**Oral Defense Preparation** – Slide design, Q&A handling, and demo rehearsals	LO4: Academic/Professional Presentation	
27	**Critical Self-Evaluation**	**Critical Self-Evaluation** – Limitations, biases, and unexpected challenges	LO5: Reflection and Future Work	
28	**Research Impact Assessment**	**Research Impact Assessment** – Contributions to academia/industry, policy implications	LO5: Reflection and Future Work	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	