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 6**		
Unit Number/ Unit Title	**UNIT 2 CYBER THREAT INTELLIGENCE AND DIGITAL FORENSICS**		
Cohort Code:	L06CTID-U2		
Unit Level	Level 6		
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 unit provides learners with advanced knowledge and applied techniques in cyber threat intelligence (CTI) and digital forensics. The module focuses on identifying, analysing, and responding to cyber threats using intelligence frameworks (e.g., MITRE ATT&CK, Diamond Model) and conducting forensically sound investigations. Learners will develop competencies in threat analysis, memory and disk forensics, artefact extraction, and reporting to support legal, operational, or policy responses.
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**
	• Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press. • Giura, P., & Wang, W. (2012). Using threat intelligence to reduce risk. IEEE International Conference on Technologies for Homeland Security. • MITRE Corporation. (2023). MITRE ATT&CK Framework. • Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The Art of Memory Forensics. Wiley. • Bejtlich, R. (2013). The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press.

Learning Outcome	Assessment Criteria
LO1. 1. Analyse the role of threat intelligence in organisational cyber defence.	1.1 Evaluate threat intelligence frameworks (e.g., MITRE ATT&CK, Cyber Kill Chain). 1.2 Assess how CTI informs security operations and risk mitigation strategies.
LO2. 2. Collect and evaluate threat data using open-source and commercial intelligence tools.	2.1 Use tools (e.g., MISP, ThreatConnect) to gather indicators of compromise (IOCs). 2.2 Correlate threat data to detect emerging threats and attack patterns.
LO3. 3. Apply forensic procedures to collect, preserve and analyse digital evidence.	3.1 Perform disk, memory, and network forensics following chain-of-custody protocols. 3.2 Extract and interpret artefacts using forensic tools (e.g., Autopsy, Volatility, FTK).
LO4. 4. Conduct root cause analysis and incident response.	4.1 Determine the origin and timeline of incidents based on forensic artefacts. 4.2 Recommend containment and remediation strategies based on forensic findings.
LO5. 5. Communicate findings through professional forensic and intelligence reports.	5.1 Structure forensic reports to meet technical, legal, and executive requirements. 5.2 Present intelligence summaries using visual tools and dashboards (e.g., Kibana, Maltego).

Week	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Cyber Threat Intelligence (CTI)**	**Introduction to Cyber Threat Intelligence (CTI)** Definition, types (strategic, tactical, operational), and lifecycle.	LO1: Threat Intelligence in Cyber Defense	
2	**Threat Intelligence Frameworks**	**Threat Intelligence Frameworks** MITRE ATT&CK Matrix: Tactics, Techniques, and Procedures (TTPs).	LO1: Threat Intelligence in Cyber Defense	
3	**Cyber Kill Chain Analysis**	**Cyber Kill Chain Analysis** Lockheed Martin's 7-stage model vs. modern adaptations (e.g., Unified Kill Chain).	LO1: Threat Intelligence in Cyber Defense	
4	**CTI in Security Operations**.	**CTI in Security Operations** Enhancing SIEM, EDR, and threat hunting with intelligence feeds.	LO1: Threat Intelligence in Cyber Defense	
5	**Risk Mitigation Strategies**	**Risk Mitigation Strategies** Using CTI for vulnerability prioritization and proactive defense.	LO1: Threat Intelligence in Cyber Defense	
6	**Case Study: APT Group Profiling**	**Case Study: APT Group Profiling** Analyzing nation-state actors (e.g., APT29, Lazarus Group) through CTI.	LO1: Threat Intelligence in Cyber Defense	
7	**Threat Intelligence Sources**	**Threat Intelligence Sources** OSINT (Open-Source INT), dark web monitoring, and vendor feeds.	LO2: Threat Data Collection & Analysis	
8	**Review**	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**IOC Collection & Management**	**IOC Collection & Management** Tools: MISP (Malware Information Sharing Platform),	LO2: Threat Data Collection & Analysis	

		ThreatConnect.		
10	**Threat Data Correlation**	**Threat Data Correlation** Identifying patterns using STIX/TAXII standards and threat graphs.	LO2: Threat Data Collection & Analysis	
11	**Emerging Threat Detection**	**Emerging Threat Detection** Machine learning in CTI (e.g., anomaly detection, clustering).	LO2: Threat Data Collection & Analysis	
12	**Threat Feeds Integration**	**Threat Feeds Integration** Automating IOC ingestion into SIEM/SOAR platforms.	LO2: Threat Data Collection & Analysis	
13	**Hands-on Lab: Building Threat Feeds**	**Hands-on Lab: Building Threat Feeds** Creating custom IOCs from malware analysis.	LO2: Threat Data Collection & Analysis	
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	**Forensic Investigation Principles**	**Forensic Investigation Principles** Chain of custody, evidence integrity, and legal admissibility.	LO3: Digital Forensics Fundamentals	
18	**Disk Forensics**	**Disk Forensics** Tools: Autopsy, FTK (Forensic Toolkit), and file system analysis (NTFS/EXT4).	LO3: Digital Forensics Fundamentals	
19	**Memory Forensics**	**Memory Forensics** Volatility Framework: Process trees, malware artifacts, and rootkit detection.	LO3: Digital Forensics Fundamentals	
20	**Network Forensics**	**Network Forensics** PCAP analysis with Wireshark, Zeek, and network flow tools.	LO3: Digital Forensics Fundamentals	

21	**Mobile & Cloud Forensics**	**Mobile & Cloud Forensics** Challenges in iOS/Android and cloud environments (AWS/Azure logs).	LO3: Digital Forensics Fundamentals	
22	**Live System Forensics**	**Live System Forensics** Using Redline/KAPE for triage and volatile data collection.	LO3: Digital Forensics Fundamentals	
23	**Review**	**Incident Response Phases** Preparation, identification, containment, eradication, recovery (NIST SP 800-61).	LO4: Incident Response & Root Cause Analysis	
24	**Timeline Reconstruction**	**Timeline Reconstruction** Using log analysis (Splunk, ELK) and forensic artifacts.	LO4: Incident Response & Root Cause Analysis	
25	**Malware Reverse Engineering**	**Malware Reverse Engineering** Static/dynamic analysis to uncover attack origins (IDA Pro, Ghidra).	LO4: Incident Response & Root Cause Analysis	
26	**Remediation Strategies**	**Remediation Strategies** Patching, credential resets, and network segmentation recommendations.	LO4: Incident Response & Root Cause Analysis	
27	**Forensic Reporting**	**Forensic Reporting** Writing technical reports for legal/executive audiences (ENISA guidelines).	LO5: Reporting & Communication	
28	**Visualizing Threat Intelligence**	**Visualizing Threat Intelligence** Dashboards (Kibana, Maltego), heat maps, and attack timelines.	LO5: Reporting & Communication	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	