INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «___» _____

Programme	**CYBER SECURITY DIPLOMA - LEVEL 7**		
Unit Number/ Unit Title	**UNIT 3 AI-DRIVEN THREAT DETECTION AND AUTONOMOUS RESPONSE SYSTEMS**		
Cohort Code:	L07ADTD-U3		
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 unit introduces learners to the use of Artificial Intelligence and Machine Learning for detecting, predicting, and responding to cyber threats. The course emphasizes practical design of intelligent systems for security operations centers (SOC), threat hunting, and automated remediation tools.
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**
	• Sommer, R. & Paxson, V. (2010). "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection." IEEE Symposium. • Ussath, M. et al. (2019). "Automated Incident Handling: A Survey of SOAR Technologies." Journal of Cyber Security Technology. • Scarfone, K. & Mell, P. (2007). NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems. • Russell, S. & Norvig, P. (2020). Artificial Intelligence: A Modern Approach. • Goodfellow, I. et al. (2014). Explaining and Harnessing Adversarial Examples.

Learning Outcome	Assessment Criteria
LO1. 1. Understand the fundamentals of AI/ML in cyber security.	1.1 Describe supervised, unsupervised, and reinforcement learning models. 1.2 Identify applications of AI in intrusion detection and response.
LO2. 2. Develop intelligent threat detection models.	2.1 Build ML models for anomaly detection. 2.2 Evaluate performance metrics (e.g., precision, recall, ROC- AUC).
LO3. 3. Assess the effectiveness of autonomous response mechanisms.	3.1 Review SOAR platforms and auto-remediation strategies. 3.2 Analyse limitations of AI-driven security automation.
LO4. **4. Mitigate adversarial AI risks.**	4.1 Explain adversarial machine learning and evasion tactics. 4.2 Propose defenses against model poisoning and spoofing.
LO5. 5. Design an AI-based cyber defence system.	5.1 Integrate ML pipelines into SOC workflows. 5.2 Present a working prototype or architecture blueprint.

Week	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to AI/ML in Cybersecurity**	**Introduction to AI/ML in Cybersecurity** – Key concepts, history, and evolution	LO1: Understand the fundamentals of AI/ML in cybersecurity	
2	**Supervised Learning for Security**	**Supervised Learning for Security** – Classification (malware detection, phishing)	LO1: Understand the fundamentals of AI/ML in cybersecurity	
3	**Unsupervised Learning for Anomaly Detection**	**Unsupervised Learning for Anomaly Detection** – Clustering, autoencoders	LO1: Understand the fundamentals of AI/ML in cybersecurity	
4	**Reinforcement Learning in Cyber Defense**	**Reinforcement Learning in Cyber Defense** – Adaptive threat response	LO1: Understand the fundamentals of AI/ML in cybersecurity	
5	**AI Applications in IDS/IPS**	**AI Applications in IDS/IPS** – Case studies (Darktrace, Vectra AI)	LO1: Understand the fundamentals of AI/ML in cybersecurity	
6	**Limitations of AI in Security**	**Limitations of AI in Security** – Bias, false positives, and interpretability	LO1: Understand the fundamentals of AI/ML in cybersecurity	
7	**Data Preprocessing for Security**	**Data Preprocessing for Security** – Feature engineering, log normalization	LO2: Develop intelligent threat detection models	
8	Review	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	

9	**Building Anomaly Detection Models**	**Building Anomaly Detection Models** – Isolation Forest, One-Class SVM	LO2: Develop intelligent threat detection models	
10	**Behavioral Analysis with ML**	**Behavioral Analysis with ML** – UEBA (User and Entity Behavior Analytics)	LO2: Develop intelligent threat detection models	
11	**Evaluating Model Performance**	**Evaluating Model Performance** – Precision, recall, F1-score, ROC-AUC	LO2: Develop intelligent threat detection models	
12	**Real-Time Threat Detection**	**Real-Time Threat Detection** – Streaming data analysis (Kafka, Spark)	LO2: Develop intelligent threat detection models	
13	**Lab: Detecting Malware with Random Forest/XGBoost**	**Lab: Detecting Malware with Random Forest/XGBoost**	LO2: Develop intelligent threat detection models	
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	**SOAR Platforms Overview**	**SOAR Platforms Overview** – Palo Alto XSOAR, IBM Resilient	LO3: Assess autonomous response mechanisms	
18	**Automated Incident Response**	**Automated Incident Response** – Playbooks, auto-containment	LO3: Assess autonomous response mechanisms	
19	**AI in Endpoint Protection**	**AI in Endpoint Protection** – CrowdStrike, SentinelOne case studies	LO3: Assess autonomous response mechanisms	
20	**Ethical and Legal Risks of Automation**	**Ethical and Legal Risks of Automation** – False positives, liability	LO3: Assess autonomous response mechanisms	

21	**Lab: Simulating Autonomous Response with TheHive + Cortex**	**Lab: Simulating Autonomous Response with TheHive + Cortex**	LO3: Assess autonomous response mechanisms	
22	**Debate: Human-in-the-Loop vs. Full Automation**	**Debate: Human-in-the-Loop vs. Full Automation**	LO3: Assess autonomous response mechanisms	
23	**Review**	**Capstone Project** – Prototype an AI threat detection system (e.g., phishing detector, network anomaly alert system)	LO4: Mitigate adversarial AI risks	
24	**Adversarial Machine Learning**	**Adversarial Machine Learning** – Evasion (FGSM), poisoning attacks	LO4: Mitigate adversarial AI risks	
25	**Defending AI Models**	**Defending AI Models** – Adversarial training, robust feature selection	LO4: Mitigate adversarial AI risks	
26	**Case Study: Fooling Facial Recognition/ML Malware Detectors**	**Case Study: Fooling Facial Recognition/ML Malware Detectors**	LO4: Mitigate adversarial AI risks	
27	**Lab: Generating Adversarial Samples with CleverHans**	**Lab: Generating Adversarial Samples with CleverHans**	LO5: Design an AI-based cyber defense system	
28	**Architecting AI-Driven SOCs**	**Architecting AI-Driven SOCs** – Integrating SIEM + ML pipelines	LO5: Design an AI-based cyber defense system	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	