INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «__» _____

Programme	**CYBER SECURITY DIPLOMA - LEVEL 6**		
Unit Number/ Unit Title	**UNIT 5 AI AND AUTOMATION IN CYBER SECURITY**		
Cohort Code:	L06AACS-U5		
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 explores how artificial intelligence (AI), machine learning (ML), and automation technologies are applied to cyber defence. Learners will gain hands-on experience with anomaly detection, automated threat hunting, and integrating AI into security operations (SOC). The module prepares students for roles in modern SOCs where intelligent automation is key to threat mitigation.
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. (2022). Automated Defenses in Modern SOCs. IEEE Security & Privacy. • Chio, C., & Freeman, D. (2018). Machine Learning and Security. O'Reilly Media. • Sculley, D. et al. (2015). Hidden Technical Debt in ML Systems. Google Research. • ENISA (2023). AI Cybersecurity Challenges. • IBM Security. SOAR and AI Playbooks Documentation.

Learning Outcome	Assessment Criteria
LO1. Understand AI and ML principles in cyber security.	**Written Exam:** 1.1 Explain supervised, unsupervised, and reinforcement learning in cyber contexts. 1.2 Compare traditional vs. AI-powered detection models.
LO2. Apply machine learning models for threat detection.	**Project-Based Assignment:** 2.1 Train and evaluate ML models using threat datasets. 2.2 Interpret model accuracy, precision, and recall.
LO3. Integrate AI tools within SOC workflows	**Practical Lab:** 3.1 Use SIEM/SOAR platforms with AI-driven playbooks (e.g., Splunk, IBM QRadar). 3.2 Automate alert triage and incident response.
LO4. Assess ethical and privacy implications of AI in security.	**Written Report:** 4.1 Analyse bias, accountability, and explainability challenges. 4.2 Propose mitigation strategies to ensure responsible use.
LO5. Evaluate emerging trends in cyber automation and autonomous defense.	**Group Presentation:** 5.1 Present a review of emerging AI-based defence platforms. 5.2 Forecast industry changes due to intelligent automation.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to AI in Cyber Security**	**Introduction to AI in Cyber Security**: Use cases, benefits, and limitations.	LO1: Foundations of AI/ML in Cyber Security	
2	**Supervised Learning**	**Supervised Learning**: Classification models (e.g., Random Forest, SVM) for malware detection.	LO1: Foundations of AI/ML in Cyber Security	
3	**Unsupervised Learning**	**Unsupervised Learning**: Clustering (e.g., K-means) for anomaly detection in network traffic.	LO1: Foundations of AI/ML in Cyber Security	
4	**Reinforcement Learning**	**Reinforcement Learning**: Adaptive threat response (e.g., automated patching).	LO1: Foundations of AI/ML in Cyber Security	
5	**Traditional vs. AI-Powered Detection**	**Traditional vs. AI-Powered Detection**: Rule-based (IDS/IPS) vs. behavioral analytics (UEBA).	LO1: Foundations of AI/ML in Cyber Security	
6	**Feature Engineering for Cyber Datasets**	**Feature Engineering for Cyber Datasets**: Selecting relevant indicators (e.g., logs, packet headers).	LO1: Foundations of AI/ML in Cyber Security	
7	**Data Preprocessing**	**Data Preprocessing**: Handling imbalanced datasets (e.g., SMOTE), normalization.	LO2: ML Models for Threat Detection	
8	**Review**	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Model Training**	**Model Training**: Using frameworks like TensorFlow/PyTorch with cyber datasets (e.g., CIC-IDS2017).	LO2: ML Models for Threat Detection	
10	**Model Evaluation Metrics**	**Model Evaluation Metrics**: Accuracy, precision, recall, F1-score, and ROC curves.	LO2: ML Models for Threat Detection	

11	**False Positives/Negatives Trade-offs**	**False Positives/Negatives Trade-offs**: Tuning thresholds for SOC efficiency.	LO2: ML Models for Threat Detection	
12	**Deep Learning for Cyber Security**	**Deep Learning for Cyber Security**: CNNs for image-based malware analysis, RNNs for log parsing.	LO2: ML Models for Threat Detection	
13	**Threat Intelligence Integration**	**Threat Intelligence Integration**: Enriching ML models with threat feeds (e.g., MITRE ATT&CK).	LO2: ML Models for Threat Detection	
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	**SIEM with AI**	**SIEM with AI**: Splunk ES, IBM QRadar with Watson, Microsoft Sentinel ML.	LO3: AI in SOC Automation	
18	**SOAR Platforms**	**SOAR Platforms**: Playbook automation (e.g., Palo Alto Cortex XSOAR, TheHive).	LO3: AI in SOC Automation	
19	**Automated Alert Triage**	**Automated Alert Triage**: Prioritization using ML (e.g., phishing email classification).	LO3: AI in SOC Automation	
20	**Incident Response Automation**	**Incident Response Automation**: AI-driven containment (e.g., isolating compromised hosts).	LO3: AI in SOC Automation	

21	**Chatbots for SOC**	**Chatbots for SOC**: Virtual analysts (e.g., Darktrace Antigena, IBM Watson Assistant).	LO3: AI in SOC Automation	
22	**Red Team Automation**	**Red Team Automation**: AI-powered penetration testing tools (e.g., BloodHound ML).	LO3: AI in SOC Automation	
23	**Review**	**AI in Zero Trust Architectures**: Continuous authentication with behavioral biometrics.		
24	**Bias in AI Models**	**Bias in AI Models**: Addressing skewed training data (e.g., demographic biases in fraud detection).	LO4: Ethical and Privacy Challenges	
25	**Explainability (XAI)**	**Explainability (XAI)**: Techniques like LIME/SHAP for SOC transparency.	LO4: Ethical and Privacy Challenges	
26	**Accountability & Legal Risks**	**Accountability & Legal Risks**: GDPR "right to explanation" and liability for AI failures.	LO4: Ethical and Privacy Challenges	
27	**Privacy-Preserving AI**	**Privacy-Preserving AI**: Federated learning, differential privacy for sensitive data.	LO4: Ethical and Privacy Challenges	
28	**Autonomous Cyber Agents**	**Autonomous Cyber Agents**: Self-healing networks, AI-driven honeypots, and future outlook.	LO5: Emerging Trends & Autonomous Defence	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	