MODULE DESCRIPTOR

Module Title

AI & Cyber Security

Reference	CM4143	Version	1
Created	November 2023	SCQF Level	SCQF 10
Approved	May 2019	SCQF Points	15
Amended	July 2022	ECTS Points	7.5

Aims of Module

This module aims to equip students with the abilities to evaluate and apply methods, tools, and techniques used in Artificial Intelligence (AI) to tackle cybersecurity challenges.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Communicate a critical comprehension of both the data science process lifecycle and the machine learning engineering pipeline.
2	Critique various machine learning algorithms applied in the field of cyber security.
3	Develop an understanding of the security features of machine learning products
4	Develop machine learning solutions for defensive and offensive security.

Indicative Module Content

The case for AI in security. ML engineering pipeline, Data sets and Data types in security (e.g. structured vs unstructured, labelled vs unlabelled, overfitting vs underfitting, class imbalance, biased). ML product development lifecycle (e.g. TDSP or CRISP-DM). ML types (e.g. supervised, unsupervised, reinforcement). ML tasks (e.g. classification, clustering, regression, dimension reduction, density estimation, deep learning). Popular ML algorithms (e.g. LDA, CART, SVM, Naive bayesian, KNN, K-means, Random forests, Genetic algorithms, ANNs, Autoencoder). Applications of AI in both defensive and offensive security contexts, breaking CAPTCHA, identifying malicious URLs, detecting malware/ransomware, spotting phishing/spam emails, recognizing network traffic anomalies and DOS attacks, and identifying credit card fraud, Programming in Python and using relevant tools and libraries. Limitations and challenges in applying AI to security, recommended guidelines for its application, an introduction to adversarial AI, and considerations for the security of AI products.

Module Delivery

Key concepts are introduced and illustrated through lectures. The necessary practical skills are developed through a series of laboratory exercises.

Module Ref:	CM4143 v1

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4
Description:	Students will design and implement a Machine Learning solution for a specified defensive or offensive security challenge.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade of D is required to pass this module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1.
B	The student needs to achieve a B in Component 1.
C	The student needs to achieve a C in Component 1.
D	The student needs to achieve a D in Component 1.
E	The student needs to achieve an E in Component 1.
F	The student needs to achieve an F in Component 1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1. HALDER, S. and OZDEMIR, S., 2018. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem. Birmingham, UK: Packt Publishing.
2. PALOMARES CARRASCOSA, I., Kalutarage, H.K and Huang, Y., eds., 2017. Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications. Springer.
3. STAMP, M., 2017. Introduction to machine learning with applications in information security. Chapman and Hall/CRC.
4. Parisi, A. (2019). Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd.
5. Hu, F., & Hei, X. (Eds.). (2023). AI, Machine Learning and Deep Learning: A Security Perspective. CRC Press.
6. Badhwar, R. (2021). The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms (pp. 3-378). Springer.
7. Alazab, M., & Tang, M. (Eds.). (2019). Deep learning applications for cyber security. Springer.