Prifysgol Wrecsam
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM666
Module Title	Security Optimisation & Automation
Level	6
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
BSc (Hons) Cyber Security	Core
BSc (Hons) Cyber Security with Industrial Placement	Core

Pre-requisites

None

Breakdown of module hours

Learning and teaching hours	12 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	12 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**24** hrs
Placement / work based learning	0 hrs
Guided independent study	176 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023
With effect from date	Sept 2026
Date and details of revision	
Version number	1

Module aims

The module aims to explore the intersection of security optimisation and automation in modern digital environments. Students will delve into the application of machine learning algorithms and models to enhance security measures and automate various security processes. They will gain an understanding of how machine learning can be used for threat detection, anomaly detection, and pattern recognition in security systems. Additionally, students will learn how to leverage machine learning to optimise security controls, such as access management, authentication, and intrusion detection. Through practical exercises and real-world examples, students will develop the skills to design and implement machine learning-based security solutions, ensuring effective protection against evolving cyber threats. By the end of the module, students will be proficient in integrating machine learning techniques into security optimization and automation strategies, bolstering the overall resilience and effectiveness of organisational security measures.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Demonstrate security optimization principles and automation techniques.
2	Analyse the benefits and limitations of using machine learning in security optimisation and automation.
3	Utilise and apply machine learning techniques for threat detection, anomaly detection, and pattern recognition in security systems.
4	Evaluate the performance of machine learning algorithms in detecting and mitigating security threats.
5	Design and propose security solutions and automated approaches using machine learning.

Assessment

Indicative Assessment Tasks:
This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The assessment strategy for this module is portfolio based which involves students compiling a robust portfolio that showcases their understanding, application, and synthesis of the module's content. The portfolio would include a variety of artifacts, such as written reports, incident response plans, case analyses, reflective journals, and practical exercises.
One of the portfolio tasks may entail students configuring a machine learning application for securing a virtual server, including a documented journal of the process they applied.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,3,4,5	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience.

Indicative Syllabus Outline

Indicative syllabus includes topic areas that may include:

- Security Optimisation and Automation
- Machine Learning Fundamentals for Security
- Automation of Threat and Anomaly detection
- Pattern recognition in Security Systems
- Security control optimisation using Machine Learning
- Automation of Security Processes
- Ethical Considerations

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

R. Martinez, *Incident Response with Threat Intelligence.* Packt Publishing, 2022

Other indicative reading

S. Halder & S. Ozdemir, *Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem*. Packt Publishing. 2019.
C. Chio, & D. Freeman, *Machine Learning and Security: Protecting Systems with Data and Algorithms.* O'Reilly Media. 2018.