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	COM660
Module Title	Threat Detection and Incident Response
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

N/A

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 on Threat Detection and Incident Response aims to equip students with a solid understanding of the principles, techniques, and best practices related to identifying and mitigating cybersecurity threats. The primary objective of the module is to enable students to develop the necessary skills to effectively detect, analyse, and respond to security incidents within a variety of organisational contexts. Additionally, the module aims to cultivate students' abilities to investigate and assess security incidents, develop incident response plans, and implement reasonable and appropriate remediation measures.

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

1	Analyse the various methods, frameworks and techniques used in threat detection and incident response.
2	Evaluate the effectiveness of threat detection mechanisms and incident response strategies.
3	Apply threat detection tools and technologies to identify and analyse potential security threats.
4	Analyse the root causes and impact of security incidents to determine appropriate remediation measures.
5	Utilize industry guidelines and best practices to develop incident response strategies.

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 primarily focused on a portfolio assessment approach, constituting 100% of the overall assessment weight. Throughout the module, students would be required to complete regular portfolio tasks, which could include tasks such as conducting threat assessments, analysing simulated incidents, developing incident response plans, and documenting incident analysis and resolution processes. These tasks would be aligned with the module's learning outcomes and designed to provide opportunities for students to showcase their understanding, critical thinking, problem-solving skills, and practical application of concepts and techniques.

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:

- Incident handling process
- Computer Security Incident Handling Guide (NIST SP 800-61)
- Principles of incident management (ISO/IEC 27035)
- Intrusion Analysis
- Intrusion Classification
- Data and Event analysis
- DevSecOps & Cloud security
- Incident Response Tools and Technologies
- Incident response lifecycle

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: Practical insights into developing an incident response capability through intelligence-based threat hunting.* Roberto Martinez. Packt Publishing. 2022.

Other indicative reading

G. Johansen, *Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response,* 3rd Edition. Packt Publishing. 2022.
V. C. Gazcon, *Practical Threat Intelligence and Data-Driven Threat Hunting.* Packt Publishing. 2021.