Module Specification

Cyber Threat Analysis

Version: 2026-27, v1.0, 20 Jan 2025

Contents

Part 1: Information

Module title: Cyber Threat Analysis

Module code: UFCEHV-15-2

Level: Level 5

For implementation from: 2026-27

UWE credit rating: 15

ECTS credit rating: 7.5

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: The Cyber Threat Analysis module equips students with the knowledge and skills necessary to analyse cyber threats, assess security risks, and develop effective mitigation strategies. Through theoretical study and practical application, students will gain an insight into different cyber incident response processes, ethical considerations, and security management principles.

Features: Not applicable

Educational aims: Develop a comprehensive understanding of cyber threat intelligence analysis, incident response processes, and evidence collection techniques.

Explore ethical principles and professional standards in the context of cybersecurity practice.

Acquire skills in developing security management plans and policies to mitigate identified risks.

Enhance communication abilities to effectively convey cyber threat analysis findings and recommendations.

Outline syllabus: Cyber threat intelligence analysis: horizon scanning, sources of threat intelligence, and vulnerability assessment.

Incident response processes: cyber incident response frameworks, evidence collection, and preservation.

Ethical principles in cybersecurity: codes of conduct, professional responsibilities, and ethical decision-making.

Security management systems: governance structures, policies, standards, and guidelines e.g. Data Protection Act 2018, Fair Use, Acceptable Use.

Part 3: Teaching and learning methods

Teaching and learning methods: Lectures covering theoretical concepts in cyber threat analysis, supplemented by practical exercises, case studies, and group discussions.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Analyse and interpret cyber threat intelligence to identify security risks and vulnerabilities.

MO2 Apply and evaluate incident response processes and evidence collection techniques to support cyber threat investigations.

MO3 Develop effective security management plans and policies to mitigate identified risks and ensure compliance with ethical principles.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 144 hours

Face-to-face learning = 36 hours

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/02EE62F0-FAF0-EC90-FA6B-DDD0A05CD0F8.html

Part 4: Assessment

Assessment strategy: Students are required to complete a 2000 word report on a simulated cyber threat analysis scenario, covering threat intelligence analysis, incident response processes, ethical considerations, and security management plans.

Tutor-led formative feedback will be provided throughout the module to support students in their learning and assignment preparation.

Resit opportunities should follow the same format. Where appropriate, assessment re-work may be considered.

Assessment tasks:

Report (First Sit)

Description: 2000 word report on a simulated cyber threat analysis scenario, covering threat intelligence analysis, incident response processes, ethical considerations, and security management plans.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Report (Resit)
Description: 2000 word report on a simulated cyber threat analysis scenario, covering threat intelligence analysis, incident response processes, ethical considerations, and security management plans.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Networking [UCW] FdSc 2025-26