Module Specification

Cyber Security Intelligence

Version: 2025-26, v1.0, 19 Sep 2023

Contents

Part 1: Information

Module title: Cyber Security Intelligence

Module code: UFCE58-30-3

Level: Level 6

For implementation from: 2025-26

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field:

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: Cyber security is an ever-evolving module where experts must deal with change impacted by various methods, such as the advancement of technology and changes in laws and regulation. Students will gain an understanding of the key concepts regarding incident management, including the professional, legal, ethical, and moral responsibilities that come with dealing with security incidents.

This module aims to prepare students on how to deal with an incident within the company, how to mitigate risk and the prevention of incidents.

Features: Not applicable

Educational aims: We aim to provide students with an understanding of the professional, legal, ethical, and moral aspects within cyber security. Students will be provided with a series of workshops which will allow students to engage in supported horizon scanning to identify and evaluate potential threats, opportunities, and future developments within a business scenario. Students will further be provided with an opportunity to identify and explore emerging trends within cyber security.

Outline syllabus: · Network monitoring and logging techniques and technologies
· How attack techniques and vulnerabilities manifest in network monitoring and logging systems
· Network monitoring and logging techniques and technologies
· The relative merits of manual and automated techniques
· The relative merits of signature-based anomaly detection and algorithmic anomaly detection
· Importance of cryptography within cyber security and the usage of practical cryptography tools (digital signatures, asymmetric and symmetric encryption, password storage)
· How to communicate with internal and/or external incident response teams, and/or customers

Part 3: Teaching and learning methods

Teaching and learning methods: Learning and teaching will come in two main forms, lectures, and lab exercises. During lectures, theoretical aspects of the module will be discussed to provide students with an understanding of the theory behind the techniques used within cyber security.
Lab exercises are designed to utilise the theory discussed in lectures and allow students to demonstrate their understanding through guided research and practical tasks. Labs also serve as an environment for requirement clarification, facilitating

discussion and further research. Students are expected to carry out the work independently outside the classes.

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

MO1 Demonstrate a broad understanding of system logging and auditing and how they may be used to mitigate risks facilitate a cyber security investigation.

MO2 Demonstrate knowledge of incident responses in accordance with moral and ethical requirements within cyber security.

MO3 Identify and understand cryptographic tools and current trends and challenges within cyber security.

MO4 Isolate, manage and recover compromised system using a range of tools and techniques

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

Face-to-face learning = 72 hours

Total = 300

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link

Part 4: Assessment

Assessment strategy: This module consists of two assessments: a 1-hour multiple choice exam based upon scenarios, followed by a series of 3 Cyber Security Laboratory assessments and summative laboratory reports.

ONLINE EXAM
The first assessment consists of a 1-hour multiple-choice exam, where students will be quizzed on their knowledge of cyber security and current legislation affecting

cyber security through questions relating to a business scenario, the application of current cyber security methodologies and practical techniques, and the usage of cryptography within cyber security.

PORTFOLIO
The second assessment will consist of a portfolio of three 1-hour practical labs and accompanying reports, one of which may be completed in a small group/pairs. Upon completion of each lab, students will be required to complete a short summary/evaluation (approx. 600 words) evaluating the key technologies used.

The resit opportunity should follow the same format as the first assessment. Consideration should be given to re-working the practical assessments as appropriate. Where group work is not possible tasks should be scaled appropriately.

Assessment tasks:

Examination (Online) (First Sit)
Description: 1 hour multiple choice exam based upon scenarios.
Weighting: 25 %
Final assessment: No
Group work: No
Learning outcomes tested: MO3

Portfolio (First Sit)
Description: 3 x 1-hour practical security labs with completed documentation.
Weighting: 75 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2, MO4

Examination (Online) (Resit)
Description: 1 hour multiple choice exam based upon scenarios.
Weighting: 25 %
Final assessment: No

Group work: No

Learning outcomes tested: MO3

Portfolio (Resit)

Description: 3 x 1-hour practical security labs with completed documentation.

Weighting: 75 %

Final assessment: Yes

Group work: Yes

Learning outcomes tested: MO1, MO2, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Digital and Technology Solutions (Cyber Security Analyst) {Apprenticeship-UCW} [UCW] BSc (Hons) 2023-24