Module Specification

Cyber Security Analytics

Version: 2026-27, v2.0, Approved

Contents

Part 1: Information

Module title: Cyber Security Analytics

Module code: UFCFFY-15-M

Level: Level 7

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: In many organisations, the role of a cyber security analyst is to help protect an organisation by deploying a range of techniques and processes that can help to prevent, detect and manage cyber threats. Such threats may relate to network-based attacks and malware attacks, where an external actor is attempting to gain access to confidential information, or conducting a denial of service attack to compromise availability of services. Other threats may include insider threats, including the leaking of company secrets, data exfiltration, and accidental or social

engineering attacks. This module will study the role of cyber security analytics, covering the technologies used in industry, the role of data analytics, statistics and machine learning to support analytical reasoning, and the domain-specific attributes relating to networking, malware and insider threat analysis, including the development of analytical testing environments and the use of industry-based tools to examine these threats.

Features: Not applicable

Educational aims: This module helps students to understand the importance of data analytics in the context of cyber security. Through practical examples, students will learn to use software tools and coding techniques to work with data, so that they can identify, assess and mitigate against cyber threats. The overarching aim is to gain experience of real-world technologies that are used by industry professionals, giving you valuable skills in the role of a cyber security analyst.

Outline syllabus: Topics are likely to include but are not limited to:
Role of a cyber security analyst and common tools used
Security Operations, Frameworks, and Monitoring techniques
Security Information and Event Management (SIEM) and virtualised environments for security analysis
Machine learning for cyber security
Data visualisation for cyber security
Case studies of cyber security analytics

Part 3: Teaching and learning methods

Teaching and learning methods: Teaching will be delivered using a variety of methods, including lectures, discussion groups, and practical lab activities. Online materials will support the delivery of in-person teaching. Students will have on-campus discussion and practical sessions where students will be encouraged to discuss and develop the ideas and concepts that build upon lecture content. Students will also be supported in the completion of practical exercises, that will help inform their ability to undertake module assignments.

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

MO1 Demonstrate critical understanding of the role and processes adopted by a cyber security analyst.

MO2 Develop advanced practical skills for data analysis processes to identify and analyse a variety of cyber security threats.

MO3 Communicate advanced understanding of tools and techniques used by cyber security professionals.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 117 hours

Face-to-face learning = 33 hours

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/modules/ufcffy-15-m.html

Part 4: Assessment

Assessment strategy: Students will undertake a series of practical activities for investigating cyber security threats. By applying data analytics techniques, both through code-based analysis and through software tooling, students will learn how to analyse data and identify threats. Students will then communicate their findings to evidence the relevance of the practical skills in the context of becoming a cyber security professional.
The practical tasks have been selected to cover a variety of challenge that may be faced, including not limited to, network traffic analysis, malware classification, and insider threat detection. Students are expected to work on individually-assigned cases, and work on individually-driven research in later stages of the module.

Practical sessions throughout the module serve as formative feedback to support

students through non-assessed exercises, that will help them to develop their assessed work.

The resit assessments will match the first sit.

Assessment tasks:

Practical Skills Assessment (First Sit)
Description: Set of practical tasks.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Practical Skills Assessment (Resit)
Description: Set of practical tasks.
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 [Frenchay] MSc 2026-27

Cyber Security [Frenchay] MSc 2026-27

Cyber Security [Frenchay] MSc 2026-27

Cyber Security [Frenchay] MSc 2026-27

Cyber Security [GCET] MSc 2026-27

Cyber Security {with International Pre-Masters} [UWEBIC] MSc 2026-27