Module Specification

Cyber Security Analytics

Version: 2024-25, v2.0, 20 May 2024

Contents

Part 1: Information

Module title: Cyber Security Analytics

Module code: UFCFFY-15-M

Level: Level 7

For implementation from: 2024-25

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:

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 will help students to understand the role of data analytics in the context of cyber security. It will address the common job role of cyber security analyst, often working security operations environments, and focus on the tasks and practices required for to examine, identify, assess and mitigate against active cyber threats. The module will introduce tools and techniques to support this function, including Security Incident and Event Management (SIEM) systems, and practical programming tasks for examining common threats in data streams such as networking traffic and computer activity.

Outline syllabus: - 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 understanding of the role of a cyber security analyst, the processes required, and the variety of tasks, tools and techniques.

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

MO3 Demonstrate practical skills that address a clear career path into technical aspects of cyber security.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 117 hours

E-learning/online learning = 11 hours

Total = 0

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/4A801EB0-30E6-4F2C-2F6F-6B7D0BF6E540.html

Part 4: Assessment

Assessment strategy: Students will produce a practical portfolio of work as their final module assessment, worth 100% of the module. Portfolio tasks will build cumulatively through practical worksheets issued during the course. Students will learn the end-to-end process of data generation, collection, aggregation, analysis, and response, using a practical experimental testbed that they have designed and developed. As part of the portfolio task, students will be expected to demonstrate the functionality of their system.

Where a resit of the module is required, the data samples and the expected indicators of compromise will differ from the main run of the module. Similar to the

main run, students will be expected to develop the different stages of the analytical process, and document this through portfolio work including a video demonstration.

Assessment tasks:

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

Portfolio (Resit)
Description: Portfolio 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 [GCET] MSc 2024-25

Cyber Security [Frenchay] MSc 2024-25

Cyber Security [Frenchay] MSc 2024-25