Module Specification

Cyber Security Analytics

Version: 2023-24, v2.0, 23 May 2023

Contents

Part 1: Information

Module title: Cyber Security Analytics

Module code: UFCFFY-15-M

Level: Level 7

For implementation from: 2023-24

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

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: Purpose of a cyber security analyst, and common tools used
- Python, Bash, Linux, Wireshark, tshark, tcpdump

Security Information and Event Management (SIEM) and Security Orchestration and Automated Response (SOAR) tools
- Splunk, ELK, SecurityOnion

Intrusion detection and Intrusion Prevention
- Snort, Suricata

Development of virtualised simulation environments for generating and analysing data
- VMware, Scapy, custom scripting

Big data analytics for cyber security, machine learning concepts
- Unsupervised, supervised

Use cases of cyber security analytics

- network traffic analysis, malware analysis, user behavioural analysis, linguistic analysis

Part 3: Teaching and learning methods

Teaching and learning methods: Teaching will be delivered using a variety of methods, including online lectures, accompanying documentation, and exercise lab sheets. 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 Understand and critically assess the role of a cyber security analyst, the tools and techniques deployed in industry, and the requirements of the role.

MO2 Analyse, assess and protect systems in a controlled virtualised environment through cyber security simulation and incident response.

MO3 Critically evaluate the current state-of-the-art, including big data analysis and machine learning techniques, to assess the strengths and weaknesses of current methods.

MO4 Demonstrate practical skills that address a clear career path into cyber security, including systems configuration, programming skills, data processing, and contextualisation of threats.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 117 hours

E-learning/online learning = 11 hours

Total = 150

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, starting with initial design and configuration of an experimentation testbed, integration with a SIEM, generation and analysis of sample data, and investigation and response to some security incident. 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 through a narrated video demonstration.

Where a resit of the module is required, students will be required to develop a suitable end-to-end experimental testbed for the analysis of security incident data, using a SIEM platform. 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 with companion video presentation.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4

Portfolio (Resit)

Description: Portfolio of practical tasks with companion video presentation.

Weighting: 100 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security [Frenchay] MSc 2023-24

Cyber Security [Frenchay] MSc 2023-24

Cyber Security [GCET] MSc 2023-24