Module Specification

Cyber Security Engineering

Version: 2024-25, v1.0, 24 Jan 2024

Contents

Part 1: Information

Module title: Cyber Security Engineering

Module code: UFCE87-15-3

Level: Level 6

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: 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: Cyber Security Engineers operate at the advance level of the cyber career pathways utilising a range of skills including penetration testing, networking security and secure programming. To work as an effective Cyber Security Engineer you need to be able to manage threats and vulnerabilities within existing infrastructure, stay current with cyber security trends and events, while maintaining good working practice as a developer so you can at minimum read and understand code (often in multiple languages). Being able to understand what an application or

service does and where potential vulnerabilities or flaws could be introduced is a key skill.

This module will cover the skills required to become a Cyber Security Engineer in industry. Students will identify and resolve vulnerabilities within existing infrastructure and practice responding to and mitigating active threats commonly experienced in industry.

Features: Not applicable

Educational aims: This module will confirm understanding covered in previous modules, building on existing knowledge of networking, security tools and programming skills.

Students will explore and understand core skills within the career pathway of a Cyber Security Engineer through a combination of lectures and practical sessions.

By the end of the module students will have used their skills to identify and resolve vulnerabilities within existing infrastructure and defend against common threats and attack techniques.

Outline syllabus: This module will cover aspects of the following:

Vulnerability Analysis: Working from black-box to white-box perspectives students will learn to consider vulnerabilities in the real world context of product delivery and support.

Auditing and Compliance: Students will explore and understand the different standards products can be held to and work through addressing non-compliance based on real world case studies.

Industry Practices: Utilising automation, containerisation and Infrastructure as Code (IaC) students will explore the basic principles behind common industry product development and best working practices.

Vulnerability and Attack Mitigation's: As the cyber security landscape changes and

new vulnerabilities emerge we must be able to adapt to these threats. Students will practice defending an existing infrastructure while ensuring core functionality is not impacted.

Part 3: Teaching and learning methods

Teaching and learning methods: Teaching will consist of lectorial sessions that will blend delivered content with practical work and lab sheets.

Sessions with allow students to implement delivered material while it is still fresh and encourage discussion and discourse so that students may build on and fully explore content covered.

Students will have a chance to practice the practical skills required for their assessments during these sessions.

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

MO1 Demonstrate critical understanding of the methods and tools used to maintain secure infrastructure

MO2 Demonstrate the implementation of secure solutions to mitigate vulnerabilities in existing infrastructure

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

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/lists/924BF11B-CCDE-8FF6-C189-8B0692F95FE4.html

Part 4: Assessment

Assessment strategy: Students will be assessed via a group demonstration with an individual reflection.

Students will present their analysis of a provided application and showcase how they were able to identify and mitigate vulnerabilities found. Students will be expected to justify decisions made and show that the secure version of their application maintains the intended functionality.

Group demonstrations have been selected to limit the chance for students to rely on automated tools (such as ChatGPT). Students will be expected to discuss and justify the decisions made - if students are unable to provide justification or demonstrate their critical understanding then this will be reflected in the marking. Individual contribution and reflection have been included to ensure no student in a group contributes nothing to the assessment.

Resit

Students will be provided with a different application and will be required to present a pre-recorded video (up to 15 minutes) covering the key details and requirements as outlined in the main sit assessment brief. As the video will be a pre-recorded group presentation, students will still be expected to complete an individual reflection on their resit.

Assessment tasks:

Presentation (First Sit)
Description: Maximum 15-minute-long, with an individual reflection per student.

Students will need to carry out a security assessment on an existing application (provided), identify vulnerabilities or potentially malicious code within the application. Mitigate, or accept these, and provide clear justification for decisions made. It is

expected that the original / intended functionality of the application is not hindered by any security based changes.

Students are expected to communicate the process of their investigation so that anyone can understand and follow the process (no matter their technical capability).
Weighting: 100 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2

Presentation (Resit)
Description: Students will be provided with a different application and will be required to present a pre-recorded video (up to 15 minutes) covering the key details and requirements as outlined in the main sit assessment brief. As the video will be a pre-recorded group presentation, students will still be expected to complete an individual reflection on their resit.
Weighting: 100 %
Final assessment: No
Group work: Yes
Learning outcomes tested: MO1, MO2

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2022-23

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2022-23

Cyber Security and Digital Forensics {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2021-22