Module Specification

Cyber Threats

Version: 2023-24, v2.0, 19 Jul 2023

Contents

Module Specification **1**

Part 1: Information **2**

Part 2: Description **2**

Part 3: Teaching and learning methods **4**

Part 4: Assessment **5**

Part 5: Contributes towards **6**

Part 1: Information

Module title: Cyber Threats

Module code: UFCFFU-30-1

Level: Level 4

For implementation from: 2023-24

UWE credit rating: 30

ECTS credit rating: 15

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:

Security is one of the most important challenges modern organisations face. Security is about protecting organisational assets, including personnel, data, equipment and networks from attack through the use of prevention techniques in the form of vulnerability testing/security policies and detection techniques, exposing breaches in security and implementing effective responses.

In order to provide protection, it is fundamental to understand the types of threats, their methods and means of attack.

In this module you will explore the different types of threat.

Features: Not applicable

Educational aims: Contributes to foundation knowledge. Explores cyber threats in the context of the concepts explored in other L4 modules.

Outline syllabus: You will cover:

foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance

application of cyber security concepts to IT infrastructure

fundamental building blocks and typical architectures of IT infrastructure

common vulnerabilities in networks and systems

vulnerabilities in computer networks, applications and systems (e.g., insecure coding and unprotected networks) and how they can be exploited

network-based attacks e.g.:
eavesdropping/sniffing, man-in-the-middle, spoofing, session hijacking, denial of service, traffic redirection, routing attacks, traffic analysis

impact of vulnerabilities in an organisational context

human dimension of cyber security and adversarial thinking applied to system development

how an employee may enable a successful attack chain without realising it

factors that may increase or decrease risks related to an organisation’s ‘cyber

culture’

links between physical, logical, personal and procedural security

ways to defend against cyber attack

adversarial thinking in the context of system development, application development and analysis

the threat landscape, threat trends, horizon scanning

the threat intelligence lifecycle and the concepts of threat actors and attribution

the significance, value and limitations of threat analyses

Part 3: Teaching and learning methods

Teaching and learning methods:
Lecture sessions cover the technical knowledge required. Designated practical work is included to give the students the opportunity to explore the technical knowledge in a hands-on fashion and the ensure that they have absorbed and understood the key principles involved.

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

MO1 Discover, identify and analyse typical threats, attack techniques, vulnerabilities and mitigations.

MO2 Research and explain the incidence of various types of threat over time and their methods to attack common vulnerabilities.

MO3 Explain how to mitigate against cyber-attacks employing a range of appropriate methods.

MO4 Carry out a threat analysis .

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 135 hours

Placement = 75 hours

Face-to-face learning = 90 hours

Total = 300

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/E44BA897-7E1C-423D-35D0-4514105FAA1E.html

Part 4: Assessment

Assessment strategy: At both first sit and resit, this module is assessed by a combination of: a threat analysis presentation (30 minutes) and a research report (3000 words)

Students will carry out a threat analysis for their employer's IT systems or a subset of them. The methods, results and recommendations will be presented.

Students will consolidate their knowledge and begin to practice their research skills by researching current cyber threats and ranking them in order of probability. This will also ensure that the module remains current and engaging for the students. Examples should be given for each type of threat, the specific vulnerability they attacked and what could have mitigated the impact.

Assessment tasks:

Presentation (First Sit)
Description: Presentation on a threat analysis.
Weighting: 50 %
Final assessment: Yes
Group work: No

Learning outcomes tested: MO1, MO4

Report (First Sit)
Description: Report on current cyber threats.
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO3

Presentation (Resit)
Description: Presentation on threat analysis.
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested:

Report (Resit)
Description: Report on current cyber threats.
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested:

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security Technical Professional {Apprenticeship-GLOSCOLL} [GlosColl] BSc (Hons) 2023-24