

**MODULE SPECIFICATION**

|  |
| --- |
| **Part 1: Information** |
| **Module Title** | Cyber threats, intelligence, malware analysis, reverse engineering and incident response |
| **Module Code** | CY104 | **Level** | 4  |
| **For implementation from** | September 2020  |
| **UWE Credit Rating** | 30 | **ECTS Credit Rating** | 15 |
| **Faculty** | Environment and Technology | **Field** |  |
| **Department** | Computer Science and Creative Technologies |
| **Contributes towards**  | BSc (Hons) Cyber Security Technical Professional Compulsory |
| **Module type:**  | Standard  |
| **Pre-requisites**  | None |
| **Excluded Combinations**  | None  |
| **Co- requisites**  | None  |
| **Module Entry requirements** | None |
|  |
| **Part 2: Description**  |
| 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 and how they penetrate personal, physical, logical and procedural in securities. Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved.This module will be based on ensuring that apprentice’s practical skills and knowledge gained in the block release sessions are carried into the workplace to inform their employment and generation of evidence of competency. You will cover:* foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance
* application of cyber security concepts to ICT infrastructure
* fundamental building blocks and typical architectures of ICT infrastructure
* common vulnerabilities in networks and systems
* vulnerabilities in computer networks 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 and analysis
* the threat landscape, threat trends
* the threat intelligence lifecycle and the concepts of threat actors and attribution
* the significance, value and limitations of threat analyses
 |
| **Part 3: Assessment**  |
| This module is assessed by a combination of: a threat analysis presentation (30 minutes) and a research report (3000 words)Component AApprentices 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. Component BApprentices will research current cyber threats and rank them in order of probability. Examples should be given for each type of threat, the specific vulnerability they attacked and what could have mitigated the impact.  |
|  |
| Identify final timetabled piece of assessment (component and element) | **Component A1** |
| **% weighting between components A and B** (Standard modules only) | **A:**  | **B**:  |
| **50%** | **50%** |
|  |
| **First Sit** |
| **Component A** (controlled conditions)**Description of each element** | **Element weighting****(as % of component)** |
| 1. Presentation (30 minutes)
 | 100% |
| **Component B** **Description of each element** | **Element weighting****(as % of component)** |
| 1. Report (3,000 words)
 | 100% |
| **Resit (further attendance at taught classes is not required)** |
| **Component A** (controlled conditions)**Description of each element** | **Element weighting(as % of component)** |
| 1. Presentation (30 minutes) | 100% |
| **Component B Description of each element** | **Element weighting(as % of component)** |
| 1. Report (3,000 words) | 100% |
|  |
| **Part 4: Learning Outcomes & KIS Data** |
| **Learning Outcomes** | On successful completion of this module students will be able to:Discover, identify and analyse threats, attack techniques, vulnerabilities and mitigations (Component A)Research and explain the various types of threat and their methods to attack common vulnerabilities (Component B)Explain how to mitigate against cyber-attacks employing these methods (Component B)Carry out a threat analysis (Component A) |
| **Key Information Sets Information (KIS)****Contact Hours****Total Assessment** |  The table below indicates as a percentage the total assessment of the module which constitutes a;**Written Exam**: Unseen or open book written exam**Coursework**: Written assignment or essay, report, dissertation, portfolio, project or in class test **Practical Exam**: Oral Assessment and/or presentation, practical skills assessment, practical exam (i.e. an exam determining mastery of a technique)  |
| **Reading List** | Reading list to be added |

***FOR OFFICE USE ONLY***

|  |  |
| --- | --- |
| **First Approval Date (and panel type)** | *Date of first {panel} approval*  |
| **Revision ASQC Approval Date** *Update this row each time a change goes to ASQC* |  | **Version**  | *1* | *Link to RIA*  |
|  |  |  |
|  |  |  |
|  |  |  |