UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD. *Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.*

MODULE CODE: COMP5002	**MODULE TITLE:** Security Operations & Incident Management	
CREDITS: 20	**FHEQ LEVEL:7**	**HECOS CODE:** 100376 **JACS CODE:** I100
PRE-REQUISITES:	**CO-REQUISITES:**	**COMPENSATABLE:** Y

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module will examine the incident management and the role it plays within modern information security systems. It will introduce key concepts in the analysis of network traffic for signs of intrusions, as well as the process of responding to computer incidents including the identification and analysis of malicious code.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical**)**	
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: COMP

Professional body minimum pass mark requirement:

MODULE AIMS:

- To design and develop organisational security operations and incident management architectures that provide a holistic solution to enabling situational awareness and incident management.
- To introduce roles, methodologies and practices underpinning incident management and the creation of Computer Security Incident Response Teams (CSIRTs).
- To introduce the range of techniques that will allow an Intrusion Analyst to intelligently examine network traffic for signs of intrusions and respond to computer incidents.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant award/ programme Learning Outcomes.

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes	Award/ Programme Learning Outcomes contributed to
1. Develop a deep understanding of the structure, roles and responsibilities of a security operations centre. 2. Design and develop technical infrastructures for the management and monitoring of cyber security. 3. Undertake analysis of data and select appropriate intrusion analysis methodologies to analyse intrusion alarms. 4. Judge the appropriateness of incident handling methodologies involved in managing and responding to computer incidents	MSc Cyber Security 13.1.2 13.2.4 13.4.3 13.5.4 MSci Computer Science 1.1 1.3 2.3 2.5 3.3 3.5

DATE OF APPROVAL: 29/11/2019	**FACULTY/OFFICE:** Science & Engineering
DATE OF IMPLEMENTATION: 01/09/2020	**SCHOOL/PARTNER:** Engineering, Computing and Mathematics
DATE(S) OF APPROVED CHANGE: XX/XX/XXXX	**SEMESTER:** Semester 1

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Framework for Higher Education Qualifications http://www.qaa.ac.uk/publications/information-and-guidance/publication/?PubID=2718#.VW2INtJVikp
- Subject benchmark statements http://www.qaa.ac.uk/ASSURINGSTANDARDSANDQUALITY/SUBJECT-GUIDANCE/Pages/Subject-benchmark-statements.aspx
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)
- QAA Quality Code http://www.qaa.ac.uk/AssuringStandardsAndQuality/quality-code/Pages/default.aspx

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be used in the KIS return and published on the extranet as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2021/22 **NATIONAL COST CENTRE:121**
MODULE LEADER: Dr Shailendra Rathore **OTHER MODULE STAFF:** Professor Nathan Clarke

Summary of Module Content

The module will consider the role of security operations and incident management. The design of suitable security and monitoring infrasturtures that provide situational awareness and enable efficient and effective incident management. The module will also develop knowledge and technqiues to enable analysis and investigation of intrusions and the role of honeypots.

Indicative content will include:

- Security operations and Incident management infrastructure.
- Network monitoring and analysis.
- Situational Awareness/cyber intelligence.
- Security Information Event Managerment.
- Honeypots.
- Incident operations, handling and CSIRT roles.
- Intrusion detection models.
- Intrusion analysis, monitoring and logging.
- Intriusion response.

SUMMARY OF TEACHING AND LEARNING ***[Use HESA KIS definitions]***		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	26	To deliver the core body of knowledge
Labs	26	Practical based activities to reinforce knowledge introduced in lectures
Self-Study and assessment	148	An opportunity to read around the subject, to obtain greater depth of understanding of the subject.
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name	Component Weighting
Written exam		% % 100%
Test		% % 100%
Coursework	W1 – Intrusion Analysis Report W2 – Security Operations Report	30% 70% 100%
Practical		% % 100%
Clinical Examination		% % 100%
Generic Assessment		

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Written exam		% % 100%
Coursework (in lieu of the original assessment)		% % 100%
Coursework	Security Operations and Intrusion Analysis Report	100% % 100%

Practical		% % 100%
Clinical Examination		% % 100%
Generic Assessment		
Test		% % 100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Date: XX/XX/XXXX	**Approved by**: Date: XX/XX/XXXX