Module Descriptor

Title	Incident Response		
Session	2025/26	**Status**	Published
Code	COMP11082	**SCQF Level**	11
Credit Points	10	**ECTS (European Credit Transfer Scheme)**	5
School	**Computing, Engineering and Physical Sciences**		
Module Co-ordinator	Althaff Mohideen		

Summary of Module

The module provides students with detailed understanding of the methodologies, practices and techniques required to respond to a network intrusion or security breach and will ensure students understand all factors involved in the required for situational preparedness, management and resilience principles.

By using reflection techniques and case study reviews, students will develop a deeper understanding of the processes required to deal with a security breach.

This module will work to develop a number of the key 'I am UWS' Graduate Attributes to make those who complete this module:

Universal

- Critical Thinker
- Ethically-minded
- Research-minded

Work Ready

- Problem-Solver
- Effective Communicator
- Ambitious

Successful

- Autonomous
- Resilient
- Driven

Module Delivery Method	On-Campus[1] ☒	Hybrid[2] ☐	Online[3] ☐	Work -Based Learning[4] ☐
Campuses for Module Delivery	☐ Ayr ☐ Dumfries	☒ Lanarkshire ☒ London ☐ Paisley	☐ Online / Distance Learning ☐ Other (specify)	

Terms for Module Delivery	Term 1	☐	Term 2	☒	Term 3	☐
Long-thin Delivery over more than one Term	Term 1 – Term 2	☐	Term 2 – Term 3	☐	Term 3 – Term 1	☐

Learning Outcomes	
L1	Demonstrate a critical understanding of the theories and concepts associated with the management of security breaches by the Computer Incident Response Team (CIRT).
L2	Apply knowledge, skills and understanding to design systems that fully utilise tools such as the SANS 6Step Incident Management Model.
L3	Critically analyse the effectiveness of practical implementations of incident management and response.
L4	N/A
L5	N/A

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	**During completion of this module, there will be an opportunity to achieve core skills in:**
Knowledge and Understanding (K and U)	**SCQF 11** Students will learn systematic and comprehensive knowledge of Incident Response. Students are expected to be familiar with the key technologies and techniques and their application in practice.
Practice: Applied Knowledge and Understanding	**SCQF 11** Students will gain in-depth, comprehensive understanding and critical awareness of knowledge of Incident Response, and apply this in planning, developing and implementing, capture a response to a network security event. They will also develop capability to apply a range of standard and specialised research skills, tools/software,

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

	development kit and related techniques in response to application requirements for their written assignment and lab tasks.
Generic Cognitive skills	**SCQF 11** To complete their written reports and laboratory tasks, students will first build skills to integrate information and apply knowledge from various sources including technology advances informed by research and industry.
Communication, ICT and Numeracy Skills	**SCQF 11** Working in interacting groups, students will develop communication skills as well as the ability to write technical reports and documentation.
Autonomy, Accountability and Working with Others	**SCQF 11** Each student will generate a comprehensive report summarizing his/her finding for a given scenario.

Prerequisites	**Module Code**	**Module Title**
	Other	
Co-requisites	**Module Code**	**Module Title**

Learning and Teaching	
In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours.	
Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture / Core Content Delivery	7
Tutorial / Synchronous Support Activity	7
Laboratory / Practical Demonstration / Workshop	14
Independent Study	72
Please select	
Please select	
TOTAL	100

Indicative Resources
The following materials form essential underpinning for the module content and ultimately for the learning outcomes: Steve Anson (2019). Applied Incident Response. Wiley Luttgens, J. (2014) 3rd Ed. Incident Response & Computer Forensics. McGraw-Hill Education

Murdoch, D. (2014) 2nd Ed. Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder. CreateSpace Independent Publishing Platform

Roberts, S and Brown, R. (2016) Intelligence-Driven Incident Response. O'Reillly

Please ensure the list is kept short and current. Essential resources should be included, broader resources should be kept for module handbooks / Aula VLE.

Resources should be listed in Right Harvard referencing style or agreed professional body deviation and in alphabetical order.

Oracle Virtual Box along with guest additions and VirtualBox Extension Pack.

(N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance and Engagement Requirements

In line with the Student Attendance and Engagement Procedure, Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time.

For the purposes of this module, academic engagement equates to the following:

The School of Computing, Engineering and Physical Sciences considers attendance and engagement to mean a commitment to attending, and engaging in, timetabled sessions. You will scan your attendance via the scanners each time you are on-campus and you will login to the VLE several times per week. Where you are unable to attend a timetabled learning session due to illness or other circumstance, you should notify the Programme Leader that you cannot attend. Across the School an 80% attendance threshold is set. If you fall below this, you will be referred to the Student Success Team to see how we can best support your studies.

Equality and Diversity

The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code.

Aligned with the University's commitment to equality and diversity, this module supports equality of opportunity for students from all backgrounds and learning needs. Using the VLE, material will be presented electronically in formats that allow flexible access and manipulation of content. This module complies with University regulations and guidance on inclusive learning and teaching practice. This module has lab-based teaching and as such you are advised to speak to the Module Co-ordinator to ensure that specialist assistive equipment, support provision and adjustment to assessment practice can be put in place, in accordance with the University's policies and regulations.

(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	**Computing**
Overall Assessment Results	☐ **Pass / Fail** ☒ **Graded**
Module Eligible for Compensation	☐ **Yes** ☒ **No** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to**

	programme accreditation requirements. Please check the associated programme specification for details.
School Assessment Board	Business & Applied Computing
Moderator	TBC
External Examiner	A Esfahani
Accreditation Details	
Module Appears in CPD catalogue	☐ **Yes** ☒ **No**
Changes / Version Number	2.01

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
Coursework 1 (50%)
Assessment 2
Coursework 2 (50%)
Assessment 3
(N.B. (i) Assessment Outcomes Grids for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed. (ii) An indicative schedule listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Review/ Article/ Critique/Paper	☒	☒	☒	☐	☐	50	4

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Report of practical/ field/clinical work	☒	☒	☒	☐	☐	50	8

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	12 hours

Change Control

What	When	Who
Attendance Update & EDI Update	20/01/2025	A Adamson
External Examiner Updated	22/01/2025	A Adamson