Module Descriptor

Title	Enterprise Security Operations		
Session	2026/27	**Status**	Published
Code	COMP09123	**SCQF Level**	9
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	**Computing, Engineering and Physical Sciences**		
Module Co-ordinator	Althaff Mohideen		

Summary of Module

Enterprise security operations play a critical role in protecting organisational information systems by continuously monitoring, analysing, and responding to security events across complex digital environments. Modern organisations rely on Security Operations Centres (SOCs) to detect cyber threats, investigate suspicious activity, and coordinate timely responses to security incidents.

This module introduces the principles and practices of enterprise security operations, focusing on the collection, monitoring, and analysis of security telemetry such as system, network, and application logs. Students will explore how security analysts use industry-standard security monitoring and analytics platforms to identify indicators of compromise, investigate potential intrusions, and support incident response activities.

Through practical exercises and case studies, students will gain experience in analysing security events, applying threat intelligence, and understanding operational workflows within a SOC environment. The module emphasises defensive cyber security practices used in enterprise settings, preparing students for roles in security monitoring, threat detection, and operational cyber defence.

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) NCL, DGC	

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	Critically analyse the role and functions of enterprise security operations and Security Operations Centres (SOCs).
L2	Analyse security events and log data to identify suspicious activity and potential security incidents.
L3	Apply threat intelligence and investigation techniques to support cyber threat detection.
L4	Demonstrate understanding of a Security Information and Event Management (SIEM) platform for security monitoring, event analysis, and incident detection.
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 9** Students will develop a critical understanding of fundamental security layers, threat intelligence and processes involved in cyber operations. They will obtain critical knowledge and understanding of the commercial and economic context of running cyber operations.
Practice: Applied Knowledge and Understanding	**SCQF 9** Students will gain in-depth knowledge about cyber operations by identifying the key attributes of an attack by investigating cyber attacks using a market-leading SIEM tool.

[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

Generic Cognitive skills	**SCQF 9** To complete their individual reports, students will first build skills to critically understand key issues in managing cyber operations. They will develop learning awareness of comprehensive security architectures based upon multiple layers of protection.
Communication, ICT and Numeracy Skills	**SCQF 9** In the labs, students will develop the ability to write formal technical reports and documentation in their reports. The labs will develop ICT skills by configuring computers and network devices to allow/disallow attacks on these devices and working on a market-leading SIEM tool.
Autonomy, Accountability and Working with Others	**SCQF 9** Students will demonstrate an ability to work independently on their own laboratory tasks and acquire autonomy and accountability through these tasks. In the lab sessions, they will autonomously plan and manage the work progress and finish the writing of the lab note and report in a timely and professional manner.

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	12
Tutorial / Synchronous Support Activity	12
Laboratory / Practical Demonstration / Workshop	24
Independent Study	152
Please select	
Please select	
TOTAL	200

Indicative Resources
The following materials form an essential underpinning for the module content and ultimately for the learning outcomes: Modern Security Operations Center by Joseph Muniz, Publisher: Addison-Wesley Professional, Publication Date: 27 July 2021.

Security Operations in Practice by Mike Sheward, Publisher: BCS, The Chartered Institute for IT, Publication date: 29 February 2020. Blue Team Handbook: SOC, SIEM, and Threat Hunting by Don Murdoch, Publication date 25 March 2019. VirtualBox software and VBOX extension
(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	Raman Singh
External Examiner	M Davis
Accreditation Details	
Module Appears in CPD catalogue	☐ **Yes** ☒ **No**
Changes / Version Number	1.04

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
Practical Logbook (60%)
Assessment 2
Security Incident Investigation Report (40%)
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**
Practical Logbook	☒	☒	☐	☐	☐	60	0

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Investigation Report	☐	☐	☒	☒	☐	40	0

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	0 hours

Change Control

What	**When**	**Who**
