Module Definition Form (MDF)

Module code: MOD007390	**Version:** 1 **Date Amended:** 24/Feb/2020

1. Module Title

Security Management, Operations and Analytics

2a. Module Leader

Hossein Abroshan

2b. School

School of Computing and Information Sciences

2c. Faculty

Faculty of Science and Engineering

3a. Level

6

3b. Module Type

Standard (fine graded)

4a. Credits

30

4b. Study Hours

300

5. Restrictions

Type	Module Code	Module Name	Condition
Pre-requisites:	None		
Co-requisites:	None		
Exclusions:	None		
Courses to which this module is restricted:	None		

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

Security Management, Operations and Analytics imparts an understanding of the underlying principles associated with security management. You will develop an understanding of security threats and vulnerabilities within modern organisational environments, and gain an understanding of the underlying principles of risk analysis and contingency planning as applied to business systems. Consideration is also given to the need for legislative compliance.

This module also focuses on the current perspective of cybersecurity analytics contrasted with the emerging trends over threat hunting and threat intelligence. The limitations of an organisations current tools used in cybersecurity will be examined especially the role and the use of SIEM in an organisations operational security management. This contributes to help you understand how organisations can better understand their cyber risks environment.

The Security Management and Governance module is delivered as a mixture of theory, through a series of lectures, and practical implementation, through a series of guided laboratory exercises.

6b. Outline Content

- Security concepts of management
- Security standards and responsibilities
- Computing law
- Ethical computing and cyber security ethics
- Identification & Mitigation of Cyber Risk
- Developing security policies
- Business continuity and contingency planning
- Promoting security awareness
- Development of Security Operations & Dashboards
- Understanding SIEM’s Role in Security Operations
- The Security Analytics Process
- The Concept of Threat Hunting

6c. Key Texts/Literature

The reading list to support this module is available at: https://readinglists.aru.ac.uk/

6d. Specialist Learning Resources

Specialist lab resources will be made available using a mixture of captive lab environments such as Netlab and cloud based resources (such as AWS/ELK) to simulate active operational IT infrastructures and potential security scenarios to display on Dashboard based systems through SIEM, threat hunting and threat intelligence

7. Learning Outcomes (threshold standards)

No.	Type	On successful completion of this module the student will be expected to be able to:
1	Knowledge and Understanding	Demonstrate knowledge and understanding of key professional & legal sources and concepts relating to information security
2	Knowledge and Understanding	Identify and analyse relevant statutes, case law and codes of practice
3	Intellectual, practical, affective and transferrable skills	Understand the limitations of the current tools used to mitigate risk and the application of analytics in operational security environments.
4	Intellectual, practical, affective and transferrable skills	Analyse the need for threating hunting techniques and threat intelligence as protection mechanisms within given operational security scenarios.

8a. Module Occurrence to which this MDF Refers

Year	Occurrence	Period	Location	Mode of Delivery
2025/6	ZZF	Template For Face To Face Learning Delivery		Face to Face

8b. Learning Activities for the above Module Occurrence

Learning Activities	Hours	Learning Outcomes	Details of Duration, frequency and other comments
Lectures	24	1-4	Lecture 2 hr x 12 weeks
Other teacher managed learning	24	1-4	Practical 2 hr x 12 weeks
Student managed learning	252	1-4	Private study
TOTAL:	300		

9. Assessment for the above Module Occurrence

Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
010	Coursework	1,2	30 (%)	Fine Grade	30 (%)
1000 word report - Information Security Management assignment					
Assessment No.	**Assessment Method**	**Learning Outcomes**	**Weighting (%)**	**Fine Grade or Pass/Fail**	**Qualifying Mark (%)**
011	Coursework	3,4	70 (%)	Fine Grade	30 (%)
2500 Word Report – Security Operations and Analytics assignment					

In order to pass this module, students are required to achieve an overall mark of 40% (for modules at levels 3, 4, 5 and 6) or 50% (for modules at level 7*).

In addition, students are required to:
(a) achieve the qualifying mark for each element of fine graded assessment as specified above
(b) pass any pass/fail elements

[* the pass mark of 50% applies for all module occurrences from the academic year 2024/25 – see Section 3a of this MDF to check the level of the module and Section 8a of this MDF to check the academic year]