ROBERT GORDON UNIVERSITY ABERDEEN

MODULE DESCRIPTOR

Module Title

Security Operations & Incident Management

Reference	CM4142	Version	1
Created	November 2023	SCQF Level	SCQF 10
Approved	April 2024	SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

This module aims to provide students with a strong understanding of Security Operations and Incident Management, covering key concepts like intrusion detection, SIEM, and modern SoC architectural principles. Practical components with hands-on experience using Open-Source Security Information Management (OSSIM) tools provide insights into the complete lifecycle of security operations.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1 Communicate a critical understanding of the principles underlying Security Operations and Incident Management.

2 Illustrate proficiency in incident management by effectively covering planning, response, recovery, and crisis management.

3 Develop a robust Security Incident Management System (SIEM) solution for a given scenario.

4 Communicate cybersecurity incidents and effective remediation to pertinent stakeholders.

Indicative Module Content

Fundamental concepts: Intrusion detection, security information and event management (SIEM), security orchestration, automation and response (SOAR), mape-k architecture; Architectural Principles: Roles of CISOs and Analysts, Cyber-Threat Intelligence (CTI), Information Sharing and Analysis Center (ISAC); Monitoring sources: Network Traffic and traffic Aggregates, Application and System Logs; Analysis Methods & Contribution of SIEM: Data Collection, Alert Correlation, Security Operations and Benchmarking; SIEM Platforms & Countermeasures: Cyber-Threat Intelligence, Situational Awareness; Incident Management (Planning, Response, Post-Incident Activities, Disaster Recovery, Crisis Management); SIEM in Practice: Alien Vault OSSIM, Legal, Business, Team Management, Data Collection, Reporting, Threat Response.

Module Delivery

Lectures introduce and illustrate key concepts, while practical skills are honed through a series of laboratory exercises.

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4

Description: Coursework consisting of both practical and theoretical elements covering all learning outcomes of the module.

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade of D is required to pass this module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1
B	The student needs to achieve a B in Component 1
C	The student needs to achieve a C in Component 1
D	The student needs to achieve a D in Component 1
E	The student needs to achieve an E in Component 1
F	The student needs to achieve an F in Component 1
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	CM1131 Cyber Security Fundamentals CM2135 Securing Networks CM3144 Information Risk & Security Management
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1 McCrie, R., & Lee, S. (2021). Security operations management. Elsevier Science.

2 Muniz, J. (2021).?The modern security operations center. Addison-Wesley Professional.

3 Anson, S. (2020).?Applied incident response. John Wiley & Sons.

4 Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: a case study of the Equifax data breach.?Issues in Information Systems,?19(3)

5 Pemble, M. W. A., & Goucher, W. F. (2018).?The CIO?s Guide to Information Security Incident Management. CRC Press.

6 Don Murdoch, D., (2019). Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. Blue Team Handbook

7 Arun E Thomas, A., (2018). Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence. Arun E Thomas