MODULE DESCRIPTOR

Module Title

Security Operations

Reference	CMM011	Version	1
Created	May 2022	SCQF Level	SCQF 11
Approved	June 2022	SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

To provide students with the ability to evaluate and apply the methods, tools and techniques used in Security/Network Operations Centres (SOC/NOC).

Learning Outcomes for Module

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

1	Critically analyse the architecture, protocols, threats and vulnerabilities of a typical enterprise network.
2	Critically analyse key incident events reported by the security incident event management system.
3	Apply appropriate tools and techniques to respond to cyber security incidents or threats.
4	Document cyber security incidents and responses.

Indicative Module Content

OSI model. Fundamentals of LAN design and configuration. Common networking protocols. Main threats and vulnerabilities. Security knowledge management (CVE, CVSS, CWE, Mitre ATT&CK). Data sources: network and host data sources (e.g., pcap, netflow, dns, server logs). Basics of network monitoring and intrusion detection. SIEM - Security Incident Event Management (e.g., Alien Vault OSSIM). Alert correlation. Incident management planning, incident handling, disaster recovery, crisis management, legal/business, team management. Legal requirements (e.g., GDPR, Computer Misuse act). Data collection, Reporting and Analysis.

Module Delivery

This module is taught using a structured programme of lectures, practical sessions, web-based learning materials, web-based activities, practical exercises and student-centred learning.

Module Ref:	CMM011 v1

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	30
Non-Contact Hours	120	120
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
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:	A case study report.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

To achieve a pass in this module requires a minimum of Grade D in Component 1.

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

Module Requirements

Prerequisites for Module	None, in addition to course entry requirements for School of Computing MSc students. For short course students: previous computing experience is beneficial.
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CMM011 v1

INDICATIVE BIBLIOGRAPHY

1	Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback ? 25 Mar. 2019
2	Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence Hardcover ? 24 Mar. 2018
3	Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices Paperback ? 22 May 2016 by Arun E Thomas
4	JARPEY, G., McCoy, R. S., 2017. Security Operations Center Guidebook: A Practical Guide for a Successful SOC. Elsevier.
5	THOMPSON, E. C., 2018. Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. Apress.
6	DAVIES, G., 2020. Networking Fundamentals: develop the networking skills required to pass the Microsoft MTA networking fundamentals exam 98-366. Packt Publishing.