MODULE DESCRIPTOR

Module Title

Security Incident Event Management

Reference	CM4127	Version	3
Created	April 2023	SCQF Level	SCQF 10
Approved	June 2021	SCQF Points	15
Amended	August 2023	ECTS Points	7.5

Aims of Module

To provide students with the technical knowledge and understanding of cyber security event management systems. To provide students with the management, legal and personnel skills to deal with and document a cyber security incident.

Learning Outcomes for Module

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

1	Select a suitable security incident management system and implement it on a small network.
2	Identify and explain key incident events reported by the management system.
3	Analyse and respond appropriately to cyber security incidents.
4	Document and report on cyber security incidents.
5	Apply remediation techniques to resolve the cyber security incident.

Indicative Module Content

SIEM - Security Incident Event Management. Alien Vault OSSIM disaster recovery, crisis management, legal/business, team management. GDPR, Computer Misuse act, ISO27001. Data collection. Reporting and Analysis. Threat Response.

Module Delivery

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

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, 5
Description:	Coursework producing a technical report which documents the implementation and analysis of an SIEM solution.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of component 1 (C1). 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 C1.
B	The student needs to achieve a B in C1.
C	The student needs to achieve a C in C1.
D	The student needs to achieve a D in C1.
E	The student needs to achieve an E in C1.
F	The student needs to achieve an F in C1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

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	Successful SIEM and Log Management Strategies for Audit and Compliance by David Swift ? November 9, 2010
4	Security Operations Center ? Analyst Guide: SIEM Technology, Use Cases and Practices Paperback ? 22 May 2016 by Arun E Thomas