MODULE DESCRIPTOR

Module Title

Secure Operations and Forensics

Reference	CMM404	Version	2
Created	June 2022	SCQF Level	SCQF 11
Approved	July 2021	SCQF Points	30
Amended	July 2022	ECTS Points	15

Aims of Module

To provide students with the ability to evaluate and apply the methods, tools and techniques used in intrusion response and forensics.

Learning Outcomes for Module

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

1 Critically appraise the techniques and tools used in security monitoring and event management.

2 Demonstrate a critical understanding of the methods used in investigating and responding to a security incident.

3 Apply the techniques used in collecting, processing and preserving digital evidence.

4 Apply a range of specialised procedures in preparing a forensics report and expert testimony.

Indicative Module Content

Security Operation Centres (SOCs). Security monitoring (logs, network traffic, SIEMs). Security event management: Incident identification, response and recovery. Digital forensic concepts, principles, tools and techniques. Digital forensic analysis: collecting, processing and preserving digital evidence; Device/Network forensics; Malware analysis. Anti-forensic techniques; Forensic report writing and expert testimony. Social, ethical and legal issues associated with digital forensics.

Module Delivery

The module is delivered via work-based learning along with structured online learning materials/activities and directed study, facilitated by regular online tutor support. Workplace Mentor support and work-based learning activities will allow students to contextualise this learning to their own workplace. Face-to-face engagement occurs through annual induction sessions, employer work-site visits, and modular on-campus workshops. Study Groups will be formed to encourage students to work collaboratively on set learning activities and share practice from their workplaces. Formative feedback will be provided to make sure teams are engaging positively and performing effectively.

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	30	N/A
Placement/Work-Based Learning Experience [Notional] Hours	240	N/A
TOTAL	300	N/A
Actual Placement hours for professional, statutory or regulatory body	240	

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:	Report on security incident response and forensics investigation.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of 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	JARPEY, G., McCOY, R. S., 2017. Security Operations Center Guidebook: A Practical Guide for a Successful SOC. Elsevier.
2	THOMPSON, E. C., 2018. Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. Apress.
3	STREET, J., 2015. Dissecting the Hack: The V3rb0ten Network. Springer.
4	Zeigler, A., 2016, Preserving Electronic Evidence for Trial: A team approach to the litigation hold, data collection, and preservation of digital evidence. Elsevier.
5	SAMMONS, J., 2016, Digital Forensics: Threatscape and best practices. Elsevier.
6	MOHANTA, A., SALDANHA, A., 2020. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. Apress.