**This Version is No Longer Current**
The latest version of this module is available here

## MODULE DESCRIPTOR

### Module Title

Security Incident Event Management

| | | | |
|---|---|---|---|
| Reference | CM4127 | Version | 1 |
| Created | June 2021 | SCQF Level | SCQF 10 |
| Approved | June 2021 | SCQF Points | 15 |
| Amended | | 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* | | |

| Module Ref: | CM4127 v1 |
|---|---|

## ASSESSMENT PLAN

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

### Component 1

| Type: | Coursework | Weighting: | 50% | Outcomes Assessed: | 1, 5 |
|---|---|---|---|---|---|
| Description: | Implementation and analysis of SIEM solution. | | | | |

### Component 2

| Type: | Coursework | Weighting: | 50% | Outcomes Assessed: | 2, 3, 4 |
|---|---|---|---|---|---|
| Description: | Research essay, case study review. | | | | |

## MODULE PERFORMANCE DESCRIPTOR

### Explanatory Text

Component 1: Prcatical Exam worth 50% of total module assessment, Component 2: Coursework worth 50% of total module assessment. Overall D grade required to pass the module.

| | | Practical Exam: | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **A** | **B** | **C** | **D** | **E** | **F** | **NS** |
| Coursework: | **A** | A | A | B | B | C | E | |
| | **B** | A | B | B | C | C | E | |
| | **C** | B | B | C | C | D | E | |
| | **D** | B | C | C | D | D | E | |
| | **E** | C | C | D | D | E | E | |
| | **F** | E | E | E | E | E | F | |
| | **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 |