COMP08078
Secure Information and Event Management

Full Title	Secure Information and Event Management		
Status	Uploaded to Banner	**Start Term**	2020
NFQ Level	08	**ECTS Credits**	10
Module Code	COMP08078	**Duration**	Stage - (26 Weeks)
Grading Mode	Numeric	**Department**	Business, Humanities and Tech
Module Author	Seamus Dowling		

Module Description

SIEM explores the concept of, and software solutions associated with Secure Information and Event Management. SIEM provides and organisation with an overall view of what is happening on IT infrastructure in real-time and helps IT teams to be more proactive in the fight against security threats. SIEM is also a recognised industry acronym associated with cybersecurity. This module will examine data collection and forensics, user activity, alert management and reporting giving IT professionals the knowledge to respond quickly and efficiently to cyberattack incidences.

The module also examine cybersecurity best practice implementations around the Mitre ATT&CK Framework and Lockheed Martin's Cyber Kill Chain Model. Case studies examining the implementation of cybersecurity controls are an essential element of this module.

	Learning Outcomes ***On completion of this module the learner will/should be able to:***
1.	Explain concepts of SIEM as part of overall cyber security
2.	Apply knowledge of the legal requirements of protecting organisational data
3.	Design effective reports for organisational compliance requirements
4.	Evaluate the tools used for data analytics and visualisation
5.	Evaluate and compare SIEM platforms
6.	Use threat intelligence to understand the risk to organisational data and infrastructure.
7.	Apply matrix solutions for threat hunting
8.	Interpret the organised approaches to manage the aftermath of a security breach or cyberattack
9.	Deploy multiple collection agents to gather security-related events from end-user devices, servers and network equipment

Indicative Syllabus

Risk Assessment and Risk Management (10%)

- Identifying, assessing and controlling threats to an organisations' capital and earnings.
- Threats stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters.
- IT security threats, data-related risks and the risk management strategies to alleviate them

Threat Management and Threat Intelligence (10%)

- Organised, analysed and refined information about potential or current attacks that threaten an organisation.
- Understand the risks of the most common and severe external threats, such as zero-day threats, advanced persistent threats (APTs) and exploits
- Incident response to manage the aftermath of a security breach, cyberattack, IT incident, computer incident or security incident.

Cyber Attack Frameworks (20%)

- Adversarial Tactics, Techniques, and Common Knowledge
- Multistage threats and techniques
- Exploration of attack frameworks such as Mitre ATT&CK and Cyber Kill Chain

- Mapping threats and alerts to SIEM solutions
- Mapping SIEM solutions to attack frameworks

SIEM System Features (10%)

- Integration with other controls.
- Artificial intelligence.
- Threat intelligence feeds.
- Extensive compliance reporting.
- Forensics capabilities.

SIEM Systems (20%)

- Compliance reporting
- Incident response and forensics
- Database and server access monitoring
- Internal and external threat detection
- Real-time threat monitoring, correlation and analysis across a variety of applications and systems
- IDS, IPS, firewall, event application log, and other application and system integrations
- Threat intelligence
- User activity monitoring (UAM).
- Limit damage and reduce recovery time and costs.

SIEM Tools and platforms (20%)

An exploration of established SIEM tools and platforms such as:

- Azure Sentinel
- SIREN
- Splunk
- IBM QRadar
- LogRhythm
- Exabeam
- Netwitness RSA

Data Analytics (10%)

- Coding for data analytics and visualisation
- User and entity behaviour analytics (UEBA)
- Security orchestration, automation and response (SOAR).
- AI and Machine learning tools to augment data analysis
- Coding in existing platforms and SIEM systems.

Teaching and Learning Strategy

Online/blended delivery.

At the start of all modules lecturers will schedule a webinar detailing how to communicate with lecturer and other students (email and forums). It will be highlighted that some assessment activities will require collaboration on the virtual learning environment (VLE) or other channels. Lecturers will interact with students on VLE forum.

Lecturers will lead by example by posting comments on their comments and facilitate discussion by posting links to relevant and interesting material. Timely feedback will be given on assessment submissions. Lecturers will encourage discussion around their solutions versus others. Live (and recorded) webinars will be posted as links and will be continuously referred to during module.

For both socially distanced face-to-face and online/blended delivery, the following information will be posted on moodle: tasks, expected deliverable, deadlines, assessment materials and other sources to complete assessment.

Social presence is encouraged in the classroom for socially distanced face-to-face and facilitated for online/blended delivery. Classroom group work and lab challenges creates an environment that promotes appropriately distanced social interaction. Online and blended delivery requires more facilitation. This will involve an initial get-to-know-you webinar. Forum discussions will ensure that all students share a little about themselves. Students in the same geographic area will be encouraged to collaborate. This overlaps with other both the cognitive and teaching presences. Period webinars will be scheduled with specific ‘agenda’ points to be discussed. Students will need to prepare for these webinar by completing e-tivities in advance, and discuss their findings during the webinar. Students will be encouraged to use their own social networking groups whereby they can get instant notifications of comments and can contribute to discussions

Cognitive presence will be ‘assessed’ and monitored for socially distanced face-to face and online/blended delivery. This should be an iterative process whereby students will demonstrate their growing knowledge of SIEM concepts. Constant feedback and participation by the lecturer (on social platforms, classroom and VLE) and feedback on their performance of past assessment items, will be provided

Teaching presence is relevant for socially distanced face-to face and online/blended delivery. This should engage and challenge the student. They should want to pursue the next task and apply what they have learned. Lab practical tasks will assess elements of all modules. Intermittent quizzes and reflective activities will also be posted although these will not contribute to assessment marks.

Independent Learning: Allied to the Approved Programme Schedule hours students will be required to pursue Independent Learning as part of the module.

Assessment Strategy

Information concerning the nature and timing of continuous assessment will be reviewed and agreed with learners and external examiners at the beginning of the academic year.

Marking criteria, deadlines and expectations will also be provided to the learner in advance.

Constructive feedback will be provided in a timely manner and in an appropriate format. A series of Lab Practical tests which are intended primarily to assess learner's ability to understand SIEM, assess SIEM products and implement SIEM solutions.

Four assessments will be spread throughout the year: two in semester 1 and two in semester 2.

- Assessment one and three (submitted online) will be formative to assess the learner's knowledge of SIEM material.
- Assessment two and four (submitted online) will be summative as the learner's apply their knowledge of SIEM from each semester.

Repeat Assessment Strategies

All assessment will be carried out in line with the programme, campus and institute assessment strategies and in line with the Code of Practice No. 3 Student Assessments: Marks and Standards.

Students can resubmit assessments on Moodle, where eligible. Decisions on nature of assessment will be linked to the need to achieve particular learning outcomes. Individuals may be interviewed or asked to present their work in a formal context to validate authenticity and ownership of work.

Indicative Coursework and Continuous Assessment:		**100 %**		
Form	***Title***	***Percent***	***Week (Indicative)***	***Learning Outcomes***
Assessment	Utilise the ATT&CK knowledge framework to develop threat models and methodologies.	25 %	Week 6	6,7,8
Essay	Use SIEM technology to develop a successful security deployment strategy	25 %	Week 13	1,2,3,5,9
Assignment	Compare and contrast SIEM product offerings	20 %	Week 20	4,5,6,8
Group Project	Develop a SIEM solution for enterprise	30 %	End of Term	1,3,4,5,6,8,9

Full Time Delivery Mode Average Weekly Workload:			**3.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Lecture	Lectures	Flat Classroom	2	Weekly	2.00
Practical	SIEM Tools & Platforms	Computer Laboratory	1	Weekly	1.00

Online Learning Delivery Mode Average Weekly Workload:			**3.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Online Learning	Online delivery of content via live and recorded lectures, webinars, activities, video and audio assignments	Online	1	Weekly	1.00
Online Learning	Online Tutorial	Online	1	Weekly	1.00
Seminar	Monthly Topical Webinar	Online	4	Monthly	1.00

Blended Delivery Mode Average Weekly Workload:			**3.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Lecture	Online delivery of content via live and recorded lectures, webinars, activities, video and audio assignments	Online	2	Weekly	2.00
Practical	SIEM Tools & Platforms	Online	1	Weekly	1.00

Required Reading Book List

Collins, M., (2017). *Network Security Through Data Analysis*.
ISBN 1491962844 ISBN-13 9781491962848

Thomas, E., (2016). *Security Operations Center - Analyst Guide*. Createspace Independent Publishing Platform.
ISBN 1533408505 ISBN-13 9781533408501

Yuri, N., (2020). *Microsoft Azure Sentinel*. Microsoft Press.
ISBN 0136485456 ISBN-13 9780136485452

Murdoch, D., (2019). *Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1. 02)*.
ISBN 1091493898 ISBN-13 9781091493896

Journal Resources

https://academic.oup.com/cybersecurity

https://www.journals.elsevier.com/computer-law-and-security-review

Online Resources

https://purplesec.us/siem-solutions/

https://www.ultimatewindowssecurity.com/webinars/default.aspx

https://www.misp-project.org/features.html

https://www.nist.gov/cyberframework

Other Resources

https://www.immersivelabs.com/

https://www.first.org/

https://dcloud2-sng.cisco.com/

Programme Membership

GA_KCYBC_L08 202000 Higher Diploma in Science in Cybersecurity Risk & Compliance