COMP09025
Incident Detection and Response

Full Title	Incident Detection and Response		
Status	Uploaded to Banner	**Start Term**	2020
NFQ Level	09	**ECTS Credits**	10
Module Code	COMP09025	**Duration**	Stage - (26 Weeks)
Grading Mode	Numeric	**Department**	Business, Humanities and Tech
Module Author	Seamus Dowling		
Co Authors	Brian Mulhern		

Module Description

When cyber security controls are circumvented, an organization must respond to cyber incidents. Security operations personnel need to have the skills to systematically neutralize a threat. These steps include formal incident response preparation and planning, threat identification, containment and eradication measures, and implementation of robust controls to mitigate against future compromises.

This module explores the necessary processes and tools used to respond effectively to a detected threat. A structured process of Incident Detection and Response will assist cyber security professionals in proactively searching for cyber security threats. Once detected, this process will ensure that the threat is analysed and neutralised. Information learned from this structured process ensures that cyber security professionals recognise the methods used by current and evolving threats. This module details the preparatory processes that are required in advance, such as incident detection and response policy documentation, teams and communication channels. These processes ensure that detection and reporting structures exist, enabling an organisation to triage a threat and assess its criticality. Containment and threat analysis can be reported back through the process ensuring that post-incident information will aid further detection and strengthen an organisation's cyber defences

	Learning Outcomes ***On completion of this module the learner will/should be able to:***
1.	Integrate advanced theoretical knowledge in the development of Incident Detection and Response policies.
2.	Independently evaluate and critically analyse data collection tools, platforms.
3.	Apply current accepted methodologies and frameworks for incident response and detection
4.	Integrate knowledge of malware forensics to identify and manage cyber threats.
5.	Apply accepted methodologies for tackling design issues associated with threat remediation.
6.	Critically evaluate Incident Detection and Response policies in industry specific environments.

Indicative Syllabus

Incident detection and Response Methodologies

- Methodologies & frameworks
- Preparation, Identification, Containment, Eradication, Recovery, and Lessons learned.
- Mitre Att&ck, CKC
- Intelligence and process driven response

Policies and Documentation

- Incident response best practice
- Incident response policies
- Communication channels
- Global repositories and reports

Logging and Data Collection

- Malware collection
- Shadow IT monitoring
- OS tools (PowerShell, WMI)

- Network device activity collection
- SIEM integration
- Proactive engagement (honeypots, IDS)

Forensics, Triage and Analysis

- Intrusion Analysis
- Tracking APTs and actors
- Sandboxing and code extraction
- Tools (Splunk, SolarWinds, Kali, EnCase, Wireshark, Forensic Toolkits)
- Endpoint Protection and Response (EDR)
- Damage assessment
- Timeline and Memory analysis

Remediation and Recovery

- Patches, fixes and blocking
- Server & router access lists
- White/Blacklisting
- Network Intelligence
- Self-Defending Networks

SIEM Functionality

- SIEM systems & platforms
- Threat management and intelligence
- Threat hunting
- Risk assessment
- Data analytics and coding

Intrusion Detection Case Studies - Industry specific

- Financial Services Organisations
- Public Service Organisations
- Healthcare
- Manufacturing/process control

Teaching and Learning Strategy

Online 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. The following information will be posted on moodle: tasks, expected deliverable, deadlines, assessment materials and other sources to complete assessment.

Social presence is encouraged for online delivery and requires facilitation by lecturers. 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 online delivery. This should be an iterative process whereby students will demonstrate their growing knowledge of Incident Detection and Response concepts. Constant feedback and participation by the lecturer (on social platforms, forums and VLE) and feedback on their performance of past assessment items, will be provided

Teaching presence is relevant for online deliver and should engage and challenge the student. They should want to pursue the next task and apply what they have learned. Online 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 Incident Detection and Response (IRD), assess IRD tools and implement IRD policies and remedial 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 IRD material.
- Assessment two and four (submitted online) will be summative as the learner's apply their knowledge of IRD 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***
Essay	Critically evaluate models and frameworks	20 %	Week 6	1,3
Practical Evaluation	Implement a data collection platform and collate information	20 %	Week 12	2,3
Performance Evaluation	Install and evaluate a suite of forensics, triage and analytics tools	25 %	Week 18	2,3,4,5
Project	Group project (3/4 pax) creating an IRD policy document	35 %	End of Term	1,2,3,4,5,6

Online Learning Delivery Mode Average Weekly Workload:			**4.00 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	2	Weekly	2.00
Online Learning	Tutorial covering online delivery of content via live and recorded lectures, webinars, activities, video and audio assignments	Online	2	Weekly	2.00

Required Reading Book List

Murdoch, D., (2014). *Blue Team Handbook*. CreateSpace.
ISBN 1500734756 ISBN-13 9781500734756

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

Maxwell, R., (2016). *Intelligence-driven Incident Response*. O'Reilly Media.
ISBN 1491934948 ISBN-13 9781491934944

Journal Resources

GMIT Library resources includes access to many online journals such as:

- https://academic.oup.com/cybersecurity
- https://www.journals.elsevier.com/ (variety of special issue journals relevant to IDR)
- Wiley Online Library of Journals https://onlinelibrary.wiley.com/
- Springer Cybersecurity Online https://cybersecurity.springeropen.com/
- Springer LNCS (Lecture Notes in Computer Science) https://www.springer.com/gp/computer-science/lncs

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

Associate Webinars from:

- SANS
- Immersive Labs
- Cisco Netacad PILOT programme
- Ultimate Windows Security

Guest Lectures from Industry Experts

Events and Seminars from regional entities such as Atlantec, ITAG and other RSF collaborators.

Additional Information

Online platforms such as Azure, AWS, SIREN will facilitate online delivery of module elements.

Programme Membership

GA_KCYOC_N09 202000 Certificate in Cybersecurity Operations
GA_KCYOC_V09 202000 Master of Science in Cybersecurity Operations