

Title	Threat Intelligence
Long Title	Threat Intelligence
Credits	5
NFQ Level	9

Module Description:

Threat Intelligence is emerging as a critical component in enterprise information security in combatting existing and emerging online threats. The effective application and development of threat intelligence systems requires both a clear understanding of the vulnerabilities of an organisation and the threat actors. In this module the student will develop expert knowledge of threat intelligence and utilize this knowledge to affect an improvement in security posture and combat specific advanced persistent threats.

Learning Outcomes

On successful completion of this module the learner will be able to:

- LO1** Analyse the theoretical underpinnings of threat intelligence
- LO2** Appraise the effect cybersecurity threat intelligence has on the security of an organisation
- LO3** Exploit and appraise threat intelligence to analyse and defeat specific advanced persistent threats
- LO4** Employ threat intelligence to enhance security posture
- LO5** Utilize specialized tools requiring advanced knowledge of threat intelligence

Indicative Content

Intelligence Strategy

Threat Intelligence, Trending, Reports, Critical Asset Identification, Protection Techniques, Attack Surface Risk Management.

Intelligence Aggregation

Open Source information, Human, Counter and Internal Intelligence, Data Formats, Sources Reputation Services, Aggregation of Intelligence

Intelligence Capabilities

Systems and Architecture, Services, Indicators of Compromise, Incident Prediction, Automated Response, Storing Threat Data.

Threat Analysis

Kill Chain, Threat Actor Profiling and Tracking, Big Data Analytics, Threat Data Visualization, Threat Intent, Threat Risk Profiling, YARA, MITRE ATT&CK Framework.

Operational Intelligence

Actionable Intelligence, Course of Action, Automated Proactive Defense, Manual Proactive Defense, Threat Dissemination and Intelligence Sharing, Intelligence Strategy, Process and Systems Review

Course Work

<i>Assessment Type</i>	<i>Assessment Description</i>	<i>Outcome Addressed</i>	<i>% of Total</i>	<i>Assessment Date</i>
Written Report	This report will assess the student's theoretical knowledge of threat intelligence, and the impact threat intelligence has on the security of an organisation. The student may be expected to write a current state of the art for threat intelligence and how it may be applied to a specific organisation.	1,2	40	Week 7
Project	The focus of this project will be to execute and analyse the effect a threat intelligence system has on the capacity of a network in combating a selection of advanced persistent threats. The student will be expected to employ both theoretical and practical knowledge learned in the module to perform this activity.	3,4,5	60	Sem End
No End Of Module Formal Examination				

Assessment Breakdown

Coursework

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type		Hours	Frequency	Average Weekly Learner Workload
Lecture	Lecture delivering theory underpinning learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent study.	3	Every Week	3.00
Total Hours				7.00
Total Weekly Learner Workload				7.00
Total Weekly Contact Hours				4.00

Workload – Part Time

Workload Type		Hours	Frequency	Average Weekly Learner Workload
Lecture	Lecture delivering theory underpinning learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent study.	3	Every Week	3.00
Total Hours				7.00
Total Weekly Learner Workload				7.00
Total Weekly Contact Hours				4.00

Recommended Book Resources

Roberts A.. (2021), *Cyber threat intelligence: The no-nonsense guide for CISOs and security managers*, Berkeley, CA, USA, [ISBN: 9781484272190].
 Kyle Without and Joseph Opacki. (2020), *Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs*, Packt, [ISBN: 9781801814683].