Unit outline

Name of unit
Cyber security analytics

Unit description
This unit provides a general introduction to the concepts, theories, principles, and practice of digital forensics. Topics include data acquisition and validation, forensic methodologies, file systems examination, graphics file investigation, network and email investigation, legal issues, professionalism and ethics, and also the current development in the field. This unit is self-contained. It also covers the required basics of IT systems and forensic sciences. In addition, the unit promotes and strengthens important generic skills, such as communication, analysis and inquiry. Problem solving skills in forensics as well as the skills of independent and group working, and professionalism and social responsibility are also covered,

SECTION 1 – GENERAL INFORMATION

1.1 Administrative details

Associated higher education awards (for example, Bachelor, Diploma)	Duration (for example, one semester, full year)	Level (for example, introductory, intermediate, advanced level, 1st year, 2nd year, 3rd year)	Unit coordinator
Bachelor of ICT	One semester	1st year, 2nd semester	

1.2 Core or elective unit

Indicate if the unit is a:

☒ core unit

☐ elective unit

☐ other (please specify below):

1.3 Unit weighting

Using the table below, indicate the credit point weighting of this unit and the credit point total for the course of study (for example, 10 credit points for the unit and 320 credit points for the course of study).

Unit credit points Example: 10 credit points	Total course credit points Example: 320 credit points
12.5	300

1.4 Student workload

Using the table below, indicate the expected student workload per week for this unit.

No. timetabled hours per week (1)	No. personal study hours per week (2)	Total workload hours per week (3)
4	6	10

(1) Total time spent per week at lectures, tutorials, clinical and other placements, etc.
(2) Total time students are expected to spend per week in studying, completing assignments, etc.
(3) Sum of (1) and (2) equals workload hours.

For those students requiring additional English language support, how many additional hours per week is it expected that they will undertake?

Additional English language support: ____ hours per week

1.5 Delivery mode

Tick all applicable delivery modes for the unit and provide details in the following text box: If necessary or preferred, you may provide this information in a separate document, using the 'Attach evidence here' function of the online form.

- ☒ Face to face on site
- ☐ E-learning (online)
- ☐ Intensive/block mode (where the unit or a face to face component is delivered in a block)
- ☐ Mixed/blended
- ☐ Distance/independent learning (untimetabled)
- ☒ Full-time
- ☒ Part-time
- ☐ External
- ☐ Fast track

☐ Other (please specify)

1.6 Work-integrated learning activity

If the unit includes a work-integrated learning component (where completion of the unit requires students to undertake learning in a workplace outside of their higher education provider), provide details including the rationale, the specification and methods for assessing the learning outcomes, monitoring arrangements and whether the work integrated learning is required for professional accreditation. If necessary or preferred, you may provide this information in a separate document, using the 'Attach evidence here' function of the online form.

Also if available, upload copies or templates of the formal agreements with third parties for the work-integrated learning activity, using the 'Attach evidence here' function of the online form.

Refer to the TEQSA Guidance Note on Work-Integrated Learning as required (available on the TEQSA website).

N/A

1.7 Prerequisites and co-requisites

Are students required to have undertaken a prerequisite or co-requisite unit for this unit?

☒ Yes ☐ No

If YES, provide details of the prerequisite or co-requisite requirements below.

1.8 Other resource requirements

Do students require access to specialist facilities and/or equipment for this unit (for example, special computer access, physical education equipment)?

☒ Yes ☐ No

If YES, provide details of specialist facilities and/or equipment below.

SECTION 2 – ACADEMIC DETAILS

Learning outcomes for the unit **On successful completion of this unit students will be able to:**
1. Protect local computing access and implementing local protection tools. ● Predicted difficulties: ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Mid-term test, final exam
2. Demonstrate foundation skills in safeguarding data, systems and networks. ● Predicted difficulties: ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Mid-term test, final exam
3. Understanding Access-Control and Monitoring Systems. ● Predicted difficulties: Access control, Security policies, Authentication systems ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Final exam
4. Identify approaches to digital forensics, application security and network security in the context of cyberspace. ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Mid-term test, final exam
5. Show understanding of data security, web security and cryptography and possible solutions to cyber threats. ● Predicted difficulties: ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Assignment I, final exam
6. Describe principles and policies of digital communication and cyber-security. ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Final exam
7. Demonstrate ability to evaluate relevant technical and ethical considerations related to the design, deployment and/or the uses of secure technologies within various business contexts. ● Suggested teaching methods: Lecture, tutorial

- Assessment strategies: Assignment II, final exam

Topics included in the unit
1. Infrastructure Security in the Real World
2. Data analytics, Machine Learning and Security?
3. Classifying and Clustering
4. Anomaly Detection 1.
5. Anomaly Detection 2.
6. Malware analysis
7. Network traffic analysis
8. Protecting the consumer web
9. Cyber analytics tools, models and platforms #1
10. Cyber analytics tools, models and platforms #2
11. Adversarial Machine Learning
12. Review of the past lecture

Assessment tasks			
Type	**When assessed – year, session and week (for example, year 1, semester 1, week 1)**	**Weighting (% of total marks for unit)**	**Cross reference to learning outcomes**
Lab Participation (Individual) - Students will participate in weekly lab activities and submit their work as required.	Weekly (week 2- 11)	20	1.2.4
Mid-term Test (Individual) - A 2-hour written test based on contents from weeks 1-6.	7	15	1, 2, 4

Assignment I (Individual) - Students will work on the literature research on cyber security-related analytics in the real-world cases. Identify the issues, analysing and providing the possible solutions with justifications.	9	15	5
Assignment II (Group) - In groups of 2-3, students will work students will write a no less than 2000 words report to provide solution via the cyber security analytics for the given practical scenario. Encourage to use the learned tools and software to detect the attacks and adversaries.	11	10	7
Final Exam (Individual) - A 3-hour written exam covering contents from weeks 1-12.	Exam Period	60	1, 2, 3, 4, 5, 6, 7, 8

2.1 Prescribed and recommended reading

Provide below, in formal reference format, a list of the prescribed and recommended reading for the unit.

Recommended Book:

- Dehghantanha, M. Conti, T. Dargahi, Cyber Threat Intelligence, Springers, 1st Ed., 2018

  Clarence Chio, David Freeman, Machine Learning and Security, 2017
- Basta, N. Basta, M. Brown, Computer Security and Penetration Testing, Cengage, 2nd Ed., 2014
- M. E. Whitman, H. J. Mattord, Principles of Information Security, Cengage, 6th Ed., 2018
- D. Shoemaker, K. Singler, Cybersecurity: Engineering a Secure Information Technology Organization, 1st ed., Cengage Learning, USA, 2015
- D. Sutton, Cyber Security: A Practitioner's Guide, BSC Learning and Development Ltd, UK, 2017
- S. Ali, T. A. Balushi, Z. Nadir, O. K. Hussain, Cyber Security for Cyber Physical Systems, Springers, Australia, 2018
- R. J. Robinson, Introduction to Blockchain Cyber Security, Kindle ed., 2016