COURSE OUTLINE

SEC300 Cyber Security and Threat Intelligence

School: School of Science, Technology and Engineering

2026 | Trimester 2

UniSC Sunshine Coast UniSC Moreton Bay UniSC Adelaide	BLENDED LEARNING	Most of your course is on campus but you may be able to do some components of this course online.
Online	ONLINE	You can do this course without coming onto campus, unless your program has specified a mandatory onsite requirement.

Please go to unisc.edu.au for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1. Description

This course offers an in-depth exploration of vulnerability and threat intelligence assessments in the context of networked systems and protected devices. Cyber Security is an ever-evolving field, and understanding the methods for identifying and mitigating vulnerabilities and threats is crucial to safeguarding critical information assets. Throughout the course, students will gain practical knowledge and hands-on experience to assess, prioritise, and respond to potential cyber risks effectively

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
BLENDED LEARNING			
Learning materials – Asynchronous learning material, including videos, articles and review questions	2hrs	Week 1	12 times
Tutorial/Workshop 1 – On campus workshop	2hrs	Week 1	12 times
ONLINE			
Learning materials – Asynchronous learning material, including videos, articles and review questions	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Online workshop	2hrs	Week 1	12 times

1.3. Course Topics

- Vulnerability assessment and management
- Threat intelligence assessments
- Threat modelling and risk analysis
- Incident response and handling
- Malware analysis and reverse engineering

2. What level is this course?

300 Level (Graduate)

Demonstrating coherence and breadth or depth of knowledge and skills. Independent application of knowledge and skills in unfamiliar contexts. Meeting professional requirements and AQF descriptors for the degree. May require pre-requisites where discipline specific introductory or developing knowledge or skills is necessary. Normally undertaken in the third or fourth full-time study year of an undergraduate program.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

COURSE LEARNING OUTCOMES On successful completion of this course, you should be able to...		GRADUATE QUALITIES Completing these tasks successfully will contribute to you becoming...
1	Discern and analyse evolving threats and justify the necessity of threat intelligence assessments for informed cybersecurity strategies	Knowledgeable
2	Apply advanced risk assessment methods to devise strategies for resolving intricate vulnerabilities in complex computing environments.	Creative and critical thinker
3	Design and advocate principles to address scalability, fault tolerance, and security considerations in a complex security context.	Empowered
4	Analyse and assess the influence of the vulnerability management lifecycle on its role in sustaining resilient systems over time and effectively reducing risk.	Empowered Sustainability-focussed
5	Clearly articulate insights and outcomes to specialist and non-specialist audiences.	Engaged

5. Am I eligible to enrol in this course?

Refer to the UniSC Glossary of terms for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1. Pre-requisites

SEC200 or SEC301

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

5.4. Specific assumed prior knowledge and skills (where applicable)

Not applicable

5.5. Microcredential Information

Not applicable

6. How am I going to be assessed?

6.1. Grading Scale

Standard Grading (GRD)

High Distinction (HD), Distinction (DN), Credit (CR), Pass (PS), Fail (FL).

6.2. Details of early feedback on progress

Students will participate in continuous peer and self-assessment during tutorials.

6.3. Assessment tasks

DELIVERY MODE	TASK NO.	ASSESSMENT PRODUCT	INDIVIDUAL OR GROUP	WEIGHTING %	WHAT IS THE DURATION / LENGTH?	WHEN SHOULD I SUBMIT?	WHERE SHOULD I SUBMIT IT?
All	1	Portfolio	Individual	30%	1000 words	Week 5	Online Assignment Submission with plagiarism check
All	2	Case Study	Individual	40%	1500 words	Week 10	Online Assignment Submission with plagiarism check
All	3	Oral and Written Piece	Group	30%	10 min presentation and report (1500 words)	Exam Period	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Doom Collection

GOAL:	The goal of this task is assemble a collection of open source articles on potential threats to Australia's networks and report on findings as they pertain to expert consensus on what are the most probable threats to Australia's critical infrastructures.
PRODUCT:	Portfolio
AUTHORSHIP STATEMENT:	
FORMAT:	Written report showing numerous cyber based threats facing public and private entities supporting Australia's critical infrastructure.
CRITERIA:	

No.		Learning Outcome assessed
1	Deep understanding of the identified threats, including technical details, attack vectors and potential consequences	1
2	Comprehensive analysis of the gathered information, highlighting patterns and trends in expert consensus regarding the most probable cyber threats to Australia's critical infrastructures	1
3	Well-structured and organised report that effectively communicates complex concepts	5

GENERIC SKILLS:	

All - Assessment Task 2: Threat Intelligence Analysis

GOAL:	This task will provide students with the opportunity to view and assess actual threat data as provided by an expert provider in threat intelligence and analysis.
PRODUCT:	Case Study
AUTHORSHIP STATEMENT:	
FORMAT:	Students will be presented with a threat intelligence dashboard and/or threat intelligence report concerning attempted intrusions into a protected networked system. Based on threat intelligence reporting, students will provide a detailed analysis on the details of the report and its applicability to their networked system.
CRITERIA:	

No.		Learning Outcome assessed
1	Thoroughness and accuracy of threat intelligence analysis.	1 2
2	Sound assessment of the threat intelligence's applicability to the networked system	2 3
3	Integration of vulnerability management lifecycle principles.	4
4	Clarity, organisation, and depth of report	5

GENERIC SKILLS:	

All - Assessment Task 3: Treat Scenario

GOAL:	In an effort to properly prepare students for employment in the public and private sectors, and create a capable workforce, students will construct threat intelligence cyber training scenarios for use in the public and private sectors.
PRODUCT:	Oral and Written Piece
AUTHORSHIP STATEMENT:	
FORMAT:	Each group will construct a suitable cyber security based training scenario which will offer employees the opportunity to deal with a cyber security incident. Deliverables include a report and 10 min presentation.
CRITERIA:	

No.		Learning Outcome assessed
1	Formulation of a well-designed and comprehensive scenario encompassing various aspects of a cyber security threat.	1 3
2	Alignment with current the current landscape and attack methodologies.	1
3	Clear and well-structured written and oral overview of the constructed cyber scenario	5

GENERIC SKILLS:	

7. Directed study hours

A 12-unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Student workload is calculated at 12.5 learning hours per one unit.

8. What resources do I need to undertake this course?

Please note: Course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Canvas site– Please log in as soon as possible.

8.1. Prescribed text(s) or course reader

> There are no required/recommended resources for this course.

8.2. Specific requirements

Not applicable

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low. It is your responsibility to review course material, search online, discuss with lecturers and peers and understand the health and safety risks associated with your specific course of study and to familiarise yourself with the University's general health and safety principles by reviewing the online induction training for students, and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1. Assessment: Academic Integrity

Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Canvas, are electronically checked through Turnitin. This software allows for text comparisons to be made between your submitted assessment item and all other work to which Turnitin has access.

10.2. Assessment: Additional Requirements

Eligibility for Supplementary Assessment

Your eligibility for supplementary assessment in a course is dependent of the following conditions applying:
(a) The final mark is in the percentage range 47% to 49.4%; and
(b) The course is graded using the Standard Grading scale

10.3. Assessment: Submission penalties

Late submissions may be penalised up to and including the following maximum percentage of the assessment task's identified value, with weekdays and weekends included in the calculation of days late:
(a) One day: deduct 5%;
(b) Two days: deduct 10%;
(c) Three days: deduct 20%;
(d) Four days: deduct 40%;
(e) Five days: deduct 60%;
(f) Six days: deduct 80%;
(g) Seven days: A result of zero is awarded for the assessment task.

The following penalties will apply for a late submission for an online examination:
Less than 15 minutes: No penalty
From 15 minutes to 30 minutes: 20% penalty
More than 30 minutes: 100% penalty

10.4. Links to relevant University policy and procedures

For more information on Academic Learning & Teaching categories including:

- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Central Examinations
- Deferred Examinations
- Student Conduct
- Students with a Disability

For more information, visit https://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

10.5. Student Charter

UniSC is committed to excellence in teaching, research and engagement in an environment that is inclusive, inspiring, safe and respectful. The Student Charter sets out what students can expect from the University, and what in turn is expected of students, to achieve these outcomes.

10.6. General Enquiries

For course-specific questions, contact your teaching staff or Course Coordinator.

For other enquiries or to access support, please contact Student Central:

- UniSC Student Central
- UniSC Adelaide Student Central