UNSW Course Outline

INFS5959 Cybersecurity Analytics - 2024

Published on the 23 Aug 2024

General Course Information

Course Code : INFS5959
Year : 2024
Term : Term 3
Teaching Period : T3
Is a multi-term course? : No
Faculty : UNSW Business School
Academic Unit : School of Information Systems and Technology Management
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

This course will cover the intelligence and data analysis techniques and skills that will help businesses improve their detection and response to cybersecurity attacks. These techniques can be applied before, during, and after an attack to gain actionable information that will reveal a

business' capability gaps, pain points, and requirements. Students will be exposed to the mindset, tactics, and techniques of cyber adversaries, so that they can leverage established frameworks and best practices to put forward effective countermeasures.

The course will also cover the fundamentals of digital forensics, which help business managers acquire a better understanding of what is behind the devices and systems they use, and leverage this body of knowledge to improve their organisation's incident response and threat prevention. Like police technology detectives in the 1990s, students will learn how to gather high-quality digital evidence, as well as analyse them to understand how information systems and networks can be compromised and, at the same time, how to protect them.

Course Aims

This course will equip students with knowledge on how to collect and analyse data to gain actionable information that will help an organisation prevent cyber-attacks and respond more effectively to cybersecurity incidents when they arise. The course will also cover the fundamentals of digital forensics so that students have a better understanding of the devices and systems that are frequently used in contemporary businesses, and are able to leverage this knowledge to safeguard the digital assets of the organisation and its employees.

Course Learning Outcomes

Course Learning Outcomes	Program learning outcomes
CLO1 : Review and apply modelling and intelligence techniques in response to cybersecurity threats.	• PLO1 : Research Excellence • PLO2 : Academic Excellence
CLO2 : Discuss the challenges of threat intelligence and digital forensics, and the techniques and best practices for overcoming these challenges.	• PLO1 : Research Excellence • PLO2 : Academic Excellence • PLO4 : Global Impact
CLO3 : Collect data on cyber adversaries and leverage this data to design and execute countermeasures.	• PLO1 : Research Excellence • PLO3 : Leadership • PLO4 : Global Impact
CLO4 : Acquire data analysis skills to better comprehend, interpret, and respond to complex cybersecurity threats.	• PLO1 : Research Excellence • PLO2 : Academic Excellence • PLO4 : Global Impact
CLO5 : Gather and document digital evidence in an effective and legally compliant manner.	• PLO2 : Academic Excellence • PLO5 : Social Engagement
CLO6 : Evaluate the existing digital forensics and threat intelligence capabilities of a business.	• PLO1 : Research Excellence • PLO2 : Academic Excellence • PLO3 : Leadership
CLO7 : Communicate information and findings effectively to external investigators and law enforcement agencies.	• PLO3 : Leadership • PLO5 : Social Engagement

Course Learning Outcomes	Assessment Item
CLO1 : Review and apply modelling and intelligence techniques in response to cybersecurity threats.	• Individual Assignment • Group Project
CLO2 : Discuss the challenges of threat intelligence and digital forensics, and the techniques and best practices for overcoming these challenges.	• Reflection Assessment • Individual Assignment
CLO3 : Collect data on cyber adversaries and leverage this data to design and execute countermeasures.	• Group Project • Individual Assignment
CLO4 : Acquire data analysis skills to better comprehend, interpret, and respond to complex cybersecurity threats.	• Reflection Assessment • Individual Assignment
CLO5 : Gather and document digital evidence in an effective and legally compliant manner.	• Reflection Assessment • Individual Assignment
CLO6 : Evaluate the existing digital forensics and threat intelligence capabilities of a business.	• Group Project • Reflection Assessment
CLO7 : Communicate information and findings effectively to external investigators and law enforcement agencies.	• Group Project

Learning and Teaching Technologies

Moodle - Learning Management System

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates	Program learning outcomes
Individual Assignment Assessment Format: Individual	40%		• PLO1 : Research Excellence • PLO5 : Social Engagement • PLO3 : Leadership • PLO2 : Academic Excellence
Group Project Assessment Format: Group	45%		• PLO4 : Global Impact • PLO3 : Leadership
Reflection Assessment Assessment Format: Individual	15%		• PLO1 : Research Excellence • PLO3 : Leadership • PLO2 : Academic Excellence

Assessment Details

Individual Assignment

Assessment Overview

In this assessment, each student assumes a specific role—Threat Analyst, ML/AI Specialist, UX Designer, or Incident Response Coordinator—and produces a professional document relevant to their role. The work includes developing an Intelligence Briefing, Technical Blueprint, Design Portfolio, or Incident Response Playbook. This assessment allows students to demonstrate their ability to apply theoretical knowledge to practical scenarios, focusing on cybersecurity threats, data analysis, and incident response.

Course Learning Outcomes

- CLO1 : Review and apply modelling and intelligence techniques in response to cybersecurity threats.
- CLO2 : Discuss the challenges of threat intelligence and digital forensics, and the techniques and best practices for overcoming these challenges.
- CLO3 : Collect data on cyber adversaries and leverage this data to design and execute countermeasures.
- CLO4 : Acquire data analysis skills to better comprehend, interpret, and respond to complex cybersecurity threats.
- CLO5 : Gather and document digital evidence in an effective and legally compliant manner.

Detailed Assessment Description

The assessments in this course are designed to help students develop and apply practical cybersecurity strategies using AI/ML techniques. Students will assume specific cybersecurity roles, contributing both individually and collaboratively to create a comprehensive, tangible cybersecurity solution. Throughout the course, students will also participate in peer reviews, providing feedback on each other's work to enhance learning and ensure a thorough understanding of the entire project. For more information, please refer to the assessment details provided in Moodle.

Submission notes

Threat Analyst: Sunday, Week 4, 11:59 PM o ML/AI Specialist: Sunday, Week 6, 11:59 PM o User Experience Designer: Sunday, Week 8, 11:59 PM o Incident Response Coordinator: Sunday, Week 9, 11:59 PM

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Generative AI Permission Level

Planning/Design Assistance

You are permitted to use generative AI tools, software or services to generate initial ideas, structures, or outlines. However, you must develop or edit those ideas to such a significant extent that what is submitted is your own work, i.e., what is generated by the tool, software or service should not be a part of your final submission. You should keep copies of your iterations to show your Course Authority if there is any uncertainty about the originality of your work.
If your Convenor has concerns that your answer contains passages of AI-generated text or media that have not been sufficiently modified you may be asked to explain your work, but we recognise that you are permitted to use AI generated text and media as a starting point and some traces may remain. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Group Project

Assessment Overview

This assessment requires students to collaborate in their roles to create an integrated AI-enhanced cybersecurity solution. The group project synthesizes the individual work into a

functional prototype, tool, or system that addresses identified cybersecurity threats. The assessment includes both a group component, focusing on the overall quality of the solution, and an individual component, assessing each student's contribution to the project.

- **Group Component:** 30%
- **Individual Component:** 15%

Course Learning Outcomes

- CLO1 : Review and apply modelling and intelligence techniques in response to cybersecurity threats.
- CLO3 : Collect data on cyber adversaries and leverage this data to design and execute countermeasures.
- CLO6 : Evaluate the existing digital forensics and threat intelligence capabilities of a business.
- CLO7 : Communicate information and findings effectively to external investigators and law enforcement agencies.

Submission notes

Sunday, Week 12, 11:59 PM (During Exam Week)

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Generative AI Permission Level

Simple Editing Assistance

In completing this assessment, you are permitted to use standard editing and referencing functions in the software you use to complete your assessment. These functions are described below. You must not use any functions that generate or paraphrase passages of text or other media, whether based on your own work or not.
If your Convenor has concerns that your submission contains passages of AI-generated text or media, you may be asked to account for your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Reflection Assessment

Assessment Overview

In this reflection assessment, students will critically analyze their learning journey, the contributions they made to the group project, and how they applied Intelligence and analytical

techniques in their role. The reflection provides an opportunity to evaluate personal and professional growth, the challenges encountered, and the strategies used to overcome them. Students will also consider how the skills and knowledge gained can be applied in future scenarios.

Course Learning Outcomes

- CLO2 : Discuss the challenges of threat intelligence and digital forensics, and the techniques and best practices for overcoming these challenges.
- CLO4 : Acquire data analysis skills to better comprehend, interpret, and respond to complex cybersecurity threats.
- CLO5 : Gather and document digital evidence in an effective and legally compliant manner.
- CLO6 : Evaluate the existing digital forensics and threat intelligence capabilities of a business.

Submission notes

Submission Date: Sunday, Week 11, 11:59 PM

Assignment submission Turnitin type

This assignment is submitted through Turnitin and students can see Turnitin similarity reports.

Generative AI Permission Level

No Assistance

This assessment is designed for you to complete without the use of any generative AI. You are not permitted to use any generative AI tools, software or service to search for or generate information or answers.
For more information on Generative AI and permitted use please see here.

General Assessment Information

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 0 : 2 September - 8 September	Other	Become acquainted with the course content
Week 1 : 9 September - 15 September	Lecture	Introduction to Cybersecurity in Business
	Laboratory	Introduction to Python for cybersecurity
Week 2 : 16 September - 22 September	Lecture	Threat Intelligence for Business Decision-Makers
	Laboratory	Using machine learning for threat classification - training a simple model to categorize threats
Week 3 : 23 September - 29 September	Lecture	Fundamentals of Network Security and Monitoring
	Laboratory	Anomaly detection in network traffic using unsupervised learning algorithms
Week 4 : 30 September - 6 October	Lecture	Understanding Malware and Its Business Impact
	Laboratory	Developing a basic machine learning model for malware detection
Week 5 : 7 October - 13 October	Lecture	Digital Forensics in Corporate Investigations
	Laboratory	Applying natural language processing to analyse email datasets for potential insider threats
Week 6 : 14 October - 20 October	Other	Recharge week no lecture
Week 7 : 21 October - 27 October	Lecture	Incident Response Planning for Businesses
	Laboratory	Using AI for automated incident triage and response simulation
Week 8 : 28 October - 3 November	Lecture	Threat Hunting and Proactive Security Measures
	Laboratory	Implementing a machine learning-based system for proactive threat detection
Week 9 : 4 November - 10 November	Lecture	Managing Cybersecurity Incidents in Business Contexts
	Laboratory	Developing an AI-powered dashboard for real-time incident monitoring and decision support
	Assessment	Submission: Phase 4: Prototype (Group Report)
Week 10 : 11 November - 17 November	Lecture	Emerging Trends and the Future of Cybersecurity in Business
	Laboratory	Designing and presenting an AI-enhanced cybersecurity strategy for a case study company

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

Course Resources

Recommended Resources

All essential content will be provided on Moodle.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Eila Erfani		Rm 2073, Level 2, West Wing, Quadrangle Building E15	0426946455	Wednesday 14-15	No	Yes
Lecturer	Saeed Amirgholipour Kasmani				Wednesday 13-14	No	No

Other Useful Information

Academic Information

COURSE POLICIES AND SUPPORT

The Business School expects that you are familiar with the contents of this course outline and the UNSW and Business School learning expectations, rules, policies and support services as listed below:

- Program Learning Outcomes
- Academic Integrity and Plagiarism
- Student Responsibilities and Conduct
- Special Consideration
- Protocol for Viewing Final Exam Scripts
- Student Learning Support Services

Further information is provided on the Policies and Guidelines page.

Students may not circulate or post online any course materials such as handouts, exams, syllabi or similar resources from their courses without the written permission of their instructor.

STUDENT LEARNING OUTCOMES

The Course Learning Outcomes (CLOs) – under the Outcomes tab – are what you should be able to demonstrate by the end of this course, if you participate fully in learning activities and successfully complete the assessment items.

CLOs also contribute to your achievement of the Program Learning Outcomes (PLOs), which are developed across the duration of a program. PLOs are, in turn, directly linked to UNSW graduate capabilities. More information on Coursework PLOs is available on the Policies and Guidelines page. For PG Research PLOs, including MPDBS, please refer to UNSW HDR learning outcomes.

Academic Honesty and Plagarism

As a student at UNSW you are expected to display academic integrity in your work and interactions. Where a student breaches the UNSW Code of Conduct with respect to academic integrity, the University may take disciplinary action. To assure academic integrity, you may be

required to demonstrate reasoning, research and the process of constructing work submitted for assessment.

To assist you in understanding what academic integrity means, and how to ensure that you do comply with the UNSW Code of Conduct, it is strongly recommended that you complete the Working with Academic Integrity module before submitting your first assessment task. It is a free, online self-paced Moodle module that should take about one hour to complete.

Submission of Assessment Tasks

SHORT EXTENSIONS

Short Extension is a new process that allows you to apply for an extended deadline on your assessment without the need to provide supporting documentation, offering immediate approval during brief, life-disrupting events. Requests are automatically approved once submitted.

Short extensions are ONLY available for some assessments. Check your course outline or Moodle to see if this is offered for your assessments. Where a short extension exists, all students enrolled in that course in that term are eligible to apply. Further details are available the UNSW Current Students page.

SPECIAL CONSIDERATION

You can apply for special consideration when illness or other circumstances beyond your control interfere with your performance in a specific assessment task or tasks, including online exams. Special consideration is primarily intended to provide you with an extra opportunity to demonstrate the level of performance of which you are capable.

Applications can only be made online and will NOT be accepted by teaching staff. Applications will be assessed centrally by the Case Review Team, who will update the online application with the outcome and add any relevant comments. The change to the status of the application immediately sends an email to the student and to the assessor with the outcome of the application. The majority of applications will be processed within 3-5 working days.

For further information, and to apply, see Special Consideration on the UNSW Current Students page.

LATE SUBMISSION PENALTIES

LATE SUBMISSION PENALTIES

For assessments other than examinations, late submission will incur a penalty of 5% per day or part thereof (including weekends) from the due date and time. An assessment will not be accepted after 5 days (120 hours) of the original deadline unless special consideration has been approved. In the case of an approved Equitable Learning Plan (ELP) provision, special consideration or short extension, the late penalty applies from the date of approved time extension. After five days from the extended deadline, the assessment cannot be submited.

An assessment is considered late if the requested format, such as hard copy or electronic copy, has not been submitted on time or where the 'wrong' assessment has been submitted.

For assessments which account for 10% or less of the overall course grade, and where answers are immediately discussed or debriefed, the LIC may stipulate a different penalty. Details of such late penalties will be available on the course Moodle page.

FEEDBACK ON YOUR ASSESSMENT TASK PERFORMANCE

Feedback on student performance from formative and summative assessment tasks will be provided to students in a timely manner. Assessment tasks completed within the teaching period of a course, other than a final assessment, will be assessed and students provided with feedback, with or without a provisional result, within 10 working days of submission, under normal circumstances. Feedback on continuous assessment tasks (e.g. laboratory and studio-based, workplace-based, weekly quizzes) will be provided prior to the midpoint of the course.

Faculty-specific Information

PROTOCOL FOR VIEWING FINAL EXAM SCRIPTS

UNSW students have the right to view their final exam scripts, subject to a small number of very specific exemptions. The UNSW Business School has set a protocol under which students may view their final exam script. Individual schools within the Faculty may also set up additional local processes for viewing final exam scripts, so it is important that you check with your School.

If you are completing courses from the following schools, please note the additional school-specific information:

- Students in the **School of Accounting, Auditing & Taxation** who wish to view their final examination script should also refer to this page.

- Students in the **School of Banking & Finance** should also refer to this page.
- Students in the **School of Information Systems & Technology Management** should also refer to this page.

COURSE EVALUATION AND DEVELOPMENT

Feedback is regularly sought from students and continual improvements are made based on this feedback. At the end of this course, you will be asked to complete the myExperience survey, which provides a key source of student evaluative feedback. Your input into this quality enhancement process is extremely valuable in assisting us to meet the needs of our students and provide an effective and enriching learning experience. The results of all surveys are carefully considered and do lead to action towards enhancing educational quality.

QUALITY ASSURANCE

The Business School is actively monitoring student learning and quality of the student experience in all its programs. A random selection of completed assessment tasks may be used for quality assurance, such as to determine the extent to which program learning goals are being achieved. The information is required for accreditation purposes, and aggregated findings will be used to inform changes aimed at improving the quality of Business School programs. All material used for such processes will be treated as confidential.

TEACHING TIMES AND LOCATIONS

Please note that teaching times and locations are subject to change. Students are strongly advised to refer to the Class Timetable website for the most up-to-date teaching times and locations.