ICT730 SECURITY ANALYTICS T325 BRIEF

All information in the Subject Outline is correct at the time of approval. KOI reserves the right to make changes to the Subject Outline if they become necessary. Any changes require the approval of the KOI Academic Board and will be formally advised to those students who may be affected by email and via Moodle.
Information contained within this Subject Outline applies to students enrolled in the trimester as indicated

1. General Information

1.1 Administrative Details

Associated HE Award(s)	Duration	Level	Subject Coordinator
Master of Information Technology (MIT)	1 trimester	Postgraduate	Dr M Sajjad Akbar sajjad.akbar@koi.edu.au P: +61 (2) 9283 3583 L: 7-11, 11 York Street. Consultation: via Moodle or by appointment.

1.2 Core/Elective

This subject is
- a core subject for the Master of Information Technology (MIT) Cybersecurity
- an elective subject for the Master of Information Technology (MIT) General

1.3 Subject Weighting

Indicated below is the weighting of this subject and the total course points

Subject Credit Points	Total Course Credit Points
4	MIT (64 Credit Points)

1.4 Student Workload

Indicated below is the expected student workload per week for this subject

No. Timetabled Hours/Week*	No. Personal Study Hours/Week**	Total Workload Hours/Week***
3 hours/week plus supplementary online material	7 hours/week	10 hours/week

* Total time spent per week at lectures and tutorials
** Total time students are expected to spend per week in studying, completing assignments, etc.
*** Combination of timetable hours and personal study

1.5 Mode of Delivery Classes will be face-to-face or hybrid. Certain classes will be online (e.g., special arrangements).

1.6 Pre-requisites ICT740 Applied Cybersecurity

1.7 General Study and Resource Requirements

- Students are expected to attend classes with the weekly worksheets and subject support material provided in Moodle. Students should read this material before coming to class to improve their ability to participate in the weekly activities.
- Students will require access to the internet and their KOI email and should have basic skills in word processing software such as MS Word, spreadsheet software such as MS Excel and visual presentation software such as MS PowerPoint.
- Computers and WIFI facilities are extensively available for student use throughout KOI. Students are encouraged to make use of the campus Library for reference materials.

Software resource requirements specific to this subject: Office 365, MS Imagine, MS Excel, Python.

1.8 Academic Advising

Academic advising is available to students throughout teaching periods including the exam weeks. As well as requesting help during scheduled class times, students have the following options:

- Consultation times: A list of consultation hours is provided on the homepage of Moodle where appointments can be booked.
- Subject coordinator: Subject coordinators are available for contact via email. The email address of the subject coordinator is provided at the top of this subject outline.
- Academic staff: Lecturers and Tutors provide their contact details in Moodle for the specific subject. In most cases, this will be via email. Some subjects may also provide a discussion forum where questions can be raised.
- Head of Program: The Head of Program is available to all students in the program if they need advice about their studies and KOI procedures.
- Vice President (Academic): The Vice President (Academic) will assist students to resolve complex issues (but may refer students to the relevant lecturers for detailed academic advice).

2. Academic Details

2.1 Overview of the Subject

One of the most important fields in both data science and cyber security is emerging: secure data science, which combines the two fields. This unit first provides an overview of cloud computing and big data security and privacy, then it discusses data science applications for cyber security. Additionally, it covers data science applications like malware analysis and insider threat identification. Next, the unit discusses the latest developments in adversarial machine learning and offers defences against attacks on data science methodologies. It addresses several new developments in reliable analytics, with the goal of protecting analytics methods from malevolent attacks. The concerns about privacy posed by the vast data collection are then the focus, along with possible remedies. It examines applications of services computing integration, including cloud-based services for secure data science, it looks at applications of secure data science to information sharing and social media. Students, researchers, software engineers, instructors, and managers who wish to comprehend both the technical specifics and the high-level ideas around the design and execution of safe data science-based systems may find this unit to be a helpful resource.

2.2 Graduate Attributes for Postgraduate Courses

Graduates of postgraduate courses from King's Own Institute will gain the graduate attributes expected from successful completion of a postgraduate degree under the Australian Qualifications Framework (2nd edition, January 2013). Graduates at this level will be able to apply advanced body of knowledge from their major area of study in a range of contexts for professional practice or scholarship and as a pathway for further learning.

King's Own Institute's generic graduate attributes for a master's level degree are summarised below:

	KOI Postgraduate Degree Graduate Attributes	Detailed Description
	Knowledge	Current, comprehensive and coherent knowledge, including recent developments and applied research methods
	Critical Thinking	Critical thinking skills to identify and analyse current theories and developments and emerging trends in professional practice
	Communication	Communication and technical skills to analyse and theorise, contribute to professional practice or scholarship, and present ideas to a variety of audiences
	Research and Information Literacy	Cognitive and technical skills to access and evaluate information resources, justify research approaches and interpret theoretical propositions
	Creative Problem Solving Skills	Cognitive, technical and creative skills to investigate, analyse and synthesise complex information, concepts and theories, solve complex problems and apply established theories to situations in professional practice
	Ethical and Cultural Sensitivity	Appreciation and accountability for ethical principles, cultural sensitivity and social responsibility, both personally and professionally
	Leadership and Strategy	Initiative, leadership skills and ability to work professionally and collaboratively to achieve team objectives across a range of team roles Expertise in strategic thinking, developing and implementing business plans and decision making under uncertainty
	Professional Skills	High level personal autonomy, judgement, decision-making and accountability required to begin professional practice

Across the courses, these skills are developed progressively at three levels:

- **Level 1 Foundation –** Students learn the skills, theories and techniques of the subject and apply them in stand-alone contexts
- **Level 2 Intermediate –** Students further develop skills, theories and techniques of the subject and apply them in more complex contexts, beginning to integrate the application with other subjects
- **Level 3 Advanced** – Students have a demonstrated ability to plan, research and apply the skills, theories and techniques of the subject in complex situations, integrating the subject content with a range of other subject disciplines within the context of the course

Generally, skills gained from subjects in the Graduate Certificate and Graduate Diploma are at levels 1 and 2 while other subjects in the Master's degree are at level 3.

2.3 Subject Learning Outcomes

Listed below, are key knowledge and skills students are expected to attain by successfully completing this subject:

Subject Learning Outcomes	Contribution to Course Graduate Attributes
a) Analyse which monitoring data types are most appropriate for identifying security incidents.	
b) Integrate the practice of a variety of machine learning and pattern recognition algorithms that are used in security analytics.	
c) Evaluate algorithms that are suitable for a particular security analysis assignment.	
d) Articulate machine learning and pattern recognition methods for complex security analysis assignments.	
e) Devise the correctness and efficiency of computational methods for security analytics in order to resolve real-world issues and understanding about the theoretical difficulties and new directions in security analytics research.	

2.4 Subject Content and Structure

Below are details of the subject content and how it is structured, including specific topics covered in lectures and tutorials. Reading refers to the text unless otherwise indicated.

Weekly Planner:

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
Week 1 27 Oct	Data Security and Privacy Data Mining and Security	Chapter 2 & 3	Tutorial activities on data science and lab environment configuration. Practical questions Formative not graded
Week 2 03 Nov	Big Data, Cloud, Semantic Web, and Social Network Technologies	Chapter 4	Practical question on Big Data and social network Formative not graded
Week 3 10 Nov	Big Data Analytics, Security, and Privacy	Chapter 5	Case study Big data analytics considerations Formative not graded
Week 4 17 Nov	Data Science for Malicious Executables Stream Analytics for Malware Detection	Chapter 6 & 7	Practical questions on malware detection Formative not graded

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
Week 5 24 Nov	Cloud-Based Data Science for Malware Detection	Chapter 8	Practical questions. Tutorial activities on Cloud based malware detection Formative not graded **Assessment 1 due date**
Week 6 01 Dec	Data Science for Insider Threat Detection	Chapter 9	Practical questions. Tutorial Activities Insider threat detection Formative not graded
Week 7 08 Dec	Privacy Preserving Decision Trees	Ch. 12	Practical questions. Tutorial Activities on privacy preservation Formative not graded
Week 8 15 Dec	Toward a Privacy-Aware Policy-Based Quantified Self-Data Management Framework	Chapter 13	Practical questions. Tutorial Activities on Data management Formative not graded **Assessment 2 due date**
Week 9 05 Jan	Access Control-Based Assured Information Sharing in the Cloud	Chapter 16	Practical questions. Tutorial Activities on access control Formative not graded
Week 10 12 Jan	Access Control for Social Network Data Management	Chapter 17	Practical questions. Tutorial Activities on Access Control for Social Network Formative not graded **Assessment 3 due date**
Week 11 19 Jan	Inference and Access Control for Big Data	Chapter 18	Practical questions. Tutorial Activities on Inference and Access Control for Big Data Formative not graded
Week 12 27Jan (Tue)	Revision	All chapters	Revision **Assessment 4 due date**
Week 13 02 Feb	Study review week and Final Exam Week		

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
Week 14 09 Feb	Examinations Continuing students - enrolments for T126 open		Please see exam timetable for exam date, time and location
Week 15 16 Feb	Student Vacation begins New students - enrolments for T126 open		
Week 16 23 Feb	• Results Released • Review of Grade Day for T325 – see Sections 2.6 and 3.2 below for relevant information. • Certification of Grades NOTE: More information about the dates will be provided at a later date through Moodle/KOI email.		
T126 2 Mar 2026			
Week 1 02 Mar	Week 1 of classes for T126		

2.5 Teaching Methods/Strategies

Briefly described below are the teaching methods/strategies used in this subject:

- *Lectures* (1 hour/week) are conducted in seminar style and address the subject content, provide motivation and context and draw on the students' experience and preparatory reading.
- *Tutorials* (2 hours/week) include class discussion of case studies and research papers, practice sets and problem-solving and syndicate work on group projects. Tutorials often include group exercises and so contribute to the development of teamwork skills and cultural understanding. Tutorial participation is an essential component of the subject and contributes to the development of many of the graduate attributes (see section 2.2 above). Tutorial participation contributes towards the assessment in many subjects (see details in Section 3.1 for this subject). Supplementary tutorial material such as case studies, recommended readings, review questions etc. will be made available each week in Moodle.
- *Online* teaching resources include class materials, readings, model answers to assignments and exercises and discussion boards. All online materials for this subject as provided by KOI will be found in the Moodle page for this subject. Students should access Moodle regularly as material may be updated at any time during the trimester
- *Other contact* - academic staff may also contact students either via Moodle messaging, or via email to the email address provided to KOI on enrolment.

2.6 Student Assessment

Assessment is designed to encourage effective student learning and enable students to develop and demonstrate the skills and knowledge identified in the subject learning outcomes. Assessment tasks during the first half of the study period are usually intended to maximise the developmental function of assessment (formative assessment). These assessment tasks include weekly tutorial exercises (as indicated in the weekly planner) and low stakes graded assessments (as shown in the graded assessment table). The major assessment tasks where students demonstrate their knowledge and skills (summative assessment) generally occur later in the study period. These are the major graded assessment items shown in the graded assessment

table.

Final grades are awarded by the Board of Examiners in accordance with KOI's Assessment and Assessment Appeals Policy. The definitions and guidelines for the awarding of final grades are:

- *HD High distinction* (85-100%): an outstanding level of achievement in relation to the assessment process.
- *D Distinction* (75-84%): a high level of achievement in relation to the assessment process.
- *C Credit* (65-74%): a better than satisfactory level of achievement in relation to the assessment process.
- *P Pass* (50-64%): a satisfactory level of achievement in relation to the assessment process.
- *F Fail* (0-49%): an unsatisfactory level of achievement in relation to the assessment process.
- *FW:* This grade will be assigned when a student did not submit any of the compulsory assessment items.

Provided below is a schedule of formal assessment tasks and major examinations for the subject.

Assessment Type	**When assessed**	**Weighting**	**Learning Outcomes Assessed**
Assessment 1: Research individual report (2500 words report)	Week 5	15%	a, b
Assessment 2: Individual report on data pre-processing and preliminary analysis (2500 words report)	Week 8	25%	c, d
Assessment 3: Group report: Real world use cases of data analytics (2500 words report)	Week 10	20%	e
Assessment 4: Individual Project: (2500 words report + demonstration)	Week 12	40%	a, b, c, d, e

Requirements to Pass the Subject:

To gain a pass or better in this subject, students must gain a *minimum of 50%* of the total available subject marks.

2.7 Prescribed and Recommended Readings

Provided below, in formal reference format, is a list of the prescribed and recommended readings.

Prescribed Book

Thuraisingham, B., Kantarcioglu, M., & Khan, L. (2022). *Secure Data Science: Integrating Cyber Security and Data Science.* CRC Press.

Recommended books, Website and papers

Khurana, M. & Mahajan, S. 2024, Security Analytics: A Data Centric Approach to Information Security, CRC Press, Boca Raton, FL.

Landauer, M., Skopik, F., Stojanović, B., Flatscher, A. and Ullrich, T., 2025. A review of time-series analysis for cyber security analytics: from intrusion detection to attack prediction. *International Journal of Information Security*, *24*(1), p.3.

Tarannum, R., Tanim, S.H., Ahmad, M.S. and Mithun, M.M.U., 2025. Business analytics for IT infrastructure projects: Optimizing performance and security. *International Journal of Science and Research Archive*, *14*(3), pp.783-792.

Vankayalapati, R.K., 2025. Zero-Trust Security Models for Cloud Data Analytics: Enhancing Privacy in Distributed Systems. *Available at SSRN 5121185*.

Ju, C. and Rao, G., 2025. Analyzing foreign investment patterns in the US semiconductor value chain using AI-enabled analytics: A framework for economic security. *Pinnacle Academic Press Proceedings Series*, *2*, pp.60-74.

Yedalla, J., 2025. UNMASKING INSIDER THREATS: HOW BIG DATA ANALYTICS IS REVOLUTIONIZING CYBERSECURITY DEFENSE. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS)*, *7*(2), p.4.

Sathupadi, K., Achar, S., Bhaskaran, S.V., Faruqui, N. and Uddin, J., 2025. BankNet: Real-time big data analytics for secure internet banking. *Big Data and Cognitive Computing*, *9*(2), p.24.

Useful Websites Regarding Security Analytics:

1. **Splunk**: Provides a platform for collecting, analyzing, and visualizing security data for threat detection and response.
    - Website:https://www.splunk.com/
2. **IBM Security QRadar**: IBM's security intelligence platform for threat detection, incident response, and security analytics.
    - Website: https://www.ibm.com/qradar
3. **Darktrace**: Provides AI-powered cybersecurity solutions for threat detection and autonomous response, including network traffic analysis and anomaly detection.
    - Website: https://www.darktrace.com
4. **FireEye Helix**: Offers a cloud-based security operations platform for threat detection, investigation, and response, leveraging advanced analytics and machine learning.
    - Website: https://fireeye.dev/docs/helix/
5. **Rapid7 InsightIDR**: Provides a cloud-based SIEM solution for detecting and investigating security incidents, with built-in behavior analytics and threat intelligence.
    - Website: https://www.rapid7.com

Useful Publications:

Kumar Kaulwar, P., 2025. Enhancing ERP Systems with Big Data Analytics and AI-Driven Cybersecurity Mechanisms. *Journal of Artificial Intelligence and Big Data Disciplines*, *2*(1), pp.27-35.

Vankayalapati, R.K., 2025. Zero-Trust Security Models for Cloud Data Analytics: Enhancing Privacy in Distributed Systems. *Available at SSRN 5121185*.

Rana, M., 2025. Quantum-Edge Synergy: A Novel Framework for Real-Time IoT Analytics Beyond Cloud and Edge Computing. *Journal of Information Systems Engineering and Management*, *10*(37s), pp.925-935.

Alshuaibi, A., Almaayah, M. and Ali, A., 2025. Machine learning for cybersecurity issues: A systematic review. *Secur Challenges*, *1*(2).

Yedalla, J., 2025. Building cyber-Resilient Smart Cities: The role of AI and big data in urban security. *International Journal of Science and Research (IJSR)*, *14*(2), pp.648-652.

Haider, N. and Dine, F., 2025. Cloud-Based AI for Big Data: Distributed Machine Learning Models for Real-Time Analytics.

Malali, N., 2025. Cloud-Native Security and Compliance in Life and Annuities Insurance: Challenges and Best Practices. *International Journal of Interdisciplinary Research Methods*, *12*(1), pp.50-73.

Jing, Xuyang, Zheng Yan, and Witold Pedrycz. "Security data collection and data analytics in the internet: A survey." IEEE Communications Surveys & Tutorials 21, no. 1 (2018): 586-618.