Faculty of Science, Engineering and Built Environment

SIT384 Cyber Security Analytics

Deakin University Unit Guide

Trimester 1, 2020

CONTENTS

WELCOME

Welcome to the Cyber Security Analytics (SIT384) unit. This is one of the core units within the IT security stream. This unit provides you with an in-depth examination of the various data analytical methodologies used to investigate cyber security problems. In particular, we focus on processing and analysing data relevant to cyber security systems and applications. You will be introduced to the scripting techniques and solutions required for data analytics in the context of cyber security. Applying appropriate data analytical methods and solving cyber security problems will be a key practical element of this unit.

We hope that you will enjoy studying this unit. The resources contained in this section of the unit site system, together with the prescribed/recommended textbook(s), forms the assessable content for this unit. Please take the time to familiarise yourself with the content provided. The Resource Map link on the unit site will provide you with a list of the resources contained in this section and where they are located.

Please begin your study by examining this Unit Guide. Among other information, you will find a list of staff members and their contact details should you have any queries, assessment requirements, breakdowns, and due dates, etc.

Because this unit requires you to have knowledge of critical thinking and problem solving, we strongly recommend you to be familiar with program design, data structure, and algorithms in addition to security concepts and skills. If you are feeling uncertain of your capability to study this unit, please approach your campus coordinator as early as possible for alternative arrangements.

I wish you an enjoyable and challenging Trimester 1.

Good luck,
Dr Shang Gao on behalf of the teaching team

This Unit Guide provides you with the key information about this Unit. For the best chance of success, you should read it very carefully and refer to it frequently throughout the trimester. Your Unit site (accessed in **DeakinSync**) also provides information about your **rights and responsibilities.** We will assume you have read this before the Unit commences, and we expect you to refer to it throughout the trimester.

WHO IS THE UNIT TEAM?

Unit chair: leads the teaching team and is responsible for overall delivery of this unit

Shang Gao

Unit chair details

Unit Chair and Geelong Waurn Ponds Campus Leader	
Campus:	Geelong Waurn Ponds Campus Pigdons Road GEELONG VIC 3217
Email:	shang.gao@deakin.edu.au
Phone:	+61 3 522 71383

Other members of the team and how to contact them

Melbourne Burwood Campus Leader: contact the campus leader for assistance at your campus

Name: Dr Keshav Sood

Email: keshav.sood@deakin.edu.au

Phone: +61 3 924 45519

Administrative queries

- Contact your Unit Chair or Campus Leader
- Drop in or contact Student Central to speak with a Student Adviser

For additional support information, please see the Rights and Responsibilities section under 'Resources' in your unit site.

ABOUT THIS UNIT

In SIT384 students will learn about the various data analytical methodologies used to investigate cyber security problems. In particular, we will focus on processing and analysing data relevant to cyber security systems and applications. You will be introduced to the scripting techniques and solutions required for data analytics in the context of cyber security. Applying appropriate data analytical methods and solving cyber security problems will be a key practical element of this unit.

Unit development in response to student feedback

Every trimester, we ask students to tell us, through eVALUate, what helped and hindered their learning in each Unit. You are strongly encouraged to provide constructive feedback for this Unit when eVALUate opens (you will be emailed a link).

In previous versions of this unit, students have told us that these aspects of the Unit have helped them to achieve the learning outcomes:

- Code samples, easy to understand exercises.
- The resources found in Cloud Deakin, as well as the feedback provided by the teaching staff.
- Freedom to problem solve using different methods

They have also made suggestions for improvement, and so this is what we have done:

- Tasks will be more relevant to cyber security problems.
- Learnt techniques to be more practical in real scenarios, while also explaining the importance to the cyber security field.
- Task deadline development.

If you have any concerns about the Unit during the trimester, please contact the unit teaching team - preferably early in the trimester - so we can discuss your concerns, and make adjustments, if appropriate.

Your course and Deakin's Graduate Learning Outcomes

GLO1	Discipline-specific knowledge and capabilities:	appropriate to the level of study related to a discipline or profession

GLO2	Communication:	using oral, written and interpersonal communication to inform, motivate and effect change
GLO3	Digital literacy:	using technologies to find, use and disseminate information
GLO4	Critical thinking:	evaluating information using critical and analytical thinking and judgment
GLO5	Problem solving:	creating solutions to authentic (real world and ill-defined) problems
GLO6	Self-management:	working and learning independently, and taking responsibility for personal actions
GLO7	Teamwork:	working and learning with others from different disciplines and backgrounds
GLO8	Global citizenship:	engaging ethically and productively in the professional context and with diverse communities and cultures in a global context

Each Deakin course has **course learning outcomes** which explain what the Deakin Learning Outcomes mean in your discipline. Learning in each unit builds towards the course learning outcomes.

Your Unit Learning Outcomes

Each Unit in your course is a building block towards these Graduate Learning Outcomes - not all Units develop and assess every Graduate Learning Outcome (GLO).

	These are the Learning Outcomes (ULO) for this Unit **At the completion of this Unit successful students can:**	**Deakin Graduate Learning Outcomes**
ULO1	Identify common formats of data stored and transmitted in the context of cyber security systems and applications.	GLO1: Discipline-specific knowledge and capabilities GLO3: Digital literacy GLO4: Critical thinking
ULO2	Apply and explain the principles of data analytics including classification, clustering, regression supervised learning and unsupervised learning.	GLO1: Discipline-specific knowledge and capabilities GLO2: Communication
ULO3	Implement and test small data analytics solutions to process cyber security data using scripting languages such as Python.	GLO1: Discipline-specific knowledge and capabilities GLO5: Problem solving
ULO4	Justify meeting specified outcomes through providing relevant evidence and critiquing the quality of that evidence against given criteria.	GLO4: Critical thinking GLO6: Self-management

These Unit Learning Outcomes are applicable for all teaching periods throughout the year

ASSESSING YOUR ACHIEVEMENT OF THE UNIT LEARNING OUTCOMES

Hurdle requirements

To be eligible to obtain a pass in this unit, students must meet certain milestones as part of the portfolio.

Brief summary of the hurdle requirement/s	Rationale
1. Pass tasks Students must complete the pass tasks by the indicated deadlines. This will involve submitting the tasks, responding to feedback, and ensuring work submitted demonstrates the required outcomes by the indicated dates. • Week 1 and 2 Pass Tasks by the end of Week 5 • Week 3 and 4 Pass Tasks by the end of Week 8 • Week 5 and 6 Pass Tasks by the end of Week 10 • All other tasks by the start of week 12 Where the deadline is not met, work submitted will be checked within the portfolio and must be of a passable standard in order for a pass grade to be awarded for the unit. Therefore, it is in the student's best interest to have submitted all pass tasks for feedback within the indicated timeframes. For higher grades, all Pass Tasks must be complete, and additional Credit, Distinction, and High Distinction tasks are also required.	The pass tasks in this unit provides students the opportunity to develop and demonstrate achievement of the Unit Learning Outcomes at the minimum expected standards. These tasks are included as hurdle requirements so that students are able to provide evidence of achievement of these ULOs through their portfolio. The portfolio artefact that they submit is used to measure their performance against the minimum standards as well as their ability to justify the outcomes that they have achieved through self-assessment and reflection. The hurdle requirement also provides a mechanism for student-staff interaction to check progress and address educational and motivational issues before it is too late in the trimester.

Summative assessments

(tasks that will be graded or marked)
NOTE: It is <u>your responsibility</u> to keep a backup copy of every assignment where it is possible (eg written/digital reports, essays, videos, images). In the unusual event that one of your assignments is misplaced, you will need to submit the backup copy. Any work you submit may be checked by electronic or other means for the purposes of detecting collusion and/or plagiarism.

When you are required to submit an assignment through your unit site (accessed in DeakinSync), you should receive an email to your Deakin email address confirming that it has been submitted. You should check that you can see your assignment in the Submissions view of the Assignment folder after upload, and check for, and keep, the email receipt for the submission.

- Summative assessment task 1

	Learning Portfolio
Brief description of assessment task	Assessment in this unit is designed to encourage and reward students for demonstrating achievement of the unit learning outcomes; with higher grades representing better achievement of these outcomes. The unit will use OnTrack to support the task-oriented assessment approach, with frequent formative feedback culminating in a portfolio for grading at the end of the teaching period.

	Tasks are designed to help students develop and demonstrate achievement of the unit learning outcomes. Tasks will consist of the following kinds of assessment activities: • Exploring the application of data analytics to support cyber security • Demonstrating the use of tools and programs • Writing Python scripts for pre-processing data • Writing Python scripts for building machine learning solutions • Evaluating performance of the built solutions • Reporting on findings
Detail of student output	In completing the unit tasks students will produce a range of artefacts that will be combined into their portfolio. This will include: • Python Code • Screenshot Images • Documents • Links to videos of demos Each student will receive formative feedback on these tasks and will be encouraged to incorporate the feedback received to ensure the work is of the expected standard when it is finally assessed to determine the unit grade in the portfolio.
Grading and weighting (% total mark for unit)	100% - marked and graded Each task in the unit is associated with a grade: either Pass, Credit, Distinction, or High Distinction. Each grade will be awarded based on completion of the tasks associated with that grade, and the lower grades. For this unit the following will set the minimum standard for each grade: • Pass – Complete all Pass Tasks • Credit – Complete all Pass Tasks and all Credit Tasks • Distinction – Completed all Pass, Credit, and Distinction Tasks • High Distinction – Complete Pass, Credit, and Distinction Tasks and at least 1 High Distinction Task In general, the graded tasks will provide the following challenge levels: • Pass – scaffolded tasks to help achieve minimum acceptable standard. • Credit – students will apply what they have learnt in the pass tasks to new problems with less guidance. • Distinction – students will apply their advanced knowledge to build programs of their own design that demonstrate integrated understanding of unit topics. • High Distinction – students will extend their understanding to demonstrate greater technical ability, more complex solution structures, advanced algorithms, or in other ways exceed the expectations of the unit.

This task assesses your achievement of these Unit Learning Outcome(s)	The portfolio must demonstrate that you have achieved all unit learning outcomes by proving evidence and self-reflection against each outcome. ULO1 Identify common formats of data stored and transmitted in the context of cyber security systems and applications. ULO2 Apply and explain the principles of data analytics including classification, clustering, regression, supervised learning and unsupervised learning. ULO3 Implement and test small data analytics solutions to process cyber security data using scripting languages such as Python. ULO4 Justify meeting specified outcomes through providing relevant evidence and critiquing the quality of that evidence against given criteria.
This task assesses your achievement of these Graduate Learning Outcome(s)	GLO1 through the assessment of student knowledge of cyber security problems and data analytics solutions GLO2 through the assessment of students ability of communicating the problems and performance of the solutions GLO3 through the assessment of student ability to using digital tools to capture and process data GLO4 through the assessment of student ability to critically evaluate their work against a set of outcomes GLO5 through the assessment of evidence of solving cyber security problems with data analytics methods. GLO6 through the assessment of student ability to reflect on their learning to determine areas of growth and areas that require further improvements.
How and when you will receive feedback on your work	Students will be required to work on and submit tasks for formative feedback each week. The teaching team will then review progress and provide individual feedback to each student to assist them in completing the tasks and achieving their target grade for the unit. To ensure that there is sufficient time to staff to provide feedback, and to help manage the learning process, tasks will have set target dates and deadlines. The target date is the date that the task is considered to be due, however, as this may require additional fixes in order to incorporate feedback provided, the work can be resubmitted up to the deadline. Work submitted after the deadline will be checked in the portfolio, and additional formative feedback will not be provided.
When and how to submit your work	At the end of the unit you will use the online task management tool to combine together the artefacts you have created and a learning summary report into a single portfolio for assessment by the end of week 12 (Sunday, 7 June 2020 by 11.59pm AEST)

Your learning experiences in this Unit - and your expected commitment

To be successful in this unit, you must:

- Read all materials in preparation for your classes or seminars, and follow up each with further study and research on the topic;
- Start your assessment tasks well ahead of the due date;
- Read or listen to all feedback carefully, and use it in your future work;
- Attend and engage in all timetabled learning experiences as follows:

Scheduled learning activities - campus

2 x 1 hour classes per week, 1 x 2 hour practical per week.

Scheduled learning activities - cloud

1 x 1 hour scheduled online workshop per week.

Students will on average spend 150 hours over the trimester undertaking learning and assessment activities for this unit. This also includes engaging in online learning activities, assessment activities, readings and study time. Students are expected to complete all allocated learning and assessment tasks for each week and actively engage in discussions with other students and teaching staff. This unit requires students to complete milestones as they progress through the unit. This requirement is to ensure that students engage with teaching staff throughout the unit. This unit has been designed to provide all students with a high level of interaction and feedback from teaching staff as a strategy to support student success.

In the online task management system:

- Task sheets
- Task resources, as required
- Individual feedback
- Alignment of tasks to unit learning outcomes
- Visualisations of your progress to help keep you on track

Your work in this unit starts on Day 1 of the trimester. You are expected to complete the prescribed readings, reproduce the practical tasks shown in the classes, and complete unit tasks in the online task management system. As you complete the tasks, you will be able to collect evidence for justifying how you have met the unit learning outcomes through your portfolio. The process of developing your portfolio is simple and easy, so keep that in mind as you read the assessment instructions below.

In order to understand how assessment in this unit works, let’s consider standard assessment practices. A typical unit has assignments and tests that you submit and get marks for. The problem is, you only get one chance to succeed, and any marks you lose are gone. This focuses your attention on marks, rather than on working to achieve good learning outcomes.

To focus your attention on learning in this unit, we avoid having marks for tasks during the unit and instead assess your final work to see how well you have achieved the outcomes at the end of the unit. This is the summative assessment at the end of the unit, where your grade is determined by the evidence you present in your portfolio.

We will work with you by providing formative feedback for these task as you submit them week by week. When you submit a task, we will review your work and provide you with feedback. Where your work does not correctly demonstrate the required outcomes, we will give you feedback to help enhance your learning and improve your work for your final portfolio submission. You then need to fix and resubmit the work, so we can check it again and sign it off as Complete when you have achieved the required standard.

We will keep track of all of this in the online task management system, which is where you submit work, receive feedback, resubmit it, and then finally see it signed off as Complete. The process for you is then just a matter of working through the required tasks week by week, and work with us to make sure they are ready for your final portfolio submission. At the end of the unit you can then combine together all of your work on the tasks and submit it for marking and grading.

So, learning in this unit is as simple as setting your target grade, and completing the unit tasks associated with that grade in the online task management system. The teaching team will work with you in providing weekly feedback so that you can achieve the goals you set, demonstrate your ability to complete the unit tasks and discuss your performance with confidence.

Note

At Deakin,

- *Lectures* are referred to as *classes* (definition: a general meeting for all students, for which students do not need to register and where students are engaged through presentations and learning activities)
- *Tutorials, workshops and seminars* are referred to as seminars (definition: more interactive meetings for smaller groups of students).
- For the complete list of agreed definitions for learning experiences, see the Course Design and Delivery Procedure.

UNIT LEARNING RESOURCES

Your unit learning resources are available in your unit site accessed in DeakinSync.

Prescribed text(s): Müller and Guido, 2017, Introduction to Machine Learning with Python: A Guide for Data Scientists, 1st Ed, O'Reilly Media.
The texts and reading list for the unit can be found on the University Library via the link below: SIT384 Note: Select the relevant trimester reading list. Please note that a future teaching period's reading list may not be available until a month prior to the start of that teaching period so you may wish to use the relevant trimester's prior year reading list as a guide only.

Essential learning resources

The prescribed textbook (as outlined above) can be purchased from the DUSA Bookshop:

Textbooks, reference books, general books and software may be ordered from the bookshop:

- phone 1800 686 681 (freecall);
- email to DUSA-Bookshop@deakin.edu.au; or
- order online from the University bookshop web site at http://www.dusabookshop.com.au/

Recommended learning resources

- Conway, 2012, Machine Learning For Hackers, 1st Ed, O'Reilly
- O'Conner, 2012, Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, 1st Ed, Syngress

KEY DATES FOR THIS TRIMESTER

Trimester begins (classes begin)	Monday 9 March 2020
Intra-trimester break (a short break during trimester)	Friday 10 April - Sunday 19 April 2020
Trimester ends (classes cease)	Friday 29 May 2020
Study period (examination preparation period)	Monday 1 June - Friday 5 June 2020
Examinations begin	Monday 8 June 2020

Examinations end	Friday 19 June 2020
Inter-trimester break (the period between trimesters)	Monday 22 June - Friday 10 July 2020
Unit results released	Thursday 9 July 2020 (6pm)

UNIT WEEKLY ACTIVITIES

Week	Commencing	Topic	Assessment activity
1#	9 March 2020	Introduction to SIT384 and Python	Submit week 1 tasks
2	16 March	Packages in Python	Submit week 2 tasks
3	23 March	Data analysis with Python	Submit week 3 tasks
4	30 March	Supervised learning (1)	Submit week 4 tasks
5^	6 April	Supervised learning (2)	Submit week 5 tasks
6	20 April	Unsupervised learning (1)	Submit week 6 tasks
7*	27 April	Unsupervised learning (2)	Submit week 7 tasks
8	4 May	Other machine learning models	Submit week 8 tasks
9	11 May	Model evaluation and improvement	Submit week 9 tasks
10	18 May	Cyber security case studies	Submit week 10 tasks
11	25 May	Unit Review	Finalise any outstanding tasks
12 (study week)	1 June	Study period	Learning Portfolio due

#Victorian Labour Day public holiday: **Monday 9 March** – University open

^Easter vacation/intra-trimester break: **Friday 10 April - Sunday 19 April 2020** (between weeks 5 and 6)

*ANZAC Day observed, **Monday 27 April (in lieu of 25 April)** - University closed