Data Analytics for Cyber Security

CT115-3-M (Version E)

Introduction and Module Overview

Lecturer Information

- Lecturer Name: Assoc. Prof. Dr. Thang Ka Fei
- Email: ka.fei@apu.edu.my
- Consultation Hours: Book via MS Teams messaging.

Pre-Requisites For This Module

- Nil.

Outcomes Based Education

- OBE is education based on producing particular educational outcomes that:
  - ➤ Focus on what students can actually do after they are taught.
  - ➤ Expect all learners / students to successfully achieve particular (sometimes minimum) level of knowledge and abilities.

- It's NOT what We want to teach.
- It's WHAT You should learn.

Aims of this Module

1. This module will familiarise students with models and algorithms for machine learning, reinforcing the thesis of injecting data analytics into security operations to efficiently uncover patterns and identify indicators of compromise.

2. The theory and principles will be presented with a focus on practical experience with using industry standard frameworks for implementation and using data visualization techniques and strategies to communicate information.

3. This will prepare them to critically assess and evaluate business problems using pattern discovery and predictive modelling in research or industry applications.

Module Learning Outcomes

CLO	Learning Outcomes	Assessment
1	Explain the procedures of data analysis with appropriate machine learning technique based on the scenario of a cyber attack (C5,PLO2)	Class Test
2	Appraise the most suitable technique or method to uncover patterns and extract valuable insights of a possible cyber attack (C4, PLO7)	Assignment 1 (Individual)
3	Perform data analysis using suitable machine learning techniques to detect attack signatures and identify relevant evidence (A5, PLO6)	Assignment 2 (Group)

Mapping of CLO with PLO

	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5	PLO 6	PLO 7	PLO 8	PLO 9	PLO 10	PLO 11	PLO12
CLO1		✓										
CLO2							✓					
CLO3						✓						

The learning domains are:
PLO2: Cognitive Skills
PLO6: Digital Skills
PLO7: Numeracy Skills

Student Learning Time

- Module Credit Value: 3
- Total Learning Hours: 120 per semester

Lecture	18 hours
Tutorial	0 hours
Practical	24 hours
Others	0 hours
Independent Learning Time	76 hours
Assessment	2 hours
Total Learning Hours	120 hours per semester

Module Content Outline

Week	Topic
1	Machine Learning Methods
2	Machine Learning Model Logic
3	Machine Learning Pipeline
4	Data Preprocessing for Machine Learning
5	Machine Learning Performance Evaluation
6	Machine Learning: Algorithms in Practice
7	Model Optimisation Strategies
8	Assignment Briefing
9	Model Selection
10	Machine Learning: Review & Revision
11	Deep Learning
12	Natural Language Processing

Assessment Summary (refer to module handbook and module descriptor)

Form of Assessment	Assessment Methods	Hand Out Date	Hand In Date	%

Continuous Assessment	Assignment:
	    Individual – 50%
	    Group – 20%
		8th Week	12th Week	70%

Final Assessment	Class Test	11th week	11th week	30%

Assessment requirement:

To pass the module, you must attempt every element of assessment and achieve at least 50% in the module overall.

Expectations

1. Abide by ALL rules and regulations of APU.
2. Proper attire.
3. No speaking of dialects during class.
4. Attendance is compulsory. Valid Medical Certs must be supported in any absence from class.
5. Three cases of Late will be equal to 1 absence.
6. Use proper academic references – APA Referencing only.
7. Academic Dishonesty / Plagiarism is a serious offence. Any suspicions will be referred to the University's Academic Dishonesty Board.
8. Formal assessments must be submitted on time in the specified format given. Failure to meet deadlines will be treated as non-submission and no marks will be awarded. Incomplete submissions will be subjected to penalty of mark deductions or forfeit.

Achievement Requirements:
Postgraduate Programmes

Marks	Alphabetical Grade	Grading Point	Classification
80-100	A+	4.0	Distinction
75-79	A	3.8	
70-74	B+	3.6	Merit
65-69	B	3.5	
60-64	C+	3.3	Pass
55-59	C	3.2	
50-54	C-	3.0	
40-49	D	2.5	Fail (marginal)
30-39	F+	2.0	Fail
20-29	F	1.5	Fail
10-19	F-	1.0	Fail
0-9	U	0	Unclassified

Reference Materials

Course Materials available in Moodle

- Module handbook
- Module descriptor
- Lecture slides
- Tutorial/Lab materials
- Sample incourse questions & answers
- Sample exam questions & answers

Essential and Further Readings

- Aurélien Géron (2022). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems (3rd Edition). O'Reilly Media; ISBN: 978-1098125974
- Jason Brownlee (2021). Machine Learning Mastery With Python: Understand Your Data, Create Accurate Models and Work Projects End-To-End. Independently published; ISBN: 979-8540446273

*Further readings will be assigned from time to time.

Your Valuable Feedback

- You are welcome to discuss your views on this module at any point of time.

- Do fill in anonymous evaluation questionnaires in the student feedback form. There are two points - mid and end of the teaching semester.

- The feedbacks you provide will be constructive for improvement of teaching and module content development.