MODULE SPECIFICATION

Part 1: Information			
Module Title	Security Data Analytics and Visualisation		
Module Code	UFCFEL-15-3	Level	Level 6
For implementation from	2018-19		
UWE Credit Rating	15	ECTS Credit Rating	7.5
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Contributes towards			
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Overview: In our modern technological society, data is gathered and stored for a variety of applications. Many security, and cyber-security, applications are beginning to utilise the large volumes of data that now exist, in order to allow security analysts to make well-informed decisions that relate to the organisations, the assets, and the people, that they are tasked with protecting.

This module is designed to take a modern data-driven approach to security analysis. With this, large volumes of data can be effectively managed to better support security analysts in their tasks of understanding and reasoning about the current state of their security.

From computer network traffic analysis to user behavioural analytics, we shall consider the variety of different data sources that can be processed, and utilised, in modern security applications.

Educational Aims: With practical assignments and coursework that allow students to develop their own tools for conducting such analytics, this course offers would-be analysts the ability to manipulate, visualize, and learn from, ever-growing large datasets.

Outline Syllabus: In this module you will cover:

Background of Data-driven security - how data is changing the way we think about security?

A simple example, (the equivalent of Hello World in programming) of Security Data Analysis – understanding the pipeline of developing data analytic tools for security applications.

Common tools and data sources that are used to conduct analysis in security domains.

Data cleansing and data pre-processing – how should the data be prepared to best support our intended application?

Machine learning – regression, classification, dimensionality reduction – how can machine learning support security data analytics

Data visualization – what is the message that we are trying to convey from our data, and what is the appropriate way to achieve this?

Visual analytics and user interaction – how can the analyst explore and interact with the data and with the underlying model in our pipeline?

Applications of security data analytics – spam filtering, intrusion detection, insider threat detection, geographic and systems visualization.

Teaching and Learning Methods: Teaching will consist of 1 one-hour session each week, where the core module content will be taught via lectures and in-class discussion. In addition, there will be 1 two-hour lab session each week, where students can develop the ideas and concepts that have been discussed in lectures through practical worksheets (10% of the grade).

Part 3: Assessment

The assessment of this module consists of :

2-hour written examination assessment - will reaffirm the theoretical understanding of security data analytics, including the development of an appropriate system pipeline and understanding the various components such as data pre-processing, data reduction, and data visualization.

One coursework assignment will be issued during the course which will allow students to demonstrate their understanding and application of the course material. The coursework assignment will bring together a variety of the course topics, and allow the students to apply this to a particular case study exercise. Typically, this will involve designing and developing an appropriate data analytics tool for solving a particular problem scenario or case study, such as identifying suspicious users from e-mail conversations, identifying malicious network activity, or identifying movement patterns of interest from GPS data. All datasets for this course are public, open-source, and readily available online.

Practical lab worksheets will be used during the practical sessions of the course. These are designed to encourage student engagement, and to build the foundational knowledge for then developing the coursework. All worksheets will need to be signed off as completed by the course leader (once the student has demonstrated this to be the case), before the submission date.

The resit will consist of an examination, coursework, and practical exercise worksheets. Whilst the practical worksheets may not be expected to be signed off and demonstrated in lab sessions, the students should complete these and provide evidence (e.g., screenshots) of the software.

First Sit Components	Final Assessment	Element weighting	Description
Practical Skills Assessment - Component B		10 %	Signed off and demonstrated practical worksheets
Examination - Component A	✓	50 %	Examination (2 hours)
Case Study - Component B		40 %	Coursework
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Practical Skills Assessment - Component B		10 %	Evidence of completed practical worksheets
Examination - Component A	✓	50 %	Examination (2 hours)
Case Study - Component B		40 %	Coursework

Part 4: Teaching and Learning Methods

Learning Outcomes

On successful completion of this module students will be able to:

	Module Learning Outcomes
MO1	Understand the emerging role that data analytics plays in security applications.
MO2	Identify appropriate sources of data for informing security decision-making.
MO3	Develop a variety of analytical tools for exploring, analysing, and making sense of large data in the context of security problems.
MO4	Develop an appropriate pipeline for security data analytics that incorporates modern databases, machine-learning concepts, and visualization.
MO5	Evaluate best practice of how to process and visualize different forms of data.

Contact Hours

Contact Hours	
Independent Study Hours:	
Independent study/self-guided study	114
Total Independent Study Hours:	114
Scheduled Learning and Teaching Hours:	
Face-to-face learning	36

	Total Scheduled Learning and Teaching Hours:	36
	Hours to be allocated	150
	Allocated Hours	150
Reading List	*The reading list for this module can be accessed via the following link:* https://uwe.rl.talis.com/modules/ufcfel-15-3.html	