MODULE SPECIFICATION

Part 1: Information			
Module Title	Security Data Analytics and Visualisation		
Module Code	UFCFEL-15-3	Level	Level 6
For implementation from	2020-21		
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		
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.

Part 3: Assessment

The assessment of this module consists of a project portfolio and a presentation. In the portfolio, students will complete and write up a set of practical lab exercises set during the module, that cover topics such as network traffic analysis, malware detection, and insider threat detection. Students will be expected to show a working demonstration of their practical implementation. The portfolio component will elaborate on the practical implementation, so that students can describe the work conducted and provide critical evaluation and reflection. Students will then present their portfolio to demonstrate understanding and further insight into the domain applications.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A	✓	25 %	Portfolio presentation to demonstrate learning and reflection from the portfolio exercises.
Case Study - Component B		75 %	Portfolio - a set of practical lab sheets complete with implementation and write-up
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A	✓	25 %	Portfolio presentation
Case Study - Component B		75 %	Portfolio - a set of practical lab sheets complete with implementation and write-up

Part 4: Teaching and Learning Methods

Learning Outcomes

On successful completion of this module students will achieve the following learning outcomes:

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

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

Part 5: Contributes Towards

This module contributes towards the following programmes of study:

Forensic Computing and Security {Dual} [Mar][FT][Taylors][3yrs] BSc (Hons) 2018-19

Forensic Computing and Security {Dual} [Aug][FT][Taylors][3yrs] BSc (Hons) 2018-19