Module Specification

Security Data Analytics and Visualisation

Version: 2023-24, v3.0, 12 Jun 2023

Contents

Part 1: Information

Module title: Security Data Analytics and Visualisation

Module code: UFCFEL-15-3

Level: Level 6

For implementation from: 2023-24

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body 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.

Features: Not applicable

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.

Part 3: Teaching and learning methods

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.

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

MO1 Understand the role that data analytics plays in cyber security and related applications.

MO2 Develop appropriate pipelines and tools for security data analytics that incorporates machine-learning concepts and data visualization.

MO3 Evaluate best practice of how to process and visualize different forms of data to address task-specific needs in cyber security.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/modules/ufcfel-15-3.html

Part 4: Assessment

Assessment strategy: The assessment of this module consists of a project portfolio. In the portfolio, students will complete 3 practical lab exercises that cover key topics from the module, primarily on network traffic analysis, malware classification, and insider threat detection. Students will be expected to write suitable program code that provides a practical solution to each challenge, and should be able to provide a written narrative of how they solved each task that demonstrates understanding and critical reflection of their work.

Resit strategy.
In the cases where a resit is required, students will be tasked with a set of 3 similar exercises to that of the main run, however, using different data sets. This will enable students to focus on the methodology of solving the tasks programmatically, despite working with different data sets to that of the main run.

Assessment tasks:

Portfolio (First Sit)
Description: Portfolio - a set of practical lab sheets complete with implementation and writeup
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Portfolio (Resit)
Description: Portfolio - a set of practical lab sheets complete with implementation and writeup
Weighting: 100 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Information Technology {Top-Up} [INTUNI] BSc (Hons) 2023-24

Information Technology {Top-Up} [Gloscoll] BSc (Hons) 2023-24

Information Technology {Top-Up} [Frenchay] BSc (Hons) 2023-24

Information Technology {Top-Up} [INTUNI] BSc (Hons) 2023-24

Information Technology {Top-Up} [Frenchay] BSc (Hons) 2022-23

Information Technology {Top-Up} [INTUNI] BSc (Hons) 2022-23

Computer Science [Sep][FT][Frenchay][3yrs] BSc (Hons) 2021-22

Computer Science [Sep][FT][Villa][3yrs] BSc (Hons) 2021-22

Computer Science [Jan][FT][Villa][3yrs] BSc (Hons) 2021-22

Computer Science [May][FT][Villa][3yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics [Sep][FT][Frenchay][3yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics [Jan][FT][NepalBrit][3yrs] BSc (Hons) 2021-22

Forensic Computing and Security {Dual} [Mar][FT][Taylors][3yrs] - Not Running BSc (Hons) 2021-22

Forensic Computing and Security {Dual} [Aug][FT][Taylors][3yrs] - Not Running BSc (Hons) 2021-22

Information Technology {Dual}[Mar][FT][Taylors][3yrs] BSc (Hons) 2021-22

Computer Science {Foundation}[Sep][FT][Frenchay][4yrs] BSc (Hons) 2020-21

Computer Science [Sep][SW][Frenchay][4yrs] BSc (Hons) 2020-21

Forensic Computing and Security {Foundation} [Sep][FT][Frenchay][4yrs] - Not Running BSc (Hons) 2020-21

Forensic Computing and Security [Sep][SW][Frenchay][4yrs] - Not Running BSc (Hons) 2020-21

Cyber Security and Digital Forensics [Sep][SW][Frenchay][4yrs] BSc (Hons) 2020-21

Cyber Security and Digital Forensics {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2020-21

Forensic Computing and Security {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2019-20