UWE Bristol | University of the West of England

Presentation by

Dr. Phil Legg

Associate Professor in Cyber Security

Security Data Analytics and Visualisation

6: Reflection and Worksheet 3

Date: Autumn 2019

Recap

- Last week we looked at different visualisation methods and visual channels
  - We also looked at examples of visual security analytics


PAUSE

What have we covered so far?

Questions about course so far?

Coursework Portfolio

- You should be well on the way to completing worksheet 1 and 2 already
- Worksheet 3 is issued **today** and is worth 35% of the overall module
  - It is a much larger assignment than the previous two
  - It is a graded task, rather than a Pass / Fail task
  - There are four possible exercises – **check which dataset you have been assigned to – completing the wrong dataset will result in a fail for the worksheet**
  - It is an **individual** exercise – any evidence of plagiarism will be investigated – *make your report your own!*

- Let's just have a brief look at this…

Coursework Portfolio

A brief summary of Worksheet 3:

You are tasked to carry out an investigation of a suspected insider threat. You will need to produce a report using Jupyter Notebooks that documents your investigation process, shows your analysis and your visualisations for examining the data using Python code, and reports on the overall findings.

Coursework Portfolio

For this assignment, you will be given a grade out of a possible maximum of 35.

- **Up to 10 marks** for identifying the user, complete with excellent justification and rationale of why they are suspected and identifying all potential indicators of threat across the different data available.
- **Up to 10 marks** for excellent analytical processes used to manipulate and examine the data carry out the investigation, with good demonstration of creative thinking.
- **Up to 10 marks** for excellent visualisation techniques adopted for examining the data, with good demonstration of how this informs the narrative for the reader.
- **Up to 5 marks** for clarity and professional presentation of your work.

To achieve the higher end of the grade scale, you need to demonstrate creativity in how you approach the problem of identifying malicious behaviours, and ensure that you have accounted for multiple anomalies across the set of data available.

Coursework Portfolio

Tips:

Look on Blackboard at the worksheet – I have given you some code to get started… figure out what it does and how you can make best use of this? There's a lot of users to deal with, so think hierarchically to decompose the problem…

I have provided a syntax guide that shows some examples of manipulating pandas dataframes – such as accessing columns and filtering data – material from your previous worksheets will also come in handy!

See what data is available in each file, and think about the possible ways that a user could be identified as an anomaly – *think about what you are comparing the anomaly against to make this judgement*

Use the documentation of Pandas / Matplotlib – and if in doubt, google what you want to do in pandas and you'll probably find someone has already done it on StackOverflow!

Coursework Portfolio

Worksheet 3 requires no lab sign-off – but do ensure you include comprehensive Markdown to curate your report so that the reader can follow the findings of your investigation clearly.

Worksheet 1 and 2 can be signed off up until Thursday 12th December
(but only during the scheduled lab sessions on Mondays and Tuesdays!)

All 3 worksheets should be saved as HTML (or PDFs of the HTML page), zipped, and submitted to Blackboard by Thursday 12th December 2019.

Any coursework questions?

Faculty Feedback Fortnight

Use the post-it notes to jot down your thoughts comments on the module so far

(I'll step outside for 5 minutes)