EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

Student: Andrew Rocke **Supervisor: Petros Karadimas**

Date: 31/12/2024 **Last diary date: 16/11/2024**

Objectives:

Initial report to be submitted on 29/11/2024 3000-word literature review with 3 paragraphs, namely ICS, IDS and Machine learning with a conclusion

Identified Latex Napier thesis outline and made thesis use main sections

Progress:

Researched the Machine Learning topic, lots of good papers on machine learning. Found the excellent paper identifying pitfalls

```
@inproceedings{arp2022and,
  title={Dos and don'ts of machine learning in computer security},
  author={Arp, Daniel and Quiring, Erwin and Pendlebury, Feargus and Warnecke, Alexander and Pierazzi, Fabio and Wressnegger, Christian and Cavallaro, Lorenzo and Rieck, Konrad},
  booktitle={31st USENIX Security Symposium (USENIX Security 22)},
  pages={3971--3988},
  year={2022}
}
```

Identified Random Forests for Binary Classification and decided to base experiment on this

Manages to run Snort on a PCAP using community Rules

Supervisor's Comments:

Title Title	Very good and intuitive
Summary of project	Really good and relevant to the student's programme.
Literature review	Very good with up-to-date references. A small paragraph at the end is missing to summarise again the contribution of the thesis.
Annotated contents list	No issues identified.
References	References are very good and up-to-date.

Work plan	It seems reasonable. Maybe more time should be allowed to the SNORT implementation just in case there are debugging issues.
Writing style	The writing style is appropriate with no issues.
Problems foreseen	The methodology seems quite robust and unless debugging issues appear, there is no problem forseen.
Any other comments	The work is very relevant to the student's programme and quite interesting as an approach. I cannot wait to read the rest of the thesis.