Wednesday, 5th July 2023
Prepared by Dr Charles Clarke

Windows Event Log Analytics

BACKGROUND AND MOTIVATION

Windows Event Logs provide wealth of information for system monitoring, troubleshooting, security, compliance, performance analysis, and more. Leveraging these logs effectively can improve system reliability, enhance security, optimize performance, and streamline IT operations. However, working with Windows Event Logs can pose many challenges. For example; log volume and scalability, log collection, management, storage and Retention; log filtering, parsing, analysis and correlation; log monitoring, alerting, security and integrity; log compatibility, versioning and performance impact; understanding logs and interpreting them.

PROBLEM

How can Windows Event log data be analysed and visualised in a manner that is interactive and intuitive for system administrators?

AIMS

The primary aims of this project are to work with a Windows Event Log data set and to create way for prospective system administrators to:

- Interactively query event logs
- Visualise event logs
- Identify correlations in the event log dataset

OBJECTIVES

- Research existing windows event log tools for working with Windows Event Logs.
- Research techniques for preparing, structuring, managing Windows Event Log raw data.
- Design an artefact that can be used for interaction with Windows Event Log data.
- Acquire resources and deploy the architecture for the artefact.
- Implement the artefact.
- Test the artefact with users.
- Capture and interpret results from testing.

TECHNOLOGIES & RESOURCES (INDICATIVE)

- Windows, Linux, Python, Splunk, Grafana, ELK Stack, Matplotlib

NEXT STEPS

- Confirm that you would like to work on this project by emailing a member of the Cyber Group supervision team.
- Organise a meeting with your supervisor.