National College of Ireland

Configuration Manual

MSc Research Project

MSc in Cybersecurity

Devanshu Saboo

Student ID: X23271370

School of Computing

National College of Ireland

Supervisor: Evgeniia Jayasekera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Devanshu Bharat Saboo
Student ID:	x23271370
Programme:	MSc. Cybersecurity **Year:** 2025-2026
Module:	MSc (Research) Practicum
Supervisor:	Evgeniia Jayasekera
Submission Due Date:	11/12/2025
Project Title:	Sequence Aware Machine Learning for Attack Pattern Detection in SIEM systems
Word Count: 671	**Page Count:** 4

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Devanshu Saboo

Date: 08/12/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only

Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Devanshu Saboo
Student ID: x23271370

1 Introduction

This Configuration Manual provides a concise guide for setting up and running the SIEM Anomaly Detection System developed for this project. The system collects Windows Security, System and Application logs. It then processes them into 5 minutes of event sequences and then applies both frequent pattern analysis and machine learning methods to detect anomalies. The manual outlines the essential environment configuration, required libraries, log collection steps, data handling procedures and instructions to execute the anomaly detection pipeline.

2 System Requirement

2.1 Hardware Requirement

The implementation was performed on an Acer Nitro 5 laptop. The specifications of the laptop are as below:

1. Processor: Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz
2. Ram: 24.0 GB
3.Storage: 1 TB
4. Operating System: Windows 11 Home Single Language, 24H2, 64-bit operating system

2.2 Software Requirement

External libraries installed and their version numbers are as below:
Note: Only externally downloaded libraries are listed here, no pre-installed libraries are listed.

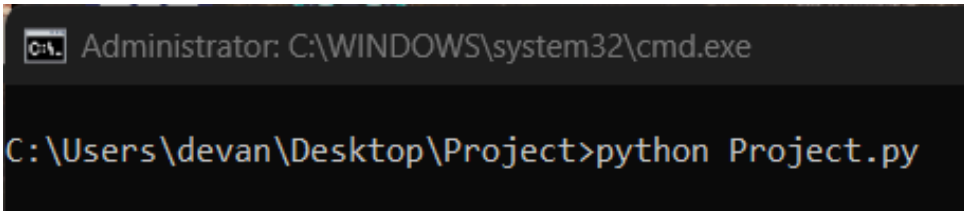
Software/Library	Version
Python	3.10
Pywin32	305
Pandas	2.2.1
Numpy	1.26.4

Scikit-learn	1.4.1
Matplotlib	3.8.2
PySide6	6.6.1

3 Execution

Open the command terminal and install all the above libraries listed above using the pip install command. You can also run this script in a virtual environment using the command "python -m venv venv". After all necessary libraries are installed, open the **command terminal as an administrator**, if the terminal is not opened as an administrator, the script will fail to execute and will not work.

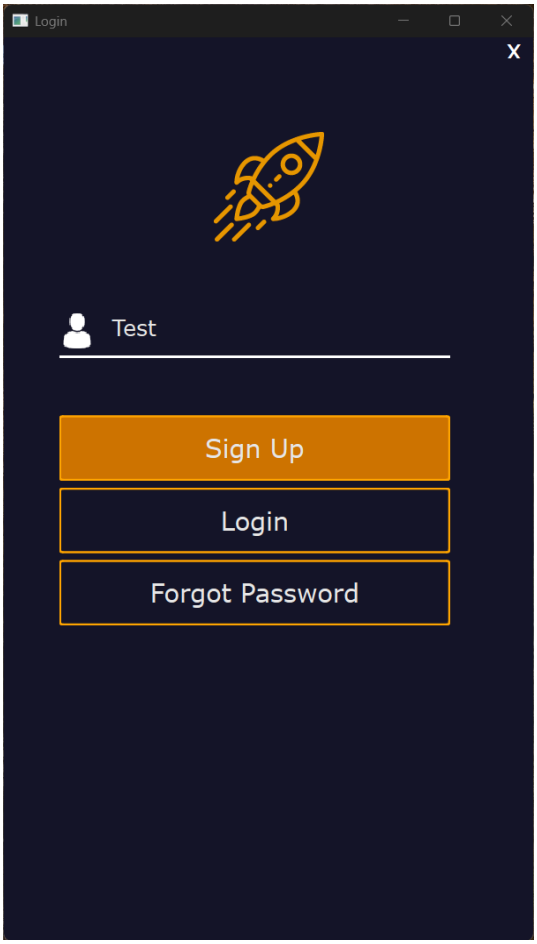
Browse to the directory where the files have been extracted using the cd command and run the command **"python Project.py".**



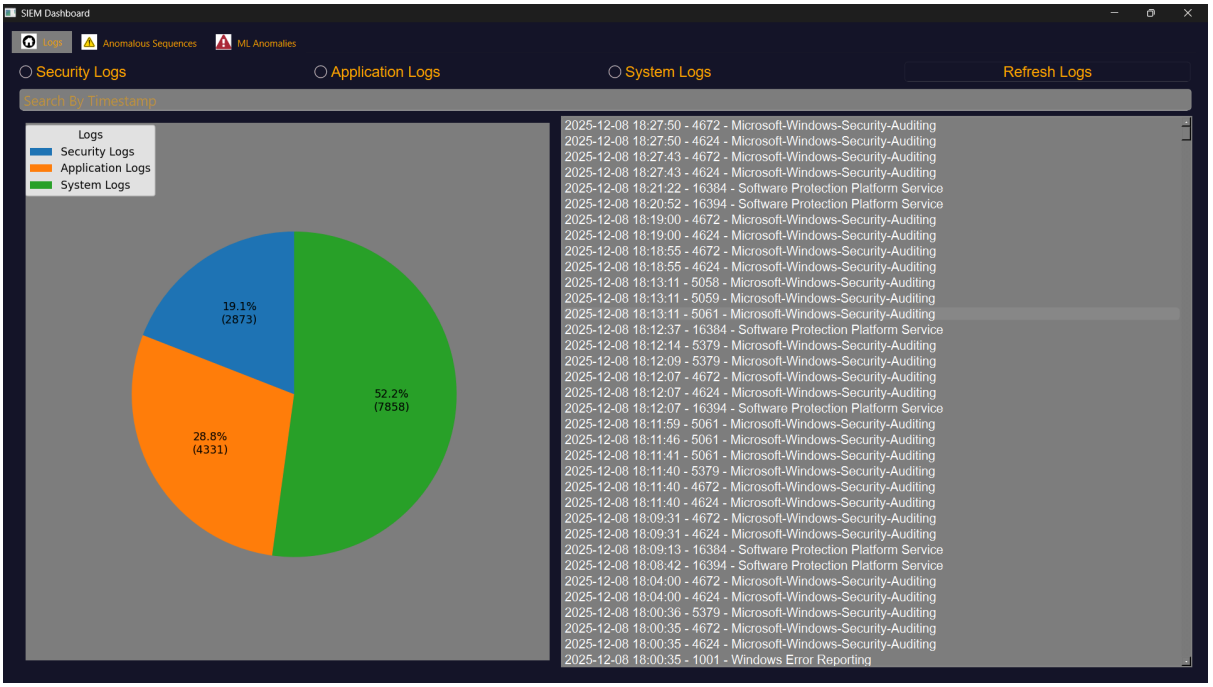
The script will start running after that and all interdependent files will also be called from the script. Ensure that all files provided are in the same directory to ensure flawless execution. The first time the script runs, it may be slower in execution as compared to each subsequent execution. After the script has successfully executed you will have an interactable GUI.

Note:- It is possible to bypass the login page as it will require administrator access to the windows keyrings to create and store a local account. To bypass this login page, simply directly run "*Dashboard.py*" in the command terminal. The login page is a simple addition to my main project and can be disregarded if required.

To use this login page simply enter a username and click on the sign in button as shown below. After that you will be prompted to select any image of your choice to be your password. Kindly select any image and click 'OK' on the following popup to create your account. Once this is done, enter your username and click on the login button and choose the same image that you used as your password and you will automatically be redirected to the dashboard where the main project and research was conducted.



Below is my main project and research module, to directly run this code, go to the directory where all files are present and simply run “python Dashboard,py”. It will skip the above login page and directly give you my lightweight SIEM in which all testing was conducted and all results were noted.



Using the mouse, kindly click on any button to interact with the script, such as Anomalous Sequences which will display tab 2 of the program or ML Anomalies that will show tab 3. The Button refresh logs, refreshes the logs in the dashboard, whereas security logs, application logs and system logs open a new instance in which only logs of those categories are displayed.

To confirm my results I have also created a small script with the name of metrics_evaluator.py, the script accesses the logs saved in the labelled logs directory which I have manually labelled as the ground truth. If you were to run that script it will print the results such as my precision, f1 score and recall in the terminal.