National College of Ireland

Configuration Manual

Industry Internship
MSc Cyber Security

Fumnanya Umunna
Student ID: X22133071

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. Fumnanya Omoniyi Umunna ……

Student ID: …… X22133071 ……

Programme: …… MSc Cybersecurity …… **Year:** …… 1 ……..

Module: …… Industry Internship ……

Lecturer: …… Vikas Sahni ……

Submission Due Date: ……5/01/2024……

Project Title: … A Novel Approach for Detecting Insider Threats by Combining Behavioural Analytics and Threat Intelligence ……

Word Count: ……471…… **Page Count:** ……10……

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: …… Fumnanya Omoniyi Umunna ……

Date: …… 31/12/2023……

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

Fumnanya Umunna
Student ID: X22133071

1 Introduction

This manual provides a step-by-step guide to configuring and running the Insider Threat Detection System. It covers the necessary setup, installation, and execution steps to replicate the project successfully.

The purpose of this manual is to assist any interested party in replicating the project environment and executing the code. It covers system requirements, data setup, and the process of running the system.

Prerequisites
Before proceeding, the following must be available:

- A device with a stable internet access
- Basic understanding of Python and data analysis concepts

2 System Requirements

Hardware Requirements

- Operating system: MacOS Sonoma 14.0
- Processor: Intel Core i5
- Hard drive: 256 GB SSD
- RAM: 8 GB

Software Requirements

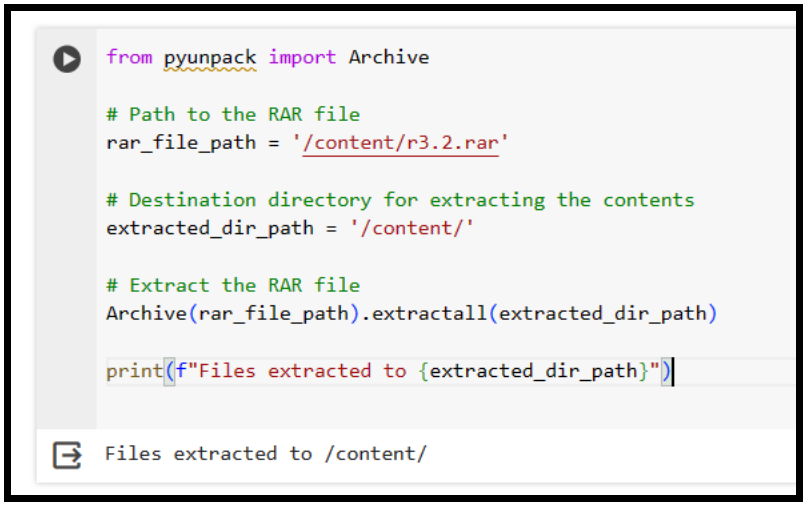
- Python 3.10.12
- Google Colab account

To seamlessly execute the code blocks, using Google Colab is recommended for its interactive and cloud-based environment. Click on the "Open in Colab" button to launch the notebook in Colab. In Colab, you will find individual code cells throughout the notebook. To run a code cell, click the play button located beside the cell.

3 Data Setup

Downloading the CERT Synthetic Dataset

1. Download the CERT Synthetic Dataset (Version 3.2).[1]
2. Upload the downloaded dataset file into the /content/ directory in Colab.
3. Run the code block in Figure 1 below to unzip the dataset.



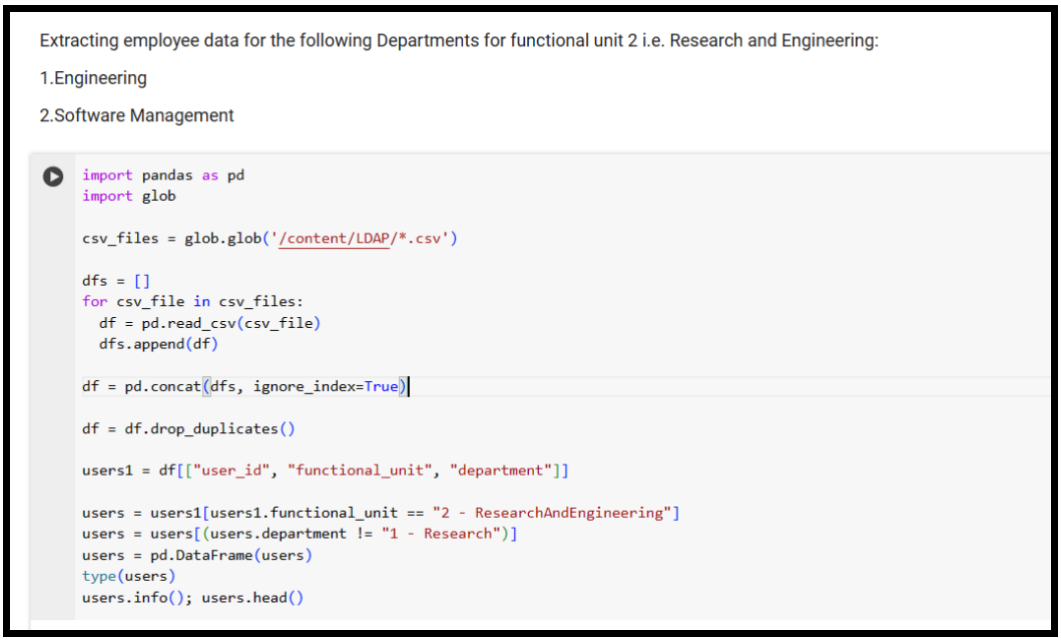
```
from pyunpack import Archive

# Path to the RAR file
rar_file_path = '/content/r3.2.rar'

# Destination directory for extracting the contents
extracted_dir_path = '/content/'

# Extract the RAR file
Archive(rar_file_path).extractall(extracted_dir_path)

print(f"Files extracted to {extracted_dir_path}")
```

```
Files extracted to /content/
```

Figure 1: Unpacking the dataset

Data Preprocessing

Run the various code blocks below (Figure 2 to 4) to preprocess the data:



Extracting employee data for the following Departments for functional unit 2 i.e. Research and Engineering:

1.Engineering

2.Software Management

```
import pandas as pd
import glob

csv_files = glob.glob('/content/LDAP/*.csv')

dfs = []
for csv_file in csv_files:
  df = pd.read_csv(csv_file)
  dfs.append(df)

df = pd.concat(dfs, ignore_index=True)

df = df.drop_duplicates()

users1 = df[["user_id", "functional_unit", "department"]]

users = users1[users1.functional_unit == "2 - ResearchAndEngineering"]
users = users[(users.department != "1 - Research")]
users = pd.DataFrame(users)
type(users)
users.info(); users.head()
```

Figure 2: Part of the Data Processing Scripts that Extracts Employee Data

[1] https://kilthub.cmu.edu/ndownloader/files/24856979

Figure 3: Part of the Data Processing Scripts that joins and Cleans the Data

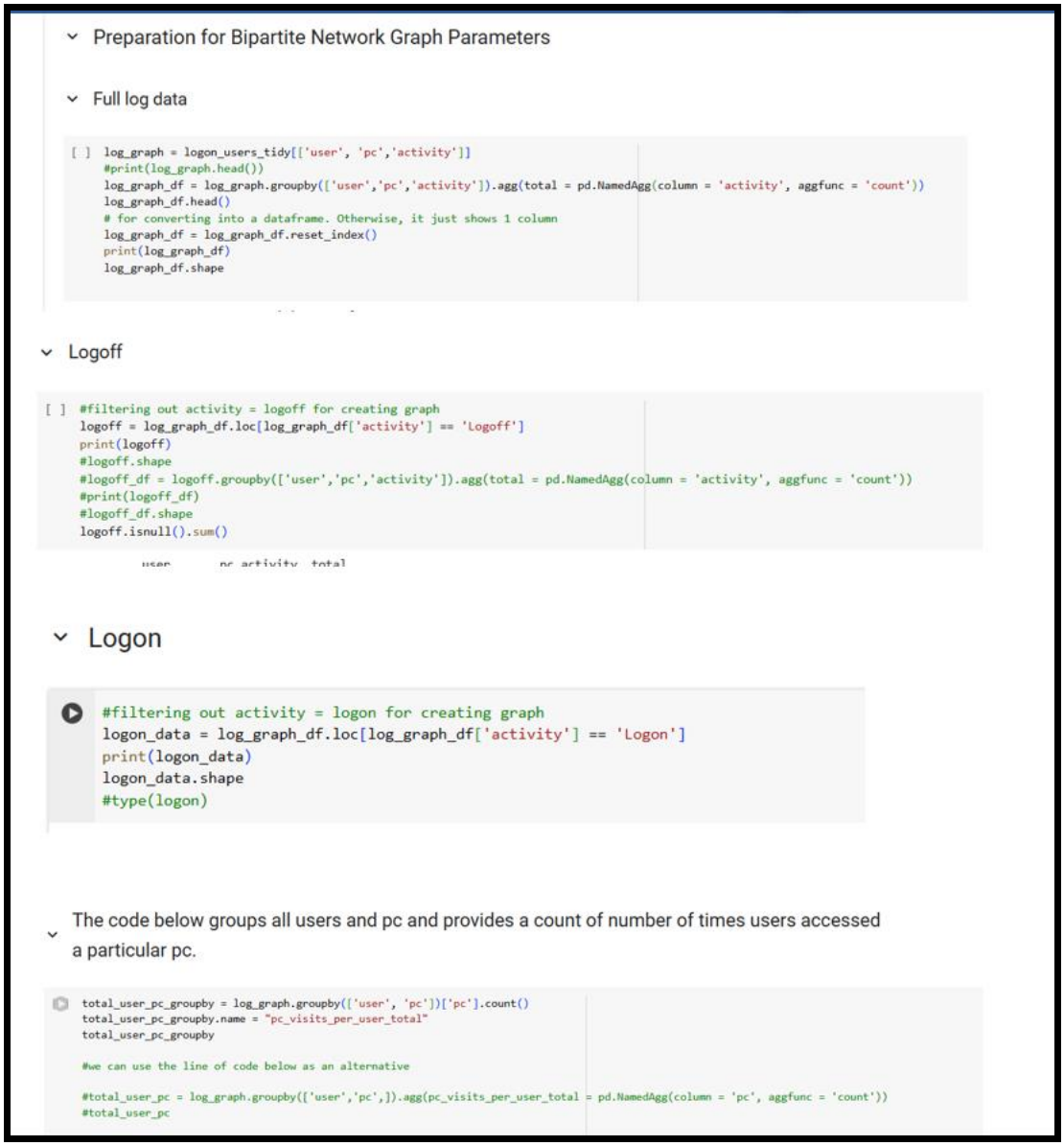


Figure 4: Preparation for Bipartite Network Graph Parameters

4 Running the System

After completing the data setup and preprocessing steps, the next phase involves feature engineering and analysis.

Within the same notebook, click the subsequent code blocks to perform the feature engineering and extraction. Please execute the cells sequentially, patiently waiting for each to finish processing before proceeding to the next. In case you encounter any issues, feel free to use the help options available in Colab, including the built-in documentation and forums for assistance.

Similar to the feature engineering phase, run the code blocks sequentially, starting from configuring the Isolation Forest Algorithm to calculating anomaly scores. Ensure each block executes successfully before proceeding to the next.

As you progress through the notebook, be attentive to any output, plots, or error messages. In case of issues, consult the help options in Colab, which include error messages, code

comments, and external documentation. The goal is to successfully configure and run the anomaly detection model.

By diligently running each code block in Colab and leveraging the available help resources, you'll navigate through the anomaly detection process effectively. Upon reaching the end of the notebook, you will have valuable insights into potential insider threats within the dataset.

5 Conclusion

Inspect generated plots, anomaly scores, and statistical analyses to verify the results and explore opportunities for further customization, experimentation, and improvements. Refer to the evaluation and discussion chapter for insights into result interpretation.

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configurationmanual as part of the portfolio submission.

Student Name: Fumnanya Umunna Student number: X22133071

Company: Cybarik Month Commencing: September 2023

- Engaged in the cyber threat intelligence sprint which was an interesting blend of technical and strategic contributions
- Tasked with information gathering using tools like theHarvesters, Maltego, and Netcraft
- Suggested a threat modelling framework based on findings
- Played a role in creating presentation slides for the sprint review
- Hands-on experience in information gathering

Employer comments

Fumnanya is a deliberate, smart intern. He takes his time to understand the task and performs it with great finesse. His research skills and attention to details have helped the team complete several projects in record time.

Student Signature: Fumnanya Umunna Date: 14/11/2023

Industry Supervisor Signature: Date: 14/11/2023

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configurationmanual as part of the portfolio submission.

Student Name:	Fumnanya Umunna	Student number:	X22133071
Company:	Cybarik	Month Commencing:	October 2023

- Gained new insights into the utilization and setup of Azure that were previously unfamiliar to me
- Implemented Role-Based Access Control (RBAC) for users
- Managed access at multiple levels, including management group, subscription, resource group, and individual resource levels
- Successfully created and deployed a virtual machine within the new AD Forest
- Established connections to the virtual machine and executed the migration of on-premise data to the cloud
- Creation of phishing email simulations and security awareness trainings

Employer comments

Fumnanya has consistently demonstrated exceptional technical and organizational skills. His ability to multitask and prioritize responsibilities has made him an invaluable asset to our team. He consistently takes initiative to enhance his skills and knowledge, which greatly benefits the team and the organization as a whole.

Student Signature: Fumnanya Umunna Date: 21/11/2023

Industry Supervisor Signature: Date: 21/11/2023

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Fumnanya Umunna Student number: X22133071

Company: Cybarik Month Commencing: November 202

- Enforced the use of multifactor authentication for all users
- Created the information security policy using the ISO 27002:2022 as a guide
- Contributed in the creation of some other policies like AI model governance, Clear desk and clear screen, and remote access policy
- Performed web exploitation on the company's web page using burp suite
- Executed directory enumeration with the use of Gobuster to identify hidden directories which can be a potential point of vulnerability
- Conducted an Nmap scan to detect open ports and potential areas of vulnerability
- Initiated Linux enumeration on the remote desktop using Linpeas to find potential privilege escalation directories

Employer comments

Fumnanya is a truly exceptional intern who has made a significant contribution to our team during his time here. His professionalism and reliability are unmatched. He has consistently met deadlines and exceeded expectations. His dedication and willingness to take on new challenges are truly admirable. He has also demonstrated a strong understanding of technical concepts and principles. I have no doubt that Fumnanya will be successful in his future endeavours

Student Signature: Fumnanya Umunna Date: 05/12/2023

Industry Supervisor Signature:  Date: 05/12/2023