

REHAN JOSEPH

Changemakers: Creativity & Value Creation

ACCA5033

Assignment

10 March 2026



Contents

Contents

Task 1: Ideation & Innovation

- Q1:Innovation
- Q2: Ideation
- Q3: Research

Task 2: Project Management

- Q1: Project Scope
- Q2: Gantt Chart (Project Timeline & Task Schedule)
- Q3: Risks/Challenges

Task 2: Project Development and Design

- Q1: Development Method
- Q2: Design Work
- Q3: Initial Practical Implementation

References

Appendix

Task 1: Ideation & Innovation

Q1 Innovation

How Innovation Shapes the World

Innovation plays a major role in shaping modern society by introducing new ideas, technologies, and methods that improve how people live and work. It allows individuals and organisations to solve problems more effectively while creating new opportunities for growth and development [1].

In everyday life, innovation can be seen through technologies such as smartphones, online learning platforms, and digital services. These tools have transformed communication, education, and business by increasing efficiency and accessibility. What once seemed impossible, such as attending classes remotely or controlling devices from a phone, has become a normal part of daily life [2].

Innovation has influenced society throughout history. Early developments such as agriculture and industrial machinery changed how communities worked and organised themselves. Today, rapid advancements in fields such as artificial intelligence, automation, and digital technology continue to reshape industries and the global economy [1].

Modern innovation is also increasingly focused on improving quality of life. Developments in healthcare, renewable energy, and sustainable technologies aim to address global challenges while supporting long-term wellbeing. This shows that innovation is driven not only by technological progress but also by social needs and values [3].

Creativity plays a key role in the innovation process. New ideas often emerge through experimentation, curiosity, and problem-solving. As technology continues to evolve, human creativity and critical thinking become even more important in developing solutions to complex problems [4].

In conclusion, innovation continues to shape the world by transforming industries, improving daily life, and helping societies address future challenges.

Q2: Ideation

As a student studying Computer Networks and Cybersecurity, I am interested in practical ways to protect networks, monitor threats, and strengthen security within university systems. Below are several potential project ideas I considered[5]:

1. **Network Login Monitoring System**

A tool designed to track user login activity across the network and generate alerts when unusual or suspicious login patterns occur.

2. **Honeypot System for Detecting Intruders**

A decoy server that mimics a real system to attract attackers, allowing their behaviour to be monitored, analysed, and used to improve security defences.

3. **Simple Ransomware Alert Tool**

A lightweight program that detects abnormal file changes, rapid encryption, or deletion patterns that may indicate the early stages of a ransomware attack.

4. **Phishing Awareness Tool**

A system that sends simulated phishing emails to users, evaluates their responses, and provides feedback to help improve awareness and reduce susceptibility to phishing attacks.

5. **University Cyber Risk Dashboard (Selected)**

An interactive dashboard that calculates risk levels for different university departments, monitors simulated live activity for unusual behaviour, forecasts future trends, and provides recommended security actions.

Selected Project

Title- Adaptive Cyber Risk Intelligence & Forecasting System for University Networks

The chosen project, **Adaptive Cyber Risk Intelligence & Forecasting System for University Networks**, brings together live network activity monitoring, risk calculation, and visualisation into a single, interactive dashboard designed specifically for a university environment.

Aim

To develop an interactive cybersecurity dashboard that monitors live university network activity, detects unusual behaviour linked to potential cyber threats, visualises departmental and overall risk levels, predicts future trends, and provides clear security recommendations to support proactive decision-making.

Brief Project Description

Universities operate with large user populations, open networks, and significant volumes of sensitive data, making them prime targets for cyber-attacks such as phishing, malware, ransomware, and credential abuse[6]. This project aims to address these challenges by developing an interactive cybersecurity dashboard that monitors simulated live network activity to identify unusual behaviour linked to potential threats.

The system will track threat activity across different university departments, calculate associated risk levels, forecast emerging trends, and provide recommended actions to strengthen security. By incorporating real-time activity monitoring, the dashboard allows users to immediately see when abnormal patterns occur, understand the cause of sudden risk spikes, and take proactive steps to mitigate issues before they escalate.

Overall, the project demonstrates practical cybersecurity decision-making in a clear and accessible way, helping users visualise risks, interpret network behaviour, and respond effectively to potential threats

Objectives

1. Monitor simulated live activity on the university network to identify unusual behaviour that may indicate potential cyber threats.
2. Track threat activity across key university departments, including the Student Network, Staff, Finance, and Research Labs.
3. Calculate risk levels for each department using a simple weighted scoring system to highlight areas of concern.
4. Display the overall university-wide risk level and classify it as Low, Medium, High, or Critical.
5. Forecast future risk levels using trend analysis to help anticipate emerging threats.
6. Develop an interactive dashboard that allows users to explore risk data, view departmental insights, and investigate abnormal activity.
7. Provide clear and actionable mitigation recommendations based on detected threats and unusual behavioural patterns.

Q3: Research

To achieve the aim and objectives of the *Adaptive Cyber Risk Intelligence & Forecasting System for University Networks*, a range of courses, academic frameworks, and university modules will be used to provide the necessary technical and theoretical foundation. These include recently completed cybersecurity training and relevant academic knowledge in network security, threat monitoring, and system development.

Key Courses Recently Completed

ISC² Introduction to Cybersecurity

I recently completed this course and earned a digital badge. It introduced core cybersecurity concepts, including threat types, attack vectors, and risk management principles. The course also covered monitoring systems used to detect abnormal network activity, which directly supports the live activity detection component of my project.

Cisco Introduction to Cybersecurity

This Cisco Networking Academy course, for which I also received a badge, provided practical insights into securing network infrastructures, understanding common network attacks, and implementing basic defensive measures. It reinforced the importance of monitoring login behaviour and protecting network access, both of which align with the dashboard's threat-tracking features.

Network Programming

In my first year, I completed this module, which introduced fundamental programming concepts using Python. I learned data structures, control flow, functions, and basic data handling. These skills will support the simulation of live network activity and the generation of threat events within the dashboard project.

Additional Academic Source

NIST Risk Management Framework (RMF)

During the Data Security and Compliance module, I wrote a research assignment on the NIST

RMF, gaining a strong understanding of structured approaches for identifying, assessing, and managing risks in IT systems. This knowledge will inform the design of the quantitative risk-scoring model used in the dashboard.



Figure 1: Cisco Certificate



Figure 2: ISC2 Certificate

The combination of recently completed cybersecurity courses, academic knowledge in network programming, and prior research experience in risk management provides a strong foundation for achieving this project's objectives.

Task 2: Project Management

Q1: Project Scope

The **Adaptive Cyber Risk Intelligence & Forecasting System for University Networks** is designed to simulate and monitor cybersecurity threats within a university network environment. The system will analyse simulated activity across different departments, calculate risk levels, identify unusual behaviour, and provide visual insights through an interactive dashboard. The following sections outline the key components of the project, including activity monitoring, risk scoring, trend analysis, the dashboard interface, and ethical considerations[7].

Monitoring Simulated Activity

The system will simulate network activity across departments such as Student Networks, Staff Systems, Finance, and Research Laboratories. This activity will include login attempts and access behaviour that mimic real network usage. Suspicious behaviour, such as repeated failed logins or unusual access patterns, will contribute to the department's calculated risk score.

Risk Scoring

A weighted scoring model will be used to calculate cybersecurity risk levels. Different threat types, such as phishing, malware indicators, brute-force attacks, insider misuse, and ransomware activity, will be assigned severity values. These scores will be used to classify risk levels as Low, Medium, High, or Critical[8].

Trend Analysis

The system will analyse historical simulated data to identify patterns and highlight departments where cybersecurity risk may be increasing. This allows the dashboard to demonstrate how organisations can monitor trends and anticipate potential threats.

Dashboard Interface

All results will be presented through an interactive dashboard, allowing users to view departmental risk scores, threat distributions, and risk trends using charts and graphs.

Ethical Considerations

All network activity used in the project will be fully simulated, ensuring that no real systems or personal data are accessed.

Proposed Solution

The proposed solution is a Python-based interactive dashboard designed to simulate and visualise cybersecurity risks within a university network.

- **Data Simulation:** Python scripts generate simulated login attempts and threat events across departments.
- **Risk Scoring Engine:** An algorithm calculates departmental and overall risk levels based on threat severity and frequency.
- **Trend Analysis:** Historical simulated data is analysed to identify changes in risk levels over time.
- **Interactive Visualisation:** The dashboard is built using **Streamlit** and **Matplotlib** to display charts and graphs of cybersecurity risks.
- **Security Recommendations:** The system provides suggested mitigation actions, such as enabling multi-factor authentication or reviewing suspicious activity.

This solution demonstrates how a cybersecurity monitoring and risk analysis system could be implemented using simulated data.

Resources/Technologies required to complete this Project

- Python

- Streamlit (web-apps)
- Matplotlib (visualisation)
- Pandas (data-analysis)
- Simulated dataset
- PyCharm (IDE)
- Computer / Laptop
- Git / GitHub (Version Control)

Q2: Project Timeline and Task Schedule

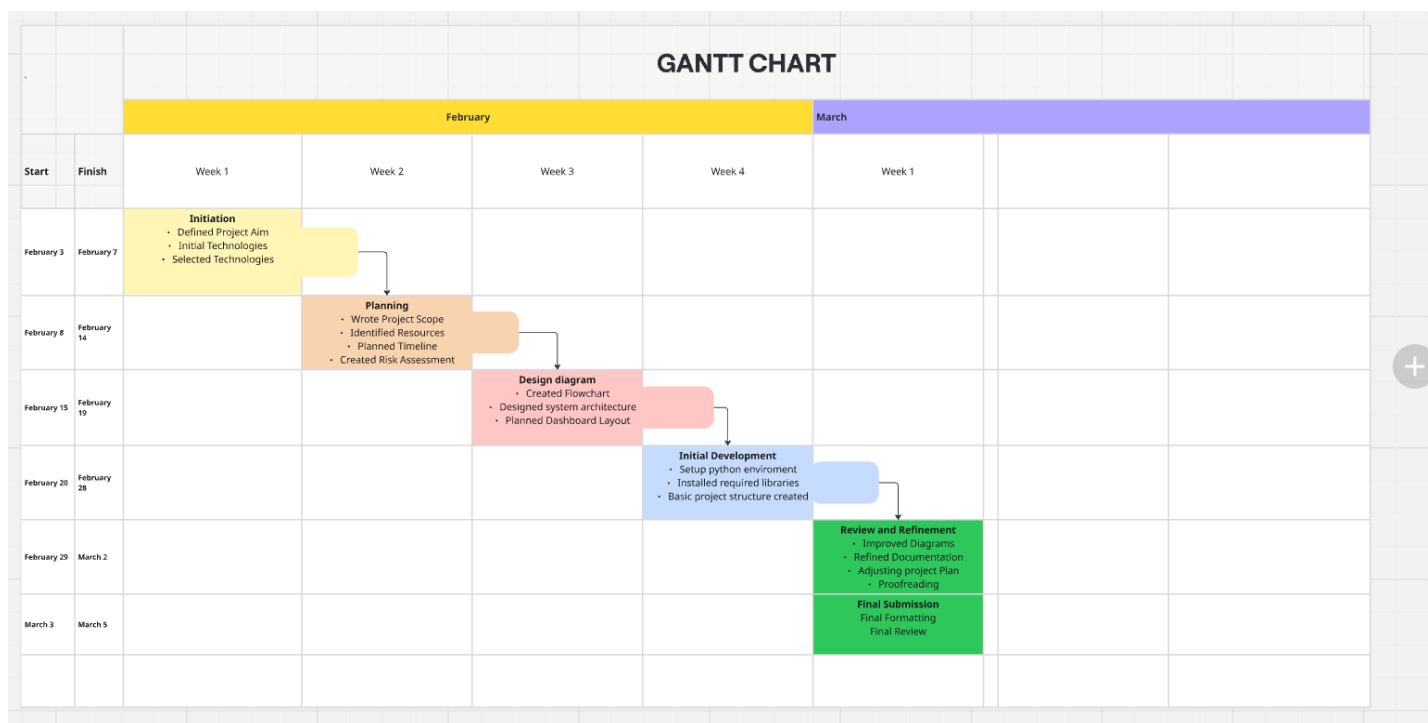


Figure 3: Gantt Chart

The project follows a structured timeline beginning with the initiation phase in early February, where the project aim and required technologies were defined. This is followed by the planning stage, where the project scope, resources, and risk assessment were developed. The design phase focuses on creating system diagrams and planning the dashboard layout. Initial development then involves setting up the Python environment and required libraries. The final stage focuses on reviewing the project, refining documentation, and preparing the final submission.

Q3: Risks and Challenges

During the development of this project, several challenges may arise. Since this project involves learning new tools and combining different components, identifying potential risks early will help ensure the project progresses smoothly and can be completed successfully.

1. Limited Experience with Matplotlib

One challenge is that I have not previously used Matplotlib, which will be required to create charts and visualisations for the dashboard. Learning how to generate clear and meaningful graphs may take additional time.

To reduce this risk, I will use online tutorials and documentation to learn the basics and begin with simple charts such as bar graphs and line charts before creating more advanced visualisations.

2. Limited Experience with Streamlit

Another challenge is that I have not used Streamlit before. Since it is used to build the interactive dashboard interface, learning how to create layouts, buttons, and navigation between pages may initially be difficult.

To manage this, I will start by building a simple dashboard prototype and gradually add more interactive features as I become more comfortable with the framework.

3. Integrating Different System Components

This project combines several elements including simulated network activity, risk scoring, and dashboard visualisation. Integrating these components together may lead to errors or unexpected issues.

To reduce this risk, I will develop and test each part of the system separately before combining them into the final application.

4. Simulating Network Activity

The project requires generating simulated network activity such as login attempts and unusual behaviour that may indicate potential cyber threats. Creating realistic simulated data may be challenging at first.

To address this, I will begin with simple simulated events and gradually expand the dataset to include more varied activity patterns.

5. Time Management

Because this project involves learning new tools while also developing the system, there is a risk that some tasks may take longer than expected.

To minimise this risk, I will follow a clear project timeline and focus on completing the core features first before improving additional elements of the dashboard.

Task 3: Project Development method & Design

Q1: Development Method

For my project, I have chosen the **Agile development method** because it is highly suitable for planning and completing tasks in an organized, flexible, and iterative manner. Agile emphasizes breaking the project into small, manageable tasks or “sprints,” allowing continuous progress and regular evaluation. This approach is ideal for projects that require creativity, adaptation, and collaboration[9].

To manage the Agile workflow, I used Trello, a project management tool that allows tasks to be organised and tracked visually. Trello supports Agile principles by enabling tasks to be organised into boards and moved through different stages of progress.

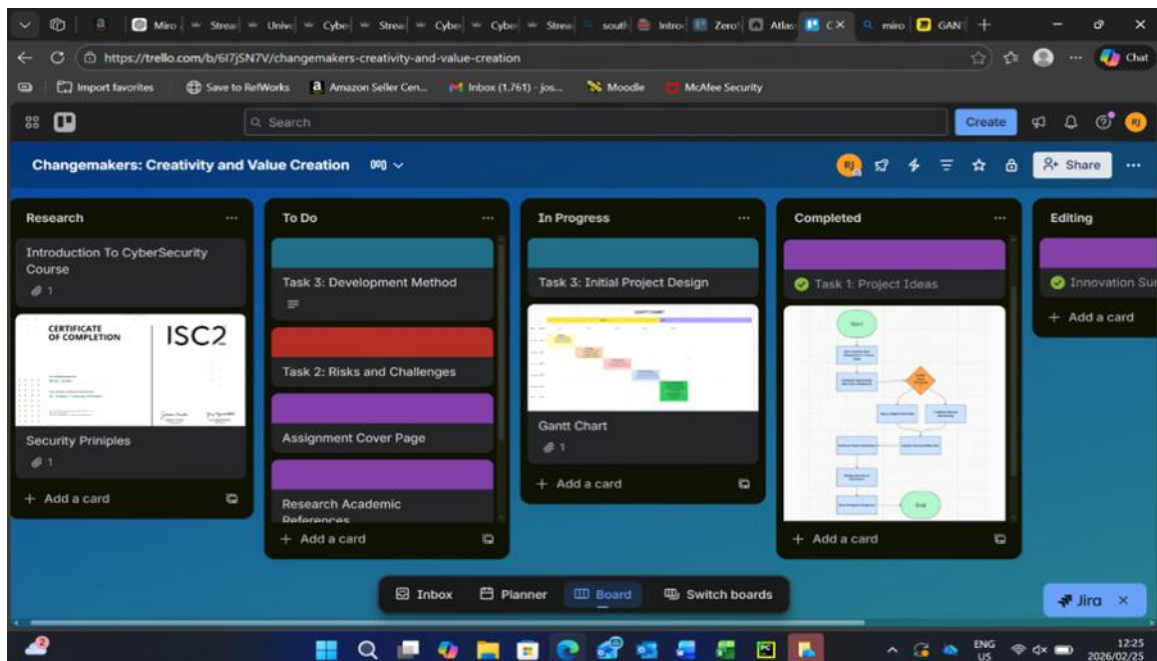


Figure 4: Trello Dashboard

Using **Trello**, I can implement Agile effectively:

- **Task Organization:** I created boards and columns representing different stages of the project, such as *Research*, *To Do*, *In Progress*, *Completed*, and *Editing*. Each task is represented as a card that can be moved through the workflow, providing clear visibility of progress.
- **Prioritization:** Tasks can be color-coded and ordered based on priority, helping to focus on critical activities first.
- **Progress Tracking:** By moving tasks across the workflow columns, I can visually track the project's progress and quickly identify any bottlenecks or delays.
- **Flexibility:** Agile allows adapting to changes in project requirements. For example, if a task needs revision or new research emerges, it can be added or reprioritized without disrupting the overall workflow.

By combining **Trello** with Agile principles, I was able to plan, monitor, and complete my project efficiently, ensuring that all tasks are organized and progress is measurable at every stage.

Q2: Design Work

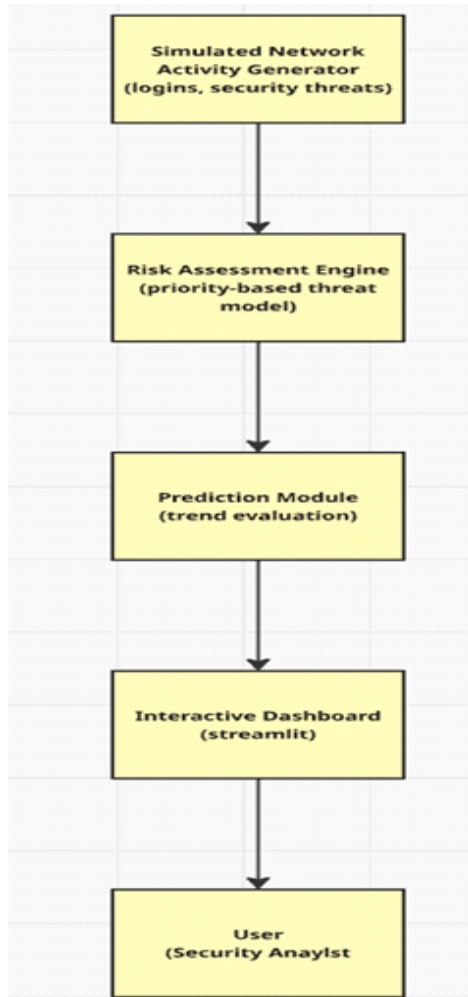


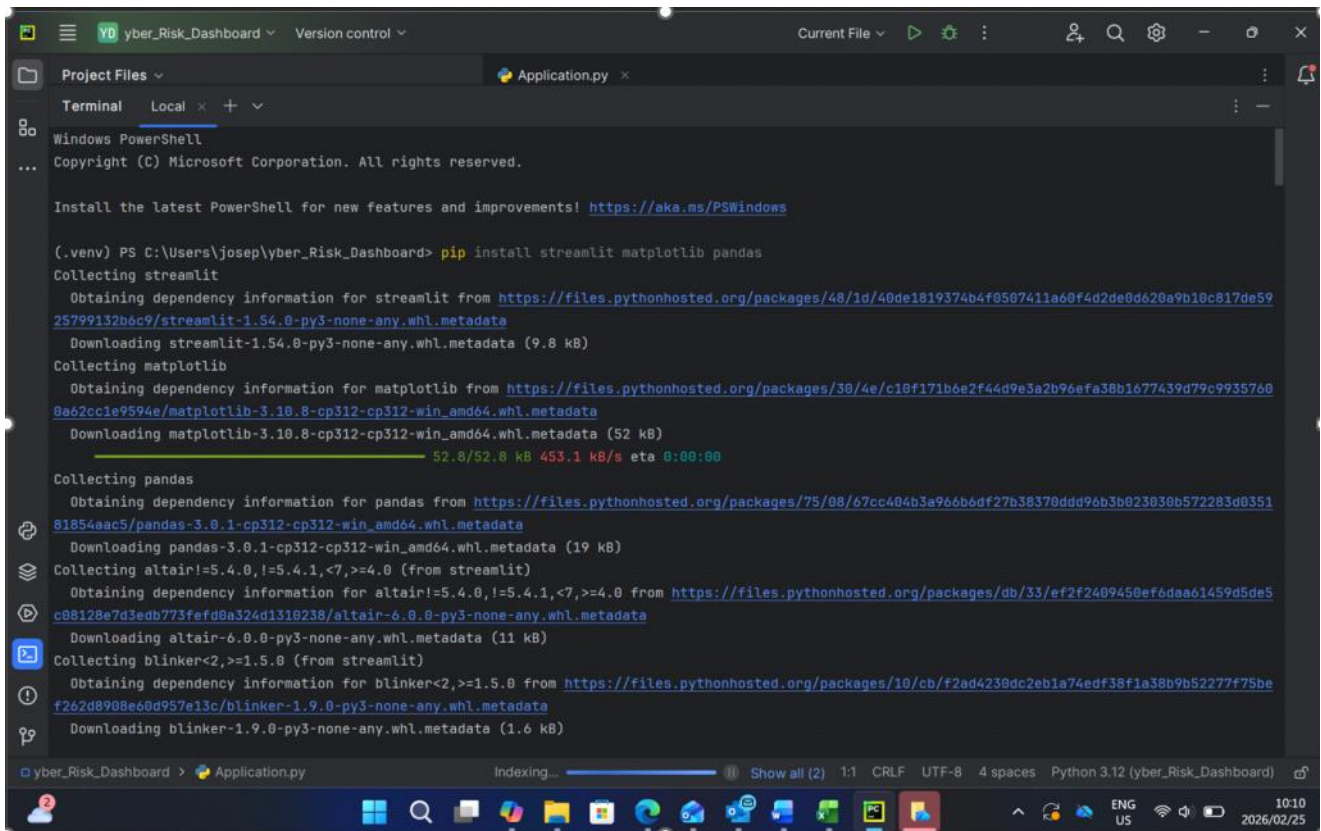
Figure 5: System Architecture Diagram



Figure 6: Flowchart

Figure 5 is a **system architecture diagram**, which illustrates the main components of the Cyber Risk Intelligence Dashboard and how they are connected within the system. It shows the key modules involved in the project, from simulated network activity generation to the interactive dashboard used by the user. Figure 6 is a **flowchart**, which represents the logical sequence of steps used in the system's risk assessment process. It visually outlines the decision-making structure and workflow used to process activity data and manage cyber risk within the system.

Q3: Initial Practical Implementation



```
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

(.venv) PS C:\Users\joseph\yber_Risk_Dashboard> pip install streamlit matplotlib pandas
Collecting streamlit
  Obtaining dependency information for streamlit from https://files.pythonhosted.org/packages/48/1d/40de1819374b4f0507411a60f4d2de0d620a9b10c817de5925799132b6c9/streamlit-1.54.0-py3-none-any.whl.metadata
  Downloading streamlit-1.54.0-py3-none-any.whl.metadata (9.8 kB)
Collecting matplotlib
  Obtaining dependency information for matplotlib from https://files.pythonhosted.org/packages/30/4e/c18f171b6e2f44d9e3a2b96efa38b1677439d79c99357608a62cc1e9594e/matplotlib-3.10.8-cp312-cp312-win_amd64.whl.metadata
  Downloading matplotlib-3.10.8-cp312-cp312-win_amd64.whl.metadata (52 kB)
Collecting pandas
  Obtaining dependency information for pandas from https://files.pythonhosted.org/packages/75/08/67cc404b3a966b6df27b38370ddd96b3b023830b572283d035181854aac5/pandas-3.0.1-cp312-cp312-win_amd64.whl.metadata
  Downloading pandas-3.0.1-cp312-cp312-win_amd64.whl.metadata (19 kB)
Collecting altair!=5.4.0,!=5.4.1,<7,>=4.0 (from streamlit)
  Obtaining dependency information for altair!=5.4.0,!=5.4.1,<7,>=4.0 from https://files.pythonhosted.org/packages/db/33/ef2f2409450ef6daa61459d5de5c08128e7d3edb773fed8a324d1310238/altair-6.0.0-py3-none-any.whl.metadata
  Downloading altair-6.0.0-py3-none-any.whl.metadata (11 kB)
Collecting blinker<2,>=1.5.0 (from streamlit)
  Obtaining dependency information for blinker<2,>=1.5.0 from https://files.pythonhosted.org/packages/10/cb/f2ad4230dc2eb1a74edf38f1a38b9b52277f75bef262d8908e60d957e13c/blinker-1.9.0-py3-none-any.whl.metadata
  Downloading blinker-1.9.0-py3-none-any.whl.metadata (1.6 kB)
```

Figure 7: Installing Libraries

Figure 7 shows the project environment in **PyCharm**, where the required Python libraries (Streamlit, Matplotlib, and Pandas) are installed using the terminal. These libraries are needed to support the development of the cybersecurity dashboard and data visualisation features

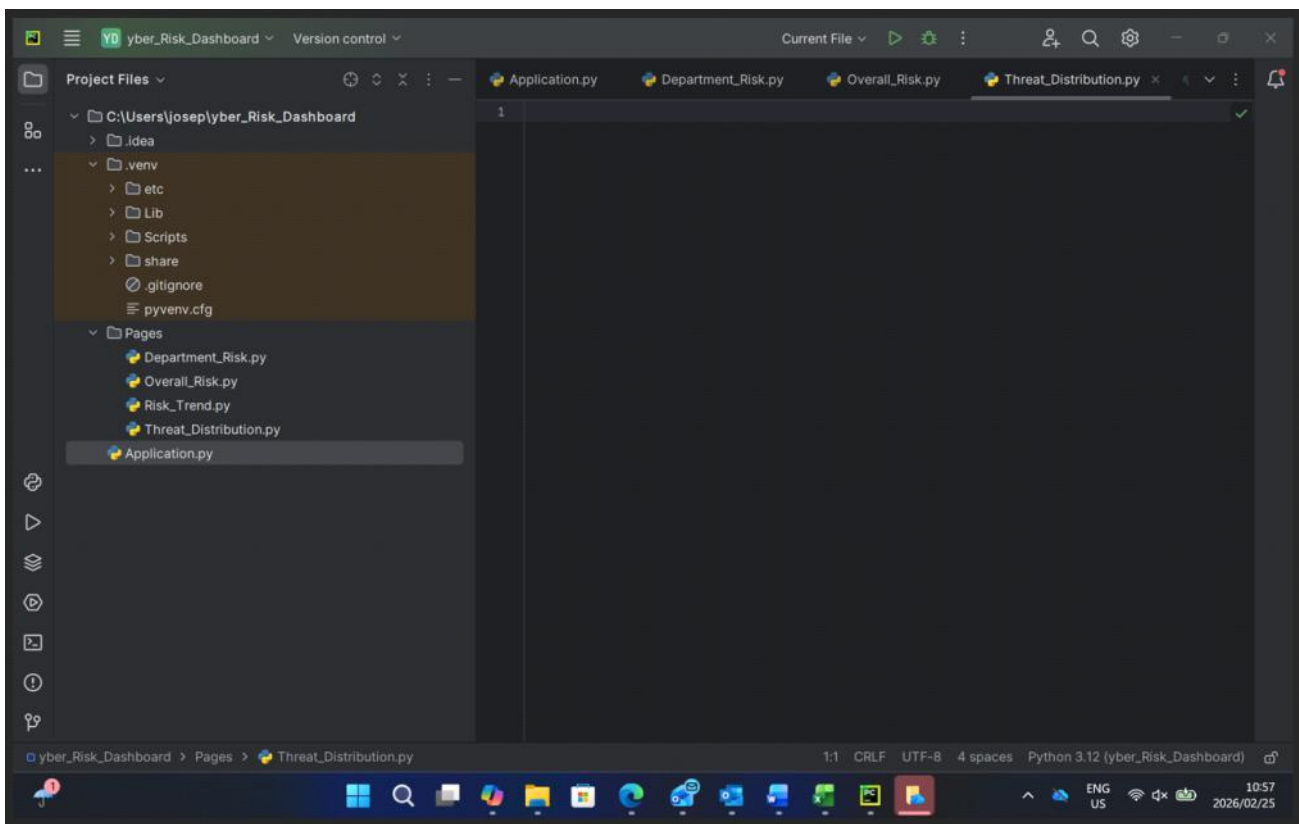


Figure 8: Project Folder Structure

Figure 8 displays the **project folder structure** within PyCharm. The main application file (Application.py) and multiple dashboard pages (such as Department_Risk.py, Overall_Risk.py, Threat_Distribution.py, and Risk_Trend.py) are organised inside the **Pages** directory, allowing the Streamlit dashboard to navigate between different sections of the system.

```

1 usage
22 def login():
23     st.title("Cyber Risk Intelligence System")
24     st.subheader("Sign in to access the dashboard")
25
26     username = st.text_input("Username")
27     password = st.text_input(label="Password", type="password")
28
29     if st.button("Login"):
30         if username in USER_CREDENTIALS and USER_CREDENTIALS[username] == password:
31             st.session_state.authenticated = True
32             st.rerun()
33         else:
34             st.error("Invalid username or password")
35
36 # -----
37 # ORIGINAL DASHBOARD
38 # -----
39 usage
40 def dashboard():
41
42     st.title("Cyber Risk Intelligence Dashboard")
43
44     st.markdown("### Select a section below to view detailed analysis")
45
46     st.divider()
47
48     col1, col2 = st.columns(2)

```

Figure 9: Python Code

Figure 9 shows the **Python code** used to implement the authentication and dashboard navigation within the Streamlit application. The login() function creates the login interface where users enter a username and password, and the system verifies these credentials before granting access. If the login is successful, the user is authenticated and redirected to the main dashboard. The code also defines the dashboard() function, which displays the main interface and allows users to navigate to different sections of the cybersecurity risk analysis system.



Figure 10: Cyber Security Dashboard

Figure 10 shows the **initial version of the cybersecurity dashboard running in the browser**. It was created to test whether the Streamlit application runs correctly and to confirm that the basic dashboard layout and components are working before further development.

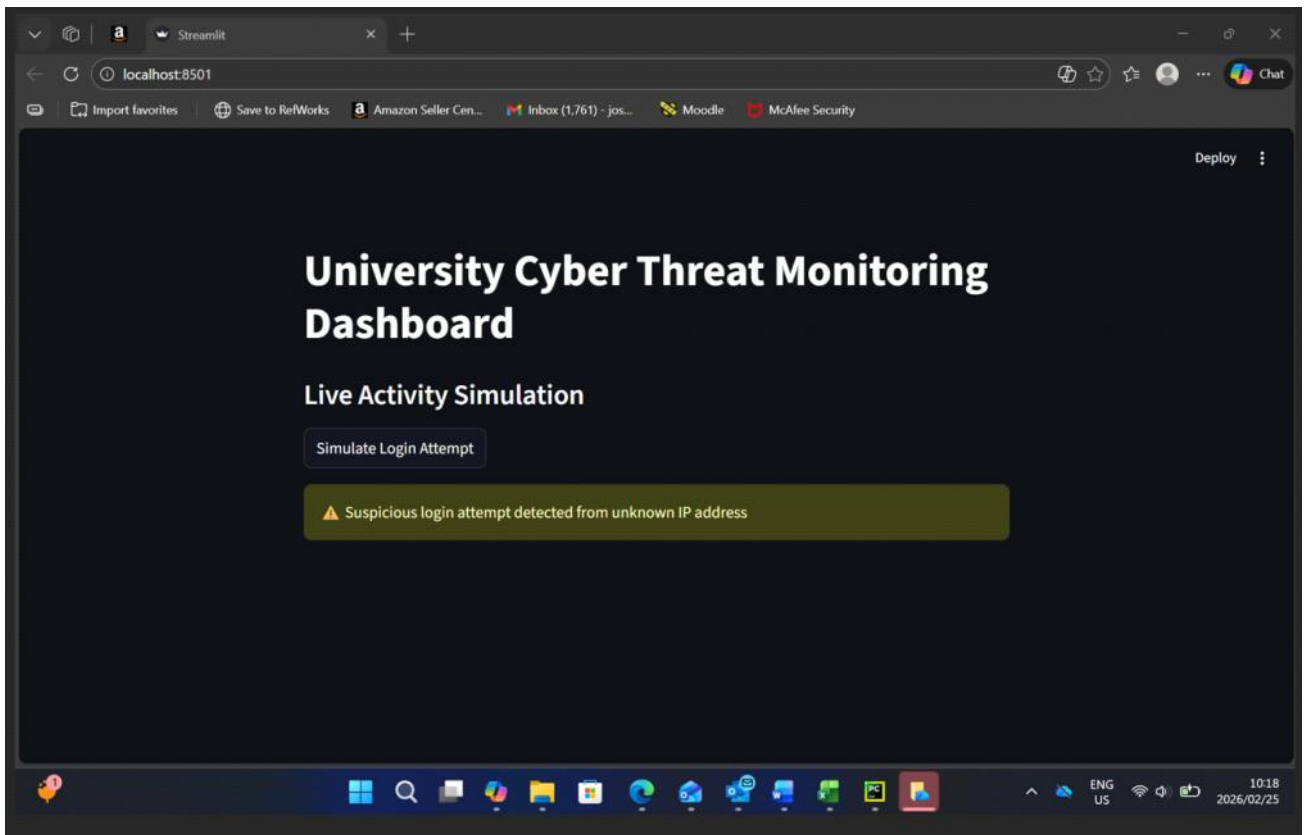


Figure 11: Authentication Page

Figure 11 shows the **authentication page of the cybersecurity dashboard**. It acts as a login and access control step before a user can enter the main dashboard. This ensures that only authorised users can access the system and view the cybersecurity monitoring data, helping simulate how real security dashboards restrict access to sensitive information.

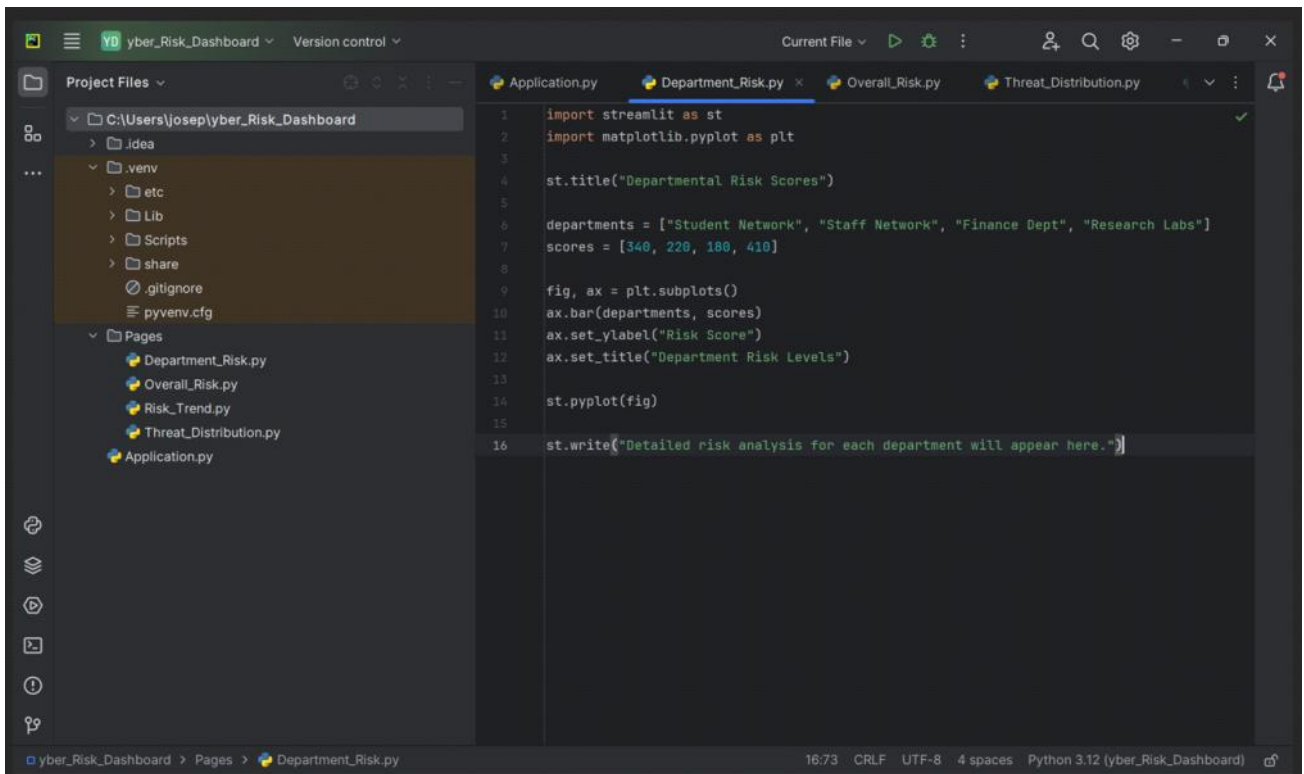


Figure 12: Python Code

Figure 12 shows the Python code that generates a basic Streamlit page displaying departmental risk scores using a Matplotlib bar chart, forming the foundation for the dashboard's risk-analysis module.



Figure 13: Bar Chart

This screenshot shows a bar chart displaying the cybersecurity risk levels for different university departments based on simulated threat activity. Only part of the graph is visible in the screenshot because the full chart could not fit on the screen.

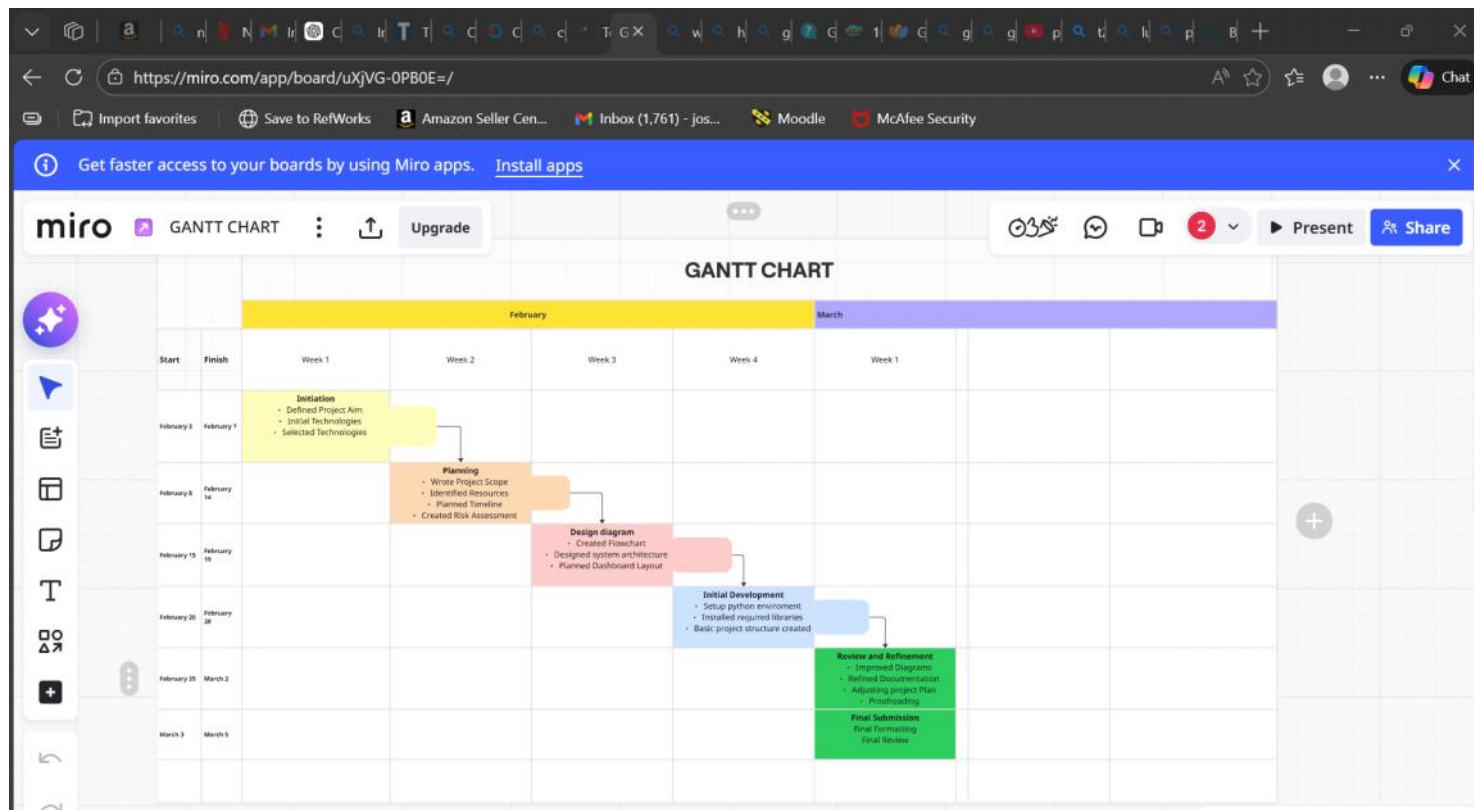
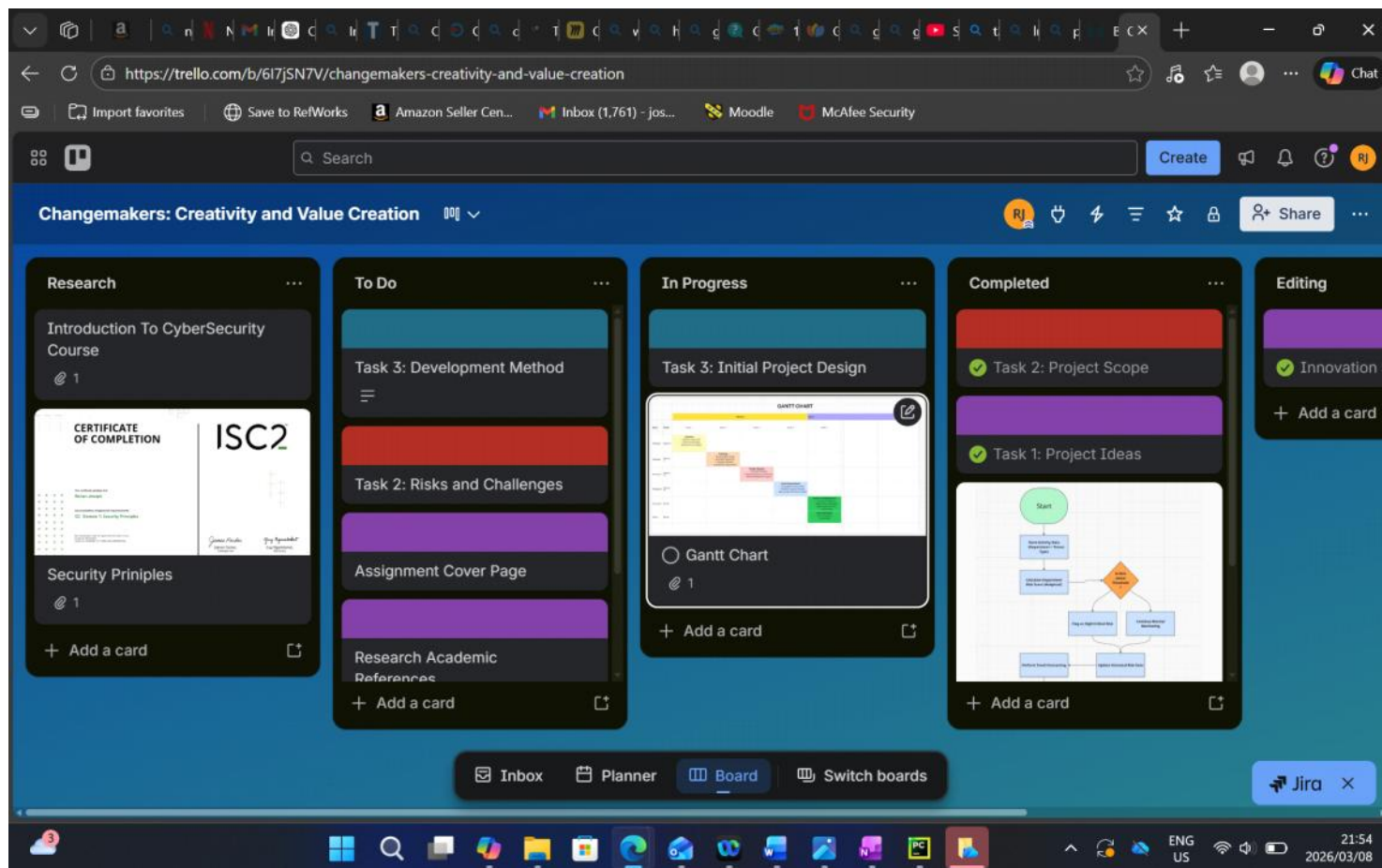
References

References

- [1] A. Dub, "The Impact of Innovations and Technological Development on Modern Society and Global Dynamics," vol. 68, no. 4, pp.2317–2325, 2023, doi: 10.46852/0424-2513.4.2023.39.
- [2] A. S. TechBullion, "The Impact of Technology on Our Daily Lives: A Deep Dive into the Advancements that Shape our World," -11-03 2023, Accessed: Feb 12, 2026. Available at: <https://techbullion.com/the-impact-of-technology-on-our-daily-lives-a-deep-dive-into-the-advancements-that-shape-our-world/>.
- [3] D. V. Trupia, A. Mathieu-Fritz and T. A. Duong, "The Sociological Perspective of Users' Invisible Work: A Qualitative Research Framework for Studying Digital Health Innovations Integration," vol. 23, no. 11, pp.e25159, 2021, doi: 10.2196/25159.
- [4] "Creativity and Innovation: The Role of Creativity in Driving Innovation and Leadership," Accessed: Feb 12, 2026. Available at: <https://fastercapital.com/content/Creativity-and-Innovation--The-Role-of-Creativity-in-Driving-Innovation-and-Leadership.html>.
- [5] Dear John, "Top 239+ Cyber Security Project Ideas 2025-26 - Best Project Ideas," -06-07 2025, Accessed: Feb 13, 2026. Available at: <https://bestprojectideas.com/cyber-security-project-ideas/>.
- [6] H. S. Lallie, A. Thompson, E. Titis and P. Stephens, "Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector," vol. 14, no. 2, pp.49, /2 2025, doi: 10.3390/computers14020049. Accessed: Feb 24, 2026. Available at: <https://www.mdpi.com/2073-431X/14/2/49>.
- [7] A. Agarwal, et al., "CyberVigilance: A Deep Learning Framework for Cyber Attack Forecasting", pp. 1–11. [Online].doi: 10.1109/INDISCON66021.2025.11254445.Available: <https://ieeexplore.ieee.org/document/11254445>
- [8] S. C. Phillips, S. Taylor, M. Boniface, S. Modafferi and M. Surridge, "Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems," vol. 12, pp.82482–82505, 2024, doi: 10.1109/ACCESS.2024.3404264. Accessed: Feb 17, 2026. Available at: <https://ieeexplore.ieee.org/document/10536896>.
- [9] "Agile Methodology," -12-13 2023, Accessed: Feb 25, 2026. Available at: <https://www.geeksforgeeks.org/software-testing/what-is-agile-methodology/>.

Appendix

The appendix contains supporting materials used during the development of the project. This includes planning diagrams created in **Miro**, as well as reference tutorials from **YouTube** that were used to learn and implement features using **Streamlit** and **Matplotlib**. These resources provide additional context and support for the methods and design decisions discussed in the main report.



March 3 March 5 Final Formulating Final Review

29%

21:43 2026/03/08

https://miro.com/app/board/uXjVG-1Q2_U=/

Get faster access to your boards by using Miro apps. [Install apps](#)

miro Changemakers flowchart Upgrade

Present Share

```
graph TD; Start([Start]) --> Store[Store Activity Data  
(Department + Threat Type)]; Store --> Calculate[Calculate Department  
Risk Score (Weighted)]; Calculate --> Decision{Is Risk  
above  
Threshold?}; Decision --> Flag[Flag as High/Critical Risk]; Decision --> Monitor[Continuous Normal  
Monitoring]; Flag --> Update[Update Historical Risk Data]; Monitor --> Update; Update --> Forecast[Perform Trend Forecasting]; Forecast --> Display[Display Results on  
Dashboard]; Display --> Mitigation[Show Mitigation Response]; Mitigation --> End([End]);
```

26%

21:50 2026/03/08

YouTube video player interface for "python matplotlib basics". The video is by Academind, has 120K views, and was uploaded 7 years ago. The video content shows a Jupyter Notebook with Python code for plotting a line graph of stock prices over time. The code includes data for 'api_price' and 'year', and uses 'plt.plot()' and 'plt.show()' to display the graph. The graph shows a line plot with markers for each year from 2014 to 2019, with the y-axis labeled 'Stock Price' and the x-axis labeled 'Year'. The video player includes a search bar, a 'Summarize' button, and a 'Create' button. The right sidebar shows a Grammarly advertisement and a recommendation for "Learn Matplotlib in 30 Minutes - Python ...".

```
api_price = [93.95, 112.15, 104.65, 144.85, 169.49]
year = [2014, 2015, 2016, 2017, 2018]

plt.plot(year, api_price, 'sk')
plt.xlabel('Year')
plt.ylabel('Stock Price')
plt.show()
```

Python - Matplotlib Tutorial for Beginners

Academind 929K subscribers

120K views 7 years ago Python for Data Analysis and Data Science

YouTube video player interface for "python streamlit basics". The video is by pixegami, has 379K views, and was uploaded 2 years ago. The video content includes a list of topics: Streamlit Basics, Building a Simple App, and Deployment. The video player includes a search bar, a 'Summarize' button, and a 'Create' button. The right sidebar shows a recommendation for "Python Dataclasses: Here's 7 Ways It Will ...".

IN THIS VIDEO

- Streamlit Basics
- Building a Simple App
- Deployment

We'll then take a look at how to create a simple

Streamlit: The Fastest Way To Build Python Apps?

pixegami 80.8K subscribers

379K views 2 years ago #pixegami #streamlit