Executable Code and Dataset

Executable Code

```
# Import required libraries
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
from sklearn.ensemble import IsolationForest

# Load dataset (sample network logs)
df = pd.read_csv('cybersecurity_logs.csv')

# Preprocessing: Selecting relevant features
features = ['packet_size', 'response_time', 'malicious_score']
df = df[features]

# Train an Isolation Forest model for anomaly detection
model = IsolationForest(n_estimators=100, contamination=0.05, random_state=42)
df['anomaly'] = model.fit_predict(df)

# Visualizing anomalies
plt.figure(figsize=(8,5))
plt.scatter(df.index, df['packet_size'], c=df['anomaly'], cmap='coolwarm')
plt.xlabel('Log Entry')
plt.ylabel('Packet Size')
plt.title('Anomaly Detection in Network Traffic')
plt.show()
```

Dataset Information

Sample Dataset: cybersecurity_logs.csv

This dataset contains network traffic logs used for anomaly detection.

Features:

1. packet_size: The size of each network packet.
2. response_time: Time taken to respond to a request.
3. malicious_score: A score indicating the likelihood of a threat.

Dataset Format:

packet_size	response_time	malicious_score
512	120ms	0.2
2048	95ms	0.8 (anomaly)
1024	110ms	0.1