Cybersecurity: Suspicious Web Threat Interactions

Cybersecurity: Suspicious Web Threat Interactions Project

By

Yashvi Vaghasiya

Introduction

- This project focuses on analyzing suspicious web traffic data collected from AWS CloudWatch.
- The goal is to detect anomalous and malicious web interactions using data analytics and machine learning techniques.
- Such detection helps organizations protect cloud-based infrastructure from cyber threats.
- Using data analytics and machine learning, the system identifies abnormal web interactions that may indicate malicious activity, helping organizations protect cloud-based infrastructure.

Tools Used

Programming & Libraries

- Python – Core programming language
- Pandas & NumPy – Data manipulation and preprocessing
- Matplotlib & Seaborn – Data visualization
- Scikit-learn – Machine learning algorithms
- TensorFlow & Keras – Neural network modeling
- NetworkX – Network graph analysis

Development Tools

- Jupyter Notebook – Analysis and experimentation

Domain:- Data Analytics, Cybersecurity and Machine Learning

Methodology

- 1. Data Collection from AWS CloudWatch logs
- 2. Data Cleaning & Preprocessing
- 3. Exploratory Data Analysis (EDA)
- 4. Feature Engineering
- 5. Machine Learning Modeling
- 6. Model Evaluation & Visualization

Data Analysis & Modeling

- EDA identified traffic patterns, country-based threats, and port usage.
- Isolation Forest was used for anomaly detection.
- Random Forest and Neural Networks were used for classification.
- Feature scaling and encoding improved model performance.

Results

- 100% accuracy across ML models
- Clear identification of suspicious web traffic
- Strong correlation between byte behavior and threat detection
- Effective detection using minimal features

Visual Outputs:

- Traffic trend plots
- Correlation heatmaps
- Country-wise detection graphs
- Network interaction graphs

Conclusion

- This project successfully demonstrates how data analytics and machine learning can be applied to detect suspicious web threat interactions.
- By analyzing AWS CloudWatch web traffic logs, the system identified abnormal patterns and classified malicious activities with high accuracy.
- The use of feature engineering and machine learning models improved threat detection efficiency, reducing the need for manual monitoring.
- Overall, this approach enhances cybersecurity by enabling automated, reliable, and scalable web threat detection in cloud environments.

Reference

GitHub Link: https://github.com/Yashu-teach/Cybersecurity-Suspicious-Web-Threat-Interactions

Thank You!