AegisShield: Adaptive Cybersecurity Threat Detection Dashboard

Project Report

1. Introduction

As digital threats grow more sophisticated, accessible cybersecurity tools are essential, especially for small-to-medium-sized enterprises and educational institutions. AegisShield addresses this need with an intuitive dashboard that leverages machine learning to enable real-time threat detection from network traffic and log data.

2. Abstract

AegisShield is an interactive dashboard that enhances traditional intrusion detection systems with dynamic threat analysis. Users can upload datasets, visualize feature distributions, and classify activities as benign or malicious using a machine learning model. Its adaptive learning module allows continuous improvement with new data, while integration with honeypot feeds enables proactive learning from real-world attack patterns.

3. Technological Stack

AegisShield's technology choices prioritize rapid development and robust performance:

- Core Language: Python for its data science libraries
- Dashboard Framework: Streamlit for a responsive user interface
- Data Science Libraries: Pandas and NumPy for data manipulation, scikit-learn for machine learning, Matplotlib and Seaborn for visualizations
- Model Persistence: Joblib for saving trained models
- Future Integrations: Planned connections with Zeek IDS, Wazuh-SOAR, and live honeypot servers

4. System Architecture and Workflow

Step 1: Data Ingestion
Users upload CSV files, which AegisShield preprocesses by encoding categorical features for analysis.

Step 2: Visualization Module
The dashboard provides insights into data characteristics through bar charts and heatmaps, helping analysts identify trends.

Step 3: Threat Detection Engine
Using a pre-trained SGDClassifier, the system classifies new data entries, flagging potential threats for quick identification.

Step 4: Performance Evaluation
A confusion matrix and classification report display model performance metrics, ensuring transparency and trust.

Step 5: Adaptive Learning
Users can retrain the model with new data, especially from honeypots, creating a continuous learning loop.

Step 6: Model Persistence
Updated models are saved as cyber_model.pkl for future use, preserving learned intelligence.

5. Conclusion

AegisShield is a user-friendly, modular platform for cybersecurity monitoring, integrating data visualization and machine learning to enhance threat detection. Its lightweight architecture is ideal for educational use and improving security in small enterprises.

6. Future Enhancements

Future enhancements may include:

- Real-time packet capture for live traffic analysis
- Advanced machine learning models like LSTMs for nuanced anomaly detection
- Automated alerting for high-confidence threats
- Cloud deployment for scalability and accessibility