Project Report: Classifying Cybersecurity Incidents

Microsoft: Classifying Cybersecurity Incidents with Machine Learning

Skills Gained:

- Data Preprocessing and Feature Engineering
- Machine Learning Classification Techniques
- Model Evaluation Metrics (Macro-F1 Score, Precision, Recall)
- Cybersecurity Concepts and Frameworks (MITRE ATT&CK)
- Handling Imbalanced Datasets
- Model Benchmarking and Optimization

Domain:

Cybersecurity and Machine Learning

Problem Statement:

Imagine you are working as a data scientist at Microsoft, tasked with enhancing the efficiency of Security Operation Centers (SOCs) by developing a machine learning model that can accurately predict the triage grade of cybersecurity incidents. Utilizing the comprehensive GUIDE dataset, your goal is to create a classification model that categorizes incidents as true positive (TP), benign positive (BP), or false positive (FP) based on historical evidence and customer responses. The model should support guided response systems in providing SOC analysts with precise, context-rich recommendations.

Business Use Cases:

- SOCs: Automate triage processes for more efficient threat response.
- Incident Response: Suggest appropriate actions based on incident type.
- Threat Intelligence: Improve detection using historical evidence.

- Enterprise Security: Prioritize real threats and reduce false positives.

Approach:

1. Data Exploration and Understanding:

- Load and inspect `train.csv`

- Visualize class distribution and check for imbalances

2. Data Preprocessing:

- Handle missing values

- Feature engineering from timestamps and categorical variables

- Encode categorical features

3. Data Splitting:

- Train-validation split with stratification

4. Model Selection:

- Baseline: Logistic Regression/Decision Tree

- Advanced: XGBoost, Random Forest, LightGBM

5. Model Evaluation:

- Metrics: Macro-F1, Precision, Recall

- Cross-validation and hyperparameter tuning

6. Model Interpretation:

- Feature importance via XGBoost

- Error analysis and model refinement

7. Final Evaluation:

- Evaluate model on `test.csv`

- Compare to baseline

8. Documentation:

- Process, performance, and deployment recommendations

Results:

- XGBoost Final Model:

- Macro F1 Score: 1.0000

- Macro Precision: 1.0000

- Macro Recall: 1.0000

- Baseline Model:

- Macro F1 Score: 0.1538

- Macro Precision: 0.1000

- Macro Recall: 0.3333

Dataset Overview:

The GUIDE dataset has three hierarchical levels: evidence, alerts, and incidents. The goal is to predict incident triage grades based on this hierarchy. 70% of the data is used for training and 30% for testing.

Technical Tags:

Machine Learning, Classification, Cybersecurity, Data Science, Model Evaluation, Feature Engineering, SOC, Threat Detection