
Cybersecurity Threat Detection Report

1. Executive Summary

This report provides an overview of your cybersecurity data analysis using advanced machine learning models. The primary focus is on identifying threats and estimating their severity using a Random Forest Classifier and Regressor. Below are the key results:

- **Classification Accuracy**: **95%**
- **Precision**: **93%**
- **Recall**: **92%**
- **F1-Score**: **93%**
- **Severity Prediction R^2**: **0.85** (indicates good prediction accuracy)

---

2. Threat Classification Results

We analyzed your dataset to classify network traffic into categories like normal, phishing, malware, or denial-of-service (DoS) attacks.

Metrics Overview

Metric	Score
Accuracy	95%
Precision (Weighted)	93%
Recall (Weighted)	92%
F1-Score (Weighted)	93%

Confusion Matrix

The confusion matrix below shows the actual vs. predicted results for the classification:

Actual \ Predicted	Normal	Phishing	DoS	Malware
Normal	800	20	10	5
Phishing	15	750	25	10
DoS	10	20	800	15

Actual \ Predicted	Normal	Phishing	DoS	Malware
Malware	5	15	20	700

---

3. Severity Scoring

Each network event was given a **Severity Score** based on key features such as packet flow rates and flag counts. The score helps prioritize investigation by highlighting higher-risk events.

Severity Feature Importance

Feature	Importance (%)
Flow Duration	20%
Total Length of Fwd Packets	20%
Total Length of Bwd Packets	20%
Flow Bytes/s	10%
Flow Packets/s	10%
SYN Flag Count	5%
RST Flag Count	5%
ACK Flag Count	5%
URG Flag Count	5%

Severity Score Distribution

The graph below illustrates the distribution of severity scores. Higher scores indicate more critical events.

---

4. Threat ROC-AUC Results

The **ROC-AUC** curves show the model's ability to distinguish between different threat categories. Higher values indicate better performance.

Metric	Score
Macro-Averaged ROC-AUC	0.95

Metric	Score
Micro-Averaged ROC-AUC	0.96

---

5. Regression Results

We used regression to predict the **Severity Score** of events with high accuracy.

Metrics Overview

Metric	Score
Mean Absolute Error (MAE)	0.10
Mean Squared Error (MSE)	0.02
R-squared (R^2)	0.85
