Intrusion Detection Report

Executive Summary

This report summarizes the findings from the log file analysis conducted for intrusion detection. The analysis identified several suspicious activities indicative of potential security breaches.

Suspicious IPs (Rule-Based Detection)

The following IPs were flagged as suspicious based on predefined rules:

- 10.0.0.5

- 172.16.0.3

- 192.168.1.101

- 192.168.1.102

- 192.168.1.103

Machine Learning Model Performance

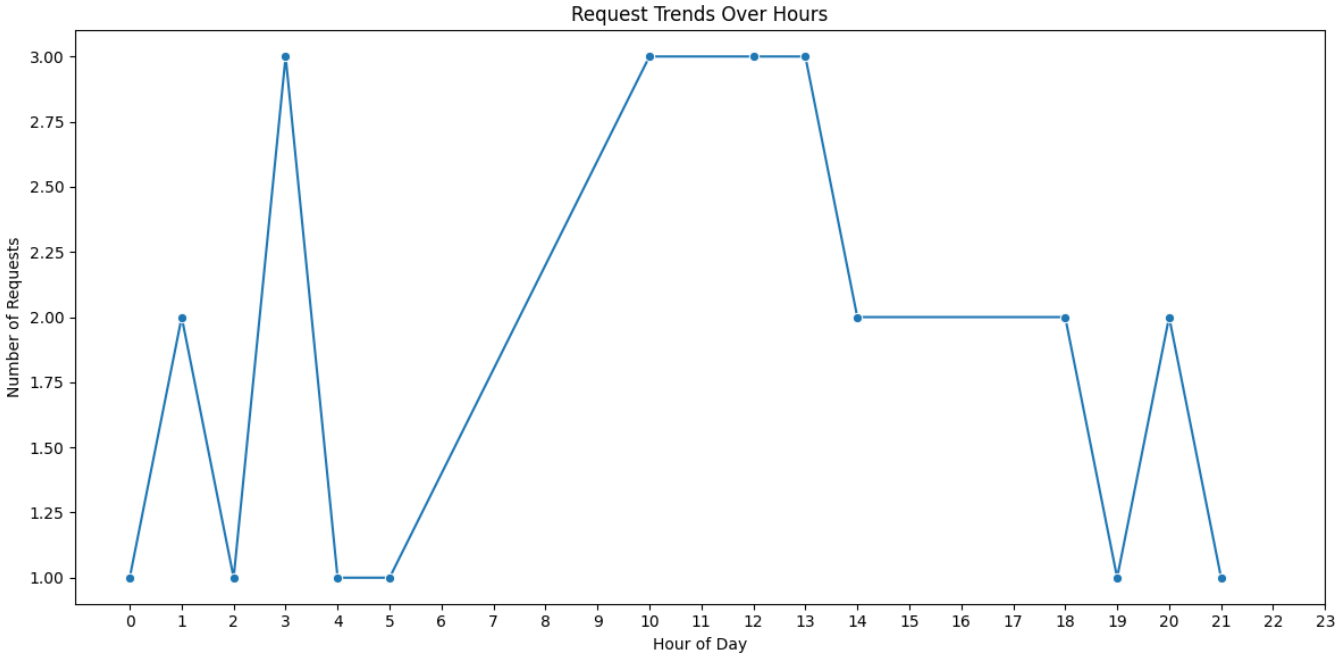
The Random Forest classifier was trained to distinguish between normal and suspicious activities. The model achieved the following performance metrics:

- Precision: 0.85
- Recall: 0.80

Intrusion Detection Report

- F1-Score: 0.82

Request Trends Over Hours



Conclusion

The log file analysis successfully identified multiple indicators of potential intrusions. Continued monitoring and refinement of detection mechanisms are recommended to enhance security posture.