■ Project Report: SIEM Alert Prioritization using ML

1. Introduction

SOC teams face alert overload. This project prioritizes alerts using Machine Learning.

2. Problem Statement

High alert volume, false positives, lack of prioritization.

3. Solution

ML model assigns risk scores and SHAP explains decisions.

4. Data

- siem_alerts.csv: alert metadata
- siem_features.csv: engineered ML features

5. Model

Supervised classifier producing risk probabilities.

6. Dashboard Workflow

Alerts → ML Scoring → Ranking → Analyst Review → Explainability

7. Explainability

Local SHAP explanations per alert.

8. Conclusion

Transparent, efficient SOC alert triage.