Forensic Investigation Report

Executive Summary

This report presents the findings of a comprehensive forensic analysis conducted on system logs. Through automated anomaly detection and entity extraction, we identified 100 anomalous events and extracted 120 key entities for further investigation.

Methodology

The investigation followed a systematic approach:

1. **Data Preprocessing**: Raw log data was cleaned and standardized
2. **Feature Engineering**: Additional analytical features were created
3. **Anomaly Detection**: Statistical methods identified unusual patterns
4. **Entity Extraction**: Natural Language Processing (NLP) using SpaCy extracted key entities

Key Findings

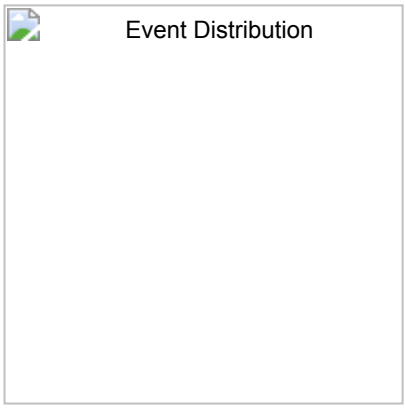
Anomaly Analysis

- Total anomalous events detected: **100**
- Most common anomalous event type: **file_access** (26 occurrences)
- Investigation period: 100 suspicious activities flagged

Entity Extraction Results

- Total entities extracted: **120**
- Entity types found: PERSON, ORG, GPE, CARDINAL
- Key persons of interest: 51 individuals identified
- Geographic locations: 17 locations flagged

Data Visualization



Conclusion

The automated analysis has successfully identified patterns and entities requiring further investigation. The anomaly detection system flagged 100 events for manual review, while entity extraction provided 120 potential leads.

Recommendations

1. Prioritize investigation of the most frequent anomalous event types
2. Cross-reference extracted entities with known databases
3. Conduct deeper analysis on flagged time periods
4. Implement continuous monitoring based on identified patterns

Report generated on: 2025-09-15 12:44:29