Cyber Log Analysis: Suspicious Activity Detection

- Prajit Giri

Project Overview

This initiative aimed to develop foundational skills in cybersecurity analysis through the examination of system log data. The primary objective was to emulate the workflow of a Security Operations Center (SOC) analyst by analyzing log entries, identifying anomalous patterns, and generating actionable alerts. A synthetic dataset of login and system events was constructed for this purpose, and rule-based detection logic was applied using both Excel and Python to identify suspicious behaviors such as repeated failed login attempts, atypical access hours, and compromised account activities. Though modest in scale, this exercise demonstrates essential principles of cybersecurity, including event log interpretation, rule creation for anomaly detection, and the translation of raw system data into human-readable alerts.

Synthetic Dataset Design

To ensure the project remained focused and transparent, a small, synthetic dataset was created representing typical authentication log fields. This dataset included:

- Timestamp
- Username
- Source IP address
- Action performed
- Authentication status

Example entries showcased events such as login attempts (both successful and failed), privilege changes, and patterns useful for basic threat detection.This table below was used as the basis for the log analysis conducted in the project.

Timestamp	User	SourceIP	Action	Status
2025-01-12 01:14:22	jdoe	192.168.1.44	login	failed
2025-01-12 01:15:10	jdoe	192.168.1.44	login	failed
2025-01-12 01:15:55	jdoe	192.168.1.44	login	failed
2025-01-12 09:22:13	admin	10.0.0.5	login	success
2025-01-12 09:23:57	guest	192.168.1.88	login	failed

2025-01-12 12:44:03	jdoe	192.168.1.44	login	success
2025-01-12 23:58:41	admin	10.0.0.5	privilegechange	success
2025-01-12 23:59:20	admin	10.0.0.5	login	failed
2025-01-13 00:01:07	admin	10.0.0.5	login	success

Table: 1

Detection Methodology

The following rules, aligned with beginner SOC analyst practices, were defined to flag potential security incidents:

- Brute-Force Attack Detection: Flag any user performing three or more failed login attempts within ten minutes.
- Unusual Login Times: Identify logins and privilege changes executed during late-night hours (00:00–05:00).
- Failed-Then-Successful Login Pattern: Flag sequences where multiple failed logins are promptly followed by a successful login, highlighting possible account compromise.

Events in the dataset such as repeated failed login attempts by a user (“jdoe”), late-night privilege changes by “admin”, and failed-to-successful login sequences were successfully identified and flagged as suspicious based on these rules.

Implementation Approach

Rule-based detection logic was implemented using both Excel and Python for accessibility:

- **Excel:** Utilized filters, time calculations, and helper columns to count failed login attempts and identify out-of-hours events. Flagged incidents were collated on dedicated summary sheets.
- **Python:** Logs represented as lists of dictionaries or simple DataFrames enabled automated counting, timestamp comparisons, and alert generation using loops and conditional statements.

The focus was on practicing the analytical core of log review and alert generation rather than building a production SIEM system.

Implementation

Rules were implemented using Excel (via filters, time calculations, and helper columns) and basic Python scripts (using lists, DataFrames, and loops). The flagged events were systematically collated and reviewed. The approach emphasized transparency and simplicity for educational analysis, rather than production deployment.

Alert Summary Table

Flagged suspicious activities from the synthetic log data:

User	Type of Suspicious Activity
jdoe	3 failed logins (possible brute-force attempt)
jdoe	Failed-to-success login pattern
admin	Late-night privilege change
admin	Failed-to-success login pattern

Reflection and Next Steps

This project provided practical experience in transforming raw event logs into actionable cybersecurity alerts. In future iterations, the methodology can be expanded to work with larger datasets, more advanced detection logic, and integrated security tools, such as SIEM platforms. This exercise marks an initial step toward a career in cybersecurity, emphasizing a commitment to mastering core analytical skills.