# Cybersecurity Log Analysis (SOC Beginner Project)

## 1. Introduction

This report analyzes authentication logs to identify suspicious login activities, brute-force attempts, abnormal IP addresses, and possible compromises. The goal is to demonstrate beginner SOC investigation techniques.

## 2. Sample Log Summary

A total of 30+ authentication log entries were analyzed, containing failed logins, successful logins, foreign IP access, account lockouts, and multi-user attacks.

## 3. Key Findings

### 1. Brute Force Attempt on User 'alex'

- 3 failed login attempts within 24 seconds.
- Followed by a 'Multiple failed attempts' alert.
- Risk Level: HIGH

### 2. Foreign Login (Possible Account Compromise)

- User: priya_p
- IP: 185.103.110.12 (Russia)
- Failed login followed by success.
- Risk Level: HIGH

### 3. Account Lockout

- User: rahul.k
- Locked after repeated failed attempts.
- Risk Level: MEDIUM

### 4. Credential Stuffing Attempt

- IP: 102.44.18.22 targeted 4 accounts (admin, guest1, guest2, guest3).
- 12 failed attempts logged.
- Risk Level: CRITICAL

### 5. Normal Login Events

- Legitimate logins from known IPs for users megha and siddharth.

4. Summary of Threat Patterns

- Brute-force attacks detected.

- Credential stuffing from a malicious IP.

- Foreign login anomalies.

- Account lockouts triggered by failed attempts.

5. Recommendations

- Enable MFA for all users.

- Block suspicious IPs.

- Implement brute-force threshold rules.

- Enforce password reset for impacted accounts.

- Add geo-restriction alerts for foreign logins.

6. Conclusion

The analysis highlights multiple security risks and demonstrates core SOC skills: log interpretation, threat pattern identification, and incident reporting.