Cybersecurity Job Simulation – Security Incident Analysis (Deloitte)

This report reflects a practical SOC-style investigation based on log analysis performed during a cybersecurity simulation.

1. Incident Overview

A data breach involving sensitive internal information was reported at Daikibo Industrials, impacting manufacturing operations. The issue was suspected to originate from the internal status dashboard.

2. Investigation Approach

The web_requests.log file was analysed to identify suspicious activity. Login patterns, request sequences, and behavioral anomalies were reviewed to differentiate between normal and abnormal usage.

3. Key Findings

The user ID mdB7yD2dp1BFZPontHBQ1Z showed suspicious activity. After a normal login, the activity shifted to automated API requests at fixed one-hour intervals without loading dashboard resources, indicating non-human behavior.

4. Security Issue Identified

The dashboard cannot be accessed directly from the internet. The activity originated internally, suggesting compromised credentials or misuse of valid access through automation.

5. Response & Recommendations

- Implement API rate limiting
- Enable real-time monitoring for abnormal patterns
- Enforce multi-factor authentication (MFA)
- Conduct regular access reviews
- Improve session validation and anomaly detection

6. Real-World Insight

Many real-world breaches occur through compromised internal accounts where attackers automate data extraction without triggering traditional security alerts.

7. What I Learned

- Log analysis helps detect hidden threats
- Automated patterns reveal attacker behavior
- Internal access can still pose risks
- Monitoring is critical alongside access control

This report presents a structured analysis of a simulated cybersecurity incident, highlighting investigation techniques, log analysis, and practical response strategies.

Report Prepared By
Shaik Abdul Rehman
Aspiring SOC Analyst | IAM Enthusiast
Project: Deloitte Cybersecurity Simulation (Forage)
Date: September 2025

"— End of Report —"