Web Log Analysis – Deloitte Australia Cybersecurity Job Simulation

This repository contains the work I completed during the **Deloitte Australia Cybersecurity Virtual Experience**, where I conducted a forensic analysis of internal web activity to investigate a suspected security breach at **Daikibo Industrials**.

Project Overview

Client: Daikibo Industrials
Situation: A major news outlet released sensitive information about Daikibo. At the same time, the company experienced a production line failure. Daikibo suspected that their internal telemetry dashboard—used to monitor machine and factory performance—may have been compromised by an external attacker.

Objective

As a member of the cyber team, my assignment was to:

- Analyze internal web request logs during the suspected incident window.
- Identify suspicious user activity, if any.
- Determine whether the breach could have originated **from the internet**, bypassing Daikibo's VPN.
- Advise the client on whether their telemetry dashboard had been compromised or remained secure.

Methodology

Each block of the web log file represents activity from a unique internal IP address. Each includes timestamped HTTP requests made to Daikibo's telemetry dashboard, including login pages, static resources, and API endpoints.

I reviewed the log file manually using Notepad, guided by a provided log inspection framework. I followed key patterns to detect anomalies, including:

- Standard login flows followed by dashboard page loading
- API request frequency and consistency (indicating possible automation)
- Unexpected patterns, such as API calls without prior login or UI resource requests

Key Finding

Suspicious User Identified:
`mdB7yD2dp1BFZPontHBQ1Z`

This user account generated a series of repetitive, structured API requests—suggesting the use of automated tools or scripts. However, all activity came from a **valid internal IP address**, and the logs show no indication of access from outside the VPN.

Conclusion

There is **no evidence** that Daikibo's telemetry dashboard was accessed from the internet. The system was not breached externally.

The suspicious activity is **internal** and may reflect policy violations or misuse of dashboard APIs by the identified user.

Recommendations

- Conduct an internal audit of the account `mdB7yD2dp1BFZPontHBQ1Z`
- Review access control rules on API endpoints
- Implement monitoring for repeated automated access patterns

Repository Contents

- `log_analysis_guide.pdf` – Reference material used to interpret log patterns
- `web_activity.log` – The raw log file showing internal web requests
- `client_advisory_report.pdf` – The professional advisory sent to Daikibo with findings and recommendations

Author

Temple Nnanna Idam-Nkama
Cybersecurity Analyst | Tech Enthusiast