# Security Advisory Report on Suspected Breach of Daikibo's Telemetry Dashboard

**Client:** Daikibo Industrials
**Subject:** Investigation into Suspicious Activity and Potential Breach
**Date:** 19th March 2025
**Prepared by:** Temple Nnanna Idam-Nkama, Cybersecurity Analyst

## Executive Summary

Following your request to investigate a suspected security breach involving your internal telemetry dashboard, I have completed a detailed analysis of your web activity logs. The objective was to determine whether your telemetry dashboard had been accessed by an external actor, potentially bypassing Daikibo's VPN.

After a full review of the `web_requests.log` file and comparison with expected behavior patterns, there is **no evidence of an external compromise**. However, one internal user account was found to exhibit suspicious activity that may require further review.

## Objectives of This Analysis

1. **Determine if the telemetry dashboard was accessed from outside the Daikibo network**
2. **Identify suspicious behavior, automated access patterns, or irregular user activity**

3. **Advise on the next steps to safeguard the integrity of the dashboard and internal systems**

## Tools and Resources Used

- **Text Editor (Notepad):** Used for line-by-line review of log file blocks
- **Web Log Analysis Guide (Provided):** Used to understand and track HTTP request sequences
- **Manual Inspection & Pattern Recognition:** To identify anomalies across user activity blocks

## Methodology

Each block of your `web_requests.log` represents traffic from a unique static internal IP address. Requests were reviewed for:

- Proper login sequences (login page → dashboard assets → API calls)
- Unauthorized or skipped login attempts
- Repeated or time-triggered API requests (possible automation)
- Any evidence of external IP access or login bypasses

## Key Findings

1. **No External Access Detected**
   All requests originated from internal IP addresses within Daikibo's network. There were no connections from unknown or public IP addresses. This confirms that **no unauthorized access occurred from outside your VPN**.

2. **Suspicious Internal Activity Identified**
   A particular user account—**User ID: `mdB7yD2dp1BFZPontHBQ1Z`**—exhibited repetitive and structured API requests that were:
   a. Made at short, fixed intervals
   b. Not accompanied by dashboard UI refreshes or logins
   c. Indicative of possible automated scripts or unauthorized background polling
3. **Telemetry Dashboard Integrity Remains Intact**
   All accessed endpoints returned `200 OK`, showing no disruptions or tampering with application logic. The telemetry dashboard performed as expected, and there is **no evidence of a breach or data compromise** through its interface.

## Conclusion

Your telemetry dashboard has **not been breached from an external source**. However, the internal activity logged under User ID: ***`mdB7yD2dp1BFZPontHBQ1Z`*** suggests non-standard access behavior that may violate usage policies or introduce performance and security concerns.

## Recommendations

- **Conduct an internal audit** on the account `mdB7yD2dp1BFZPontHBQ1Z` to confirm its intended usage and legitimacy
- **Implement rate-limiting or usage thresholds** for API endpoints to detect and mitigate automated polling
- **Enable internal alerting and logging mechanisms** to catch repeated API access patterns without corresponding UI interaction
- **Reinforce internal access controls** by monitoring which roles have access to sensitive machine status APIs

## Attached Documents

- `web_requests.log`: Full internal request log file reviewed
- `log_analysis_guide.pdf`: Reference material used to interpret request flow
- `user_activity_summary.txt`: Breakdown of suspicious user access patterns

## 📞 Contact

Temple Nnanna Idam-Nkama
Cybersecurity Analyst
📧 templeanthony500@gmail.com
🔗 GitHub Profile  LinkedIn Profile

**Thank you for entrusting me with this investigation.** If further support or extended security assessment is needed, I remain available to assist.