**SIEM Log Analysis Report  
Prepared by:** Adefolaji Fasanya **Organization:** TriAxis Infrastructure Corp **Date:** 05/08/2025 **Tools Used:** Splunk Enterprise, TryHackMe Lab Environment

**Objective**This report documents the analysis of network security event logs collected from May 6 to May 13, 2025. The purpose is to identify indicators of compromise (IOCs), detect abnormal behaviors, and recommend actions to improve the security posture of TriAxis Infrastructure Corp, a national utility infrastructure contractor.

**Summary of Findings**

* Detected multiple failed SSH login attempts from internal IP 192.168.1.150, indicating a potential brute-force attack.
* Unusual outbound traffic on port 443 observed from host TRIAX-OT-07, flagged for possible data exfiltration.
* PowerShell scripts executed from engineering workstation TRIAX-WKS-ENG-02, which is outside normal user behavior.

**Detailed Event Analysis**

| **Date/Time** | **Event Description** | **Source IP / Host** | **Destination IP** | **Severity** | **Action Taken** |
| --- | --- | --- | --- | --- | --- |
| ***2025-05-12 14:33:22*** | 10 failed SSH login attempts | 192.168.1.150 | Internal server | Medium | IP blocked; admin alerted |
| ***2025-05-13 09:45:10*** | PowerShell script execution detected | TRIAX-WKS-ENG-02 | N/A | High | Endpoint scanned and isolated |
| ***2025-05-13 15:21:55*** | High outbound data transfer on port 443 | TRIAX-OT-07 | 212.103.88.54 | High | Host quarantined; logs reviewed |

**Recommendations**

* Apply strict firewall rules using updated threat intelligence feeds to block suspicious IPs.
* Restrict PowerShell execution using Group Policy or AppLocker for non-admin users.
* Update SIEM correlation rules to detect unusual outbound traffic and after-hours activity.
* Reinforce employee cybersecurity training focused on credential safety and phishing awareness.

**Appendix**

* Splunk search queries used in detection
* Redacted log samples
* Screenshots of triggered alerts and dashboards
* Full list of IOCs with timestamps