

## **Incident Report – Hybrid Style**

**Analyst:** Martin Inyang

**Date:** 2026

### **1. Executive Summary**

An authentication anomaly was detected involving unusual login attempts from an external IP address. Initial analysis confirms multiple failed authentication attempts, suggesting potential credential stuffing or brute-force activity. No confirmed compromise occurred.

### **2. Technical Details**

- Multiple failed logins detected within a short time window.
- Suspicious geolocation mismatch for attempted login.
- Privilege escalation attempts observed in logs.
- Activity mapped to MITRE ATT&CK; T1110 (Brute Force).

### **3. Business Impact**

Although no systems were compromised, repeated authentication attempts indicate possible probing of critical accounts. If successful, this could lead to unauthorized access, data exposure, or system misuse.

### **4. Actions Taken**

- Conducted Splunk log review and correlation.
- Confirmed lack of successful access.
- Blocked suspicious IP at firewall level.
- Recommended MFA enforcement and password hardening.

### **5. Recommendations**

- Implement geolocation-based login alerts.
- Conduct password hygiene awareness training.
- Review administrative account activity weekly.

### **6. Conclusion**

The investigation confirms attempted unauthorized access but no breach. Continued monitoring and preventive measures are recommended to strengthen security posture.