Security Incident Investigation Report

---

1) Investigation Steps

Step 1: Log Analysis in SIEM (Splunk)

1. Accessed **Splunk SIEM** to review authentication logs.
2. Filtered logs by **Event ID 4625 (Failed Login Attempts)**.
3. Noted a series of **50+ failed login attempts** from the same IP address within a short time frame.
4. Identified a **successful login attempt** after multiple failures.

Step 2: Identifying Malicious Activity

1. Investigated user activity post-login.
2. Detected **Event ID 4672 (Admin Privilege Granted)**, indicating privilege escalation.
3. Found commands executed for data exfiltration.

Step 3: Threat Intelligence & Verification

1. Checked the **IP address (192.168.1.100)** against threat intelligence databases.
2. Found the IP flagged for malicious activity in previous cyberattacks.

---

2) Key Findings

Timestamp	Source IP	Username	Action	Status
03:15:22	192.168.1.100	admin	Login Attempt	Failed
03:16:45	192.168.1.100	admin	Login Attempt	Failed
03:17:10	192.168.1.100	admin	Login Attempt	Success
03:18:30	192.168.1.100	admin	Privilege Escalation	Success
03:19:45	192.168.1.100	admin	Data Accessed	Success

•

- The **attacker gained access after multiple failed attempts**, indicating a **brute-force attack**.
- The attacker **elevated privileges**, allowing access to sensitive data.
- Post-attack activities suggest **potential data exfiltration**.

3) Recommendations & Mitigation Strategies

☑ **Enable Multi-Factor Authentication (MFA):** Adds an extra layer of security.
☑ **Block IP Addresses with Excessive Failed Logins:** Implement automated firewall rules.
☑ **Monitor Security Logs Regularly:** Set up alerts for unusual login patterns.
☑ **Implement Account Lockout Policies:** Restrict login attempts after a set number of failures.
☑ **Conduct Security Awareness Training:** Educate employees on password hygiene and phishing attacks.

---

4) Conclusion

This investigation highlights the importance of **proactive log monitoring** and **access control measures** in preventing security breaches. Implementing the recommended security controls will strengthen system defenses against future attacks.

Prepared by: Vanessa Christy
Date: 17 March 2025