INCIDENT RESPONSE REPORT

Incident ID: SOC-IR-20250703-002
Date/Time Detected: 2025-07-03 09:02:14
Reported By: Splunk SIEM (manual search)

Summary of Incident

Multiple failed login attempts were observed for user account david, including one from **public IP address 203.0.113.77**. These login failures may indicate **unauthorized access attempts** or a **brute-force attack** in progress.

User Involved

- **Username:** david
- **IP Address:** 203.0.113.77
- **Host:** SOC-simulated
- **Location:** Unknown (public IP range)

Log Evidence

Example log event from Splunk:

```
2025-07-03 09:02:14 | user=bob | ip=203.0.113.77 | action=login failed
```

Additional context: Previous activity from this IP also includes file accessed and malware detected events, raising the risk level.

Severity: Medium

Impact Assessment

- Possible attempt to gain unauthorized access to user account
- May be part of a broader brute-force or credential stuffing campaign
- Risk of data exposure if login eventually succeeds

Recommended Response Actions

- Lock or temporarily disable the account bob
- Force password reset and enable MFA (Multi-Factor Authentication)
- Monitor further login attempts from this IP or similar IP ranges
- Correlate with other user or IP events

Communication Plan

- Notify SOC lead and account administrator
- Flag the IP 203.0.113.77 for monitoring or blocking in firewall rules
- Escalate to Tier 2 SOC analyst if further activity is observed

Status:

Being monitored