3.2 SITREP (Google Docs Submission Version)

Title: Unauthorized Access on Server-Y

Date: 2025-08-22
Author: Mayuri Sawle

1. Summary

At 13:00 on 2025-08-18, unauthorized access attempts were detected on Server-Y. The source IP, 192.168.1.200, attempted authentication using valid credentials, aligning with MITRE ATT&CK Technique **T1078 – Valid Accounts**. The activity was identified through abnormal login patterns and flagged as high severity.

2. Impact Assessment

- Affected Asset: Server-Y (Business-critical)
- Potential Risk: Credential compromise, unauthorized access, data exposure
- Severity: High
- Current Status: Server isolated to prevent further activity

3. Actions Taken

- Isolated Server-Y from the internal network.
- Blocked suspicious IP address at firewall.
- Created a High-severity case in TheHive.
- Conducted credential integrity check.
- Escalated case to Tier 2 for deeper investigation.

4. Next Steps

- Conduct memory and disk forensics on Server-Y
- Analyze authentication logs for additional anomalies
- Reset or rotate compromised accounts
- Perform threat-hunting for T1078-related behavior across environment.

Summary:

A high-severity unauthorized access attempt on Server-Y was escalated from Tier 1 to Tier 2 via TheHive. A SITREP documented the event, actions, and impact. A Splunk Phantom playbook was created to auto-assign all High-priority alerts to the Tier 2 queue, improving escalation speed and workflow consistency.