SITREP Draft

Incident Summary

- **Incident Type:** Unauthorized Access
- **Severity:** High
- **Detection Time:** 2025-08-18 13:00
- **Affected System:** Server-Y
- **Source IP:** 192.168.1.200
- **MITRE ATT&CK Technique:** T1078 – Valid Accounts

Situation Overview

On 18 August 2025 at 13:00, security monitoring systems detected unauthorized access activity on Server-Y. The activity originated from internal IP address 192.168.1.200 and was identified as suspicious due to abnormal authentication behavior. Initial analysis suggests potential misuse of valid credentials, aligning with MITRE ATT&CK technique T1078. Based on the assessed risk, the incident was classified as High severity and escalated for further investigation.

Actions Taken

- Alert validated by Tier-1 SOC analyst
- Server-Y isolated from the network to contain potential impact
- Relevant logs identified and preserved
- Incident escalated to Tier-2 SOC for advanced analysis

Current Status

The incident is currently under investigation by the Tier-2 SOC team. No confirmed data exfiltration has been observed at this time.