# SITREP: Unauthorized Access on Server-Y

## Summary

- Detected: 2025-09-18 13:00 UTC  
- Source IP: 192.168.1.200  
- MITRE Technique: T1078 (Valid Accounts)

## Brief

Monitoring detected unauthorized access to Server-Y originating from IP 192.168.1.200. Indicators suggest valid-credential usage consistent with MITRE T1078. The server has been isolated and forensic images acquired.

## Actions Taken

- Isolated Server-Y from production network.  
- Collected forensic image (/forensics/Server-Y-20250818.img).  
- Created case in TheHive and escalated to Tier-2.  
- Uploaded authentication logs and session artifacts.

## Impact

- Server-Y removed from production; no confirmed data exfiltration.

## Next Steps

- Tier-2 to validate account compromise, enumerate lateral movement, and preserve forensic artifacts.  
- Coordinate remediation (password resets, user re-provisioning) if compromise confirmed.  
- Notify stakeholders per escalation policy.

## Status

Escalated to Tier-2 — investigation in progress.