Unauthorized Access on Server-Y

1. Summary

An unauthorized access incident was detected on Server-Y at 2025-12-18 13:00 involving IP address 192.168.1.200. The activity aligns with MITRE ATT&CK T1078 (Valid Accounts), indicating possible misuse of legitimate credentials.

2. Actions Taken

- Alert triaged and validated by SOC L1
- Server-Y isolated to prevent further access
- Logs and access evidence preserved
- Incident escalated to SOC L2

3. Current Status

Contained and under SOC L2 investigation.

4. Next Steps to be taken

- Credential compromise assessment
- User behavior and access pattern analysis
- Lateral movement and environment-wide threat hunting
- Remediation and recovery planning