Unauthorized Access on Server-Y

Incident Summary

On **18 August 2025 at 13:00**, suspicious authentication activity was detected on **Server-Y** originating from **IP address 192.168.1.200**. The activity indicated possible misuse of valid credentials and aligns with **MITRE ATT&CK technique T1078 (Valid Accounts)**. The incident was identified during routine security monitoring and classified as **High Priority** due to the potential risk of unauthorized access and lateral movement.

Impact Assessment

At the time of detection, no evidence of data exfiltration, service disruption, or system modification was observed. However, the use of valid credentials presents a moderate risk and requires further investigation to confirm the scope of access and ensure no persistence mechanisms were established.

Actions Taken

- Isolated Server-Y from the network to prevent further access
- Flagged the source IP for monitoring and investigation
- Escalated the incident to **Tier 2 SOC** for detailed analysis and response

Current Status

- Incident contained
- Investigation in progress by Tier 2 SOC
- Monitoring continues for related activity

Next Steps

- Review authentication logs for additional suspicious activity
- Validate affected user credentials
- Implement enhanced monitoring for similar access attempts