Unauthorized Access Detection on Server-Y

Executive Summary

On 18 August 2025, a security incident involving unauthorized access attempts was detected on Server-Y during routine monitoring activities. Alerts indicated suspicious authentication behavior originating from IP address 192.168.1.200. Initial analysis suggested possible misuse of valid credentials, aligning with MITRE ATT&CK technique T1078 (Valid Accounts). Immediate containment actions were taken to reduce risk and prevent potential lateral movement. No confirmed data exfiltration was observed during the investigation.

Timeline of Events

- **13:00** – Suspicious authentication activity detected on Server-Y
- **13:05** – Alert triaged and classified as high priority
- **13:10** – Server-Y isolated from the network
- **13:20** – Incident escalated to Tier 2 for deeper investigation

Actions Taken

- Affected server was isolated
- Suspicious IP was flagged for monitoring
- Credentials associated with the incident were reviewed

Recommendations

- Enforce stronger authentication controls
- Monitor login activity outside business hours
- Improve alerting for repeated authentication failures
- Conduct periodic access reviews