Tier-2 Escalation Summary

On 2025-08-18 at 13:00, a high-priority alert was generated for unauthorized access activity on Server-Y originating from IP address 192.168.1.200. Tier-1 analysis confirmed abnormal authentication behavior consistent with MITRE ATT&CK technique T1078 (Valid Accounts). The affected server was isolated as an immediate containment measure to prevent potential lateral movement. Relevant authentication and system logs were preserved for investigation. No confirmed data exfiltration has been identified at this stage. Due to the likelihood of credential misuse and the elevated risk to the environment, the incident is escalated to Tier-2 for in-depth forensic analysis, credential impact assessment, and scope determination.