Title: Escalation Summary: Unauthorized Access on Server-Y

Summary:
On 2025-09-18 at 13:00 UTC, monitoring detected unauthorized access to Server-Y from IP 192.168.1.200. Initial indicators include valid-credential usage consistent with MITRE T1078, anomalous session activity, and suspicious privilege escalation attempts. The host has been isolated from the network and forensic images collected. Authentication logs and session artifacts are available in the case. Immediate objectives for Tier 2: validate account compromise, enumerate lateral movement, and determine attacker persistence. Preserve volatile evidence and coordinate containment with systems team. Escalate to IR manager if compromise persists and notify stakeholders as per policy.