Hunting Report

MITRE ATT&CK Tactic & Technique: Initial Access / Persistence (T1078 - Valid Accounts).

A threat hunt for unauthorized privilege escalation identified the service account svc_backup being granted local administrative privileges (Event ID 4672) on 2025-09-27. Subsequent log analysis revealed the account performing an interactive logon and executing nc.exe. Cross-referencing logs with AlienVault OTX intel showed svc_backup was communicating with 203.0.113.50, an IP linked to T1078 account compromise. This validates the hypothesis, confirming a potential Valid Accounts compromise that achieved Persistence and Defense Evasion via legitimate credentials and privilege escalation. Immediate isolation of the compromised host and password rotation for svc_backup is recommended.