# Threat Hunting Report – MITRE ATT&CK T1078

A threat-hunting exercise was conducted on 11 February 2026 to identify potential abuse of valid accounts within the environment. Elastic Security analysis of Event ID 4672 revealed unexpected privilege assignment to a non-administrative user account. Threat intelligence research in AlienVault OTX identified related activity under MITRE ATT&CK technique T1078 (Valid Accounts), including a suspicious IP indicator, 185.220.101.45, associated with credential abuse campaigns. Cross-validation using Velociraptor process queries confirmed active processes running under elevated privileges. Although no confirmed compromise was established, the correlation of privilege escalation events and threat intelligence indicators suggests heightened risk requiring further monitoring and credential review.