HUNTING REPORT

During this hunt, Windows Event Logs were examined for anomalous login activity, focusing on privileged and standard account usage. Test events including Event ID 4672 (privileged account assignments) and 4625 (failed login attempts) were generated and tracked. Logs were successfully captured through Velociraptor and verified in Elasticsearch on the Kali server. Analysis indicated potential misuse of valid accounts, highlighting unauthorized access attempts and failed login patterns. Observations confirmed that correlating endpoint event logs with centralized logging enhances detection of suspicious authentication. Findings correspond to MITRE ATT&CK T1078, emphasizing continuous monitoring and validation of legitimate accounts to prevent compromise.