Detection of Valid Accounts, Detection Strategy DET0724

Archived: 2026-04-02 11:02:26 UTC

AN1857

Monitor for an authentication attempt by a user that may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
Monitor for logon behavior that may abuse credentials of existing accounts as a means of gaining Lateral Movement or Persistence. Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).
Monitor for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account.

Log Sources
