T1136.001 Detection Strategy - Local Account Creation Across Platforms, Detection Strategy DET0447

Archived: 2026-04-05 16:19:39 UTC

AN1235

Adversary uses built-in tools like 'net user /add', PowerShell, or WMI to create a local user. Sequence: Account creation event (4720) follows process creation of a suspicious executable (e.g., powershell.exe or net.exe).

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Attackers may use cmd.exe, wscript.exe, or renamed binaries to evade detection
TimeWindow	Define time threshold between process start and user creation event (e.g., 5s–2m)
UserContext	Correlate if process runs under SYSTEM, Administrator, or untrusted account

AN1236

Local user accounts are created via binaries like 'useradd', 'adduser', or by editing passwd/shadow. Behavior chain includes execution of user management binaries or modification of user database files.

Log Sources

Mutable Elements

Field	Description
BinaryPath	Account creation may be scripted via shell scripts, cron jobs, or remote shells
ExecutionSource	Flag if commands are issued from remote sessions (e.g., sshd)

AN1237

Account creation using 'dscl -create' or via GUI tools. Detection involves command execution and file changes to the local directory services database.

Log Sources

Mutable Elements

Field	Description
UsernamePattern	Accounts like 'svc*', 'backup*' may blend into legit naming patterns
SessionOrigin	Identify if dscl was run locally, via ARD, or Terminal.app

AN1238

Account created using esxcli commands. Sequence includes esxcli execution and successful modification to account DB.

Log Sources

Mutable Elements

Field	Description
CommandOrigin	Console sessions vs SSH vs vSphere CLI session may affect alert fidelity

AN1239

Account created in a running container (e.g., via 'useradd' or by modifying /etc/passwd directly). Detectable via runtime telemetry (e.g., Falco or eBPF hooks).

Log Sources

Mutable Elements

Field	Description
ContainerContext	Distinguish between ephemeral containers and long-lived service containers
NamespaceScope	Determine if account was added inside host, user, or PID namespace

AN1240

Account created via CLI using 'username' command or REST API. Detectable through AAA logging or CLI history telemetry.

Log Sources

Mutable Elements

Field	Description
PrivilegeLevel	Some devices allow unprivileged user creation—adjust based on role risk
RemoteSessionFlag	Creation via Telnet, SSH, or serial console affects detection priority

---