Suspicious Addition to Local or Domain Groups, Detection Strategy DET0310

Archived: 2026-04-05 17:54:55 UTC

AN0865

Detects unauthorized additions of users or machine accounts to privileged local or domain groups (e.g., Administrators, Remote Desktop Users).

Log Sources

Mutable Elements

Field	Description
TargetGroup	Set to detect high-privileged groups like 'Administrators', 'Domain Admins', or 'Remote Desktop Users'
TimeWindow	Restrict detections to business hours or approved maintenance windows
UserContext	Filter out known automated processes or provisioning systems

AN0866

Detects unexpected use of usermod, gpasswd, or direct modification of /etc/group to elevate user group membership.

Log Sources

Mutable Elements

Field	Description
GroupName	Focus on 'sudo', 'wheel', or custom high-privilege groups
UserContext	Account that initiated the change (e.g., service account or unrecognized user)
TimeWindow	Detect elevation outside change windows

AN0867

Detects use of `dseditgroup` or `dscl` to add users to privileged macOS groups (e.g., admin).

Log Sources

Mutable Elements

Field	Description
GroupName	Focus on 'admin' or 'com.apple.access_ssh'
UserContext	Detect unknown or transient users making group changes
TimeWindow	Detect group modifications at suspicious times
