Account Manipulation Behavior Chain Detection, Detection Strategy DET0096

Archived: 2026-04-05 16:49:31 UTC

AN0265

Account attribute changes (e.g., password set, group membership, servicePrincipalName, logon hours) correlated with unusual process lineage or timing, indicating privilege escalation or persistence via valid accounts.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time between suspicious process and account change (e.g., 5m).
HighPrivilegeGroupList	Customize group list (e.g., Domain Admins, Enterprise Admins) to monitor.
SubjectTargetMismatch	Flag if account modifier != modified user (potential hijack).

AN0266

Use of native tools or scripting (e.g., `usermod`, `passwd`, `groupmod`) to escalate permissions or persist access on existing users, correlated with login or process events.

Log Sources

Mutable Elements

Field	Description
SudoPath	Common sudo or privilege escalation paths (e.g., `/usr/bin/passwd`).
ModifiedShellList	Detect if user shell is changed to unusual one (e.g., /bin/sh -> /bin/bash).

AN0267

Modifications to user accounts via `dscl`, `pwpolicy`, or System Preferences CLI (`sysadminctl`) that alter user groups, enable root, or bypass MDM restrictions.

Log Sources

Mutable Elements

Field	Description
ModifiedUserList	Track known non-system user UIDs or service accounts.
GroupMembershipChanges	List of sensitive groups (admin, _developer, _analyticsd).

AN0268

Modifications to SSO/SAML user attributes (e.g., `isAdmin`, `role`, MFA bypass, App assignments) often through CLI, API, or rogue IdP apps.

Log Sources

Mutable Elements

Field	Description
RoleAssignmentBaseline	Expected user-role pairings per app or org unit.
APIUsageContext	Caller identity or IP address ranges for identity admin actions.

AN0269

Addition of new users or changes to role permissions (e.g., ReadOnly -> Admin) via API or vSphere Client, particularly from non-jumpbox IPs.

Log Sources

Mutable Elements

Field	Description
VMAdminAccountName	Expected account name patterns for ESXi/vCenter admins.
NetworkAccessLocation	Expected IPs/subnets for legitimate ESXi access.

AN0270

Role escalation (e.g., Editor → Owner) in cloud collaboration tools (Google Workspace, O365) or file sharing apps to maintain elevated access.

Log Sources

Mutable Elements

Field	Description
SharingSensitivityLabel	Threshold for labeling sensitive document access escalation.
CrossOrgChanges	Track changes made across organizational boundaries (e.g., guest users).
