Detection Strategy for Masquerading via Account Name Similarity, Detection Strategy DET0383

Archived: 2026-04-05 16:44:28 UTC

AN1077

Detects adversary behavior where a newly created or renamed user account closely resembles existing service or administrator accounts to blend in and avoid detection. Common patterns include prefix/suffix modifications, homoglyphs, or use of names like 'admin1', 'adm1n', or 'backup_help'.

Log Sources

Mutable Elements

Field	Description
SimilarityThreshold	Defines how close in Levenshtein or visual distance an account name must be to a legitimate one to raise an alert.
MonitoredAccountList	Set of known legitimate accounts to compare new account names against.
TimeWindow	Period within which anomalous account creation or renaming is evaluated in relation to discovery or deletion activity.

AN1078

Detects creation or renaming of accounts with names that closely match known service, root, or admin accounts. Behavior often follows account discovery or deletion, attempting to blend into system activity logs using trusted name conventions.

Log Sources

Mutable Elements

Field	Description
AllowedSystemAccounts	Whitelist of legitimate service accounts used for validation.
LevenshteinThreshold	Edit distance sensitivity between created account and existing account names.
ScriptInitiatorDetection	Whether to flag account creation events triggered from suspicious scripts or shell histories.

AN1079

Detects adversary creation of cloud or IdP accounts whose names resemble existing privileged or service accounts. May indicate preparation for privilege escalation or defense evasion.

Log Sources

Mutable Elements

Field	Description
RoleScope	Whether created users have privileged or scoped roles assigned at creation.
NamingHeuristics	Regex patterns or heuristics for detecting suspicious naming conventions (e.g., helpdesk_support_, root-admin).

AN1080

Monitors for the creation of accounts inside containers using names that resemble legitimate orchestrator or backup identities to mask adversary persistence.

Log Sources

Mutable Elements

Field	Description
ContainerContextScope	Limit detection to containers with persistent volumes or specific workloads
MasqueradePatternList	Custom list of commonly abused names to blend into container environments (e.g., kubelet, cronjob_sync)
