Detection Strategy for Additional Cloud Credentials in IaaS/IdP/SaaS, Detection Strategy DET0531

Archived: 2026-04-05 17:37:51 UTC

AN1469

Addition of credentials (keys, app passwords, x.509 certs) to existing cloud accounts, service principals, or OAuth apps via portal or API by non-standard identities or IP ranges.

Log Sources

Mutable Elements

Field	Description
MFABypassMechanism	App password or legacy auth activity bypassing MFA policies.
SourceIPAllowlist	Expected IPs allowed to perform admin identity operations.
ApplicationCredentialType	Track types like `client_secret`, `certificate`, `password`, `federated`.

AN1470

Cloud API usage to create/import SSH keys or generate new access keys (CreateAccessKey, ImportKeyPair, CreateLoginProfile) from non-console access or unusual principals.

Log Sources

Mutable Elements

Field	Description
CallerIdentityContext	Track root, federated identities, and STS tokens separately.
NewCredentialUsageWindow	Time between key creation and first use (default: 5 min).
IAMRoleBaseline	Expected services/accounts allowed to create keys.

AN1471

Credential-related configuration changes in productivity apps, such as API key creation in Google Workspace, app tokens in Slack, or user-level OAuth credentials in M365.

Log Sources

Mutable Elements

Field	Description
OAuthClientRedirectURIBaseline	Detect suspicious redirect URI mismatches in new clients.
TokenScopeSensitivity	Highlight credentials granting excessive read/write org-wide.
