Detection Strategy for Cloud Application Integration, Detection Strategy DET0539

Archived: 2026-04-05 12:38:59 UTC

AN1487

Detects suspicious OAuth application integrations within Office 365 or Google Workspace environments, such as new app registrations, unexpected consent grants, or privilege assignments. Defenders should correlate between application creation/modification events and associated user or service principal activity to identify persistence via app integrations.

Log Sources

Mutable Elements

Field	Description
PrivilegedUserList	Defines which accounts are authorized to consent or register applications; deviations indicate possible adversary persistence.
ApplicationScopeThreshold	Defines which OAuth scopes are considered risky (e.g., Mail.ReadWrite, Files.ReadWrite.All).

AN1488

Detects anomalous SaaS application integration activity across environments such as Slack, Salesforce, or other enterprise SaaS services. Focus is on unauthorized app additions, unusual permission grants, and persistence through service principal tokens.

Log Sources

Mutable Elements

Field	Description
AppWhitelist	Defines approved SaaS integrations for the enterprise; deviations indicate suspicious persistence.
ConsentDelegationPolicy	Threshold for which users can self-consent integrations; lowering this may reduce false positives.

Source: https://attack.mitre.org/detectionstrategies/DET0539#AN1487