Detection Strategy for Disable or Modify Cloud Logs, Detection Strategy DET0289

Archived: 2026-04-05 13:25:53 UTC

AN0801

Cloud API events where logging services are stopped, deleted, or modified in a way that disables audit visibility. Defender view: unauthorized StopLogging, DeleteTrail, or UpdateSink operations correlated with privileged user activity.

Log Sources

Mutable Elements

Field	Description
AdminRoles	Define which roles are authorized to stop or modify logging.
RegionScope	Adjust monitoring to ensure multi-region logging tampering is caught.

AN0802

Disabling or modifying sign-in or audit log collection for user activities. Defender view: policy or configuration updates removing logging coverage for critical accounts.

Log Sources

Mutable Elements

Field	Description
CriticalAccounts	Tune to prioritize logging changes that affect administrative or high-value accounts.

AN0803

Disabling mailbox or tenant-level audit logging, often using Set-MailboxAuditBypassAssociation or downgrading license tiers. Defender view: sudden absence of mailbox activity logging for monitored users.

Log Sources

Mutable Elements

Field	Description
UserScope	Tune alerts for users where mailbox auditing should always remain enabled.

AN0804

Disabling or altering security and audit logs in SaaS admin panels (e.g., Slack, Zoom, Salesforce). Defender view: API calls or admin console changes that stop event exports or logging integrations.

Log Sources

Mutable Elements

Field	Description
IntegrationScope	Define which SaaS log integrations are required and alert if removed.
