

Behavioral Detection of Malicious Cloud API Scripting, Detection Strategy DET0078

Archived: 2026-04-05 16:07:59 UTC

AN0215

Detects adversarial use of cloud APIs for command execution, resource control, or reconnaissance. Focuses on CLI/SDK/scripting language abuse via stolen credentials or in-browser Cloud Shells. Monitors for anomalous API calls chained with authentication context shifts (e.g., stolen token -> privileged action) and cross-service impacts.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Off-hours API usage or configuration changes are more suspicious outside business context.
UserAgent	Unexpected SDK usage (e.g., `boto3`, `azcopy`, unknown User-Agent strings).
CredentialType	High-risk if access token or API key used outside expected geographic/IP behavior.
APISequence	Unusual or rapid chaining of provisioning, IAM, and execution APIs.
ConsoleContext	Browser-based Cloud Shell vs local CLI may indicate insider vs external use case.

Source: <https://attack.mitre.org/detectionstrategies/DET0078>