Detection Strategy for Cloud Service Hijacking via SaaS Abuse, Detection Strategy DET0147

Archived: 2026-04-05 13:41:20 UTC

AN0417

Adversary gains access to cloud-hosted services such as AWS SES, SNS, or OpenAI API, enables or modifies usage policies, and initiates resource-intensive actions (e.g., mass email/SMS or LLM queries), often from unauthorized regions or under anomalous identity conditions.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Define threshold period over which request spikes are measured. E.g., 10 min or 1 hour windows.
UserContext	Alert only if role/user is outside expected automation identity list.
RequestVolumeThreshold	Customize the number of emails/SMS or API calls considered anomalous.
GeoVelocityThreshold	Tune geolocation jump logic (e.g., login from US, then use service in Asia within minutes).
ModelUsageQuotaSpike	Set maximum allowable deviation from past 7-day average OpenAI/GPT token usage.