Detection Strategy for Disable or Modify Cloud Firewall, Detection Strategy DET0424

Archived: 2026-04-05 17:11:51 UTC

AN1188

Creation, deletion, or modification of security groups and firewall rules in cloud control plane logs that expand access to cloud resources beyond expected baselines. Defender view: unexpected ingress/egress rules permitting 0.0.0.0/0 or opening atypical ports, often correlated with privileged role or API key activity.

Log Sources

Mutable Elements

Field	Description
AllowedIPRanges	Whitelist approved IP ranges; detect unexpected addition of 0.0.0.0/0 or untrusted CIDRs.
PortScope	Define expected ports for services; flag additions outside this range (e.g., SSH/RDP open to all).
RoleContext	Tune alerts based on whether changes are made by break-glass or admin roles versus automation accounts.
TimeWindow	Correlate rule changes with subsequent suspicious network activity to reduce false positives.