Modify Cloud Compute Infrastructure: Delete Cloud Instance, Sub-technique T1578.003 - Enterprise

Archived: 2026-04-05 16:29:29 UTC

DET0084 Detection Strategy for Modify Cloud Compute Infrastructure: Delete Cloud Instance AN0234

Defenders can detect suspicious cloud instance deletions by correlating events across authentication, instance lifecycle, and account activity. From a defender’s perspective, behaviors of interest include instances deleted shortly after creation, deletions initiated by new or rarely used accounts, deletions following snapshot creation, and deletions originating from anomalous geolocations or access keys. These may indicate adversarial attempts to destroy forensic evidence or evade detection.
