Detection Strategy for Cloud Administration Command, Detection Strategy DET0545

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

AN1502

Monitor for suspicious use of cloud-native administrative command services (e.g., AWS Systems Manager Run Command, Azure RunCommand, GCP OS Config) to execute code inside VMs. Detect anomalies such as commands/scripts executed by unexpected users, execution outside of maintenance windows, or commands initiated by service accounts not normally tied to administration. Correlate cloud control-plane activity logs with host-level execution (process creation, script execution) to validate if commands materialized inside the guest OS.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	AWS:CloudTrail	SendCommand, StartSession, ExecuteCommand: Unexpected AWS Systems Manager command execution targeting EC2 instances
Script Execution (DC0029)	azure:activity	Microsoft.Compute/virtualMachines/runCommand/action: Abnormal initiation of Azure RunCommand jobs or PowerShell/Bash payloads
Process Creation (DC0032)	azure:vmguest	Unexpected execution of cloud agent processes (e.g., WindowsAzureGuestAgent.exe, ssm-agent) followed by arbitrary script or binary execution

Mutable Elements

Field	Description
UserContext	Differentiate between known admin/service accounts and non-administrative users triggering RunCommand or SSM.
TimeWindow	Correlate cloud control-plane API calls with host-side execution events within a bounded timeframe (e.g., 5 minutes).
AllowedScripts	Whitelist approved scripts or automation invoked via RunCommand to reduce false positives.

Source: https://attack.mitre.org/detectionstrategies/DET0545