Detection Strategy for Hijack Execution Flow through Service Registry Premission Weakness., Detection Strategy DET0427

Archived: 2026-04-05 12:35:49 UTC

AN1195

Unauthorized modification of service-related registry keys such as ImagePath, FailureCommand, ServiceDll, or Performance/Parameters keys. Defender correlates registry modifications, anomalous service metadata changes, and subsequent service process executions that deviate from baseline configurations.

Log Sources

Mutable Elements

Field	Description
MonitoredServiceKeys	Registry subkeys for critical services (ImagePath, ServiceDll, FailureCommand, Parameters).
BaselineServiceConfig	Known good service registry configurations and paths for comparison.
TimeWindow	Correlation interval between registry/service modifications and service execution.
PrivilegedAccounts	Accounts permitted to modify service configurations.
