Behavioral Detection of Event Triggered Execution Across Platforms, Detection Strategy DET0010

Archived: 2026-04-05 17:21:06 UTC

AN0024

Correlates unexpected modifications to WMI event filters, scheduled task triggers, or registry autorun keys with subsequent execution of non-standard binaries by SYSTEM-level processes.

Log Sources

Mutable Elements

Field	Description
UserContext	Filters triggering on SYSTEM or LOCAL SERVICE vs. user-initiated triggers
TimeWindow	Correlates trigger definition and execution timing (e.g., within 5 minutes)
PathAnomalyThreshold	Process or binary path deviation scoring for execution anomalies

AN0025

Detects inotify or auditd configuration changes that monitor system files coupled with execution of script interpreters or binaries by cron or systemd timers.

Log Sources

Mutable Elements

Field	Description
ExecutablePathRegex	Regex defining suspicious binary/script paths triggered by cron/systemd
WatchTargetPaths	Paths monitored by auditd/inotify for suspicious event registration

AN0026

Correlates launchd plist modifications with subsequent unauthorized script execution or anomalous parent-child process trees involving user agents.

Log Sources

Mutable Elements

Field	Description
PlistNamePattern	Regex pattern matching known rogue or unrecognized launchd plist names
ParentProcessBaseline	Expected parent-child relationships during plist-triggered execution

AN0027

Monitors cloud function creation triggered by specific audit log events (e.g., IAM changes, object creation), followed by anomalous behavior from new service accounts.

Log Sources

Mutable Elements

Field	Description
TriggerEventType	Specific cloud event (e.g., PutObject, CreateRole) that causes function invocation
ServiceAccountRole	Expected permissions for roles used in function execution

AN0028

Correlates Power Automate or similar logic app workflows triggered by SaaS file uploads or email rules with data forwarding or anomalous access patterns.

Log Sources

Mutable Elements

Field	Description
TriggerCondition	Event types that initiate SaaS automation (e.g., file add, new email)
AppIdentityScope	Scopes/permissions granted to automation app accounts

AN0029

Detects macros or VBA triggers set to execute on document open or close events, often correlating with embedded payloads or C2 traffic shortly after execution.

Log Sources

Mutable Elements

Field	Description
MacroFunctionNames	Names of event-bound functions like Auto_Open that initiate execution
TimeDeltaMacroToC2	Time threshold to correlate macro execution with outbound connections

---