Detection Strategy for Serverless Execution (T1648), Detection Strategy DET0374

Archived: 2026-04-05 18:41:16 UTC

AN1053

Correlate creation or modification of serverless functions (e.g., AWS Lambda, GCP Cloud Functions, Azure Functions) with anomalous IAM role assignments or permissions escalation events. Detect subsequent executions of newly created functions that perform unexpected actions such as spawning outbound network connections, accessing sensitive resources, or creating additional credentials.

Log Sources

Mutable Elements

Field	Description
RoleScope	Which IAM roles or privileges are considered sensitive when applied to functions
AllowedFunctions	Known baseline list of approved serverless functions to reduce false positives
TimeWindow	Temporal threshold for correlating function creation with anomalous execution

AN1054

Monitor for creation of new Power Automate flows or equivalent automation scripts that trigger on user or file events. Detect anomalous actions performed by these automations, such as email forwarding, anonymous link creation, or unexpected API calls to external endpoints.

Log Sources

Mutable Elements

Field	Description
UserContext	Business units or users where automation creation is expected (developers, admins)
FlowActions	Specific automation actions (email forwarding, file sharing) that should be considered suspicious

AN1055

Track creation or update of SaaS automation scripts (e.g., Google Workspace Apps Script). Detect when these scripts are bound to user events such as file opens or account modifications, and correlate with subsequent abnormal API calls that exfiltrate or modify user data.

Log Sources

Mutable Elements

Field	Description
ScriptScope	Which SaaS apps or APIs can be legitimately automated in the environment
TriggerTypes	Event-driven triggers (e.g., on file open, on user creation) considered suspicious

---