Behavior-chain detection for T1134 Access Token Manipulation on Windows, Detection Strategy DET0283

Archived: 2026-04-05 14:50:49 UTC

Analytics

- Windows

AN0786

Detection of suspicious token manipulation chains: use of token-related APIs (e.g., LogonUser, DuplicateTokenEx) or commands (runas) → spawning of a new process under a different security context (e.g., SYSTEM) → mismatched parent-child process lineage or anomalies in Event Tracing for Windows (ETW) token/PPID data → abnormal lateral or privilege escalation activity.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation time between suspicious API usage, runas, and process creation (e.g., 5–10m).
AllowedServiceAccounts	Whitelist of service accounts permitted to spawn SYSTEM-level processes.
KnownAdminTools	Legitimate administrative utilities that trigger token changes.
ParentProcessAnomalyThreshold	Deviation threshold for PPID mismatches detected via ETW.
