Behavioral Detection Strategy for WMI Execution Abuse on Windows, Detection Strategy DET0364

Archived: 2026-04-05 18:35:37 UTC

AN1031

Detects adversarial abuse of WMI to execute local or remote commands via WMIC, PowerShell, or COM API through a multi-event chain: process creation, command execution, and corresponding network connection if remote.

Log Sources

Mutable Elements

Field	Description
WMIQueryScope	Restrict detection scope to suspicious WMI namespaces like `\root\cimv2`, `\root\subscription`.
TimeWindow	Set maximum allowable time window to correlate WMI process creation and remote connections.
UserContext	Tune based on interactive vs. system-level execution (e.g., via SYSTEM or low-privileged users).
RemoteDestinationThreshold	Number of unique remote hosts contacted using WMI within a time window.
SuspiciousCommandPatterns	Regex patterns to identify adversary-like usage (e.g., `wmic process call`, `powershell Invoke-WmiMethod`).
