Detection Strategy for File/Path Exclusions, Detection Strategy DET0051

Archived: 2026-04-05 17:36:28 UTC

AN0139

Creation or modification of files in directories known to be excluded from AV scanning (e.g., C:\Windows\Temp, Exchange server directories, or default AV exclusions). Defender perspective: correlate file creation with execution behavior or anomalous parent processes writing to excluded paths.

Log Sources

Mutable Elements

Field	Description
ExcludedPaths	List of directories excluded from scanning in the environment (customizable per organization).
ProcessAllowlist	Legitimate processes typically writing to excluded paths to minimize false positives.

AN0140

Adversaries writing or moving payloads into directories configured as AV/EDR exclusion paths (e.g., /tmp, /var/lib, or custom directories from auditd exclusion rules). Defender perspective: detect file creation in paths matching known exclusions correlated with unusual parent processes.

Log Sources

Mutable Elements

Field	Description
ExcludedDirectories	System- or security-tool-configured exclusion directories where files should rarely change.
CorrelationWindow	Time window to correlate file creation in excluded paths with execution or network activity.

AN0141

Suspicious file creation or modification in directories ignored by XProtect or AV exclusions (e.g., ~/Library, temporary cache directories). Defender perspective: monitor file events in ignored paths with correlation to execution or persistence activity.

Log Sources

Mutable Elements

Field	Description
AVExclusionPaths	Paths ignored by AV/XProtect that should be monitored for abnormal writes.
ProcessContext	Expected user or application context writing to excluded directories.
