Detection Strategy for Data Manipulation, Detection Strategy DET0059

Archived: 2026-04-05 16:35:52 UTC

AN0162

Correlate unauthorized or anomalous file modifications, deletions, or metadata changes with suspicious process execution or API calls. Detect abnormal changes to structured data (e.g., database files, logs, financial records) outside expected business process activity.

Log Sources

Mutable Elements

Field	Description
MonitoredFilePaths	List of critical data directories or files; environment-specific tuning required.
TimeWindow	Threshold for correlating process execution with rapid data changes.
AuthorizedProcesses	Expected processes permitted to modify business-critical data.

AN0163

Detect unauthorized manipulation of log files, database entries, or system configuration files through auditd and syslog. Correlate shell commands that alter HISTFILE or data-related processes with abnormal file access patterns.

Log Sources

Mutable Elements

Field	Description
WatchedDirectories	Specific log or data directories critical to integrity; tune per organization.
CommandExclusions	Legitimate scripts/tools excluded from data manipulation monitoring.

AN0164

Detect manipulation of system or application files in `/Library`, `/System`, or user data directories using FSEvents and Unified Logs. Identify anomalous process execution modifying plist files, structured data, or logs

outside expected update cycles.

Log Sources

Data Component	Name	Channel
File Modification (DC0061)	macos:unifiedlog	Anomalous plist modifications or sensitive file overwrites by non-standard processes
OS API Execution (DC0021)	macos:osquery	open, execve: Unexpected processes accessing or modifying critical files

Mutable Elements

Field	Description
AllowedPlistEditors	Whitelisted processes authorized to modify plist or configuration files.
FileIntegrityBaseline	Baseline hash values for key files to support integrity validation.
