# Behavioral Detection of Malicious File Deletion, Detection Strategy DET0140

Archived: 2026-04-05 12:47:46 UTC

### AN0392

Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| TimeWindow | Defines correlation window after suspicious binary execution or login session. |
| FilePathPattern | Focuses on deletion of temp files, malware staging dirs, or known indicators. |
| UserContext | Privilege level or impersonated user deleting sensitive files. |

### AN0393

Detects deletion of suspicious files (e.g., payloads, temp exes, scripts) via `rm`, `unlink`, or secure deletion tools like `shred`, especially when performed by unexpected users or shortly after execution.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| PathRegex | Pattern matching known attacker staging directories or hidden file paths. |
| TimeWindow | Deletion shortly after process execution or privilege escalation. |
| SecureDeletionTool | Uncommon presence or use of `shred`, `wipe`, or `srm`. |

### AN0394

Detects removal of adversary artifacts via `rm`, `unlink`, or secure tools, with focus on shell sessions, temp files, and modified LaunchAgents or system directories.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| FilePathRegex | Focus on LaunchAgents, /tmp/, or user folders. |
| ToolUsageAnomaly | Detecting use of unfamiliar tools by common users. |

### AN0395

Detects manual or scripted removal of logs, artifacts, or malware droppings via `rm` or PowerCLI in ESXi shell. Focus on deletions from /tmp/, /var/core/, or /scratch.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| LogFilePath | Match deletion actions in system-critical locations or malware drop zones. |
| TimeWindow | Typically follows suspicious admin login or unexpected shell session. |

---