

# Behavioral Detection of Indicator Removal Across Platforms, Detection Strategy DET0184

Archived: 2026-04-05 13:23:28 UTC

## AN0520

Monitors sequences involving deletion/modification of logs, registry keys, scheduled tasks, or prefetch files following suspicious process activity or elevated access escalation.

### Log Sources

### Mutable Elements

Field	Description
TimeWindow	Correlate indicator removal within X mins after persistence/setup activities
TargetFilePathPattern	Customize detection to log file paths or common registry hives

## AN0521

Detects deletion or overwriting of bash history, syslog, audit logs, and .ssh metadata following privilege elevation or suspicious process spawning.

### Log Sources

### Mutable Elements

Field	Description
MonitoredPaths	Adjust based on syslog/auditd file paths (/var/log/messages, /var/log/audit/audit.log)
UserContext	Scope to root/sudo usage or anomalous user behavior

## AN0522

Detects clearing of unified logs, deletion of plist files tied to persistence, and manipulation of Terminal history after initial execution.

### Log Sources

### Mutable Elements

Field	Description
PlistTargetPaths	Define which plist paths relate to LaunchAgents or LaunchDaemons
ExecutionChainDepth	Allow tuning for multi-process persistence chains

**AN0523**

Monitors tampering with audit logs, volumes, or mounted storage often used for side-channel logging (e.g., /var/log inside containers) post-compromise.

**Log Sources****Mutable Elements**

Field	Description
LogMountPaths	Tune based on how logs are exported (bind-mount, overlay)
ContainerLabelScope	Limit detection to suspicious containers or runtime classes

**AN0524**

Tracks suspicious use of ESXi shell commands or PowerCLI to delete logs, rotate system files, or tamper with hostd/vpxa history.

**Log Sources****Mutable Elements**

Field	Description
LogSourceType	Tune per vCenter, vSphere, ESXi CLI telemetry collection
LogPathPattern	Target specific high-value log paths (e.g., /var/log/hostd.log)

**AN0525**

Detects deletion or hiding of security-related mail rules, audit mailboxes, or calendar/log sync artifacts indicative of tampering post-intrusion.

**Log Sources****Mutable Elements**

<b>Field</b>	<b>Description</b>
TargetMailboxScope	Limit by VIP mailboxes or external-facing users
AuditLogDepth	Tune for log deletion following lateral movement

---

Source: <https://attack.mitre.org/detectionstrategies/DET0184#AN0521>