Agent harness logging: what to record per action

RUN RECORD run-2026-09-02-0417 parent run: none
Started / ended: 2026-09-02 14:05:12 UTC / 14:09:47 UTC
Agent identity: svc-triage-agent, credentials "art-triage-rw" (write scope: system.yaml on art-prod-02 only) and "art-ops-restart" (restart of the Access service on art-prod-02 only)
Versions: harness triage-agent 0.4.2, prompt v11, model example-model-2026-08 (ID string as returned by the API)
Trigger: finding FND-3187, CVE-2026-82329, on art-prod-02.example.internal
Data read: inventory row; JFrog advisory table (fetched 2 Sep 2026 14:05); proxy log window 28 Aug to 2 Sep
Tool calls in order:
1. get_version(art-prod-02) -> 7.133.20 (affected, below 7.133.29)
2. read_proxy_log(art-prod-02, window) -> 0 POSTs to /access/api/v1/registry/join returning 201
3. edit_system_yaml(art-prod-02, add shared.security.additionalJoinKeys) [approval required; art-triage-rw]
4. restart_access_service(art-prod-02) [approval required; art-ops-restart]
Approval: requested 14:06:30; approver m.rivera; decision approve; 14:07:18; scope "workaround only, no token revocation"
Proposed change: diff of system.yaml (key value redacted; SHA-256 fingerprint of the new key 9f2c...e1a7)
Outcome read back: system.yaml hash before 4d1b...90c2, after a7e3...55f0; additionalJoinKeys present: yes;
Access service state after restart: running; get_version still 7.133.20 (patch not applied)
Not done, handed over: token revocation and join-key rotation (tokens issued since 28 Aug 2026), to owner platform-team, ticket SEC-2210
Human edits: approver changed ticket text "patched" to "workaround applied, patch pending"
Tokens used / cost: 41,200 / USD 0.31
Previous record hash: c0b8...3d19 This record hash: 5e47...a2b6

Agentic AI in Cybersecurity, Agent harness logging: what to record per action, edition 19 Nov 2026, https://agenticaiincybersecurity.com/agent-harness/logging-and-evidence/. License CC BY 4.0.