AI agent audit trail for a security agent

Illustrative entry, one change, values invented for the format:

{
 "run_id": "run-20261112-0417",
 "started": "2026-11-12T09:14:03Z", "ended": "2026-11-12T09:21:48Z",
 "agent": "dep-fix-agent", "agent_version": "1.8.2",
 "model": "claude-sonnet-5-5", "prompt_version": "p-2026-11-01",
 "trigger": {"source": "ticket SEC-4821", "received": "2026-11-12T09:14:00Z", "input_hash": "sha256:9f2c..."},
 "input": {"finding": "examplelib 2.4.1 in service payments-api", "fixed_in": "2.4.7"},
 "steps": [
  {"n": 1, "t": "09:14:11", "decision": "read manifest before proposing a version", "reason": "fixed_in is 2.4.7; manifest pins 2.4.x"},
  {"n": 2, "t": "09:14:12", "tool": "repo.read_file", "params": {"path": "requirements.txt"}, "result": "ok, 41 lines", "identity": "svc-depfix-agent"},
  {"n": 3, "t": "09:15:20", "tool": "web.fetch_url", "params": {"url": "https://example.org/examplelib/releases/2.4.7"}, "result": "ok, 1 page, no API change listed", "identity": "svc-depfix-agent"},
  {"n": 4, "t": "09:16:40", "decision": "bump to 2.4.7; no API change in release notes", "reason": "same minor version"},
  {"n": 5, "t": "09:17:02", "tool": "repo.open_pull_request", "params": {"branch": "depfix/SEC-4821", "files": 1}, "result": "PR 1932 opened", "identity": "svc-depfix-agent"},
  {"n": 6, "t": "09:18:30", "tool": "ci.read_status", "params": {"pr": 1932}, "result": "tests passed, run 77310", "identity": "svc-depfix-agent"},
  {"n": 7, "t": "09:19:05", "tool": "repo.merge_pull_request", "params": {"pr": 1932}, "result": "BLOCKED: approval required", "identity": "svc-depfix-agent"},
  {"n": 8, "t": "09:21:30", "tool": "repo.merge_pull_request", "params": {"pr": 1932}, "result": "merged, commit c41e9b0", "identity": "svc-depfix-agent"}
 ],
 "data_read": ["requirements.txt (step 2)", "release notes for examplelib 2.4.7 (step 3)"],
 "approval": {"required_by": "tool rating: write, reversible", "approver": "owner-payments", "decision": "approved", "t": "09:21:10"},
 "agent_claim": "PR 1932 merged, examplelib 2.4.7 in payments-api",
 "downstream_refs": {"git_merge_commit": "c41e9b0", "ci_run": 77310},
 "independent_check": {"run_id": "verify-20261112-1000", "t": "2026-11-12T10:00:12Z", "identity": "svc-verify-job", "queried": "git ref main; resolved lockfile of payments-api", "result": "match: c41e9b0 is on main; examplelib 2.4.7 resolved"}
}

Agentic AI in Cybersecurity, AI agent audit trail for a security agent, edition 19 Nov 2026, https://agenticaiincybersecurity.com/evaluation-checklist/evidence-and-audit-trail/. License CC BY 4.0.