Agent harness memory and context


```
{
 "cve": "CVE-2026-9198",
 "host": "lf-prod-1",
 "created": "2026-08-04",
 "due": "2026-08-07",
 "checks": [
  {"id": "version", "condition": "Langflow OSS 1.0.0 through 1.10.0",
   "method": "pip show langflow", "status": "pending", "evidence": ""},
  {"id": "auto_login", "condition": "LANGFLOW_AUTO_LOGIN is true; unset on 1.10.0 or earlier counts
as enabled",
   "method": "read the effective environment and the --env-file", "status": "pending", "evidence": ""},
  {"id": "reachable", "condition": "listening address reachable from an untrusted network",
   "method": "ss -ltnp, then firewall and security group rules", "status": "pending", "evidence": ""},
  {"id": "no_auth_proxy", "condition": "no authenticating reverse proxy in front",
   "method": "read the reverse proxy configuration", "status": "pending", "evidence": ""}
 ],
 "decision": {"outcome": "", "decided_by": "", "decided_at": ""}
}
```


Agentic AI in Cybersecurity, Agent harness memory and context, edition 19 Nov 2026, https://agenticaiincybersecurity.com/agent-harness/context-and-memory/. License CC BY 4.0.