AI agent guardrails for a security team

```text
2026-10-28T09:14:07Z run=r-0412 svc=billing-api tool=edit_branch decision=allow limit=scope path=package.json cycle=2 calls=11 approval=FS-111497-01
2026-10-28T09:16:51Z run=r-0412 svc=billing-api tool=edit_branch decision=deny limit=scope path=.github/workflows/ci.yml action=halt notify=release-owner
2026-10-28T09:30:02Z run=r-0413 started_by=release-owner svc=orders-api tool=none
2026-10-28T09:31:20Z run=r-0413 svc=orders-api tool=none decision=handover limit=stop reason=node-20.x-no-fix
```

Agentic AI in Cybersecurity, AI agent guardrails for a security team, edition 19 Nov 2026, https://agenticaiincybersecurity.com/guides/ai-agent-guardrails/. License CC BY 4.0.