agent-policy.yaml, patch-response agent, version 2026-10-28.1

```yaml
tools:
  edit_branch:
    scope:    repos in the inventory; branches agent/cve-2026-111497-*; no paths under .github/ or
deploy/
    identity:  repo-token-agent-branches (no merge right, no protected branches)
    approval:  fact sheet confirmed, approval ID required on every call
    stop:     max_edit_test_cycles 3 per service; max_tool_calls 25 per service
  merge_pull_request: withheld
  deploy_or_restart:  withheld
run_limits:
  max_services_per_run: 40
  max_agent_prs_per_hour: 5
  on_stop: halt the run, notify the release owner
```

Agentic AI in Cybersecurity, agent-policy.yaml, patch-response agent, version 2026-10-28.1, edition 19 Nov 2026, https://agenticaiincybersecurity.com/guides/ai-agent-guardrails/. License CC BY 4.0.