Measuring a security agent after it ships

AGENT REVIEW RECORD
Agent and version: ____ (model, prompt, tool list versions)
Review date: ____ Window: ____ to ____ Reviewer: ____
Proposals reviewed: ____ Accepted: ____ Reverted: ____ Review minutes: ____
Runs: ____ Escalations: ____ Threads: ____ Blocked: ____
Model spend: ____ Tasks completed: ____
Six metrics vs baseline: ____
Thresholds crossed: ____
Sample drawn (n and method): ____ Wrong items found: ____
Decision: continue / pause widening / rerun evals / roll back / switch route
Owner of the action and date due: ____
Change in model, prompt or tools since last review: ____ (counts as a new version)

Agentic AI in Cybersecurity, Measuring a security agent after it ships, edition 19 Nov 2026, https://agenticaiincybersecurity.com/guides/measuring-an-agent-after-it-ships/. License CC BY 4.0.