AI agent autonomy levels for security work

LEVEL CHANGE RECORD
Action: ____ (one of the rated actions; merge is never promoted to L5)
Change: L4 to L5 / L5 to L4 / L4 to L1 or L2
Date: ____ Decided by (name) and stand-in: ____
For a promotion:
 Window: ____ to ____ (at least 14 days)
 Proposals approved without edits in a row: ____ (example value: 50)
 Sample reviewed: ____ (example value: 10) Wrong calls: ____ (must be 0)
 NCSC ratings now: potency __ scope __ criticality __ rollout __ recoverability __ total __ (0 to 8)
 Model, prompt and tool versions the evidence was gathered on: ____
 Sample cadence after promotion: ____ Who can set it back to L4: ____
For a demotion:
 Trigger (model/prompt/tool change, false clear, new data source, revert-rate rise): ____
 Actions taken since the last clean sample: ____ Reviewed by: ____ Wrong items: ____
 Rerun passed on: ____ Level restored on: ____

Agentic AI in Cybersecurity, AI agent autonomy levels for security work, edition 19 Nov 2026, https://agenticaiincybersecurity.com/guides/autonomy-levels/. License CC BY 4.0.