AI agents for response to a new disclosure

Agent disclosure record

[ ] Advisory ID, and the time the agent first read it
[ ] Inventory snapshot used (SBOM or asset data), and its date
[ ] Per asset: affected, not affected, or could not verify, with the evidence
[ ] Method used to verify (for example a read-only check through EDR)
[ ] Proposed stopgap, and who must approve it
[ ] Time of approval, approver, and time the stopgap went live
[ ] Time and method of the rollback, if any

Agentic AI in Cybersecurity, AI agents for response to a new disclosure, edition 19 Nov 2026, https://agenticaiincybersecurity.com/use-cases/new-disclosure-response/. License CC BY 4.0.