Tools and permissions in an agent harness for security work

Tool register row (copy one per tool)

Tool name:
System it touches:
Operations (read / comment / ticket / configure / block / delete):
Identity used and its permission on that system:
Issued by, issued on, expires on:
Where the credential lives (never in the sandbox):
Reversible? (yes / no / how):
Approval rule (none / always / by argument, with the argument test written out):
Where the limit is enforced (downstream system, harness rule or hook):
Owner, and next review date:

Agentic AI in Cybersecurity, Tools and permissions in an agent harness for security work, edition 19 Nov 2026, https://agenticaiincybersecurity.com/agent-harness/tools-and-permissions/. License CC BY 4.0.