Where a security agent must stop and ask a person

APPROVAL MAP for <agent name>, version <date>
Owner: <role> Deputy: <role> Reviewed: <date>, next review <date>

Action class	Tool	Risk (low/medium/high)	State (unattended / approve first / never)	Approver role	If nobody answers in <hours>	Evidence shown with the proposal
Read a finding	read_finding	Low	Unattended	none	n/a	n/a
Comment on a ticket	add_ticket_comment	Low	Unattended, logged	none	n/a	n/a
Open a pull request	open_pull_request	Medium	Approve first (merge)	Code owner of the repository	Reject	Diff, test result, rescan result
Change a cloud setting	apply_config_change	High	Approve first, before each call	Cloud platform on-call	Reject	Current value, new value, prior-state copy, owner of the asset
Delete a remote branch or a resource	delete_resource	High	Never	n/a	n/a	n/a

Rules: the state is stored in the harness configuration and enforced there. A tool missing from this table is not callable. Changing a state needs a ticket signed by <role>.

Agentic AI in Cybersecurity, Where a security agent must stop and ask a person, edition 19 Nov 2026, https://agenticaiincybersecurity.com/evaluation-checklist/human-approval-points/. License CC BY 4.0.