Agency Level	Agentic Capabilities	Example	Why It Fits This Level
AG-1	Single LLM call; no tools; no memory; no actions beyond reasoning	Convert threat modeling session notes into a polished summary	One-shot reasoning with no retained state, external access, or ability to act
AG-2	Single-step execution; read-only tools (optional); memory (optional); negligible or low-impact actions	Employee-facing chatbot answering questions using internal documentation	Limited reasoning with optional context and read-only access, producing low-impact outcomes
AG-3	Multi-step reasoning; read-only tools; low-impact write tools (optional); memory; mostly human-approved actions	Generate security metrics and propose remediation steps	Agent reasons across steps and may prepare changes, but execution is largely human-controlled
AG-4	Multi-step reasoning; memory; read/write tools; mostly autonomous actions	Execute approved configuration or access changes within defined boundaries	Agent can perform meaningful actions independently, with humans overseeing higher-impact decisions
AG-5	Multi-step reasoning; memory; read/write tools; unbound actions; event-driven initiation; full autonomy	Fully autonomous agent managing firewall rules based on telemetry	Agent initiates decisions and actions without human involvement across systems