

MCP Access Audit

Five business days, fixed price, read-only. One agreed workflow where AI agents or MCP tools reach your systems.

THE QUESTION IT ANSWERS

When an AI agent acts inside your systems, what does each credential it holds actually authorise, and could you prove afterwards what it did? This review documents what the available evidence supports for one workflow you choose. It is a look, not an accusation: it does not assume your current controls are deficient.

WHAT YOU GET

- Permission map for the agreed workflow: what each credential authorises, at server, tool and parameter level.
- Observed risks and limitations, stated against your existing configuration.
- Prioritized RBAC and audit-trail actions.
- One-page executive summary plus permission-map/evidence appendix, then a 30-minute walkthrough.

FIVE BUSINESS DAYS

Day 1 - Confirm the agreed scope and evidence inventory; start the review.

Days 2-3 - Map identities, tokens and scopes; trace what the workflow can reach and what gets logged.

Day 4 - Write up risks, limitations and prioritized actions.

Day 5 - Summary and evidence appendix delivered; 30-minute walkthrough.

Before the clock starts, agree the workflow, environment, inventory limits, evidence sample and read-only access. Expanded scope needs a revised quote.

WHAT WE NEED FROM YOU

- A named workflow owner and engineer for scoping, walkthrough and short questions.
- Read-only configuration and permission evidence, plus relevant redacted logs. Use exports or screen-share where direct access is inappropriate; do not send live secrets.
- An agreed workflow description and any available architecture or policy records; missing evidence is recorded as a limitation.

HOW YOUR DATA IS HANDLED

- Agree permitted evidence access and handling before work. Redact customer records and secrets from exports; retain only the agreed review evidence.
- Agree report recipients, confidentiality and retention terms before sharing evidence.

OUT OF SCOPE

- Remediation work. Implementation is a separate engagement, from \$5,000.
- Penetration testing, exploit development, or vendor selection.
- Runtime assurance, certification, continuous monitoring or incident response.
- Anything outside the agreed workflow, environment and inventory limits.