DEMONIC BINARY

SERVICE BRIEF

AI AGENTS / AUTOMATION

AI Agent Development & Security

Useful automation. Accountable actions.

Integrate tool-using agents with APIs, permission controls and evaluations.



WHAT WE DO

- AI agents and API integrations
- Prompt-injection and abuse testing
- Human review and approval workflows
- MCP and tool orchestration
- User-scoped authorization policies
- Evaluations, audit logs and observability

HOW WE WORK

- Define a bounded business task
- Connect tools behind authenticated policies
- Test unsafe actions and failure modes
- Deploy with review and monitoring

YOUR DELIVERABLES

- Agent workflows and tool adapters
- Permission and approval matrix
- Negative-path evaluation suite
- Operational handoff and telemetry plan

THE OUTCOME

Ship AI workflows with real safeguards at the API and business-action boundary.

LET'S GET STARTED

info@demonicbinary.com

demonicbinary.com/flagship/ai-agent-development