

Markus Walker

AI Engineer, End to End | Secure AI | Forward Deployed Engineering

Brisbane, Queensland, Australia | markus@markuswalker.com
markuswalker.com | linkedin.com/in/markus-walker-au | github.com/Markus-Doc
Australian citizen | Eligible for NV1 and NV2 | Remote preferred

Summary

AI engineer who scopes, designs, builds and deploys AI solutions end to end: agents, the knowledge they work from and the controls around them. Thirteen years across cybersecurity, IT infrastructure and operational technology (OT), including seven running IT and OT for remote gas operations and the last two in AI engineering and Secure AI. Recent work spans sovereign Azure AI environments for enterprise clients, an agent-run knowledge base of AI agent security controls covering 151 platforms, and a cloud-run governed AI agent with 208 passing automated tests. Builds so the model can be swapped, using open knowledge formats, the Model Context Protocol (MCP) and agent instructions any assistant can read.

Skills

AI engineering: Large language models (LLMs), AI agents, multi-agent systems, agentic workflows, retrieval-augmented generation (RAG), prompt engineering, LLM evaluation, model routing, MCP servers, custom plugins, n8n, LiteLLM.

AI platforms: Claude and Claude Code, OpenAI Codex, ChatGPT, Azure AI Foundry, Azure OpenAI, Amazon Bedrock, Bedrock AgentCore, Ollama.

Secure AI: AI threat modelling, prompt injection testing, MCP governance, agent least privilege, AI supply-chain review, secure SDLC, AI governance, identity and access management (IAM), incident response planning. OWASP Top 10 for LLM Applications, MITRE ATLAS, NIST AI RMF, ISO/IEC 42001.

Knowledge engineering: Open Knowledge Format (OKF), knowledge graphs and ontologies, Neo4j, vector embeddings and semantic retrieval, source provenance, citation validation.

Software and cloud: Python (FastAPI, Pydantic, pytest), TypeScript, React, Playwright, PowerShell, Docker, GitHub Actions CI/CD, Microsoft Azure, AWS, Cloudflare Workers, Oracle Cloud Infrastructure, Entra ID, Intune.

Experience

Security Transformation Specialist | Accenture | Sep 2026 to Oct 2026

Equivalent Secure AI role following Accenture's acquisition of CyberCX, with a greater share of the work as a forward deployed engineer.

Senior Engineer, Secure AI | CyberCX | Jun 2026 to Sep 2026

- Delivered secure AI solutions for enterprise clients end to end, from use-case assessment and solution architecture through build, security controls and handover.
- Deployed sovereign AI environments on Azure: virtual machines built from golden images, Azure AI Foundry with Azure OpenAI models hosted in an Australian region, and device management and access controls restricting each machine to approved models.
- Presented client workshops on frontier AI and security, including the Claude Mythos briefing, and advised on MCP governance, secure SDLC and enterprise AI adoption.
- Built custom AI plugins and agentic workflows, distributed as versioned releases through a GitHub Enterprise marketplace.
- Built knowledge bases for people and AI agents, and AI-assisted document generation workflows with reusable skills, agents and review steps.
- Wrote AI security guidance for enterprise teams and a white paper on telling AI-driven attacks apart in the security operations centre (SOC).

Independent Practitioner and Professional Development | 2025 to 2026

- Contract work for clients alongside the Certificate IV in Cyber Security, the AWS Solutions Architect certification and three Oracle Cloud certifications, with portfolio projects in AWS security architecture and incident response, and Splunk and Active Directory security labs.

IT Field Engineer | Tata Consultancy Services | May 2019 to Aug 2025

Embedded contractor running IT and OT for Shell QGC and QCLNG upstream and midstream operations in Queensland, on assets he had helped build and commission in earlier site roles.

- IT field engineering across more than 20 remote sites, including camps, plants and drilling environments, covering planned work, escalations and after-hours support.
- Kept Microsoft 365, networking and telecom platforms running for control-room operations and service continuity.
- Network transformation across the operations area, including more than 300 Cisco to Aruba access point replacements, and Starlink connectivity for remote operations from project development through deployment.
- Administered Entra ID identity and access management, including role-based access and device compliance, and supported the move from SCCM to Intune, Windows Autopilot and Azure AD Join.

Junior Network Engineer | Data#3 | Jan 2019 to May 2019

Field engineering and cutover coordination for the Shell QGC Enterprise Network Transformation project.

Earlier Roles | 2005 to 2019

QGC site roles with MSS, ECM and Protech (2012 to 2019) on gas plant projects, from laying the copper earth grid through construction and commissioning to handover. Lighting and sound engineering with Airco Audio, USA (2005 to 2012), running networked control systems for live production.

Projects

Offerings Atlas and Ask the Atlas | Oct 2026 | markuswalker.com/atlas

- Agent-run knowledge base of AI agent security controls: 151 platforms and tools against 44 controls, 6,644 researched findings backed by 3,655 sources. Researcher, evaluator, freshness and curator agents work under narrow permissions, and the evaluator confirms every quoted passage against a hash-stored source page. 160 automated tests.
- An enterprise questionnaire answers client concerns from it with every citation checked. Ask the Atlas runs a public sample live.

Governed AI Agent | Sep 2026 | github.com/Markus-Doc/governed-ai-agent

- Cloud-run agent that draws its knowledge from an open knowledge base, on Cloudflare Workers, Cloudflare Access and GitHub Actions. Headless Claude Code with a tool allowlist, policy as code, human holds, prompt-injection controls, encryption at rest and a tiered model cascade.
- Logged 8,782 deterministic decisions at zero model cost in its first nine days, with all 208 automated tests passing.

Local LLM Gateway | Oct 2026 | github.com/Markus-Doc/headless-llm-gateway

- One OpenAI-compatible endpoint that routes agent calls to headless Claude Code, Codex or an API model, with JSON Schema output and a proof record per call. Loopback only, hash-pinned dependencies.

RESYNTH and MCP Tooling | Jun 2026 to Oct 2026 | github.com/Markus-Doc/resynth

- RESYNTH consolidates several AI deep-research reports into one verified document through five gated stages, with every claim traced to a verbatim source excerpt. Also built an MCP configuration security auditor with SARIF output and an AI governance proof of concept in n8n.

Writing | 2026 | markuswalker.com

- Human, script or AI? Spotting AI-driven attacks in the SOC (white paper, v5). Securing Claude Cowork: controls, gaps and safer defaults (v1.4).

Certifications

- Anthropic: Claude Certified Associate, Foundations (2026)
- Amazon Web Services: AWS Certified Solutions Architect, Associate (2025)
- Oracle: three Oracle Cloud Infrastructure 2025 certifications, including Generative AI Professional and Architect Associate (2025)

Education

- Certificate IV in Cyber Security (22603VIC), TAFE Queensland, Mar 2026
- University studies in audio engineering, St. Louis, USA