CHRIS McNABB

Application Security Architect | AI & LLM Security | GWAPT
Easley, SC (Remote) | chrismcnabbjob@gmail.com | linkedin.com/in/chrismcnabb

SUMMARY

Application Security Architect with 25+ years across enterprise software engineering and application security, including a decade architecting and running the AppSec program that protected 250+ enterprise applications at a national insurance provider. GWAPT-certified web application penetration tester who designs, automates, and scales security across the full SDLC: DAST, SAST, SCA, threat modeling, and vulnerability management. Built automation that compressed a multi-day vulnerability-scanning workflow to under three hours, and drove triage and remediation of thousands of findings annually. Hands-on engineer (Python, C#/.NET, SQL) with 2+ years building AI-driven automation and multi-agent systems, extending deep AppSec expertise into the security of AI and agentic systems.

CORE COMPETENCIES

Application Security: Web application penetration testing, DAST, SAST, SCA, threat modeling, vulnerability management, secure SDLC, secure code review, SOAR (Swimlane, Cortex XSOAR).

Security Tooling: Burp Suite Professional (including custom extension development), HCL AppScan Enterprise, HCL AppScan Source, SonarQube, Traceable/Harness (API security), ServiceNow integration.

AI Security & Automation: LLM and agentic-system security, multi-agent pipelines (LangGraph, CrewAI), Claude (Anthropic), Gemini (Google), GPT (OpenAI), Claude Code, Claude Cowork, GitHub Copilot, MCP, workflow automation (n8n, Make.com), RAG.

Languages & Frameworks: Python, C#/.NET, Ruby on Rails, Node.js, JavaScript, SQL.

Cloud & Platform: AWS, Azure, Cloudflare, Supabase, FastAPI, GitHub Actions, Git, VS Code.

PROFESSIONAL EXPERIENCE

American Fidelity — Oklahoma City, OK (Remote)
Software Security Architect | 2016 – July 2026

- 250+ enterprise web applications and APIs secured across the full software development lifecycle as one of two AppSec practitioners, owning program strategy, tooling, and prioritization for the entire portfolio.
- Reduced a multi-day manual DAST workflow to under three hours by engineering a fully automated scan-management system integrated with the ServiceNow ticket lifecycle.
- Thousands of vulnerabilities triaged and remediated annually in partnership with development teams, embedding security directly into delivery.
- 150+ developers trained through a Secure Coding curriculum I owned and delivered, raising secure-development practice across engineering teams.
- Authored and reviewed enterprise cybersecurity standards and policies supporting PCI DSS, HIPAA, and SOC 2, embedding regulatory obligations into the secure SDLC.
- Executed hands-on web application penetration testing with Burp Suite Professional, developing custom extensions to extend testing coverage beyond out-of-the-box capability.
- Integrated enterprise AppSec tooling (HCL AppScan Enterprise, AppScan Source, SonarQube, Traceable) and SOAR platforms (Swimlane, Cortex XSOAR) into automated scanning and remediation pipelines.
- Championed AI-assisted development (GitHub Copilot) to build internal security and automation tooling, accelerating AppSec delivery and cutting manual effort.

Onlife Health — Franklin, TN (Remote)
Senior Software Consultant, part-time contract | 2014 – 2017

- 500,000+ members served by a custom, HIPAA-compliant health and wellness platform designed and built end to end.

CIC, Inc. — Cleveland, TN (Remote)
Consultant, Senior Software Developer & Architect, part-time contract | 2014 – 2017

- Delivered full-stack custom software for consulting clients using C#/.NET and SQL Server.

Earlier Software Engineering Experience | 2000 – 2014

- Senior Developer, Team Lead, and Architect roles at Firma8, Cloudswell, Ticketsoft, GHN Online, and Intervoice, Inc., spanning open-source translation systems, cloud services, enterprise point-of-sale, healthcare claims processing, and telecommunications/IVR platforms.

SELECTED PROJECTS

- **MCP Intake & Risk Gate** — Designed a security intake and risk-scoring framework for Model Context Protocol servers, applying threat modeling and secure-SDLC gating to agentic tool integrations before they reach production.
- **Bastros** — Built a full-stack DAST orchestration console demonstrating stateful multi-agent workflow patterns in LangGraph, including checkpointing, human-in-the-loop interrupt and resume, and fan-out/fan-in scan coordination.
- **Chief of Staff Dashboard** — Engineered a production LangGraph and FastAPI backend with a React front end, implementing Google OAuth 2.0 with PKCE and multiple coordinated agent graphs.

AI & AUTOMATION

- Built agents, MCP servers, Claude Skills, and custom GPTs across the Claude, Gemini, and GPT ecosystems, working hands-on with Claude Code, Claude Cowork, and the Opus, Sonnet, and Fable model families.
- Deployed end-to-end workflow automation with n8n, Make.com, and GitHub Actions, orchestrating LLMs, APIs, and business systems into production pipelines.
- Member, Anthropic Claude Partner Network.

EDUCATION

- M.S., Cybersecurity & Information Assurance, Western Governors University (expected 2027).
- B.S., Electrical Engineering, New Mexico State University.

CERTIFICATIONS

- GWAPT, GIAC Web Application Penetration Tester (held continuously since 2018).
- ISC2 Certified in Cybersecurity, CC (2026).
- CAISP, Certified AI Security Professional (in progress).
- Swimlane SOAR Certified: SCSU, SCSA, SCSD.
- Distinguished Toastmaster (DTM). Earlier career: Microsoft MCSD, MCAD, MCDBA, MCSE.