

MICHAEL ALLEN HART.COM

SENIOR AI SECURITY ARCHITECT | AI STRATEGY & GOVERNANCE CONSULTANT

United Kingdom | SC Cleared

PROFESSIONAL PROFILE

Senior AI security, strategy and governance consultant with 15+ years across global financial services, UK Government, defence, energy and critical national infrastructure. Combines enterprise security architecture and cloud engineering experience with current AI governance, agentic security, RAG, model and integration assurance. Advises stakeholders on AI adoption, risk-based decisions, operating models and architecture controls, supported by a substantial portfolio of technical designs, threat assessments and non-destructive integration validation.

SELECTED AI SECURITY ARCHITECTURE & ASSURANCE WORK

- Designed a vendor-neutral Enterprise AI Security Reference Architecture (V5.8) spanning agent identity and bounded delegation, dedicated model gateways, governed RAG, integration trust boundaries, final business-effect authorisation, outbound disclosure controls and independent assurance.
- Developed six integrated Mermaid architecture views (D0–D5), security requirements, design decision records and adversarial challenge scenarios addressing agent overreach, revocation, API bypass, indirect prompt injection, callback integrity and concurrency-safe workflow limits.
- Conducted live, non-destructive security validation of a Salesforce Developer Edition MCP integration: verified tool discovery, object/schema metadata and authenticated principal details; identified a provisional least-privilege risk associated with an administrator-profile connector identity and defined further assurance requirements.
- Evaluated SaaS backend security patterns, including conditional writes, restricted adapters and transaction-coupled enforcement; documented residual authorisation-to-commit races and the limits of evidence from synthetic testing.

CORE EXPERTISE

Enterprise AI security architecture • Agentic AI and delegated authorisation • LLM / model gateway controls • RAG and data governance • Security threat modelling • Cloud / DevSecOps • SaaS / MCP integration assurance • AI strategy, operating models and responsible AI • Executive advisory • NIST AI RMF, ISO/IEC 42001, OWASP and MITRE ATLAS

PROFESSIONAL EXPERIENCE

Security Consultant – AI Strategy, Governance & Architecture | Barclays Bank PLC | Nov 2025 – Present

- Lead AI security and governance engagements in a regulated global banking environment, working across business, architecture, engineering, data, risk and compliance stakeholders.
- Translate business priorities into governed AI use cases, controls, pilot acceptance conditions and accountable roadmap decisions; assess Copilot, Databricks Genie, Bedrock, Claude and enterprise AI-enabled workflows.
- Advise on LLM, RAG, agentic, embedding and AI integration patterns, including prompt injection, data disclosure, delegated identity, supply-chain threats and operational resilience.
- Contribute to an enterprise AI future-roadmap steering group; lead a critical payments application-security workstream covering Apple Pay and Google Pay.

Independent AI Strategy, Security & Governance Consultant | Sep 2024 – Nov 2025

- Developed enterprise AI strategy, governance and assurance frameworks, decision methods and a practitioner-led MAH Playbook, referencing NIST AI RMF, ISO/IEC 42001, ISO/IEC 23894, GDPR and the EU AI Act.

Cyber Security Instructor – Defence (Purple Team) | Royal Navy, HMS Collingwood | Aug 2023 – Aug 2024

- Delivered cyber and cloud security instruction in a high-assurance MOD setting, including Zero Trust, DevSecOps, secure architecture and defensive technical labs.

PROFESSIONAL EXPERIENCE — CONTINUED

Cyber Security Specialist – RNIR Programme | Maritime & Coastguard Agency | Jun 2022 – Jul 2023

- Security lead for a UK Government Tier 1 modernisation programme spanning 165+ sites; provided architecture assurance across complex multivendor critical infrastructure.
- Designed secure AWS and DevSecOps controls, with Microsoft Sentinel and Defender monitoring across operational technology and IT estates.

Network Security Engineer | OVO Energy | Oct 2020 – May 2022

- Managed enterprise firewall and network-security architecture in production; implemented automation and infrastructure-as-code controls.
- Supported security for Kubernetes and cloud workloads within a wider platform transformation.

IT / Infrastructure Manager | The Royal British Legion | Jun 2014 – Aug 2020

- Led regional IT operations, identity administration, service continuity and support aligned with central standards and ITIL processes.

TECHNICAL & DELIVERY TOOLKIT

AI / Data: Microsoft Copilot, Azure AI / Azure OpenAI, Databricks Genie, AWS Bedrock, GCP / Vertex AI, RAG, vector databases, MCP, API/tool security, evaluation tooling.

Cloud / Engineering: AWS, Azure, GCP, Docker, Kubernetes, Terraform, GitLab, Jenkins, Python / FastAPI, DevSecOps, secure SDLC.

Security / Governance: NIST AI RMF, ISO/IEC 42001 and 23894, ISO 27001/2, OWASP LLM Top 10, MITRE ATLAS, NCSC guidance, GDPR, EU AI Act, Zero Trust, architecture threat modelling and risk acceptance.

SELECTED ARCHITECTURE PORTFOLIO

Enterprise AI Security Architecture (V5.8) — six architecture lenses; defence-in-depth trust boundaries, original-user permissions, delegated agent identity, final-effect enforcement, independent outcome verification, integration assessment and structured adversarial review. Selected diagrams, architecture decision records and security assessment findings available upon request.

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

AWS Certified Security – Specialty | AWS SysOps Administrator | Microsoft SC-200 / SC-900 | Splunk Enterprise Certified Admin | Cisco CCNA | SANS SEC455 Cyber Architecture | Oxford University AI & ML for Cybersecurity | NVIDIA DLI AI for Cybersecurity

EDUCATION

BA (Hons), Communication | Manchester Metropolitan University