**Sam Arora**

**Principal AI/ML & DevSecOps Architect | Hands-on Cloud & Enterprise Strategist**

**Hornchurch, Greater London | 07706070809 | sam.arora@samokash.com** **LinkedIn:** [linkedin.com/in/sam-arora](https://www.linkedin.com/in/sam-arora-2739b515) | **GitHub:** [github.com/get2sammy](https://github.com/get2sammy) | **Hugging Face:** [huggingface.co/get2sammy](https://huggingface.co/get2sammy)

**Professional Summary**

A highly accomplished and hands-on technology leader with over 20 years of experience architecting and delivering transformative AI, DevSecOps, and cloud solutions for the world's leading financial, insurance, and enterprise organisations. I excel at bridging the gap between C-suite vision and engineering execution, building high-performing teams, and designing future-proof platforms that are secure, scalable, and intelligent by default. My leadership is rooted in a passion for purposeful innovation, fostering a culture of experimentation and continuous learning to solve complex business challenges.

**Key Achievements**

* **Delivered £100k+ in annual savings** by re-architecting costly, persistent cloud infrastructure into an intelligent, on-demand resource model.
* **Architected and deployed secure agentic AI applications** for finance and insurance, ensuring full compliance with stringent NIST, ISO27001, and SOC standards.
* **Led the design of secure, multi-region platforms on Azure and GCP**, enabling high availability and disaster recovery for mission-critical enterprise workloads.
* **Pioneered keyless authentication strategies in regulated cloud environments**, eliminating secrets management risks and significantly enhancing enterprise security posture.
* **Successfully presented AI innovation roadmaps to C-suite stakeholders**, influencing enterprise-level investment and strategic direction at major global firms.

**Technical Expertise**

|  |  |
| --- | --- |
| **Category** | **Skills** |
| **AI / ML** | Llama 3.x, Fine-Tuning (Ollama, Hugging Face), RAG, Agentic Workflows, Azure OpenAI, GCP Vertex AI (Gemini), LangChain, Prompt Engineering, Model Ops |
| **Cloud & Infrastructure** | Azure, GCP, AWS, Kubernetes (AKS, GKE), Terraform, Ansible, Multi-Region Architecture, Landing Zones, Infrastructure as Code (IaC) |
| **DevSecOps & CI/CD** | GitHub Actions, Jenkins, GitLab CI, Prisma Cloud, SAST/DAST/SCA Integration, Policy-as-Code (OPA), Secretless Architecture |
| **Security & Compliance** | ISO27001, NIST, SOC2, GDPR, Cloud Security Posture Management (CSPM), Secure SDLC, Keyless Authentication (OIDC, Workload Identity) |
| **Languages & Frameworks** | Python, React, Node.js, Flask, PowerShell |

**Marquee Engagements & Experience**

**Director & Principal Consultant** | Samokash Ltd | *Apr 2023 – Present* *Engaged by leading global firms to architect and deliver strategic AI, Cloud, and DevSecOps initiatives. Notable direct client engagements include:*

* **Principal AI & Cloud Technical Solutions Architect (Contract) | Legal & General (UK & America)**
* **Principal DevSecOps Technical Solutions Architect (Contract) | Euroclear**
* **Principal DevSecOps & AI Technical Solutions Architect (Contract) | Pret**
* **Principal AI Strategist (Contract) | Chase**

**Senior DevOps Engineer (AI/ML & DevSecOps)** | London Stock Exchange | *Aug 2022 – Apr 2023*

**DevSecOps Lead (AI/ML Integration)** | Allianz UK | *Mar 2022 – Aug 2022*

**DevSecOps Architect (Blockchain & AI)** | Genesis Trading Custody | *Nov 2021 – Feb 2022*

**DevOps Lead / Enterprise Architect** | WPP | *Apr 2021 – Nov 2021*

**DevOps Lead (Infrastructure & Security)** | Defra (UK Government) | *Nov 2020 – Apr 2021*

**DevSecOps Lead (AI & DevOps Enablement)** | Nationwide Building Society | *Jun 2020 – Nov 2020*

**Head of DevOps (Blockchain & AI Model Ops)** | EY (Insurwave) | *Mar 2018 – Jun 2020*

**DevOps Lead** | Legal & General | *Nov 2018 – Mar 2019*

**DevOps Cloud Solutions Architect** | Vanquis Bank | *Dec 2017 – Mar 2018*

**DevOps Technical Consultant** | Deutsche Bank / Sandhata | *Sep 2017 – Dec 2017*

**Project Lead / DevOps Engineer** | Bank of America | *Apr 2016 – Sep 2017*

***Previous Foundational Experience***

* **Commerzbank (London)** – Infrastructure Consultant | *Jan 2016 – Apr 2016*
* **CLOSE BROTHERS GROUP (London)** – Infrastructure, Security Consultant | *Jan 2015 – Jan 2016*
* **MARKIT GROUP LTD** – AVP DevOps, WinOps | *Jul 2012 – Dec 2014*
* **CAPITA IT SERVICES** - Windows Technical Lead/Deputy Team Leader | *Jan 2008 – Jul 2012*
* **PATNI COMPUTER SYSTEMS LTD (India)** – Senior Analyst | *Mar 2004 – Jan 2005*
* **Microsoft (India)** – EMEA Server Support/Operations | *Mar 2002 – Mar 2004*

**Key Projects**

**Local AI Model for Insurance Underwriting** *Problem:* A client needed to leverage proprietary medical data for risk assessment without exposing sensitive information to public cloud AI services. *Action:* I architected and led the development of an internal, air-gapped AI system. This involved **hands-on fine-tuning of a Llama 3-based model** on anonymised historical data to extract medical insights. The entire solution was deployed on-premise within a secure, compliant environment. *Result:* The system enhanced underwriting accuracy, accelerated processing, and ensured full data sovereignty and compliance with GDPR, SOC, and NIST frameworks.

**AI Risk Guard for Financial Services** *Problem:* Deploying generative AI in a high-stakes financial services environment carried significant risks of model hallucination, bias, and compliance violations. *Action:* I designed and implemented a **hybrid AI safety system** that acts as a firewall for LLM outputs. The solution uses a combination of rule-based heuristics and a lightweight, distilled "guard" model to scan API responses for risks before they are exposed to users or other systems. *Result:* Enabled the safe, responsible adoption of generative AI for underwriting and customer service use cases, with auditable controls that satisfy regulatory scrutiny.

**Keyless Authentication & Secretless CI/CD for GCP** *Problem:* Managing and rotating secrets for cloud infrastructure and CI/CD pipelines was a significant operational burden and security vulnerability. *Action:* I architected and deployed a **fully keyless access solution for Google Cloud**. Using Workload Identity Federation and OIDC-based trust, I eliminated the need for service account keys in Terraform and GitHub Actions deployments, enforcing short-lived, ephemeral credentials. *Result:* Eradicated a whole class of security risks, simplified compliance, and reduced operational overhead associated with secrets management.

**Multi-Region Cloud Platform (Azure + GCP)** *Problem:* An enterprise client required a standardised, resilient, and secure foundation for deploying new applications across multiple cloud providers. *Action:* I led the end-to-end design and implementation of scalable landing zones using Terraform. The architecture featured modular pipeline templates, automated compliance checks via **policy-as-code (OPA)**, and DR-ready configurations for FinServ-grade workloads. *Result:* Accelerated application onboarding by 40%, enforced consistent security and governance, and ensured business continuity with a robust high-availability and disaster recovery posture.