Karan Bansal

+919821974890 | karanb192@gmail.com | linkedin.com/in/karanb192 | github.com/karanb192

Education

IIT Kanpur — Kanpur, UP
B.Tech. in CSE (IITJEE - AIR 192) — *July 2012 – April 2016*

Experience

AI Architect, CTO's office — December 2023 – Present
ArmorCode — *Gurugram*

- Aligned AI strategies with C-level goals, ensuring tech roadmaps drove measurable corporate growth
- Launched Anya, a context-aware, agentic AI security assistant, delivering real-time, high-fidelity vulnerability insights and proactively orchestrating security workflows, sharply improving enterprise risk posture
- Built AI-powered correlation engine analyzing billions of security findings, pinpointing bucketized remediation actions (one fix resolves multiple issues) and surfacing unique actionable findings
- Orchestrated the end-to-end onboarding experience revamp, achieving a 40% reduction in time-to-proficiency
- Automated the ingestion & interpretation of VAPT reports using AI workflows, eradicating tedious manual effort

Engineering Manager — April 2021 – July 2023
Urban Company — *Gurugram*

- Drove security initiatives as head of security, covering privacy, IPO readiness, product security, etc.
- Spearheaded core platform initiatives achieving 99.999% uptime: auto-failover, rate limiting, load shedding, canary reverts, HA setups, disaster recovery, multi-AZ/multi-region architecture, MTTR reduction, etc.
- Built and scaled product security and core platform teams from the ground up, ensuring strategic growth
- Implemented scalable "Crypto Shredding" privacy solution, encrypting all persistent personal data

Engineering Manager — July 2018 – April 2021
Avid Secure (acquired by Sophos) — *Gurugram*

- Founding engineer for the multi-cloud security start up and built the first version (MVP) of the security platform
- Hired the initial high-performing team for the start up and scaled it to 25 engineers after acquisition
- Re-designed the architecture to make infra scalable, reliable, secure, resilient and highly available to support from 10 customers to 10K customers post acquisition
- Collaborated with PM to define the product vision and guided teams on planning, designing and building software
- Managed team members including setting goals, performance reviews & establishing a positive work environment
- Led the engineering excellence, SSDLC, external pen-test and launched the bug bounty program for the product

Sr. Software Engineer — May 2016 – July 2018
NTRO (Prime Minister's Office) — *New Delhi*

- Developed secure software solutions, collaborating with cross-functional teams to protect the CII

Summer Internships

- **FireEye** (Summers'15): Developed a vulnerability scanner tool for windows and was offered a PPO
- **Citrix** (Summers'14): Built a SETI-style distributed fuzzing system presented at c0c0n'14

Open Source Contributions

- Published multiple tech blogs on Caching Library, EKS, Access Control, and a case study with AWS
- Contributor to find-sec-bugs, the most popular open source java plugin for security audit of Java web apps
- Conducted a workshop on Web Application Security in Hacker's Day Conference held in Jan'17
- Gave a talk and conducted a training on Applied Crypto for InfoSec at DEFCON—OWASP 2016

Technical Skills

GenAI/LLM: OpenAI ChatGPT, o1, o3, o1-pro, o3-pro, Anthropic Claude, Opus 4, Sonnet 4, Reasoning Models, Claude Code, Windsurf, Gemini, RAG, Fine-tuning, Vector DBs, Prompt Engineering, LLM Evaluation, Reinforcement Learning, RLHF, RLAIF, Model Context Protocol (MCP), Prompt Injection, Agentic AI
Security & Cloud: AWS, VAPT, OWASP Top 10, RBAC, Threat Modeling, Applied Crypto, Code Signing
Software Engineering: Java, Python, Go, Javascript, Spring Boot, Kubernetes, Kafka, Distributed Systems, Scaling