

PRASHANTH SIVARAJAN

Mob:+91 9342766228

prash.siv@gmail.com

Address : Bangalore, India



EXPERIENCE SUMMARY

Product security leader with 21+ years securing enterprise environments across SaaS, cloud-native, and AI-powered platforms. Currently as Security Consultant at AWS, driving product security for Agentic AI platforms, large-scale cloud migrations, and compliance automation. Deep expertise in secure SDLC, threat modeling, DevSecOps, vulnerability management, AI/ML security, and incident response, aligned to industry frameworks like ISO 27001, OWASP Top 10, GDPR, EU AI Act, etc. Known for building security programs from scratch and bridging technical and executive teams to deliver compliant, scalable security solutions.

LEADERSHIP

Experienced in leading diverse, cross-functional teams across secure architecture, vulnerability management, application security, and infrastructure hardening. Known for cultivating a culture of ownership, where teams are trusted to drive outcomes and contribute beyond their roles. Comfortable influencing across all levels from hands-on engineers to senior executives to align security priorities with strategic goals.

WORK EXPERIENCE

Wipro	RSA / EMC	Infosys	Sage Group	AWS
Software Engineer / Test Automation Lead	Senior Risk Analyst & Quality Engineer	Senior Consultant	Senior Security Architect	Senior Security Consultant
Jul 2005 - Mar 2008 Bengaluru	Mar 2008 – Jun 2013 Bengaluru	Jun 2013 – Dec 2017 Bengaluru/Jersey City	Dec 2017 – Dec 2022 Atlanta	Dec 2022 – Present Atlanta/Bengaluru

PROFESSIONAL EXPERIENCE

Amazon Web Services (AWS) - Senior Security Consultant / Delivery Consultant

- Owned product security for an enterprise Agentic AI platform on Amazon Bedrock AgentCore — from threat modeling to secure deployment and governance.
- Defined Agentic AI security controls and GenAI guidelines covering Responsible AI, GxP compliance, guardrails, and secure data pipelines — aligned to NIST AI RMF, MITRE ATLAS, EU AI Act, ISO 42001, and OWASP LLM Top 10.
- Extended the AI SDLC with threat modeling for prompt injection, model abuse, data governance, and observability risks.
- Owned security for a global SAP cloud migration spanning 20+ platforms and 1,500+ servers across 4 regions.
- Built a cloud security assessment tool that cut review time from 6 hours to minutes across 1,500+ servers.
- Led incident response for customers, coordinating cross-functional response across global teams.

Sage Group — Senior Security Architect

- Owned product security for 40+ products across North America, Europe, and APAC — including SaaS platforms and Salesforce integrations.
- Built Sage's AI/ML security practice from the ground up, translating strict financial security policies into developer-friendly guardrails.
- Built secure data pipelines with data classification, minimization, and MLSecOps processes for the AI team.
- Managed 2 security engineers and a 50+ developer security champions network across global product teams.
- Designed a full Secure SDLC program integrating SAST, DAST, SCA, secrets detection, and CI/CD security gates.
- Led vendor security reviews using CAIQ/CCM, SIG, and other assessment frameworks to evaluate third-party risk.
- Led ISO 27001 alignment and audit readiness, reducing the application risk portfolio below 20%.
- Led an enterprise-wide threat modeling initiative, reducing manual security review effort by 60%.
- Delivered executive dashboards covering quarterly risk posture, remediation trends, and security KPIs.

Infosys Technologies — Senior Consultant

- Led and executed comprehensive penetration testing engagements across web, mobile, APIs, and thick-client applications, identifying and mitigating critical security risks for Fortune 500 clients.
- Built internal tooling to automate application on-boarding and self-service vulnerability management at scale increasing efficiency by over 60%
- Enabled a 25% reduction in high-risk findings across key client environments by designing custom CVSS/FAIR-based risk scoring models and tailored remediation plans.
- Designed and rolled out end-to-end cybersecurity programs to implement PCI-DSS compliance controls, enhance security maturity and build internal security capabilities.
- Authored client proposals and led presales engagements, solution architecture, and effort estimation.

RSA Security / EMC — Senior Risk Analyst & Quality Engineer

- Performed penetration testing and risk assessments across internal tools, products, and infrastructure - covering web apps, Flex/AMF, HVAC/BMS, Salesforce, and thick clients.
- Automated infrastructure security scans across large IP ranges using Nessus and Qualys, cutting assessment turnaround time by 80%.
- Performed architecture reviews and risk assessments, communicating findings directly to business and engineering stakeholders.
- Earlier in tenure as Senior Quality Engineer at RSA (SecureID division): led threat modeling, third-party VA reviews, and security test planning — with ~50% of time on application security.

Wipro Technologies — Software Engineer / Test Automation Lead

- Progressed from functional tester to test automation lead and Java developer; led a team of 3 engineers on feature development including RADIUS integration.
-

CORE COMPETENCIES

- Product & Application Security
- DevSecOps & Secure SDLC
- Vulnerability Assessment & Penetration Testing
- Secure Coding Standards & Code Review
- Vendor Security & Third-Party Risk (CAIQ/CCM)
- Security Program Ownership & Champions Programs
- Compliance (NIST AI RMF, ISO 27001, GDPR, PCI-DSS)
- AI/ML & Agentic AI Security
- Threat Modeling
- Vulnerability, Risk & Remediation Management
- Cloud Security (AWS,Azure)
- Incident Response
- Executive Stakeholder Management & Team Mentoring
- Containers and Kubernetes security

TOOLS & TECHNOLOGIES

- **Application Security:** Checkmarx, Semgrep, Snyk, Fortify, Burp Suite, Acunetix, OWASP ZAP, Metasploit, Nmap, MobSF
- **DevSecOps & CI/CD:** GitHub Actions, Terraform, Checkov, Kyverno, SonarQube
- **Container & Kubernetes Security:** Trivy, Aqua Security, Falco, Sysdig, kube-bench
- **Cloud Security & CSPM:** AWS (Security Hub, Config, Control Tower, Bedrock, AgentCore, CDK), Prisma Cloud, Wiz, ScoutSuite, Prowler
- **Threat Modeling:** Threat Modeler, AWS Threat Composer, Microsoft Threat Modeling Tool, OWASP Threat Dragon, IriusRisk
- **Vulnerability Management:** Qualys, Tenable, Nessus
- **Compliance & Risk:** RSA Archer, OneTrust, AuditBoard

EDUCATION

B.Tech, Information Technology — SASTRA University, India

CERTIFICATION

Certified Information Security Manager (CISM)	Certified Information Systems Security Professional (CISSP)	Certified Cloud Security Professional (CCSP)
Certified Secure Software Lifecycle Professional (CSSLP)	Offensive Security Certified Professional (OSCP)	AWS Certified Security Specialty
AWS Certified AI Practitioner	AWS Certified Solutions Architect Associate	