Viplove Karhade

(617) 982-8632 | viplovekarhade@gmail.com |https://www.linkedin.com/in/viplovekarhade

PROFESSIONAL PROFILE:

Technical leader and strategic architect specializing in secure 'Paved Paths' for AI, Agentic, and Public Cloud ecosystems. Proven track record in quantifying systemic risk and unblocking significant business value, including large-scale facility-level cost savings and the safe enterprise-wide onboarding of AI tools for the global developer population.

PROFESSIONAL EXPERIENCE:

Salesforce Inc.

Senior Infrastructure Security Engineer June 2022 - Present

AI & Agentic Security Leadership

- Architected Secure 'Paved Paths' for Emerging Tech: Established security research and governance for the **Model Context Protocol (MCP)**, implementing enterprise-wide authentication and access standards to mitigate "Shadow AI" risks
- Strategic AI Enablement: Conducted deep-dive security assessments for industry-leading AI coding tools (e.g., **Cursor, Windsurf, Claude Code**), facilitating safe adoption for the global developer population.
- Global Threat Response: Spearheaded an enterprise-wide investigation into emerging prompt injection vulnerabilities, leading proactive forensic scanning across internal source code management (SCM) systems

Infrastructure Security & Systemic Risk

- Design & Cost Optimization: Drove complex secure design reviews for critical infrastructure decommissions and public cloud migrations, unblocking significant facility-level cost savings
- Security Transformation: Led large-scale network security transformations for core database hosting and modernized enterprise malware scanning architectures to enhance systemic resilience
- Identity & Access Governance: Engineered a privileged access governance framework for production infrastructure, significantly reducing the attack surface for core cloud services

Strategic Influence & Capability Uplift

- Standardized Assessment Frameworks: Authored the Security Review Playbook, establishing a consistent framework for technical assessments and stakeholder engagement across the security organization
- Global Skill Development: Developed and led technical training paths for GCP Security, upskilling team members in cloud-native security

Synopsys Inc.(Previously Cigital Inc.)

Associate Principal Consultant Jan 2016 - May 2022

- Strategic Architecture & Threat Modeling: Advised business units on the secure design and deployment of cloud-native and on-premise applications, performing deep-dive Architecture Risk Analysis to identify and mitigate systemic design flaws.
- Security Assurance & Pentesting: Led end-to-end security assessments for web, network, and API services; leveraged industry-standard tools (e.g., Burp Suite Professional, IBM AppScan) to identify critical vulnerabilities and provide prioritized remediation roadmaps.
- Mobile & Code Security Specialization: Performed advanced penetration tests and secure code reviews for iOS and Android applications developed in Java and .NET, ensuring robust protection for complex mobile ecosystems.
- Risk Governance & Stakeholder Management: Guided global stakeholders through formal Risk Acceptance and Remediation procedures, translating technical security findings into actionable business risk

assessments.

TECHNICAL KNOWLEDGE:

AI & Agentic Security

- Architectural Standards: Model Context Protocol (MCP), MCP Gateway, Multi-tier authentication (MFA/mTLS), RBAC for AI clients
- Emerging Threats: Prompt Injection Mitigation, Shadow AI Governance, Forensic scanning for AI-specific indicators of compromise (IoC)
- Secured Tooling: Cursor, Windsurf, Claude Code, Agentic workflow hardening

Infrastructure & Cloud Security

- Platforms & Orchestration: Google Cloud Platform (GCP), Amazon Web Services (AWS), Kubernetes (CKA Certified), Docker
- Identity & Access: Zero Trust Architecture, Privileged Access Governance, Credential Management, 2FA/MFA

Product Security & Engineering

- Methodologies: Secure Software Development Life Cycle (S-SDLC), Threat Modeling, Architecture Risk Analysis, Secure Design Reviews
- Specializations: Web Application Security, Mobile Application Security (iOS/Android), Web Services and Network Pentesting
- Security Tooling: Burp Suite Professional, IBM AppScan, Snyk, Prisma Cloud, Trivy, TruffleHog, Metasploit, Wireshark, Nmap, Checkmarx
- Languages: Java, C++, C, Android, .NET, Python, Shell Scripting

EDUCATION & CERTIFICATIONS:

Northeastern University, **Boston, MA** Sept 2013 – Dec 2015

Master of Science in Information Assurance

CKA: Certified Kubernetes Administrator March 2024 -March 2027