HARSH BHETARIA, CISSP

Staff Product Security Engineer

harsh@mail.hnbhetaria.com | (347) 668-7172 | Indianapolis, IN | linkedin.com/in/harsh-bhetaria | hnbhetaria.com

SUMMARY

Staff-level Product Security Engineer with 10+ years driving platform security, threat modeling, and AppSec programs across enterprise and consumer products serving 50M+ users. Provide technical leadership across 15+ engineering orgs through security architecture, AI-powered automation (LLM threat modeling, AI-assisted code review, CI/CD security gates), and cross-functional program design. Deep expertise in secure SDLC, DevSecOps, MCP security, and securing agentic AI systems. CISSP certified.

CORE COMPETENCIES

Product & Application Security: Threat Modeling (STRIDE/PASTA), Security Architecture, Security Design Reviews, Penetration Testing, SAST/DAST, Secure Code Review, Vulnerability Management, Secure SDLC, DevSecOps

AI & Agentic Security: MCP protocol security, MCP attack surface analysis (tool poisoning, prompt injection, privilege escalation), securing agentic AI flows, agentic access control, LLM threat modeling, AI-assisted code review, prompt engineering for security automation

Leadership: Cross-functional technical leadership, security program design, mentorship, RFC authoring, security strategy, stakeholder communication, Security Champions programs

Tools: Burp Suite Pro, Semgrep, GitHub Advanced Security, SonarQube, Checkmarx, OWASP ZAP, Claude Code, Copilot, Cursor

Languages & Platforms: Python, Go, JavaScript, TypeScript, Hack, SQL, AWS, Docker, Kubernetes

Compliance & Frameworks: SOC 2, PCI DSS, GDPR, CCPA, SOX, OWASP Top 10, NIST CSF, MITRE ATT&CK

EXPERIENCE

Slack Technologies (Salesforce) | *Senior Product Security Engineer* May 2022 – Present

- Lead product security strategy for Slack's 20M+ DAU platform, owning threat modeling, security architecture, and incident response across core services and integrations consumed by Fortune 500 enterprises.
- **Auto Threat Modeling:** Architected and shipped LLM-based automated threat modeling pipeline used across 15+ engineering teams, generating STRIDE models from architecture diagrams with auto-triaged findings—reducing org-wide manual effort by ~60% and unblocking faster service launches.
- **AI-Assisted Code Review:** Designed Semgrep + LLM hybrid PR review pipeline detecting logic-layer vulns missed by SAST, deployed as GitHub Actions workflow across the engineering org—cutting AppSec manual review load by ~40% and accelerating dev velocity.
- **CI/CD Security Automation:** Integrated automated security gates across CI/CD (dependency scanning, secret detection, container scanning) and built a self-service risk posture portal enabling engineering teams to ship securely without AppSec bottlenecks.
- **Security Champions:** Founded and scaled Security Champions program across 15+ engineering teams with tiered certification and quarterly workshops, driving 35% reduction in critical/high findings reaching production over 18 months.

Amazon Lab126 | *Security Engineer II – Device Security* June 2021 – May 2022

- Secured Fire TV platform (50M+ users) via threat modeling, architecture reviews, and IoT/embedded pentesting. Led Sev-1 incident response, achieving 30% MTTR reduction.

Synopsys, Inc. | *Senior Security Consultant* Aug 2015 – June 2021

- Led team of 5–8 consultants delivering 200+ application security assessments (web, mobile, API) for Fortune 500 clients. Drove OWASP/NIST-based AppSec engagements, M&A security due diligence, and built internal training and CTF programs.

SELECTED PROJECTS & TECHNICAL LEADERSHIP

- **Security Review Modernization RFC:** Authored Slack's internal RFC for modernizing the security review process—covering risk-based service tiering, AI-assisted PR code review, automated CI/CD security gates, and a self-service developer security portal—adopted as the security org's multi-quarter roadmap.
- **MCP & Agentic Security Research:** Researched and documented MCP attack surface analysis (tool poisoning, indirect prompt injection, privilege escalation across tool chains) and authored internal guidance for securing agentic AI integrations across the product surface.
- **Mentorship & Knowledge Sharing:** Mentor junior and mid-level security engineers across the org through 1:1 coaching, threat modeling workshops, and code review pairing—contributing to multiple promotions and onboarding standards.
- **Homelab & Independent Research:** Maintain a self-hosted security stack (password vault, reverse proxy, Cloudflare Access) used as a personal R&D environment for security tooling experiments and AI automation prototypes.

EDUCATION & CERTIFICATION

M.S. Cybersecurity, New York University

B.Tech Information Technology, CHARUSAT University

CISSP — ISC2 | September 2024