

Pankaj Mouriya

Product Security Engineer

📞 (+91) 7087408408 | ✉️ pankajmouriya9@gmail.com | 🌐 pankajmouriya | in pankajmouriya | Bengaluru, India

Security Engineer with proven expertise in DevSecOps, cloud security, and supply chain protection across large-scale distributed systems, now specializing in **AI-driven security automation**. Track record of building **agentic AI systems** and LLM-powered workflows that scale vulnerability management, leading incident response, and ensuring compliance across SOC2/ISO27K frameworks. Daily hands-on user of **AI coding agents** (Cursor, Claude Code, Windsurf/Devin, Codex), Claude skills and LLM APIs to execute faster, smarter and at scale, while enabling organizations to build resilient, secure platforms.

Core Competencies

AI & Automation	Agentic AI systems, LLM-powered vuln management, Claude skills, Cursor/Claude Code/Windsurf (Devin)/Codex, LLM & Bedrock APIs, MCP
DevSecOps	CI/CD security, IaC scanning, automated vulnerability management, pipeline design
Supply Chain	SBOM, build provenance, container signing, dependency analysis
Incident Response	Incident command, threat analysis, incident response automation, crisis coordination
Cloud/Container Security	AWS/GCP/Azure, Kubernetes, Runtime Security, Cloud Native Security Tools
Compliance	SOC2, ISO27001, security controls, audit, risk assessment

Experience

Harness

Senior Product Security Engineer

Bengaluru, India

November 2025 - Present

- **Vulnerability Management Platform (SoS):**
 - Architected and launched **SoS**, a vulnerability-management and security-posture platform **used daily by engineering and leadership** across Harness and four acquired companies; processed **90K+ CVEs in one day** while tracking SLA compliance, burndown, and security KPIs
 - Scaled SoS to analyze reports with **10K+ CVEs**, leveraging **scanner reachability/exploitability** analysis for critical/high findings and combining **EPSS and KEV** signals for prioritization
 - Delivered an end-to-end **customer CVE report triage** feature: when customers scan Harness images pre-deployment and report critical/high CVEs, the dashboard **auto-triages** across any number of reports/images by matching the deployed image version against newer releases to check whether the CVE is already fixed, runs **multiple scanners** for maximum coverage, and enables one-click **Jira ticket creation** for end users - cutting manual triage from **weeks to hours** and saving **months** of engineering effort
- **Security Scanning & Pipeline Automation:**
 - Built **20+ security scanning, orchestration and automation pipelines** on Harness CI covering secret scanning, SAST and supply-chain/compromised-package detection, with automated suppression, approval and policy workflows
 - Onboarded **all core codebases, PRs and binary/image builds** across Harness Engineering onto these scanning pipelines, enforcing pipeline-embedded security gating and build-time controls
 - Gated every **new package/dependency upgrade** behind **manual security-governance approval**, ensuring only approved packages get baked into production builds
 - Authored multiple **Harness Security Advisories** for internet-wide supply-chain incidents, running **in-house scanning/analysis** to determine whether Harness was compromised and publishing guidance for **Harness customers**
- **AI & Agentic Automation:**
 - Embedded **AI and agentic workflows** into SoS for on-demand CVE validation and automated triage of external vulnerability and pentest reports by integrating **MCP servers** for Jira, Atlassian, HackerOne and Harness, saving hours per report at less than **~\$1** each.
 - Built an in-house **AI Assistant/Agent observability platform** for endpoints/CI to **monitor agents** on what shell/Web API and file-system ops are being performed and flag for **risk signals** such as PII, credentials and malicious package installation
 - Built **agentic AI systems** leveraging **AI skills**, LLM/Bedrock APIs and MCP integrations to automate and scale vulnerability management, triage and reporting workflows
 - Leveraged **AI coding agents** (Cursor, Claude Code, Windsurf/Devin, Codex) and Bedrock APIs programmatically to build automations and accelerate delivery **~10x**
 - Selected for the **Mythos program**, applying **Mythos for SAST testing** to surface bugs and security issues not detectable by conventional scanners or models
 - Contributed to the **internal LLM guardrail service**, adding new **guardrails** for broader coverage at the **Harness LLM Gateway**
- **Benchmarking & Cross-Org Leadership:**

- Led **multiple benchmarking efforts and PoCs** (including during acquisitions), producing detailed **SAST/SCA tooling benchmark** reports that drove **internal product improvements** and a **competitive marketing edge**

Kong

Bengaluru

Senior Security Engineer

May 2024 - October 2025

- **DevSecOps & Security Automation:**
 - Maintain comprehensive security scanning (SAST, SCA, SBOM, secrets detection) across **100+ Kong software repositories**
 - Develop and maintain centralized security controls for Kong's infrastructure
 - **Resolved critical CI/CD pipeline failures** during security tool outages by implementing "break glass" mechanisms, preventing extended development blocks
 - **Reduced pipeline failures** through vulnerability database mirroring solutions for upstream outage resilience
 - Maximized security tool availability by configuring ECR pull-through cache infrastructure
 - Streamlined incident response through Tines workflow automation integrating CrowdStrike, PagerDuty, Jira and Slack
 - Enriched CrowdStrike alerts and Jira tickets with MDM data for automated user correlation
- **Supply Chain Security & Standards:**
 - Established **auditable build processes with provenance tracking** for production software releases
 - Implemented **container image signing** to ensure artifact integrity and authenticity verification
 - Lead GitHub Advanced Security implementation across Kong repositories
- **Cloud Security & Infrastructure:**
 - Deployed **multi-cloud scanning (AWS, GCP, Azure)** with scheduled assessments and Tines-automated alerting
 - Enriched vulnerability findings with remediation guidance, enabling platform engineers to triage critical/high risks efficiently
 - Validated security findings to reduce false positives and deliver actionable items
- **Vulnerability Management & Incident Response:**
 - Coordinated penetration testing engagements and triaged findings with engineering teams
 - Established AI-assisted CVE determination processes for efficient vulnerability classification
 - Serve as **Incident Commander** for CSIRT/PSIRT security incidents with **proven resolution track record**
- **Compliance & Documentation:**
 - Implemented GitHub misconfiguration scanning across Kong products (Mesh, Gateway, Insomnia, Konnect) covering **200+ repositories**
 - Contributed to **successful SOC2/ISO27K audit outcomes** through security control implementation
 - Authored comprehensive security documentation, playbooks and vulnerability assessment frameworks
- **Innovation & Leadership:**
 - Evaluated and deployed **AI-powered code analysis tools** including CodeRabbit and Claude Code for automated PR security reviews
 - Collaborate cross-functionally with engineering teams across multiple time zones for security integration
 - Champion security initiatives through technical demonstrations to engineering staff
 - Provide technical mentorship and handle ad-hoc security support requests

DeepSource

Bengaluru, India

Security Engineer III

September 2022 — May 2024

- Implemented **Teleport OSS for Just-in-Time access management** across applications, VMs, Kubernetes and CloudSQL infrastructure
- Established **runtime security** for static analyzers using Falco and KubeArmor, **preventing RCE and data exfiltration** through syscall detection and policy enforcement
- Deployed infrastructure as code using Terraform and Atlantis for automated GCP IAM management via PR workflows
- Centralized vulnerability management through DefectDojo deployment, aggregating findings from multiple security tools with continuous monitoring
- Deployed Scout Suite (CSPM) for cloud security posture assessment, identifying and prioritizing critical vulnerabilities
- Conducted **quarterly IAM audits**, access reviews and unauthorized access detection with comprehensive remediation
- Secured device access and internal applications through Tailscale VPN implementation
- Authored **responsible vulnerability disclosure policy** establishing organization's bug bounty program
- Developed **Kubernetes Validating Admission Controller** to detect security misconfigurations in API requests
- Built Go-based security scanning APIs integrating CNCF tools (Kube-Bench, Kube-hunter) for comprehensive assessments
- Architected **serverless vulnerability scanner** using Go, Trivy and ECS Fargate for automated assessments
- Created management APIs for AWS ECR operations using AWS SDK for Go
- Implemented dashboard interfaces using AWS SDK and Kubernetes client-go for Arch0 platform
- Developed cluster management APIs for DigitalOcean Kubernetes Service (DOKS) using DO SDK
- Deployed Kubernetes Informers for **real-time resource monitoring** and event-driven responses across clusters

InVideo

Mumbai, India

Security Engineer

November 2021 — September 2022

- Automated **bug bounty program operations** including issue triaging and researcher communications
- Built **SAST/DAST pipeline** integrating Checkov, Semgrep, Trivy and OWASP ZAP for continuous security testing
- Performed cloud infrastructure audits and **CIS compliance assessments** using Prowler
- Designed comprehensive DevSecOps pipeline following OWASP best practices throughout SDLC

Appsecco Consulting

Security Analyst

Bengaluru, India

January 2020 — November 2021

- Conducted web application security assessments and network penetration testing for **enterprise clients**
- Performed AWS and GCP cloud security audits evaluating posture and compliance requirements
- Published technical security research and **presented findings at security conferences**

Certifications

Certified Kubernetes Administrator (CKA)

CNCF

AWS Certified Security - Specialty

AWS

Technical Leadership

Conference Speaking

- **BSides Goa 2024**: “Safeguarding Against RCE through Dependency Management and eBPF”
- **Rootconf 2022**: “Do’s & Don’ts on Setting up a Bug Bounty Programme”
- **H@cktivityCon 2021**: “Learn a Few Patterns, Secure your Applications in the Cloud”
- **BSides Newcastle 2021**: “Map and Conquer: Application Security over Cloud Infrastructure”
- **Community Meetups**: “Active community member and speaker at various meetups and conferences”

Technical Writing

- Security blog and e-books at noshellaccess.com
- Professional portfolio at pankajmouriya.com

Education

Chandigarh University

B.E. in Computer Science (Information Security)

Chandigarh, India

2016-2020