PIYUSH KUMAWAT

Staff Product Security Engineer | AI Security | Threat Modeling | Supply Chain Security | DevSecOps | Offensive Security

Bangalore, India | +91-8562808965 | piiiiyush22@gmail.com | linkedin.com/in/piyush-kumawat | securitycipher.com

PROFESSIONAL SUMMARY

Staff Product Security Engineer with 7+ years in product security, AI security and software supply chain security. At Harness, owns vulnerability management and release security sign-off for 900+ container images, runs the external pen test and bug bounty triage programs, supports FedRAMP, SOC 2 and PCI DSS, and leads security incident response. Builds AI security tooling, including ThreatFolio for automated threat modeling, an LLM-assisted reachability framework and a ProdSec AI on-call agent. Previously ran product security and bug bounty at OLA and tested 300+ applications across web, API, mobile and network.

CORE SKILLS

Product Security: Threat Modeling (STRIDE, PASTA), Secure Design Review, Security Architecture Review, Secure Code Review, Penetration Testing (Web, API, Mobile, Network), Secure SDLC, Incident Response, OWASP Top 10, MITRE ATT&CK, Bug Bounty and Pen Test Programs (HackerOne, Synack)

AI Security: OWASP Top 10 for LLM Applications, AI Agent and MCP Security, LLM-Assisted Vulnerability Triage, AI Threat Modeling, Agentic Security Automation

Vulnerability Management: Container Security, Software Supply Chain, SBOM, Reachability Analysis, Risk-Based Prioritization, SLA Governance, Exemption Workflows, Security Advisories, Secret Detection, External Attack Surface

Compliance: FedRAMP, SOC 2, PCI DSS, DISA STIG, ISO 27001, GDPR, RBI

Leadership: Mentoring, Onboarding, Security On-Call, Release Sign-Off, Cross-Team Programs, Executive Reporting

Cloud and Platform: AWS, Azure, GCP, Kubernetes (GKE, Helm), Docker, IAM Review, WAF

CI/CD and Automation: Harness CI/CD, Jenkins, Security Gates, Slack Alerting, Python, Go, Bash, REST APIs

Security Tools: Burp Suite, Prisma Cloud, Wiz, Snyk, Grype, Trivy, Semgrep, Qwiet AI, Gitleaks, Joern, Checkmarx, SonarQube, Coverity, Mend, Black Duck, TruffleHog, OpenSCAP, Metasploit, Nessus, Nmap

PROFESSIONAL EXPERIENCE

Staff Product Security Engineer **May 2024 – Present**

Harness | Bangalore, India

- **AI threat modeling:** Built ThreatFolio, an AI threat modeling platform that generates STRIDE threat models and data flow diagrams from Confluence design docs, with OWASP LLM Top 10 coverage, human review, Jira export and a CI/CD gate.
- **Reachability analysis:** Designed an LLM-assisted framework combining Joern code property graphs, Semgrep and OSV/GHSA/NVD data with Claude on AWS Bedrock; validates every cited code path to reject hallucinated verdicts and cut false positives.
- **AI security agents:** Built the ProdSec AI on-call agent (Slack, GKE) that answers scan, exemption, secret and customer CVE questions, cutting on-call response time.
- **Offensive AI:** Evaluated Anthropic Claude Mythos and other AI pentest agents for autonomous vulnerability discovery against Harness services.
- **CI/CD security:** Built 20+ Harness security pipelines, including a unified scanner (Prisma Cloud, Grype, Trivy, Snyk) for 900+, SBOM, EOL and SCA checks, and daily Slack alerts for new vulnerabilities; rolled out Semgrep and Gitleaks as mandatory PR checks and Qwiet AI scans.
- **Release security:** Own security sign-off for Harness SMP releases (93–95% SLA compliance across 740–790 unique critical and high CVEs per release); set up pipelines that publish advisories and STIG reports to the Harness Trust Center for SMP, Delegate, Traceable SMP and Agents.
- **Vulnerability management:** Established SLAs, ownership routing to 25+ teams, exemption workflows, a Jira Vulnerability issue type, executive dashboards and automated Jira creation and escalation digests.
- **Pen test and bug bounty:** Run the external pen test program : scoping, walkthroughs of 14 product modules, severity validation and 30-day remediation; HackerOne report triage into ProdSec with a program guideline.
- **Secret detection:** Built a secret scanning orchestrator in Go for scheduled, incremental scans of public GitHub orgs and DockerHub images, with secret revalidation and recon of public-facing assets.

- **Compliance:** Support FedRAMP with deviation requests, evidence and compensating controls; provide SOC 2 audit evidence and drove remediation
- **Incident response and customer support:** Led response to supply chain and credential incidents, including the npm Mini Shai-Hulud compromise, a PAT leak and exposed-credential reports; triage customer vulnerability reports and security questionnaires.
- **Mentoring:** Onboard and mentor ProdSec engineers through tooling and code walkthroughs, and present internal sessions such as a Brown Bag on AI threat modeling.

Product Security Engineer **Jan 2022 – May 2024**

OLA | Bangalore, India

- Led the company bug bounty program, owning triage, validation, severity and reward decisions, and remediation tracking.
- Performed threat modeling, SAST, DAST and white-box testing for OLA Mobility, OLA Electric and OLA Financial Services, finding OWASP Top 10 and business-logic flaws and retesting fixes.
- Owned application security requirements for PCI DSS, ISO 27001, GDPR and RBI audits; managed WAF configuration and tuning.

Security Services Associate Consultant **Jun 2019 – Jan 2022**

Synopsys Inc. | Bangalore, India

- Performed black-box and grey-box penetration tests of web, API, mobile and network targets for US, Canada and EU clients.
- Conducted cloud security configuration reviews on AWS, Azure, GCP and Alibaba Cloud.
- Integrated Checkmarx, WhiteSource and Burp Suite into client CI/CD pipelines to shift security left.

Cyber Security Intern **Jan 2019 – May 2019**

Synopsys Inc. | Bangalore, India

- Automated multiple SAST, SCA and DAST tools into a single Jenkins CI/CD security platform for internal use.

System / Network Administrator Intern **Mar 2017 – Apr 2017**

Shah Technical Consultants Pvt. Ltd. | Jaipur, India

- Managed network and server infrastructure and resolved day-to-day technical issues.

PROJECTS & COMMUNITY

- **Bug Bounty:** Active researcher on Bugcrowd and private, invite-only bug bounty programs.
- **Security Blog:** securitycipher.com, writing on AI security, application security and bug bounty.
- **Android Apps:** Windows Server Administration (20,000+ downloads, Google Play) and Penetration Testing (Google Play) learning apps.

CERTIFICATIONS

- Microsoft Certified: Azure Security Engineer Associate (AZ-500)
- Microsoft Certified: Azure Fundamentals (AZ-900)

EDUCATION

M.Sc. Digital Forensics and Information Security **2017 – 2019**

Gujarat Forensic Sciences University (now NFSU) | Gandhinagar, India

BCA, IT Infrastructure Management and Cloud Technology **2014 – 2017**

Poornima University | Jaipur, India