

SHIVAM SARASWAT

Product Security Engineer

@ shivamsaraswat044@gmail.com
shivamsaraswat.com

+91-9084280701

shivamsaraswat

Bengaluru, Karnataka

shivamsaraswat

PROFESSIONAL SUMMARY

Accomplished DevSecOps and Cybersecurity professional with 3.5+ years of expertise in architecting enterprise-grade security solutions and driving cloud-native implementations. Demonstrated ability to build and optimize secure pipelines for large-scale environments, develop innovative in-house security tools, and implement cloud security best practices. Proven track record of reducing security risks, streamlining compliance processes, and enhancing developer productivity through innovative tools and workflows. Committed to bridging the gap between development and security to create resilient, scalable, and efficient systems.

EXPERIENCE

Senior Cybersecurity Engineer

PayPal

April 2025 – Ongoing

Bengaluru, Karnataka

- Architected Container Security Framework & Security Policies:** Spearheaded unified container-scanning framework, standardizing vulnerability checks for Docker images across all development teams while designing and enforcing security policies to achieve 100% compliance and accelerate remediation cycles.
- Orchestrated CI/CD-Native Security Enforcement:** Integrated container security scans into CI/CD pipelines automating checks that block non-compliant images and improving vulnerability detection by 50%.
- Led Container Scanning Tool Evaluation:** Conducted comparative analysis of industry tools across detection accuracy, performance impact, cost, and API support, and piloting top choice to boost scan throughput without affecting pipeline SLAs.
- Architected End-to-End Third-Party Vendor Image Scanning Framework:** Designed comprehensive security solution including automated CI/CD Pipeline templates, and developer documentation, establishing standardized onboarding workflow for external vendor container images across the organization.
- Built Intelligent Vulnerability Deduplication & Differentiation System:** Engineered an automated CVE-, package name-, and version-based deduplication solution across Container and SCA scanners and developed an image layer-based vulnerability analysis system—eliminating duplicate findings, reducing alert fatigue, and improving patch efficiency by 30%.
- Led Cross-Language Vulnerability Research:** Investigated and documented complex security scenarios including Go vulnerabilities appearing in Node.js applications and build-time versus runtime exploitability, providing clarity on risk assessment and remediation prioritization.
- Researched Supply Chain Attack Prevention:** Evaluated and documented malicious package detection capabilities in JFrog Xray policies, establishing additional security layers for preventing supply chain attacks in containerized environments.
- Developed Comprehensive Container Security Documentation Hub:** Established a centralized knowledge hub, authored key Architecture Decision Records (ADRs) for container scanning, and created technical integration docs for JFrog Xray and Harness OPA policies—reducing onboarding time by 40% and streamlining security operations.

EDUCATION

B.Tech in Computer Science and Engineering (Cyber Security)

GLA University, Mathura

May 2022

8.25 CGPA

SKILLS

Security Expertise:

- DevSecOps & AppSec:** SSDLC, Container Security, Application Security, Cloud Security, Vulnerability Management, Policy as Code, Supply Chain Security
- Security Frameworks:** OWASP Top 10, Threat Modeling, Secure Code Review
- Vulnerability Research:** CVE Analysis, Security Research, Root Cause Analysis (RCA), Vulnerability Triage & Prioritization

Security Tools & Platforms:

- SAST:** Semgrep, CodeQL (GHAS), Bandit
- SCA & Dependency Management:** Dependabot, Renovatebot, SBOM (Syft), Dependency-Track
- Secret Scanning:** Gitleaks, TruffleHog, GitHub Advanced Security, Talisman
- Container Security:** JFrog Xray, Trivy, Hadolint
- DAST & Security Testing:** Nuclei, OWASP ZAP, Burp Suite Professional
- Network & Vulnerability Scanning:** Nmap, Nessus, Wireshark
- Monitoring & Observability:** Elasticsearch, New Relic, Datadog

Core Technical Skills:

- Programming & Scripting:** Python, Bash, PowerShell, Git
- Cloud & Infrastructure:** Google Cloud, AWS, Docker, Kubernetes (K8s)
- CI/CD & DevOps:** GitHub Actions, GitLab CI/CD, Harness CI/CD
- Databases & APIs:** MongoDB, REST APIs, Swagger, Postman

Security Engineer

Tekion

⌚ August 2024 – March 2025 ⚖ Bengaluru, Karnataka

- **Architecting DevSecOps Pipelines:** Architected and implemented comprehensive DevSecOps security scanning pipelines across 2,000+ production repositories, integrating SAST, SCA, Secret Scanning, Container Scanning and Dockerfile Scanning, resulting in 40% reduction in security vulnerabilities.
- **DevSecOps Pipelines Migration:** Led the migration of 2,000+ production repositories to GitLab's Pipeline Execution Policy, ensuring seamless transition with zero production disruption.
- **Pipeline Optimization & Developer Collaboration:** Optimized pipeline execution time by 35% through workflow and configuration enhancements, while refining pipeline templates based on systematic troubleshooting and developer feedback to improve overall efficiency and developer experience.

Product Security Engineer

IKEA

⌚ April 2023 – August 2024 ⚖ Bengaluru, Karnataka

- **Architecting Security Solution & Deployment:** Engineered an in-house Automated Web and API Security Monitoring Solution, reducing external engagement costs by 20% through improved responsible disclosure programs. Orchestrated cloud deployment using GitHub Actions, Cloud Run, and Artifact Registry.
- **SSDLC Automation & Integration:** Key architect for developing "Argos", an organization-wide proactive automated SSDLC maturity model. This includes one-click enablement via platform engineering, instant on-demand security assessment, security maturity score, actionable insights for better decision-making and automated secure template integration for developers.
- **Collaborative Innovation & Pioneering Exploration (PoC):** Spearheaded collaborative R&D initiatives with cross-functional engineering teams to enhance IKEA's product security infrastructure by integrating advanced tools into CI/CD pipelines and prototyping cloud-first security architectures, resulting in a 30% improvement in overall security posture.
- **Automated Cloud Vulnerability Management & Visualization:** Built an end-to-end triage and notification system with centralized dashboard for Google Security Command Center (SCC) that slashed critical-issue response time by 40%.
- **Governance, Controls & Documentation:** Architected Google Cloud access-control policies and optimized vulnerability workflows, while maintaining comprehensive investigation and research documentation to drive informed mitigation decisions.
- **Shadow IT Asset Management:** Resolved numerous DNS dangling issues associated with shadow IT assets, preventing potential subdomain takeovers.
- **Managed Bug Bounty Program:** Investigated and resolved multiple issues reported by external Security Researchers.
- **Security Awareness:** Delivered 10+ engaging sessions with actionable cybersecurity strategies to non-security co-workers.

ACCOMPLISHMENTS



Best Security Product of the Year
2nd Annual Cyber Security Excellence Awards 2023 by Quantic India



Hackathon Runner Up
IKEA's InnerSource Hackathon 2024



Speaker at Disobey Conference
Selected to present on – "Guarding Your Digital Realm: Heimdall – Your Shield in the World of Web and API Security" at the largest Nordic Security Event in Helsinki, Finland - 2024



Top 1% (God Rank) on TryHackMe
Completed 120+ rooms on DevSecOps, Pentesting, CTFs, OWASP Top 10, etc.

PERSONAL PROJECTS



SeCoRA (Secure Code Review AI Agent)
An AI-powered tool for detecting and remediating security vulnerabilities in codebases

PUBLICATIONS



Conference Proceedings

- A. Tiwari, S. Saraswat, U. Dixit, and S. Pandey, "Refinements in zeek intrusion detection system," in 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, 2022, pp. 974–979. DOI: 10.1109/ICACCS54159.2022.9785047.

Security Automation Engineer

BreachLock

⌚ March 2022 - April 2023

📍 Noida, UP

- **Cyber Threat Research & Automation Code:** Researched on the latest cybersecurity threats and devised automation code for Vulnerability Scanners and External Attack Surface Management (EASM) platform.
- **Vulnerability Scanner Enhancement:** Enhanced Automated Vulnerability Scanner effectiveness by analyzing and incorporating insights from Pentester-discovered vulnerabilities, ensuring continuous improvement.
- **Security Automation & Testing:** Developed modular and efficient security automation plugins with comprehensive documentation and robust test cases using Pytest to ensure optimal functionality, scalability, and reliability of the Scanner.

CERTIFICATIONS

- EC-Council - Certified Ethical Hacker (Practical)
- IBM - Cyber Security Graduate
- PentesterLab - Unix Badge
- Fortinet - NSE 1 Network Security Associate

LANGUAGES

English

Hindi

