SHIVAM SARASWAT

Product Security Engineer

shivamsaraswat044@gmail.com +91-9084280701 Bengaluru, Karnataka
shivamsaraswat.com shivamsaraswat shivamsaraswat

PROFESSIONAL SUMMARY

Experienced DevSecOps and Cybersecurity professional with 3 years of expertise in architecting enterprise-grade security solutions and driving cloud-native implementations. Skilled at building and optimizing secure pipelines for large-scale environments, creating innovative in-house security tools, and implementing cloud security best practices. Recognized speaker at global security events and recipient of industry awards for excellence in product security. Proven ability to reduce security risks, streamline compliance processes, and enhance developer productivity through innovative tools and workflows. Committed to bridging the gap between development and security to create resilient, scalable, and efficient systems.

EXPERIENCE

Security Engineer

Tekion

August 2024 – Ongoing 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 large-scale migration to GitLab's Pipeline Execution Policy from legacy compliance pipelines for 2000+ production repositories, modernizing security scanning processes while ensuring zero production disruption.
- **Pipeline Optimization**: Reduced pipeline execution time by 35% through optimization of security scanning workflows and configuration improvements.
- **Developer Feedback**: Enhanced DevSecOps pipeline templates through systematic troubleshooting and developer feedback, streamlining security scanning workflows and improving developer experience with optimized configurations.

Product Security Engineer

IKEA

April 2023 – August 2024 Bengaluru, Karnataka

- **Architecting Security Solution & Deployment**: Engineered Heimdall, 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, ensuring seamless functionality.
- **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**: Worked with Engineering teams to pioneer R&D efforts aimed at significantly strengthening IKEA's product security infrastructure, integrating advanced tools into CI/CD pipelines.

EDUCATION

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

GLA University, Mathura

May 2022 8.25 CGPA

SKILLS

Security Expertise:

- DevSecOps, Application Security, Product Security, Security Automation, Cloud Security, Vulnerability Management
- OWASP Top 10, Secure Code Review, Policy as Code, Pentesting (Web, Network), Threat Modelling

Security Tools & Platforms:

- **SAST:** Semgrep, CodeQL (GHAS), GitLab Advanced SAST, Bandit
- **SCA:** Dependabot (GHAS), Gemnasium (GitLab)
- **Secret Scanning:** Gitleaks, TruffleHog, GHAS, Talisman
- **DAST:** Nuclei, Nuclei Templates, OWASP Zap
- **Container Security:** Trivy, Dockle, Hadolint
- **Security Testing:** Burp Suite, Wireshark, Nmap, Nessus
- **Monitoring Tools:** Elasticsearch (ELK), New Relic

Development & Infrastructure:

- **Scripting:** Python, Go, Bash, PowerShell
- **Cloud Platforms:** GCP, AWS
- **CI/CD:** GitHub Actions, GitLab CI/CD
- **Containers & Orchestration:** Docker, Kubernetes (K8S)
- **Version Control:** Git, GitHub, GitLab, BitBucket
- **Database:** MongoDB
- **API Tools:** Swagger, Postman
- **OS:** Linux, MacOS, Windows

- **Pioneering Exploration (PoC)**: Led cross-functional teams in prototyping and implementing cloud-first security architecture, resulting in 30% improvement in security posture.
- **Automated Vulnerability Management**: Reduced average response time to critical issues by 40% by streamlining the extraction of critical issues from Google Security Command Center (SCC), integrating real-time Slack notifications, and implementing a centralized dashboard for efficient triaging, follow-ups, and patching.
- **Operationalize Cloud Security**: Pioneered Google Cloud access control policies and best practices. Led cloud vulnerability management, prioritizing fixes, detecting false positives, and reporting to stakeholders. Visualized vulnerabilities on an internal dashboard to deduce trends and make informed decisions for mitigation.
- **Detailed Documentation**: Thoroughly documented Cloud Security findings investigations and research.
- **Shadow IT Asset Management**: Resolved numerous DNS dangling issues associated with shadow IT assets, which were critical in preventing potential subdomain takeovers.
- **Bug Bounty Program Management**: Investigated and resolved multiple issues reported by external Security Researchers on the Bug Bounty program.
- **Comprehensive Security Assessments**: Conducted regular Pentesting, Threat Modeling, and Secure Code Reviews for Internal Products.
- **Security Awareness**: Delivered 10+ engaging sessions with actionable cybersecurity strategies to non-security co-workers.

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 the effectiveness of the Automated Vulnerability Scanner by meticulously analyzing and incorporating insights from Pentester-discovered vulnerabilities, ensuring continuous improvement.
- **Modular Security Automation Code**: Developed modular and efficient code for security automation plugins, optimizing functionality and scalability while ensuring comprehensive documentation.
- **Test Case Development**: Created comprehensive test cases using Pytest, ensuring robust and reliable performance of the Scanner.
- **Microservice API Development**: Designed and implemented Backend Microservice APIs using Swagger, Postman, Flask, and MongoDB, contributing to the creation of a resilient and responsive ecosystem for security tools.

ACCOMPLISHMENTS

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

InnerSource Hackathon Runner Up
Achieved 1st runner up in IKEA's InnerSource Hackathon 2024

Speaker at Disobey 2024 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

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

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.

CERTIFICATIONS

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

LANGUAGES

English
Hindi