Shivang P Swain

Bengaluru, IN · me@shivangswain.com · shivangswain.com · linkedin.com/in/shivangswain

Professional Summary

Security engineer specializing in AI platform security, cloud infrastructure, and container ecosystems with more than 4 years of experience. Proven track record in threat modelling, building scalable security guardrails, and enabling secure AI innovation across AWS, GCP, and Kubernetes environments. Strong foundation in risk assessment and secure architecture design that ensure robust protection for complex data pipelines and model deployments.

Work Experience

Goldman Sachs — Bengaluru, India

Senior Security Architect – AI Security (Associate) — Jan 2025 – Present

- Leading AI platform security initiatives by developing risk models and secure architecture designs for GenAI and LLM integrations, directly addressing data leakage and prompt injection risks.
- Devising novel security controls and firm-wide standards for agentic AI use cases to curb escalation of privileges and lack of attribution during agent execution.
- Collaborating with cross-functional engineering teams to implement guardrails for ML pipelines, automating security controls to support rapid innovation while maintaining regulatory compliance.
- Partnering with engineering teams to remediate enterprise risks and strengthen regulatory readiness.

Security Architect – GCP & Container Security (Analyst) — Jul 2022 – Dec 2024

- Threat modelled OpenShift container platform strengthening Kubernetes configurations and workload isolation.
- Built AWS CDK guardrails to standardize security across ECS and EKS environments.
- Conducted comprehensive security reviews and governance for flagship data platforms built on Google BigQuery and Spanner, ensuring alignment with enterprise risk standards.
- Drove GCP security posture improvements by developing platform guardrails, service guidance, and risk models for critical workloads.

Core Skills

AI, Platform & Application Security: AI Security, LLM Risk Mitigation, OWASP Top 10, OWASP LLM Top 10, Threat Modelling, Secure Architecture, Prompt Injection Defense, Data Leakage Prevention

Frameworks & Standards: NIST SP 800-53, NIST AI RMF, ISO 27001, CIS Benchmarks, STRIDE

Cloud & Platforms: Amazon Web Services, Google Cloud Platform, Kubernetes, Red Hat OpenShift, Container Security, IAM, Secrets Management

Engineering & Automation: Python, REST APIs, Git, YAML, Bash, CI/CD Concepts, Infrastructure as Code

Education & Certifications

B.Tech in Information Technology · Veer Surendra Sai University of Technology — Aug 2018 – Jul 2022

CompTIA Security+ CE Certification · CompTIA — Jul 2024

Additional Strengths

- Strong understanding of AI/ML security risks and secure deployment considerations.
- Experience in cross-functional collaboration with engineering, platform and compliance teams.
- Adaptive to translating security requirements into scalable engineering controls.