Shivang P Swain

Bengaluru, India

shivangswain.com · me@shivangswain.com · in shivangswain

Summary

Security Engineer with 2.5+ years of experience excelling in threat analysis, threat modelling, and implementing robust security controls across container, cloud, and AI platforms. Proven ability to collaborate effectively across teams, ensuring timely risk remediation and strong compliance posture. Passionate about proactively identifying emerging threats for effective risk identification and mitigation.

Experience

Associate

Goldman Sachs · *Platform Security*

Jan 2024 - Present
Bengaluru, India

- **Enhanced AI platform security**, collaborating closely with cross-functional stakeholders to mitigate vulnerabilities ahead of SLA timelines.
- **Engineered detective guardrails** (custom SHA modules) significantly improving GCP security visibility.
- Successfully **secured the launch of the firm's critical CTL ledger platform** on GCP, ensuring compliance and robust protection against threats.

Analyst

Goldman Sachs · *Platform Security*

Jul 2022 - Dec 2024
Bengaluru, India

- Performed **threat modelling of firm's OpenShift platform**, devising and implementing **20+ essential security controls** for High-Risk Applications.
- Led security assessments for all SRE platforms & projects, achieving a **100% security hygiene score** for their flagship BigQuery-based product's roll-out.
- Developed **60+ preventative guardrails** for Gatekeeper to safeguard critical GCP resources.
- Collaborated with app teams to **remediate over 200 security findings** under regulatory scrutiny.
- **Led TLS Upliftment initiative**, securing over 13,000 internal VM hosts reducing their exposure.

Front-End Intern

Airblack · *Engineering*

Jan 2022 - Jun 2022
Gurugram, India

Education

Veer Surendra Sai University of Technology

BTech, Information Technology · 2018 - 2022

Licenses & certifications

CompTIA Security+

CompTIA · Issued Jul 2024

Show credential

Skills

Standards	NIST SP 800-53 · ISO/IEC 27001 · NIST AI RMF · OWASP · STRIDE Framework
Expertise	Threat Modelling · Control Development · Threat Analysis · Threat Assessment · Risk Management · Regulatory Compliance
Domains	Cloud Security · AI Security · Container Security
Areas of Focus	Identity & Access Management (IAM) · Network Security · Data Security · Information Security Secure SDLC · Business Continuity & Resiliency Planning
Technologies	Google Cloud Platform (GCP) · Amazon Web Services (AWS) · Kubernetes · OpenShift · Python JavaScript/TypeScript · C/C++ · Nix · Git · Bash