

Saksham Goyal

📍 Delhi, India | 📞 +918923220689 | 📧 Sakshamgoyal0301@gmail.com | GitHub: <http://github.com/sakshamgoyal01>

SUMMARY

Entry-level DevSecOps Engineer with hands-on experience in building automated security workflows using AI-driven threat detection, infrastructure as code, and cloud-native technologies. Skilled in integrating tools like Jenkins, Trivy, and SonarQube into CI/CD pipelines. Proficient in IaC using Terraform on AWS and Kubernetes, with expertise in building LLM-powered security co-pilots and implementing Zero Trust architectures for scalable, secure deployments.

TECHNICAL PROFICIENCIES

Programming & Scripting: Python, Bash, YAML, Regular Expressions

Cloud & IaC: AWS, Terraform, MicroK8s, EC2, VPC, S3, EKS, IAM, GuardDuty, Verified Access

DevSecOps: Jenkins, GitHub Actions, GitLab CI, Docker, Kubernetes, Trivy, Syft, Grype, SonarQube

Monitoring & Security: Prometheus, Grafana, Falco, Loki, OPA/Gatekeeper, WAF, Secrets Manager

LLM/ML: HuggingFace, LangChain, OpenAI, Sentence Transformers, Pinecone, Weaviate, PyTorch

Tools: VSCode, Streamlit, Jupyter, DVC, MLflow, ArgoCD

RELEVANT PROJECT EXPERIENCE

AI-SOC Co-Pilot

June 2025

- Engineered an LLM-powered SOC platform on Kubernetes for real-time threat detection and automated incident response.
- Achieved continuous vulnerability management using Trivy, Syft, and SonarQube, along with automated SBOM generation.

TestPilot – AI SaaS Testing & QA Platform

May 2025

- Built AI test platform with LLM-based code reviews, risk scoring, and CI/CD integration (Trivy, Syft, OPA).
- Boosted release stability with automated testing, compliance, and Slack alerts.

Zero Trust DevSecOps Pipeline

April 2025

- Designed full CI/CD pipeline with Jenkins, GitHub Actions, Trivy, Syft, SBOM & container scanning
- Deployed workloads to MicroK8s on EC2 using Terraform, secured with AWS Verified Access & GuardDuty.

Web-Application-pentesting-suite

March 2025

- Built a modular Python tool to scan and visualize OWASP Top 10 vulnerabilities on apps like DVWA, bWAPP, Juice Shop.

EDUCATION

B.Tech, Computer Science Engineering

Specialization: CSE (Artificial Intelligence & Machine Learning) | Cyber Security (hons.)

Dr. A.P.J. Abdul Kalam Technical University, Uttar Pradesh, India

CERTIFICATIONS

Microsoft

May 2025

AZ-400: Development for enterprise DevOps

- Demonstrates expertise in enterprise DevOps practices and Azure development (AZ-400).

FORAGE - AWS

December 2024

Solutions Architecture Job Simulation

- Devised a scalable AWS Elastic Beanstalk solution to resolve growth and performance challenges, delivering clear client communication on architecture and costs.

Generative AI Fundamentals

December 2023

Google Cloud (Skill Badge)

- Skilled in Generative AI, with hands-on expertise in model design, fine-tuning (OpenAI GPT, LangChain, DeepSeek, Gemini), and advanced prompt engineering for varied use cases.

ACHIEVEMENTS

- Developed 5+ open-source security tools on GitHub across DevSecOps, LLM security, and infrastructure automation domains.
- Projects include AI-SOC Co-Pilot and TestPilot, addressing SBOM compliance, vulnerability scanning, and zero-trust enforcement.