

DEV V JOSHI

📍 Chennai, Chennai, Tamil Nadu ✉ devvjoshi2005@gmail.com ☎ +918778734365 📄 in/devjoshi2005

SUMMARY

Computer Science engineering student with hands-on experience in cloud security architecture, DevSecOps, and GRC compliance across AWS, GCP, and Azure. Engineered production-grade CI/CD security pipelines reducing remediation time by 99.5% using AI-powered automation. Skilled in Infrastructure-as-Code, SAST/DAST integration and incident response. Seeking Associate Cloud Security Engineer internship.

EXPERIENCE

Cybersecurity Job Simulation - Deloitte

Forage

1st July 2025 - 7th July 2025

- Investigated a simulated breach at a manufacturing client — dug through raw web request logs and found a user ID making perfectly timed hourly API calls with zero front-end activity, which is not how humans browse.
- Traced the suspicious traffic to an internal IP behind VPN — ruled out external attacker, confirmed insider threat scenario consistent with credential compromise or automated scraping.
- Built an incident report documenting the attack chain, evidence trail, and recommended fixes including session invalidation and VPN access review for the security team.

PROJECT

DevSecOps Container Remediation Engine

devjoshi2005/DevSecOps-Container-RemediationProject

- Plugged AWS Bedrock into the vulnerability pipeline so container CVEs get patched automatically — MTTR dropped from 48 hours to 2.3 seconds.
- Built the full CI/CD security chain: SonarQube for code, OWASP ZAP for runtime, Trivy for container images — all triggering before deploy.
- Terraform handles the entire ECS infrastructure; when Bedrock generates a fix, it auto-opens a GitHub PR — no human in the loop needed & also implemented AWS Inspector for Post-Deployment Vulnerability Assessment.

Multi-Cloud GRC Compliance & Remediation Engine

devjoshi2005/Grc-Compliance-Engine

- Built a GRC engine that puts a rupee value on every compliance gap — flagged 1.7Cr (\$20K) in exposure across AWS and Azure resources.
- Auditors used to wait 3 days for compliance answers; the Llama_Index + ChromaDB RAG system now returns cited responses in seconds.
- Evidence collection for SOC2, NIST, and ISO 27001 runs automatically — pulls configs, logs, and policy docs without manual screenshots.

Google Cloud Security Environment

devjoshi2005/Google-Cloud-Security-Environment

- Set up a full Zero Trust environment on GCP covering 5 security domains — IAM, networking, storage, VPC isolation, and monitoring.
- Cloud Armor WAF + VPC Flow Logs handle the perimeter; every inbound request and internal flow gets logged and inspected.
- Built DLP pipelines using Google's Cloud DLP API to catch and redact PII/PCI data before it leaks — mapped to GDPR and DPDPA rules.

ResilienceOps — Cloud Native Incident Response Engine

devjoshi2005/ResilienceOps

- Built a SOAR platform that pulls GuardDuty and CloudTrail events, runs them through an Isolation Forest ML model to catch anomalies, and responds to critical incidents in under 60 seconds — 99% MTTD/MTTR drop.
- Used Neo4j to map how an attacker could move laterally across cloud resources — the graph shows the full kill chain, not just isolated alerts.
- Remediation is fully automated: the system generates Terraform fixes, validates them against OPA policies, and applies containment — no manual intervention needed.

EDUCATION

Bachelor of Engineering - Computer Science

Meenakshi Sundararajan Engineering College, Chennai · Chennai · September 2023 - Present · 8.10*/10

Higher Secondary Education (XII) & (X)

Sindhi Model Senior Secondary School, Kellys, Chennai · Chennai · 2023 · 83.3%

CERTIFICATIONS

Microsoft Azure Security Engineer & Microsoft Security Fundamentals (AZ-500,SC-900)

• Implementing IAM, Platform Governance, Encryption (rest & transit), Logging/Monitoring, Cybersecurity foundations, Platform risk & governance..

AWS Fundamentals & IBM AppSec DevOps

• Cloud foundations, container security, CI/CD integration.

SKILLS

AWS (ECR, ECS, IAM, Inspector), GCP (VPC, IAM, Cloud Armor, SCC), Azure (AD, Sentinel)

DevSecOps & CI/CD Security, Container Security (Docker, Kubernetes), Zero Trust IAM, GRC Automation, Threat Detection

Python (Boto3, LLM APIs), Terraform, GitHub Actions, OPA/Rego (Policy-as-Code), Ansible, SonarQube, Trivy, OWASP ZAP, Graylog, Neo4j Aura, Temporal.io, Slack Bolt, Cloud Custodian
