# Joshua Jebaraj

joshuajebaraj.z@gmail.com | +91 7708295395 | joshuajebaraj.com |
https://www.linkedin.com/in/joshuajebaraj | https://github.com/JOSHUAJEBARAJ

DevOps Engineer with 4+ years of experience architecting cloud-native systems on AWS, with deep expertise in Infrastructure as Code (Terraform, Terragrunt), Kubernetes orchestration, and CI/CD automation (GitHub Actions). Experienced in zero-downtime migrations, fault-tolerant architecture design, and operating production workloads at scale.

## EXPERIENCE

**Cognara** | DevOps Engineer (Contract) | *May 2025-Aug 2025* | *Nov 2025 - April 2026*

- Built a reusable EKS-based data migration tool (AWS DataSync, DMS, SQS) using IRSA for AWS access, with PodDisruptionBudgets and PriorityClasses to protect long-running jobs during cluster operations.
- Migrated a business-critical internal application from a single EC2 instance to a fault-tolerant ECS + RDS architecture, eliminating the single point of failure, ensuring zero-downtime resilience, and replacing hardcoded AWS credentials with ECS task roles for keyless access to AWS services
- Migrated 150+ alerts from legacy Icinga to Prometheus, modernizing the observability stack and establishing a unified monitoring foundation

**arch0** | Cloud Integration Engineer | *November 2023 - February 2025*

- Automated infrastructure provisioning across dev, staging, and production AWS environments using Terraform and Terragrunt with GitHub Actions (OIDC-authenticated, no long-lived AWS keys), reducing environment setup time by 85% and enabling consistent, repeatable deployments at scale.
- Expanded the CSPM platform's coverage by building GCP, GitHub, and Google Workspace integrations from scratch.
- Developed 30+ automated GCP security checks for the core CSPM engine, enabling customers to proactively detect and remediate misconfigurations across their cloud environments.

**we45** | Cloud Native Security Lead | *June 2021 - August 2023*

- Designed the first GCP sandbox on AppSecEngineer with per-student isolation provisioning a dedicated GCP project and Workspace user per learner, with Organization Policy constraints restricting blast radius
- Authored 50+ hands-on GCP and Kubernetes security labs covering IAM, network security, KMS, Secret Manager, Kubernetes workload security, and runtime/policy enforcement using Falco and Kyverno
- Developed and delivered Google Cloud and Kubernetes security training to 200+ clients across international conferences and private sessions, including Black Hat.

## CORE COMPETENCIES

**AWS**: IAM, ECS, EKS, EC2, S3, RDS, Lambda, SQS, SNS, DMS, DataSync, ECR, Secrets Manager, Parameter Store, KMS, CloudTrail, GuardDuty, Security Hub, VPC

**GCP**: IAM, GCS, BigQuery, Compute Engine, GKE, KMS, Secret Manager, Organization Policy

**Container & Orchestration**: Docker, Kubernetes,Helm

**Observability**: Prometheus, Grafana, Loki, Mimir, Alloy

**CI/CD & IAC**: GitHub Actions, GitLab CI, Terraform, Terragrunt,Ansible

**Programming**: Python, Go, Bash

## PROJECTS

**GCP-Goat**

A deliberately vulnerable GCP environment for learning cloud security, covering IAM privilege escalation, GCS misconfigurations, hardcoded service account credentials, and GKE attack scenarios Featured at DEF CON Cloud Village and Hack In The Box Armory.

## OPEN SOURCE & TALKS

**Speaker/Trainer:**

- **DEF CON Cloud Village** - Understanding Common Google Cloud Misconfigurations using GCP-Goat
- **Hack In The Box Armory** - GCP-Goat (Tool Showcase)
- **OWASP Seasides** - Introduction to Building & Securing your CI/CD Pipelines

**Contributor:**

- **Prowler:** Fixed false positive GCP security checks in Prowler, an open-source cloud security tool used by thousands of companies worldwide (link)

## CERTIFICATIONS

**Google Cloud Certified - Associate Cloud Engineer**

## EDUCATION

**M.Tech Software Engineering (Integrated)** - Vellore Institute of Technology, Chennai | CGPA: 8.9