Sharath S Naik

Senior Cloud Security & DevSecOps Engineer

Bengaluru, India

sharathnaik.contact@gmail.com | +91-8296237529

linkedin.com/in/sharath029

PROFESSIONAL SUMMARY

Cloud Security & DevSecOps Engineer with 3+ years of experience securing and scaling AWS and Azure environments. Specialized in Kubernetes (EKS/AKS), Terraform-based Infrastructure as Code, CI/CD security automation (SAST/DAST), IAM governance, and Zero Trust architecture. Improved security posture through AWS Security Hub, Azure Defender, and SIEM integrations while optimizing cloud spend by 50%. Experienced in SOC 2 and ISO 27001 compliance, audit automation, and secure Platform Engineering practices.

TECHNICAL SKILLS

Cloud Platforms: AWS, Azure

Compute & Containers: Kubernetes, EKS, AKS, Docker, Helm

Infrastructure as Code: Terraform, CloudFormation, Ansible

CI/CD & GitOps: Jenkins, GitHub Actions, GitLab CI, AWS CodePipeline, ArgoCD

Cloud Security: IAM, AWS Security Hub, GuardDuty, CloudTrail, AWS WAF, Azure Defender, Azure Sentinel, Zero Trust

Application Security: SAST, DAST, SonarQube, OWASP ZAP, Trivy

Compliance Frameworks: SOC 2, ISO 27001, CIS Benchmarks, NIST

Secrets & Key Management: HashiCorp Vault, Secrets Management, AWS KMS

Monitoring & SIEM: Prometheus, Grafana, CloudWatch, ELK, SIEM

FinOps: Cost Governance, Budget Monitoring, Resource Optimization

Languages: Python, Bash

PROFESSIONAL EXPERIENCE

Senior Cloud Security & DevSecOps Engineer

Mareana, Inc. | Mar 2023 – Present | AWS

- Strengthened AWS IAM governance across multi-account architecture using AWS Organizations and AWS Config, decreasing privilege sprawl by 30%.
- Consolidated AWS Security Hub, GuardDuty, and CloudTrail findings into centralized dashboards, improving threat visibility and compliance tracking.
- Configured AWS WAF managed rules and rate controls to secure public-facing workloads from OWASP Top 10 vulnerabilities.
- Engineered Terraform-based landing zones aligned with CIS Benchmarks and NIST controls, accelerating provisioning cycles from days to under 2 hours.
- Embedded SAST and DAST security gates into Jenkins pipelines, cutting critical vulnerabilities in production by 35%.
- Hardened EKS clusters using RBAC, Network Policies, OPA/Kyverno admission controls, and signed container image validation.
- Supported Vault-based Secrets Management implementation for dynamic credential rotation in CI/CD workflows.
- Contributed to Incident Response procedures by analyzing SIEM alerts and coordinating remediation workflows.
- Optimized infrastructure utilization through automated FinOps workflows, reducing monthly AWS spend by 50%.
- Enabled audit readiness for SOC 2 and ISO 27001 through automated evidence generation and compliance-as-code validation.

Senior Cloud Security & DevSecOps Engineer

Johnson & Johnson (Client Engagement) | Mar 2023 – Present | Azure

- Delivered secure AKS environments using Helm-driven blue/green deployment strategies, ensuring uninterrupted releases.
- Leveraged Azure Defender and Azure Sentinel for centralized SIEM monitoring and proactive threat detection.

- Integrated SAST, DAST, and container security scanning into CI/CD workflows using Jenkins and GitHub Actions, lowering security violations by 33%.
- Implemented Azure RBAC and Zero Trust access policies for multi-tenant workloads.
- Automated Terraform-based environment provisioning, improving deployment efficiency by 40%.
- Established observability stack using Prometheus and Grafana, maintaining MTTR under 2 hours.
- Participated in Threat Modeling sessions during new service design and architecture reviews.

Senior Cloud Security & DevSecOps Engineer

Kenvue (Client Engagement) | Mar 2023 – Present | Azure

- Built hardened AKS container platforms with secure image lifecycle management and compliance controls.
- Implemented GitOps workflows using ArgoCD to automate Kubernetes deployments with rollback capabilities.
- Standardized Infrastructure as Code modules to support Platform Engineering self-service environments.
- Introduced cost governance automation across storage and compute services, lowering cloud expenditure by 50%.
- Sustained zero-downtime patch management and audit-compliant configurations across environments.

KEY INITIATIVES

DevSecOps Modernization

- Developed enterprise CI/CD framework integrating Terraform, Kubernetes, SAST, DAST, and supply chain validation.
- Increased deployment velocity by 60% while preserving security compliance.

Security & Compliance Automation

- Implemented CIS Benchmark alignment and NIST-based control mapping.
- Enhanced compliance visibility through SIEM integration and centralized logging.

FinOps Optimization

- Automated idle resource detection and policy enforcement.
- Reduced operational waste while maintaining SLA commitments.

CERTIFICATIONS

- AWS Certified Solutions Architect – In Progress
- Certified Kubernetes Administrator (CKA) – In Progress
- Terraform Associate – In Progress

EDUCATION

Bachelor of Engineering (B.E.)

Visvesvaraya Technological University | 2022