

Anurag Vaidhya

anuragvaidhya786@gmail.com | +61451228653 | www.anuragvaidhya.com | Melbourne, Australia

Professional Summary

DevSecOps & Cloud Engineering Leader | Platform Engineering | Automation | Cloud Transformation

Experienced **DevSecOps, Platform and Cloud Engineering Leader** with **14+ years of hands-on expertise** in designing, automating, and securing **scalable cloud infrastructures**. A trusted expert in **platform engineering, security automation, and cloud-native architecture**, with a proven track record of **embedding security into engineering workflows while accelerating development velocity**.

A leader who thrives at the intersection of **security, automation, and cloud infrastructure**, driving **resilient, compliant, and high-performing platforms**. Adept at **balancing strategic vision with deep technical execution**, ensuring security and performance go hand in hand.

Hands-On Technical Expertise & Execution

- ◆ **CI/CD & Automation:** Designed and developed **CI/CD pipelines** with integrated security controls, automating **build, test, and deployment** processes for secure, high-velocity releases.
- ◆ **Infrastructure as Code (IaC):** Hands-on experience in **writing and managing IaC (Terraform, CloudFormation, CDK)** to automate cloud infrastructure provisioning and policy enforcement.
- ◆ **Cloud Landing Zones:** Designed and implemented **secure, scalable Cloud Landing Zones**, ensuring **standardized, compliant, and multi-account cloud environments** for enterprises.
- ◆ **Cloud Migrations:** Led **large-scale workload migrations** from **on-premises to cloud**, ensuring **cost-efficient, secure, and seamless transitions** while modernizing infrastructure.
- ◆ **Application & Container Security:** Integrated **SAST, DAST, SCA, and container security tools** into CI/CD pipelines to **proactively detect and remediate vulnerabilities** across the software supply chain.
- ◆ **Kubernetes & Platform Engineering:** Deep hands-on experience with **Kubernetes, Docker, and service mesh technologies (Istio,)** to **orchestrate, secure, and scale containerized applications**.

- ◆ **Monitoring & Observability:** Designed and deployed **end-to-end monitoring and logging solutions** using **centralized logging, distributed tracing, and SIEM platforms**, ensuring **real-time visibility and threat detection**.
- ◆ **Scalable Cloud Architectures:** Designed and optimized **highly available, fault-tolerant, and resilient cloud-native architectures**, ensuring **scalability, performance, and security best practices**

Leadership & Cloud Security Strategy

- ✓ Built and scaled **DevSecOps & Platform Engineering teams**, driving a culture of **automation, security-first development, and operational excellence**.
- ✓ Led **end-to-end cloud transformations**, enabling **secure, scalable, and cost-efficient adoption** of cloud services while ensuring compliance with industry standards (**ISO 27001, SOC2, GDPR, NIST**).
- ✓ Designed and implemented **enterprise-wide security automation strategies**, embedding **policy-as-code, security-as-code, and compliance-as-code** to reduce risk and improve developer efficiency.
- ✓ Partnered with **engineering, security, and C-level stakeholders** to align **cloud, DevOps, security, and business goals**, ensuring security supports innovation rather than slowing it down.

Business Impact & Innovation

- 🚀 **Bridged security and engineering**, implementing **frictionless security** that enhances rather than hinders development workflows.
 - 🚀 **Reduced security incidents and vulnerabilities** through **proactive automation, continuous monitoring, and AI-driven anomaly detection**.
 - 🚀 **Enabled faster and more secure deployments** by **automating security, compliance, and infrastructure provisioning**.
 - 🚀 **Mentored and upskilled engineering teams**, fostering a **culture of security awareness, DevSecOps best practices, and automation-first thinking**.
-

Key Skills & Expertise

Cloud & Platform Engineering

- ✓ **Cloud Platforms:** AWS, GCP (Google Cloud Platform)
- ✓ **Cloud Architecture:** Designing highly scalable, resilient, and secure cloud-native solutions
- ✓ **Cloud Landing Zones:** Architecting secure multi-account cloud environments with

centralized security & governance

- ✓ **Cloud Migration:** Leading on-premises to cloud migrations, ensuring cost-efficient and seamless transitions
- ✓ **Multi-Cloud & Hybrid Cloud Strategies**

DevSecOps & Security Automation

- ✓ **Security in CI/CD:** Embedding security at every stage of the pipeline
- ✓ **Application Security Scanning:**
 - SAST (Static Application Security Testing): SonarQube, Checkmarx, Fortify.
 - DAST (Dynamic Application Security Testing): OWASP ZAP
 - SCA (Software Composition Analysis): Snyk, Black Duck.
- ✓ **Container & Kubernetes Security:**
 - Container Image Scanning: Trivy, Snyk
 - Runtime Security & Policy Enforcement: Gatekeeper
- ✓ **Cloud Security Posture Management (CSPM):** Enhancing AWS & GCP security postures with automated guardrails
- ✓ **Zero-Trust Security:** Implementing identity-driven access controls, least privilege models, and secure service-to-service communication
- ✓ **Security-as-Code:** Automating policy-as-code, compliance-as-code, and governance frameworks
- ✓ **IAM & Access Control:** Managing RBAC, ABAC, OAuth, OpenID Connect, and IAM policies

Infrastructure & Automation

- ✓ **Infrastructure as Code (IaC):** Terraform, CloudFormation, Pulumi, AWS CDK
- ✓ **Configuration Management:** Ansible, Chef, Puppet
- ✓ **Service Mesh & API Security:** Istio, Linkerd, Consul for secure service-to-service communication
- ✓ **Container Orchestration:** Kubernetes (EKS, GKE, OpenShift), Docker, Helm
- ✓ **OpenShift Platform Engineering:** Deploying and managing OpenShift clusters, optimizing security, and enabling self-service developer platforms
- ✓ **Platform Engineering:** Designing developer self-service platforms with secure, scalable infrastructure
- ✓ **Serverless Architectures:** AWS Lambda, Google Cloud Functions, Event-Driven Computing

CI/CD & Automation

- ✓ CI/CD Pipelines: Jenkins, GitHub Actions, GitLab CI/CD, ArgoCD, Tekton
- ✓ Automated Deployments: Blue-Green, Canary, A/B testing strategies
- ✓ Software Supply Chain Security: Implementing proactive security controls in CI/CD workflows

Monitoring, Logging & Observability

- ✓ Monitoring & Logging: Prometheus, Grafana, ELK (Elasticsearch, Logstash, Kibana), CloudWatch
- ✓ Tracing & Telemetry: OpenTelemetry, Jaeger, Zipkin
- ✓ SIEM & Threat Detection: Security analytics & incident response

Compliance & Governance

- ✓ Compliance Frameworks: ISO 27001, SOC2, GDPR, NIST, CIS Benchmarks
- ✓ Automated Compliance: Embedding security & compliance into cloud operations

Leadership & Strategy

- ✓ Building & Scaling High-Performing Teams: Led and mentored DevSecOps, Platform Engineering, and Cloud Security teams, fostering a culture of automation, security-first development, and operational excellence.
- ✓ Cloud & Security Strategy: Defined and executed cloud security, DevSecOps, and automation strategies, aligning engineering, security, and business goals to drive innovation.
- ✓ Cross-Functional Collaboration: Partnered with engineering, security, compliance, and C-level executives to drive secure software delivery, regulatory compliance, and operational resilience.
- ✓ Compliance & Risk Management: Ensured adherence to ISO 27001, SOC2, GDPR, NIST, and CIS Benchmarks, embedding security as a business enabler rather than a blocker.

Professional Experience

DevSecOps & Platform Engineering Lead Accenture Australia (June 2022-)

- Led the DevSecOps & Platform Engineering strategy, operationalizing multiple delivery pipelines and managing various environments (Dev, QA, UAT, Prod) with best security and scalability practices.

- Built & led high-performing DevSecOps & Platform Engineering teams, driving automation and security-first culture.
- Defined & executed cloud security and DevSecOps strategies, aligning with business and engineering goals.
- Led enterprise-scale cloud migrations, optimizing cost, security, and performance.
- Integrated security into SDLC, ensuring seamless developer experience without compromising security.
- Partnered with cross-functional teams (engineering, security, compliance, leadership) to drive secure software delivery.
- Ensured compliance with ISO 27001, SOC2, GDPR, NIST, embedding security and governance at scale.
- Architected and deployed secure, scalable cloud solutions in AWS & GCP.
- Developed Cloud Landing Zones for centralized security, IAM, and governance.
- Executed cloud migrations, ensuring cost-efficient and seamless transitions.
- Embedded security into CI/CD pipelines with SAST, DAST, SCA, and container security tools.
- Implemented Cloud Security Posture Management (CSPM) for AWS & GCP security hardening.
- Designed and enforced zero-trust security models and IAM best practices.
- Developed Infrastructure as Code (IaC) using Terraform, CloudFormation.
- Engineered secure Kubernetes (EKS, GKE, OpenShift) clusters, including service mesh (Istio).
- Deployed end-to-end monitoring & logging solutions (Prometheus, Grafana, ELK, OpenTelemetry).
- Integrated SIEM and threat detection for proactive security monitoring.

Senior DevSecOps Engineer | Platform Engineer

Cognizant Technology Solutions (Feb 2020- June 2022)

- Led DevSecOps, Cloud, and Platform Engineering initiatives, driving automation, security, and operational excellence.
- Defined and implemented cloud security, DevSecOps, and platform engineering strategies, ensuring scalability and resilience.
- Collaborated with engineering, security, and leadership teams to integrate security best practices into development workflows.
- Spearheaded cloud migration and modernization projects, ensuring performance optimization and compliance with ISO 27001, SOC2, GDPR, and NIST standards.
- Developed self-service platform engineering solutions, enabling developers to deploy securely and efficiently.

- Designed and built secure, scalable, and highly available cloud architectures in AWS & GCP.
- Developed and managed Cloud Landing Zones to enforce security policies, IAM governance, and network segmentation.
- Led workload migration from on-premises to cloud, optimizing for performance, security, and cost.
- Implemented Kubernetes and OpenShift platforms, enabling microservices, service mesh (Istio), and workload orchestration.
- Integrated security into CI/CD pipelines, automating vulnerability detection using SAST, DAST, SCA, and container security tools.
- Implemented Cloud Security Posture Management (CSPM) to continuously monitor and improve cloud security.
- Developed and enforced zero-trust security models, securing service-to-service communication and IAM policies.
- Automated security compliance as code, ensuring continuous monitoring for regulatory adherence.
- Developed Infrastructure as Code (IaC) modules using Terraform, CloudFormation, and Pulumi for automated cloud provisioning.
- Built secure Kubernetes (EKS, GKE, OpenShift) environments, implementing RBAC, network policies, and container security scanning.
- Engineered platform automation and self-service tools, enhancing developer experience and reducing deployment friction.
- Designed and implemented monitoring & logging solutions using Prometheus, Grafana, ELK, CloudWatch, and OpenTelemetry.
- Integrated SIEM and threat detection tools, enhancing security incident response and anomaly detection.
- Designed and consumed REST, GraphQL, and gRPC APIs, ensuring security best practices and optimized API performance.
- Led troubleshooting and debugging efforts using AWS CloudWatch, CloudTrail, and other logging services.

DevSecOps Engineer and Various Roles

Wipro Technologies (Feb 2011- Feb 2020)

Certifications:

- AWS Certified DevOps Engineer – Professional
 - AWS Certified Developer – Associate
 - Certified Kubernetes Application Developer (CKAD)
 - Certified Jenkins Engineer
 - Terraform Associate
 - GCP Cloud Architect – Professional (Expired)
 - ISC Scrum Master
-

Education:

Bachelor of Engineering (2006-2010)