**ADEYINKA FAJOBI** | Cloud Security | DevSecOps Engineer
United Kingdom | +44 788 216 4499 | afajobi@securedbyfajobi.com | linkedin.com/in/fajobi10 | securedbyfajobi.com

---

## PROFESSIONAL SUMMARY

DevSecOps & Cloud Security Engineer with 7+ years of experience securing AWS and Kubernetes environments, automating secure infrastructure provisioning, and embedding security into CI/CD pipelines. Proven expertise in AWS security services, Kubernetes hardening, Terraform, and GitLab. Strong track record enabling secure delivery pipelines with SAST/DAST integration, enforcing zero-trust principles, and aligning engineering with GDPR, ISO 27001, and PCI-DSS compliance frameworks.

---

## PROFESSIONAL SKILLS

- Cloud Security: AWS Security Hub, GuardDuty, Inspector, Config, KMS, IAM Analyzer, Macie, Wiz, Prisma Cloud
- Kubernetes Security: RBAC, Network Policies, Pod Security Standards, Falco, Sysdig, Trivy, Aqua, OPA/Gatekeeper
- CI/CD & DevSecOps: GitLab CI/CD, Jenkins, GitHub Actions, Argo CD, SAST/DAST (Checkmarx, OWASP ZAP, SonarQube)
- Infrastructure as Code: Terraform, CloudFormation, Ansible, GitOps, Policy-as-Code
- Containerization: Docker, Kubernetes, Helm, Istio (mTLS, traffic policies)
- Monitoring & Logging: Prometheus, Grafana, Splunk, CloudWatch, ELK, Datadog
- Programming & Scripting: Python, Bash
- Compliance: ISO 27001, GDPR, HIPAA, NIST, FedRAMP, PCI-DSS, SOC 2
- Databases: PostgreSQL, MySQL, MongoDB, DynamoDB
- Version Control: Git, GitHub, GitLab

---

## PROFESSIONAL EXPERIENCE

**SARGENT-DISC LTD UK — DevSecOps Engineer** ***Mar 2025 – Present***

- Integrated GitLab SAST/DAST and Snyk into CI/CD pipelines, detecting and remediating 95% of vulnerabilities pre-deployment, reducing post-deployment issues by 30%
- Hardened Kubernetes workloads with RBAC, Network Policies, and Pod Security Standards, achieving CIS Kubernetes Benchmark compliance and improving security posture by 25%
- Optimized Kubernetes resource allocation and AWS compute/storage usage, reducing cloud costs by 20% while maintaining performance
- Architected secure AWS environments using Terraform with GuardDuty, Inspector, Config, and KMS, automating threat detection and encryption
- Implemented GitOps with Argo CD and Helm-based standardization, eliminating configuration drift and reducing deployment errors by 35%
- Deployed Falco for runtime threat detection, reducing mean time to detection (MTTD) by 40%
- Implemented Istio service mesh for zero-trust networking with mTLS encryption and fine-grained policies
- Automated incident response using AWS Lambda/SNS, reducing mean time to resolution (MTTR) by 35%
- Automated compliance controls (IAM validation, key rotation, audit logging) to maintain GDPR and ISO 27001 alignment

Key Achievements: Achieved 99.9% infrastructure uptime, reduced container security risks by 35%, cut security tooling costs by 20%

**GIBRALTAR TECHNOLOGIES UK — Cloud Security Engineer (DevSecOps)** ***Mar 2022 – Mar 2025***

- Embedded security scanning (Snyk, Trivy, Aqua) in CI/CD pipelines, improving early detection of vulnerabilities
- Hardened Kubernetes clusters with Pod Security Standards, Network Policies, and runtime monitoring (Falco, Tracee)
- Built highly available AWS environments with Terraform, implementing auto-scaling, fault-tolerant architectures, and least-privilege IAM
- Centralized security monitoring & logging with CloudWatch, Prometheus, Grafana, and Splunk for comprehensive threat visibility
- Automated ISO 27001/GDPR reporting with AWS Config Rules and Python, reducing manual audit effort by 70%

Key Achievements: Reduced incident response time by 50%, delivered secure GitOps pipelines with policy enforcement, strengthened regulatory compliance through automated encryption and access controls

**MBL TECHNOLOGIES — DevOps Engineer** ***May 2019 – Mar 2022***

- Embedded SAST/DAST (SonarQube, OWASP ZAP, Checkmarx) in pipelines, achieving 95% vulnerability detection pre-production
- Hardened multi-tenant Kubernetes clusters with Aqua Security and Pod Security Standards, reducing runtime vulnerabilities by 40%
- Automated secure infrastructure provisioning with Terraform/Ansible, reducing manual setup time by 30%
- Enhanced runtime monitoring with Tracee and Falco, detecting anomalous container behavior in production environments
- Standardized CI/CD release pipelines, reducing build times and deployment rollbacks by 20%
- Achieved PCI-DSS compliance through TLS encryption, network segmentation, and comprehensive access logging

Key Achievements: Reduced deployment errors by 20%, automated security policy enforcement across SDLC, achieved PCI-DSS Level 1 compliance

**DELOITTE & TOUCHE LLP — Cloud/DevOps Engineer** ***Nov 2018 – May 2019***

- Migrated monolithic applications to secure microservices architecture on AWS using Docker and Kubernetes
- Automated cloud resource provisioning with CloudFormation and shell scripting, reducing operational costs by 15%
- Maintained 99.9% service availability through proactive monitoring and incident response
- Managed containerized application deployments, improving deployment efficiency and reducing downtime by 25%

---

## CERTIFICATIONS

- AWS Certified DevOps Engineer – Professional
- AWS Certified Security Specialty
- AWS Certified Solutions Architect – Associate
- Certified Kubernetes Administrator (CKA)
- HashiCorp Certified: Terraform Associate
- CompTIA Security+
- In Progress: Certified Kubernetes Security Specialist (CKS), AWS AI Practitioner

---

## EDUCATION

Graduate Certificate in Cloud Development and Operations
Conestoga College, ON, Canada

---

## NOTABLE PROJECTS

- CI/CD Automation & Security: Designed GitLab CI/CD and Argo CD pipelines with integrated security scanning (Snyk, Trivy, GitLab SAST/DAST), reducing deployment time by 60%
- Kubernetes Security Hardening: Secured high-traffic Kubernetes deployments using Falco and Aqua Security tools, reducing runtime vulnerabilities by 40%
- Service Mesh Security with Istio: Deployed Istio across Kubernetes clusters to enforce zero-trust networking via mTLS, traffic control, and runtime policy auditing
- Hybrid Network Implementation: Configured AWS Direct Connect + VPN tunnels to securely connect on-premise workloads to AWS with encrypted paths
- Web Application Firewall Tuning: Deployed AWS WAF for multiple Kubernetes-based workloads behind ALB and CloudFront, designed rule sets targeting OWASP Top 10 risks, reducing malicious traffic by 60%