
OBIANUJU OGAZIECHI

Port Harcourt | +2349038937578 | ogaziechi.o@gmail.com

PROFESSIONAL SUMMARY

Cloud Infrastructure Engineer with hands-on experience designing, deploying, automating, and securing AWS cloud environments using Infrastructure as Code, DevOps practices, and cloud security principles. Skilled in AWS services including VPC, EC2, ECS/Fargate, Application Load Balancer, Auto Scaling, IAM, S3, RDS, DynamoDB, Lambda, CloudFront, Route 53, CloudWatch, CloudTrail, Guardduty, Security Hub, AWS Config, Inspector, and WAF. Experienced in building scalable cloud architectures using Terraform, improving infrastructure reliability, and applying security best practices across identity, networking, monitoring, and application delivery. Committed to leveraging problem-solving abilities and communication skills to drive resourceful solutions in cloud environments.

SKILLS

- **Cloud Platform:** AWS (VPC, EC2, IAM, ECS/Fargate, S3, RDS, DynamoDB, ALB, CloudFront, Route 53, Auto Scaling, Budgets)
- **Infrastructure as code:** Terraform (modular architecture, infrastructure provisioning and lifecycle management, remote state, multi environment design) CloudFormation (familiarity)
- **Networking and Security:** Vulnerability assessment, VPC design (multi-AZ, public/private/isolated subnets), security groups, NAT Gateway, DNS/ACM certificate management, IAM policy design, least-privilege access control
- **Security Tooling:** Prowler, Trivy, CSPM assessment
- **CI/CD and Automation:** GitHub Actions, OIDC federated authentication
- **Monitoring and Reliability:** CloudWatch (metrics, log groups, alarms), Auto Scaling (target tracking), load testing
- **Scripting and Tools:** Bash, AWS CLI, Git
- **SIEM and EDR tool:** Wazuh, Suricata (Working knowledge)
- Self-motivated, ability to work independently and in fast paced environments
- Security-first mindset
- Ability to multitask, Excellent communication, Organization and time management,
- Analytical and problem-solving skills.
- Troubleshooting
- Continuous learner with strong focus on cloud security

RELEVANT EXPERIENCE

Cloud Infrastructure Engr | 2026 to present **Expodox Lab** - Remote

- Provisioned AWS infrastructure as 12+ modular Terraform components for a 3-team production build under a 3-week deadline reducing manual AWS console configuration by 90% and enabling repeatable environment creation
- Built a multi-AZ VPC across 2 AZs and 6 subnets, with VPC Flow Logs and NAT Gateway routing
- Migrated 5 application secrets to Secrets Manager, eliminating hardcoded credentials from the codebase.
- Deployed ECS/Fargate behind an HTTPS ALB with dual-metric Auto Scaling (CPU 70%, memory 75%)
- Replaced static CI/CD credentials with GitHub Actions OIDC federation, scoped per repo/branch
- Migrated cross-team AWS access for 2 teams to IAM Identity Center, capping sessions at 4 hours
- Diagnosed a load-test blocker by correlating CloudWatch metrics to isolate an app-layer root cause
- Implemented tiered cost alerting and an ECR lifecycle policy capping stored images at 10
- Identified a 57% control failure rate using Prowler, with critical findings concentrated in IAM and CloudTrail configuration, directly shaping remediation priorities
- Built and operated a DIY Cloud Security Posture Management (CSPM) stack against a live AWS account
- Performed vulnerability scanning across cloud infrastructure using Trivy

VAPT Project | 2025 to 04/2026 **TSAcademy** – Remote

- Conducted Vulnerability assessments and penetration testing in simulated enterprise environment, identifying and documenting critical and medium risk vulnerabilities across target systems
- Identified about 5 security weaknesses, documented findings and recommended remediation strategies that improved overall security posture of environment
- Developed detailed VAPT reports aligned with cybersecurity best practices, improving technical documentation and risk communication skills
- Performed hands on risk assessment and security analysis to evaluate infrastructure vulnerabilities and recommend mitigation controls

Cloud Security Engineer | 2023 – 2025 **Gozirim Sciences LLC** – MD (Remote)

- Enforced IAM best practices, including least-privilege roles, MFA, and role-based access for users and services.
- Implemented encryption at rest and in transit for s3 and RDS to protect sensitive data.
- Provided input and feedback on security architectures and employed automation for security controls where possible to improve process efficiency, effectiveness and response.
- Experience in deploying AWS
- Audited cloud configurations using AWS Config and Macie to protect sensitive data
- Detected and remediated security events with AWS native tools such as Config, CloudTrail, Inspector, IAM, and Security Hub

CERTIFICATION

- **AWS Certified Cloud Practitioner (CCP)**
- **Azure Fundamentals**
- **AWS Certified Security Specialty (CSS) – in progress**
- **TSAcademy: cybersecurity**
- **AWS Security Specialty (in view)**

EDUCATION

University of Port Harcourt- Port Harcourt
Bachelor of Science - Honours