## A close up of a sign Description automatically generated A close up of a sign Description automatically generated A picture containing text, sign, picture frame Description automatically generated Logo Description automatically generated A picture containing text, clipart Description automatically generated A red and white logo Description automatically generated with low confidence

**BETRAND E METUGE**

**Sr Cloud Security Engineer/DevSecOps**

**enangmetug@gmail.com (346)-387-5680**

**Professional Summary**

An innovative, resourceful **Cloud Security Engineer** with **10 years of hands-on experience**. **Business-minded** and detail-oriented with **a passion for Cloud Security**. A **Subject Matter Expert in Multi-Cloud security (AWS/Azure)**, design and deployment of diverse monitoring, reporting, and security solutions for large enterprises. Proficient with multiple technologies within an infrastructure element. **Strong skills in integrating security tools in CI/CD build pipelines including Project Setup, Build and Release process setup, Build Automation, Continuous Integration, AWS and Azure**. Adept in identifying business risks, compliance issues and designing proactive solutions. **Ability to work both as an individual contributor and member of a team,** **ability to stay organized within fast - paced organizations. A U.S Citizen with ability to secure and maintain a SECRET security clearance.**

**SKILLS SUMMARY**

* Strong Technical Skills in AWS security **services, Linux, JSON, and RDS Databases**, **Containers.**
* Experience working with AWS and Azure services such **as AWS S3, EC2, AWS Glacier, AWS RDS, AWS VPC, AWS SNS, AWS SQS, AWS Elastic Beanstalk, AWS Cloud Watch, AWS CloudFormation, AWS CloudFront, AWS Route53, AWS Trusted Advisor, AWS IAM, AWS Lambda, AWS SecurityHub, MS Defender for Cloud, Azure PIM and KV, Azure AD, Azure Sentinel**.
* Good experience in creating **Bucket/objects**, enabling versioning, deployed static website on S3, and Data management using **Lifecycle Management**.
* Excellent **interpersonal** and **communication** skills, **technically competent** and result-oriented with problem solving and leadership skills.
* **Security Automation Tools**: **Veracode, Snyk, Checkmarx, Fortify, GitSecrets,**
* Strong experience with **CASB** to monitor enterprise cloud usage.
* Great knowledge **in SAFe/Agile methodologies**, **DevSecOps**, **Agile tools (**JIRA**), and waterfall**.

**TECHNICAL PROFICIENCES**

|  |  |
| --- | --- |
| **Area of Expertise** | Enterprise Cloud Information Security, Compliance, Monitoring, forensic investigation, vulnerability management, DevSecOps (**SAST, DAST, SCA and IAC**) |
| **Languages** | SQL, PL/SQL, UNIX shell Scripting, Python, JSON, YAML, Bash Scripting, Java. |
| **Tools** | PrismaCloud, GitHub, JIRA, ServiceNow, Terraform, Ansible, Quay.io, Prowler, RSA, DigiCert, Alert Logic, Abnormal Security, SecurEnds, Invicti, Chef, Ansible, Sysdig, Zscaler. |
| **Solutions** | Cloud Application and Database Migration, IAAS, PAAS, DRAAS, SAAS, CI/CD Pipe |
| **Databases** | Aurora. MySQL, HBase, SQL Server, Oracle, DynamoDB, Redshift, Postgres, RDS |

**EDUCATION & CERTIFICATION**

* **University of Buea- Bachelor of Computer Science**
* AWS Certified Solution Architect-**Associate**
* AWS Certified Solution Architect-**Professional**
* AWS Certified DevOps Engineer – **Professional**
* Certified Information Systems Security Professional **(CISSP)-**In Progress
* AWS Certified **Security Specialty**
* Microsoft Certified: **Azure Security Engineer Associate**
* Microsoft 365 Certified: **Security Administrator Associate**
* Certified Kubernetes **Administrator (CKA)**
* CompTIA **Security plus**
* Certified **Scrum Master**
* Certified **SAFe® Agilist**

**PROFESSIONAL EXPERIENCE**

**Freeman-Dallas, TX April’2022-Present**

**Senior Cloud Security Engineer/DevSecOps**

* Perform daily operational real-time monitoring, analysis, and resolution of security events from multiple sources including, but not limited to, events from Security Information Monitoring tools, network and host-based intrusion detection systems, content filtering solutions, firewall logs, & system logs matching existing SLA.
* Integrated **security tools like Fortify, Veracode, Snyk, SonarQube, Checkmarx in Jenkins Ci/CD build pipeline**.
* Performed **SAST, DAST, SCA and IAC security testing on applications** and performed False positive analysis.
* Used **Privileged Access Management (PAM)** to give list privileged access into our cloud environments.
* Deployed operational excellence monitoring solution to respond efficiently to job failure/outage.
* Improved Organization’s Security Posture by Assisting in the Creation of Disaster Recovery Protocols.
* Produced and managed AWS services such as VPCs, KMS, S3 buckets, and IAM...
* Using cloud security tools such Azure Defender for Cloud, AWS SecurityHub and other tool to make sure we stay compliant and increase our secure score.
* Installing SentinelOne agent to our Azure and AWS machines.
* Strong experience in **NIST Cybersecurity Framework** and **MITRE ATT&CK Framework** and all security compliance.
* Wrote chef Cookbooks and recipes to automate build/deployment process and do an overall process improvement to any manual process using recipes with ruby scripts.
* Ensured security best practices are in place during architectural reviews of a wide variety of application.
* Engineered different security solutions based on given requirements.

**EviCore HealthCare-Franklin, TN Dec’2019-April’2022**

**Sr Cloud Security Engineer/DevSecOps**

* Implemented Static and Dynamic Vulnerability Scanning Pipeline Tools.
* Wrote chef Cookbooks and recipes to automate build/deployment process and do an overall process improvement to any manual process using recipes with ruby scripts.
* Responsible for application Build & Release process which includes Code Compilation, Packaging, Security Scanning and code quality scanning, Deployment Methodology and Application Configurations.
* Worked as an active team member for both product development and the operations teams to provide the best DevOps Practices and supported their applications with feasible approaches.
* Defining Release Process & Policy for projects early in SDLC and responsible for source code build, analysis and deploy configuration.
* Created IAM roles for the **Kubernetes cloud setup**.
* Reviewing Vulnerability Reports and Working with Engineering Teams to Resolve Code Flaws
* Installed and setup **Kubernetes cluster** on AWS manually from scratch.
* Working with **account and agile/scrum DevOps teams to identify core security** areas and drive proposals in that area and security best practice.
* Lead our agile cloud security team of 6 security engineers and **a point of contact for security queries and data quality.**

**Shell Tech Center, Houston Jan’2016-Dec’2019**

**AWS Security Engineer/Architect**

* Creation of user accounts, policies and roles on amazon Web Services using **IAM**.
* Designed and created **Highly Available 3 tier Application**.
* Supervised Vulnerability Reports and Working Closely with Engineering Teams to Resolve CVEs
* Created, configure, and ensure connection to RDS databases.
* Secure Migrate Databases in **High Available Architecture** from On Premise to AWS Cloud redshift using Data Migration Services (DMS) and Schema Change Tool (SCT).
* Configured and integrate EC2 instances (applications) with different environments to automatically provision and create new machines using configuration management/provisioning tools.
* Perform log management and threat analysis set up and fine tuning. Design and architect tools for optimization.
* Collaborate with DevOps teams for issue resolution and mitigation. Participate and help remediate the security incidents.
* **Exposed Kubernetes microservice** to consumers using Nodeport, Load balancer, Nginx.

**MTN Cameroon, Douala Feb’2013 -Dec’2015**

**AWS Security Engineer/AWS Architect**

* I Supported the implementation and building of Hybrid Cloud environments with **High performance, High availability, and secured** connectivity to AWS using **Direct Connect** for MTN.
* Analyze systems, processes, or events as a part of formalized Incident Management procedures, including digital forensic investigation and event log analysis.
* At MTN **instantiated Amazon EC2 and assigned required firewalls** using security group (SG) and Network Access Control List (NACL) rules.
* Experience with **analysis of logs and performing root cause analysis** for issues coming up on daily basis using CloudWatch and CloudTrail.
* I **analyzed defects and prevented different attacks** coming into the company.
* Performed **security Scanning on OS, App, network components** and software to see where there are **Vulnerabilities.**
* Carried out **Security patches for Vulnerabilities found based on criticality** and advised organization on **security best practices.**