FRED MADUIKE

|  |
| --- |
| [*Tel: +1*](mailto:Tel:%20+1) *832 670-1696 | e-mail: maduike.fred@gmail.com* |

**Professional Summary**

Results-driven and self-motivated cloud IT professional with about 5 years of experience in Security and Architecting AWS Cloud Solutions in various cloud environments. Performance-driven with cross-functional experience in project management and cloud solutions across a variety of industries. Highly proficient in cloud orchestration, security, Identity & access management, event management, monitoring, governance and compliance, application delivery, data protection, image and patch management. In-depth expertise in building, planning, implementing and maintaining system applications on AWS Cloud platforms. Helping clients achieve business Agility and Flexibility, providing strong AWS ecosystem expertise as a Solutions Architect. Good team player & can adapt in all environments.

**Certifications**

* Project Management Professional (PMP)
* AWS Certified Cloud Practitioner (CCP)
* AWS Certified Solution Architect (CSA)
* AWS Certified Security Specialty (CSS)
* Microsoft Certified Azure Fundamentals
* Certified Ethical Hacker (CEH)
* CompTIA Security+
* ITILv4 Certified

**Core Competences**

|  |  |
| --- | --- |
| Security, Identity, Compliance, Management & Governance, Networking & Content Delivery, Database. Database Querying Language;  PostgreSQL, Apache MySQL, Microsoft SQL  server, NOSQL/DynamoDB, Puppet, Chef, Terrafom, Ansible, AWS inspector, AWS Shield, Amazon Macie, Guard Duty, Aws Secret Manager, Cloud Passage, Qualys, Tenable Nessus,  VMWARE, OpenVAS, Symantec DLP, (IDS/IPS) SIEM (Splunk/Qradar). Working knowledge of NIDS (Network Intrusion Detection Systems) and HIDS (Host Based Intrusion Detection Systems), Firewalls and Log Analysis, SIEM, etc. | CI / CD -Jenkins, BitBucket, GitHub, Bash, Yaml, Json, PowerShell, Gitlab. Security like Dome9, Barracuda Security Guardian, SonarCube, WASP Top 10.  Orchestration Services ECS Docker Containers, Kubernetes, Elastic Beanstalk – Amazon Web Services (EC2, EBS, S3, IAM, AMI, VPC, VPC Peering, WAF, NACL, Security Groups, Route53, Auto Scaling, ELB, SNS Cloud Watch, and Cloud Formation).  Code Deploy using AWS, CI/CD Pipelines, DoD ACAS (Assured Compliance Assessment Solution), STIGs, IAVM (IA Vulnerability Management) AWS Managed Firewall |

**Work History**

Willbros Group | Houston, Texas 04/2020 – Current

Consultant: *Lead AWS Solutions Architect/Security Engineer*

* Presentation skills with a high degree of comfort speaking with executives, IT Management, and developers; strong communication skills with an ability to right level conversations.
* Assist with leading the development and implementation of the cloud security strategy (i.e. SaaS, IaaS, and PaaS) by partnering closely with stakeholders.
* Design, implement, and monitor security measures to protect sites, cloud networks, and information privacy.
* Enable AWS cloud journey, gather requirements, analyze TCO and create a business case, make the Cloud dream become reality
* Good understanding and exposure to Network Layer like VPC, ACL, Subnets, Security Group, Load balancer, Route 53.
* Design, build, upgrade and operate multiple cloud environments. Hands on installation and configuration within the AWS/Azure clouds
* AWS – built VPCs from scratch, creating both private and public sub-nets, creating security groups and network access lists, configuring internet gateways. OpenVPN, creating AMI, understanding of user access management role-based access/multi factor authentication and API access, configuration of auto scaling and elastic load balancer for scaling services, configuration of SNS to send notifications and cloud watch to collect logs and metrics.
* Configuring and deploying micro-services and instances for example AMI's, EC2, ECS, Auto-scaling, S3, Security groups using Cloud-formation.
* Configured multi account architecture, identity and access management, governance, data security, network design and logging within provisioned AWS landing zones using AWS cloud formation.
* Use JSON polices to create Identity-based polices, resource-based policies and Permission Boundaries within the AWS environment.
* Enabled cloud trail log file validation so that any changes made to the log file itself after it has been delivered to the S3 bucket is trackable to ensure log file integrity.
* Manage a CI/CD (LAMBDA) methodology for server-based technologies within AWS.
* Security endpoint PKI Encryption to secure large public and private cloud environments.
* Turned on Redshift audit logging in order to support auditing and post-incident forensic investigation for a given database.

Citi Bank | New York, NY 05/2018 – 04/2019

Consultant: *AWS Solutions Architecture/ Cloud Security*

* Created Solutions for SaaS deployment of data migration from on-premise to cloud focusing on duplication to sync both storage data as changes are made.
* Extensive knowledge in migrating applications from on-premise hosting to AWS Web Services
* Review entire environment and execute initiatives to reduce failures, detects and improve overall performances. Provide incident management support on escalated troubles ticket when necessary.
* Experienced in the management and implementation of database models, database schemas, database scripts, to support a robust data management infrastructure.
* Communicate with internal and external groups (DBAs, Unix Admins, App Owners, Cyber Security, Network) to achieve successful implementation of database security.
* Worked with engineers and development teams to ensure that architecture solutions are compliant with security frameworks such as NIST, FedRamp, ISO 27001/27002, HIPPA, PCI etc.
* Worked on configuring Cross-Account deployments using AWS Code Pipeline, Code Build and Code Deploy by creating Cross-Account Policies & Roles on IAM.
* Assisted with designed and security oversight of next generation firewalls, intrusion prevention systems, DDos solutions, SSL-terminating load balancers, WAF, security groups and NACL.
* Built automated and flexible detection and response programs using tools like CloudWatch, Cloud, Trail, and AWS Lambda. Leveraged Identity Access Management features to setup Multi-Factor Authentication (MFA) for added security layer to root account, enterprises user account and assigning roles based on lease privilege to users.
* Experience in deploying and monitoring applications on various platforms using Elastic BeanStalk, setting up the life cycle policies to back the data from AWS S3 to AWS Glacier.
* Amazon Cognito for user sign-ins and storage, Amazon API Gateway and Lambda for cloud logic, Push notifications using Amazon SNS
* Proactively monitor resources and applications using the AWS Cloud Watch including creating alarms to monitor metrics such as EBS, EC2, ELB, RDS, S3, SNS and configured notifications on alarms generated based on events defined.
* Configuring and provisioning EC2 instances for development and production activities and create EBS volumes for storing application files. Create S3 buckets to store files, attach bucket policies and configure various life cycle policies to archive the infrequently accessed data to storage classes based on requirement.
* Assess the customer cloud maturity, review existing AWS cloud implementations, identify gaps and suggest improvements.
* Configure NACL, Security Groups and WAF to secure the application and VPC network depending on access parameters provided and conditions.
* Architecting and operating solutions built on AWS platform, deployed palo alto, F5, Aviatrix Transit Gateway boxes and configured boxes with customer’s requirements.
* Conduct full technical discovery, identifying pain points, business and technical requirements, "as is" and "to be" scenarios.

Walgreens | Deerfield, IL 05/2015 – 05/2018

Consultant: *Solutions Architect/Cloud Engineer*

* Responsible for working with designers to assist company in securing their cloud computing platforms; Work alongside Senior Cloud Architect in creating, designing, developing, testing and implementing a proprietary cloud and functional areas of the cloud
* Leverage AWS Cloud Endure to migrate 100s of VMWare on-prem VMs to Cloud
* Create Security groups that have access to both SSH and HTTP access; modify user access in AWS using the IAM feature including creating users to IAM, password resets, and adding users to different security groups in Amazon Web Services.
* Rotated IAM access keys regularly and standardized on a selected number of days for password expiration to ensure that the data cannot be accessed with a potential lost or stolen key.
* Leverage AWS Cloud Endure to migrate 100s of VMWare on-prem VMs to Cloud.
* Hands-on experience using AWS cloud monitoring tools (Cloud watch, Cloud trail)
* Create AWS Route53 to route traffic between different regions and CloudFront for distributions to serve content from edge locations to users to reduce the load on the frontend servers.
* Experience in maintenance and configuration of user accounts for to servers and created user, roles and groups for using resources in AWS Identity Access Management, Roles for EC2, RDS, S3, Cloud Watch, EBS resources to communicate with each other using IAM.
* Design, implement, test and document a serverless solution capable of monitoring service usage within an account using Lambda, CloudWatch, VPC, and Python.
* Work in the Cloud Security team as Security architect overseeing the automated security processes such as NACL, Security Groups, VPC, IAM, S3 etc. un-authorized access and modifications then alerting the incident details and responding to them with Reversal actions.
* Operational experience with network security appliances with a clear understanding of the architecture behind secure networks, DMZ’s, NAT’s, rule placement, VPN setup, and system maintenance.
* Management and Administration of AWS Services CLI, EC2, VPC, S3, ELB Glacier, Route 53, CloudTrail, IAM, and Trusted Advisor services.
* Setup multiple VPC environments, making connections between different zones and blocking suspicious IP/subnet via stateless Network ACL.
* Configure CloudWatch to receive logs from CloudTrail and visualize the logs, search on events and take actions.
* Deployed Barracuda to assist in comprehensive security architecture and a more seamless experience across the cloud, providing enhanced security against cyberattacks and advanced threats.
* Ensure business continuity and uninterrupted operational flows by designing and architecting Disaster Recovery Plan and Data Backups.

**Education**

Bachelor of Science: Cloud and System Administration In-View

Western Governors University–Salt Lake City, UT

Certificate of Completion: Cloud Security Architecture and Operations 09/2019

SANS INSTITUTE – Bethesda, MD

Bachelor of **Engineering:** Mechanical Engineering 12**/**2012

Yaba Institute of Technology – Overseas

**REFERENCES**

Upon request