Daniel Nwosu

**6411 Kilmer Street, Cheverly, MD 20785  
Home: (240) 604-2150 - Cell: (240) 604-2150 -** [**daniel.nwosu2319@gmail.com**](mailto:daniel.nwosu2319@gmail.com) **– Open to Relocation!**

**LinkedIn:** [**https://www.linkedin.com/in/danielnwosu/**](https://www.linkedin.com/in/danielnwosu/)

**Professional Summary**

AWS Cloud Solutions Architect/Cloud Security Professional with Five (5) + years of experience working as a Cloud Solutions architect/DevOps Engineer for several customers and managing server infrastructures and data center operations. Implementing upgradable, scalable, Hyper-converged infrastructure and micro-services across multiple platforms (Windows, Linux, Amazon Linux).

**Certifications**

**• AWS Certified Cloud Practitioner - Certified  
• AWS Solutions Architect Associate - Certified  
• AWS Developer Associate - Certified  
• AWS SysOps Administrator Associate - (Feb 29th 2020)**

**ITIL V4 Certified**

**Skills**

|  |  |
| --- | --- |
| Database Querying Languages; PostgreSQL, MySQL, SQL server, NOSQL/DynamoDB. Jenkins, Puppet, Chef, Terraform, Ansible. AWS Inspector, AWS Shield, Macie, Guard Duty, AWS Secret Manager, Cloud Passage, Qualys, Nessus, OpenVAS, Symantec DLP. (IDS/IPS) SIEM (Splunk/Qradar) Palo. | Firewalls & Log Analysis, SIEM, etc. Orchestration Services ECS, Docker Containers, Elastic Beanstalk – Amazon Web Services (EC2, EBS, S3, IAM, AMI, VPC, VPC Peering, NACL, Security Groups, Route53, Auto Scaling, ELB, SNS, Cloud Watch and Cloud Formation). Dome9, Barracuda Guardian Security, F5, |

**Work History**

|  |  |
| --- | --- |
| 01/2017 to 12/2019 | Consultant: AWS Solutions Arch/Cloud Security Engr  Capital One Bank – Reston, VA   * Providing expertise to client's early adoption strategy such as end user training, evangelizing cloud solutions, bringing experience and best-practice in the AWS cloud ecosystem * Proactively monitor resources and applications using AWS Cloud Watch including creating alarms to monitor metrics such as EBS, EC2, ELB, RDS, S3, SNS and configured notifications for the alarms generated based on events defined * Established the appropriate monitoring and alerting of solution events related to performance, scalability, availability and reliability * 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 * Provisioned AWS Landing Zones to create a customized baseline of AWS accounts, networks, and security policies * Configured multi-account architecture, identity and access management, governance, data security, network design, and logging within provisioned AWS Landing Zones. * AWS – built VPCs from scratch, creating 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 * Worked with engineers and development teams to ensure that architecture solutions are compliant with security frameworks, such as NIST, FedRAMP, ISO 27001/27002, PCI, etc * Designed and contributed to security architecture processes that enable the enterprise to develop and implement secure solutions and capabilities that are clearly aligned with the business, technology, and threat drivers * Participated in application and infrastructure projects and other business initiatives to provide security-planning guidance with the following drivers: reduce risk, protect business applications while ensuring the highest level of data and infrastructure (endpoints, servers, networks, data center, cloud) security * Reviewed and evaluated current access routes, sites, vendor integration points, and security platform integrations; recommended improvements and develop corrective strategies to improve security prior to implementation * Assisted with designed and security oversight of next-generation firewalls, intrusion prevention systems, DDoS solutions, SSL-terminating load balancers, WAF, security groups and NACL * Recommended and managed transmission protection requirements for all environments (systems, applications, containers, etc.) such as VPC peering best practices, SSL certificate management, key pairs, etc * Performed security monitoring, security event triage, and incident response; coordinate with other team members and management to document and report incidents * Participated in deep architectural discussions to build confidence and ensure customer success when building new and migrating existing applications, software and services on AWS platform * Technical liaison between the customer's service engineering & support teams * Create a case to increase AWS WorkSpaces to 150 for a customer and Deployed all 120 WorkSpaces for customer's end users offshore and nearshore in Mexico * 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 * Architecting/operating solutions built on AWS Platform; Deployed Palo Alto, F5, Aviatrix Transit Gateway boxes and configured boxes with customer's requirements * Experienced with "on-premise to cloud" migrations and IT transformations with the aid of AWS solutions |

|  |  |
| --- | --- |
| 02/2014 to 01/2017 | Consultant: Solutions Architect/Cloud Engineer  Walgreens – Deerfield, IL   * Designed and implemented system security and data assurance * Hands-on experience writing Production-ready automation code to implement solutions with Puppet, Ansible, CloudFormation or similar - e.g.: Chef, Terraform * Strong interpersonal, organizational, and communication skills with the ability to work effectively across internal and external organizations and virtual teams * Proven experience in systems and cloud network design and development * Strong understanding of information processing principles and practices * In-depth technical knowledge of networks, storage systems and computing platforms including Amazon AWS, .NET, Windows, and CI/CD pipelines * As a last line of defense against a compromised account, I ensured all IAM users have multi-factor authentication activated for their individual accounts, and limited the number of IAM users with administrative privileges * Rotated IAM access keys regularly and standardize on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key * Turned on Redshift audit logging in order to support auditing and post-incident forensic investigations for a given database * Encrypted data stored in EBS as an added layer of security * Encrypted Amazon RDS as an added layer of security * Enabled require\_ssl parameter in all Redshift clusters to minimize the risk of man-in-the-middle attack * Restricted access to RDS instances to decrease the risk of malicious activities such as brute force attacks, SQL injections, or DoS attacks * Encrypted highly sensitive data such as protected health information (PHI) or personally identifiable information (PII) using customer-controlled keys * Granted the fewest privileges possible for application users * Involved IT security teams throughout the application development life-cycle * Inventoried and categorized all existing custom applications deployed in AWS * Assisted with designed and security oversight of next-generation firewalls, intrusion prevention systems, DDoS solutions, SSL-terminating load balancers, WAF, security groups and NACL * Recommended and managed transmission protection requirements for all environments (systems, applications, containers, etc.) such as VPC peering best practices, SSL certificate management, key pairs, etc * Designed and implemented monitoring and protection capabilities to help identify and protect against DoS attacks, MITM, EC2 instance compromise, secret compromise, etc * Developed tactical response procedures for security incidents * Performed security monitoring, security event triage, and incident response; coordinate with other team members and management to document and report incidents * 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 * Led root cause analysis, debugging, support, and postmortem analysis for security incidents and service interruptions * Enabled Cloud Trail across all geographic regions and AWS services to prevent activity monitoring gaps * 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 * Enabled access logging for Cloud Trail S3 bucket so that you can track access requests and identify potentially unauthorized or unwarranted access attempts |

**Education**

|  |  |
| --- | --- |
| 12/2016 | Bachelor of Science: Mechanical Engineering  Rochester Institute of Technology - Rochester, NY |

|  |  |
| --- | --- |
| Expected in 12/2020 | Bachelor of Science: Cloud System Administration  Western Governors University - Online |

|  |  |
| --- | --- |
| 06/2019 | Certificate of Completion: Cloud Security Architecture and Operations  SANS INSTITUTE - Washington, DC |