

Abideen Oni

8176733261 | oniabideen@gmail.com | linkedin.com/abideenoni

Education

University of Texas San Antonio

Bachelor of Science in Cybersecurity — GPA: 3.74/4.00

San Antonio, TX

2026

Experience

Amazon AWS

Cloud Support Engineer Intern

May–August. 2026

Dallas, TX

- Developed a serverless automated pipeline for moderation and metadata extraction, accelerating image processing from months to <1 day with 97% cost savings.
- Delivered 96.72% accuracy with systemic technical troubleshooting across EC2 failures, VPC errors, web application outages, and cross-service issues using Linux tools in misconfigured environments.
- Architected scalable, highly available applications with Auto Scaling Groups and Load Balancers across multi-AZ VPCs, enforcing subnet isolation and least-privilege access.
- Troubleshoot Linux, Windows, networking, identity access, and secure communications issues in AWS-aligned environments.
- Utilized Lambda,S3,ALB,Fargate,ECS,EKS(Kubernetes) etc to Deploy Multiple Resilient Severless, High Avalability Application

Rocket Mortgage

Technolgy Security Engineering Intern

May. 2025–Aug. 2025

Detroit , MI

- Performed Regular Application tests like encryption, phishing, access and least privilege, security logging and monitoring
- Collaborate with IT teams and business stakeholders to support IT projects and initiatives.
- Drafts, updates, and maintains technical documentation, local policies, and standard operating procedures (SOPs).
- Analyzed application and security logs in Splunk to support incident response, root cause analysis, issue escalation, and service reliability.

Apple

Technical Support Intern

Oct. 2024–Jan. 2025

San Antonio , TX

- Performed software installations, updates, and system patches.
- Configured, image, deploy, and set up new desktop and laptop computers
- Maintained inventory of IT assets including laptops, desktops, monitors, and accessories.
- Supported Apple MDM configurations and provided secure device onboarding and two-factor authentication setup

GOS

System Administrator

Feb. 2025–Present

San Antonio , TX

- Pionnered Implementation of LDAP, SCIM, REST APIs, and enterprise application integrations.
- Performed QA on customer-facing products, identifying bugs and automating critical test cases with WebdriverIO to improve reliability and reduce manual testing effort.
- Worked on escalated Tickets to Assist users with password resets, account access, printer connectivity, and peripheral devices.
- Maintained 99.9 % uptime across 150 physical and virtual servers supporting 2,000 users across 5 office locations.
- Automated server provisioning with PowerShell scripts, reducing deployment time from 3 hours to 20 minutes per server

Projects

Allons-y – AWS CloudHacks Winner | Python, S3, Textract, Bedrock, Polly, MoviePy

- Reduced manual editing time by 90% by building a serverless AWS pipeline that converted PDFs into viral, ready-to-post short-form videos with user customization.
- Automated script-to-video creation using S3 for storage, Textract OCR, Bedrock LLMs for dialogue creation, and Polly for realistic voiceover, then synchronized narration with visuals via MoviePy.

Personal Cloud Infrastructure Homelab |

- Built a Proxmox-based cloud lab with Ubuntu, Debian, Red Hat, and Windows workloads to simulate hosted desktops, servers, storage, endpoints, and cloud infrastructure.
- Configured VLAN segmentation, firewall rules, reverse proxies, secure remote access, centralized logging, and service monitoring for root cause analysis.

Talos Kubernetes Homelab |

- Planned a 6-node Talos Kubernetes cluster on Proxmox using OpenTofu, including static IP design, bridge networking, storage, and infrastructure validation.

Active Directory Attack and Defense Homelab |

- Built a Windows Active Directory lab with domain controllers, Windows endpoints, and a Kali Linux attacker machine to simulate enterprise authentication and network environments.
- Executed and documented common attacks, including password spraying, Kerberoasting, pass-the-hash, privilege escalation, and lateral movement using tools such as BloodHound and Impacket.
- Implemented defensive controls with Windows Event Logging, Sysmon, Wazuh, Group Policy, account lockout policies, and detection rules to identify and respond to malicious activity.

Technical Skills

Languages & Knowledge: Python, Java, C, JavaScript, HTML, CSS, Linux, DNS, TCP/IP, HTTP, VLAN,,Proxmox,VM Ware,Linux

Tools & Platforms: Git, AWS (S3, Bedrock, Polly, Lambda, Rekognition, DynamoDB, SQS, SNS),Jenkins,Terraform,Kubernetes

Certification: AWS Solutions Architect Associate, AWS AI Practitioner, CompTIA Security+