**Bern Abeh**

**(443) 868-4891 -** [**abehbern@gmail.com**](mailto:abehbern@gmail.com)

**Richmond, TX**

**PROFESSIONAL SUMMARY**

A Cloud Security Engineer and IT Professional with 12+ years of experience offering proficiency in AWS Cloud Orchestration, Azure, and System Security Assurance. Skilled in Cloud Computing, Networking, Compliance Security, Linux OS, Risk Management Framework. Delivered several organizational projects with AWS and Azure cloud platform, working with different cross functional teams and management styles. Open minded and great desire to learn new skills to achieve the organization goals.

**SKILLS \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| * VPC, EC2, IAM Role, Route 53, Lambda, S3 | * Firewall, Guard Duty, Control Tower |
| * JSON, Python, Jenkins, Ansible, AWS CLI, SQL | * Security Hub, WAF, IAM, Palo Alto |
| * Detective, Shield, Secret Manager, Inspector | * Docker, Git, GitHub, Gitlab, MySQL |
| * CloudWatch, CloudTrail, Network Security * Terraform, Ansible, DevSecOps | * Jira, Confluence, eMASS, Nessus * NIST, HIPAA and PCI DSS, FedRAMP |

**CLEARANCE LEVEL: PUBLIC TRUST**

**SECRET CLEARANCE**

**TOP SECRER CLEARANCE SCI**

**CERTIFICATION \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* CompTIA Security**+** Certification
* AWS Certified Security Specialty - Professional
* AWS Certified Solutions Architect – Associate
* AWS Certified Developer – Associate
* Certified Ethical Hacker
* Certified Scrum Master (Scrum Alliance)
* Certified SAFe® Agilist
* ITIL 4 Certified in IT Service Management

**EDUCATION \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* Bachelor of Science in Computer Science; University of Buea – 2013
* Master’s in cyber security; In progress

**WORK HISTORY \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Sr. AWS Cloud Security Engineer**

**Department Of Defense – Broadleaf Inc** – Aberdeen MD February 2019 to Present

As a Cloud Security Engineer for DNS migration with the integration of Read-Only Domain Controller, I’m in charge of the making sure the team is following DevSecOps security aspects for the deployment of infrastructure in the Cloud. Details of my tasks assigned contained but not limited to the following:

* Implementing security best practices in AWS including multi factor authentication, access key rotation, encryption using KMS, firewalls- security groups and NACLs, S3 bucket policies and ACLs, mitigating DDOS attacks, etc.
* Designed and implemented Secure, Resilient, Cost Effective, H.A and Self-healing Architectures with Fail Over Routing Policies leveraging AWS Best Practices.
* Provisioned SSL/TLS security Certificates using AWS Certificate Manager
* Expertise in working with Terraform key features such as Infrastructure as a code, execution plans, resource graphs, change automation and created infrastructure in a coded manner using Terraform.
* Created IAM security roles for the Kubernetes cloud setup and identified unintended access to other resources and data and stopped that access.
* Used CloudWatch Logs to monitor, store and access log files from Amazon EC2 instances, CloudTrails and others.
* Utilized CloudTrail to capture API calls for IAM and AWS STS as events, with analysis of security logs and performing root cause analysis for issues coming up on daily basis.
* Involved heavily in setting up the CI/CD pipeline using Jenkins, Maven, Nexus, GitHub, Puppet, Terraform and AWS.
* Utilized GuardDuty to continuously monitor feeds from DNS logs CloudTrail, EKS logs and VPC flow logs to identify malicious IP addresses and domains, escalations of privileges and exposed credentials.
* Performed vulnerability management using Amazon Inspector to scan the workloads for vulnerabilities.
* Improved the environment security posture by utilizing AWS Shield for DDoS detection and mitigation.
* Utilized AWS WAF to monitor HTTP(S) requests forwarded to the API gateway REST API and Load Balancers
* Configures Cloud Watch alarm rules for Operational and Performance Metrics for our AWS Resources and Applications.
* Deployment to AWS with Ansible and Terraform towards AWS, and using Terraform for building, updating, and versioning infrastructure safely and efficiently, as well as creating custom in-house solutions with Chef or Puppet configurations.
* Configured S3 events to set up automated communication Between S3 and Other AWS Services.
* Designed and implemented Highly Available Infrastructure using Elastic Load Balancer and Auto Scaling For web Servers, which scaled in and scales out automatically, also isolated environment by having security groups and NACLs across subnets for EC2 Instances.
* Used Secrets Manager to replace hardcoded credentials in the code, including passwords.
* Knowledge of DNS, Kerberos and Windows Authentication, to include authentication with other technologies for Single Sign-On
* Utilized AWS Resource Access Manager (RAM) to securely share resources within AWS accounts.
* Designed for high availability and business continuity using self-healing-based architectures, Fail Over Routing Policies, Multi–AZ Deployment of EC2 Instances, ELB health checks, Auto Scaling.
* Implemented AWS Systems Manager Management service capabilities to automatically collect Software Inventory, apply OS patches and automate Administration Tasks, and complex workflows.
* Automatically Remediated Trusted Advisor findings using amazon cloud watch events and AWS Lambda
* Implemented AWS Organization to centrally manage multiple AWS Accounts including consolidated billing and policy-based restrictions.
* Implemented Control Tower Preventive and detective Guardrails and leveraged Account Factory Integrated with Lambda for new AWS Account Creation, Vending and setup.

**Cloud Security Engineer/ AWS Solution Architect**

**Verizon** – Arlington Virginia, VA March 2017 – January 2019

Monitoring performance bottlenecks of Serverless Architecture, and key metrics to optimize software and system performance duties also included but not limited to the following:

* Leverage Different design Principles for Security, in the cloud and implemented Various AWS Services to improve our security posture for Authentication, Authorization, Monitoring Auditing, Encryption, and Data Path Security.
* Utilized IAM to securely control access to AWS resources by creating groups, users, and assigning users into the groups and administering permissions to these groups based on “Need to Know Basis”.
* Act as subject matter expert on AWS and provide a backup or upgraded solution to improve the performance of the application
* Designed architecture strategies for large-scale [System]-wide application deployments. Developed baseline VPC and Network Design including leveraging VPN Connectivity, and direct connect
* Utilized AWS Network Firewalls as an intrusion detection and preventions service for the VPCs in the environment.
* Provisioned the highly available EC2 Instances using Terraform and cloud formation and wrote new plugins to support new functionality in Terraform.
* Develop Baseline AWS account Security, implemented/integrated end point protection, vulnerability, scanning and intelligent threat detection.
* Used IAM to implement Single Sign On and MFA (SSO) to increase security of the environment.
* Used AWS WAF to control access to the environment by specifying the trusted IP address
* Managed Security Patches systems Updates, IDS/IPS for 100,000 EC2 instance per day
* Conducted periodic reviews of existing cloud environments for compliance with industry standards such as PCI DSS or HIPAA. Configured Secrets Manager to automatically rotate the secrets to reduce risk of compromise.
* Implemented best practices for Terraform configuration management, including code reviews, version control, and automated testing, to ensure the reliability and maintainability of Terraform code.
* Used Amazon Detective to analyze, investigate and identify root cause of security findings.
* Built Serverless Architecture with Lambda integrated with SNS, Cloud watch logs, and other AWS Services
* Leverage Automated DevOps tools deployment and blue green deployment Patterns and strategies
* Configured CI/CD Pipelines Using Jenkins Connected to GitHub (Dev, Stage and Prod)
* Implement AWS Organization to centrally manage multiple AWS Accounts including consolidated billing and company-based restrictions.
* Implementing security best practices in AWS including multi factor authentication, access key rotation, encryption using KMS, firewalls- security groups and NACLs, S3 bucket policies and ACLs, mitigating DDOS attacks, etc.

**AWS Solutions Architect /** **Cloud Administrator**

**Shell** – Houston, TX December 2015 – February 2017

Proposed AWS Cloud Solutions and their value during Operations meetings and implement them when they are approved as best for the business goals or received the design from supervisors and implement them. Duties also included

* Managed, Monitor, Troubleshoot, and solve problems on AWS infrastructure using resources such as CloudTrail, CloudWatch, SNS etc
* Utilized Rapid7 and Qradar for vulnerability management and log management.
* Administered AWS Cloud Security – Allowing access to service and users with IAM, Security Group, Network Access Control List, MFA, KMS, CloudHSM
* Defined methods of performance in the AWS Cloud as they relate to the business goals using: CloudFront, CloudFormation, Lambda etc
* Leverage EC2 Lifecycle manager to create snapshots of EBS Volumes on scheduled intervals for backup and define a retention Period as a cost saving measure.
* Designed the Overall Virtual Private Cloud (VPC) environment including server instance, storage instances, subnets. Availability Zones, and managed Provisioning of AWS Infrastructures Using Terraform.
* Structured cluster Auto scaler for Azure Kubernetes Service (AKS) by using Terraform and worked with scheduling, deploying, and managing pods and replicas in AKS.
* For the platform high availability using the services like ELB, ALB, EFS, Auto Scaling, Lifecycle Management, Database Replica, Multi-AZ configuration S3, Glacier, and Versioning.
* Extensive Knowledge and hands-on experience implementing PaaS, IaaS, SaaS style delivery models inside the Enterprise (Datacenter) and in Public Clouds using AWS, Google Cloud, and Kubernetes, etc
* Design for high availability and business continuity using self-healing-based Architectures, fail over Routing Policies, Multi AZ deployment of EC2 instances, ELB Health checks, Auto Scaling, and other disaster recovery models.
* Managed Terraform state files and used remote backends like Amazon S3 for state locking and consistency.
* Managed installation, upgrade and deployment projects and provided on-site direction for network engineers.
* Designed and implemented for scalability and Elasticity using Elasticache cloud front, Edge locations and RDS, (Read replicas, instance sizes)
* Created Patch Management Using Systems Manager automation using multiregional and multi account execution
* Implementation of Transit Gateway using Direct Connect Service in AWS to connect the on-premises environment to Cloud in each region.
* Set up Ansible master nodes and target nodes and developed playbooks to Automation Configuration Servers Across Automation.

**Cyber Security Analyst**

**Department Of Defense (Remedi CS) –** Essex, MD February 2012 – December 2015

* Perform updates to System Security Plans (SSP) using NIST 800-18
* Risk Assessments, and Incident Response Plans (create/change control procedures, draft & review) Using NIST SP 800-53A
* Identify trends and root causes of system failures or vulnerabilities using NESSUS Vulnerability Scanner, Nmap to scan ports, weak configuration, and missing patches.
* Knowledge in the use of information security practices and standards such as NIST, CIS Critical Security.
* Implemented innovative process, which increased response time to technical issues by 23%.
* Performed Information Assurance Vulnerability Management to improve security posture and ensure configuration compliance with organization policies and standards.
* Automated infrastructure provisioning and configuration management with Terraform, Ansible, Git.
* Researching, analyzing, and reviewing vulnerabilities reports, working with developers, system admins and engineers to remediates vulnerabilities on scan report and create POA&M to track remediation process.
* Decreased security breaches by 3% through conducting risk assessments and authorizing new security standards.