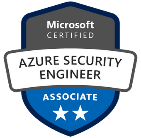
A close up of a sign

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

**Lacbane Lima G**

**Sr Cloud Security Engineer/Cloud Engineer(DeSecOps)**

gillslim87@gmail.com **3376771733**

**Professional Summary**

A **Cloud Security Engineer who** acts as the technical representative for enterprise security while engaging with other senior technical leaders throughout the organization in the design and implementation of cloud and cloud/hybrid-based implementations and solutionswith **10 years of hands-on experience**. **Business-minded** and detail-oriented with **a passion for Cloud Security**. Perform infrastructure security design, Firewalls ,Intrusion detection and prevention systems (IDS/IPS), Security information and event management (SIEM), Vulnerability scanners, Identity and access management, Maintain an understanding of various cloud platforms, Perform cloud security design, Determine security requirements, Create security procedures, Create security policies, Create security awareness / training, Define security controls, 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, DevSecOps. Adept in identifying business risks, compliance issues and designing proactive solutions.

**SKILLS SUMMARY**

* A Certified AWS solutions Architect with over 8 plus years of ITops
* Experience and 4 plus years in Architecting and Administration of self-healing, highly scalable, fault tolerant, performant &amp; secure cloud-based services and applications for PaaS, IaaS &amp; SaaS environments using Amazon AWS services
* like Elastic Compute Cloud (EC2), Simple Storage Service(S3), CloudFormation,
* CloudWatch, CloudFront, Lambda, Route 53, Auto Scaling, ELB, RDS, AMI,
* IAM, VPC, Elastic Beanstalk and KMS Excellent **interpersonal** and **communication** skills, **technically competent** and result-oriented with problem solving and leadership skills.
* Strong experience with **CASB** to monitor enterprise cloud usage.
* Great knowledge **in Safe/Agile methodologies**, **DevSecOps**, **Agile tools (**JIRA**), and waterfall**.
* 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 Security Hub, MS Defender for Cloud, Azure PIM and KV, Azure AD, Azure Sentinel**.

**TECHNICAL PROFICIENCES**

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

**PROFESSIONAL EXPERIENCE**

**Capital one Bank TX April’2022-Present**

**Senior Cloud Security Engineer/DevSecOps**

Drive the security standards and tool strategies for public and private cloud solutions. Conduct technology assessments to establish and validate an enterprise security baseline and establish a technical direction. Set technical standards for Cloud infrastructure, containers, security baselines, policies, and procedures. Develop and implement security controls for various cloud infrastructure providers. Analyze security configurations and provide vulnerability reports. Provide subject matter expertise on, and conduct in-depth security reviews of, new OS, database, middleware, solutions as they are identified for use.Good experience in creating Bucket/objects, enabling versioning, deployed static website on S3, and Data management using Lifecycle Management Automated security testing and auditing to prevent regressions and catch issues before they reach production. Codify traditional security processes to take humans out of the equation making security consumable as a service.Provide security expertise on system, network, encryption, authentication, and governance.AWS Cloud including - Rehosting (Lift and Shift), Replat forming,Repurchasing, Refactoring/Re-architecting, Retiring, and Retaining

* Experience with cloud security, compliance, and accreditation. Work with Security team to ensure solutions comply with FISMA/FedRAMP ,controls Federal security policies. Advise and achieve ATO accreditation.
* Experience with cloud cost estimation, management, and optimization
* Hands on experience in designing and deploying AWS technologies such as VPC, EC2, EBS, S3, ELB, Auto scaling, Elastic Beanstalk, IAM, RDS,Route 53 &amp; Redshift, Experience architect and deploying a multi-account strategy using AWS
* control tower for account Vending and creating guardrails using some IAM, permission boundaries and AWS organization services control policies, Configured KMS using IAM to provide encryption/decryption keys to
* secure Amazon S3, EBS and RDS.Provide hands-on support to the IT security systems administration, incident response team, and architecture development team, including monitoring and capacity planning.
* Support the regulatory compliance initiatives, processes, and documentation for ISO, NIST, CSA, PCI, SOC2, etc.
* Develop scripts and automation to scale and accelerate the implementation and audit of security configurations, risks, and assessments.
* Review modern technologies and products for security implications.
* Design, develop, and implement new cloud security technologies to support business and technology solutions.

**Abet HealthCare-Franklin, TX Dec’2019-April’2022**

**Sr Cloud Security Engineer/DevSecOps**

Assist the Cloud Network team in performing security design, analysis, and recommendation for a wide variety of IT systems and technologies. Research and stay up to date on the latest security threats and trends. Monitor and validate compliance with security policies and procedures. Interactions, document requests, and walkthrough meetings with auditors and regulators when needed. Participate on automation of incident prioritization, false positives identification, correlation, vulnerability remediation. Implemented Static and Dynamic Vulnerability Scanning Pipeline Tools. Designed and implemented Resilient, cost effective, H.A and Self-healing Architectures with Fail Over Routing Policies leveraging AWS services and security Best Practices. Created IAM roles for the Kubernetes cloud setup. Performed migrations using tools like DMS, SCT. Experience on Version Control System (VCS) like GIT, GIT-Hub, Performed backup and recovery in on premise oracle environments.

* Created and managed users, permissions, directories and files in Linux
* Installed Apache and Nginx Web Server on EC2, (proxy server as needed).
* Implemented compliance with CIS Benchmark on AWS environment.
* Troubleshoot various customer technical problems and adhere to best practices.
* Created and configured Amazon direct connect and Placement groups.
* Migrated the production MySQL schema Reviewing Vulnerability Reports and Working with Engineering Teams to Resolve Code Flaws

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

**AWS Security Engineer/Architect**

Audit all existing security standards: to include engineering designs, implementation, and guidelines. Handles operational problem escalations and vendor concerns related to security. Deploy and maintain internal security systems such as IDS/IPS, SIEM, WAF, FIM, DDOS and internal/external vulnerability scanners and ASV’s.Work with business colleagues to review RFPs, RFIs etc., and provide security and risk-related input into proposals. Monitor the external threat environment and information security trends while keeping business leadership informed about information security-related issues and activities potentially affecting the organization.Serve as the information security subject matter expert for the Incident Response team and handle escalations of any possible incidents impacting the company.

* Designed and created Highly Available 3 tier Application.
* 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.
* Collaborate with DevOps teams for issue resolution and mitigation. Participate and help remediate the security incidents.Exposed Kubernetes microservice to consumers using Node port, Load balancer, Nginx.

**Diamond Island UAE Feb’2013 -Dec’2015**

**AWS Security Engineer/AWS Architect**

Monitor system events, logfiles and alerts, Evaluate new security products and solutions Oversee enterprise patch management and vulnerability remediation. Maintain a knowledge of various programming languages.Performed **security Scanning on OS, App, network components** and software to see where there are **Vulnerabilities.** Involved in 24x7 support rotation for Production, Test and Development. Built and configured virtual data center in AWS to support Enterprise Data.Some minimal knowledge and experience in Containerization using docker,Kubernetes, AWS ECS and ECR

* Ability to Champion Agile best-practices, processes, and tools in support of DevOps processes
* Ability to write CloudFormation scripts (independently) – Infra As A Codefor AWS Core Services. Carried out **Security patches for Vulnerabilities found based on criticality** and advised organization on **security best practices.**

**EDUCATION & CERTIFICATION**

* **University of Buea- Bachelor of Computer Science**
* AWS Certified Solution Architect-**Associate**
* AWS Certified Solution Architect-**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**