**Lokesh Kanakamedala**

Dallas, TX | 409-999-0430 | lok.cd7@gmail.com

**Summary of Qualifications**

* Lead AWS Cloud Engineer skilled in Security and Cost-Effective Approach.
* Experience with a broad set of information security technologies and processes (e.g., Data Protection, Encryption, Identity and Access Management, Logging and Monitoring, Security Governance, Risk Management, Network Security) within cloud environments.
* Professional level of understanding on AWS Services - AWS EC2, VPC, ELB, S3, RDS, Cloud Trail, Route 53, IAM, Cloud watch, Cloud Formation, EMR, Athena, Beanstalk, KMS, ACM, Guard Duty, Cloud Trail, Config, CloudWatch, WAF, AWS Security Hub, IAM Roles, Security Groups, Network ACLs, AWS Cost Explorer, AWS Trusted Advisor, AWS Cost and Usage Report, AWS Budgets Kinesis, DMS, SNS, SQS and Systems Manager.
* Managed a Cross-functional Team (Platform, Finance, Cloud Delivery and Operations) and coordinated with business Partners towards the successful launch of Remediation and Cost Optimizing Tools

**Professional Experience**

**Client – Goldman Sachs Dallas, TX Jan 2024- Present**

**Lead Cloud Auditor – Internal Audit**

------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Responsibilities:**

* Leveraged cloud security and risk management expertise to proactively assess and mitigate security and operational risks across Goldman Sachs' cloud infrastructure.
* Performed regular cloud security audits, utilizing tools and techniques for vulnerability scanning, configuration management, and access control review.
* Partnered with cloud engineering, security operations, and business stakeholders to remediate identified security issues and ensure continuous improvement.
* Conduct comprehensive security audits of cloud container deployments using CIS Benchmarks and custom security checklists.
* Optimized cloud resource utilization through cost analysis and identifying opportunities for infrastructure consolidation.

**Client - The Depository Trust & Clearing Corporation (DTCC)-Dallas, TX Jun 2021- Jan 2024**

**Product Lead – Senior Cloud Engineer**

------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Responsibilities:**

* **Led a cross-functional team** (developers, Ops engineers) to implement a new cloud-based security solution using CI/CD pipeline that helped customers achieve regulatory compliance from self-healing systems triggered by monitors, near real-time metrics, & log information. (Config, SSM, Lambda, CloudWatch, and Splunk).
* Launched an alternative compliance tool that runs on Jenkins with manual triggering jobs - for bulky remediations requiring downtime or following the extensive process. (Jenkins, AWS, Python, and Splunk)
* Implemented innovative features in new software releases, involved collaborating with product managers to understand market needs, analyzing user feedback, and prioritizing functionalities to ensure high user adoption and business value.
* Developed a strategic integration plan, Including evaluating different cloud solutions, analyzing transaction data, and collaborating with stakeholders to ensure a seamless transition with minimal disruption to operations.
* Identified and addressed security vulnerabilities within the cloud environment, leading to improved overall security posture.
* Streamlined remediation and security workflows by automating manual tasks and implementing best practices, resulting in increased efficiency and accuracy.
* Developed Splunk dashboards for efficient monitoring of cloud remediation and automation processes, enabling proactive identification and resolution of potential issues.
* Developed and implemented cost-efficient strategies that helped customers reduce their cloud spending while maintaining high levels of performance and availability.
* Partnered with Financial Management and Technology partners to ensure deployment plans for new/enhanced services are transitioned successfully into operations.
* Identified and implemented process improvements for vulnerability management, reducing remediation time by 50%.
* Productized backup and restore procedures, including data retention policies and archiving, leveraging Python automation.
* Experienced in building and maintaining robust observability platforms and implementing resiliency strategies to ensure high system availability and performance.
* Led a team of developers and worked closely with stakeholders to develop a suite of compliance and cost optimization tools for our customers.
* Migrated and centralized AWS Cloud metrics, traces, and logs into Splunk for comprehensive cloud observability and enhanced troubleshooting capabilities.
* Collaborated with Architecture, Ops, and security teams to develop and implement security playbooks for incident response and vulnerability management processes.
* Managing business relationships with key stakeholders (Product, Business, and IT), understanding their business problems, and appetite for business risk and guiding them on IT strategy and direction.
* Maintain and update critical tools and infrastructure with a strong focus on Cloud-based services and Technology.
* Contributed to creating system support documents, operational run books, and job aids.
* Conducted technology assessments to validate Security Baselines and provide technical directions if desired.
* Defined product requirements, prioritized feature development, and ensure successful product delivery.
* Managed cross-functional teams to deliver high-quality solutions that meet customer needs.

*Accomplishments:*

* Automated remediation tools delivering improved Compliance and enhanced security controls.
* Successfully implemented Expense Optimization strategies for cloud infrastructure and applications, resulting in significant cost savings ~ 60K $ Monthly
* **Environment**: AWS (EC2, VPC, ELB, S3, RDS, Cloud Trail, Route 53, IAM, Cloud watch, Cloud Formation, EMR, Athena, Beanstalk, KMS, ACM, Guard Duty, Cloud Trail, Config, CloudWatch, WAF, AWS Security Hub, IAM Roles, Security Groups, Network ACLs, AWS Cost Explorer, AWS Trusted Advisor, AWS Cost and Usage Report, AWS Budgets Kinesis, DMS, SNS, SQS and Systems Manager), AWS CLI, Jenkins, Bitbucket, Python, Terraform and Splunk.

**Client - The Depository Trust & Clearing Corporation (DTCC)-Dallas, TX Feb 2019- May 2021**

**Cloud Security and Compliance Engineer**

------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Responsibilities:**

* Acted as point of contact to executive leadership for dimensioning, managing, and driving remediation of information security risk within the context of the DTCC Cloud Infrastructure.
* Provided front-line support for all information security-related issues, such as **Managing SSL Certificates, security policy compliance, handling data confidentiality issues, Monitoring, Detection, and responding to emerging threats**.
* Ensured adequate automated security solutions and controls were in place throughout the Cloud platform and services using tools like **Dome9 and a homegrown tool.**
* **Troubleshot the recurring security findings**, pinpointing the root cause and implementing solutions to prevent recurrence.
* Conducted testing and validation of backup and recovery procedures.
* Developed governance policies, and helped rewrite policies by the new technologies.
* Leveraged SIEM tools (e.g., Splunk) to analyze security logs and identify potential threats, enabling proactive security monitoring.
* Worked collaboratively to define and design secure database access controls and IP restrictions within the firewall configuration, mitigating potential security risks.
* Designed and implemented a consolidated logging solution on Cloud WAF (secure firewall configuration) mitigating potential security risks by restricting inbound/outbound traffic.
* Consolidated WAF logs from multiple AWS accounts into a central SecOps Log Management Account and forwarded them to an SIEM tool for comprehensive threat monitoring and analysis. This enhanced our ability to detect and respond to security incidents across the entire cloud environment.
* Collaborated and communicated with functional-area specialists, cloud architects, and security specialists to design, configure, and/or develop security solutions for the cloud platform.
* Streamlined vulnerability management process by identifying areas for improvement and implementing corrective actions.
* Collaborated with security teams to develop and implement security playbooks for incident response and vulnerability management processes.
* Designed IAM **roles and policies** for services and users in **IAM** limiting to Actions and resources required.
* Provided effective resolutions to issues and escalated problems with knowledgeable support.
* Stayed closely with external auditors and internal audit teams on managing and supporting the audits.
* Effectively communicated complex security concepts to both technical and non-technical audiences, fostering security awareness
* Supported implementation, modification, and improvement of sponsor risk management framework workflow and parts. Driving secure coding initiatives across the company by defining training, identifying weaknesses, and educating developers.

*Accomplishments:*

* Driven and remediated many applications for data protection, access and privilege concerns in Cloud resulting improved compliance across the organization.

**Environment**: AWS (EC2, VPC, ELB, S3, RDS, Cloud Trail, Route 53, IAM, Cloud watch, Cloud Formation, EMR, Athena, Beanstalk, KMS, ACM, Guard Duty, Cloud Trail, Config, CloudWatch, WAF, Kinesis, DMS, SNS, SQS), AWS CLI, Jenkins, Bitbucket, Python, Terraform, Splunk, Dome9.

------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Client- Santander Bank- Boston, MA Sept 2016- Jan 2019 *Cloud Engineer – Infrastructure Support***

------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Responsibilities:**

* Deployed AWS services **specifically VPC, EC2, S3, EBS, IAM, ELB and Cloud Watch** using AWS Console and AWS Command Line Interface.
* Operated in partnership as part of larger delivery teams which include project managers, business analysts, architects, developers, and change management professionals.
* Experienced in engineering a detailed design of highly available, high capacity geographically distributed applications.
* Authored proof-of-concept prototype applications for demonstration and evaluation purposes.
* Tested and troubleshot application and documented issue resolutions for development team.
* Generated reports and performs analysis on usage, capacity and performance on storage and backup systems.
* Oversaw costing, design, build, and management of infrastructure environments needed in the AWS hosting platform.
* Automated infrastructure using **Terraform** and made it auditable by storing infrastructure changes to a version control system like **GIT**.
* Created Snapshots and Amazon Machine Images for backup and creating clone instances.
* Configured **VPC** with multiple private/public subnets in different **availability zones** for high availability.
* Worked on automating Secure deployments and configuration management tasks with Chef on Cloud Ec2 instances.
* Used Jira for Bug Tracking, **Nagios and Graphite** for System monitoring, **Cloud Watch and Cloud Trial** for monitoring the cloud environment and used SNS for notifying in case of exceeding threshold.

*Accomplishments:*

* Designed highly available, Cost saving and fault tolerant systems using multiple EC2 instances, Auto Scaling, Elastic Load Balance and AMIs.
* Implemented a data processing pipeline using AWS Lambda functions, S3, SNS, SQS, and other services.

**Environment:** AWS (EC2, VPC, ELB, S3, RDS, Cloud Trail and Route 53, IAM, Cloud watch, Cloud Formation), AWS CLI, AWS Auto Scaling, Kinesis, Splunk, Nagios, Terraform, Chef, JSON, Maven, Git, Jenkins, Unix/Linux, Shell scripting.

------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Anjalee Business Solution- Hyderabad, TL May. 2013-Dec 2014**

***Systems Administrator- Infrastructure Support***

------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Responsibilities:**

* Planned and monitored of version control, release management, and configuration management for application development and maintenance.
* Maintained, and troubleshooted issues in Linux servers.
* Established cron jobs scripts on production servers.
* Monitored system activities like CPU, memory, disk, and swap space usage to avoid performance issues.
* Serviced and configured Ubuntu, Centos on remote and desktop servers.
* Installed patches and packages using RPM and YUM in Red Hat Linux.
* Created and modified users and groups with SUDO permission.
* Identified and resolved issues related to setup and network connectivity with the aid of net stat and ping tools.
* Kept flexible schedule and resolved after-hours and weekend emergencies quickly and accurately.

*Accomplishments:*

* Monitored system performance and prevented resource exhaustion using ssh, vmstat, iostat, netstat and nmon.
* Worked with other administrators to strategize and improve systems/productivity.

**Education**

***Master’s Degree***, Engineering Management, Lamar University

***Bachelor's Degree***, Electrical and Electronics Engineering, KL University

**Certificates**

* AWS Certified Security – Specialty
* AWS Certified Developer Associate
* Cisco Certified Network Associate (CCNA).