**Charan Kummarapurugu**
charancloud99@gmail.com

Ph: +1- 202 570 4082
Brambleton, Virginia 

**SYNOPSIS**

I am a Senior Cloud and DevSecOps engineer with over 12+ years of experience in designing and implementing technical solutions to achieve business needs. My expertise is in application development, configuration management, delivery pipelines, scalable systems, building serverless applications, containerization technologies, modernization of delivery pipelines, Linux, and automation.

**SUMMARY**

* Experienced as a Cloud Security Engineer, designing and implementing robust security frameworks for IaaS, PaaS, and SaaS platforms.
* Proficient in securing cloud environments through Cloud Security Posture Management (CSPM) and vulnerability management tools.
* Hands-on experience with SIEM solutions, network firewalls, host-based security systems, and security configuration management.
* Secured containerized environments and microservices architectures using Kubernetes, Docker, and industry-standard security practices.
* Successfully integrated and secured Content Delivery Networks (CDNs) for global application delivery.
* Worked with Managed Detection & Response (MDR) providers to set up and investigate security alerts, minimizing response times and enhancing incident handling.
* Investigated security incidents and breaches, developing strategies for response, recovery, and preventing future occurrences.
* Administered serverless and cloud-based enterprise applications across AWS, Azure, and GCP, ensuring optimal security and compliance.
* Developed automation and delivery pipelines for provisioning cloud infrastructure/applications.
* Implemented robust IAM frameworks across multiple cloud platforms, integrating zero-trust security principles to minimize unauthorized access and enhance overall cloud security posture.
* Designed and executed comprehensive security strategies on AWS, employing AWS Security Hub to monitor and manage security alerts effectively
* Extensive experience integrating security tools such as SonarQube (SAST) and OWASP ZAP (DAST) into CI/CD pipelines, enhancing software security during development and deployment.
* Proficient in automating security testing and monitoring within CI/CD pipelines using Jenkins, GitLab CI, and other tools to detect vulnerabilities early in the development cycle.
* Strong background in conducting regular security assessments and audits, developing incident response plans, and maintaining comprehensive security documentation.
* Hands-on experience with AWS security services, including AWS IAM, AWS KMS, and AWS Shield, to enhance cloud security.
* Skilled in managing and optimizing Docker images using Anchore Engine to ensure compliance and security standards
* Implemented Secure Cloud Computing Architecture (SCCA) by following Defense Information Systems Agency (DISA) guidelines and best practices.
* Proficient in writing Infrastructure as a Code (IaC) using Terraform, Azure ARM, Cloud Formation Templates, AWS CDK(typescript) for cloud infrastructure setup.
* Have experience in creating CI/CD pipelines using multiple tools like Jenkins, AWS CodeCommit, Gitlab Pipelines, Azure DevOps, Argo CD, Spinnaker as per application team requirements.
* Created Golden images in multiple clouds using tools like Hashicorp Packer.
* Created serverless and automation solutions using python, AWS Lambda.
* Implemented continuous integration and continuous delivery (CI/CD) of the applications using Git, Github Actions, SonarQube, IaC(terraform), ansible playbooks.
* Experienced in installation, configuration and administration of Windows, Ubuntu Linux, Cent OS and RedHat Environments.
* Developed CIS benchmark reports using python, these reports were used for cloud security assessments.

#### CERTIFICATIONS

* AWS Certified Solutions Architect
* AWS Certified Developers Associate
* AWS SysOps Administrator
* ITIL V3 Foundation certified.

#### EDUCATION

* Masters in Internet and Web Design (August 2014 to Dec 2015)
* Bachelors in Electronics and Communication Engineering (May 2005 to April 2009)

**SKILLS**

**Cloud Platforms** : AWS, Azure and Google Cloud

**AWS Services/SDKs** : VPC, EC2, S3, IAM, RDS, DynamoDB, SSM, CloudFront, SNS, ---------Elastic Beanstalk, Lambda, Step Functions, DynamoDB, Auto Scaling, --ELB, ALB, Kinesis, SQS, ECS, AWS CDK, boto3, CLI, Cloudformation and other services

**Azure Services** : Storage, ARM templates, App Service, Virtual Machines, DevOps Project, AzureBackup, --Cosmos DB, Azure AD, Kubernetes Service (AKS), Logic Apps, ------------Cognitive Services, Functions, Service Bus, and other    services.

**Google Cloud** : Networking Services (VPC, Cloud Load Balancing, NAT, DNS, Hybrid - Connectivity, Cloud Storage, Compute, IAM, GKE

**DevOps Skills** :  Jenkins, Chef, Ansible, Git, Terraform, Vagrant, HashiCorp Vault, --------Vagrant, Docker, Kubernetes, Kubeless, OpenShift, Serverless.

**Programming Languages** : Python, Typescript, Ruby, Shell Scripting, Powershell Scripting

**Source Control Tools** : GIT, AWS CodeCommit, Azure Repos, Bitbucket, Gitlab

**Markup Languages** :  HTML, XML

**Monitoring Tools** : Splunk, Datadog

**OS** : RHEL 5.x/6.x/7.x, HP-UX 11i, CentOS

**Other Skills** : Apache Kafka, ServiceNow, BMC Remedy AR System, ITSM, CMDB, Apache, JBoss, --Web Logic

**EXPERIENCE
CSAA Insurance Group (Remote) Feb 2024 – Till date**(Implementation Partner**: Encloud Services)**

**Sr Cloud Security & DevOps Engineer**

* Designed and implemented robust security frameworks to ensure compliance with CSAA’s regulatory and operational requirements.
* Evaluated, implemented, and optimized security controls and tools, including SIEM solutions, network firewalls, host-based security, and security configuration management, tailored to CSAA’s cloud infrastructure.
* Implemented CDN-based security features such as DDoS protection, Web Application Firewall (WAF), and bot mitigation.
* Leveraged edge computing capabilities within CDNs to reduce the load on origin servers, enabling efficient handling of high traffic volumes during peak insurance periods.
* Secured containerized environments and microservices-based applications using Kubernetes, Docker, and industry best practices.
* Integrated and secured CDNs to improve the delivery speed and security of customer-facing applications.
* Collaborated with Managed Detection & Response (MDR) providers to monitor and investigate security alerts, strengthening CSAA’s incident response capabilities.
* Implemented Cloud Security Posture Management (CSPM) tools and conducted continuous vulnerability assessments to proactively mitigate risks.
* Collaborated with Managed Detection & Response (MDR) providers to monitor and investigate security alerts, strengthening CSAA’s incident response capabilities.
* Utilized tools like AWS Security Hub, Azure Security Center for Cloud Security Posture Management (CSPM).
* Managed cloud resources using Terraform and AWS CDK (TypeScript) for Infrastructure as Code (IaC).
* Setup and managed Kubernetes clusters, deploying applications to Kubernetes.
* Developed and maintained Helm charts for efficient and repeatable Kubernetes deployments.
* Managed a Kubernetes cluster that runs Jenkins workloads, ensuring that the CI/CD environment was highly available and scalable. This included implementing monitoring and alerting solutions to maintain performance and quickly address any issues.
* Used AWS CDK (TypeScript) for deploying application and service-specific AWS resources such as Lambda functions, API Gateways, S3 buckets, and DynamoDB tables, ensuring efficient and tailored infrastructure setup.
* Developed an AWS CDK library tailored to organizational needs and best practices, facilitating the deployment of common resources such as VPCs, IAM roles, launch templates, S3 buckets, and many more.
* Applied fine-grained IAM policies adhering to the principle of least privilege to enhance security.
* Developed and maintained CI/CD pipelines using AWS CodePipelines and Jenkins for building, testing, and deploying applications across various environments.
* Utilized HashiCorp Vault to manage credentials, integrated it with CI/CD pipelines for secure credential management, and to generate temporary credentials.
* Developed a Groovy library for commonly used Jenkins scripts, enabling the team to standardize CI/CD processes across various projects.
* Developed library for CDK in TypeScript to be used by the application team. This library includes services configured with security and best practices, ensuring consistent and reliable deployments.
* Designed and implemented APIs integrated with AWS API Gateway for secure and efficient access.
* Developed serverless APIs using AWS Lambda and Step functions to handle backend processing.

 **Canoo (Torrance, CA)**   **Mar 2022 – Jan 2024**

**Sr Cloud DevSecOps Engineer**

* Evaluated, designed, and deployed security controls, tools, and technology services aligned with Canoo's innovative automotive cloud ecosystem.
* Hands-on experience in deploying SIEM solutions, configuring network firewalls, host-based security systems, and ensuring secure configurations for Canoo’s infrastructure.
* Designed and implemented of CI/CD pipelines using Jenkins, enhancing deployment processes with Jenkinsfiles and Groovy scripting.
* Integrated security tools such as SonarQube (SAST) and OWASP ZAP (DAST) into CI/CD pipelines using Jenkins and GitLab CI.
* Implemented Anchore Engine for scanning Docker images, ensuring compliance and security standards are met before deployment.
* Developed security configurations for Kubernetes environments, focusing on securing containerized applications and ensuring network security, employing automated tools for continuous security assessments.
* Authored and enforced security policies using OPA (Open Policy Agent) to automate governance across cloud environments, enhancing security compliance and operational reliability.
* Automated security testing and monitoring within CI/CD pipelines to detect vulnerabilities early in the development cycle.
* Conducted regular security assessments and audits to identify and mitigate potential security risks.
* Developed incident response plans and procedures, ensuring a rapid and effective response to security incidents.
* Collaborated closely with development, operations, and security teams to ensure seamless integration and adoption of security practices.
* Maintained comprehensive documentation of security processes, tools, and procedures.
* Used AWS security services like AWS IAM, AWS KMS, and AWS Shield to enhance cloud security.
* Designed and implemented automated Image creation pipelines using HashiCorp Packer and Ansible to build secure and reliable AMIs on AWS and GCP.
* Developed RESTful APIs using FastAPI.
* Managed Kubernetes application deployments utilizing Argo CD for reliable and streamlined operations.
* Wrote Infrastructure as Code templates (Terraform) to automate the provisioning and management of cloud infrastructure, ensuring efficient, repeatable deployments.
* Automated various operational tasks through scripting in Python, Powershell, Bash.
* Developed and implemented Jenkins Infrastructure as Code (JIAC) with Groovy scripts and seed jobs, automating Jenkins job management.
* Authored and optimized Jenkinsfiles for multiple projects, orchestrating CI/CD pipelines for automated build, test, and deployment processes.
* Created and maintained a shared Jenkins library, encapsulating commonly used pipeline functionalities to streamline and standardize CI/CD processes across projects.
* Implemented Hashicorp Packer for automated image bakery, streamlining the process of creating consistent and pre-configured virtual machine images for various platforms.
* Implemented and managed cloud security measures, including identity and access management, network security, and compliance adherence.
* Implemented GitHub Actions for automated CI/CD pipelines, enhancing efficiency and reliability of software delivery.
* Develop and maintain microservices and serverless architectures, ensuring scalability and efficient resource utilization.
* Automate security and compliance checks to ensure continuous adherence to standards and best practices.
* Developed Serverless solutions using python, boto3, lambda, step functions, and serverless-framework.

**Sr Cloud DevOps Engineer Hitachi Vantara and REAN Cloud Sep 2015 – Mar 2022**

 (REAN Cloud acquired by Hitachi Vantara on Oct 2018)

* Designing and executing end-to-end cloud implementations for multiple organizations.
* Designed and Implemented landing zones / secure cloud architectures for cloud platforms such as AWS, Google cloud, and Azure.
* Experience developing, implementing, and maintaining highly secure and reliable solutions that meet organizational Cybersecurity and Information Assurance requirements (FedRAMP, DISA STIG, CIS benchmarks)
* Conduct systems design, feasibility and cost studies and recommend cost-effective cloud solutions.
* Automate build, test, and release processes.
* Develop automation and delivery pipelines for provisioning cloud infrastructure and applications.
* Designing architecture, deployment, and migration of the applications from the physical environment to the Cloud environments.
* Design, implemented, and tested Disaster Recovery (DR) plan for workloads running in AWS.
* Design and develop Serverless solutions using python, boto3, lambda, step functions, and serverless-framework.
* Developed Serverless solutions using python, boto3, lambda, step functions, and serverless-framework.
* Developed continuous integration and continuous deployment (CI/CD) pipeline for deploying applications to the cloud, starting from nothing, and resulting in a running application, with everything fully customizable, and utilizing both architecture and security best practices.
* Implemented continuous integration and continuous delivery (CI/CD) for applications using Jenkins, Git, Terraform & AWS CFT (Infrastructure as a code), SonarQube, ansible playbooks & chef cookbooks (Configuration management), Serverless-framework, JFrog (Artifact management), XL release (release pipeline).
* Implemented CI/CD pipelines to run workloads on Kubernetes cluster as well. Used GitHub, Jenkins, SonarQube, Anchore (for container security), Shell checks, Hadolint, Spinnaker (for deployments), Container registries such as AWS ECR, Google Container registry (for storing docker images), Helm charts (package manager), chart museum (chart repository) and Grafana + Prometheus (for monitoring).
* Developed CIS benchmark reports using python, these reports were used for cloud security assessments.
* Created and deployed functions on Kubernetes cluster using Kubeless (Kubernetes-native serverless framework).
* Experience with various IaC tools – AWS CloudFormation, AWS CDK (typescript), Terraform, Azure ARM Templates.
* Designed and implemented backup solution in serverless fashion.
* Created docker images using Docker file and deployed images on Kubernetes cluster.
* Created pipelines using Domain Specific Language (DSL)
* Used serverless-framework to develop, deploy and test serverless solutions in cloud(AWS/Azure/GCP)
* Designed and Developed CloudWatch logs archival and deletion solution. This solution is helpful to reduce costs and archive the huge number of logs that are getting accumulated in CloudWatch logs.
* Developed scripts to identify resource and service health issues and outages, and send email alerts to the team.
* Designed and implemented centralized logging architecture to store all logs in one place and feed them to monitoring tool such as Splunk.
* Fortified cloud network architectures by deploying sophisticated security group and ACL configurations, reducing the risk of unauthorized access and potential data leaks
* Automated vulnerability scanning and compliance checks using tools like AWS Inspector and third-party security tools.
* implemented SIEM/SOAR solutions to streamline threat detection and response.
* Utilized Python to create scripts for security automation and observability, improving the efficiency and responsiveness of security operations across cloud infrastructures
* Experience with network protocols such as DNS, TCP/IP, SMTP & SNMP.

**Tata Consultancy Services Ltd, Hyderabad, India**  **Oct 10 – July 14**

**Systems Engineer**

* Administration of Linux Server which includes Disk checks, permission related issues, user and group administration, File system management partitions, and scheduling tasks using cron jobs
* Implemented Continuous Integration / Continuous Deployment (CI/CD) using Jenkins for automated builds.
* Used Shell to automate the Linux System Maintenance tasks and to develop Deployment utilities.
* Used Github as version control and source code repository for storing Application code and scripts.
* Performed customizations in BMC Remedy ITSM & SR as required by client.
* Worked on Automations using Python and Shell scripting
* Maintained and administered source code archive databases (e.g., Source Repository for version management of source code which included Subversion and Bug Reporting for adding users and fields, and changing permissions).

**Environment**: Linux, Shell, Python, BMC Remedy, Git, Jenkins, CI CD.