Muni Naga Agastya Eeswar Reddy Katamreddy

· **LinkedIn:** Agastya Reddy
· **Mobile No:** +91 (868)-864-4884
· **GitHub:** Agastya Reddy
· **Gmail:** katamreddyagastya@gmail.com

PROFESSIONAL SUMMARY

- Around 1 years of teaching experience as an Associate Cloud Security Engineer with focus on DevSecOps practices.
- My exceptional ability in organizational and communication skills has enabled me to execute and manage multiple projects to meet set objectives.
- Strong in concepts of AWS Services, DevSecOps, Cloud Security, Database Systems, Web Application Development, Python, etc.
- Good knowledge and hands-on experience with the AWS services including EC2, S3, RDS, DynamoDB, Lambda, Beanstalk, VPC, IAM, Route53, Cognito, CICD, Cloud Formation, etc.
- Good knowledge and hands-on experience with Docker/ECS/EKS/Kubernetes and integrating security into containerized environments.
- Proficient in Terraform for infrastructure as code (IaC) provisioning, deploying, and managing AWS resources securely.
- Experience implementing security automation in CI/CD pipelines using tools like Jenkins, GitLab CI, and security scanning tools (SAST, DAST, SCA).
- Skilled in security tools including OWASP ZAP, DefectDojo, and other SAST/DAST tools for vulnerability assessment and management.

KEY COMPETENCIES

- AWS
- DevSecOps
- Python
- Azure DevOps
- Terraform
- CI/CD
- SAST/SCA/DAST
- Kubernetes
- Docker
- OWASP ZAP
- Cloud Security
- Jenkins

PROFESSIONAL EXPERIENCE

WE45 Solutions, India
Associate Cloud Security Engineer **September 2024 to Present**

- Contributed to AppSecEngineer (WE45's learning platform) by creating and maintaining security training content
- Conducted comprehensive cloud security assessments for client environments across multiple industries
- Integrated security automation into DevSecOps pipelines using Jenkins, GitLab CI/CD, GitHub Actions, and Azure DevOps
- Implemented and configured security tooling including OWASP ZAP, DefectDojo, Nuclei, and Gaia for DAST, SAST, and SCA in CI/CD pipelines

- Developed and implemented threat models and security blueprints for cloud-native applications
- Created technical documentation and implementation guides for AWS security services
- Worked extensively with AWS services including EC2, S3, RDS, DynamoDB, Lambda, VPC, IAM, CloudTrail, GuardDuty, AWS Security Hub, KMS, and WAF
- Developed lab environments for hands-on security training and demonstrations
- Designed and implemented secure Docker and Kubernetes environments with proper security controls
- Automated infrastructure provisioning using Terraform with built-in security best practices

Sree Venkateshwara college of Engineering, Nellore
Assistant Professor **November 2021 to September 2023**

- Instruct and accumulate reports in a precise and convenient way and grade the assignments, projects, and tests.
- Encouraged students to develop communication skills and higher order thinking skills to tackle complex assignments.
- Actively engage in the areas of pedagogy, curriculum, student advising, and Computer Science initiatives.
- Delivered engaging polytechnic course in Computer Science, employing innovative teaching methods, developing course materials, and providing mentorship, resulting in positive student feedback.

PROFESSIONAL DEVELOPMENT

- Hands on experience in AWS Cloud Infrastructure for designing and building web environments. Deployment, automation, management, and maintenance of AWS cloud-based production systems using AWS EC2, S3, Route53, ASG, Load Balancing, ECR, ECS, SQS, SNS, IAM, Lambda, RDS, VPC, Beanstalk, Cloud Formation, Dynamo DB, CICD, Cognito, etc.
- **Docker/ECS** to orchestrate the deployment, scaling, and management of containers for CI/CD systems to build, test, and deploy.
- Proficient in using Configuration Management tools such as Terraform.
- Created hands-on labs for AWS cloud security covering services like CloudTrail, GuardDuty, Security Hub, KMS, and WAF.
- Developed practical laboratory environments for DevSecOps implementations using Jenkins, GitLab CI/CD, GitHub Actions, and Azure DevOps.
- Built interactive training labs for security tools including OWASP ZAP, DefectDojo, Nuclei, and Gaia to demonstrate secure scanning and vulnerability management.
- Created Docker container security labs focusing on security best practices, secure images, and runtime protection.
- Developed Infrastructure as Code labs using Terraform with emphasis on secure provisioning and compliance as code.

PROJECTS

- ### Title: Comprehensive DevSecOps Pipeline with Multi-Tool Security Testing

  Description: Designed and implemented a robust DevSecOps pipeline integrating three security testing approaches for complete application security coverage. Created a unified Azure DevOps CI/CD solution that performs Dynamic Application Security Testing (DAST) using OWASP ZAP for runtime vulnerability detection, Static Application Security Testing (SAST) for source code analysis of Python and Node.js applications to identify issues like hardcoded credentials and insecure functions, and Software Composition Analysis (SCA) to detect vulnerable third-party dependencies with known CVEs. The pipeline automatically deploys test applications, executes all three security testing methods in sequence, and generates comprehensive reports in standardized formats published as pipeline artifacts. This implementation ensures vulnerabilities are detected early in the development lifecycle through a fully automated process, enhancing application security without manual intervention.

  Services used: Azure DevOps, Azure Pipelines, OWASP ZAP, Python, Node.js, Docker, Custom Security Scanning Tools, CI/CD integration, and automated vulnerability reporting.

- ### Title: Secure Content Streaming Platform with Tiered Access Control

  Description: Developed a secure digital content delivery platform with tiered access control using AWS cloud services. Designed and implemented an architecture that distinguishes between free and premium content through secure signed URLs. Created a user management system with secure profile image uploads via pre-signed URLs. Premium content is protected using CloudFront signed URLs with time-limited access tokens, preventing unauthorized sharing and access. Free content is delivered through optimized direct delivery paths. Implemented comprehensive security measures including access policies, time-based URL expiration, content encryption, and secure storage configurations to protect valuable digital assets.

  Services used: Amazon CloudFront, Amazon S3, AWS IAM, AWS Lambda, Amazon EC2, AWS SDK (Boto3), Amazon RDS, Amazon Route 53, Amazon VPC, CloudFront Key Pairs, and Terraform for infrastructure provisioning.

- ### Title: Scalable Nginx Deployment with Auto Scaling and Load Balancing on AWS EC2.

  Description: This project focuses on deploying a scalable and highly available Nginx web server on AWS EC2 instances. It leverages AWS Auto Scaling Groups (ASG) to ensure the deployment dynamically adjusts to traffic demands, maintaining optimal performance. An Elastic Load Balancer (ELB) is configured to distribute incoming traffic across multiple EC2 instances, enhancing fault tolerance and availability. The ASG is set with a minimum of 1 instance, desired capacity of 2 instances, and a maximum of 3 instances to balance cost and performance. The setup is designed to handle varying load conditions efficiently while providing seamless user experiences. This infrastructure ensures robust, automated scaling and reliable load balancing, ideal for web applications requiring high availability and scalability.

  Services used: Amazon EC2, Amazon VPC, Amazon ASG, Elastic Load Balancing, Amazon Security Groups, Amazon EC2 Key Pairs and Amazon Machine Image.

- ### Title: Multi-VPC Infrastructure with Secure Communication and Enhanced Security Measures.

  Description: This project entails the creation of an advanced and secure AWS multi-VPC architecture utilizing Terraform. It includes the setup of two Virtual Private Clouds (VPCs) named Chennai and Nellore, each with distinct subnets to segregate public and private traffic. VPC peering was established to enable seamless and secure communication between the two VPCs. A NAT Gateway is deployed in the Chennai VPC to facilitate internet access, for instance in private subnets, while a Bastion Host provides secure SSH access. Enhanced security measures are implemented through security groups and network ACLs, ensuring robust protection for all resources. This comprehensive infrastructure setup is designed for high availability, scalability, and security, making it suitable for complex and demanding applications.

Services used: Amazon VPC, Amazon EC2, Amazon VPC Peering, Amazon EIP, Amazon NAT Gateway, Amazon Internet Gateway, Amazon Route tables, Amazon Security Groups, Amazon Network ACLs and Terraform.

EDUCATION

Bachelor of Technology (B. Tech) · Computer Science · Jawaharlal Nehru Technological University · August 2021

CERTIFICATION

- AWS Certified Developer Associate Course Completed from **UDEMY.**

LEADERSHIP AND ACHIVEMENTS

- Led the team and Presented on the topic **“Insight into Modern Robotics.”**
- Led the team and presented on the topic **“Smart Trashcans.”**
- Led the team and presented on the topic **“Firewall.”**

ACADEMIC PROJECTS

Bachelor’s project **“Detecting group shilling attacks online based on K-means clustering algorithm.”**

- Led the team by overseeing everyday work of the team, distributing the workload evenly among team members and making sure motivation and performance levels are maintained.
- A method was developed to identify and reduce the fake profile reviews to any online products.