**Singaaravelavar Jagannathan**

**Senior Security Engineer** **– Cloud**

**Email:** [singaaravelavarjl@gmail.com](mailto:singaaravelavarjl@gmail.com) **Phone No:** +91 7349094128 **DOB:** 10-04-1995

# Career Objective

Seeking a challenging career in Cloud Computing **(AWS, Azure & GCP).** Looking to solve **business problems** of organization by contributing with **development of Technology solutions** and to grow professionally.

# Experience Summary

* 4+ years of IT experience as a Senior Cloud Security Engineer, specializing in multi-cloud security solutions (AWS, Azure, GCP).
* Extensive hands-on experience in implementing security technologies, cloud architectures, and security tools (Wiz.io, Prisma Cloud) to meet enterprise and regulatory security requirements.
* Proficient in streamlining cloud security operations, ensuring compliance with industry standards such as HIPAA, NIST, and healthcare-specific frameworks.
* Expertise in automating security tasks using Python, Shell, and PowerShell scripts to enhance operational efficiency and reduce manual effort.
* Developed and integrated custom policies, alerts, and monitoring systems for cloud platforms, ensuring consistent compliance and improved visibility.
* Led vulnerability management efforts by identifying and mitigating security risks (e.g., SQL injection, XSS), ensuring secure deployments across cloud environments.
* Strong experience in managing IAM, service accounts, and endpoint security, ensuring least privilege and proper access controls.
* Skilled in using tools like Prisma Cloud, Wiz.io, and AWS CloudWatch for monitoring, alerting, and reporting on security incidents, incidents, and non-conformances.
* Successfully implemented security policies, cost optimization strategies, and automation workflows across healthcare, semiconductor, and pharmaceutical sectors.
* Expertise in ITIL processes (Incident, Problem, Change Management) and cross-team collaboration to resolve critical security issues and improve overall security posture.

**Projects Walkthrough**

1. **Genpact – Dec 2020 to September 2022**

|  |  |
| --- | --- |
| **Designation** | Technical Associate |
| **Role** | Cloud Operations & Security Engineer |
| **Projects Description** | * Hands-on experience with AWS services (IAM, EC2, EBS, S3, VPC, CloudWatch, SNS, Guard Duty, Trusted Advisor, Lambda, RDS, Security Hub, WAF, Systems Manager). * Extensive Linux server administration (Ubuntu, Red Hat, Debian, CentOS) across production, development, and test environments. * In-depth knowledge of VMware technologies, server automation, and virtual infrastructure. * Deployed SSL/TLS certificates for AWS services and managed budgets using AWS Calculator. * Developed Shell/PowerShell scripts for automation and managed patching for 1000+ Linux/Windows instances. * Worked with ServiceNow ticketing tool (GEIT) for incident and access management. * Ensured compliance with security frameworks (HIPAA, GE HealthCare) in collaboration with engineering and cybersecurity teams. * Familiar with ITIL processes (Incident, Problem, and Change Management) and AWS CloudWatch for alerting and monitoring. * Managed security incidents, non-conformance remediation, and threat management in hybrid cloud environments. |

1. **Micron – Sep 2021 to Dec 2023**

|  |  |
| --- | --- |
| **Designation** | Security Engineer |
| **Role** | Cloud Security Engineering & Operations |

|  |  |
| --- | --- |
| **Projects Description** | * Conducted security whitelisting across AWS, Azure, and GCP, implementing robust security controls. * Automated resource provisioning in AWS, Azure, and GCP using Terraform, streamlining deployment. * Leveraged Shell/Python/PowerShell for task automation within GCP, AWS increasing operational efficiency. * Managed Prisma Cloud activities, including setup, RQL queries, and custom report generation. * Resolved configuration, network, anomaly, IAM, and attacker path alerts in Prisma Cloud. * Implemented endpoint security measures (S1 agent, Qualys, Active Directory, Defender, etc.). * Developed Splunk dashboards, Azure Workbooks, and QuickSight visualizations for monitoring. * Created Azure policies to enforce security and compliance best practices. * Utilized GCP Organization policies, VPC service controls, and IAM policy analyzer for security enforcement. * Defined custom roles in GCP and AWS to ensure granular access control and least privilege. * Optimized Azure logging to reduce costs and improve resource utilization. * Used Cortex XSOAR for automation, creating playbooks for security processes. * Managed Azure DevOps for sprint tracking, project management, and code deployment. |

1. **Bristol Myers Squibb – Dec 2023 to Till Date**

|  |  |
| --- | --- |
| **Designation** | Senior Cloud Security Engineer |
| **Role** | Cyber Engineering & Operations |

|  |  |
| --- | --- |
| **Projects Description** | * Designed and implemented security policies in Wiz.io for AWS, Azure, and GCP, enhancing visibility, compliance, and multi-cloud control. * Collaborated with engineering teams to integrate security into development workflows, ensuring compliance and secure deployments. * Resolved non-conformances (configurations, networking, IAM, attacker paths) and monitored alerts to address issues within SLA. * Identified and prioritized vulnerabilities (SQL injection, XSS) while managing container image vulnerabilities with timely communication and follow-up. * Conducted malware analysis, threat modelling, and GitHub workflow reviews to detect threats, secrets, and attack vectors. * Established a data security posture program with risk assessments, security controls, and incident response plans. * Managed service accounts in Wiz by configuring, rotating, and securing them while cleaning up unused accounts. * Created custom controls and dashboards in Wiz to monitor access keys, endpoints, CDN configurations, and vulnerabilities. * Explored auto-remediation processes to automate issue resolution and optimized controls to reduce false positives, saving operational effort. * Conducted Wiz training sessions, onboarded the different environment into Wiz, and collaborated with end users on remediation steps. |

**Technical Skills**

|  |  |
| --- | --- |
| **Cloud** | AWS, Azure, GCP |
| **Scripts** | CloudFormation, Shell, Python, PowerShell, Terraform |
| **Tools** | Prisma, Grafana, Sisense, ServiceNow, JIRA, GitHub, Splunk, Azure DevOps, Bitbucket, Cortex XSOAR, Wiz.io |
| **Operating Systems** | Linux, Windows |

**Training / Certifications**

|  |  |
| --- | --- |
| **Certificate Name** | **Certified By** |
| **AWS Certified Solution Architect Associate** | Amazon Web Services |
| **Microsoft Azure Administrator Associate AZ 104** | Microsoft Azure |
| **Microsoft Azure Fundamentals AZ 900** | Microsoft Azure |

**Educational Qualification**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **Institute/University** | **Year** | **CGPA** |
| **Bachelor of Engineering in Electronics and Communication Engineering** | Kongu Engineering College, Erode | 2012 - 2016 | 6.9 |

**Awards and Recognition**

* 1. Awarded for driving down the security issues in HealthCare by Compliance Team
  2. Given lead role to streamline the SecOps in Cloud environment.
  3. Received recognition from the Wiz team for reducing critical alerts to zero by working with cross-functional teams.