

SARATH S

+91 7356562246 | sarath.sunilkumar@outlook.com | linkedin.com/in/sarath-s | github.com/Sarathyez

PROFESSIONAL SUMMARY

MCA graduate and Computer Science enthusiast with experience in software analysis and development. Passionate about cybersecurity and cloud infrastructure with a strong interest in SOC operations, threat detection, and log analysis, cloud technologies. Focused on continuous learning, problem-solving, and contributing to secure, reliable and scalable system environments.

EDUCATION

Master of Computer Applications

College of Engineering Trivandrum, APJ Abdul Kalam Technological University

2021 – 2023

BSc. Computer Science

Government College Kariavattom, University of Kerala

2017 – 2020

Work EXPERIENCE

No-Code Developer L4

Claysys Technologies, Infopark Kochi

2023 – 2025

- Coordinated and contributed to the development of secure web applications using No Code Platform, handling task planning, workload allocation, team collaboration, and delivery management.
- Supported internal teams in troubleshooting incidents and improving application reliability.
- Conducted code reviews, testing, and deployment to ensure application integrity and compliance.
- Managed and optimized SQL databases, ensuring data security and performance.
- Collaborated with cross-functional teams to analyze and resolve application security findings identified during internal security assessments and reviews, ensuring secure and compliant system behavior. Contributed to strengthening application controls by investigating root causes, validating fixes, and supporting continuous security improvements.

TECHNICAL SKILLS

- Security & SIEM Tools: Microsoft Sentinel, Microsoft Defender XDR, Wireshark, UEBA, KQL, Windows Event Logs, Linux logs.
- SOC & Security: Incident Response, Alert Triage, Escalation Workflow, Log Analysis, Threat Detection, MITRE ATT&CK, ISO 27001 Basics, Network Security Fundamentals, Security Monitoring.
- Cloud & Infrastructure: AWS Cloud Fundamentals, Azure Cloud Fundamentals, IAM / RBAC, Virtual Networks, Firewall Basics, Secure Configuration Practices, Windows & Linux Administration Basics, Monitoring & Logging Concepts.
- Programming: Python, SQL, C/C++, JavaScript, HTML, CSS.
- Frameworks: Django, Flask, Flutter.
- Server & Databases: IIS, MS SQL Server, SQL Server Management Studio (SSMS).
- Platforms & OS: Windows, Linux.
- Others: Data Analytics, AppForms (Low-Code Development), Excel.

PROFESSIONAL SKILLS

- Strong Analytical & Problem-Solving Skills, Attention to Detail & Structured Thinking, Clear Documentation & Reporting Discipline, Team Collaboration & Knowledge Sharing, High Integrity and Compliance Awareness.
-

PERSONAL PROJECTS

- **SOC Incident Detection & Triage Lab** - Developed a simulated SOC lab using Microsoft Sentinel to monitor security events, detect brute-force and anomalous login patterns, investigate alerts with KQL, enrich findings with basic checks, and document triage actions while generating automated alerts.
 - **Audio Book App** - Flutter app using NLP to provide seamless listening experience for book lovers.
 - **Wine Quality Evaluator**- Predicts and rates the Quality of Wine using ML Algorithms.
-

CERTIFICATIONS

- Introduction to Cybersecurity – Cisco Networking Academy
- Microsoft Sentinel Introduction Badge – Microsoft
- Data Analytics Job Simulation – Deloitte Australia via Forage
- Python – Grab Ur Vernacular Imprint (GUVI)

- Database Management Systems – NPTEL (IIT KGP)
-

ACHIEVEMENTS

- Awarded Certificate of Merit for Best Performance – Claysys Technologies, Q4 2024.