SUDARSAN P

Linux | Virtualization | AWS | Networking | SOC

📧 **Email:** sudarsanjuhi@gmail.com | 📞 **Phone:** +91 9789578250
🔗 **LinkedIn:** linkedin.com/in/sudarsanpalaniappan | 🌎 **Portfolio:** pvs-apps.in

---

PROFESSIONAL SUMMARY

Cloud, Linux & SOC Engineer specializing in Linux system administration, cloud architecture, networking, DevOps automation, and security operations support. Proficient with AWS services (EC2, S3, IAM, RDS, ECR, ECS) and Terraform for infrastructure-as-code deployments, along with building secure web servers and containerized environments for scalable delivery. Skilled in SOC-aligned activities including SIEM log onboarding, alert tuning, dashboards/reports, and supporting incident triage workflows. Contributed to SIEM migration activities (SolarWinds SEM to SentinelOne SIEM) by integrating and validating log sources across large endpoint environments. AWS Certified Cloud Practitioner with 40+ deployments/projects across cloud and on-premises environments, focused on delivering secure, reliable, and high-performing systems for Cloud Engineering, DevOps, System Administration, and SOC-aligned roles.

TECHNICAL SKILLS

- **Cloud & DevOps:** Linux, AWS (EC2, S3, IAM, RDS, ECR, ECS), Docker, Terraform, CI/CD, Jenkins
- **Programming & Scripting:** C#,Bash, HTML, MySQL, Python (basic)
- **Frameworks:** ESPHome, Flutter, Magento
- **Cybersecurity Tools:** Metasploit, Nmap, burp suite
- **Technologies & Tools:** Nginx, Apache, VMware, AWS CLI, Visual Studio Code, Photoshop
- **Other Skills:** Networking, Home Automation, IoT Hardware Design, Photography, Video Editing

---

EDUCATION

Diploma in Computer Engineering – Sakthi Polytechnic College, Erode
📅 **June 2020 – June 2023** | **Percentage:** 94%

CERTIFICATIONS

- **AWS Certified Cloud Practitioner** (1000/1000 score) – AWS
- **AWS Data Analyst Certification** –AWS, AICTE

ACHIEVEMENTS

- **Scored 1000/1000 in AWS Certified Cloud Practitioner (CLF-C02)**
- **Best Outstanding Student Award**
- **2nd Place – National Level ISTA Project Expo**

WORK HISTORY

DevOps, Cloud and Linux Engineer | Freelance / Self-Employed (2022` – Present)

- Designed and maintained CI/CD pipelines using Jenkins, GitHub Actions, AWS CodePipeline to automate builds, tests, and deployments.
- Provisioned and managed AWS infrastructure using Terraform, enabling scalable and consistent deployments.
- Containerized applications using Docker and deployed on AWS ECS; managed secure image workflows with AWS ECR.
- Administered and hardened Linux servers (patching, SSH hardening, firewall rules, backups, performance tuning, HA).
- Configured and optimized Nginx reverse proxy (TLS/SSL, routing, caching, rate limiting) for web applications.
- Implemented monitoring and logging (alerts, dashboards, retention policies) for proactive availability and performance management.

SOC Engineer | Freelance / Self-Employed (2025 – Present)

- Supported SOC onboarding and SIEM integration by collecting logs from ~500 workstations and servers plus network/security devices; ensured parsing, timestamps, and completeness.
- Built and standardized log onboarding templates (source type, facility/severity, event categories, retention, and validation checklist).
- Created and tuned alert rules/use cases (brute force, suspicious logins, privilege escalation indicators, malware/IOC matches, lateral movement signals) and reduced false positives through suppression/allow-lists and threshold tuning.
- Developed incident triage workflow (severity classification, escalation matrix, evidence collection steps, containment recommendations).
- Integrated SIEM alerts with email/Teams/Slack and ticketing tools (as per client environment) to ensure traceable incident tracking.
- Performed daily health checks for log pipelines/agents/collectors (ingestion lag, dropped events, forwarder failures) and implemented alerting for data gaps.
- Coordinated incident response support: log investigation, timeline creation, endpoint isolation guidance (where applicable), and post-incident reporting.

- Delivered SOC documentation: runbooks/playbooks, SOPs, onboarding guides, and knowledge transfer sessions for analysts and IT teams.
- Assisted in implementing security best practices: least privilege, audit logging enablement, baseline monitoring, and periodic review of high-risk alerts.

Govt. vetri nichayam Trainer (OCT-2025-JAN 2026)

AWS Training Delivery

• Delivered instructor-led AWS Cloud training for students/professionals under Govt. Vetri Nichayam program (online/classroom).

• Conducted hands-on labs covering core AWS services: EC2, S3, IAM, VPC, RDS, CloudWatch, Route 53.

• Explained cloud fundamentals: IaaS/PaaS/SaaS, shared responsibility model, regions/AZs, pricing & billing basics.

• Designed training sessions with real-world use cases (web hosting, backup, monitoring, scaling, security).

Lab & Project Setup

Built and guided learners through mini-projects such as:

- Static website hosting using S3 + CloudFront
- EC2 deployment with security groups, key pairs, Linux setup
- VPC networking (public/private subnets, route tables, NAT basics)
- Monitoring & alerts using CloudWatch metrics/alarms/logs

• Created lab manuals, step-by-step notes, and troubleshooting guides for smoother learning.

Cloud Security & Best Practices

• Trained learners on AWS security practices: IAM users/roles/policies, MFA, least privilege.

• Implemented and taught account governance basics: tagging, cost control, resource cleanup, budgeting.

• Introduced Well-Architected Framework concepts: security, reliability, cost optimization, performance efficiency.

Outcomes & Soft Skills

• Mentored learners with doubt-clearing, assignments, and interview preparation (cloud + Linux basics).

• Evaluated progress through quizzes, lab assessments, and project reviews; improved practical readiness.

• Coordinated batches, maintained attendance/performance tracking, and ensured course completion.

Cybersecurity Intern | Ediglobe (2024)

- Conducted security assessments and implemented phishing awareness campaigns.
- Applied cybersecurity best practices to strengthen system defenses.

AWS Cloud Virtual Intern | March 2023 – May 2023

- Gained hands-on experience with AWS services including EC2, S3, IAM, ECR, ECS, and implemented cloud security best practices.
- Contributed to real-world AWS projects involving cloud solution deployments and infrastructure management.

PROJECTS

Current Project: SolarWinds SEM → SentinelOne SIEM Migration

Led an end-to-end SIEM migration from SolarWinds SEM to SentinelOne SIEM, covering discovery, target architecture, log source onboarding, detection use-case rebuild, dashboards, alert routing, and go-live cutover. Standardized log parsing/normalization, improved alert fidelity, and established operational runbooks/playbooks for SOC monitoring. Delivered a stable SIEM environment with validated ingestion, reporting, and incident workflows across endpoint and network log sources.

- Integrated logs from **~500 workstations and servers** plus network devices; validated ingestion quality (parsing, timestamps, completeness).
- Rebuilt and tuned priority detection rules, dashboards, and alerting to reduce false positives and improve incident visibility.
- Established SOC operations with alert routing/escalation workflows, runbooks, and knowledge transfer.

Past projects :

- **Giga-Drive & S-Drive**: Secure file storage and sharing platforms.
- **ShopKing E-commerce**: Scalable online store with mobile app.
- **CineFlex**: Movie streaming with personalized recommendations.
- **Private AI**: Privacy-focused AI automation solution.
- **Customer Care IVR**: Automated phone support system.
- **AI Chatbots**: Smart customer support bots using NLP and OpenAI.