VISHNU RAJAN

NOC Engineer | SOC Analyst | System Administrator

vishnudevagiri303@gmail.com
+91 9048XXXXXX
linkedin.com/in/vishnudevagiri
Trivandrum, Kerala, India

PROFESSIONAL PROFILE

Cyber Defence-trained IT professional with hands-on experience in SOC operations, network/system administration, and security monitoring. Holds Microsoft SC-200 (Security Operations Analyst) and Cisco CCNP certifications. Proven in Splunk-driven log analysis, incident response, and enterprise system support. Credited security researcher via Open Bug Bounty (OBB-4097375) with real-world vulnerability assessment experience.

CORE SKILLS

Security	Splunk · SIEM · SOC Operations · Threat Intelligence · Log Analysis · Incident Response
Systems	Windows Server · Linux (Ubuntu/CentOS) · Active Directory · Virtualisation · Backup & Recovery
Networking	Routing & Switching · Network Monitoring · TCP/IP · Firewall Management · VPN · Remote Support
AppSec	Burp Suite · OWASP Top 10 · Penetration Testing · CVE Research · Bug Bounty

WORK EXPERIENCE

Network & IT Support Engineer | Verbat Technologies

2024 – Present • Trivandrum

- Installed, configured, and hardened Windows and Linux systems across enterprise environments, maintaining security baselines and operational uptime
- Monitored system performance and security logs using Splunk to detect anomalies, escalate incidents, and reduce mean time to respond (MTTR)
- Managed server administration, virtualisation workflows, and backup & recovery operations for business continuity
- Delivered tier-1/2 remote helpdesk support and end-user troubleshooting; reduced ticket resolution time through process documentation
- Collaborated on network infrastructure maintenance including switches, routers, and VPN configuration

Independent Security Researcher | Verbat Technologies (verbat.com)

2026 • Trivandrum

- Conducted a full security audit of a production Laravel 8 web application, uncovering multiple critical vulnerabilities (CWE-284 Improper Access Control)
- Discovered exposed .env file with live SMTP credentials and APP_DEBUG=true in production — directly enabling CVE-2021-3129 Remote Code Execution via facade/ignition
- Identified end-of-life dependencies (Laravel 8, Guzzle 7.0) carrying known CVEs for RCE, SSRF, and authentication bypass through exposed composer.json
- Responsibly disclosed all findings via Open Bug Bounty (OBB-4097375), demonstrating ethical research and professional vulnerability disclosure practices

CERTIFICATIONS

SC-200: Microsoft Security Operations Analyst — Microsoft	*July 2025*
CCNP Routing & Switching 300-101 ROUTE — Cisco Networking Academy	*March 2025*
Advanced Diploma in Cyber Defence (ADCD) — RedTeam Hacker Academy	*Nov 2024*

EDUCATION

B.Sc. Computer Programming
Indira Gandhi National Open University
2024 – 2027 (Ongoing)

Adv. Diploma — Cyber Defence
RedTeam Hacker Academy
Jan 2023 – Nov 2024

Diploma in Computer Application
C-DIT Kerala
2023