

ROOPESH VP

SOC Analyst L1

📞 +91 7994494235 | ✉ roopeshvp377@gmail.com | 📍 Perinthalmanna, Kerala, India

🔗 LinkedIn: [linkedin.com/in/roopesh-vp-691093260](https://www.linkedin.com/in/roopesh-vp-691093260)

SUMMARY

Recent cybersecurity graduate with hands-on SOC operations experience through internships and practical labs. Skilled in log analysis, threat detection, and incident response using tools like Splunk, Wireshark, Metasploit, and Nmap. Strong understanding of SIEM operations, vulnerability assessment, and network security monitoring. Passionate about identifying and mitigating cybersecurity threats, with a commitment to continuous learning and industry best practices.

EXPERIENCE

SOC Analyst Intern

📍 **Technovalley Software India Pvt Ltd** | 06/2024 - 09/2024

- Monitored security alerts and analyzed logs using SIEM (Splunk) for threat detection.
- Assisted in real-time threat analysis, incident response, and vulnerability assessment.
- Gained expertise in Windows & Linux security hardening and intrusion detection.

Python Developer Intern

📍 **Riss Technologies** | 08/2023 - 09/2023

- Developed and debugged Python-based applications, focusing on automation and security scripting.
- Implemented efficient code for data processing, API interactions, and application security.
- Strengthened problem-solving skills through hands-on coding challenges and debugging tasks.

EDUCATION

Bachelor of Computer Applications

SNDP YSS College, University of Calicut | 06/2021 - 06/2024

Higher Secondary Education

GVHSS Mankada | 06/2019 - 06/2021

CERTIFICATIONS

- ✓ **Certified SOC Analyst (CSA)** – EC-Council
- ✓ **ITF+ & TCSP** – Technovalley Software India Pvt Ltd

KEY ACHIEVEMENTS

TryHackMe Achievements

🔗 Profile: <https://tryhackme.com/p/roopeshvp377>

- Completed hands-on labs in SOC operations, threat intelligence, and penetration testing.
- Developed skills in log analysis, incident response, and password cracking using tools like John the Ripper, Hashcat, and Hydra.
- Earned multiple badges for demonstrating practical cybersecurity skills.

LANGUAGES

- **Malayalam** – Native
- **English** – Proficient
- **Hindi** – Intermediate

CYBERSECURITY SKILLS

- Security Information and Event Management (SIEM) – Splunk
- SOC Monitoring & Incident Triage
- Log Analysis & Correlation
- Threat Hunting & Incident Response
- Vulnerability Assessment & Risk Management
- Windows & Linux Security Hardening

SECURITY TOOLS

- **SIEM Tools:** Splunk
- **Network Analysis:** Wireshark, Nmap
- **Pentesting & Exploitation:** Metasploit, Burp Suite
- **Password Cracking:** John the Ripper, Hashcat, Hydra
- **Scripting & Automation:** Python, Bash

ACADEMIC PROJECT

Clinic Management System

- Developed a mobile web application that streamlines clinic operations.
- Automated appointment scheduling, patient tracking, and medical record management.
- Integrated a pharmacy module for prescription processing and medication tracking.