Nasarul Naseer

Cybersecurity Analyst (SOC/NOC)

Kochi, Kerala • +91 77368-82643 • nasarulnaseer.career@gmail.com • Linkedin • Github

Education

MG UNIVERSITY Edappally, Kerala
BSc Cyber Forensics October 25 – April 25

TECHNOVALLEY LIMITED Kochi, Kerala
Technovalley Certified SOC Practitioner August 24 – December 24

Technical Skills/ Soft Skills

Security Monitoring: Splunk, Sentinal, Wazuh, EDR/XDR, Threat hunting, Incident triage
Network & Logs: TCP/IP, DNS, HTTP/S, SSH, Wireshark
System & Cloud Admin: Linux (AlmaLinux, RHEL, Ubuntu), WHM/CPanel, Plesk, AWS, VMware, SSH
Vulnerability & IDS/IPS: Qualys, Nessus, Snort, Suricata
Web Security: Apache, NGINX, MariaDB, PHP, WordPress, Magento
Compliance & Frameworks: MITRE ATT&CK, OWASP Top 10, NIST, ISO 27001
Soft Skills: Analytical, Clear communicator, Quick learner, Team player, Calm under pressure

Practical Projects

Cloud Based SOC Operations & Threat Detection

- Built a SOC lab using VMware with LimaCharlie EDR, Sysmon, and Sliver C2 to simulate real-world attacks
- Authored detection and response rules for behaviors like LSASS access and PowerShell persistence
- Analyzed endpoint telemetry, performed threat hunting, and tuned detections to reduce false positives

Experience

LINUX SERVER ADMINISTRATOR Kochi, Kerala
HashRoot | Internship April 25 – Present

- Configured Apache, NGINX, SSL, virtual hosts, and basic firewall rules on Linux servers
- Performed WordPress migrations: DNS, database, backups, and troubleshooting.
- Worked with cPanel and Plesk: domain setup, AutoSSL, mail records, PHP settings, backups.

DIGITAL FORENSICS INTERN Kochi, Kerala
Cyber Cell Kochi City Police | Internship January 25 – February 25

- Conduct disk imaging, malware analysis & log reviews for digital evidence
- Support incident response and root-cause investigations in active cybercrime cases

VIDEO EDITOR/ CONTENT CREATION Kochi, Kerala
Freelance | Part time September 21 – October 24

- Produced high-performing content for Instagram (800K+ followers) and YouTube (100K+ subscribers)
- Managed editing workflows and file security, ensuring timely and confidential content delivery
- Implemented remote collaboration tools and resolved technical issues to maintain workflow uptime

Certifications

- ★ **Certified SOC Analyst v1 - EC Council**
- ★ **Qualys Vulnerability Management - Qualys**
- ★ **ISO/IEC 27001:2022 Lead Auditor - Mastermind**
- ★ **SOC Essentials: Investigating with Splunk - Splunk**
- ★ **Intro to Threat Hunting - Security Blue Team**
- ★ **Google Cloud Cybersecurity Certificate (Expected 06/25) - Google**