Mohan Kumar M

SECURITY ANALYST

+91 8951676291

mohanmdvg@gmail.com

TOOLS & TECHNOLOGIES

- Splunk
- IPvoid.com
- VirusTotal.com
- Wireshark
- MXToolbox.com
- Any.run
- Nmap
- Nessus
- TrendMicro EDR

AREAS OF INTEREST

- Threat Hunting
- Threat Intelligence
- Malware Analysis
- Vulnerability & Patching
- Endpoint Security

CERTIFICATIONS

- SPLUNK fundamentals
- SOC Experts Certified Security Analyst

EDUCATION

Bachelors - Computer Science

Jain Institute of technology,

Davangere,Karnataka

OBJECTIVE

Seeking to further my cybersecurity career by growing with a team where my acquired skills will be utilized for the betterment of the company.

SUMMARY

- 2.5 years of experience in Security Operations.
- Solid understanding of common network services anda protocols.
- Good knowledge on cyberattacks and attack vectors.
- Working knowledge on security solutions like antivirus, firewall, IPS, Proxy, WAF etc.
- Exposure to using MITRE ATT&CK for threat hunting.
- Good experience in working/communicating with cross-functional IT infrastructure

WORK EXPERIENCE

Virtusa Consultancy Services
Security Analyst
Sep 2021 – Till Date

- Monitoring Security alerts generated by SIEM.
- Analyzing SIEM alerts by following runbooks and using various tools.
- Generating tickets for validating incidents.
- Assist in identifying Root Causes of incidents and follow-up with SMEs for incident closure.
- Assist the team lead in generating weekly report.
- Documentation of alerts.
- Draft Shift Handover.