MIDHUNRAJ M

Cybersecurity Analyst
LinkedIn Profile | **midhunr402@gmail.com** | **+91 8590580691**

Objective

A passionate cybersecurity analyst with hands-on experience in SOC operations, SIEM tools, and incident response. Eager to leverage my technical expertise and problem-solving skills to protect organizational assets and contribute to a secure digital environment.

Education

B.Sc in Digital and Cyber Forensic Science Sree Saraswathi Thyagaraja College, Tamil Nadu
2021 – 2024

Certifications

- SOC Expert Certified Security Analyst
- Kerala Police Cyber Security Internship
- Fortinet NSE 1 & NSE 2
- Cybersecurity Foundation (IBM Skill Build)
- Social Networks (NPTEL)
- Digital Forensics Essentials (DFE)
- Splunk E-Learning

Skills

Technical Skills

- **Networking Concepts**: OSI Model, NAT, PAT, Ports, Protocols, TCP 3-way handshake
- **Cybersecurity Principles**: CIA Triad, AAA, Encryption, System Hardening, Defense in Depth
- **Attack Mitigations**: Malware analysis, phishing investigations, brute force alert handling, Event ID correlation
- **Security Solutions**: Firewalls, IPS, WAF, Proxy Servers, Email Gateways
- **Digital Forensic Tools**: FTK, Autopsy, MOBILedit Forensic, EnCase, Stellar

Tools and Technologies

- SIEM: Wazuh, Splunk
- Threat Intelligence: IPVOID, VIRUSTOTAL, ABUSEIPDB, URL VOID
- Scanning Tools: Nessus, Nmap, Wireshark, Metasploit
- Malware Analysis Tools: ANY.RUN, VIRUSTOTAL, Hybrid Analysis
- Server Management: Active Directory, DNS, DHCP

Languages

- English
- Malayalam
- Tamil

Professional Experience

SOC Analyst Intern SOC
Expert | 2023

- Monitored and analyzed logs to identify security incidents.
- Investigated SIEM alerts using playbooks and generated tickets for validated incidents.
- Worked extensively with Wazuh and Splunk for alert creation, dashboard management, and reporting.
- Leveraged forensic tools for data acquisition and analysis.
- Understanding of analyzing SIEM alerts by following playbooks.
- Understanding of the importance of documenting security incidents

Security Analyst IARM Information Security | 2024 – Present

- Proactive monitoring and response of known and or emerging threats.
- Working in 24X7 Security Operations Center
- Raise tickets for validated incidents.
- Preparing daily, weekly and monthly reports as per the client requirement.
- Conducted log reviews and correlation using SIEM tools to identify anomalies.
- Actively participated in incident response, root cause analysis, and remediation.
- Ensured timely resolution of tickets within defined SLAs.
- Perform shift handover at the end of every shift to provide situational awareness to the incoming shift

---

Achievements

- Developed a strong foundation in cybersecurity principles and SOC operations.
- Successfully identified and documented security incidents, improving response efficiency.
- Gained practical expertise in log analysis and SIEM alert management.