HASHIM KM

SOC ANALYST

Phone no: +91-8086104592

Email: hashimkm2001@gmail.com

LinkedIn: www.linkedin.com/in/hashim-k-m
Malappuram, India

OBJECTIVE

Motivated and Certified Cybersecurity professional with hands-on experience in Vulnerability Assessment, Penetration Testing, and Security Operations. Holding EC-Council Certified SOC Analyst (CSA) certification. Seeking an entry-level SOC Analyst position to apply my skills in threat detection, incident response, and continuous learning.

EDUCATION

2023-2024
Certified IT Infrastructure and Cyber SOC Analyst

- RedTeam Hacker Academy, Perinthalmanna

2020-2023
Bachelor of Computer Applications

- Nilgiri College of Arts and Science, Nilgiri, Tamilnadu

TECHNICAL SKILLS

- SQL, JavaScript, HTML
- SIEM
- Splunk | Elastic Stack
- Security monitoring tools
- VAPT
- Exploitation Techniques
- Network Protocols
- Network Traffic Analysis
- Log Analysis
- Tools: Nmap, Burp Suite, Nessus, Wireshark, Metasploit framework

SOFT SKILLS

- Analytical Thinking
- Attention to Detail
- Problem Solving
- Effective Communication
- Team Collaboration

LANGUAGES

- English
- Malayalam
- Tamil

WORK EXPERIENCE

January 2025 - Present
Purple Nexus, Kochi - Intern

- Conducted vulnerability assessments on web applications and discovered critical security flaws.
- Provided actionable remediation reports to strengthen organizational security posture.
- Expanded skill set into SOC operations, gaining real-time experience in monitoring and incident response.

CERTIFICATIONS

Certified SOC Analyst (CSA)

- EC-Council | Valid until September 2027

Tata Group - Cybersecurity Analyst Job Simulation
August - November 2024

- Identity and access management (IAM) fundamentals

CyberSec Infotec - Cyber Security Virtual Internship
March - April 2022

- Gained foundational knowledge of cybersecurity and its principles

PROJECTS

Email Phishing Analysis (Purple Nexus, 2025)

- Analyzed multiple real-world phishing email samples to identify attack patterns and indicators of compromise (IOCs).
- Conducted detailed header analysis, link inspection, and sandbox testing to assess malicious payloads.
- Prepared phishing analysis reports documenting findings, mitigation steps, and prevention recommendations

Web Application VAPT (Purple Nexus, 2025)

- Identified stored/reflected XSS, SQL Injection, weak SSL, and file upload vulnerabilities
- Extracted sensitive data via SQLMap; discovered hidden paths using Dirb.
- Tools Used: Burp Suite, sqlmap, Dirb, Nmap,WhatWeb