MOHAMED RIYAS J

Entry-Level SOC Analyst | Cybersecurity Enthusiast

91+ 9952484540 ☎
mohamed.soc2001@gmail.com ✉
Chennai, TamilNadu, India
Linkedin
Github

SUMMARY

Entry-level SOC Analyst with around 6 month of hands on experience and a strong foundation in threat detection, SIEM tools, and incident response. Trained in cybersecurity fundamentals with hands-on skills in log analysis, phishing detection, and vulnerability scanning. Eager to leverage my IT background to identify, analyze, and mitigate security threats in a modern SOC environment. Committed to continuous learning and contributing to a proactive, risk-aware security posture.

EDUCATION

M.A.M College of Engineering & Tech / Anna University

- BE / Electronics and Communication Engineering - 2022 - 89%

St John's Vestry Anglo Indian Hr Sec School.

- 12th / HSC - 2018 - 74%

CERTIFICATIONS

Cisco Certified – Introduction to Cybersecurity

- Cisco Networking Academy, Issued Aug 2025

Microsoft Student SOC Program – Foundations Training

- Microsoft Issued Jul 2025

Certified in Network Scanning

- **Issued by Cyber Twinkle**

TECHNICAL SKILLS

Security Operations & Monitoring:

- SIEM - performed alert triage and log analysis using security playbooks.
- EDR - monitored endpoints and investigated threats.
- Network Monitoring - analyzed packets, detected anomalies.
- Incident Response: Familiar with response lifecycle, triage, and documentation process.
- Vulnerability Scanning for identify vulnerabilities.
- Malware Analysis: Basic static/dynamic analysis.
- Frameworks: Basic knowledge of MITRE ATT&CK; involved in threat hunting techniques.
- Phishing & Email Analysis: Investigated phishing attacks through email header analysis.
- Security Concepts: Understanding of VPN, SSL/TLS, IPSec, IDS/IPS, and common threats like XSS, SQLi, DDoS.

Tools

- SIEM - Splunk, Wazhu
- EDR platform - CarbonBlack, Crowd Strike
- Network Security Monitoring - Wireshark, Zeek, Suricata
- Vulnerability Scanning - Nessus, OpenVAS
- Fortinet Firewall - Basic configuration knowledge
- Malware Analysis - PEStudio
- Phishing & Email Analysis - Virus Total, MX Tool Box.
- Ticketing - ServiceNow, Jira.

INTERNSHIP EXPERIENCE

ELEVATE LABS

SOC Trainee - Intern | 01-July-2025 to 01-Aug-2025

- Monitored and triaged security alerts using SIEM platforms (Splunk).
- Performed email phishing analysis and conducted IOC investigations using VirusTotal and AbuseIPDB.
- Conducted vulnerability scanning using Nessus, Nmap, and OpenVAS.
- Worked on endpoint protection solutions including CrowdStrike.

PURPLESYNAPZ

Cyber Security Analyst Intern | 01-Jan-2025 to 01-Jun-2025

- Monitor and Analyse the logs or incident from various network security and SIEM tools splunk, zeek, wireshark.
- Detect the unauthorized login or attempt and investigate to determine false positive or true positive.
- Analyze the logs from IDS/IPS, firewall to identifying the potential threat.
- Learn Advanced technology artificial intelligence & machine learning.
- Setup SOC Lab and continuously self weekly report the task.

PROJECTS

SOC Simulation – LetsDefend.io

- Performed alert triage and phishing email analysis; closed alerts, completed full investigations, and finished SOC challenges simulating real-world incidents.

Encrypted Keylogger PoC with Simulated Exfiltration

- Built a proof-of-concept keylogging system for red-team learning and defensive security training. The project simulated encrypted data exfiltration in a controlled environment to understand attacker tactics and improve detection strategies.

Log File Analyzer for Intrusion Detection

- Designed and implemented a Python-based tool to parse and analyze system and network log files for detecting suspicious patterns and indicators of compromise (IOCs). Focused on enhancing log visibility, correlation, and real-time threat detection.