MOHAMED RIYAS J

Entry-Level SOC Analyst | Cybersecurity Enthusiast

91+ 9952484540 ☎
mohamed.soc2001@gmail.com ✉
Chennai, TamilNadu, India
https://www.linkedin.com/in/mohamed-riyas-9905a3326/
https://github.com/riyaz12765

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 Engg & Tech / Anna University

- Electronics and Communication Engineering - 2022 - 89%

St John's Vestry Anglo Indian Hr Sec School.

- 12th / HSC - 2018 - 74%

CERTIFICATIONS

Introduction of Cyber Security - NASBA

- Completed a foundational course on cybersecurity principles at National Association Boards of Accountancy.

Certified in Network Scanning - Cyber Twinkle.

- Completed a Essential course on cybersecurity Nmap Network Scanning at Cyber Twinkle.

TECHNICAL SKILLS

Security Operations & Monitoring:

- Knowledge with SIEM tools: Splunk, Wazhu.
- Performed alert triage and log analysis using security playbooks
- Familiar with EDR tools: CrowdStrike, CarbonBlack.
- Phishing detection and email header analysis.
- Used VirusTotal and AbuseIPDB for IOC enrichment.
- Scanned vulnerabilities with Nessus, OpenVAS, Nmap.
- Basic knowledge of MITRE ATT&CK and threat hunting techniques.
- Familiar with VPN, SSL/TLS, IPSec, and firewall basics, IDS/IPS.
- Knowledge with Types of Threats including XSS, SQL, DDOS.
- Incident response procedure and documentation

Additional Tools & Skills (Self-Learned):

- SIEM - Splunk, Wazhu.
- EDR platform - CarbonBlack, Crowd Strike.
- Network Security Monitoring - Wireshark, Zeek, Suricata.
- Fortinet Firewall – Basic configuration knowledge.
- Malware Analysis Tools – Basic static/dynamic tools like Any.Run, Hybrid Analysis.
- MISP – Threat intelligence sharing and analysis.

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.