Mohamed Riyaz J - Security Operation Center Analyst L1

Ph Number : +91 9952484540

Linkedin : www.linkedin.com/in/mohamed-riyaz-9905a3326

Email : mohamed.soc2001@gmail.com

Github : https://github.com/riyaz12765

A passionate and detail-oriented aspiring SOC Analyst with a strong foundation Knowledge in cybersecurity principles, network protocols, and threat detection methodologies. Completed a 90-day hands-on challenge simulating real-world SOC tasks involving tools like Zeek and other security tools Splunk. Knowledge in analyzing logs, identifying suspicious activities, and documenting incidents in a structured format. Proficient in setting up virtual labs to simulate attacks using Metasploit and monitoring them using defensive tools. Eager to join a dynamic SOC team to contribute to threat monitoring, incident response, and continuous security improvement.

Profile Summary

- Basic Networking Fundamentals such as **TCP/IP, OSI Model, Port, Protocols, Routers**.
- Core Security Technologies: Perform with **core security technologies**, including **SIEM, firewalls, IDS/IPS**, HIPS, proxies.
- Knowledge in different types of threats such as **Malwares, Phishing, Advanced Persistent Threat & MITRE Attack Framework, Cross Site Scripting, Dos & DDos attack**.
- Alert Analysis and Investigation: **Analyzed and investigated alerts in SOC monitoring tools**, identifying abnormal behaviors, suspicious activities, and traffic anomalies.
- **Vulnerability Management** Tools For Continuous Monitoring, Identify, Analyze, Access, Prioritize based on Severity, Impact and Remediate

Technical Skills

- SOC (Security Operation Centre).
- SIEM (Security Information and Event Management) : Splunk, Arc Sight
- Malware Analysis : Defender, McAfee, VirusTotal.
- Phishing Email Analysis tools : Cofense, HoxHunt
- SOAR Automation : Palo Alto Cortex XSOAR
- EDR (EndPoint Detection & Response) : Crowd Strike, CarbonBlack.
- Incident Response

Experience

Role : Cyber Security Analyst Intern

Company : PurpleSyNapz

Location : Benguluru, Karnataka, India.

Duration : 3 Months

Project : Simulated SOC Attack Detection Lab

- Tools Used: Zeek, Kali Linux, Metasploitable2, VirtualBox
- Built a 3-VM lab using Kali Linux, Metasploitable2, and Zeek to simulate cyberattacks and monitor logs.
- Launched attacks from Kali, exploited the victim machine, and captured real-time logs using Zeek.
- Analyzed HTTP, DNS, and connection logs to detect suspicious activity and document findings.

ADDITIONAL SKILLS

- Strong verbal and written communication skills.
- understanding the concepts of TTPs and security threats.
- Strong analytical and problem-solving skills.
- English and Tamil Language.

EDUCATION

- Degree - Bachelors of Engineering / **Electronics and communications Engineering.**
- Institute - M.A.M College Of Engineering & Technology - **Anna University** / 2018 - 2022 / Chennai.