MOHAMMED FAHIZ C K

+91 8547219158
fahizckmohammed@gmail.com
Bengaluru, India.
linkedin.com/in/mohammedfahizck

SOC ANALYST

Skilled Information Security Analyst in the field of cyber security, wide range of vulnerabilities and threats. Well-versed in direct and remote analysis with strong critical thinking, communication and people skills. Able to thrive in fast-paced and challenging environments where accuracy and efficiency matter.

SOC ANALYST SKILLS

- Experience in utilizing Security Information and Event Management (SIEM) tools such as ELK Stack and Splunk for real-time analysis of security alerts, log management, and correlation of event data from multiple sources.
- Acquired basic proficiency in using Wireshark for network traffic analysis and troubleshooting. Able to capture and interpret network packets to detect anomalies and understand network behaviors.
- Trained in the use of vulnerability scanning tools like Nessus and Qualys during coursework and labs. Understand the process of conducting scans, reviewing reports, and identifying common vulnerabilities in systems.
- Developed foundational skills in malware detection using VirusTotal for scanning suspicious files and URLs. Familiar with interpreting scan results to recognize malicious activity and providing insights for further investigation.
- Gained an introductory understanding of security frameworks such as MITRE ATT&CK and the Cyber Kill Chain, enabling the identification of attacker behaviors and threat tactics in a cybersecurity context.
- Demonstrated problem-solving abilities in lab environments, working on cybersecurity challenges that involved identifying vulnerabilities and proposing solutions to mitigate risks.
- Completed training on vulnerability scanning and reporting, with experience generating reports that highlight vulnerabilities and suggest remediation actions, based on lab exercises and internship tasks.

EXPERIENCE

1) SYSTEM ADMINISTRATOR

SunTec Business Solutions (2023 to Present)

- Utilized ELK Stack (Elasticsearch, Logstash, Kibana) for real-time log monitoring and analysis to detect and mitigate security threats.
- Performed incident response by analyzing security alerts, identifying potential security incidents, and escalating issues when necessary.
- Handled alerts generated by various security tools, ensuring timely triage and classification to determine the severity and priority of incidents.
- Created and maintained custom dashboards, providing insightful visualizations to monitor system performance and security events.
- Worked with different teams to quickly resolve incidents and minimize downtime.
- Experience in configuring and managing DLP rules using ManageEngine to safeguard sensitive data. Proven ability to create and enforce security policies that prevent unauthorized access, data leaks, and ensure compliance with regulatory requirements.
- Expertise in creating, configuring, and managing virtual machines and user pools within VMware environments. Adept at provisioning VMs, allocating resources, and ensuring that virtual infrastructure meets organizational demands for performance and scalability.

- Skilled in configuring and managing secure VPN with Fortinet VPN solutions. Experienced in setting up and allocating VPN access for remote users to ensuring secure communication.

2) SECURITY ANALYST
INFOVIRTECH (2022 - 2023)

- Gained hands-on experience in monitoring and analyzing security logs using the ELK Stack during the internship.
- Skilled in configuring dashboards and alerts to track security events, and identifying potential threats by correlating log data from multiple sources.
- Utilized Wireshark to analyze network traffic and detect anomalies that could indicate security threats or performance issues.
- Applied packet analysis techniques to troubleshoot network issues, enhancing overall security and network performance.
- Experienced in conducting port scans using Nmap to identify open ports and potential vulnerabilities in network infrastructure.
- Performed detailed vulnerability assessments with Nessus to identify security weaknesses across systems and networks.
- Practiced executing brute force attacks on systems using Metasploit as part of ethical hacking exercises.

EDUCATION

- **Infrastructure and cyber SOC Analyst**

(RED TEAM HACKER ACADEMY OF SCIENCE AND TECHNOLOGY, Kerala Certified IT | 2021-2022)

- **B TECH - COMPUTER SCIENCE AND ENGINEERING**

(VIDYA ACADEMY OF SCIENCE & TECHNOLOGY | 2017-2021)

SOFT SKILLS

- Excellent written and verbal communication skills for reporting and collaboration.
- Ability to work effectively within a team and coordinate with other departments.
- Flexibility to adapt to evolving threats and changing security landscapes.
- Effective time management skills to handle multiple tasks and incidents simultaneously.
- Commitment to continuous learning and staying updated with the latest security trends and technologies.

TOOLS

- ELK Stack
- Splunk
- Wireshark
- Nessus
- VirusTotal
- MITRE ATT&CK
- Indefend DLP
- Fortinet VPN and Firewall
- Python

CERTIFICATIONS

- Cybersecurity Essential (cisco Networking Academy)
- Introduction to cybersecurity (cisco Networking Academy)
- Technical Support Fundamentals (coursera)
- Splunk Fundamental (Splunk)
- Vulnerability Management (Detection & Responce Qualys)
- Foundations of Operationalizing (MITRE ATT&CK Attack IQ)