Bibin Babu

Kochi, Kerala | bibinbabu3507@gmail.com | +91 6282629550 | linkedin.com/in/bibinbabu
github.com/bibinbabu

Career Overview

I am a cybersecurity professional specializing in blue team and Red teaam operations and Security Operations Center (SOC) analysis. With experience in leading IT companies in Trivandrum, I have expertise in threat detection, incident response, log analysis, and security monitoring. Skilled in SIEM tools, malware analysis, and network defense, I am dedicated to proactively identifying and mitigating cyber threats to ensure robust security postures.

Experience

Cybersecurity Specialist Intern, Acmeflare Technology , Trivandrum, Kerala June 2022 – Aug 2023

- Specialize in blue team operations, focusing on threat detection, incident response, and vulnerability management.
- Monitor and analyze security events using SIEM tools to identify potential threats and mitigate risks.
- Conduct forensic investigations and malware analysis to strengthen security postures.
- Perform security assessments, log analysis, and real-time monitoring to prevent breaches.
- Collaborate with SOC teams to develop and implement cybersecurity policies and best practices.
- Work with tools such as Wireshark, Splunk, Nmap, Metasploit, Burpsuit and EDR solutions to enhance network security.
- Provide security awareness training and assist in compliance audits.

Projects

SOC Analyst – Log Analysis Project

- Conducted in-depth log analysis to detect anomalies, threats, and security incidents.
- Utilized SIEM tools to monitor, analyze, and correlate logs for effective threat hunting.
- Developed automated alerting mechanisms to enhance incident response.

Cybersecurity Tools

- Developed a Caesar Cipher tool for encrypting and decrypting messages using a shift-based method.
- Created a keyboard input capturing tool for automation and security monitoring.
- Built an image encryption tool using a numeric key for securing digital images.
- Designed a network traffic analyzer to capture and analyze TCP, UDP, and ICMP traffic.
- Developed a password strength evaluation tool that provides feedback on password security.

Phishing Attack Investigation

- Investigated real-world phishing attacks to understand attack vectors and methodologies.
- Analyzed phishing emails, URLs, and payloads to identify malicious indicators.
- Used email header analysis, sandboxing, and threat intelligence tools to detect phishing campaigns.
- Developed strategies for phishing awareness and mitigation to enhance organizational security.

Education

Diploma in Cyber Security, Tech By Heart Science Sept 2024 – 2025

BA Literature, MSM collage Sept 2019 – 2022

Certification

- EC Council | Certified Ethical Hacker Master (CEH v12 ELITE)
- EC Council | Certified Ethical Hacker (CEH v12)
- EC Council | Ethical Hacking Essentials (EHE)
- Certified SOC Analyst (CSA)
- CISCO | Ethical Hacker
- arcX | Cyber Threat Intelligence 101
- LetsDefend | Network Fundamentals

Skills

Tools & Software: SIEM, Splunk, Nmap, Metasploit, Burpsuit, Nessus, SQLmap, Nikto, Wireshark, Shodan, Maltego, Snort.

Soft skills: Teamwork, Time management, Critical thinking

Operating System: Windows, Kali Linux, Parrot Security,

Languages: English,Malayalam,Hindi