NASARUL NASEER

Cybersecurity Analyst

Address: Ernakulam, Kerala, India
Phone: +91 77368 82643
Email: nasarulnaseer.career@gmail.com
LinkedIn: linkedin.com/in/nasarulnaseer
Portfolio: github.com/nasarul10

Summary

Cybersecurity professional skilled in SIEM, threat detection, and incident response. Proficient in log analysis, network monitoring, and EDR/XDR, with exposure to cloud security. Familiar with NIST, MITRE ATT&CK, and OWASP frameworks. Continuously expanding expertise through hands-on labs, simulations, and real-time security operations.

Skills & tools

- **SIEM Tools:** Splunk, Wazuh, Microsoft Sentinel (Basics)
- **EDR & XDR Solutions:** LimaCharlie
- **Vulnerability Management:** Qualys VMDR
- **Operating Systems:** Windows, Linux
- **Log Analysis & Threat Monitoring:** Windows & Linux Security Logs, Wireshark
- **Network Security:** TCP/IP, Network Traffic Monitoring
- **Security Frameworks:** MITRE ATT&CK, NIST, OWASP Top 10, ISO 27001
- **Cloud Security:** Basic exposure and monitoring practices
- **Compliance & Risk Management:** Security Compliance methodologies
- **Database Security:** MySQL (Basics)
- **Soft Skills:** Analytical Thinking, Attention to Detail, Team Collaboration, Stress Management, Communication Skills, Adaptability, Problem-Solving Mindset, Time Management, Critical Thinking, Curiosity & Eagerness to Learn

Projects

Project Title: **Cloud Based Security Operations & Threat Detection**
Source: blog.ecapuano.com/Eric's Substack
Tools Used: VMware Workstation - Windows, Linux, EDR - LimaCharlie, Sliver, Log Analytics

- Built a cloud-based SOC lab using LimaCharlie for threat detection and response.
- Developed detection rules using YARA and adversary emulation.
- Analyzed endpoint logs to investigate attacks and enhance response.

Certifications

- Certified SOC Analyst - EC Council
- Qualys Vulnerability Management - Qualys
- SOC Essentials: Investigating with Splunk - Splunk
- Introduction to Threat Hunting - Security Blue Team
- SOC Analyst Strong Foundation Course - Udemy
- Introduction to Microsoft Sentinel - Microsoft
- CompTIA Security+ (Expected 05/2025) - Coursera

Education

Bachelor's Degree in Cyber Forensics - MG University, Edappally

AUGUST 2021 - MARCH 2024

Certified SOC Bundle Expert - Technovalley Software India Ltd., Edappally

AUGUST 2024 - NOVEMBER 2024

Experience

Cyber Forensic Intern - CyberCell Kochi City Police

JANUARY 2025 - FEBRUARY 2025

- Conducted forensic investigations by performing disk imaging, malware analysis, and log reviews to gather critical evidence.
- Supported incident response efforts by identifying attack vectors and determining root causes.
- Documented forensic procedures and response strategies, improving team reference material by 30%.

Digital Media Editor/ Content Creation - Freelance

SEPTEMBER 2021 - OCTOBER 2024

- Implemented secure storage and access controls, reducing data breach risk by 90% across multiple client projects.
- Developed secure remote workflows, increasing collaboration efficiency while maintaining 100% data confidentiality.
- Resolved technical issues with a 95% first-time fix rate, ensuring consistent uptime and data integrity for creative teams.