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

Driven and detail-oriented Cybersecurity Analyst with hands-on experience in SIEM tools, EDR/XDR, Linux server administration, and cloud infrastructure. Seeking to contribute to a dynamic security operations team by leveraging strong threat detection, log analysis, and incident response skills. Eager to grow in a collaborative environment focused on proactive cyber defense and continuous improvement.

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:** AWS - 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: github.com/nasarul10/soc-home-lab-project
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 v1 - EC Council
- Qualys Vulnerability Management - Qualys
- ISO/IEC 27001:2022 Lead Auditor - Mastermind
- SOC Essentials: Investigating with Splunk - Splunk
- Introduction to Threat Hunting - Security Blue Team
- SOC Analyst Strong Foundation Course - Udemy
- CompTIA Security+ (Expected 06/2025) - 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

Server Administration Intern - Hashroot Technologies

APRIL 2025 - PRESENT

- Managed and maintained Linux-based production servers, configuring Apache/Nginx with SSL, virtual hosts, firewall rules, and ensuring system security and uptime.
- Executed full WordPress site migrations, including database transfers, DNS updates, backups, and post-migration troubleshooting to ensure seamless transitions.
- Handled advanced cPanel/WHM operations including mail server setup and diagnostics (SPF, DKIM, DMARC), EasyApache and PHP configuration, cron jobs, and account management.

Cyber Forensic Intern - CyberCell Kochi City Police

JANUARY 2025 - FEBRUARY 2025

- Performed disk imaging, malware analysis, and log review for digital evidence collection.
- Aided incident response and root cause analysis in live cybercrime cases.

Digital Media Editor/ Content Creation - Freelance

SEPTEMBER 2021 - OCTOBER 2024

- Implemented secure storage and access controls, reducing data breach risk by 90%.
- Developed secure remote workflows that improved collaboration while maintaining full data confidentiality.
- Resolved technical issues with a 95% first-time fix rate, ensuring uptime and data integrity.