NASARUL NASEER

CYBER SECURITY ANALYST

+91 77368 82643 · nasarulnaseer.career@gmail.com · linkedin.com/in/nasarulnaseer
Kochi, Kerala, India

SUMMARY

Dedicated cybersecurity professional with hands-on experience in SIEM, threat detection, and incident response. Skilled in log analysis, network monitoring, and forensic investigations, with exposure to cloud security and EDR/XDR solutions. Passionate about threat hunting, detection engineering, and risk mitigation, continuously refining expertise through real-world projects.

EDUCATION

Bachelor of Science in Cyber Forensics **08/2021-08/2024**
Mahatma Gandhi University

Certified SOC Bundle Expert - Cybersecurity **09/2024-01/2025**
Technovalley Software India Pvt Ltd

TRAINING AND CERTIFICATIONS

- **Certified SOC Analyst** (EC-Council Certification, 02/2025)
- **SOC Essentials: Investigating with Splunk** (Splunk Certification, 02/2025)
- **Qualys Vulnerability Management Detection & Response** (Qualys Certification, 02/2025)
- **SOC Analyst Strong Foundation Course** (Udemy Certification, 03/2025)
- **Telstra Cyber Security Job Simulation** (Forage Job Sim, 02/2025)
- **Mastercard Cybersecurity Job Simulation** (Forage Job Sim, 02/2025)
- **Introduction to Threat Hunting** (Blue Team Certification, 02/2025)
- **Tenable One Introduction** (Tenable Training Course, 02/2025)
- **Introduction to Microsoft Sentinel** (Microsoft Training, 02/2025)
- **Data and Tools for Defense Analysts** (Splunk Certification, Expected 28/03/25)
- **CompTIA Security+ (**Self-paced learning, Expected 30/03/25)

PRACTICAL PROJECTS

Project: Cloud-Based SOC Operations & Threat Detection
Source: blog.ecapuano.com/Eric’s Substack
Platforms and Technology Used: VMware Workstation, LimaCharlie, Sliver, Yara, Log Analytics

SKILLS & TECHNOLOGIES

Security Monitoring & Analysis, Incident Detection & Response, Log Analysis & Correlation, SIEM Tools (Splunk, Wazuh, Microsoft Sentinel), Threat Intelligence & Indicators of Compromise (IOCs), Vulnerability Management (Qualys, Nessus), Endpoint Detection & Response (EDR/XDR - LimaCharlie), Firewall & IDS/IPS Monitoring (Snort, Suricata), Basic Network Security (TCP/IP, DNS, HTTP, TLS, VPNs).

PROFESSIONAL EXPERIENCE

Cyber Cell Kochi City Police
Internship (15 Days)

- 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.
- Executed vulnerability assessments and network mapping to identify and mitigate security risks.
- Developed comprehensive documentation for security incident response and forensic best practices.

Digital Media Editor/ Content Creation
Freelance (3 Years)

- Data Security Expertise: Implemented secure file storage and access controls, preventing unauthorized data breaches.
- Secure Collaboration Practices: Developed and enforced secure remote collaboration protocols to protect sensitive information.
- Technical Troubleshooting & Security: Diagnosed and resolved technical issues while maintaining data integrity and system security.

ADDITIONAL INFORMATION

- Strong analytical and problem-solving skills; ability to operate effectively under pressure in a 24x7 SOC environment.
- Detail-oriented with a strong ability to analyze security alerts and logs for potential threats.
- Excellent verbal and written communication skills for incident reporting and stakeholder coordination.
- Knowledge of threat tactics, kill chain, and advanced attack techniques.
- Open to working in different shifts, including weekends, as required for SOC operations.