NISHOK KUMAR S

SOC Analyst

CONTACT

6382422061

nishokkumar96@gmail.com

Gandhi Nagar, Periya Mathur,
Chennai - 68

git\NISHOKKUMAR

linkedin.com/in/nishokkumars

EDUCATION

2024 - 2026

PANIMALAR ENGINEERING COLLEGE

- M.E CSE 8.8

2020 - 2024

SRM VALLIAMMAI ENGINEERING COLLEGE

- B.E CSE 8.3

2018 - 2020

SKNS PMC Vivekananda Vidyalaya

- HSC 92%

SKILLS

- Red Hat (RHEL) | Ubuntu
- Network Fundamentals
- Log Analysis
- ELK Stack | Splunk (SIEM)
- Wazuh
- MITRE ATT&CK Framework
- Programming Language : C++, PHP, Python, Bash

PROFILE SUMMARY

Driven and aspiring SOC Analyst with hands-on experience in threat detection, log analysis through self-developed and online labs. Proficient in SIEM tools such as Splunk, ELK, and Wazuh (EDR), with a solid understanding of blue team operations. Eager to contribute to a collaborative SOC environment, grow professionally, share innovative ideas, and take on challenges that drive team and organizational success.

PROJECT EXPERIENCE

Elastic SIEM Deployment & Secure Log Ingestion (ELK Stack | Ubuntu | Windows | SSL/TLS)

- Configured and deployed Elastic SIEM (ELK Stack) on Ubuntu, integrating with Winlogbeat on Windows endpoints for real-time log ingestion.
- Implemented two-way SSL/TLS encryption between SIEM and endpoints, ensuring secure log transmission.
- Optimized log pipelines for centralized monitoring, threat detection, and SIEM rule tuning, improving detection efficiency by 20%.

Network Traffic Analysis Using Wireshark

- Monitored network traffic using Wireshark to analyze and troubleshoot performance issues, including HTTP, DNS, and TCP protocols.
- Captured and analyzed packets to identify latency issues, failed connections, and packet loss affecting system performance.
- Optimized network performance by analyzing TCP handshakes and packet retransmissions.
- Configured firewall rules (UFW) based on packet analysis to block malicious IPs and secure server access.

Bash Automation Scripts Github

CERTIFICATION

- LAHTP MASTERY (Learn the Art of Programming Through Programming) by SNA
- Learn Bug Bounty Hunting & Web Security Testing From Scratch by Udemy

LANGUAGES

- Tamil
- English
- Korean