ALEN JOHN

Kochi, India | + 91 8848603693 | alenyohannan0007@gmail.com | LinkedIn | Portfolio

WORK EXPERIENCE

1. Soc Analyst - CyberDisti Pvt Ltd, Kochi India — June 2025 – Present

- Working as a SOC Analyst with hands-on experience in threat monitoring, incident response, and cybersecurity operations using platforms like **Seceon aiSIEM & aiXDR**.
- Handling real-time alert analysis and log correlation within a live SOC environment.

2. Cyber Security Researcher - RedTeam Hacker Academy Trivandrum, India — Nov 2024 – April 2025

- Hands-on experience with log analysis, IDS/IPS, endpoint detection and response (EDR), and vulnerability assessment tools.
- Gained **hands-on experience** in security monitoring using tools like **Splunk, Wazuh, Wireshark, IBM QRadar, and the ELK Stack**.
- Skilled in VAPT with expertise in web security, SQL injection, networking (OSI, TCP/IP), tools like Kali Linux, Metasploit, Wireshark, Nmap, and server security (Apache, HTTPS).

TECHNICAL SKILLS

- Network protocol
- Intrusion Detection/Prevention
- Security protocols
- Vulnerability assessment
- Firewall Management
- Incident response
- SPLUNK
- LINUX
- Web application security
- SIEM
- Penetration testing
- Wazuh
- VAPT
- Web development
- HTML/CSS/JAVASCRIPT/SQL

PROJECTS

1. Website Log Monitoring using Splunk — SOC Project

- Implemented a **Splunk**-based monitoring solution to analyse and visualize real-time log data from a website.
- Detected anomalies and generated actionable insights to strengthen security and improve application performance.

2. System Log Monitoring using Wazuh in Windows 11 — SOC Project

- Integrated **Wazuh** with **Windows 11** by deploying the Wazuh agent for real-time log monitoring.
- Conducted security event detection, incident analysis, and proactive threat management using the Wazuh dashboard.

3. Vulnerability Assessment and Penetration Testing (VAPT) on Web Applications — VAPT Project

- Performed VAPT on multiple web applications using tools like **Burp Suite**, **OWASP ZAP**, and **Nikto**.
- Discovered vulnerabilities like **SQL Injection**, **XSS**, **CSRF**, and **Parameter Tampering** and documented in a VAPT report.

EDUCATION

Master of Computer Applications (M.C.A) - 75% — September 2022 - November 2024
Mar Thoma Institute of Information Technology, Ayur/Kollam, Kerala

Bachelor of Computer Applications (B.C.A) - 69% — June 2019 - August 2022
Catholicate College, Pathanamthitta, Kerala

CERTIFICATIONS

1- Certified IT Infrastructure and Cyber SOC Analyst - RedTeam Hacker Academy, Trivandrum

2- Web Development - Softzane Solutions, Ayur, Kollam