Abel Thomas

India | abelthomas.pro@gmail.com | +918078429706 | LinkedIn | GitHub| Portfolio

SUMMARY

Cybersecurity Analyst Fresher with hands-on training in SOC operations, network security, and incident response. Experienced in log analysis, alert triage, IDS/IPS monitoring, and vulnerability assessment in virtualized lab environments. Familiar with OWASP Top 10 web vulnerabilities and basic penetration testing concepts. Background in MERN development helps in understanding application-level security risks. Seeking a Cybersecurity Intern role to contribute to real-world security monitoring and threat analysis.

AREAS OF EXPERTISE

- **Security Operations & Incident Response:** Exposure to alert triage, basic incident investigation, escalation workflows, and analyzing suspicious network and endpoint activity.
- **SIEM & Log Monitoring:** Hands-on experience with Splunk and Wazuh for log ingestion, alert analysis, detection rule tuning, and SOAR-based workflow automation using Shuffle and TheHive.
- **Network Security & Monitoring:** Understanding of TCP/IP, TCP/UDP/ICMP traffic, firewall concepts, IDS/IPS monitoring, and packet analysis using Wireshark and Nmap.
- **Application Security Fundamentals:** Basic web security testing using Burp Suite with knowledge of **OWASP Top 10** vulnerabilities such as SQL Injection, XSS, Broken Authentication, and Security Misconfiguration.
- **Analytical & Problem-Solving Skills:** Strong analytical thinking, attention to detail, and structured problem-solving applied during log analysis and security investigations.

TOOLS & TECHNOLOGIES

- **SIEM:** Splunk, Wazuh
- **SOAR:** Shuffle, TheHive
- **Network Tools:** Wireshark, Nmap, Hydra, Burp Suite
- **Threat Intelligence:** VirusTotal, AbuseIPDB
- **Platforms:** Linux (Kali, Ubuntu), Windows 10/11, VirtualBox, VMware
- **Scripting:** Basic Bash, Basic Python
- **Development Knowledge:** JavaScript, Node.js, MongoDB, Express, ReactJs, MySQL

EDUCATION

Bachelor of Computer Applications (BCA) 2021 – 2024
CMS College, Kottayam

TECHNICAL TRAINING

CERTIFIED IT INFRASTRUCTURE & CYBER SOC ANALYST (CICSA) 2025
RedTeam Hacker Academy, Ernakulam

- Completed comprehensive training focused on core **SOC methodologies**, network defense, incident handling, and **IT infrastructure security**.
- Gained foundational knowledge in **Basic Ethical Hacking** principles, including reconnaissance and vulnerability identification, to understand the attacker mindset.

MERN STACK DEVELOPMENT PROGRAM 2024 – 2025
Brototype, Kochi

- Completed an intensive **self-learning program** focused on the MERN stack (MongoDB, Express.js, React, Node.js) for full-stack application development.
- Enhanced technical communication and problem-solving through regular participation in **interview-like reviews**

and technical seminars.

CERTIFICATIONS

Learn Ethical Hacking from Scratch 2024
Instructor: Zaid Sahib, Z Security
Platform: Udemy

- Gained knowledge of fundamentals of ethical hacking, including reconnaissance, scanning, and basic exploitation techniques.

PROJECTS

Automated SOC Triage Pipeline (Wazuh, Shuffle, TheHive, VirusTotal).

- **Objective:** Engineered a Security Orchestration, Automation, and Response (**SOAR**) pipeline for automated incident triage, simulating **Mimikatz** credential dumping detection.
- **Tools Used:** **Wazuh** for detection, **Shuffle** for orchestration, **TheHive** for case management, **VirusTotal** for IOC enrichment.
- **Impact:** Reduced **MTTD/MTTR** by automating triage, enrichment, and analyst notifications.
- **Skills Demonstrated:** SOAR automation, TI correlation, SIEM configuration, Docker deployment, incident response.
- **Code:** [GitHub Repository]

Snort and Splunk IDS Integration Project.

- **Objective:** Deployed and configured a complete **Network IDS** using **Snort** on Ubuntu and integrated alerts into **Splunk Enterprise**.
- **Setup Overview:** Snort VM → Splunk UF → Splunk Enterprise for dashboards and alerting.
- **Detection Scenarios:** Custom rules detected **port scans**, **SSH brute-force attempts**, and attacker traffic.
- **Skills Demonstrated:** Snort rules, packet inspection, log forwarding, SPL dashboards.
- **Code:** [GitHub Repository]

Splunk Log Analysis for Real-Time Brute-Force Detection.

- **Objective:** Built a real-time **SSH brute-force detection** pipeline using Splunk.
- **Impact:** Converted raw logs into actionable alerts (Trigger count > 5).
- **Skills Demonstrated:** UF config, SPL design, alert logic.
- **Code:** [GitHub Repository]

Personal Portfolio Website (MERN Stack).

- **Objective:** Built a responsive portfolio website.
- **Tech Stack:** React, MongoDB, Express, Node.js.
- **Live Site:** abelthomas.site