Abel Thomas

SOC Analyst Fresher | Cybersecurity Intern

India | abelthomas.pro@gmail.com | +91 80784 29706
LinkedIn | GitHub | Portfolio

SUMMARY

SOC Analyst **Fresher** with hands-on lab experience in Security Operations Center (SOC) monitoring, alert triage, log analysis, and incident response. Strong foundation in SIEM, SOAR, IDS/IPS, and network security. Proven ability to detect brute-force attacks, port scans, and suspicious activity using Splunk, Wazuh, and Snort. Also skilled in **MERN stack development**, enabling strong understanding of application-level security risks. Seeking SOC Analyst L1 or Cybersecurity Intern roles.

TECHNICAL SKILLS

- **SOC & Security:** SOC Monitoring, Alert Triage, Incident Investigation, Escalation Handling
- **SIEM / SOAR:** Splunk, Wazuh, Shuffle, TheHive
- **Network Security:** TCP/IP, Firewalls, IDS/IPS, Packet Analysis
- **Threat Intelligence:** VirusTotal, AbuseIPDB, OWASP Top 10
- **Programming & Scripting:** JavaScript, Python (Basic), Bash (Basic)
- **Web Technologies (MERN):** MongoDB, Express.js, React.js, Node.js
- **Operating Systems:** Linux (Kali, Ubuntu), Windows 10/11

PROFESSIONAL SKILLS

- Incident Communication and Documentation
- Analytical Thinking and Problem Solving
- Attention to Detail in Log Analysis
- Ability to Work in 24x7 Shift Environments

PROFESSIONAL TRAINING & EXPERIENCE

Certified IT Infrastructure and Cyber SOC Analyst (CICSA) 2025
RedTeam Hacker Academy, Ernakulam

- Comprehensive cybersecurity training covering IT infrastructure, network security, and SOC operations
- Hands-on exposure to SIEM, IDS/IPS, incident response, and log analysis in lab-based environments
- Trained in ethical hacking fundamentals to understand attacker techniques and defensive strategies

MERN Stack Developer – Trainee 2024 – 2025
Brototype (Self-Learning & Mentorship Program), Kochi

- Built full-stack web applications using MongoDB, Express.js, React, and Node.js
- Implemented authentication, REST APIs, and database integrations
- Gained strong understanding of application workflows and security considerations

EDUCATION

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

CERTIFICATIONS

Certified Cyber Security Analyst Jan 2024
RedTeam360
Learn Ethical Hacking from Scratch 2025
Z Security (Udemy)

PROJECTS

Automated SOC Triage Pipeline (Wazuh, Shuffle, TheHive)
GitHub Repository

- Built SOAR-based incident triage workflows for malware and credential dumping alerts
- Automated IOC enrichment using VirusTotal and case creation in TheHive
- Reduced mean time to detect and respond through alert automation

Snort & Splunk IDS Integration
GitHub Repository

- Deployed Snort IDS and forwarded alerts to Splunk using Universal Forwarder
- Created custom detection rules for port scans and SSH brute-force attacks
- Designed dashboards and real-time alerts using SPL

Personal Portfolio Website (MERN Stack)
Live Website

- Developed a responsive portfolio website using React, Node.js, Express, and MongoDB
- Showcases cybersecurity projects, SOC labs, and technical skills