Abel Thomas

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

SUMMARY

Cybersecurity Analyst Fresher trained extensively in **SOC methodologies** and **IT Infrastructure Security**. Proven ability in log analysis, alert triage, and simulating threat scenarios in virtualized environments. Combines foundational **ethical hacking** knowledge with a unique perspective from **MERN development** to understand application vulnerabilities and build robust defense strategies. Eager to contribute practical skills immediately to incident response and threat analysis.

AREAS OF EXPERTISE

- **Security Operations & Incident Response:** Experience with alert triage, correlation, escalation processes, and investigating suspicious endpoint and network activity.
- **Cybersecurity Analysis & Threat Intelligence:** Understanding of attacker techniques, reconnaissance patterns, vulnerability concepts, and threat hunting fundamentals using OSINT.
- **SIEM & Log Monitoring:** Hands-on with Splunk and Wazuh for log ingestion, detection rule creation, alert investigation, and workflow automation with Shuffle SOAR and TheHive.
- **Network & Endpoint Monitoring:** Knowledge of TCP/UDP/ICMP, Windows event logs, Linux logs, and tools such as Wireshark and Nmap for traffic inspection.
- **Application Security & Web Testing:** Experience with Burp Suite for intercepting traffic, testing authentication/authorization flaws, scanning endpoints, and analyzing API behavior.

TOOLS & TECHNOLOGIES

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

SOFTWARE PROFICIENCY

- **Microsoft Office Suite:** Word, Excel, PowerPoint, Outlook
- **Google Workspace:** Docs, Sheets, Slides, Gmail

EDUCATION

BACHELORS OF COMPUTER APPLICATION 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.

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** for centralized monitoring.
- **Setup Overview:** Snort (Ubuntu VM) generating alerts $\rightarrow$ Splunk UF forwarding logs $\rightarrow$ Splunk Enterprise (Windows 11) for indexing, dashboards, and alerting.
- **Detection Scenarios:** Custom rules successfully detected **port scans**, **SSH brute-force attempts**, and attacker traffic from a **Kali Linux** VM.
- **Impact:** Achieved full end-to-end IDS visibility, validating Snort rule creation, packet inspection, and SIEM integration workflows.
- **Skills Demonstrated:** Snort IDS configuration, rule tuning, UF log forwarding, dashboard creation, attack simulation in virtualized lab.
- **Code:** [GitHub Repository]

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

- **Objective:** Built a real-time **SSH brute-force detection** pipeline using Splunk with live attack traffic generated via **Hydra**.
- **Tools Used: Splunk UF** on Kali Linux, **Splunk Enterprise** Indexer, SPL for correlation queries.
- **Impact:** Implemented a reliable real-time alert (Trigger Count > 5), converting raw logs into actionable detections.
- **Skills Demonstrated:** Log ingestion, SPL query design, alerting logic, Linux UF configuration.
- **Code:** [GitHub Repository]

Personal Portfolio Website (MERN Stack).

- **Objective:** Built a responsive portfolio site to showcase cybersecurity and MERN projects.
- **Tech Stack:** React, Node.js/Express, MongoDB; deployed on Vercel and Render.
- **Features:** Custom UI, project listings, contact API.
- **Live Site:** abelthomas-portfolio.vercel.app