Abel Thomas

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

SUMMARY

Entry-level SOC Analyst with hands-on experience in log analysis, alert triage, threat monitoring, and security automation. Skilled in SIEM (Splunk, Wazuh) and SOAR (Shuffle, TheHive) with practical exposure to detecting brute-force attacks, anomalous login patterns, and network threats. Previously trained as a MERN Stack Developer, providing strong understanding of application behavior, API security, and real-world system workflows—adding value in identifying security issues from both development and security perspectives.

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.

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

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 the detection and processing of **Mimikatz** activity on a Windows endpoint.
- **Tools Used:** Integrated **Wazuh** (SIEM) for detection; **Shuffle** for orchestration via webhooks; **TheHive** for centralized case management; and **VirusTotal** for threat intelligence enrichment (SHA256 hash reputation).
- **Impact:** Achieved near-instantaneous alert processing, significantly reducing **MTTD** (Mean Time To Detect) and **MTTR** (Mean Time To Respond) by automating alert triage, IOC enrichment, and analyst notification via email.
- **Skills Demonstrated:** SOAR implementation, Threat Intelligence (TI) correlation, SIEM/HIDS configuration, Docker deployment, Incident Response Automation.
- **Code:** [GitHub Repository]

Splunk Log Analysis for Real-Time Brute-Force Detection

- **Objective:** Constructed a complete **SIEM pipeline** focusing on real-time threat detection of **SSH brute-force attacks** simulated using the **Hydra** tool against a Kali Linux target.
- **Tools Used:** Configured **Splunk Universal Forwarder (UF)** on Kali Linux to ingest logs into a Windows-hosted **Splunk Enterprise** Indexer; utilized **Search Processing Language (SPL)** for complex query creation.
- **Impact:** Developed and implemented a dependable Real-time Alert (Trigger Count > 5) on the `auth.log` data, successfully verified against live attack traffic, demonstrating proficiency in converting raw logs into **actionable threat detection**.
- **Skills Demonstrated:** Data Ingestion/Forwarder Setup (Linux UF), Advanced SPL query design, Real-Time Alerting, Log Correlation, Debugging data stream reliability.
- **Code:** [GitHub Repository]