Dishitha Somasekharan

| Srivari Forest Breeze, Subramanyapura, Bangalore | +91 (894)369-1761 | dishithapks@gmail.com |

SUMMARY

Cybersecurity Enthusiast with hands-on experience in SOC monitoring, threat detection, and incident response through practical cybersecurity projects. Experience working with Wazuh SIEM and Elastic Stack for log analysis, honeypot deployment for threat monitoring, and SOC automation using LimaCharlie and Tines. Understanding of networking fundamentals including TCP/IP, firewalls, IDS/IPS, and VPN concepts.

TECHNICAL SKILLS

- Security Tools: Wazuh, Elastic Stack (ELK), T-Pot Honeypot, Shuffle (SOAR), TheHive.
- SIEM & Monitoring: Log Analysis, Alert Monitoring, Incident Investigation.
- Networking: TCP/IP, DNS, HTTP/HTTPS, Firewalls, VPN Concepts.
- Operating Systems: Linux (Ubuntu), Windows 10.
- Cloud & Virtualization: DigitalOcean, Virtual Machines.
- Security Concepts: MITRE ATT&CK, Incident Response Lifecycle, IOC Analysis.
- Tools: SSH, Git, CyberChef.

INTERNSHIP EXPERIENCE

Cyber Security Trainee | Unified Mentor Private Limited | January 2026 -Present

Wazuh SIEM Dashboard Implementation

- Built SIEM + SOAR workflow for automated threat detection and response.
- Collected Windows logs using Wazuh and automated alert handling via Shuffle.
- Performed IOC enrichment and integrated TheHive for case management.
- Simulated analyst-driven response actions.

T-Pot Honeypot Deployment & Threat Monitoring Implementation

- Built cloud-based honeypot to capture real attacker activity.
- Installed T-Pot on Ubuntu VM and monitored attacks using Kibana dashboards.
- Generated logs for SIEM ingestion and SOC analysis.

SOC Automation Playbook Implementation

- Developed automated SOC workflow using Lima Charlie and Tines.
- Simulated threat detection, alert enrichment, and automated response actions.

- Implemented analyst approval workflow for endpoint isolation.

CERTIFICATIONS

- Certified IT Infrastructure & Cybersecurity Specialist (EC Council) — Red Team Hacker Academy
- Java and Android Programming Certification — CDAC, Trivandrum.
- ISTQB Certification — Canadian Software Testing Board
- AI for Cyber Security: Threat Detection & SOC Automation — Udemy (Currently Pursuing).

EDUCATION

- B.Sc. in Physics – Kannur University.
- Master of Computer Applications – University of Calicut.