

# VINAY S

+91-6366250772 | vinaygowdas835@gmail.com | Bangalore, Karnataka

## **SUMMARY**

Aspiring SOC Analyst with hands-on internship experience at **Avigdor Cybertech**. Proficient in **SIEM** tools, threat detection, incident response, and security frameworks. Strong understanding of networking, malware analysis, and common attack vectors. Eager to contribute technical expertise and analytical skills in cybersecurity operations.

## **EXPERIENCE**

### **SOC Intern, Avigdor Cybertech, Bangalore (June-Present)**

- **SIEM Tools:** Gained knowledge of SIEM (Security Information and Event Management) tools such as Splunk, and ticketing systems (Jira, ServiceNow).
- **Malware and Phishing Analysis:** Have experience with malware and phishing email analysis, which involves identifying and mitigating potential security threats.
- **IoCs and Incident Response:** Understanding on IoCs and incident response workflows, which are critical for detecting and responding to security incidents.
- **Networking Concepts:** Have a hands-on understanding of networking concepts such as TCP/IP, DNS, HTTP, VPN, Firewalls, and Routers.
- **Attack Vectors:** Understanding on attack vectors of phishing, DDoS, malware, and ransomware
- **NIST Framework:** Applied NIST framework in analyzing and responding to security alerts.
- **Operating System Security:** Experience with Windows, Linux, and macOS environments in security contexts.

## **EDUCATION**

- **2021-2024:** Bachelor of Computer Application  
REVA University, Bangalore.

## **TECHNICAL SKILLS**

- **SIEM Tools:** Splunk, AlienVault.
- **Threat Analysis:** URL Scanner, VirusTotal, IP Lookup, DNS Lookup,
- **Networking:** Firewalls, VPNs, TCP/IP, IDS/IPS.
- **Operating Systems:** Windows, macOS, Linux.
- **Frameworks:** MITRE ATT&CK, NIST CSF.

## **CERTIFICATIONS**

- TryHackMe SOC Level 1
- Cybersecurity Certificate– EthicalByte
- Splunk Basics
- Avigdor Certified SOC Analyst
- Network Fundamentals. (CISCO)

## **SKILLS**

- Strong analytical and reporting skills
- Problem solving and threat/risk assessment
- SIEM, IDS, and IPS expertise
- Excellent communication and collaboration
- Vulnerability management
- Fast learner and adaptable in shifts

## **DECLARATION**

- I here by declare that all the above mentioned information is true and correct to the best of my knowledge