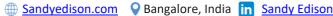
# SANDY EDISON A

## SOC Level 1

📞 +91 63606 30776 🛛 @ sandyastra19@gmail.com



## **INTERNSHIP**

#### Cyber Security Intern | Avigdor Cybertech

- Gained practical experience with SIEM tools like Splunk (via TryHackMe labs) and ticketing platforms such as Jira and ServiceNow
- Built a strong foundation in core networking concepts including TCP/IP, DNS, HTTP, VPNs, Firewalls, and Routers
- Conducted basic analysis of phishing emails, malware behavior, and identified indicators of compromise (IoCs)
- Analyzed and responded to security alerts related to phishing, DDoS, malware, and ransomware threats
- Developed collaboration and communication skills through cross-functional team interactions
- Prepared for 24/7 SOC operations with flexibility for rotational shift work

## CERTIFICATIONS

- Cybersecurity Professional Certification (Offensive & Defensive) – Avigdor CyberTech
- TryHackMe SOC Level 1
- Network Fundamentals (TryhackMe)
- Splunk Basics (TryhackMe)
- Google Cyber Security Professional
- Offensive Penetration Testing by Cybrary
- Cyber Security Beginners & Advance by Guvi
- Full Stack Web Development by Harsha Informatics
- Course Completion of ISC2 CC
- Introduction to Cyber Security by Cisco (Karnataka Innovation & Technology Society)
- Cyber Security Fundamentals by IBM

## TECHNICAL SKILLS

- Networking: Firewalls. VPN, TCP/IP, IDS/IPS
- SIEM: Splunk, AlienVault
- Threat Detection: URL Scanner, VirusTotal, IP Lookup
- OS: Windows, Mac
- Frameworks: MITRE ATT&CK, NIST, CSF, OWASP Top 10

## **SKILLS**

- TCP/IP protocols and OSI model
- Threat and risk assessment
- MITRE ATT&CK framework and TTPs
- SIEM, IDS, and IPS tools
- Vulnerability management
- Analytical and reporting skills
- Problem-solving and critical thinking
- **Excellent communication skills**

## **OBJECTIVE**

Entry-level SOC Analyst with hands-on experience in threat detection, alert triage, and incident response using tools like Splunk, IDR, and XDR. Skilled in identifying phishing, impersonation, and suspicious activity across platforms. Strong research and analytical skills for generating accurate security alerts. A resilient bone cancer survivor, bringing adaptability, focus, and problem-solving to 24/7 security operations.

## **EDUCATION**

#### **Bachelor of Computer Applications**

Indira Gandhi National Open University (IGNOU) Present

#### History, Economics, Business Studies, Accountancy, English and Hindi

Karnataka School Examination and Assessment **Board** 

2023-2024

#### Physics, Chemistry, Mathematics and Electronics

St. Claret Pre-University, Bangalore, India 2018-2018

#### Schooling

St. Claret School, Bangalore, India 2009-2018

#### LANGUAGES

- English
- Hindi
- Kannada
- Tamil
- Telugu