

SAI ABBHIRAM VALUPADASU

valupadasusaibbhiram@gmail.com | LinkedIn | GitHub | Portfolio | +91 9849786297

PROFESSIONAL SUMMARY

Enthusiastic and detail-oriented Computer Science graduate with hands-on experience in **SOC operations, incident monitoring, and threat analysis**. Skilled in **log analysis, malware investigation, and triaging alerts**, with proficiency in security tools such as **Wireshark, Nmap, Snort, Splunk (basic)** and scripting in **Bash & Python**. Strong foundation in networking, operating systems, and cloud security. Seeking a **SOC Analyst role** to contribute to proactive defense and incident response in a 24/7 environment.

EDUCATION

Vignana Bharathi Institute of Technology	Hyderabad
• B.Tech in Computer Science & Engineering (Business Systems) GPA: 7.8	2021 – 2024
Central Institute of Tool Design	Hyderabad
• Diploma in Automation & Robotics Engineering GPA: 7.7	2019-2021

SKILLS SUMMARY

Security Tools:	Wireshark, Nmap, Burp Suite, Snort, Splunk (basic), ELK Stack (basic), Kali Linux
Operating Systems:	Windows, Linux, OS X
Scripting/Programming:	Shell Scripting (Bash), Python, Java, SQL, C
Networking:	TCP/IP, Firewalls, IDS/IPS, Packet Analysis, Log Monitoring
Soft Skills:	Incident Triage, Threat Hunting, Team Collaboration, Communication

RELEVANT EXPERIENCE & LABS

Cybersecurity Labs & Blue Team Practice TryHackMe, HackTheBox	2024 – 2025
<ul style="list-style-type: none">Completed hands-on labs covering SOC fundamentals, alert triage, malware investigation, and log analysis.Performed network packet captures using Wireshark to detect brute force, phishing, and data exfiltration attempts.Conducted vulnerability scans with Nmap and implemented incident response steps following defined playbooks.Used Splunk queries for log searching, correlation, and initial triage of events.	
Independent Projects	2023 – Present
<ul style="list-style-type: none">Built monitoring dashboards and data analytics pipelines (Python, SQL) to strengthen anomaly detection skills.Developed automation scripts in Python and Bash for log parsing, alerting, and remediation.Designed and deployed applications on cloud (AWS, Docker) with security best practices for authentication and access control.	

PROJECTS

Network Security Monitoring Lab Self-Project	2024
<ul style="list-style-type: none">Configured Wireshark and Snort to capture and analyze suspicious traffic patterns from simulated attacks.Performed incident triage following SOC playbooks, escalating critical findings to simulated higher-tier analysts.Documented detailed root cause analysis reports with remediation strategies to mitigate vulnerabilities.Continuously tuned detection rules to improve monitoring accuracy and reduce false positives.	
Cartlytics – Market Basket Analysis LINK	2023
<ul style="list-style-type: none">Applied data mining techniques to identify hidden patterns in datasets, showcasing analytical problem-solving.Built interactive Streamlit dashboard with support, confidence, and lift metrics to visualize insights.Drew parallels to SOC use cases by leveraging anomaly detection methods for identifying outliers in logs.	
Threat Hunting Challenges TryHackMe	2024
<ul style="list-style-type: none">Investigated simulated phishing, brute force, and malware attacks using forensic log analysis.Followed structured triage and escalation workflows similar to SOC environments.Created post-incident reports detailing timeline, indicators of compromise (IOCs), and preventive measures.	

CERTIFICATIONS

Cyber Security 101 TryHackMe	Feb 2025
Advent of Cyber TryHackMe	Dec 2024
Networking Essentials Cisco NetAcad	Oct 2022
AWS Academy Cloud Foundations AWS	Dec 2022