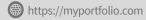
SUMEDH MORE

SECURITY ANALYST









SUMMARY

Focused and driven SOC Analyst with hands-on experience in monitoring, analyzing, and responding to real-time security threats. Proficient in SIEM tools, incident handling, and using automation/AI to boost detection. Passionate about threat intelligence and defensive operations.

SKILLS

- Incident response with Al
- Web Application Penetration Testing
- Ethical Hacking
- Linux CLI
- Network Security
- Computer Networking
- Security Analysis using SIEM tools (splunk)
- · Programming languages -
- 1) C++
- 2) Python
- 3) SQL

PROJECTS & PRACTICAL EXPERIENCE

Vulnerability Assessment of College Web Portal

Cybersecurity Project | 2024

- Performed black-box testing on the internal web application using Burp Suite and OWASP ZAP
- Discovered multiple security flaws including input validation issues and missing authentication headers
- Documented and submitted a detailed vulnerability report to the admin team
- Tools Used: Burp Suite, OWASP ZAP, Nmap

AI-Driven Log Analyzer for SIEM

Al-Cyber Project | 2025

- Built a Python-based log analyzer using Natural Language Processing (NLP) to detect abnormal events in log data
- Integrated the system with sample SIEM logs to simulate real-world threat detection
- Tools Used: Python, Scikit-learn, ELK Stack (ElasticSearch + Kibana)

TryHackMe and Hack The Box Challenges

Ongoing | Self-Paced Learning

- Completed over 50+ rooms on TryHackMe and multiple machines on HTB
- Specialized in Linux privilege escalation, web exploitation, and network attacks
- Practiced real-world attacks using Metasploit, Hydra, SQLMap, and Nmap

EDUCATION

B. Tech in Information Technology

Dr. Babasaheb Ambedkar Technological University • 2023–2027

Minor in Computer Engineering

Dr. Babasaheb Ambedkar Technological University • 2023–2027

CERTIFICATIONS

CompTIA Security+

CompTIA • 2025-2026

Google Cybersecurity Professional

Coursera • 2025

DCSC - Web Application Penetration Testing

DROP ORGANIZATION 2023-2024