

# SOURABH MANE

CYBERSECURITY | SOC ANALYST (L1) | NETWORK SECURITY

+91 75072 54167 · saurabhmane2525@gmail.com · linkedin.com/in/sourabhmane · Maharashtra, India

CISCO CERTIFIED NETWORK ASSOCIATE (CCNA)

GOOGLE CYBERSECURITY CERTIFICATE

AWS CLOUD PRACTITIONER

## PROFESSIONAL SUMMARY

Cisco Certified Network Associate (CCNA) and results-driven cybersecurity professional with hands-on experience in SIEM monitoring, intrusion detection and network traffic analysis. Built end-to-end detection and monitoring labs spanning AWS CloudTrail/EC2 log ingestion into Splunk, custom SPL dashboards, Python-based PCAP analysis and machine-learning anomaly detection. Strong foundation in routing & switching, VLANs, ACLs and TCP/IP, with working knowledge of Wireshark, Nmap, Qualys, the OWASP Top 10, Linux, Python and Bash. Seeking an entry-level **SOC / Cybersecurity Analyst (L1)** or **Network Engineer** role where detection engineering and network fundamentals add immediate value to a security operations team.

## CERTIFICATIONS & CREDENTIALS

|                                               |                                                                           |         |
|-----------------------------------------------|---------------------------------------------------------------------------|---------|
| Cisco Certified Network Associate (CCNA)      | Cisco · globally recognised industry certification (Exam 200-301)         | 2026    |
| Google Cybersecurity Professional Certificate | Coursera · SIEM, incident response, Linux, SQL and threat detection       | 2024    |
| AWS Cloud Practitioner Essentials             | AWS Training · cloud architecture, IAM and shared-responsibility security | 2025    |
| TryHackMe – Practical Lab Track               | Attack simulation, malware analysis, packet analysis, OWASP Top 10        | Ongoing |

## TECHNICAL SKILLS

|                     |                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------|
| Networking          | Routing & Switching (CCNA), VLANs, STP, OSPF, ACLs, NAT, TCP/IP, DNS, DHCP, ICMP             |
| Security Operations | Intrusion Detection, Network Traffic Analysis, Incident Triage, Threat Hunting, Log Analysis |
| SIEM & Monitoring   | Splunk (log monitoring, SPL query development, dashboards), Security Alert Triage            |
| Cloud               | AWS EC2, CloudTrail, CloudWatch, IAM & cloud security best practices                         |
| Tools & AppSec      | Wireshark, Nmap, Qualys, Cisco Packet Tracer; OWASP Top 10 & web vulnerability assessment    |
| Programming         | Python (Pandas, Scikit-learn, Matplotlib), Bash / Shell scripting, SPL                       |
| Automation & AI     | Isolation Forest anomaly detection, time-series analysis, LLM APIs (Groq / Llama)            |
| Operating Systems   | Linux (Kali, Ubuntu), Windows Server, Windows 10/11                                          |

## PROJECTS

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| AI-Powered Network Health Monitor   Python, Pandas, Scikit-learn, Matplotlib, Groq API                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026 |
| <ul style="list-style-type: none"><li>Developed a Python-based monitoring tool that collects real-time ICMP latency and packet-loss data from gateways, DNS resolvers and live hosts.</li><li>Implemented Isolation Forest for unsupervised anomaly detection, identifying abnormal latency spikes without relying on fixed thresholds.</li><li>Automated time-series analysis, CSV logging and visualisation of network health metrics with Pandas and Matplotlib.</li><li>Integrated Llama via the Groq API to generate data-driven network engineering reviews and prioritised troubleshooting recommendations.</li></ul> |      |
| AWS-Based SIEM Monitoring Lab   Splunk, AWS CloudTrail, EC2, SPL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2025 |
| <ul style="list-style-type: none"><li>Architected a centralised security monitoring pipeline by ingesting AWS CloudTrail API activity and EC2 system logs into Splunk Free, creating a single pane of glass for cloud telemetry.</li><li>Performed log analysis to surface failed authentication attempts and anomalous user behaviour patterns in a controlled lab environment.</li><li>Developed custom SPL queries and Splunk dashboards to visualise cloud security events, cutting manual investigation time and enabling faster alert triage.</li></ul>                                                                |      |
| Network Packet Analyzer   Python, Wireshark, PCAP, Matplotlib                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2025 |
| <ul style="list-style-type: none"><li>Developed a Python-based packet analysis tool that parses Wireshark PCAP captures to profile network traffic patterns and flag anomalies.</li><li>Implemented custom parsers extracting key metrics: packet types, protocols, source/destination IP pairs and port activity.</li><li>Visualised traffic volume over time with Matplotlib to identify traffic spikes and potential DDoS-style patterns.</li></ul>                                                                                                                                                                       |      |

## EDUCATION

|                                                                                |             |
|--------------------------------------------------------------------------------|-------------|
| Bachelor of Technology (B.Tech), Information Technology                        | 2022 – 2026 |
| Dr. Babasaheb Ambedkar Technological University (DBATU), Lonere, Raigad, India |             |

## LEADERSHIP & RESPONSIBILITIES

|                                                                                                                                                                                                                                         |             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Technical Secretary, Department of Information Technology · DBATU                                                                                                                                                                       | 2023 – 2024 |
| <ul style="list-style-type: none"><li>Coordinated 5+ technical events and workshops, increasing student participation by 25%.</li><li>Led cross-functional communication between faculty administration and the student body.</li></ul> |             |