SUDARSHAN RANGAPPA

www.linkedin.com/in/sudarshan-rangappa | P: +91 8302720020 | Sudarshan_rangappa@proton.me |
https://sudarshanrangappa.github.io/portfolio/

PROFESSIONAL SUMMARY

Entry-level Security Analyst with hands-on experience in SOC monitoring, incident response, alert triage, and log analysis using tools like Splunk, Wazuh, and Shuffle SOAR. Proven ability to detect and respond to real-world attack simulations in a blue team lab setup. Familiar with EDR concepts, IOC analysis, and correlating multiple data sources across Windows, Linux, and cloud environments. Strong grasp of ports, protocols, SIEM investigations, and case documentation. Eager to contribute to fast-paced SOC teams protecting global organizations from cyber threats.

EDUCATION

National Forensic Sciences University — Gandhinagar, Gujarat
Master of Science, Cybersecurity — Aug 2023- May 2025
Cumulative GPA: 8.24
Relevant Coursework: Threat Detection, VAPT, SIEM Operations, Network Security, Incident Response

Bengaluru City University — Bengaluru, Karnataka
Bachelors of Computer Applications — Jul 2020 - Jul 2023
Cumulative GPA: 8.16

UNIVERSITY PROJECTS

INTEGRATED CYBER DEFENCE SYSTEM [ICDE] — May 2025

Designed and deployed a scalable cybersecurity operations lab simulating enterprise-grade blue team workflows using real-world security tools and attack scenarios.

- Built a virtual SOC environment integrating industry tools: Splunk, Wazuh, Suricata, Zeek, Cowrie, OpenVAS, Shuffle
- Monitored logs from 3 endpoints (Windows Server 2025 AD, Windows 11, Ubuntu) using Wazuh and Splunk
- Created 3+ SOAR playbooks in Shuffle to automate IP blocking, alert forwarding, and GeoIP enrichment
- Simulated 10+ attack scenarios including brute-force, privilege escalation, and SSH honeypot interaction, achieving 100% detection in Splunk and Wazuh
- Achieved real-time alert correlation and incident response workflow across all components

LOCATION-BASED IOT SECURITY KEY — November 2024

Developed a location-aware authentication mechanism for IoT devices using ESP8266 (NodeMCU) and GPS module for physical-layer access control.

- Implemented geofencing logic with ±5m accuracy to dynamically permit or deny access based on GPS coordinates
- Achieved 90%+ accuracy in unauthorized access prevention in field tests
- Reduced false access triggers by tuning GPS sampling frequency and incorporating time-based validation

ADDITIONAL

Technical Skills: SIEM (Splunk, Wazuh), SOAR (Shuffle), Log Analysis, Alert Triage, Incident Response, IOC Investigation, Threat Detection, Case Documentation, OSINT, MITRE ATT&CK, Packet Analysis (Wireshark, Zeek), EDR concepts, Windows/Linux log sources, Sysmon, PowerShell/Bash (basic), OpenVAS, CrowdStrike (familiar), Email Security (familiar), Protocols (DNS, HTTP, SMB, SSH, FTP), Ports (1-65535), Communication (Report Writing, Escalation), Team Collaboration in SOC workflows.
Tools: Nmap, wireshark, metasploit, OpenVAS, Wazuh, Suricata, Splunk siem, Shuffle SOAR, aircrack-ng, OSINT, theharvester, Maltego, Dirbuster, Ghidra, Autopsy, Docker, FTK Imager, x64dbg.
Certifications & Training: Certified Ethical Hacker [CEHv11], Fundamentals of Deep Learning [Nvdia], Basel's Open Source Intelligence [OSINT], Cyber Threat Intelligence 101 [ArcX]