

Sudarshan Rangappa

[LinkedIn](#) | [GitHub](#) | [Portfolio](#)

Email: Sudarshan_rangappa@proton.me

Mobile: +91 8302720020

EDUCATION

National Forensic Sciences University

Master of Science in Cybersecurity; GPA: 8.2

Gandhinagar, Gujarat

Aug 2023 – May 2025

Bengaluru City University

Bachelor of Computer Applications; GPA: 8.16

Bengaluru, Karnataka

Jul 2020 – Jul 2023

SKILLS SUMMARY

- **Application Security & Secure SDLC:** OWASP Top 10, CWE-25, Threat Modeling, SAST (SonarQube), DAST (OWASP ZAP, Burp Suite), Fuzzing, Security Code Review, Secure Coding Guidelines (Java, C, JavaScript, HTML, Python)
- **Web & Network Security:** Web Application Penetration Testing, Authentication/Authorization Security, Data Protection, API Security, SSL/TLS Configuration, Layer 7 Security
- **Offensive Security & Red Teaming:** Nmap, Metasploit, SQLMap, OpenVAS, MSFvenom, Privilege Escalation (Windows/Linux), Credential Dumping, Lateral Movement
- **Monitoring & Analysis:** Splunk (SPL), Wazuh, Suricata, Wireshark, Log Correlation, Incident Analysis
- **Tooling & Frameworks:** Git, Docker, MITRE ATT&CK, Shuffle SOAR, Threat Intelligence Platforms
- **Soft Skills:** Threat Reporting, Risk Communication, Technical Documentation, Developer Security Training

WORK EXPERIENCE

Co-Lead | Anti Cyber Crime Society | [CERTIFICATE](#)

Sep 2022 - Feb 2023

- Supervised and mentored 10 interns in phishing response, threat validation, and IOC triage workflows.
- Reviewed 200+ phishing emails, URLs, and attachments, extracting indicators using VirusTotal and URLScan.
- Delivered training sessions on phishing kits, social engineering, and OSINT data gathering methods.

Volunteer | Anti Cyber Crime Society | [CERTIFICATE](#)

Jul 2022 - Aug 2022

- Collected and analyzed 100+ phishing submissions from Indian users; flagged domains tied to malware C2s.

PROJECTS

Integrated Cyber Defence System | [LINK](#)

May 2025

- Developed full-scale SOC lab simulating enterprise operations using Splunk, Wazuh, Suricata, Shuffle, and OpenVAS.
- Correlated logs across 3 VMs (Windows Server 2025, Windows 11, Ubuntu); achieved 100% alert detection rate.
- Simulated 10+ APT-style attacks (brute force, lateral movement, privilege escalation, data exfiltration).
- Built and deployed SOAR playbooks in Shuffle for IP blocking, WHOIS lookup, and GeoIP enrichment.

Location-Based IoT Security Key | [LINK](#)

Nov 2024

- Designed access-control system using ESP8266 + GPS with geofencing logic ($\pm 5m$) to authorize device access.
- Achieved 90%+ accuracy in real-world unauthorized access prevention across 20+ field test iterations.
- Tuned sampling frequency and implemented time-based validation to eliminate GPS spoof false positives.

CERTIFICATES

Certified Ethical Hacker (CEH v11) | [CERTIFICATE](#)

Jan 2023

- Mastered ethical hacking lifecycle: Recon, Scanning, Gaining Access, Maintaining Access, and Covering Tracks.
- Performed simulated penetration tests using Nmap, Metasploit, and Burp Suite against lab environments.
- Conducted vulnerability assessments using Nessus and manual exploitation techniques.
- Demonstrated proficiency in web application attacks (OWASP Top 10) and social engineering vectors.

Fundamentals of Deep Learning (NVIDIA) | [CERTIFICATE](#)

Dec 2023

- Trained image classification CNN models using TensorFlow and PyTorch with GPU acceleration.

Basel's OSINT Certificate | [CERTIFICATE](#)

June 2025

- Collected public threat intelligence using Maltego, Google Dorks, DNSDumpster, and social media scraping.

Cyber Threat Intelligence 101 (ArcX) | [CERTIFICATE](#)

July 2025

- Applied CTI lifecycle to case studies; aligned TTPs with MITRE ATT&CK framework for threat reports.