

Sidharth M

Cybersecurity Analyst | Incident Response | Red Teaming | Security Hardening

+91 7012950681 | sidharthmannikoth@gmail.com | [linkedin.com/in/msidharth](https://www.linkedin.com/in/msidharth) | github.com/ERROR-SIDDH
portfolio-resume-91o.pages.dev | ORCID: 0009-0004-6473-8482

SUMMARY

Cybersecurity practitioner with hands-on experience in critical infrastructure - responding to compromised web infrastructure, analysing phishing campaigns and supporting red-team engagements. Secured 10+ compromised domains, remediation and hardening. Builds security automation for CIS compliance auditing (Linux and FortiGate), and has authored peer-reviewed research on cloud-native attack detection and next-generation firewalls. Background in DevOps and infrastructure operations.

EXPERIENCE

Cyber Dome, Kerala Police Kozhikode, Kerala, India

Volunteer — Cybersecurity Operations Aug 2025 – Present

- Secured 10+ compromised domains: investigated each compromise, identified the exploited weaknesses, and supported restoration and hardening of the affected sites.
- Contribute to cybersecurity threat analysis and operational security support for the division.
- Deliver community security awareness programs on cyber threats and safe online practices.

Security Intern May 2025 – Jul 2025

- Analysed phishing campaigns — mapped attacker TTPs, identified malicious infrastructure, and contributed to threat-detection improvements.
- Deployed and configured OPNsense next-generation firewalls; documented firewall rule-bypass techniques for internal red-team research.
- Supported red-team exercises and network reconnaissance to identify security gaps.

VIT Chennai — School of Computer Science (SCOPE) Chennai, India

Security Research Intern (SRIP 2025) | Supervisor: Dr. T. Subbulakshmi May 2025 – Jul 2025

- Built a cloud-native attack dataset and an ML classification model for cloud security threats ([dataset repo](#)).
- Combined threat intelligence with machine learning; work published in IJCNC (peer-reviewed).

ACM VIT Chennai Chapter Chennai, India

Vice Chair (Oct 2025 – Aug 2026) · Membership Chair & Web Lead (Apr – Oct 2025) Apr 2025 – Aug 2026

- Own the security posture and technical operations of the chapter website and infrastructure for a 200+ member technical community.
- Hardened and maintained the chapter website; led technical event operations and onboarding.

KSRP Kerala, India

DevOps Specialist Oct 2020 – Jan 2022

- Managed DevOps operations and server infrastructure for 1 year 4 months.

SECURITY PROJECTS

CIS Benchmark Hardening Toolkit — Level 1 2025 – 2026

Bash, UFW, iptables, auditd, AppArmor [GitHub](#)

- Modular toolkit implementing CIS Ubuntu 22.04 LTS Level 1 hardening across authentication, SSH, filesystem, kernel/network sysctl, logging, firewall, AppArmor and sudo controls.
- Defence-in-depth firewall module: SSH brute-force rate limiting, anti-spoofing (RFC 1918 drops), scan protection (NULL/XMAS/FIN/non-SYN), ICMP hardening and strict outbound allowlist.
- Compliance validator audits 73 CIS controls with a PASS/FAIL/WARN HTML dashboard and auto-rollback on failure.

FortiGate CIS Compliance Checker

Python, FortiOS REST API, SSH [GitHub](#) | [Project page](#)

- Read-only auditor that checks a FortiGate firewall against hardening controls modelled on the CIS FortiGate 7.x Benchmark (admin policy, management access, SNMP, NTP, remote logging).
- Read-only by design at two layers: GET-only REST client with an allow-listed SSH command set, plus a device-side read-only API access profile.
- Produces console, CSV and HTML reports, with the FortiOS remediation commands for every failed check.

DDoS Visual Forensic Analysis

2022

Python, dpkt, MaxMind GeoLite2, Plotly, Folium

[GitHub](#)

- Forensic analysis of a real volumetric UDP flood (152k+ PPS) against a game server; stream-parsed 18.3M+ packets from raw PCAP.
- Automated pipeline for traffic metrics, IP-spoofing detection via TTL analysis, and geo-enrichment; interactive maps of botnet distribution and attack origin clusters.

AEGIS ExamLab — Secure Proctored Exam Platform

2025

Next.js 14, TypeScript, MongoDB, Google Genkit, Docker

[GitHub](#)

- Platform for administering and monitoring proctored exams across lab PCs, with a 5-step server-side validation chain (PC approval → student mapping → exam assignment → status check → duplicate-submission guard).
- Real-time PC telemetry (15 s heartbeat), full admin audit logging, and an AI-assisted question bank (Gemini).

PUBLICATIONS

Analysis and Visualization of Cloud Native Attacks in a Secure Testbed

2026

Subbulakshmi T, Adithyan P, Sidharth M, Arun Santhosh R A — *International Journal of Computer Networks & Communications (IJCNC)*, Vol. 18, No. 2 | DOI: [10.5121/ijcnc.2026.18206](#)

Next Generation Firewall: A Comprehensive Analysis and Practical Applications

Book Chapter, 2025

Brindhya Subburaj, Subbulakshmi T, Sidharth M — *IGI Global, Implementing Enterprise Cybersecurity with AI (Ch. 9)* | DOI: [10.4018/979-8-3373-2252-0.ch009](#)

Setting Up A Security Testbed In Windows Using Docker

Jul 2025

T. Subbulakshmi, Aditya Kushwaha, Sidharth M — *Open Source For You (OSFY) Magazine* | [Read article](#)

TECHNICAL SKILLS

Offensive Security: Web Application & Network Penetration Testing (VAPT), Red Teaming, Network Reconnaissance, Firewall Bypass, OSINT

Defensive Security: Incident Response, Phishing Analysis, Threat Intelligence, Threat Detection, PCAP Forensics, CIS Compliance Auditing, Linux & Firewall Hardening

Tools: Burp Suite, Nessus, Nmap, Wireshark, tcpdump, Hydra, VirusTotal, Kali Linux, FortiGate, OPNsense, UFW, iptables, auditd, AppArmor

Frameworks: MITRE ATT&CK (TTP mapping), OWASP Top 10, OWASP Testing Guide, CIS Benchmarks, Zero Trust Architecture, Site-to-Site VPN

Engineering: Python, Bash, C/C++, SQL, TypeScript, Next.js, MongoDB, Flask, Nginx, Docker, Git, Cloudflare

EDUCATION

Vellore Institute of Technology (VIT), Chennai

2024 – 2028

B.Tech, Computer Science & Engineering — Specialisation in Cybersecurity