SUDHARESHAN V

B.E. Computer Science & Engineering (Cyber Security) • Final Year
Coimbatore, Tamil Nadu • +91 77089 39021 • vsudhareshan@gmail.com
linkedin.com/in/sudhareshan-v-b99733144 • github.com/BlackDeath-1708

SUMMARY

Final-year Computer Science (Cyber Security) student who builds backend services, Linux networking tools and kernel-level (eBPF) programs. Research intern at CAIR, DRDO, and former co-founder and CTO of a cybersecurity startup, bringing strong communication, problem-solving and time-management skills from leading delivery and collaborating with client stakeholders.

EDUCATION

B.E. Computer Science & Engineering (Cyber Security) *2023 – 2027*
Sri Krishna College of Engineering and Technology, Coimbatore • CGPA 8.49 / 10 (approx. 3.4 / 4.0 GPA)

Higher Secondary (Class XII) — Bharathi Matric Higher Secondary School • 91.6% *2023*

EXPERIENCE

Research Intern — Centre for Artificial Intelligence & Robotics (CAIR), DRDO *Jul 2026 – Dec 2026*
Bengaluru | Python, Streamlit, traceroute, RIPE Atlas / RIPEstat, Globalping, MaxMind GeoLite2

- Designing measurement-based and topology-based methods to geolocate IP addresses at city level across Indian ISP networks, as a more precise alternative to OSINT geolocation databases.
- Collecting and cleaning traceroute data from distributed probes; analyzing hop timing and topology to infer location.
- Building Python and Streamlit tooling to run measurements and explore results.

Co-Founder & Chief Technology Officer — XecureOne *May 2025 – Nov 2025*
Cybersecurity startup, Coimbatore

- Engineered backend services on the MERN stack and deployed websites on AWS, owning the path from code to production.
- Owned technical architecture and on-time delivery, collaborating with the founding team and client stakeholders; deployed a centralized SIEM platform and Zeek/Suricata traffic-inspection pipelines for real-time threat detection across enterprise endpoints.
- Communicated security concepts to non-specialists through training on SIEM operations and incident response; hardened identity infrastructure with Active Directory and Group Policy.

PROJECTS

ODIN — Passive Network Threat Detection (Smart India Hackathon) | *Python, Zeek, Kafka, Flask, React, Docker*

- Built a threat-detection system for one-way mirrored network traffic: Zeek → Kafka → six threat detectors → correlation engine → Flask API with live SSE streaming → React dashboard, all running on Docker Compose.
- Raised pipeline throughput 4.74× by micro-batching inference; diagnosed and fixed pipeline bugs surfaced by real traffic, including a Zeek log join that had silently disabled TLS detection.

PhishGuard — Web Vulnerability Scanner | *Python, Django, JavaScript, Chrome Extension, Docker*

- Built a Chrome extension with a Django backend that runs 9 client-side security checks per page, including missing security headers, mixed content, weak cookie flags, open redirects and outdated JS libraries.
- Assigns a severity level and remediation steps to every finding; containerized with Docker and deployed on Render.

Endpoint Application Firewall | *Python, Flask, Linux, iptables, NFQUEUE*

- Built a host-based firewall that maps each outgoing connection to its originating process via /proc and netlink sockets, with a rule-based allow / deny / throttle policy engine.
- Created a Flask REST management console for multi-endpoint administration, traffic logging and alerts; enforced policy on encrypted traffic via TLS metadata (JA3, SNI).

Kernel-Level Endpoint Security (self-initiated, ongoing) | *C, eBPF / XDP, BPF-LSM*

- Writing eBPF programs at the XDP hook for line-rate in-kernel packet classification, and BPF-LSM hooks for per-process network access control that resists root bypass.
- Built a telemetry pipeline streaming events from eBPF programs to a userspace daemon through shared-memory ring buffers.

SKILLS

Languages: Python, Java, JavaScript, C, Bash

Backend & Platforms: MERN (MongoDB, Express, React, Node.js), Flask (REST APIs), Django, Streamlit, Kafka, AWS, Linux, Docker, VMware, Windows Server

Systems & Networking: eBPF / XDP, Netfilter / NFQUEUE, netlink sockets, /proc, TCP/IP, TLS

Security & Identity: SIEM (Wazuh), Suricata, Zeek, Wireshark, Nmap, Metasploit, OpenVAS, Active Directory

Professional: Communication (verbal & written), teamwork & collaboration, stakeholder management, time management, problem-solving, initiative

ACHIEVEMENTS

- **Top 5, Rajasthan Police Hackathon (National Level)** — national cybersecurity challenge organized with law enforcement.
- **Winner, Pitch Perfect, Anokha 2024** — technical innovation competition, Amrita Vishwa Vidyapeetham, Coimbatore.
- **Winner, Ideathon, Cauvery College, Trichy** — design of a real-time network threat detection system.