

Suraj Vishwanath

Cybersecurity Student · Software Engineer

☎ +91 7893636415 — ✉ hello@surajv5.in — 📍 Hyderabad, India — 🌐 surajv5.in — 📄 suraj-vishwanath — 🕹 svlord5

Summary

Cybersecurity student focused on SOC operations, Digital Forensics and Incident Response (DFIR), threat detection and threat intelligence. Developed **ThreatLens**, an AI-powered SOC/SOAR platform using Wazuh, Google Gemini and automated DFIR workflows. Hands-on experience in incident investigation, MITRE ATT&CK, log analysis, Linux and Python through TGCSB, CTFs and cybersecurity projects.

Education

GITAM University, Hyderabad

2023–2027

B.Tech in Computer Science & Engineering, Cybersecurity Specialisation

Technical Skills

Cybersecurity: SOC Operations, Incident Response, Digital Forensics, Threat Detection, Threat Intelligence, MITRE ATT&CK

Security Tools: Wazuh, FTK, Autopsy, Wireshark, Nmap, Burp Suite

Programming: Python, JavaScript, TypeScript, SQL

Development: Next.js, React, Supabase, REST APIs

Systems: Linux, Windows, Docker, Git

Experience

Information Security Associate Intern — Telangana Cyber Security Bureau (TGCSB), Telangana Police
Jun 2026 – Jul 2026

- Developed **ThreatLens**, an AI-powered SOC, SOAR and DFIR platform for threat detection and incident response.
- Integrated **Wazuh SIEM** with Windows and Linux endpoints for real-time security telemetry and alert monitoring.
- Implemented IOC extraction, MITRE ATT&CK mapping and AI-assisted incident triage using Google Gemini.
- Built DFIR workflows for host isolation, memory acquisition, evidence collection and file quarantine using Wazuh Active Response.
- Validated detections using Event ID 1102 log clearing, EICAR malware and LSASS credential dumping simulations.

Head of Technical Domain — HackOps GITAM

Jan 2025 – Present

- Lead cybersecurity initiatives and technical infrastructure; author bi-weekly security newsletters reaching 1,000+ students.

Head of Technical Innovation & Support — National Service Scheme, GITAM Hyderabad

Feb 2024 – Present

- Lead digital infrastructure, technical support and technology initiatives.

Founder & Lead Developer — OneRiki Services

2023 – Present

- Build and deploy web platforms using Next.js, TypeScript and modern authentication systems.

Projects

surajv5.in — Personal Portfolio & Cybersecurity Platform

2023 – Present

- Designed and developed a modern personal portfolio showcasing cybersecurity projects, certifications, CTF achievements and technical work.
- Built and maintained web tools and interactive labs using Next.js, TypeScript and modern web technologies.

ThreatLens — AI SOC, SOAR & DFIR Platform

2026

Next.js, TypeScript, Supabase, Wazuh, Docker, Google Gemini

- Built an AI-augmented SOC platform with live SIEM monitoring, IOC extraction, MITRE ATT&CK mapping and AI-generated incident summaries.
- Implemented Active Response, Chain of Custody and DFIR workflows for investigation and automated response.
- Implemented an integrated **OSINT reconnaissance module** for domain and website intelligence, including DNS records, WHOIS data, subdomains, IP information and technology fingerprinting.

Achievements

- **3rd Place** — HackOps GITAM Capture The Flag (CTF) Competition.
- **19th Nationwide** — Breach Point 2026 National-Level CTF, Offline Grand Finale.
- **ACE Awards 2025–26** — Outstanding Contribution to Student Life and Excellence in Community Impact, GITAM NSS.

Certifications

TryHackMe: Cyber Security 101, Pre Security, Advent of Cyber 2025 — **Hack The Box:** Networking Foundations

Google: Foundations of Cybersecurity, Assets Threats & Vulnerabilities, Linux and SQL — **Proofpoint:** AI Email Security

Additional

Languages: English, Hindi, Telugu — **Interests:** SOC, DFIR, Threat Detection, CTFs, Cybersecurity Research