SAHIL ANIL NIKAM

SOC Analyst (L1) | Blue Team | SIEM • Wazuh • Splunk | Incident Response

Nashik, Maharashtra, India • +91 8329935878 • sahilnikam133@gmail.com
Portfolio: hackwithsahil.vercel.app • linkedin.com/in/sahil-nikam • github.com/sahilnikam2410
Immediate joiner — open to relocation: Pune / Mumbai / Bengaluru / Hyderabad / Gurugram

5-Module Certified SOC Program | **3-Month** Enterprise SOC Internship | **Wazuh + Splunk** Hands-On | **Cyber 50** Founder

PROFESSIONAL SUMMARY

B.Tech Computer Science graduate (2026, CGPA 8.53) with hands-on SOC experience from a 3-month SOC Analyst internship at ESCOSS LLP and a prior cybersecurity internship. Certified across all five modules of the SevenMentors SOC Analyst Program — Networking, Linux, CEH, WAPT and Python for SOC. Skilled in SIEM deployment and administration (Wazuh, Splunk), log monitoring, event correlation, alert triage, incident response, threat intelligence and active-response automation, with detection logic mapped to MITRE ATT&CK.

CORE TECHNICAL SKILLS

SOC & Blue Team ▸ SIEM (Wazuh, Splunk), Log Monitoring & Correlation, Alert Triage, Incident Response, Threat Hunting, MITRE ATT&CK, Sysmon & Windows Event Log Analysis, IOC & Threat Intelligence, Active-Response Automation, Security Configuration Assessment, SOC Reporting & Escalation
Security Tools ▸ Wazuh, Splunk, Sysmon, Nmap, Wireshark, Burp Suite, DVWA, VirtualBox
Offensive Security ▸ Ethical Hacking (CEH methodology), Web Application Penetration Testing (WAPT), OWASP Top 10, Vulnerability Assessment
Networking ▸ TCP/IP, OSI Model, DNS, DHCP, HTTP/HTTPS, CCNA Fundamentals, Firewalls, VPN, Network Scanning & Traffic Analysis
Operating Systems ▸ Windows 10 / Server, Linux (Kali, Ubuntu), Linux CLI, System Hardening
Scripting for SOC ▸ Python — log parsing, IOC enrichment, alert automation, API integration; Bash

CERTIFICATIONS

> **SOC Analyst Program — SevenMentors Pvt. Ltd.** — certified in all five modules: **Networking**, **Linux**, **CEH (Certified Ethical Hacker)**, **WAPT (Web Application Penetration Testing)** and **Python for SOC**.

- TATA Cybersecurity Analyst Job Simulation — Forage (2024)
- Cybersecurity — Tech Mahindra Foundation / Skill India (2024)
- IT Security Foundations: Network Security — LinkedIn Learning (2025)
- Ethical Hacking: SQL Injection — LinkedIn Learning (2024)

PROFESSIONAL EXPERIENCE

SOC Analyst Intern — Mar 2026 – Jun 2026
ESCOSS LLP

- Deployed and administered **Wazuh SIEM** and implemented **Splunk**, building integrations that centralised log collection across Windows and Linux endpoints.
- Monitored security events, performed log correlation and alert triage, and executed incident-response workflows to investigate and contain threats.
- Configured active-response automation to auto-contain suspicious activity such as brute-force login attempts, reducing manual response effort.
- Ran security configuration assessments and authored structured SOC technical reports. **Internship certified by the COO and Director.**

Founder & Security Lead — 2024 – Present
Vrikaan — AI-Powered Cybersecurity & Fraud Detection Platform (vrikaan.com)

- Founded and lead security engineering for a consumer platform covering phishing and scam detection, real-time monitoring and dark-web exposure scanning.
- Analysed live phishing and social-engineering campaigns and converted attacker techniques into automated detection and classification logic.
- Designed a multi-tier LLM routing architecture balancing complex threat-reasoning workloads against high-volume classification tasks.

Cyber Security Intern — Aug 2023 – Sep 2023
Academor Online E-Learning Services Pvt. Ltd.

- Performed network scanning and reconnaissance with Nmap; analysed phishing, DoS/DDoS and session-hijacking techniques from a defensive perspective; completed cryptography and ethical-hacking labs on Kali Linux.

KEY PROJECTS

The Silent Operator — SOC Detection & Red-Team Simulation Lab — Final-Year Project • 2025–2026

- Built an end-to-end SOC lab (Wazuh SIEM, Kali Linux, Windows 10, VirtualBox) ingesting Sysmon and system logs from multiple endpoints into centralised dashboards.
- Simulated controlled red-team attacks mapped to MITRE ATT&CK, then detected them via log correlation, custom alert rules, triage and threat hunting — exposing and closing detection gaps.

Protocol Honeypot — Network Intrusion Detection System — Security Project • 2025

- Designed and deployed a network-based IDS and honeypot to lure, log and analyse unauthorised access and reconnaissance activity, correlating attacker behaviour into actionable alerts.

Protocol Cinema — Covert-Channel Detection Research — Security Research • 2025

- Studied a steganographic C2 technique tunnelling data through public APIs in an authorised lab and translated the attacker TTPs into defensive detection logic for covert exfiltration, mapped to MITRE ATT&CK (Command & Control).

EDUCATION

B.Tech, Computer Science & Engineering — 2022 – 2026 • CGPA 8.53 / 10
Sandip University

Programming: Python, C, C++, Java, Bash • **Languages:** English (Professional), Hindi (Native), Marathi (Native)