Himangshu Pan

SOC Analyst · Blue Team

India researchersheru@gmail.com +91 9332943989 linkedin.com/in/sheru-pan github.com/sheru-pan
tryhackme.com/p/researchersheru

SUMMARY

Python developer turned **defensive security researcher**. Strong programming and systems background (Python, Linux, backend, blockchain) re-applied to blue-team work: detection engineering, log analysis, incident response, and SOC operations. CEH (2018). Active on TryHackMe (@researchersheru) — SOC and defensive paths. Comfortable in the terminal, in Wireshark, and in a SIEM query bar.

CORE SKILLS

SIEM / Log Analysis — Splunk, ELK / OpenSearch, Wazuh, KQL, Sigma rules **Network Forensics** — Wireshark, tcpdump, Zeek, Suricata, PCAP triage **Endpoint** — Sysmon, Microsoft Defender, OSQuery, Velociraptor **Scripting** — Python, Bash, PowerShell, Regex **Frameworks** — MITRE ATT&CK, D3FEND, NIST CSF, Cyber Kill Chain **Lab** — Linux, Docker, VMware, Git, Ghidra (basics)

CERTIFICATIONS

- **Certified Ethical Hacker (CEH)** — EC-Council, 2018
- Blue Team Level 1 (BTL1) — *in progress*
- CompTIA Security+ — *in progress*

EXPERIENCE

Independent Defensive Security Research · 2025 – Present

Returned to security with a deliberate blue-team focus.

- Building a personal lab (ELK + Wazuh + Sysmon) to reproduce attacker behavior and write Sigma detections against it.
- Writing public CTF and detection-engineering walkthroughs at sheru-pan.github.io.
- Working through TryHackMe SOC paths and CTF rooms as @researchersheru — focusing on detection-side learning, not just flag capture.
- Studying Microsoft Defender, KQL, and MITRE ATT&CK mappings via BTL1-style scenarios.

Freelance Backend / Blockchain Developer · 2021 – 2024

- Built and deployed **Secret Invoice** on the Secret Network (privacy-preserving smart contracts).

- Contributed to **Emprops** (NFT + AI platform) — backend logic, test coverage, secure system design.
- Deepened practical experience with secure system design while working outside formal cybersecurity roles.

Klizo Solutions Pvt. Ltd. · Backend / Blockchain Engineer · 2019 – 2021

- Built decentralized-identity solutions on **Hyperledger Indy** and **Aries**.
- Production Python backend work; took ownership of security-sensitive integrations.

AQB Solutions Pvt. Ltd. · Python Developer · 2016 – 2018

- Built data crawlers, PDF parsing pipelines, and structured-data ingestion services.
- Earned **CEH** in 2018 — laying the foundation for the eventual blue-team pivot.

Government of India · CCTNS Project — Contract Trainer · 2015 – 2016

- Delivered training for the Crime and Criminal Tracking Network & Systems project (police-department digitization).
- Taught fundamentals and basic programming at Unique Computer Academy in parallel.

EDUCATION

Add formal qualifications here (degree, institution, year).

WHAT I'M LOOKING FOR

A SOC Tier-1 / detection-engineering / DFIR-leaning role where I can contribute code-comfortable analysis, write detections, and grow alongside a defensive team.