Sarthak Mishra

sarthakatwork08@gmail.com | +91 77030 86808 | www.shaivarth.com |
linkedin.com/in/shaivarth | github.com/shaivarth

Summary

Computer Science undergraduate with hands-on experience building Python-based security and backend systems, including network monitoring, telemetry processing, static malware analysis, and RESTful applications. Strong foundation in Linux, networking, Python, databases, and security engineering.

Education

Vellore Institute of Technology *Bhopal, India*
Bachelor of Technology in Computer Science and Engineering **CGPA:** 7.70/10.00

Technical Skills

Security: Threat Detection, Security Monitoring, Log Analysis, Event Correlation, Alert Triage, Incident Response, IOC Analysis, Threat Hunting, Malware Analysis, Phishing Fundamentals, MITRE ATT&CK

Security Tools & SIEM: Splunk, SPL, Microsoft Sentinel, KQL, Wireshark, Nmap, Scapy, Firewalls, IDS/IPS, EDR

Networking & Systems: Network Traffic Analysis, Packet Analysis, Linux (Ubuntu), Windows

Languages: Python, SQL, Bash, C++

Backend & Databases: FastAPI, Flask, REST APIs, API Security, Authentication, PostgreSQL, Redis

Development Tools: Git, GitHub, Postman, Pytest

Projects

Xentinel – SOC Telemetry & Detection Platform *| Python, Flask, Linux, JSON*

- Built a real-time SOC simulation platform that generates authentication telemetry, processes security events, and produces severity-based alerts through a modular detection pipeline.
- Engineered detections for SSH brute-force, password-spray, user-enumeration, suspicious administrative logins, and multiple-session abuse, with MITRE ATT&CK technique mapping and source-IP telemetry.
- Developed a SIEM-style dashboard with live alert feeds, threat analytics, interactive analyst workflows, and incremental alert streaming for investigation and triage.

Arpex – ARP Spoofing Detection & Network Monitoring *| Python, Scapy, Flask, SQLite, Pytest*

- Engineered a real-time ARP monitoring system that discovers network devices, establishes IP-to-MAC baselines, and detects suspicious mapping changes.
- Implemented verification workflows to validate anomalous ARP activity and reduce false positives, while tracking attacks, affected devices, and security events.
- Built forensic evidence handling with PCAP capture/download, persistent SQLite storage, and a Flask dashboard for device inventory, network anomalies, and incident investigation.

Hexora – Static File Analysis & Triage Platform *| Python, FastAPI, SQLAlchemy, SQLite*

- Built a static file-analysis platform that inspects files without execution, using cryptographic hashing, file-signature detection, metadata extraction, entropy analysis, and heuristic risk scoring for security triage.
- Implemented detection of suspicious strings, URLs, IP addresses, and file characteristics to identify artifacts requiring further investigation.
- Developed a FastAPI backend with SQLAlchemy and SQLite for structured analysis workflows and detailed security-report generation.

Eagle – Digital Forensics & Image Intelligence Tool *| Python, FastAPI, EXIF, OSINT*

- Developed a Python-based digital forensics and OSINT tool that extracts EXIF metadata, camera information, GPS coordinates, and image properties across JPEG, PNG, HEIC/HEIF, TIFF, WebP, and BMP formats.
- Built a CLI and Python library interface supporting structured JSON output, optional reverse geocoding, and integration into automated OSINT workflows.
- Implemented local-first analysis and input validation, including 100-megapixel image limits and binary-tag sanitization to mitigate decompression and malformed-metadata risks.

Certifications

- **Certified Ethical Hacker (CEH) v13** – EC-Council *(Training in Progress; Exam Enrolled)*
- **Pre Security Learning Path** – TryHackMe