Sarthak Mishra

Email: sarthakatwork08@gmail.com | Phone: +91 77030 86808 | Shaivarth.com |
LinkedIn: linkedin.com/in/shaivarth | GitHub: github.com/Shaivarth

Professional Summary

Computer Science undergraduate with experience building security tooling, detection systems, backend applications, and real-time monitoring platforms using Python, FastAPI, Flask, SQL, and Linux. Passionate about Blue Team operations, Security Engineering, Detection Engineering, and backend software development, with hands-on experience designing telemetry pipelines, SIEM-style monitoring systems, network analysis tools, and security-focused developer applications.

Education

Vellore Institute of Technology *Bhopal, India*
Bachelor of Technology in Computer Science and Engineering
CGPA: 7.60/10.00

Technical Skills

Languages: Python, C++, SQL, Bash

Defensive Security: Splunk, Microsoft Sentinel, MITRE ATT&CK, Wireshark, Nmap, Scapy, KQL, Log Analysis, Threat Detection, Event Correlation.

Frameworks & Libraries: FastAPI, Flask, Pydantic, SQLAlchemy, Jinja2, Requests, Pytest, Asyncio.

Operating Systems & Networking: Linux(Ubuntu), Windows, macOS, TCP/IP, DNS, HTTP/HTTPS, ARP, SSH

Databases & Web Technologies: PostgreSQL, SQLite, Redis, REST APIs, HTML, CSS, JavaScript.

Developer Tools: Git, GitHub, GitLab, Docker, VS Code, Postman, UTM VMs

Core Concepts: Data Structures and Algorithms, Object-Oriented Programming (OOP), Database Management Systems (DBMS), Operating Systems, Computer Networks.

Projects

Hexora – Static Malware Analysis Platform *| Python, FastAPI, SQLAlchemy, SQLite, Docker*

- Developed a FastAPI-based web application for static file analysis, capable of analyzing **90+ diverse file samples across multiple formats** through a secure browser-session isolated workflow without executing uploaded content.
- Designed a modular analysis pipeline integrating cryptographic hashing, file signature detection, metadata extraction, entropy analysis, heuristic scoring, and persistent report storage using SQLAlchemy and SQLite.
- Built an interactive web interface supporting detailed analysis reports, searchable history, and containerized deployment using Docker for consistent development and execution.

Arpex – Real-Time Network Monitoring Platform *| Python, Flask, Scapy, SQLite, Jinja2*

- Developed a real-time network monitoring platform that discovers devices, captures live network traffic, maintains IP-to-MAC mappings, and monitors network state using Python and Scapy.
- Designed a modular backend architecture for device discovery, packet processing, verification workflows, event logging, persistent SQLite storage, and PCAP evidence management.
- Built a Flask-based dashboard to visualize network topology, device inventory, monitoring events, and captured packet evidence through an interactive web interface.

Xentinel – SIEM & Detection Engineering Platform *| Python, Flask, Chart.js, JSON*

- Developed a real-time monitoring platform using Python and Flask to ingest telemetry, process telemetry streams, and generate structured alerts through a modular backend architecture.
- Built an interactive web dashboard with live visualizations, severity-based event monitoring, and JSON-driven analytics using HTML, CSS, JavaScript, and Chart.js.
- Engineered a Linux-based development workflow using Ubuntu, VS Code Remote SSH, and Git to develop, test, and manage monitoring services inside an isolated virtualized environment.

Certifications & Achievements

- Completed the **HackerRank Software Engineer Intern** Certificate.
- **Pre Security Learning Path** Completion Certificate by TryHackMe.
- Earned **5-Star Gold badges** in both **Python** on HackerRank.

Security Research & Responsible Disclosure

- Conducted independent **security research** on **JSTOR's PDF delivery workflow** and privately submitted a responsible disclosure report documenting an authorization workflow observation and remediation recommendations.