JAY KAWA

SOC Analyst | SIEM, Threat Detection & DFIR
jaykawa56@gmail.com | +91 9867554174 | linkedin.com/in/jaykawa | github.com/Jay8590

EXPERIENCE

Karpuragaurai Technologies
Lead Software Developer — Security Automation & DFIR Tooling
Nov 2024 – Present | Mumbai, India | Remote
Project: MyFRT — Python-based digital forensics platform

- Lead the MyFRT development team — engineered a Python DFIR platform that reduced incident triage time by 90%, including automated EVTX parsing from E01/DD forensic images
- Migrated search and storage from Elasticsearch/MongoDB to OpenSearch/CouchDB with pre-computed indexing, sustaining near real-time search across 100GB+ datasets
- Automated live RAM acquisition (AVML) and E01/DD disk imaging with hash verification (MD5/SHA-256) for evidentiary integrity
- Built a secure Flask REST API (JWT/RBAC), an HTML reporting engine, and packaged the platform as a Windows installer (NSIS)

PROJECTS

- **Security Operations (SIEM) Home Lab**
  - Built a Security Information and Event Management (SIEM) lab (Wazuh EDR, Snort IDS, Splunk, Wireshark) in a virtual enterprise network to practice detection and monitoring.
  - Created Splunk dashboards and detection rules that identified simulated brute-force and lateral-movement attacks.
- **Log Analyzer**
  - Built a Python/Streamlit tool to parse, filter, and investigate security log files — supporting incident investigation workflows
  - Tech Stack: Python, Streamlit
- **Homomorphic Encryption — Secure Grade Management System**
  - Preserved data privacy by encrypting student grades while allowing computation on encrypted data without decryption using Homomorphic Encryption techniques
  - Tech Stack: Python, Cryptography
- **Dynamic Data Anonymization Tool**
  - Built a Python/Streamlit tool to automatically detect and redact PII from large datasets using configurable hashing and masking rules
  - Tech Stack: Python, Streamlit, pandas

TECHNICAL SKILLS

- **SIEM & Security Analytics:** Splunk, OpenSearch, Elastic Stack, Wazuh, Wireshark, Log Analysis
- **Threat Detection & Response:** Incident Response, Threat Detection, Alert Triage, EDR
- **Digital Forensics (DFIR):** Autopsy, Volatility, EVTX Analysis, YARA, John the Ripper, Magnet Forensics, FTK Imager
- **Network & Vulnerability Assessment:** Snort, Nmap, OpenVAS
- **Programming & Automation:** Python, Bash Scripting, Flask, API Development
- **Operating Systems:** Linux, Windows, macOS
- **Offensive Security Tools:** Metasploit, Burp Suite

EDUCATION

University of Mumbai — B.E. Information Technology
2020–2024 | CGPA: 8.1/10 | Cybersecurity Club Leader — Burp Suite & Metasploit

CERTIFICATIONS & TRAINING

- Google Cybersecurity Professional Certificate | Jul 2024
- TryHackMe: Cyber Security 101 | Sep 2025
- Cisco Introduction to Packet Tracer | Nov 2022
- CEH — Certified Ethical Hacker (In Progress)
- CTFs: TryHackMe, picoCTF, OverTheWire (cryptography, web exploitation, Linux command-line security)
- Simulations: ANZ Australia | Mastercard | AIG Shields Up (Oct 2023)