Samaranjan Manjhi

+91 9082650120 • samaranjanedu01@gmail.com • LinkedIn • Portfolio • Kandivali, Mumbai

SUMMARY

C/C++ Systems & Security Engineer with **3 years** of experience building production-grade endpoint security tools, kernel-level monitors, binary integrity frameworks, and DLP systems for **macOS and Linux**. Deep expertise in Endpoint Security framework, Ed25519 cryptographic signing, inotify/fanotify execution gating, syscall hooking, Qt GUI development, and cross-platform C++ architecture. Delivered **16 enterprise security modules** at MicroWorld Software Services.

TECHNICAL SKILLS

Languages: C, C++, Bash, SQL
Frameworks: Qt5/6, Endpoint Security (ESF), fanotify, inotify, libcups, FSEvents, BSM Audit, CoreFoundation
Security: Ed25519 (libsodium), PCRE2, OpenSSL (MD5/SHA/AES-256), pf firewall (pfctl), Tesseract OCR, Poppler
Tools: Git, Xcode, GDB, Valgrind, SQLite3, libcurl, libxml2, libmagic, pugixml, Boost, libarchive
CS Core: DSA, Multithreading, IPC (Unix Sockets), OS Internals, Linux (Ubuntu/RHEL), macOS (10.14+)

PROFESSIONAL EXPERIENCE

Programmer — C/C++ Systems & Security | MicroWorld Software Services Pvt. Ltd. — Mumbai *Aug 2023 – Present*

- Designed and delivered **16 production security modules** spanning kernel monitors, DLP engines, binary integrity systems, firewall rule generators, and cloud backup agents — integrated into eScan EDR/XDR/DLP enterprise products.
- Worked across the full systems stack: Linux kernel modules (.ko), macOS ESF, fanotify/inotify event loops, Unix domain socket IPC, multi-threaded C++ daemons, and Qt GUI applications.

KEY PROJECTS

MW Guardian — Binary Integrity & Execution Gating | C/C++, fanotify, Ed25519, Linux .ko *Feb 2026 – Present*

- Used **fanotify FAN_OPEN_PERM** to freeze binaries at kernel exec() — verifier validates Ed25519 signatures synchronously while frozen; tampered binaries receive SIGKILL before executing a single instruction.
- Multi-key signing pipeline (keygen → signer → verifier) with key rotation; old public keys retained so previously signed binaries remain valid across rotations.
- Self-verification at startup: guardian and verifier both verify their own signatures before the event loop starts, closing the bootstrap trust gap.

Linux Ransomware Defense — Kernel Module | C, Linux .ko, ftrace, syscall hooking *Dec 2025 – Feb 2026*

- Hooks **sys_rename, sys_execve, sys_open** via ftrace; detects ransomware by suffix pattern matching and bulk-rename behavioural thresholds, then SIGKILLs the offending process with JSON log to dmesg.
- Module hides from lsmod post-load; exposes a password-protected sysfs interface — attacker cannot rmmod without the correct passphrase even after discovering it via dmesg.
- Configurable at insmod time: custom max-rename threshold, behaviour detection toggle, and password — no recompile needed for policy changes.

Printer Control & DLP — macOS | C/C++, ESF, libcups, Xcode *Oct 2025 – Jan 2026*

- Responds ALLOW on **AUTH_OPEN**; on NOTIFY_CLOSE scans the complete CUPS spool file — if PII (PAN, SSN, email) detected, deletes file and cancels job before cupsd dispatches to the printer.
- Supports application-level whitelist/blacklist; whitelisted apps bypass content scan, blacklisted apps are blocked regardless of content — enforced via ESF process identity.
- Archives scanned print jobs with scan result metadata for compliance reporting and forensic audit trail of all blocked/allowed print events.

File Integrity Monitoring (FIM) — macOS | C/C++, FSEvents, SQLite3, OpenSSL *Jun 2025 – Aug 2025*

- FSEventStream daemon storing MD5 hash, permissions, size, and timestamps in SQLite; raises real-time alerts on any unauthorized modification, deletion, or rename of watched paths.
- Baseline snapshot on first run; subsequent runs diff against snapshot and emit structured event logs — supports multiple watch directories from a config file.

Content Scanner — DLP Engine & CLI | C/C++, PCRE2, Tesseract OCR, Poppler, libarchive *Sep 2024 – May 2025*

- PII detection across **15+ file formats** via PCRE2 regex and OCR; packaged as shared library (.dylib/.so) and standalone CLI tool.
- Real-time Unix socket server variant — clients send file paths and receive scan results without re-initialising the regex engine, reducing per-scan latency significantly.

macOS Firewall — pf Rule Engine | C/C++, pfctl, libxml2, IP range arithmetic *Sep 2025*

- Generates and applies **pf firewall rules** from XML policy files; supports zone-based rules, trusted-MAC enforcement, Trojan IP blocklists, IP range arithmetic, and live reload without reboot.
- Parses multi-zone XML policies into pf.conf anchor rules; detects active network interface automatically and binds rules to the correct interface at runtime.

COMPETITIVE PROGRAMMING

Coding Ninjas • GeeksForGeeks • LeetCode — Practised DSA: arrays, trees, graphs, DP, sliding window, and binary search.

EDUCATION

Bachelor of Engineering — Computer Engineering
Shree L.R. Tiwari College of Engineering, Mumbai University — 2019 – 2023 — CGPA: **8.56 / 10**