MANIKANDAN S

manikandan.sathish44@gmail.com | LinkedIn | GitHub | Portfolio

OBJECTIVE

Computer Science student with hands-on experience securing production infrastructure serving 1500+ users, building SIEM-driven detection rules, and developing Python-based security automation for real-time alerting and response. Seeking a **Security Engineer** role focused on automated threat detection and incident response workflows. Demonstrated technical depth through competitive CTF performances (5th place DEFCON DCxTCTF'26, Top 5% PicoCTF, Top 15% HTB), Active Directory penetration testing, and production security engineering with zero security incidents.

EDUCATION

Vellore Institute of Technology (VIT) Aug 2023 – Present
B.Tech, Computer Science & Engineering **CGPA: 9.09/10**
Coursework: Network Security, OS, Cryptography, DBMS, AWS Cloud
Research: Contributor to Secure IoT Initialization and Encryption Framework (accepted, pending publication)

CERTIFICATIONS

Digital Forensics Essentials v1 (DFEv1) – EC-Council Jul 2025 – Jul 2028

TECHNICAL SKILLS

- **Security:** Vulnerability Assessment & Penetration Testing, SIEM (Azure Sentinel) rule authoring, EDR Policy Tuning (CrowdStrike), Network Analysis (Wireshark, Nmap), Digital Forensics, Incident Response, Active Directory Security
- **Infrastructure:** SSH Hardening, Access Control, Linux Server Administration, Log Aggregation & Analysis, Secure Configuration
- **Programming:** Python (security automation & scripting), Bash, C/C++, Java, Rust
- **Tools:** Burp Suite, Metasploit, GDB, Binary Ninja, Git, Kali Linux

PROFESSIONAL EXPERIENCE

Production Security & Infrastructure Engineer Vellore Institute of Technology
Part-time May 2024 – Present

- Architected and maintained hardened production infrastructure for the VISTA Capstone Project Management System, supporting 1500+ active users with 99.5% uptime and zero security incidents; established automated backup systems, disaster recovery procedures, and security patch management workflows to ensure business continuity

Cybersecurity Intern Genzeon

- Conducted penetration testing and vulnerability assessments on web applications; delivered detailed security reports with remediation recommendations
- Configured Azure Sentinel SIEM infrastructure with custom analytics rules for real-time threat detection and automated incident response
- Tuned CrowdStrike EDR policy so authorized test payloads stopped being quarantined mid-engagement, scoping the exception to the security team and gating file execution behind senior approval rather than disabling the control

TECHNICAL PROJECTS

VISTA Capstone Project Management System – *Security & Infrastructure* VIT Chennai

- **Secured production infrastructure for 1500+ users:** Architected hardened MongoDB deployment with SSH key-only authentication, IP whitelisting, and encrypted communications; achieved 99.5% uptime with zero security incidents
- **Built automated detection & alerting pipeline:** Deployed comprehensive logging infrastructure with anomaly detection; developed Python-based automation to trigger real-time alerts and initiate response actions on suspicious activity
- **Maintained defense-in-depth operations:** Established automated backup systems, disaster recovery procedures, and security patch management; performed regular security audits and vulnerability scans

DockSec – *AI-Powered Container Security* GlitchCon'25 Finalist

- Built ML-based anomaly detection for containerized environments: an LSTM model trained on Docker logs cross-references predictions against system utilization metrics to auto-pause compromised containers
- Integrated Anchore-backed CVE scanning for DevSecOps coverage; Python/FastAPI backend concurrently monitors multiple containers for real-time alerting

ACHIEVEMENTS

CTF Competitions: DEFCON DCxTCTF'26 (5th Place), PicoCTF'25 (Top 5%), HTB Cyber Apocalypse'25 (Top 15%), DawgCTF'26 (84th Place)
Security Labs: TryHackMe Ossuary – Active Directory penetration testing against Windows Server 2022 DC
Hackathons: MLH Devshouse'25, Glitchcon'25 Finalist
Community: Microsoft Innovations Club, Open Source Programming Community (OSPC)