

Syed Abdul Mateen

AI-Driven Security Tools | Python & System Monitoring Final-Year B.Tech CSE Student – ICFAI Tech Hyderabad

Kollur, Hyderabad, Telangana, India | syedabdulmateen284@gmail.com | +91 7286830284

SUMMARY

Final-year B.Tech CSE student at ICFAI Tech Hyderabad focused on building production-level AI and cybersecurity tools. Experienced in developing Python-based applications for threat detection, real-time process tracking, and data leak risk assessment. Built and tested systems to monitor 1000+ system events, detect suspicious behavior, and verify file integrity. Currently deploying tools that combine automation, risk scoring, and report generation to address real-world security use cases.

SKILLS

Core Software Engineering Skills:

Data Structures & Algorithms • Object-Oriented Programming (OOP) • Problem Solving • SDLC
Version Control (Git) • REST APIs • Debugging & Testing • Agile / Scrum Collaboration

Programming & Tools:

Python • Scikit-learn • OpenCV • Flask • Streamlit • ReportLab • psutil • win10toast • YAML • Git • GitHub

Cybersecurity & AI:

Threat Detection • File Integrity Monitoring • Real-time Process Tracking • Prompt Engineering
AI for Security • Basic ML Models

Soft Skills:

Communication • Technical Writing • Incident Response Coordination • Root Cause Analysis

CAREER OBJECTIVE

To secure a role in AI-driven cybersecurity where I can build intelligent defense tools, automate threat detection, and contribute to safer digital systems. Currently focused on deploying real-world security solutions using Python, AI, and automation.

LANGUAGES

English • Telugu • Hindi • Urdu • Arabic

ONLINE PROFILES

GitHub: <https://github.com/Syed-Abdul-Mateen>

LinkedIn: <https://www.linkedin.com/in/syed-abdul-mateen-2-8-4/>

Portfolio: <https://syed-abdul-mateen.github.io/>

EDUCATION

IFHE University

B-Tech CSE

Narayana jr. college

MPC

Shishu vihar high school

SSC Board

TECHNICAL ACHIEVEMENTS

- Automated threat detection across 10,000+ log events
- Reduced resume screening time by 70% using LLMs
- Developed real-time system monitoring tools used across 3+ simulated environments

CORE PROJECTS

1. **AI-Driven Real-Time Cyberattack Detection System**(Python, Scapy, NetworkX, Flask, ReportLab)
 - Detected live cyber threats from 1000+ packets/min using Scapy
 - Auto-generated PDF reports for 20+ anomalies via Flask dashboard
2. **Suspicious Process Activity Detector**(Python, psutil, Tkinter, YAML, win10toast)
 - Auto-killed 40+ blacklisted processes using psutil & custom rule engine
 - Added GUI + rule toggles, improving manual review time by 50%
3. **AI Resume Screener**(Python, LangChain, OpenAI API, Streamlit)
 - Reduced screening time by 70% via AI-based resume scoring
 - Analyzed 50+ resumes with real-time results on Streamlit UI
4. **Endpoint Ransomware Behavior Analysis Engine**(Python, Scikit-learn, psutil, JSON)
 - Simulated ransomware and profiled 30+ encryption behaviors
 - Logged risky patterns and isolated processes using ML logic
5. **System Log Anomaly Detection Framework**(Python, Pandas, Matplotlib, IsolationForest)
 - Analyzed 10K+ log entries to detect anomalies with Isolation Forest
 - Visualized risk clusters, cutting incident triage time by 60%
6. **Insider Threat Behavior Detection System**(Python, Time-Series Analysis, Heatmaps)
 - Flagged suspicious user activity using time-series patterns
 - Generated heatmaps highlighting access misuse trends
7. **Data Leak Risk Assessment Toolkit**(Python, Regex, Logging)
 - Scanned directories & flagged 30+ leak patterns with 90% accuracy
 - Generated risk scores using regex heuristics & log analysis
8. **File Integrity Verification & Alert System**(Python, Hashlib, CLI)
 - Verified 500+ files using hash comparison; flagged tampered ones
 - Triggered alerts within 2 sec/file via lightweight CLI tool

