# CHANDRAPRAKASH C

## Aspiring Cybersecurity Intern | SOC Analyst Enthusiast

📍 Dindigul, Tamil Nadu | 📞 +91 9786475035 | ✉️ cyberchandru87@gmail.com
**Portfolio:** https://chandruthehacker.github.io | **LinkedIn:** https://linkedin.com/in/chandraprakash87 |
**GitHub:** https://github.com/chandruthehacker

## SUMMARY

Cybersecurity-driven Computer Science student with hands-on experience in offensive security, SIEM log analysis, and threat detection. Developed AI-powered security tools and automated workflows using Python/Bash. Passionate about blue team operations, with a proven ability to reduce false positives by 20% and analyze attack patterns. Seeking to leverage technical skills in a SOC or penetration testing role.

## TECHNICAL SKILLS

- **Security Tools:** Burp Suite, Wireshark, Nmap, Wazuh SIEM, Metasploit, Splunk (Basic)
- **Programming:** Python (Flask, Pandas), Bash, Regex, PowerShell
- **Threat Detection:** Log Analysis, IDS/IPS, YARA Rules, Sigma Alerts
- **Networking:** TCP/IP, DNS, Firewall Configs, VPNs
- **Documentation:** Incident Reports, MITRE ATT&CK Mapping, Markdown

## EDUCATION

**B.Sc. Computer Science**
*GTN Arts College, Tamil Nadu* | 2023 – 2026

- Relevant Coursework: Network Security, Cryptography, Python, Databse

## CERTIFICATIONS

- Google Cybersecurity Professional Certificate – Coursera | April 2025
- Ethical Hacking Training – Internshala | November 2024

## EXPERIENCE

**Cybersecurity Project Developer – Freelance**
*Jan 2024 – Present*

- Refined Wazuh detection rules to reduce false positives by 20%.
- Performed log analysis and drafted incident reports.
- Automated alerting with custom Python/Bash scripts.

## PROJECTS 🔗 View My Projects

**AI-Powered Phishing Email Detector | GitHub**

- AI-based tool that classifies phishing emails using Google Gemini and regex, achieving 85% accuracy.

**Admin Login Honeypot Trap | GitHub**

- Deceptive login interface that captures attacker IPs and logs unauthorized credential attempts.

**Log Parser Tool | GitHub**

- Automated log parser for Apache/Syslog/authlog/nginx to detect brute-force patterns and generate quick insights.

## ADDITIONAL

**Availability:** Immediate | Remote/Hybrid/On-site.