

ADNAN KAKKATTIL

CYBER SECURITY ANALYST

+91 9744466737 | contact.adnanks@gmail.com | [Linkedin](#) | [Github](#)

SUMMARY

Results-oriented Cyber Security Professional with deep expertise in Purple Teaming, bridging the gap between offensive (Red Team) and defensive (Blue Team) strategies. Proven track record in architecting Security Operations Centers (SOC), developing custom security automation tools in Python, and conducting advanced penetration testing. Dedicated researcher and educator with published work on AI integration in cyber security frameworks.

PROFESSIONAL EXPERIENCE

Gritstone Technologies LLP | Cyber Security Lead & Information Security Analyst June 2024 – Present

- Penetration Testing:** Executed comprehensive Vulnerability Assessments and Penetration Testing (VAPT) across web, mobile, thick client applications, and cloud infrastructure.
- Defensive Engineering:** Enhanced organizational security posture through routine firewall audits, log analysis, and integrating secure coding practices into the SDLC.
- Red Teaming & Training:** Conducted internal Red Team exercises to evaluate employee awareness and delivered training sessions to significantly reduce phishing susceptibility.

Room Number 404 Community | Tech Lead & Keynote Speaker

August 2025 – Present

- Platform Engineering:** Led the full-stack development of the "Room 404" community platform and custom web applications to streamline security operations and knowledge sharing.
- Community Leadership:** Designed and executed competitive Capture The Flag (CTF) events and hands-on workshops to foster practical skill development within the cyber security community.
- Public Speaking:** Served as a Chief Speaker at major events, delivering technical presentations on emerging security trends and threat landscapes.

PROJECTS

Zyra: AI-Powered SIEM Platform

- Innovation: Engineered "Zyra," a custom SIEM platform using FastAPI and Flask, centralized for advanced security operations.
- Threat Detection: Integrated custom Machine Learning models to automate log analysis, accelerating the identification of subtle network anomalies and threats.
- Incident Response: Built remote incident response capabilities, including malware analysis tools, remote system control, and real-time evidence gathering.

AI Agent-Powered Email Attack Detection System

- Phishing Defense: Developed an AI-driven system to proactively classify and block sophisticated phishing attacks, outperforming traditional filtering rules.
- Automation: Leveraged n8n to connect email infrastructure with AI filtering agents, executing multi-channel alerts via Discord and email.
- Metrics Dashboard: Created a custom UI to track attack frequency and classification metrics, providing actionable intelligence on threat vectors.

SECURITY CONTRIBUTIONS & DISCLOSURES

Tamil Nadu Education Management System

- Tamil Nadu Education Management System
- Critical Vulnerabilities: Discovered and reported 5+ critical vulnerabilities, including severe logic flaws.
- Data Breach Prevention: Identified an exposed unauthenticated Grafana server containing sensitive PII for students and faculty, leading to immediate remediation.
- Account Takeover: Disclosed critical Response Manipulation and Mass Assignment vulnerabilities that allowed for full account takeovers and password reset bypasses.

University Management System

- Access Control: Uncovered severe IDOR (Insecure Direct Object Reference) flaws that allowed unauthorized access to sensitive university data.

SKILLS

- Core Competencies: Penetration Testing, Vulnerability Assessment (VAPT), SOC Operations, Red/Blue/Purple Teaming, Threat Hunting, Incident Response.
- Technical & Tools: SIEM Implementation, Python Security Automation, Firewall Auditing, Web & Mobile App Security, n8n Automation, FastAPI/Flask.
- Soft Skills: Technical Mentorship, Public Speaking, Team Leadership, Research & Documentation.

EDUCATION

- MSc Computer Science | Nilgiri College of Arts and Science, Thaloor | 2025 – Present
- BSc Computer Science | Nilgiri College of Arts and Science, Thaloor | 2022 – 2025
- Certified Penetration Tester | Red Team Hacker Academy | 2024

PUBLICATIONS & PRESENTATIONS

- International Conference (Nilgiri College): Presented peer-reviewed paper on "AI Agent-Powered Malicious Email Attack Detection System."
- International Conference (Providence College): Published findings on IoT security in "CCTV Hacking and Prevention."
- National Conference (Don Bosco College): Presented strategic research on "AI in Cyber Security," highlighting future industry trends.