# Aditya Rajendra Kadam

+91 87670 07682 | kadamaditya457@gmail.com | linkedin.com/in/aditya-kadam | github.com/Adi-hub56 | Pune, Maharashtra, India

*SOC Operations · Incident Response · Vulnerability Assessment · Penetration Testing*

## Professional Summary

Entry-level cybersecurity professional with hands-on SOC operations, incident response, and vulnerability assessment experience, backed by 100+ practical labs and a top-4% TryHackMe ranking. Skilled in SIEM log analysis and penetration testing tools including Burp Suite, Nmap, and Metasploit. Built and deployed independent Python security tools, including an AI-powered SOC incident-response platform and a phishing-detection engine. Strong foundation in MITRE ATT&CK, the Cyber Kill Chain, and OWASP Top 10.

## Technical Skills

**Programming:** Python, SQL, Bash scripting

**Security Tools:** Burp Suite, Nmap, Metasploit, sqlmap, Nessus, Wireshark, tcpdump, hping3

**SIEM & Monitoring:** Splunk, ELK Stack, log analysis, security monitoring

**Networking:** TCP/IP, DNS, HTTP/HTTPS, SSH, VPN, firewalls

**Operating Systems & Cloud:** Kali Linux, Ubuntu, Windows Server, AWS

**Security Concepts:** OWASP Top 10, MITRE ATT&CK, Cyber Kill Chain, incident response, threat hunting, vulnerability assessment, IAM

**Development & Tools:** FastAPI, Next.js, TypeScript, JWT authentication, Git, GitHub

## Projects

**Asta SOC Agent — AI-Powered SOC Platform** | Next.js, FastAPI, SQLAlchemy, JWT, TOTP, Groq LLM

- Engineered a full-stack SOC incident-management platform with Next.js and FastAPI, integrating the Groq LLM API to auto-generate incident-response recommendations aimed at speeding up analyst decision-making.
- Implemented JWT-based authentication with TOTP two-factor login, API key management, and session tracking to secure multi-user access.
- Deployed the application to Vercel and Render and load-tested it to confirm stable performance under concurrent multi-user activity.

**PhishGuard — AI-Powered Phishing Detection Tool** | JavaScript, HTML, CSS, heuristic threat scoring

- Developed a standalone phishing-detection tool applying 14 heuristic checks (DNS reputation, TLS validation) with a 0–100 automated risk-scoring engine, in a fully offline single-HTML deployment with no third-party API dependency.
- Published the detection methodology in a peer-reviewed paper in the International Journal of Innovative Research in Technology.

**Cowrie SSH Honeypot — Threat Intelligence System** | Python, Linux, log analysis, Wireshark

- Configured a Cowrie SSH honeypot that captured 200+ real attacker sessions, automating log parsing in Python to extract 500+ attacker IPs, credentials, and behavioral patterns.
- Analyzed malware traffic across 50+ sessions in Wireshark, tracing command-and-control infrastructure and attacker behavior patterns.

## Virtual Experience

**Hydroficient IoT Cyber Defense Externship — Extern** **Jul 2026 – In Progress**

- Selected for an 8-week live cybersecurity externship in IoT threat modeling and defense — covering Python for IoT security data analysis and securing MQTT communication pipelines.

**Mastercard Cybersecurity Job Simulation — Forage** **July 2026**

- Identified and reported simulated phishing threats as an analyst on Mastercard's Security Awareness Team, assessing business units for security-awareness gaps.

**Tata Cybersecurity Analyst Job Simulation — Forage** **July 2025**

- Completed an identity and access management (IAM) simulation for Tata Consultancy Services, applying IAM principles and delivering documentation aligned with business objectives.

## Certifications

- CompTIA Security+ — Exam Scheduled September 2026
- Cisco Networking Academy — Introduction to Cybersecurity
- Fortinet Network Security Expert (NSE 1, NSE 2, NSE 3)

## Education

**MIT ADT University, Pune** **2023 – 2026**

*B.Tech, Computer Science (Cybersecurity and Forensics)*

## Achievements

- Ranked in the top 4 percent globally on TryHackMe (100+ labs) and finished 10+ PortSwigger Web Security Academy labs covering OWASP Top 10 exploitation, including SQL injection and XSS.