ADITYA D

Email: adityadiv204@gmail.com **Mobile:** +91 9901830608 **Location:** Bengaluru, India

Portfolio | **LinkedIn** | **GitHub** | **LeetCode**

EDUCATION

BMS Institute of Technology & Management, Bengaluru, India — 2023 – Present
Bachelor of Engineering in Computer Science Engineering — **CGPA: 9.35**

Chethana PU College, Bengaluru, India — 2021 – 2023
Pre-University (PCMC) — **94.00%**

Vidyaniketan School, Bengaluru, India — 2011 – 2021
ICSE Grade 10 — **94.80%**

EXPERIENCE

Cybersecurity Trainee - CySecK Finishing School Program — **IISc Bengaluru, August 2026**

- Explored network and web security, cryptography, CVEs, threat modeling, spoofing, and RATs through hands-on attack simulations and security labs using Nmap, Wireshark, Burp Suite, Metasploit, Nikto, DIRB, and John the Ripper.
- Configured Snort for IDS/IPS and deployed Pentbox honeypots to detect live intrusions, while performing VAPT exercises across web (DVWA), Android (ADB, JADX, Genymotion), and IoT (Binwalk, Ghidra) CTF environments.
- Learned SIEM, SOC, IAM, and GRC frameworks through CISO-led sessions, including live device exploitation demos.

UNISYS – Industry Project Associate (Academic Industry Collaboration) — **Remote, December 2025 - July 2026**

- Built a rule-based auto-remediation system (PowerShell + Python/Flask + Flutter + SQLite) for Windows, achieving 2.8s mean detection time and 94.8% remediation success across 55 predefined rules.
- Designed a time-based event correlation & deduplication engine with event-specific lookback windows to identify related events and root causes, reducing duplicate alerts by 89%.
- Implemented a three-tier command-injection defense (isolated subprocess + sanitized env vars) and a human-in-the-loop approval gate, achieving an MTTR of 11.4s for automated remediation.

PROJECTS

1. ForenSys – Real-Time SOC & Automated Incident Response Platform

- Built a real-time SOC platform (FastAPI, Next.js, WebSockets, MySQL) streaming live host, process, and network telemetry on a 3-second cycle for continuous monitoring.
- Implemented live packet capture and protocol analysis with Scapy (BPF sniffer), along with RBAC for controlled system access.
- Built a modular threat correlation engine mapping 7 detection rules to MITRE ATT&CK, feeding SOAR playbooks for automated incident response, achieving an MTTR of approximately 10.9s.

2. OpenRecon – OSINT-Based Passive Reconnaissance Platform

- Built a full-stack recon platform (Python + FastAPI + React), also shipped as a CLI tool with 15 passive modules across DNS, WHOIS, SSL, IP, subdomains, security headers & analysis without active probing.
- Developed a concurrency engine using asyncio to run all 15 modules in parallel, cutting average scan time from 45s to 11s (75% faster than sequential execution).
- Built an interactive D3.js graph that visualizes target findings across security categories and auto-generates PDF scan reports.

3. ZK Vault - Zero Knowledge Password Manager

- Built a zero-knowledge password vault (Next.js 14) using Argon2id for password hashing and a KEK/VEK key-wrapping scheme to encrypt vault data with AES-GCM-256.
- Built an atomic registration flow requiring TOTP 2FA verification before account creation, plus a server-blind recovery protocol (HKDF-SHA256) that re-wraps keys without touching vault data.
- Hardened session security with DB-backed SHA-256 session tokens, Upstash Redis rate limiting, and global session revocation.

SKILLS

- **Programming Languages:** Python, C, C++, Java
- **Security Tools & Concepts:** Nmap, Wireshark, John the Ripper, Metasploit, Maltego, Splunk, OWASP ZAP, Burp Suite, OSINT, VAPT, Networking & Protocols, Encryption & Cryptography
- **Web Development:** HTML, CSS, JavaScript, Figma, Framer, Blender
- **Databases:** MySQL, SQLite
- **DevOps:** Git, GitHub, Docker
- **Cloud & AI:** AWS, Vercel, Google AI Studio, Claude Code, Antigravity

CERTIFICATIONS

- **Cloud Computing Foundations – Google Skills** — March 2026
  Scalable cloud infrastructure and deployment fundamentals.
- **Introduction to Cyber Security – Cisco Networking Academy** — September 2025
  Core cybersecurity principles, threat models, and risk mitigation strategies.