Chaitanya Dhotre

Junior Cybersecurity Engineer · Defensive, Offensive and Cloud Security

Mumbai, India · chaitanyad301@proton.me · chaitanyadhotre.dev · github.com/chaitanya-dhotre · linkedin.com/in/chaitanya-dhotre

PROFILE

Cybersecurity graduate-to-be (BSc Hons, University of Lancashire, 2027) who builds security tools end to end. Built and ran a data-collection pipeline for a threat-intelligence platform during an internship at CyArt Tech LLP; built a risk-adaptive AWS access-control system, a Windows evil-twin Wi-Fi detector, and an end-to-end encrypted messenger with a self-hosted cloud backend. Comfortable on both sides: detection, forensics and cloud hardening, plus hands-on exploitation labs. Available full-time from January 2027.

EXPERIENCE

Cybersecurity Intern – CyArt Tech LLP, Mumbai Aug 2026 – Dec 2026

Threat-intelligence / OSINT platform monitoring public Telegram groups · team of 7

- Built and ran a data-collection pipeline for a threat-intelligence platform: source discovery and registration over the Telegram MTProto API, a crawl runner with live log streaming and scheduling, and per-source health status.
- Verified the pipeline end to end (discover → register → crawl): 536 live messages collected in the first run with zero duplicates.
- Kept live and demo data strictly separate across 11+ API routes so analysts never saw demo data in live mode.
- Hardened the platform after PR review: audit logging on every write, typed confirmation plus a constant-time-compared operator token for mode switching, rate limiting on discovery, no internal paths in API responses.

TypeScript, Next.js, Node.js, Prisma, SQLite, GramJS (MTProto), Git / GitHub PR review

PROJECTS

RiskGate – risk-adaptive access control for AWS (final-year project) Sep 2026 – Jul 2027

- Scores CloudTrail activity using behaviour, IAM-policy and misconfiguration signals, ranks attack paths to critical assets, and grants only human-approved, time-bound STS sessions.
- Detected 6/6 malicious core scenarios with no false alarms (a severity-only baseline raised one), and 2/2 on scenarios written after the weights were frozen. Measured real AWS revocation delay (238 s) and reported it as a limit.

Python, FastAPI, AWS IAM/STS/CloudTrail, moto, pytest, SHA-256 hash-chained audit log

RogueAP Shield – evil-twin Wi-Fi detection for Windows 2026

- Windows service with a weighted seven-signal engine (BSSID baseline, beacon fingerprinting, gateway TTL, DNS probing, signal-strength outliers) and auto-learning of trusted networks.
- AES-256-GCM storage with PBKDF2-derived key wrapping, hash-chained audit log, and a VPN kill switch enforced through the Windows Filtering Platform.
- Validated against a live evil-twin attack and 53 access points on a university campus; all 15 functional and 7 non-functional requirements met.

C#, .NET 9, WPF, Windows Services, WireGuard

Kuch Bhi – end-to-end encrypted messenger 2026 – ongoing

- Flutter app with X25519 + AES-256-GCM encryption in a background isolate, offline-first storage and versioned group-key rotation.
- Self-hosted PocketBase backend on an Oracle Cloud VM with server-side membership rules and hooks; ran two security audits of my own code and fixed and device-tested every confirmed finding.

Flutter/Dart, Riverpod, Drift/SQLite, PocketBase, Oracle Cloud, Firebase Cloud Messaging

Offensive and forensics coursework 2025 – 2026

- Exploitation write-ups: SQL injection chain for CVE-2019-20183 (Nmap, Burp Suite, SQLMap), SNMP enumeration, ARP-spoofing credential capture, Windows unquoted-service-path privilege escalation (Metasploit), each with remediation.

- Digital forensics investigation plan for the Marriott Starwood breach: evidence acquisition (FTK Imager, EnCase, KAPE), order of volatility, steganography detection.

EDUCATION

BSc (Hons) Cyber Security and Networking – University of Lancashire (formerly UCLan), UK Sep 2026 – Jul 2027

Final-year top-up, studied online from India via Vidyalankar Institute · results expected July 2027

NCC Education Level 4 and Level 5 Diplomas in Computing – Vidyalankar Institute, Mumbai 2024 – 2026

Level 4: 82% · Level 5: 79%

CERTIFICATIONS

- **Completed:** EC-Council NSTDM (completion certificate).
- **Planned / in progress (2027):** Microsoft SC-200 · CompTIA CySA+ · TryHackMe SAL1 and PT1 · ISC2 Certified in Cybersecurity (CC).

SKILLS

Defensive	Log analysis, Wireshark, digital forensics (FTK Imager, Autopsy, KAPE, memory capture), detection logic, Microsoft Sentinel/Defender and KQL (learning)
Offensive	Nmap, Burp Suite, Metasploit, SQLMap, Wi-Fi attacks, Windows privilege escalation
Cloud	AWS IAM, STS, CloudTrail; Oracle Cloud (Linux VM, systemd); Azure (learning)
Crypto	AES-256-GCM, X25519, PBKDF2, hash-chained audit logs, key wrapping (DEK/KEK)
Code	Python, C#/.NET, TypeScript, Dart/Flutter, SQL, Bash, Git; Linux (Arch/CachyOS, Fedora, Ubuntu)
Languages	Marathi (native), English (C1, self-assessed), Hindi (fluent)