Chaitanya Dhotre

SOC Analyst (L1) · Detection, Threat Intelligence 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) with threat-intelligence internship experience: built and ran a data-collection pipeline that fed a Telegram OSINT platform. Builds detection and risk-scoring logic, reads logs for a living, and documents results honestly. Studying for SC-200 and the TryHackMe SOC Level 1 path. Available full-time from January 2027.

EXPERIENCE

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

- Built and ran a data-collection pipeline for a threat-intelligence platform: Telegram source discovery and registration (MTProto), crawl orchestration with live event streaming, scheduling and per-source health status.
- Collected 536 live messages in the first verified run with zero duplicates; kept live intelligence separate from demo data across the platform's API.
- Added audit logging on every write, operator-token authorisation and rate limiting after security review.

TypeScript, Next.js, Prisma, SQLite, GramJS (MTProto), Git

DETECTION PROJECTS

RiskGate – CloudTrail-driven risk scoring for AWS access Sep 2026 – Jul 2027

- Detectors for behavioural anomalies, risky IAM policies and misconfigurations feeding an explainable risk score (every alert lists the rules that fired); attack-path ranking shows which fix matters first.
- 6/6 malicious scenarios caught with zero false alarms, against one false alarm from a severity-only baseline; tamper-evident hash-chained audit log.

RogueAP Shield – evil-twin Wi-Fi detection 2026

- Seven-signal weighted detection engine with tuned alert throttling (no repeated popups, escalation on severity change); tested on a live attack and 53 campus access points.

Digital forensics investigation plan – Marriott Starwood breach 2026

- Evidence acquisition across workstations, mail and database servers (FTK Imager, EnCase, KAPE), order of volatility, chain of custody, steganography detection.

EDUCATION

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

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

Level 4: 82% · Level 5: 79%

CERTIFICATIONS

Completed: EC-Council NSTDM (completion certificate). **Planned 2027:** Microsoft SC-200 · CompTIA CySA+ · TryHackMe SAL1 · ISC2 CC.

SKILLS

SOC	Log and event analysis, alert triage, Wireshark, threat intelligence / OSINT collection, Microsoft Sentinel/Defender and KQL (learning)
Forensics	FTK Imager, Autopsy, KAPE, memory capture, Windows artefacts (MFT, Prefetch, registry)
Cloud	AWS IAM, STS, CloudTrail; Oracle Cloud Linux
Code	Python, TypeScript, C#, SQL, Bash