

Het Kotadiya

AI Safety & Cybersecurity | OSINT & Investigative Work

India · Remote | hetkotadiya0303@gmail.com | hetkotadiya.com | linkedin.com/in/het-kotadiya | github.com/Het-Kotadiya

SUMMARY

Cybersecurity master's student (graduating Nov 2026) working at the intersection of AI safety and cybersecurity, with a long-standing pull toward OSINT and investigative work. Hands-on with OSINT investigations, offensive-security labs, and AI agent safety research — red-teaming and evaluating large language models, and monitoring AI agents. Pivots on indicators to connect weak signals across public sources, preserves evidence, and writes clear, well-sourced reports. Learns new tools fast and works independently.

EDUCATION

DePaul University | *Master of Science, Cybersecurity* Sep 2025 – Nov 2026

- **Coursework:** Security Capstone (OSINT and offensive-security labs), Software Security Assessment, Network Security, Digital Forensics

P.P. Savani University | *B.Tech, Computer Science and Engineering* Oct 2021 – Jun 2025

AI SAFETY & RESEARCH

Layered AI Safety Defense for LLMs | *Security Capstone, DePaul University* In progress, Autumn 2026

- Red-teaming a large language model with jailbreak and prompt-injection attacks and building a multi-layer defense (working code)
- Built an evaluation that grades whether each attack succeeds and measures how much the defense reduces the attack success rate

Apart Research | *AI Collusion & AI x Epistemics Research Sprints* Oct–Nov 2026

- Building an LLM judge/monitor to grade whether an AI agent's stated reasoning matches its actions; follow AI agent failures and red-teaming incidents daily

OSINT & SECURITY

OSINT Investigations | *M.S. coursework and Security Capstone, DePaul University* 2025–2026

- Rebuilt a near-complete identity of a target from a single username (academic exercise): pivoted across social media, forums, DNS/WHOIS, web archives, code repos, and breach data, with evidence preserved and reported

Web Security & Threat Analysis Labs | *DePaul, TryHackMe, PortSwigger, picoCTF*

- 100+ HTTP requests analyzed in Burp Suite; Nessus scans with CVSS reports; 19+ TryHackMe rooms, 10+ picoCTF challenges; attacker TTPs via MITRE ATT&CK

EXPERIENCE

DePaul University | *Python Tutor* Oct 2025 – Present

- Coach 35+ undergraduates each quarter in Python and analytics; tutored students saw a 28% average accuracy gain; guides adopted by 70% of students; faculty error analysis contributed to a 15% higher course pass rate

DePaul University | *Grader, Internship for Accounting course* One quarter

- Reviewed and graded student submissions in voice, video, and written formats against consistent criteria

PROJECTS & LEADERSHIP

- **Power BI dashboards (B.Tech):** university results (pass/fail rates by subject) and sales (trends, top products/regions)
- **Red House Captain (school):** led 150–200 students to the inter-house cup, managed school events and budgets; ran a SEVA food project

SKILLS

- **OSINT & investigation:** pivoting on indicators across social media, forums, DNS/WHOIS, web archives, code repos and breach data; Sherlock, holehe, reverse image search
- **Security:** Burp Suite, Nmap, Nessus, Metasploit, Wireshark; OWASP Top 10; MITRE ATT&CK; CVSS
- **AI & programming:** red teaming & evals (prompt injection, jailbreaks); Python, Bash, Linux; Claude Code & LLMs daily