**1) Links to 3 selected job postings**

1. **OSINT Analyst — Moonshot (London, hybrid).** [moonshotteam.com](https://moonshotteam.com/careers/?utm_source=chatgpt.com)
2. **Threat Intelligence Analyst — Tech Against Terrorism (London).** [techagainstterrorism.org](https://techagainstterrorism.org/careers?utm_source=chatgpt.com)
3. **Digital Media Assessor (Police Staff) — Counter Terrorism Policing West Midlands (Birmingham).** [Counter Terrorism Policing+1](https://www.counterterrorism.police.uk/careers/digital-media-assessor-police-staff-counter-terrorism-policing-wm-2/?utm_source=chatgpt.com)

**2) Company research & “fit” (2–3 sentences each)**

**Moonshot**:Social impact company tackling online harms (extremism, terrorism, and organised crime) via OSINT, investigations, and data-driven interventions; current openings include OSINT Analyst (London, hybrid). Culture skews mission-driven and research-heavy; great if you enjoy analysis, client reporting, and measurable impact. Fit:Strong for your counter-terror OSINT interest and UK hybrid work. [moonshotteam.com](https://moonshotteam.com/careers/?utm_source=chatgpt.com)

**Tech Against Terrorism (TAT)** :NGO working with the UN, major tech platforms, governments, and civil societyto disrupt terrorist activity online while upholding human rights; hiring a Threat Intelligence Analyst in London. Excellent exposure to platform policy, takedowns, and CT threat landscapes. Fit: Ideal if you want CT intelligence work focused on terrorist exploitation of the internet. [techagainstterrorism.org+1](https://techagainstterrorism.org/careers?utm_source=chatgpt.com)

**Counter Terrorism Policing (CTP)**: UK national network with intelligence partners to prevent, deter, and investigate terrorism; police-staff role reviewing and classifying digital material/CCTV for intelligence and evidential value. Real CT casework; expect process discipline, legal awareness, and teamwork. Fit: Great if you want hands-on CT evidence assessment inside policing. [Counter Terrorism Policing+1](https://www.counterterrorism.police.uk/?utm_source=chatgpt.com)

**3) Job description reviews (from the postings)**

**Moonshot — OSINT Analyst (London, hybrid)**

* **Core:** Gather/analyse open-source data, produce intelligence on online harms/extremism, deliver client-ready reporting.
* **Signals:** OSINT tradecraft, social-media/network analysis, strong writing; experience with Python/SQL a plus; stakeholder comms. *(See careers listing.)* [moonshotteam.com](https://moonshotteam.com/careers/?utm_source=chatgpt.com)

**Tech Against Terrorism — Threat Intelligence Analyst (London)**

* **Core:** Produce terrorism/VE threat intelligence, track platform abuse, support industry/government partners, contribute to research outputs.
* **Signals:** Knowledge of terrorist ecosystems online, platform policy, indicators & behaviours, concise reporting. [techagainstterrorism.org+1](https://techagainstterrorism.org/careers?utm_source=chatgpt.com)

**CTP West Midlands — Digital Media Assessor (Police Staff)**

* **Core:** Review/assess large volumes of **CCTV and digital media**; identify intelligence on extremist/terrorist activity; maintain accurate viewing logs; flag undermining material (disclosure).
* **Signals:** National Intelligence Model awareness, meticulous records, chain-of-custody mindset; working in a CTU environment. [Counter Terrorism Policing](https://www.counterterrorism.police.uk/careers/digital-media-assessor-police-staff-counter-terrorism-policing-wm-2/?utm_source=chatgpt.com)

**4) Skills gap analysis (across the three postings)**

| **Required Skill / Qualification** | **I Have This Skill** | **Evidence / Example** | **How to Develop (if needed)** |
| --- | --- | --- | --- |
| OSINT tradecraft (collection, verification, pivoting, ethics) | Developing | Cybersecurity projects show investigative mindset; no explicit OSINT portfolio yet. | Complete an intro OSINT course (e.g., Bellingcat/SANS-style), build 2 public OSINT case studies (collection → verification → report), use Hunchly/SpiderFoot/Maltego on safe topics. |
| Social-media/network analysis | Developing | Programming + data skills (Python/SQL) but no SM analysis examples. | Practise graphing small datasets (e.g., follower networks) and write a short intel brief per case. |
| Threat intelligence writing (concise client reports) | Developing | University presentations and project write-ups; no CTI samples. | Produce 3× two-page briefs (exec summary, findings, sources, caveats) on public CT/online harms topics; get feedback. |
| Knowledge of terrorist/extremist online ecosystems & indicators | Developing | Interest evident from target roles; not documented in CV. | Create a safe reading plan (gov/NGO reports), maintain a glossary of TTPs/indicators; summarise weekly in a short memo. |
| Platform policy / content-safety workflows (moderation, TOS) | Developing | Not yet evidenced. | Read major platform policies; write a one-page comparison of enforcement signals and escalation paths. |
| Python for collection/analysis & automation | Yes | Python listed; built a honeypot and log analysis. | Extend with small OSINT scripts (API pulls, parsing, de-duplication). |
| SQL / data handling | Yes | SQL/MySQL listed in skills. | Practise joins/aggregations on small OSINT datasets; document queries in a notebook. |
| Stakeholder communication | Yes | Led teams in hospitality; customer support at Santander; clear client comms. | Convert comms strength to analyst briefings; rehearse 5-minute verbal read-outs. |
| Analytical attention to detail / record-keeping | Yes | Cash handling, reconciliations, accurate records in prior roles. | Use checklists and viewing logs in portfolio work to mirror policing standards. |
| Digital evidence handling (CCTV review, viewing logs) | No | Not yet evidenced. | Study ACPO Good Practice Guide (digital evidence), practise on sample CCTV datasets, create example viewing logs and rationales. |
| Chain of custody / CPIA disclosure awareness | No | Not yet evidenced. | Take a short CPD on UK disclosure/CPIA; draft a one-page SOP for evidence handling. |
| National Intelligence Model (NIM) awareness | No | Not yet evidenced. | Read an NIM primer; map how an intel product supports tasking/collection/assessment. |
| Data protection (GDPR), security & ethics | Developing | Security+ prep; care-sector ethics background. | Add GDPR basics; include a data-handling statement in each portfolio piece. |
| Bilingual (EN/ES) for multilingual collection | Yes | Spanish (native), English (fluent). | Add one bilingual OSINT sample to portfolio. |
| Git / version control | Yes | Listed in skills. | Keep all scripts/notebooks in a public repo with a clear README. |
| Security+ (or equivalent baseline) | Developing | Actively preparing for CompTIA Security+. | Schedule exam and complete two full practice tests; add cert upon pass. |

**5) Short action plan — top 3 skills to develop next**

1. **OSINT tradecraft + social-media/network analysis**
   * Complete an intro OSINT course; build **two** portfolio case studies with full methodology and citations.
   * Implement small Python/SQL workflows for collection/parsing; publish in a GitHub repo.
2. **Digital evidence handling for CTP-style roles**
   * Learn **CPIA/disclosure**, **chain of custody**, and **viewing-log** practice; produce a mock SOP and a sample CCTV review with logs and timestamps.
3. **Threat-intel reporting (concise client-ready writing)**
   * Create **three** 2-page intel briefs (exec summary, findings, confidence levels, sourcing limits) on public, safe topics relevant to online harms/CT; rehearse a 5-minute verbal brief for each.

Optional parallel: **finish Security+** to evidence baseline security knowledge and discipline.