Making a Career in
Threat Intelligence

Know your enemy. Track them. Stop them.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 10 of 12
AUDIENCE	Students and analysts interested in threat intelligence

Contents

Digitally signed by Baba Shaheer Gutappa
Date: 2026.04.24 09:53:05 +01'00'

1. What Is Threat Intelligence?

Threat intelligence is the discipline of collecting, processing and analysing information about adversaries — who is attacking, how they operate, what they are targeting, and what their next move is likely to be. It transforms raw data about threats into actionable knowledge that helps organisations defend themselves more effectively.

The word 'intelligence' is key. Data is a list of malicious IP addresses. Information is those IPs linked to a known threat actor. Intelligence is understanding that this actor targets UK financial institutions in Q1 every year using spear-phishing, so your organisation should increase monitoring and awareness in January and February. That final step — turning information into a decision that changes behaviour — is what separates intelligence from noise.

Threat intelligence is not a product. It is a process.
You cannot buy a threat intelligence 'solution' and call the job done.
Intelligence must be relevant, timely, accurate and actionable to have value.

Level	Typical UK Salary	Roles
Junior / Analyst	£30,000 – £45,000	Junior CTI Analyst, Threat Intelligence Analyst, OSINT Analyst
Mid-level	£45,000 – £70,000	Senior CTI Analyst, Threat Researcher, Intelligence Engineer
Senior	£70,000 – £95,000	Lead Intelligence Analyst, Principal Threat Researcher, CTI Manager
Specialist	£85,000 – £120,000+	Strategic Intelligence Advisor, Nation-State Threat Analyst, CTIIC equivalent

Table 1: UK salary ranges for threat intelligence roles (CW Jobs, 2024)

2. Strategic, Operational, Tactical and Technical Intelligence

Not all threat intelligence is the same. It operates at four distinct levels, each serving a different audience with a different timescale and a different level of detail. Understanding this is fundamental — producing the wrong type of intelligence for your audience is one of the most common failures in CTI programmes.

Type	Audience	Timescale	Format	Example
Strategic	Board, C-suite, CISO	Months to years	Reports, briefings, risk assessments	Nation-state actors are increasingly targeting UK critical infrastructure. Recommend board-level risk discussion and investment in OT security.
Operational	Security managers, SOC leads, IR teams	Days to weeks	Campaign briefings, actor profiles, playbooks	LockBit 3.0 affiliate group has been observed targeting UK logistics companies via RDP exploitation. IR team should review RDP exposure immediately.
Tactical	SOC analysts, incident responders	Hours to days	TTPs, attack pattern summaries, hunting hypotheses	This threat actor uses WMI for persistence and Cobalt Strike for C2. SOC should hunt for anomalous WMI activity and known CS beacon patterns.
Technical	Firewall, SIEM, EDR engineers	Minutes to hours	IOCs — IPs, domains, hashes, YARA rules	Block these 14 IPs and 27 domains. Deploy this YARA rule to your EDR. Hash list attached for file-based blocking.

Table 2: The four levels of threat intelligence

Most CTI analysts produce all four types — but the most impactful and rarest is strategic.
The ability to write a clear, jargon-free strategic briefing for a board audience
is what separates senior CTI professionals from those who stay at the analyst level.

3. The Intelligence Cycle

Intelligence is not produced randomly — it follows a structured cycle that ensures the right questions are answered, the right data is collected, and the output reaches the right audience. The intelligence cycle has been used by government and military intelligence services for decades. The CTI community has adapted it for cybersecurity.

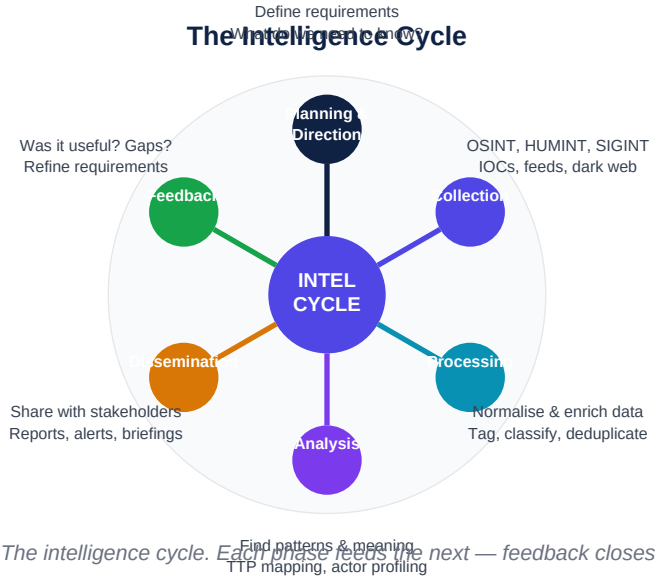


Figure 1: The intelligence cycle. Each phase feeds the next — feedback closes the loop.

Phase	What Happens	Common Failure
Planning & Direction	Define intelligence requirements (PIRs). What decisions will this intelligence support? Who needs it?	Skipping this — collecting data without a defined question produces intelligence nobody uses
Collection	Gather data from OSINT, commercial feeds, dark web, HUMINT, internal telemetry, ISACs	Over-reliance on one source. IOC feeds without context are not intelligence.
Processing	Normalise, deduplicate, enrich and tag collected data. Convert raw data into usable format.	Analysts buried in low-quality, unprocessed data with no tooling to manage it
Analysis	Identify patterns, attribute activity, assess intent, map to ATT&CK.; Produce the actual intelligence.	This is the hardest and most underinvested phase — often rushed
Dissemination	Deliver intelligence to the right audience in the right format at the right time.	Sending a 40-page technical report to the CISO. Wrong format, wrong audience.
Feedback	Consumers confirm whether the intelligence was useful and whether requirements have changed.	This almost never happens — closing the loop is consistently neglected

Table 3: Intelligence cycle phases, activities and common failure points

4. IOCs, TTPs and the Pyramid of Pain

Indicators of Compromise (IOCs) are the artefacts left behind by attackers — IP addresses, domain names, file hashes, email addresses. They are the most common form of threat intelligence shared between organisations. But not all IOCs are equally valuable. The Pyramid of Pain (Bianco, 2013) maps IOC types to the amount of pain it causes an attacker when you detect and act on them.

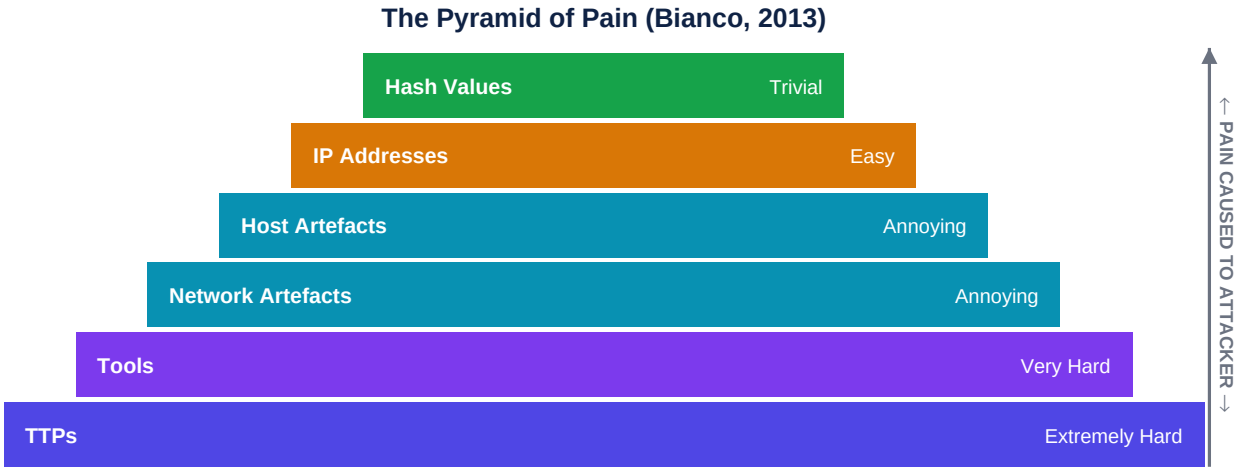


Figure 2: The Pyramid of Pain. Acting on TTPs hurts attackers most — they must fundamentally change how they operate.

The lesson of the Pyramid of Pain is that IOC-sharing — while valuable — is low on the pyramid. An attacker can change their IP address in minutes. Changing their TTPs — the way they move laterally, establish persistence, or communicate with their C2 — requires significant effort and retraining. The most valuable threat intelligence is TTP-level: understanding how an adversary operates, not just what artefacts they leave behind.

IOC Type	Example	Attacker Cost to Change	How to Use
File Hash (MD5/SHA)	d41d8cd98f00b204e9800998ecf8427e	Trivial — recompile or re-pack	Block in EDR. Low durability — expires quickly.
IP Address	185.220.101.47	Easy — rotate VPS or use Tor	Block at firewall. Add to SIEM detection. Verify context first.
Domain Name	updates.microsoft-cdn.net	Easy — register new domain	DNS sinkhole. Proxy block. Check for typosquatting patterns.
Network Artefact	HTTP header: User-Agent: Go-http/1.1	Annoying — modify tool config	SIEM rule. Useful for detecting specific tooling.
Host Artefact	Registry key: HKCU\Run\WindowsDefender_x64	Annoying — change persistence method	EDR hunt. Indicator of specific malware family.
Tool	Cobalt Strike beacon — watermarked	Hard — tool cost, retraining, new infra	YARA rules targeting tool signatures. High-value detection.

IOC Type	Example	Attacker Cost to Change	How to Use
TTP	WMI for persistence + LSASS dump for creds	Very Hard — requires new attack methodology	SIEM/EDR behavioural detection. Highest durability.

Table 4: IOC types, attacker cost to change, and how to operationalise each

5. OSINT — Open Source Intelligence

Open Source Intelligence (OSINT) is intelligence derived from publicly available sources — the internet, social media, code repositories, leaked databases, technical forums, company registrations and more. The majority of threat intelligence work involves OSINT in some form. It is free, legal and enormously productive when done methodically.

Key OSINT sources and techniques for CTI analysts

Source / Technique	What You Find	Tools
Passive DNS / Domain history	Historical IP resolutions for a domain — even after the attacker moves infrastructure, past associations remain	PassiveTotal, VirusTotal, SecurityTrails, WHOIS
Certificate Transparency logs	TLS certificates issued for domains — attackers registering phishing infrastructure leave cert records	crt.sh, Censys, Shodan
Shodan / Censys / Greynoise	Internet-connected devices, open ports, banner information — map attacker infrastructure	Shodan.io, Censys.io, Greynoise.io
Malware repositories	Known malware samples — analyse, extract C2 configs, identify campaign patterns	MalwareBazaar, VirusTotal, Any.Run, Hybrid Analysis
GitHub / code repositories	Accidentally exposed credentials, threat actor tooling, leaked internal documents	GitHub search, Gitrob, TruffleHog
Social media / forums	Threat actor communications, recruitment posts, CVE exploit announcements — often on Telegram, XSS forums	Manual review, social listening tools, Maltego
Breach / leak databases	Compromised credentials that may indicate targeted organisations or actor infrastructure	HaveIBeenPwned, IntelX, DeHashed (legal access only)
WHOIS / company registrations	Actor infrastructure registration patterns — same registrar, same email, similar naming conventions	DomainTools, WHOIS, Companies House

Table 5: Key OSINT sources and tools for CTI analysts

OSINT operational security (OPSEC) matters.
Querying VirusTotal or Shodan for a threat actor's infrastructure can alert them.
Use API access rather than the web interface. Use a dedicated analyst VM and VPN.

6. Threat Actor Profiling

Threat actor profiling is the process of building a comprehensive picture of an adversary — their identity (as far as can be assessed), motivation, capabilities, infrastructure, preferred victims and likely next actions. A well-built actor profile is the foundation of predictive threat intelligence.

Figure 3: Example threat actor profile card — showing attribution confidence, TTPs and known IOC counts.

Attribution — what it means and what it does not

Attribution is the process of connecting attack activity to a specific threat actor, group or nation-state. It is one of the most discussed — and most misunderstood — aspects of threat intelligence. Perfect attribution is rare. What analysts produce is assessed attribution with a stated confidence level.

- **Technical attribution:** Connecting attacks through shared infrastructure (same IP ranges, hosting providers, domain registrars), shared code (same malware family, reused functions), or shared TTPs. This is what CTI analysts primarily do.
- **Operational attribution:** Connecting attacks through operational patterns — working hours, language artefacts in code, target selection patterns, timing relative to geopolitical events.
- **Strategic attribution:** Connecting a threat actor to a nation-state or organised criminal group based on motivation, target selection and tasking. This typically requires intelligence beyond open sources.
- **Confidence levels:** Never state attribution without a confidence level. 'High confidence', 'moderate confidence' and 'low confidence' are the minimum — many analysts use the Admiralty Scale (1A through 6F) from military intelligence.
- **Attribution is rarely binary:** 'This was China' is almost always an oversimplification. 'We assess with moderate confidence that this activity is consistent with a Chinese state-sponsored threat actor, based on targeting and TTP overlap with APT40' is intelligence.

Actor Category	Motivation	Typical TTPs	UK Relevance
Nation-State (APT)	Espionage, sabotage, geopolitical goals	Sophisticated, patient, custom tooling, long dwell times	GCHQ/NCSC track dozens targeting UK government, defence, CNI
Ransomware Groups	Financial — extortion	Phishing/RDP entry, lateral movement, data theft + encryption	Major threat to UK businesses — LockBit, ALPHV active vs UK

Actor Category	Motivation	Typical TTPs	UK Relevance
Initial Access Brokers	Financial — sell access to others	Specialise in gaining access only — sell to ransomware affiliates	Prolific — UK companies frequently listed on criminal forums
Hacktivists	Political/ideological	Website defacement, DDoS, data leaks	Active — increase during geopolitical events
Insider Threats	Financial, grievance, coercion	Legitimate access abuse, data exfiltration, sabotage	Significant and often underreported — hard to detect with external intel
Cybercriminals	Financial — fraud, BEC, credential theft	Phishing, BEC, banking trojans, credential harvesting	Pervasive — affects every sector

Table 6: Threat actor categories, motivations and UK relevance

7. Dark Web and Underground Monitoring

The dark web — specifically Tor-hosted forums, markets and communication channels — is where significant threat intelligence exists. Ransomware groups announce victims. Initial access brokers list corporate network accesses for sale. Criminal forums discuss new exploits, trade credentials and recruit affiliates. Monitoring this space is a legitimate and important CTI activity when done lawfully.

- **Ransomware leak sites:** Most major ransomware groups operate public Tor-hosted 'leak sites' where they list victims and post stolen data. Monitoring these is legal and provides early warning — often before the victim is even aware of the breach.
- **Criminal forums (XSS, Exploit.in, RAMP):** Russian-language cybercriminal forums where exploits, initial access, stolen data and malware are traded. Monitoring requires caution — purchasing anything is illegal. Reading and monitoring is generally lawful.
- **Telegram channels:** Many threat actors communicate, recruit and share tools on Telegram. Channels are often public. This is a growing source of near-real-time threat intelligence.
- **Paste sites (Pastebin, Raidforums archives):** Stolen credentials and data are frequently posted here, sometimes as proof of compromise before a ransom demand.
- **Legal and ethical boundaries:** Monitoring is lawful. Accessing systems without authorisation, purchasing stolen data, or interacting with criminal services is not. Many organisations use commercial dark web monitoring services (Recorded Future, Flare, DarkOwl) rather than direct access.

8. Sharing Intelligence — MISP, ISACs and TLP

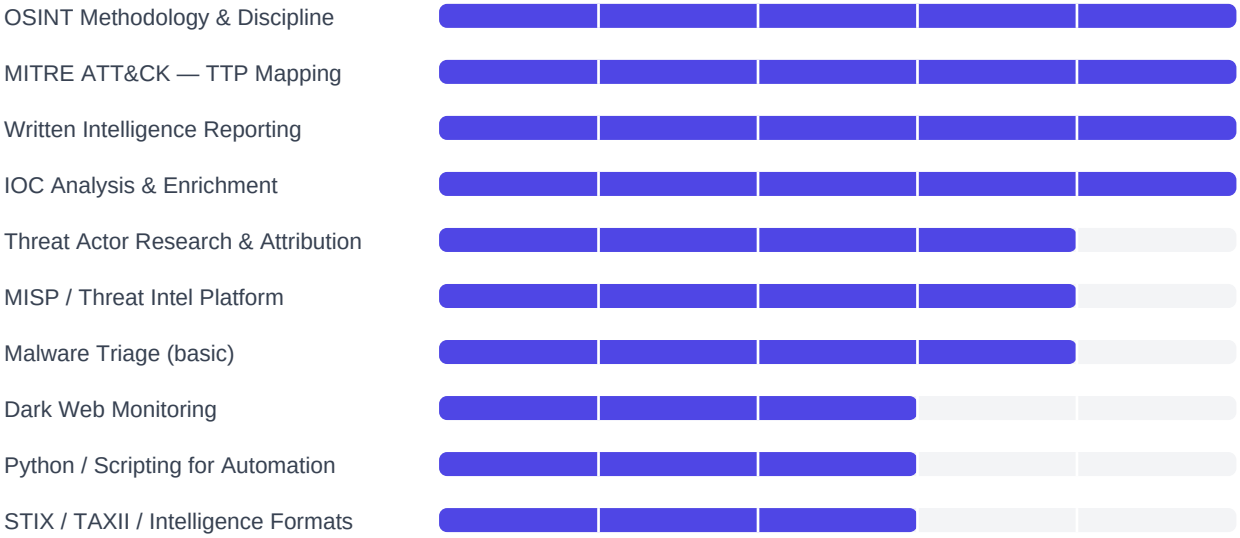
Intelligence is most valuable when shared. A single organisation detecting a new attack technique benefits from sharing it — 50 organisations can then detect the same technique. The threat intelligence community has built structured sharing mechanisms to enable this safely.

Mechanism	What It Is	How Analysts Use It
MISP — Malware Info Sharing Platform	Open-source platform for sharing IOCs and threat intelligence in structured formats (STIX/TAXII)	Host internally or join a community instance. Share IOCs, import feeds from partners, automate SIEM/EDR integration
ISACs — Info Sharing & Analysis Centres	Sector-specific trusted communities (FS-ISAC for finance, H-ISAC for health, etc.) sharing threats affecting that sector	Join your sector's ISAC. Receive vetted threat intelligence. Share indicators from your own environment.
NCSC CiSP — Cyber Security Info Sharing Partnership	UK government threat sharing platform — free to join for UK businesses across all sectors	Join CiSP. Receive NCSC threat briefings. Share incident information with the UK threat intelligence community.
TLP — Traffic Light Protocol	Standard for indicating how widely intelligence can be shared: TLP:RED (recipient only) through TLP:CLEAR (public)	Tag all intelligence you produce and receive. Respect TLP markings — a breach of TLP destroys trust.
STIX/TAXII	Structured Threat Information eXpression / Trusted Automated eXchange — machine-readable formats for sharing	Ingest TAXII feeds into MISP. Export your IOCs in STIX format for automated sharing with partners.

Table 7: Intelligence sharing mechanisms used by CTI analysts

9. Core Skills and Tools

Skills expected at mid-level CTI analyst level:



Tool / Platform	Category	What It Does	Cost
Maltego	Link Analysis	Visualise relationships between domains, IPs, people, organisations. Essential for infrastructure mapping.	Free (Community) / Commercial
MISP	Intel Sharing Platform	Collect, store, share and correlate IOCs and threat intelligence. Industry-standard open-source TIP.	Free (open source)
VirusTotal	IOC Enrichment	Check file hashes, IPs, domains and URLs against 70+ AV engines. See relationships and historical data.	Free tier / Commercial API
Shodan	Infrastructure Recon	Search internet-connected devices. Find attacker infrastructure, exposed services, certificate patterns.	Free tier / Commercial
Recorded Future	Commercial TIP	Enterprise threat intelligence platform — actor profiles, real-time alerts, dark web monitoring.	Commercial
OpenCTI	Intel Platform	Open-source threat intel platform with STIX support, actor profiles and ATT&CK; integration.	Free (open source)
Spiderfoot	OSINT Automation	Automates OSINT collection across 200+ sources for an IP, domain, email or person.	Free / Commercial
theHarvester	OSINT	Email, subdomain and IP enumeration from public sources — useful for brand/infrastructure monitoring.	Free

Tool / Platform	Category	What It Does	Cost
MITRE ATT&CK; Navigator	TTP Mapping	Visualise and annotate the ATT&CK; framework with actor TTPs for comparison and hunting.	Free (web)
Flare / DarkOwl	Dark Web Monitoring	Commercial services that monitor criminal forums, ransomware sites and Telegram for your brand/IOCs.	Commercial

Table 8: Core tools for threat intelligence analysts

10. Career Paths in Threat Intelligence

Threat intelligence draws people from two directions — security operations (SOC analysts who develop a passion for knowing why attacks happen) and non-technical backgrounds like journalism, politics, language or military intelligence (people who bring analytical rigour and geopolitical understanding). Both pathways are valid and produce excellent analysts.

Role	What You Do	Where You Work	UK Salary
Junior CTI Analyst	IOC enrichment, OSINT research, intel report writing support, feed management.	MSSP, financial services, NCSC	£30k–£45k
CTI Analyst	Full intelligence cycle — collection, analysis, reporting across strategic, operational and tactical levels.	Enterprise, financial services, government	£45k–£65k
Threat Researcher	Deep technical research into malware families, threat actor TTPs, new attack techniques.	Cybersecurity vendors, research firms	£55k–£75k
Intelligence Engineer	Build and automate intelligence collection and processing pipelines. MISP admin, STIX/TAXII integration.	Large enterprises, MSSPs	£55k–£75k
Dark Web / Underground Monitor	Monitor criminal forums, ransomware sites, breach listings. Early warning for clients.	Threat intel vendors, consultancies	£45k–£65k
CTI Manager / Lead	Lead a CTI team. Define intelligence requirements. Manage relationships with ISACs and government bodies.	Financial services, large enterprises	£70k–£95k
Strategic Intelligence Advisor	Provide geopolitical and nation-state threat analysis to board and C-suite. Advise on long-term risk.	Government, defence, top-tier banks	£85k–£120k+

Table 9: Career paths in threat intelligence (Reed, 2024; CW Jobs, 2024)

11. The Learning Roadmap

Threat intelligence has a less prescriptive learning path than most cybersecurity disciplines because it draws on such diverse backgrounds. But the practical core — OSINT, MITRE ATT&CK;, IOC analysis, report writing — can be learned systematically.

1. **Learn MITRE ATT&CK deeply**
   Go to attack.mitre.org. Read through every tactic and technique. Understand what each one looks like in practice, what tools are associated with it, which threat groups use it. Use the ATT&CK Navigator to build actor heat maps. 3–4 weeks.

2. **Master OSINT methodology**
   Work through the OSINT Framework (osintframework.com). Practice pivoting — start with a domain and see how far you can go: WHOIS, passive DNS, certificate transparency, Shodan. Document your methodology. SANS FOR578 course outline is free and excellent. 4–6 weeks.

3. **Learn threat actor tracking with Maltego**
   Install Maltego Community Edition (free). Practice building link analysis graphs from public IOCs. Map infrastructure — connect a domain to an IP to a certificate to another domain. This skill directly translates to CTI work. 2–3 weeks.

4. **Practise IOC enrichment**
   Take malware samples from MalwareBazaar. Extract IOCs. Enrich each one in VirusTotal, Shodan, Censys, PassiveTotal. Map the infrastructure. Write up what you find. Do this for 20 samples. Pattern recognition develops fast. Ongoing.

5. **Set up MISP in your lab**
   Deploy MISP (free, Docker) and import public threat intel feeds (CIRCL, abuse.ch). Practice creating events, tagging TTPs with ATT&CK, and exporting STIX. Understanding the platform from both user and admin perspectives is valuable. 2–3 weeks.

6. **Write intelligence reports**
   Practice writing all four types — technical IOC report, tactical TTP brief, operational campaign summary, strategic threat assessment. Get feedback. The ability to communicate intelligence clearly in writing is the rarest and most valued CTI skill. Ongoing.

7. **Engage with the CTI community**
   Follow CTI researchers on LinkedIn and X/Twitter. Read threat intelligence blogs (Mandiant, CrowdStrike, ESET, Sekoia). Engage with CTI League, OpenCTI community and FIRST.org. The community is open and collegial.

8. **Get certified and apply**
   CTIA (EC-Council) or CPTIA are recognised CTI certifications. FOR578 (SANS) is the gold standard but expensive. Start with OSINT-focused roles in threat intelligence teams, MSSPs or financial sector CTI functions.

CTI is uniquely accessible to people without deep technical backgrounds.
Analysts from journalism, military intelligence, languages and politics bring analytical rigour and geopolitical knowledge that pure technical analysts often lack.

12. Certifications That Matter

Threat intelligence certifications are fewer and less standardised than in other cybersecurity disciplines. Employers often weight portfolio evidence — published research, blog posts, OSINT challenge completions — as highly as formal certifications. That said, the following are recognised and respected:

Certification	Level	Provider	Focus	Why It Matters
CompTIA Security+	Beginner	CompTIA	Broad security foundations	Baseline for many roles. Good starting point if coming from non-technical background.
CTIA — Certified Threat Intelligence Analyst	Mid	EC-Council	Full CTI lifecycle — collection, analysis, OSINT, reporting, sharing	Most widely recognised CTI-specific certification. Covers the full intelligence cycle.
FOR578 — Cyber Threat Intelligence	Mid–Senior	GIAC / SANS	Advanced CTI — actor profiling, campaign analysis, intelligence sharing, MISP	The gold standard for technical CTI professionals. Expensive but highly respected globally.
GCTI — GIAC Cyber Threat Intelligence	Mid–Senior	GIAC	Certification associated with FOR578	The exam credential for FOR578 course content. Respected across all sectors.
BTL1 — Blue Team Level 1	Beginner–Mid	Blue Team Labs Online	SOC + threat intelligence + OSINT — practical foundation	Good for those entering CTI from SOC background. Practical exam.
OSCP / CEH	Mid	OffSec / EC-Council	Offensive techniques — valuable context for understanding attacker behaviour	Understanding how attacks work makes you a better threat analyst.

Table 10: Certifications for threat intelligence analysts in order of progression

13. Case Study — From a Single IOC to a Full Actor Profile

> This is a fictional case study illustrating real CTI analyst methodology.
> The techniques described are genuine OSINT and threat intelligence methods.

Starting point — one suspicious domain

A SOC analyst at **Meridian Bank** escalates an alert to the CTI team. A workstation has made DNS queries to **payroll-update.meridian-hr-portal.com** — a domain that looks like it could be internal but is not registered by the bank. The CTI analyst, Aisha, begins with a single question: *Who owns this domain and what is it connected to?*

Phase 1 — Domain and infrastructure analysis

OSINT pivot: domain → IP → certificate → cluster

WHOIS lookup: domain registered 14 days ago via Namecheap, privacy-protected. Registration email: admin@securemail-relay.com — noted for later.

Passive DNS (SecurityTrails): domain resolved to 185.220.101.93 for 11 days, then moved to 185.220.101.104 two days ago. Both IPs appear on AbuseIPDB with 'phishing' and 'C2' tags.

Certificate Transparency (crt.sh): the same SSL certificate was also issued for accounts-meridian-update.com and

Phase 2 — Infrastructure clustering and actor identification

Pivoting to find the full infrastructure cluster

Shodan search for the hosting ASN (AS44477 — Stark Industries): 14 servers with similar open ports (443, 8443, 50050). Port 50050 is the default Cobalt Strike Team Server port.

Cross-referencing in MISP against shared community IOCs: 6 of the 14 IPs match indicators previously shared by FS-ISAC (Financial Services ISAC) as part of a campaign attributed with moderate confidence to a group tracked as 'SilverLynx' — known for targeting UK financial institutions.

Phase 3 — TTP mapping and intelligence production

Aisha maps the observed activity to MITRE ATT&CK;: T1566.002 (Spearphishing Link), T1071.001 (Web Protocols for C2), T1583.001 (Domain acquisition). She pulls the existing SilverLynx actor profile from OpenCTI and adds the new infrastructure. She then produces three intelligence outputs:

- **Technical report (TLP:AMBER):** Full IOC list — 14 IPs, 3 domains, SSL cert fingerprint, Cobalt Strike beacon config (extracted from a sandbox run). Shared via MISP with FS-ISAC partners.
- **Operational briefing (TLP:GREEN):** Two-page summary for the SOC and IR team — what the actor does, how they gained initial access here, what to hunt for across the estate right now.
- **Strategic note (TLP:WHITE):** One-paragraph note to the CISO — UK financial institutions are being targeted by a financially motivated group using fake HR portal phishing. Recommend all-staff phishing awareness reminder.

Total time from one suspicious domain to a full intelligence package: 4 hours.
Output: 14 IPs blocked, 3 domains sinkholed, SOC hunting hypothesis created,
CISO briefed, 47 FS-ISAC partner organisations automatically received the IOCs via MISP.

14. Breaking In — Getting Your First Role

CTI is one of the most diverse entry points in cybersecurity. Technical backgrounds are valued but not always required. Analytical thinking, curiosity and the ability to write clearly matter enormously. Many excellent analysts came from journalism, military intelligence, academia or political science.

Build visible evidence of CTI capability

- **OSINT challenge write-ups:** TraceLabs, OSINT CTF competitions, Bellingcat challenges. Document your methodology. These demonstrate structured analytical thinking better than any certification
- **Threat actor research blog:** Pick a publicly documented threat group (APT28, Lazarus Group). Write a detailed profile using only open sources — MITRE ATT&CK;, vendor reports, crt.sh, VirusTotal. Publish it.
- **MISP instance:** Deploy MISP in your lab, import public feeds, create a few well-documented threat events. Screenshot your work. Shows platform familiarity employers value.
- **IOC analysis write-ups:** Take published IOCs from a threat report. Pivot on each one using free tools. Document what you found. This is the core daily activity of a CTI analyst.
- **Contribute to open-source intelligence:** Submit IOCs to MalwareBazaar, contribute to OpenCTI community feeds, or engage with the CTI community on LinkedIn. Visibility matters in this field.

Where to Look	Notes
CyberSecurityJobs.com	Search 'threat intelligence analyst', 'CTI analyst', 'OSINT analyst'
LinkedIn	CTI roles post heavily here. Follow and engage with threat researchers at CrowdStrike, Mandiant, ESET, Recorded Future
Financial services CTI teams	Banks and insurers run dedicated CTI teams — FS-ISAC membership means they are active consumers and producers
NCSC / GCHQ / government	NCSC runs a threat intelligence function and hires analysts. GCHQ GCHQ Intelligence Analyst roles are highly competitive but well-regarded
Threat intelligence vendors	Recorded Future, Flashpoint, Mandiant/Google, CrowdStrike, Sekoia, Intel 471 all hire analysts globally
Managed Security Service Providers	MSSPs run CTI functions that feed their SOC teams — often good entry-level CTI roles

Table 11: Where to find threat intelligence roles

Interview questions to prepare for

- What is the difference between strategic, operational, tactical and technical threat intelligence? Give an example of each.
- Explain the Pyramid of Pain. Why is TTP-based intelligence more valuable than IOC-based intelligence?
- You receive a suspicious domain from the SOC. Walk me through your OSINT investigation process.
- What is the MITRE ATT&CK; framework and how would you use it in a threat actor profile?
- What is the difference between correlation and attribution? Why does this distinction matter?
- An IOC you shared last week turns out to be a false positive. What went wrong and what do you do?

- What is TLP and why is it important for intelligence sharing?
- How would you write a strategic threat briefing for a non-technical board of directors?

> **The best CTI interview answer:**
> "Here is a threat actor profile I researched using only open sources."
> Published analytical work — even a blog post — is the strongest signal of CTI capability.

15. References

1. Bianco, D. (2013) *The Pyramid of Pain.* Available at: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html [Accessed: 12 April 2026].
2. CIRCL (2024) *MISP — Open Source Threat Intelligence Platform.* Available at: https://www.misp-project.org [Accessed: 12 April 2026].
3. CrowdStrike (2024) *Global Threat Report 2024.* Available at: https://www.crowdstrike.com/resources/reports/global-threat-report/ [Accessed: 12 April 2026].
4. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 12 April 2026].
5. EC-Council (2024) *CTIA — Certified Threat Intelligence Analyst.* Available at: https://www.eccouncil.org/programs/certified-threat-intelligence-analyst-ctia/ [Accessed: 13 April 2026].
6. FIRST.org (2024) *Traffic Light Protocol (TLP) Standard.* Available at: https://www.first.org/tlp/ [Accessed: 13 April 2026].
7. GIAC / SANS (2024) *FOR578: Cyber Threat Intelligence.* Available at: https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/ [Accessed: 13 April 2026].
8. Mandiant / Google (2024) *M-Trends 2024 Threat Intelligence Report.* Available at: https://www.mandiant.com/resources/m-trends [Accessed: 14 April 2026].
9. MITRE Corporation (2024) *ATT&CK; — Adversarial Tactics, Techniques and Common Knowledge.* Available at: https://attack.mitre.org [Accessed: 14 April 2026].
10. NCSC (2024) *CiSP — Cyber Security Information Sharing Partnership.* Available at: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp [Accessed: 14 April 2026].
11. OASIS (2021) *STIX Version 2.1 Specification.* Available at: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html [Accessed: 14 April 2026].
12. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 14 April 2026].
13. Recorded Future (2024) *Annual Threat Landscape Report 2024.* Available at: https://www.recordedfuture.com/research/threat-landscape-report [Accessed: 15 April 2026].

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 10 of 12.