THE CTI RESEARCH GUIDE

Curated Intelligence

About

This guide was created by Will Thomas
It was reviewed and had contributions from members of Curated Intelligence
Published in November 2024

Contents

Acknowledgements

Thanks to Curated Intelligence members Steve Ragan, Freddy Murstad, Parthiban Rajendran, Øystein Brekke-Sanderud, Xena Olsen, Chris Campbell, and Grace Chi for reviewing this research guide and providing their insights.

Introduction

The cyber threat intelligence (CTI) lifecycle is a well-documented methodology containing multiple consecutive phases that ultimately convert raw data into finished intelligence (FINTEL).

The output then goes back to key stakeholders (such as a CISO and other Infosec Department Team Leaders), who can use it to continuously support their decision-making process around resource prioritisation.

This CTI Research Guide aims to help practitioners learn more about how to effectively perform the collection, processing, analysis, and production stages of the CTI lifecycle.

The Collection Problem

What is the Collection Problem? This is where CTI teams fall into the issue of being unable to do collection consistently and suitably for their organisation or customers. Many CTI teams end up missing things, not seeing the bigger picture. They forget to stop and think about *why* they are collecting what they are collecting, when they should be considering “who are we collecting this for?” and “what is the value of collecting this?” These issues are compounded by other issues around collection, such source biases, overreliance on single sources, or simply spreading themselves too thin by trying to collect everything – making them unable to analyse anything.

A Potential Solution: The CTI Research Guide

Not every organisation has access to valuable incident response (IR) data or telemetry from across the customer base of a managed security service provider (MSSP). Only certain commercial IR or MSSP firms truly have this information, such as CrowdStrike, Microsoft, SentinelOne, ESET, Mandiant, Secureworks, Sophos, Huntress, Symantec, and Trend Micro, among others.

Many analysts and researchers outside of this group of vendors – such as in-house cyber defenders, non-government entities, and academics – rely heavily on open source intelligence (OSINT), with the potential for some paid premium FINTEL reports as well as trust groups and intel-sharing partnerships, like information sharing and analysis centers (ISACs).

The CTI Research Guide aims to promote a repeatable method to keep track of all your sources, categorise them, extract meaningful information, form meaningful takeaways from your research, and document your findings. It is also useful from a perspective of knowing and tracking what you have looked at and already digested. By refocusing on what is important for your organisation, you will notice improvements on output and stakeholder satisfaction.

Important: The CTI Research Guide is largely intended for established CTI teams who have already completed the planning stage of the intelligence lifecycle (i.e., they should know what their stakeholders want and are looking for already).

Resources are available online and linked in the **References** section at the end of this report to guide you through the planning stage. If you have not yet done so, we recommend reading through these resources to complete planning, then return to this guide to start collection.

What is Intelligence Collection?

Intelligence collection from a CTI perspective must begin with planning, directing all collection efforts around established stakeholder requirements. It is a fool's errand to collect everything. It is not possible nor a worthwhile investment of resources, no matter how big your team is.

CTI collection requires inputs from the individuals you are expected to provide intelligence to. This requires setting clear boundaries, with examples of what your stakeholders are not interested in. These boundaries set collection expectations and realistic deliverables.

Overall, CTI teams should be researching topics they have been asked about, as opposed to deciding to research whatever they prefer. It is essential to understand the priorities of your stakeholders.

Planning and interviewing stakeholders for their requirements is not the focus of this CTI Research guide. However, it is a necessary step that all CTI teams need to master to be successful.

CTI analysts who plan to perform their own collection will need to prepare for a combination of automated collection and manual extraction. With this process, you will be reviewing what you've collected and extracting information. In theory, this would ideally take one hour per day, up to five days per week.

Getting Started

Getting started with CTI research is a multi-step process. First, you need to decide, based on stakeholder requirements, what to research, then build up your knowledge base and gather sources. Once these steps are established, you can start collection. Following collection, you can update the knowledge base and sources, then continue to do so as you uncover more.

See Figure 1 below for a high-level overview of these steps. The coloured arrows in this flow diagram signify how analysts will be continuously updating their knowledge base and sources after they have started collection.

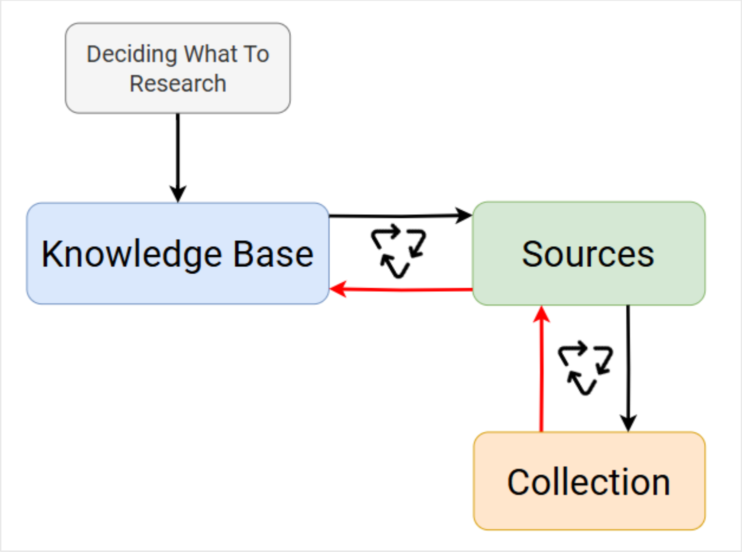


Figure 1: Getting started with CTI research.

Establishing a Knowledge Base

1. Deciding What to Research	• A type of adversary or adversaries • A certain country or countries • A certain industry or industries
2. Establishing a Knowledge Base for State-Sponsored Threats	• List of all known adversary groups • List of government agencies • List of government contractors • List of target sectors and countries • List of notable incidents • List of indictments or arrests
3. Establishing a Knowledge Base for Cybercriminal Threats	• List of priority adversaries and groups • List of types of adversaries of interest threat (e.g., ransomware operator, affiliate, initial access broker, data broker, malware distributor, malware developer, etc) • List of communities of interest • List of criminal activities • List of notable incidents • List of indictments or arrests
4. Establishing a Knowledge Base for Hacktivist Threats	• List of priority adversaries and groups • List of types of adversaries of interest • List of communities of interest • List of political motivations • List of notable incidents • List of indictments or arrests

Building Up Your Sources of Intelligence to Begin Collecting

Type	**Description**
News Sites	• Infosec • Mainstream • Topical experts (e.g., gaming, finance, insider blogs, groups, newsletters)
Vendor Blogs	• CTI • MDR • DFIR
Public Sector Alerts	• Government • Law Enforcement
Non-Government Organisations (NGOs) Blogs	• Human Rights Defenders • Think Tanks
Social Media	• English-language: Twitter, Instagram, TikTok, Facebook, etc • Russian-language: Telegram, VK, OK, etc • Chinese-language: WeChat (Weixin), Weibo, RenRen, etc
Forums	• Reddit • Discord
HUMINT & RUMINT	• Take these with a pinch of salt

Once you build up your sources, you can begin collecting using a variety of methods and tools. These include commercial platforms that ingest RSS feeds, scrape forums, and store messages from various platforms. The most used vendors across the CTI industry include Recorded Future, Intel471, Flashpoint, Anomali, and Feedly, among others. There are free ways of doing this yourself, but you will be starting from scratch with no prior collection.

One solution that is accessible to almost all users is leveraging a free Discord account to create a free server that you can then turn into a collection platform. Here is a guide about how to create a Discord CTI server that is fairly straightforward for anyone to follow and a learning experience to understand how these commercial CTI platforms work.

Download the Collection Worksheet

A collection spreadsheet is available via the Curated Intelligence GitHub account that contains several tabs related to each section of this guide.

Download the XLSX file available here: https://github.com/curated-intel/The-CTI-Research-Guide/blob/main/CTI_Research_Guide.xlsx

Tracking Adversary Activity

Once you progress from the initial phase of CTI research, you can shift into tracking adversary activity. This involves using the information collected to begin researching the adversaries you are interested in and turning it into intelligence products, such as reports or presentations. Remember: it is important to only track adversaries identified as key or potential threats to your organisation. Attempting to collect everything will lead to information overload; it is impossible and futile to try to collect and analyse everything.

See Figure 2 below for a high-level overview of this process. This is not a new standard or framework – merely a workflow diagram of how the CTI research process takes place.

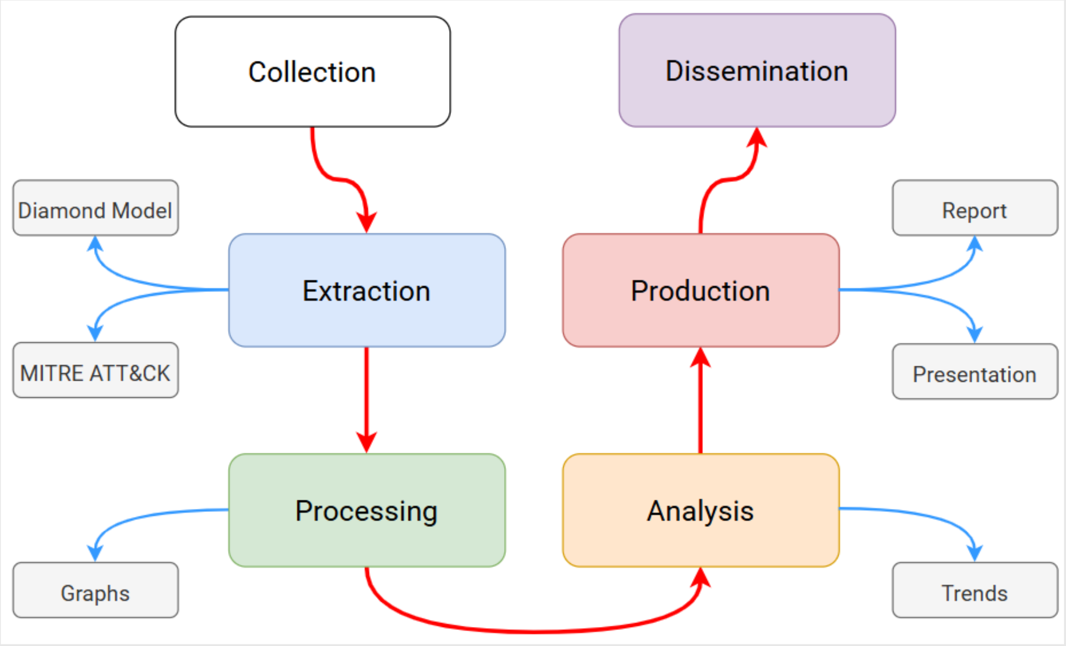


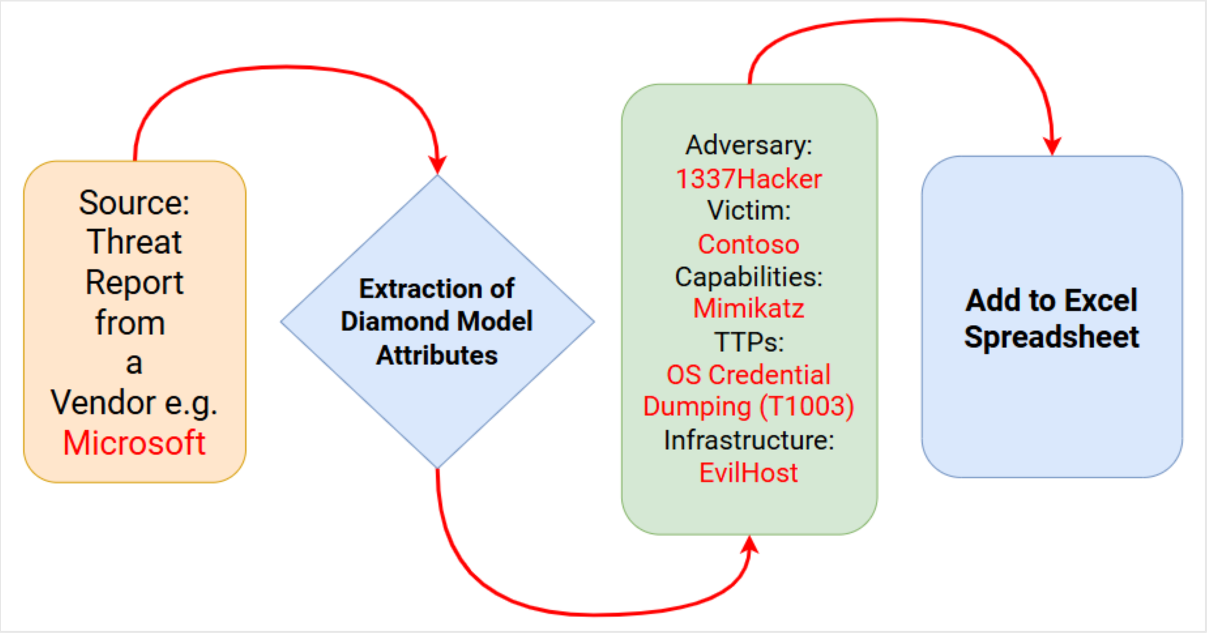
Figure 2: Beginning the CTI Research Lifecycle.

With a knowledge base established and activity reports collected, you can start to make sense of it. One popular approach is to extract certain attributes from the report based on the Diamond Model of Intrusion Analysis: Adversary, Victim, Capabilities, and Infrastructure. It is also possible to extract MITRE ATT&CK tactics, techniques, and procedures (TTPs).

Extracting attributes and mapping them to the Diamond Model and/or MITRE ATT&CK framework makes the intelligence collected more actionable for CTI stakeholders. By using the Diamond Model, you can articulate the significance of any intrusion campaign in a standardised way. The same goes for the MITRE ATT&CK framework – it allows you to articulate the capabilities leveraged during an intrusion in a standardised way. This enables defenders to check their controls and make decisions based on information they are already used to consuming in other ways, such as endpoint detection and response (EDR) software, which can map detections to the MITRE ATT&CK framework.

After you have collected many activity reports and extracted key information, you can now build graphs and charts in Microsoft Excel based on your findings. Using these charts, you can then start to analyse the data and look for potential trends.

See Figure 3 below for an example illustrating how the extraction process works.



Source: Threat Report from a Vendor e.g. Microsoft

Extraction of Diamond Model Attributes

Adversary: 1337Hacker
Victim: Contoso
Capabilities: Mimikatz
TTPs: OS Credential Dumping (T1003)
Infrastructure: EvilHost

Add to Excel Spreadsheet

Figure 3: The CTI Research extraction process involving the Diamond Model and MITRE ATT&CK.

What To Look for When Reading Threat Reports on Adversary Activities

1. Extract key information	• Use the Diamond Model or ATT&CK • Decide which primary threat actor naming scheme you will use • Establish a standardized system for industry verticals
2. Citations	• Cite every source • Cite original source(s) • Find the cause of the news • Find vendor blogs, a forum post, a Tweet, a Telegram channel message, or files leaked to a Tor site, etc.
3. Start analysing data collected	• Number of groups active per quarter • Countries targeted per quarter • Sectors targeted per quarter
4. Highlight significant findings	• Breaches: Notable victims (newsworthy or those that impacted your organisation the most) • Capabilities: Notable or new techniques leveraged during intrusions • Vulnerabilities: Zero-days, use of public proof-of-concepts (PoCs), vulnerability types (CWEs) • Anomalies: Something that was totally new or unexpected could be worth tracking to identify a new trend
5. Results of efforts	• You are now providing novel insights • Identify, to the best of your ability: ○ Which sectors or countries each adversary prefers to target ○ What tools or capabilities each adversary prefers to use ○ What infrastructure each adversary uses
6. Production	• Create a report of your findings • Alternatively, create a presentation
7. Dissemination & feedback	• Share with stakeholders • Ask them for feedback

Tracking Industry-Specific Activity

While CTI analysts are often concerned about specific adversaries, they need to pay attention to the *types of threats* that specific industries or sectors face. If you are on the security team of an organisation such as a bank or telecommunications company, it is best practice to look at the types of cyber threats targeting neighbouring organisations in the same industry.

To research threats targeting neighbouring organisations in the same industry as you, start by monitoring for activity reports that contain industry-specific keywords. Once gathered, you can investigate, analyse, and process industry-specific threat activity.

See Figure 4 below for a high-level view of industry-specific threat tracking.

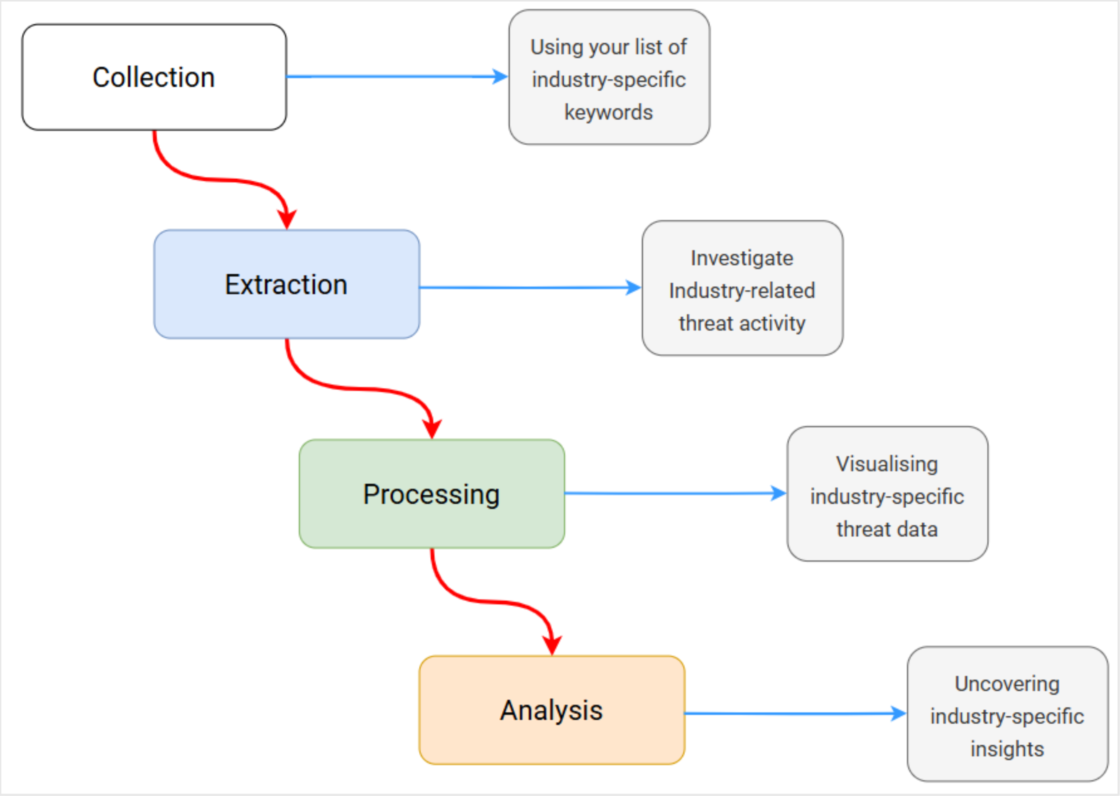

Collection
Using your list of industry-specific keywords
Extraction
Investigate Industry-related threat activity
Processing
Visualising industry-specific threat data
Analysis
Uncovering industry-specific insights

Figure 4: Process for tracking industry-specific cyber threats.

Looking for Industry-specific Threats

1. Build your knowledge base	• Gather Industry Keywords, Terms, and Acronyms • Build a keywords list
2. Begin collection	• Monitor sources for Incidents and Events • Note dates they took place • Write short titles • Split them up by week, month, or quarter
3. Processing and analysis	• Take the data from each source • Note event type(s) • Describe the event's key data (Who, What, Where, When, Why) • Add to a spreadsheet or notes • Look for industry-specific trends • As relevant, refer to the table above on tracking adversary activities
4. Citations	• Cite every source • Cite original source(s) • Find the cause of the news • Find vendor blogs, a forum post, a Tweet, a Telegram channel message, or files leaked to a Tor site, etc.

Tracking Geo-Specific Activity

CTI researchers may be tasked with tracking the threat landscape surrounding certain geographic regions to keep stakeholders informed of relevant cyber threat activity and the implications following globally significant incidents. The process for tracking geo-specific activity is similar, with some significant differences. It should be noted that infosec media sources and cybersecurity vendor blogs, among other sources mentioned above, may not cover major regional developments or geopolitical events as they unfold. However, cybersecurity and geopolitics will forever be intertwined with one another.

Therefore, for CTI researchers tasked with tracking geo-specific activities, you will have to exit your infosec cave and venture out into other sources of information for collection. This could include mainstream news media sources (online, TV, or both) that cover regional developments and geopolitical events.

Two examples of globally significant events with major cyber threat activity include 1) the Russia-Ukraine War that began in February 2022, and 2) the Israel-Hamas War that started in October 2023. In both the Russia-Ukraine and Israel-Gaza theatres of war, destructive cyberattacks have taken place against critical infrastructure organisations. Monitoring that activity and its implications for other emerging conflicts and regions of tension is of importance for many CTI researchers and their stakeholders.

See Figure 5 below for a high-level flow diagram of performing geo-specific threat research.

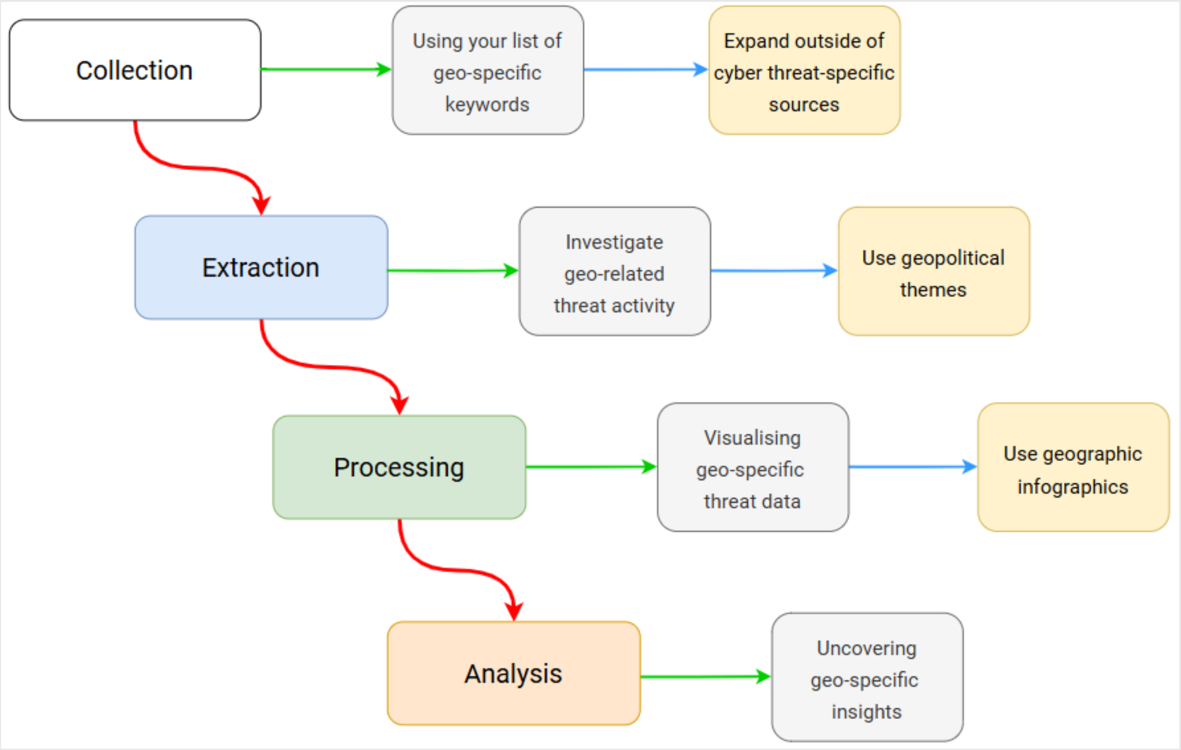

Collection
Using your list of geo-specific keywords
Expand outside of cyber threat-specific sources
Extraction
Investigate geo-related threat activity
Use geopolitical themes
Processing
Visualising geo-specific threat data
Use geographic infographics
Analysis
Uncovering geo-specific insights

Figure 5: Process for tracking geo-specific threat activity.

Looking for Geo-specific Threats

1. Build your knowledge base	• Start with the country/countries you are focused on (like national CERT does) • Think about its alliances (militarily, economically, historically) • Think about its neighbours on its borders and region • Think about its opposition • Think about its major industries (e.g., Taiwan is known for semi-conductors (TSMC), Belgium is known as the political capital as it has the European Union Headquarters and the North Atlantic Treaty Organisation (NATO) headquarters) • Consider brainstorming with colleagues to uncover additional research points, such as key targets (organisations or industries) in escalation scenarios
2. Begin tracking	• Monitor sources for Incidents and Events • Note date(s) they took place • Write short titles • Split them up by week, month, or quarter
3. Extraction	• Take the data from each source • Note event type(s) • Describe the event's key data (Who, What, Where, When, Why) • Add to a spreadsheet or notes • As relevant, refer to the table above on tracking adversary activities
4. Citations	• Cite every source • Cite original source(s) • Find the cause of the news • Find vendor blogs, a forum post, a Tweet, a Telegram channel message, or files leaked to a Tor site, etc.

Additional Types of Collection

Alongside OSINT activity reports, CTI researchers may also have access to many other sources of information.

The more sources of information a CTI researcher can leverage, the more collection and extraction activities they can perform to provide in-depth analysis around a certain topic. There are a vast variety of possible sources out there (see Figure 6) and whether you target them for collection will depend on a multitude of factors, such as your organisation's requirements, your team's resources, and the telemetry available to you.

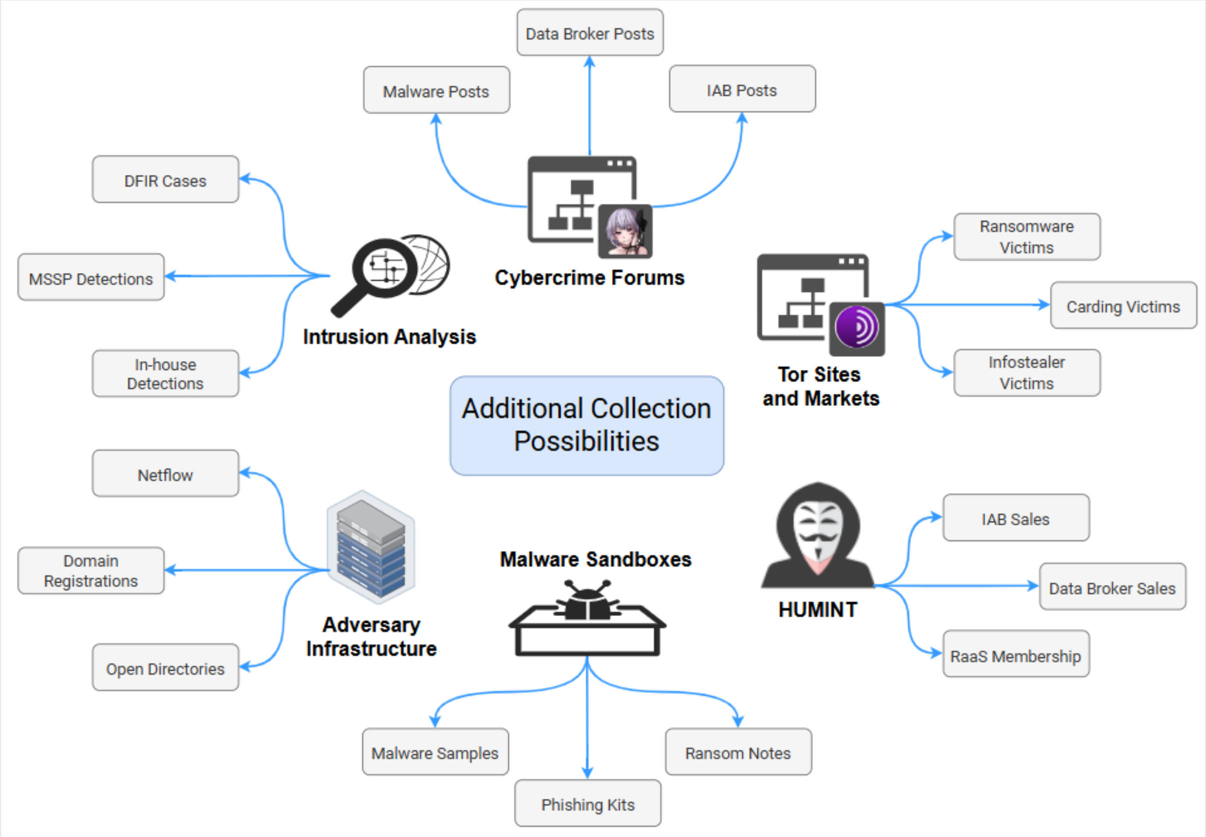


Figure 6: Additional collection possibilities for CTI researchers to discover.

Source	Types
Cybercrime Forums	• Initial Access Broker posts • Data Broker posts • Malware-as-a-Service posts
Darknet Tor Sites	• Ransomware leak sites • eCrime markets (Infostealers Logs)
Infrastructure Analysis	• Netflow C2 to targets • Typosquatting domains • Payload staging severs • Web services • C2 communications servers
Malware Sandboxes	• Submitter's metadata • Malware configuration
Intrusion Analysis	• Diamond Model & Kill Chain Analysis • DFIR cases • MSSP detections • In-house detections • Platform abuse

Processing, Analysis, and Production

Following the process outlined above, you will have gathered all this information over an allotted period. This information can now be turned into a report or briefing presentation.

How often you generate these reports is up to your stakeholder's requirements. Typical reporting cadence may be monthly, quarterly, twice a year, or annually. The frequency of reporting also depends on the CTI team's capacity and resources to write such reports. Smaller teams, without dedicated regional specialists, may only be able to provide annual landscape reports, as an example.

Report Writing

Shared in the table on the following page are the names of sections in a report and corresponding contents. These can be used as is, excluded, or changed around in order – it is up to the author, so long as it still makes sense and flows well.

These sections follow standard CTI reporting requirements, such as explaining the "What?" and the "So What?" of your research. It is vital to include an *Executive Summary* to help readers short on time and underscore the importance of the research by tying it back to your organisation's needs in the *Potential Impact* section.

The *Geopolitical Update* section is designed to provide a useful overview of recent activities related to the country that is the target of your research, whether is it one of the "Big 4" hostile states (China, Russia, North Korea, and Iran) known to Five Eyes countries or some other state your organisation is interested in.

Section	Contents
Title	• Cadence of report (Monthly, Quarterly or Annually) • Example: “Q1 2025 Country_XYZ APT Activity report”
Executive Summary	• What you did • Why you did it • Previous work you have done
Potential Impact to [Your Organisation]	• Impact to tech stack • Impact to brand • Operations disruption • Impact to customers • Impact to suppliers
APT Activity Highlights	• Most active groups • Appendix of sources • Number of Campaigns per APT Group (e.g., bar graph) • Number of Campaigns per Victim Sector (e.g., pie chart) • Number of Campaigns per Victim Country (e.g., map graph)
Latest Tactics, Techniques, and Procedures	• Consider mapping these to the MITRE ATT&CK framework or Cyber Kill Chain stages • Highlight which TTPs were novel or becoming increasingly popular, worth investigating further for follow-up actions • You may also split TTPs into three sections from the unified cyber kill chain, e.g. 1) Initial Access (IN), 2) Post-Compromise Activities (THROUGH), 3) Actions on Objectives (OUT)
Geopolitical Update	• Interdiction on Country_XYZ • Cyberattacks on Country_XYZ • Interference by Country_XYZ • Country_XYZ foreign relations updates • Country_XYZ military operations updates
[Your Team]’s Actions	• Describe any threat hunting that was done • Share any related vulnerability escalations • Share any related RFIs, reports, or briefings
Recommended Best Practices	Examples of recommendations may include: • Tabletop exercises (TTXs) • Adversary emulation • Threat hunting • Detection engineering • Risk analysis • Asset inventory review
Appendix	• Cited in APT activity highlights • Taken from your collection worksheet • Table headings: Publish Date, Adversary, Source

Production Considerations

There are several key considerations when writing these reports:

- **Traffic Light Protocol (TLP):** When sharing findings via a report, it is highly recommended and a cybersecurity industry standard to use the TLP system to classify information and indicate boundaries for recipients. You will need to consider setting an overall TLP level (e.g., TLP:RED, TLP:GREEN, etc.) for the report to designate the sensitivity of information and how it may be subsequently used by recipients.

- **Know Your Audience:** When writing any CTI report, it is important to keep in mind who your intended audience is and what level of intelligence consumer they are – strategic, operational, or tactical. Explain *why* the information is important to your audience so they can make judgements to act on it. Some CTI teams may provide a more general 'Recommended Best Practices' section in reports that suggest examples of defensive strategies and actions that can be taken based on the provided intelligence.

- **Cite Your Sources:** It cannot be stressed enough how important it is to cite sources and references in CTI reports. It is vital to know where the information and evidence you are basing your analysis on is from, and to consider source analysis using the admiralty system to enhance the reliability or your intelligence.

- **Analytic Standards:** The US Office of the Director of National Intelligence (ODNI) released in a resource in 2015 called Intelligence Directive 203 (ID203), which aimed to standardise a way of properly expressing and explaining uncertainties associated with major analytic judgments. This assigns an actual percentage of probability to saying something as "likely" in a report. If analysts and stakeholders adhere to these standards, this should reduce confusion, improve consistency, and increase confidence.

Creating Graphs to Process the Data

To create the recommended graphs for APT Activity Highlights section, you can use the data gathered in the *Collection Worksheet*.

1. For the "*Number of Campaigns per APT Group Bar Graph*", gather all the data from the Adversary Column in the Adversary Reports Tab in the Collection Worksheet.

2. For the *"Number of Campaigns per Victim Sector Pie Chart"*, gather all the data from the Victim Sector Column in the Adversary Reports Tab in the Collection Worksheet.

3. For the *"Number of Campaigns per Victim Country Map Graph"*, gather all the data from the Victim Country Column in the Adversary Reports Tab in the Collection Worksheet.

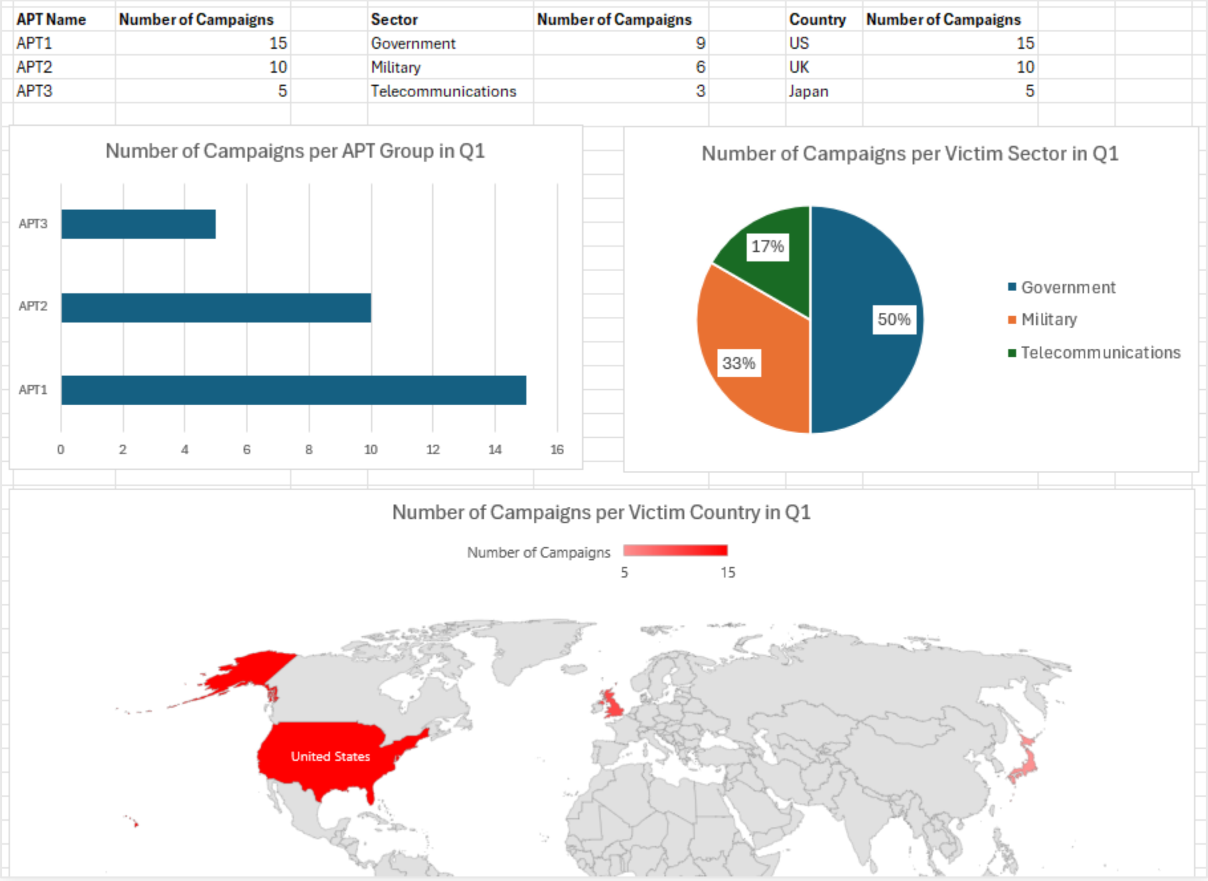
Once you have gathered all the data, you can then perform the following steps to process the data for each of the graph types above:

1. Extract the Criteria: Copy and Paste all the cells into another tab or app like Notepad++ and perform an operation to remove all duplicate lines (edit > line operations > remove duplicate lines). Make sure you keep a copy of the original list of data collected containing the duplicates (this will be our range).

2. Once you have your criteria and range, you can use an Excel Formula called **COUNTIF** to count how many times the contents of one cell appears in a list. If you type **=COUNTIF** then you will find it is followed **(range, criteria)** which you will select in the worksheet. You need to type this for each criteria cell to calculate how many times it appears in the range.

3. Once you have performed the **COUNTIF** stage you can then use data sorting to order it into a table to show the Largest to Smallest.
4. To create a graph or chart, highlight the table of data and head to the **Insert** Tab in Excel and then select the **Bar Graph** for the *"Number of Campaigns per APT Group"* table and the **Pie Chart** for the *"Number of Campaigns per Victim Sector"* table.
5. For the **Map**, you will need to use the offline version of Excel, but it is the same method again. Highlight the *"Number of Campaigns per Victim Country"* and head to the **Insert** Tab and select **Maps**.

If all above steps are followed, you should have a result similar to the graphs shown in Figure 7 below. Under the *view* options in Excel, you can uncheck 'Gridlines' for a cleaner look.



APT Name	Number of Campaigns
APT1	15
APT2	10
APT3	5

Sector	Number of Campaigns
Government	9
Military	6
Telecommunications	3

Country	Number of Campaigns
US	15
UK	10
Japan	5

Number of Campaigns per APT Group in Q1
APT3
APT2
APT1
0
2
4
6
8
10
12
14
16
Number of Campaigns per Victim Sector in Q1
17%
50%
33%
■ Government
■ Military
■ Telecommunications
Number of Campaigns per Victim Country in Q1
Number of Campaigns
5
15
United States

Figure 7: Tables and Graphs recommended for creation to track adversary activities.

CTI Research Justification

There are many available resources out there discussing the importance of CTI research. The key reasons highlighted in this CTI Research Guide are as follows:

- **Stakeholder Situational Awareness:** Findings from the research will highlight key issues and provide insights to support informed decision making.
- **Resource Prioritisation:** Stakeholders can make investments and allocate resources based on the insights provided through research.
- **Detection Engineering and Threat Hunting:** Enterprise security operations teams can decide what threats to prioritise writing detection rules for or threat hunt for based on your research insights.
- **Adversary Emulation:** Enterprise security operations teams can decide what threats to prioritise for testing the detection and response capabilities when directly leveraged against their organisation's defences through this research.
- **Risk Management:** Enterprise security operations teams can identify and prioritise risks uncovered through researching the types of systems and processes that adversaries are targeting and the capabilities they have to achieve their goals.

References

1. Curated Intelligence – CTI Fundamentals
   https://github.com/curated-intel/CTI-fundamentals
2. Diamond Model of Intrusion Analysis
   https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
3. MITRE ATT&CK framework
   https://attack.mitre.org
4. The Recorded Future Intelligence Handbook
   https://go.recordedfuture.com/book
5. The Intel471 Cybercrime Underground Handbook
   https://intel471.com/resources/cyber-underground-handbook
6. The Traffic Light Protocol
   https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage
7. Types of Threat Intelligence
   https://cwsisecurity.com/types-of-threat-intelligence/
8. The Admiralty System
   https://www.sans.org/blog/enhance-your-cyber-threat-intelligence-with-the-admiralty-system/
9. Intelligence Directive 203
   https://www.dni.gov/files/documents/ICD/ICD-203_TA_Analytic_Standards_21_Dec_2022.pdf