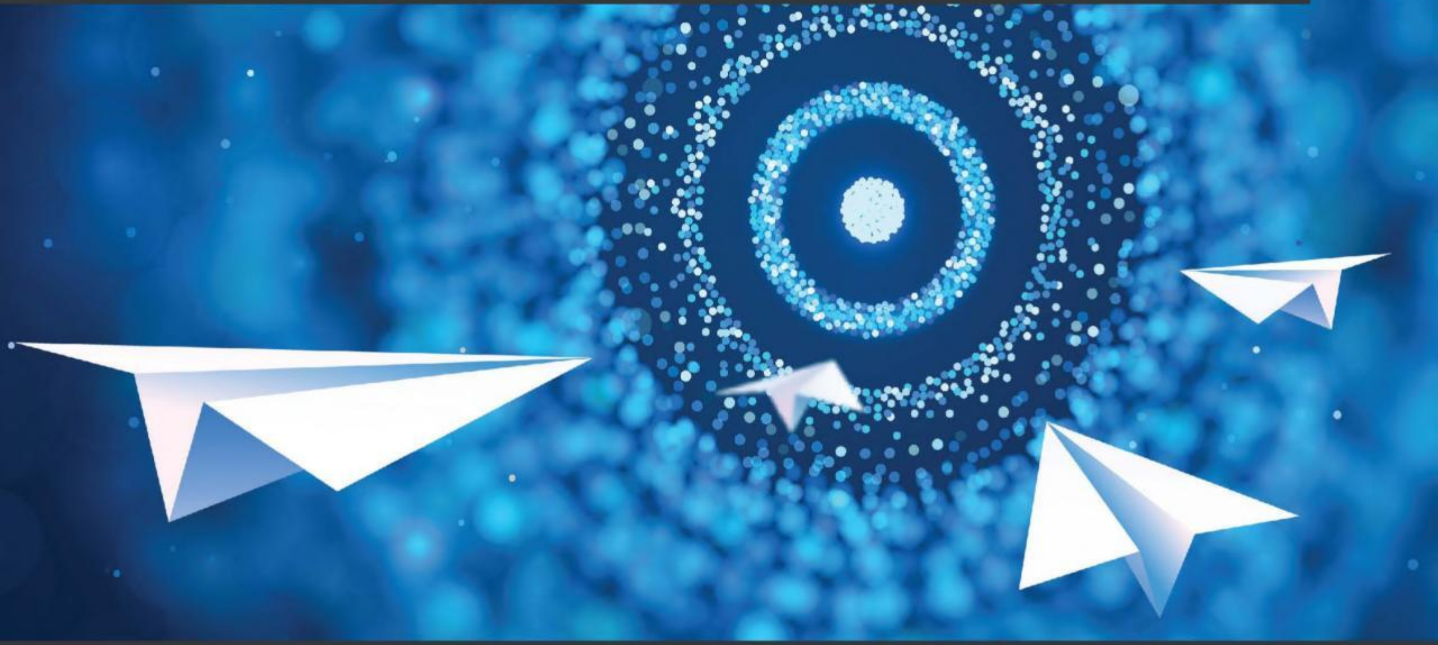
Mastering
Cyber Intelligence

Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense



Jean Nestor M. Dahj

Mastering Cyber Intelligence

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author(s), nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Vijin Boricha

Publishing Product Manager: Shrilekha Malpani

Senior Editor: Arun Nadar

Content Development Editor: Yasir Ali Khan

Technical Editor: Rajat Sharma

Copy Editor: Safis Editing

Project Coordinator: Ajesh Devavaram

Proofreader: Safis Editing

Indexer: Hemangini Bari

Production Designer: Joshua Misquitta

Marketing Coordinator: Hemangi Lotlikar

First published: April 2022

Production reference: 1010422

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-80020-940-4

www.packt.com

Table of Contents

Section 1: Cyber Threat Intelligence Life Cycle, Requirements, and Tradecraft

1
Cyber Threat Intelligence Life Cycle

2
Requirements and Intelligence Team Implementation

3
Cyber Threat Intelligence Frameworks

4
Cyber Threat Intelligence Tradecraft and Standards

5

Goal Setting, Procedures for CTI Strategy, and Practical Use Cases

Section 2: Cyber Threat Analytical Modeling and Defensive Mechanisms

6

Cyber Threat Modeling and Adversary Analysis

7

Threat Intelligence Data Sources

8

Effective Defense Tactics and Data Protection

9

AI Applications in Cyber Threat Analytics

10

Threat Modeling and Analysis – Practical Use Cases

Section 3: Integrating Cyber Threat Intelligence Strategy to Business processes

11

Usable Security: Threat Intelligence as Part of the Process

12

SIEM Solutions and Intelligence-Driven SOCs

13

Threat Intelligence Metrics, Indicators of Compromise, and the Pyramid of Pain

14

Threat Intelligence Reporting and Dissemination

15

Threat Intelligence Sharing and Cyber Activity Attribution – Practical Use Cases

Index

Other Books You May Enjoy

Preface

The increase in security breaches and attacks in the last two decades indicates that the traditional security defense methods are falling short. The sophistication of attacks – such as the **Advanced Persistent Threats** (**APTs**) – leaves organizations with more worries despite the heavy investment in security tools, which often work in silos. The lack of analytics skills, the struggle to incorporate security into processes, and the gap in structured security analytics are the main concern in the fight against augmented cyber threats.

Cyber Threat Intelligence (**CTI**) is a collaborative security program that uses advanced analysis of data collected from several sources (internal and external) to discover, detect, deny, disrupt, degrade, deceive, or destroy adversaries' activities. Because it is actionable and encourages information sharing between community members, individuals, and so on, it is becoming the de facto method to fight against APTs. However, many organizations are still struggling to embrace and integrate CTI in their existing security solutions and extract value from it.

This book, *Mastering Cyber Intelligence*, provides the knowledge required to dive into the CTI world. It equips you with the theoretical and practical skills to conduct a threat intelligence program from planning to dissemination and feedback processing. It details strategies you can use to integrate CTI into an organization's security stack from the ground up, allowing you to effectively deal with cyber threats.

Through step-by-step explanations and examples, you learn how to position CTI in the organization strategy and plan, and set objectives for your CTI program, collect the appropriate data for your program, process and format the collected data, perform threat modeling and conduct threat analysis, and share intelligence output internally (with the strategic, tactical, and operational security teams) and externally (with the community). By the end of the book, you will master CTI and be confident to help organizations implement it to protect revenue, assets, and sensitive information (and data).

Who this book is for

This book is for organizations that have basic security monitoring and intend to adopt cyber threat intelligence from scratch but do not know where to start, have good security infrastructure and intend to integrate threat intelligence in the security stack for optimal security posture, or have a good threat intelligence program and intend to enhance TTP prioritization, defense techniques, and threat tracking.

It is also useful for security professionals who want to learn and master cyber threat intelligence and help organizations in developing CTI strategies, possess theoretical knowledge and want to add some practical CTI skills, or want to enhance their career by preparing for professional CTI certifications such as the SANS FOR578 CTI and the EC-Council CTIA – this book is the perfect start as it covers most of the topics in those courses' curriculums.

What this book covers

Chapter 1, *Cyber Threat Intelligence Life Cycle*, discusses the steps involved in a CTI program implementation which include planning, objective, and direction; data collection; data processing; analysis and production; dissemination; and feedback. It provides a high-level overview of each step with some examples to help you understand what needs to be done. The chapter highlights the benefits of threat intelligence and its role in the defense against modern, sophisticated attacks such as APTs. It equips you with the knowledge required to plan and set directions for your program.

Chapter 2, *Requirements and Intelligence Team Implementation*, discusses threat intelligence requirement generation and task prioritization. It shows you how to generate sound intelligence requirements for your program by using advanced methods used in the military and warfare. As part of the planning phase of the CTI life cycle, the chapter discusses the team layout and how to acquire the right skill set to kick off your program. And finally, through the chapter, you learn how CTI relates to other units of the security stack.

Chapter 3, *Cyber Threat Intelligence Frameworks*, introduces the different frameworks that you, as a CTI analyst, can use for your threat intelligence program. It highlights their benefits and discusses the three most popular threat intelligence frameworks – the Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model of intrusion analysis frameworks. Using examples, the chapter also shows how each framework applies to threat and intrusion analyses.

Chapter 4, *Cyber Threat Intelligence Tradecraft and Standards*, discusses analytic tradecraft and standards that analysts can apply to CTI programs. It highlights the benefits of using common languages and processes in threat intelligence. The chapter teaches you how to apply already established analytic tradecraft and standards to your CTI program to increase its chance of success. Some of the analytics tradecraft and standards discussed in this chapter include the United States **Central Intelligence Agency**'s (**CIA**) compendium of analytic tradecraft notes, the **Intelligence Community Directive** (**ICD**) 203, the **Air Force Instruction** (**AFI**) 14-133, and their applications to CTI. Two important collaborative standards are practically described in the chapter, the **Structured Threat Information eXpression** (**STIX**) and the **Trusted Automated eXchange of Indicator Information** (**TAXII**).

Chapter 5, *Goal Setting, Procedures for CTI Strategy, and Practical Use Cases*, demonstrates how to integrate CTI into an organization's security profile from a practical standpoint. It introduces **threat intelligence platforms** (**TIPs**) (an essential tool for CTI) and provides guidelines for selecting the right TIP. You learn about open source and paid intelligence platforms, and which one would benefit you. The chapter uses practical case studies to show you how level 1, level 2, and level 3 organizations (those new to CTI, those with specific CTI knowledge, and those with a CTI program) can effectively embrace CTI and set goals. As an analyst or part of the CTI team, you can use the methods described in this chapter to kick-start a CTI program in your organization.

Chapter 6, *Cyber Threat Modeling and Adversary Analysis*, discusses strategic modeling of threats and analytics of the adversary's behavior. It gives you the theoretical and practical knowledge required to perform manual and automated threat modeling. You learn the different threat modeling methodologies with examples, **user behavior logic** (**UBA**), and adversary analysis techniques. At the end of the chapter, you will be able to perform threat modeling for your organization.

Chapter 7, *Threat Intelligence Data Sources*, discusses different threat intelligence sources and where to find the data. To conduct CTI, you need data and a lot of data most of the time. The chapter covers the three data source types: open source (OSINT or OTI), shared (STI), and paid (PTI) threat intelligence sources. It equips you with the knowledge to select the suitable data sources for your program based on the CTI requirements, the organization budget, and operational strategy. You learn about data source selection and evaluation, malware data sources, parsing, and analysis for CTI. You also learn the benefits of shared and paid threat feeds. Finally, you learn intelligence data structuring and storing.

Chapter 8, *Effective Defense Tactics and Data Protection*, discusses how to build a robust defense system to prevent and contain cyber-attacks. It details the best practices to achieve reliable data protection. In the chapter, you learn about enforcing the **Confidentiality, Integrity, and Availability** (**CIA**) by evaluating the loopholes in current cyber threat defense infrastructures and applying the appropriate tactics for defense; data monitoring and active analytics in CTI; vulnerability assessment and risk management in modern system protection; using encryption, tokenization, masking, and other obfuscation methods to make it difficult for adversaries; and finally, endpoint management.

Chapter 9, *AI Applications in Cyber Threat Analytics*, discusses how **Artificial Intelligence** (**AI**) can help transit from reactive to proactive threat intelligence programs to stay ahead of adversaries. This chapter teaches you AI-fueled CTI and how it makes a difference in security. You learn cyber threat hunting and how you perform it and integrate it into your security operations to anticipate attacks and ensure effective defense. You understand the benefits of combining threat hunting and threat intelligence for reliable protection. You learn AI's impact on adversaries' attack and procedures' enhancements. Finally, you acquire the knowledge and skills to position AI in CTI and your organization's security stack to maximize its value. We use the IBM QRadar as an example of how AI can enhance security functions and tools.

Chapter 10, *Threat Modeling and Analysis - Practical Use Cases*, is a hands-on, practical chapter that teaches you how to use CTI to perform intrusion analysis manually and automatically. It shows you how CTI analysts go from a received or discovered **indicator of compromise** (**IOC**) to understanding the extent of the intrusion. In this chapter, you learn how to gather and contextualize IOCs. You also learn to pivot through data sources and use intelligence frameworks for analysis. You gain the skills to perform basic memory and disk analysis to extract pieces of evidence to solve cybercrimes. You acquire the skills to gather malware data, perform basic malware analysis for your case, fill the Cyber Kill Chain matrix, and extract adversaries' **tactics, techniques, and procedures** (**TTPs**). Finally, you learn to use the open-source **Malware Information Sharing Platform** (**MISP**) for analysis and intelligence data storage.

Chapter 11, *Usable Security: Threat Intelligence as Part of the Process*, discusses how threat intelligence can be applied to business operations and system (software and hardware) development's security. As an analyst, this chapter equips you with the required knowledge to assess, advise, and assist in incorporating CTI into products and services that your organization develops from the conception phase. You learn how to use threat analysis output in authentication applications, use threat modeling to enforce sound policies into system development and business operations, apply mental models to improve threat defense, and finally, implement secured system architectures considering cyber threats.

Chapter 12, SIEM Solutions and Intelligence-Driven SOCs, discusses the importance of CTI in SIEM tools and SOCs. It explains the process of integrating intelligence in a SIEM solution. The chapter demonstrates how SIEM tools include and correlate data from multiple feeds and sources to provide automated intelligence. This chapter shows you how to automate and unify SOC operations for reactive and proactive defense. You learn how to optimize a SOC team's performance using threat intelligence. You also learn how to integrate threat analytics models to **Incident Response** (**IR**) to minimize the **Mean-Time-To-Respond** (**MTTR**). You gain the practical knowledge to use open source SIEMs and intelligence sharing platforms such as the AlienVault **Open Threat Exchange** (**OTX**) and **Open-Source Security Information and Event Management** (**OSSIM**) as a starting point. You learn intelligence-led penetration testing and incident response. Finally, you learn how to make your organization's SOC intelligent.

Chapter 13, Threat Intelligence Metrics, Indicators of Compromise, and the Pyramid of Pain, discusses security metrics for intelligence evaluation and program effectiveness. It also shows you how to evaluate your CTI team based on intelligence programs' output. The chapter then explains IOCs, the pyramid of pain, and their respective importance in a CTI analyst profile. In this chapter, you learn about CTI metrics and how they can be used to define the program success criteria. You learn the importance of IOCs, their categories, and how you recognize them in a system. You gain effective knowledge on the pyramid of pain and its application to CTI. You also learn how to apply the seven **Ds** (courses of action) of the Kill Chain in a threat analysis use case. Finally, you learn about the **indicators of attack** (**IOAs**) and how they differ from or relate to IOCs.

Chapter 14, Threat Intelligence Reporting and Dissemination, discusses threat intelligence reporting and sharing. It shows you how to write effective documentation for the strategic, operational, and tactical teams. It also shows you how to extract threat intelligence report elements such as adversary campaigns and malware families. In this chapter, you learn how to write threat intelligence reports, build adversary groups and campaigns, share intelligence using best practices, and finally, collect threat intelligence feedback.

Chapter 15, Threat Intelligence Sharing and Cyber Activity Attribution – Practical Use Cases, is a hands-on chapter that focuses on threat intelligence sharing and demonstrates how to attribute cyber activities to campaigns, threat groups, or threat actors. It provides you with the skills necessary to develop and share IOCs for internal security enhancement and external dissemination. In this chapter, you learn how to develop IOCs using YARA rules and use them to detect and stop attacks. You also learn how to set up a STIX/TAXII platform for intelligence dissemination using Anomali STAXX as an example. You learn how to use a threat intelligence sharing platform for intelligence dissemination. You gain the practical skills to build activity groups from threat analyses and associate analyses to each group (activity tracking). Finally, you learn how to conduct an **Analysis of Competing Hypotheses** (**ACH**) to attribute cyber activities to state-sponsored groups and actors.

To get the most out of this book

You need a basic knowledge of cybersecurity and networking to get the most out of this book. For practical exercises, you need the SANS SIFT workstation installed as a virtual machine or in any UNIX-based operating system, such as Ubuntu or Kali Linux. SIFT workstation comes with the necessary tools for security analysis. You need the MISP virtual machine and the Anomali STAXX platform to do the practicals in *Chapter 15, Threat Intelligence Sharing and Cyber Activity Attribution - Practical Use Cases*.

All the commands are executed directly on the guest platforms mentioned here or the host environment terminal. We have used a Windows 10 host environment.

Note that the book also explains the steps required to get you ready for practical exercises.

Software/hardware covered in the book	**Operating system requirements**
VirtualBox 6.1 as virtualization environment	Windows, macOS, or Linux
SANS-SIFT workstation 5.13.0-27-generic	Linux Ubuntu
MISP_v2.4.146	Linux Ubuntu
Anomali STAXX 3.10.0-693	CentOS Linux 7

Download the color images

We also provide a PDF file with color images of the screenshots and diagrams used in this book. You can download it here: `https://static.packt-cdn.com/downloads/9781800209404_ColorImages.pdf`.

Conventions used

There are a number of text conventions used throughout this book.

`Code in text`: Indicates code words in the text, indicators of compromise, port number, folder names, filenames, file extensions, and pathnames. Here is an example: "We pivot through the proxy logs, searching for `/sys/files/` patterns in all web transactions, not in the `125.19.103.198` IP communication."

A block of code is set as follows:

```
{
      ""title"": "CTI TAXII server",
      ""description"": "This TAXII server contains a listing
of ATT&CK domain collections expressed as STIX, including PRE-
ATT&CK, ATT&CK for Enterprise, and ATT&CK Mobile.",
      "contact": "attack@mitre.org",
      "default": "https://cti-taxii.mitre.org/stix/",
      "api_roots": [
          "https://cti-taxii.mitre.org/stix/"
      ]
}
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
raw_data.scan.port:554
raw_data.ja3.fingerprint:795bc7ce13f60d61e9ac03611dd36d90
```

Any command-line input or output is written as follows:

```
$ mkdir css
$ cd css
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For instance, words in menus or dialog boxes appear in **bold**. Here is an example: "Select **System info** from the **Administration** panel."

> **Tips or important notes**
>
> Appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, email us at customercare@packtpub.com and mention the book title in the subject of your message.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit www.packtpub.com/support/errata and fill in the form.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Share your thoughts

Once you've read *Mastering Cyber Intelligence*, we'd love to hear your thoughts! Please click here to go straight to the Amazon review page for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Section 1: Cyber Threat Intelligence Life Cycle, Requirements, and Tradecraft

The section introduces the concept of **Cyber Threat Intelligence** (**CTI**) and breaks down its life cycle, explaining the main building blocks of threat intelligence life cycle and strategy. It also discusses intelligence requirements and their importance in a CTI program's success. The section, then, covers standards and tradecraft that analysts can apply to CTI programs. Finally, it concludes with practical use cases to help organizations and individuals adopt CTI. Upon completion of this section, you should have mastered the CTI life cycle, acquiring a global idea of what is required at each stage of the cycle; understand how to generate requirements and build an effective team for your CTI program; understand and use threat intelligence frameworks for threat and intrusion analyses; be familiar with different standards and tradecrafts adopted by the cybersecurity community, military, and intelligence agencies to conduct intelligence and apply them to your CTI program; be able to start a CTI program in an organization, whether it is new to CTI or has experience in the matter; and finally, select the appropriate threat intelligence platform for your program.

This section contains the following chapters:

- *Chapter 1*, Cyber Threat Intelligence Life Cycle
- *Chapter 2, Requirements and Intelligent Team Implementation*
- Chapter 3, *Cyber Threat Intelligence Frameworks*
- Chapter 4, *Cyber Threat Intelligence Tradecraft and Standards*
- Chapter 5, *Goal Setting, Procedures for CTI Strategy, and Practical Use Cases*

1
Cyber Threat Intelligence Life Cycle

This chapter will explain the steps of the threat intelligence life cycle. We will provide a high-level description of each step while looking at some practical examples to help you understand what each step entails. By the end of the chapter, you will be able to explain each stage of the intelligence life cycle and join the practical with the theoretical. This chapter forms the baseline of this book, and various intelligence strategies and processes will be built on top of this knowledge.

By the end of this chapter, you should be able to do the following:

- Clearly explain what cyber threat intelligence is, why organizations must integrate it into the business and security team, who benefits from it, and be able to define its scope.
- Understand the challenges related to threat intelligence and cybersecurity in general.
- Know and understand the required components to effectively plan and set directions for a threat intelligence project.
- Know and understand the data required to build an intelligence project and how to acquire it globally.

- Understand intelligence data processing, why it is essential in integrating a CTI project, and justify the need for automating the processing step.
- Understand the analysis step, its application, and its impact on the entire CTI project. In this step, you will also learn about intelligence analysis bias and different techniques that can be used to avoid a biased intelligence analysis.
- Explain the cycle's dissemination step and how to share an intelligence product with the relevant stakeholders. You should also understand the importance of the audience when consuming the product.
- Understand and explain the feedback phase of the cycle and state why it is critical in the project.

In this chapter, we are going to cover the following main topics:

- Cyber threat intelligence – a global overview
- Planning, objectives, and direction
- Intelligence data collection
- Intelligence data processing
- Intelligence analysis and production
- Threat intelligence dissemination
- Threat intelligence feedback

Technical requirements

For this chapter, no special technical requirements have been highlighted. Most of the use cases will make use of web applications if necessary.

Cyber threat intelligence – a global overview

Many businesses and organizations aim for maximum digital presence to augment and optimize visibility (effectively reach the desired customers), as well as maximize it from the current digitalization age. For that, they are regularly exposed to cyber threats and attacks based on the underlying attack surface – the organization's size, architecture, applications, operating systems, and more.

Threat intelligence allows businesses to collect and process information in such a way as to mitigate cyberattacks. Hence, businesses and organizations have to protect themselves against threats, especially human threats. **Cyber threat intelligence** (**CTI**), as approached in this book, consists of intelligent information collection and processing to help organizations develop a proactive security infrastructure for effective decision making. When engaging in a CTI project, the main threats to consider are humans, referred to as *adversaries* or *threat actors*. Therefore, it is essential to understand and master adversaries' methodologies to conduct cyberattacks and uncover intrusions. **Tactics, techniques, and procedures** (**TTPs**) are used by threat actors. By doing so, organizations aim for cyber threats from the source rather than the surface. CTI works on evidence, and that evidence is the foundation of the knowledge required to build an effective cyber threat response unit for any organization.

Many organizations regard threat intelligence as a product that allows them to implement protective cyber fences. While this is true, note that threat intelligence hides an effective process behind the scenes to get to the finished package. As the intelligence team implements mechanisms to protect against existing and potential threats, adversaries change tactics and techniques. It becomes crucial for the intelligence team to implement measures that allow new threats to be analyzed and collected. Hence, the process becomes a cycle that is continually looked at to ensure that the organizations are not only reactive but proactive as well. The term *threat intelligence life cycle* is used to define the process required to implement an efficient cyber threat intelligence project in an organization. The following diagram shows this process:

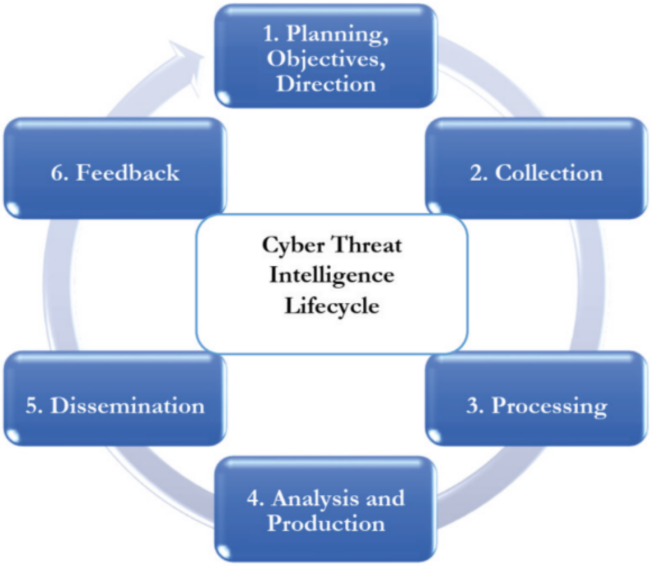

1. Planning, Objectives, Direction
2. Collection
3. Processing
4. Analysis and Production
5. Dissemination
6. Feedback
Cyber Threat Intelligence Lifecycle

Figure 1.1 – Threat intelligence life cycle

Threat intelligence is an ongoing process because adversaries update their methods, and so should organizations. The CTI product's feedback is used to enrich and generate new requirements for the next intelligence cycle.

Characteristics of a threat

Understanding what a *threat* is helps organizations avoid focusing on security alerts and cyber events that may not be a problem to the system. For example, a company running Linux servers discovers a `.exe` trojan in the system through the incident management tool. Although dangerous by nature, this trojan *cannot* compromise the company's structure. Therefore, it is not a threat. As a security intelligence analyst, it is vital to notify the system manager about the file's low priority level and its inability to infect the network. Secondly, government agencies are one of the highest adopters and owners of cyber projects. Governments have the tools and the knowledge necessary to attack each other. However, to avoid a cyberwar and ruin their friendship, the Canadian and American governments have no *intention* of attacking each other. Thus, they are not a threat to each other. If one party announces a spying tool's design, that does not mean that it wants to use it against another. Although there is the capability of spying, there might be no intent to do so. Therefore, one is not always a threat to another. Lastly, you can have the capability and the intent, but would need the *opportunity* to compromise a system.

Therefore, we can summarize a *threat* as everything or everyone with the *capability*, the *intent*, and the *opportunity* to attack and compromise a system, independent of the resource level. When the intelligence team performs threat analysis, any alert that does not meet these three conditions is not considered a threat. If any of these three elements is missing, the adversary is unlikely to be considered a threat.

Threat intelligence and data security challenges

Organizations face a lot of challenges when it comes to data protection and cybersecurity in general. Those challenges are located in all the functional levels of the organization. There are several challenges, but the most common ones include the following:

- **The threat landscape**: In most cases, cyberattacks are orchestrated by professionals and teams that have the necessary resources and training at their disposal. This includes state-sponsored attacks. However, with access to specific tools and training, private groups have developed sophisticated ways to conduct destructive cyberattacks. The landscape of threats is growing and changing as adversaries rely on new exploits and advanced social engineering techniques. McAfee Labs reported an average of 588 threats per minute (a 40% increase) in the third quarter of 2020, while Q3 to Q4 2020 saw more than a 100% increase in vulnerabilities and more than a 43% increase in malware.

Targeted attacks such as ransomware were the main concern for organizations in 2020, with more than a 40% increase by the end of the year (`https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-apr-2021.pdf`). Approximately 17,447 vulnerabilities (CVEs) were recorded in 2020, with more than 4,000 high-severity ones (`https://www.darkreading.com/threat-intelligence/us-cert-reports-17447-vulnerabilities-recorded-in-2020/d/d-id/1339741`). Thus, the threat landscape presents a dangerous parameter for organizations that have most of their resources, assets, services, and products on the internet. And understanding the threat landscape facilitates the risk mitigation process. Personal information is one of the most targeted components on the internet – **Personally Identifiable Information** (**PII**), payment card data, and HIPAA data, to name a few.

- **Security alerts and data growth**: Organizations are acquiring different security platforms and technologies to address security concerns and challenges – sandbox, firewalls, incident response, threat hunting, fraud detection, intrusion detection, network scanners, and more. According to an IBM study, an average IT company possesses 85 general security tools from at least 25 vendors. In most cases, those tools are not integrated across all teams. They have different security requirements. Each tool generates security alerts of different levels, and in most cases, security professionals rely on manual processes or external automation tools (with limited functionalities) to aggregate, clean, correlate, analyze, and interpret the data. The more tools an organization has, the more data is being collected, and the more exhausted and overwhelmed the security analysts become when having to mine the voluminous data. There is then a high chance of not using data effectively, thereby missing out on critical alerts. Having a high volume of alerts and data makes it difficult, if not impossible. for a human to handle correctly. This is known as visibility loss.
- **Operational complexity**: The core business components may involve several organizational departments that interact with different applications to reach their goals. The embrace of big data and the adoption of cloud technologies have facilitated the management of IT infrastructures. However, it has also opened doors to more attack points as cloud security is becoming a hot topic. This is because many third-party tools, resources, and suppliers (which also have their own vulnerabilities) are used to address the security problem. Third-party tools are somehow not transparent to the organization where they are installed because most of the processes happening in the backend are not exposed to the consumers. Therefore, they increase operational complexity, especially regarding ownership of each security aspect (such as incident management, intrusion detection, traffic filtering, and inspection). Policies and procedures must be set if organizations wish to have useful data security solutions. Organizations must find ways to regulate the authority of third-party and other external tools internally.

- **New privacy regulations**: New requirements are frequently put in place to address data security and privacy concerns worldwide. Regulations are used to enforce the law. However, as the number of regulations increases for different industries – medical, financial, transportation, retails, and so on – them overlapping becomes a challenge as organizations must comply with all policies. Should an organization fail to comply with regulations, penalties could be imposed independently of a breach's presence or absence. This is why it's important to have security solutions that are regulation-compliant.

  Nevertheless, different regions and agencies have different security policies that need to be followed. A typical example is the European Union's **General Data Protection Regulation** (**GDPR**), which is used to protect EU citizens' privacy and personal information. The GDPR applies to the EU space, which means any organization (independent of its origin, EU or not EU) operating or rendering services in the EU region needs to comply with the GDPR. Tradecrafts and standards will be explained in *Chapter 4*, *Cyber Threat Intelligence Tradecraft and Standards*. Another example is the South African **Protection of Personal Information** (**POPI**) Act, which protects South African citizens' privacy and how their personal information is handled. Complying with such policies can be challenging, and organizations need to ensure compliance with regulations.
- **Cybersecurity skills gap**: As organizations grow, manual processes become a challenge, and the lack of a workforce manifests. According to the ISC2 2019 report (`https://bit.ly/2Lvw7tr`), approximately 65% of organizations have a shortage of cybersecurity professionals. Although the gap is being reduced over the years, the demand for cybersecurity professionals remains high. And that is a big concern. The job concerns relating to cybersecurity professionals, as reported by ISC2, are shown in the following diagram:

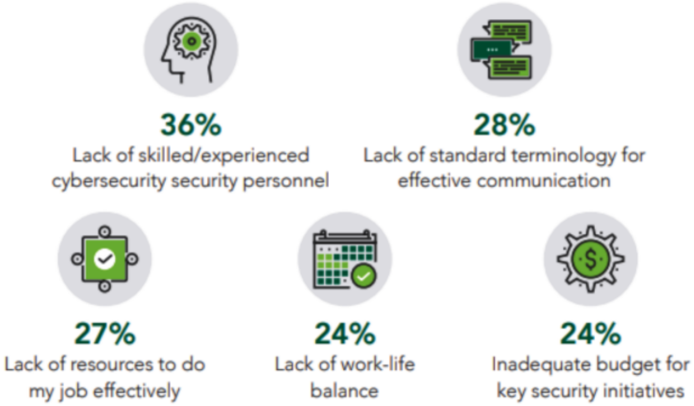


Figure 1.2 – ISC2 job concerns among cybersecurity professionals

Organizations spend more time dealing with security threats than training or equipping the team with the necessary knowledge. Adversaries keep on attacking and breaking through conventional security systems daily. This is why there is a great demand for cybersecurity professionals worldwide who are compliant with the industry standards and methods who are dependable, adaptable, and, most importantly, resilient. Organizations need to invest in empowering and training individuals in the field of cybersecurity and threat intelligence.

Importance and benefits of threat intelligence

Cyber threat intelligence (**CTI**) addresses the aforementioned challenges by collecting and processing data from multiple data sources and providing actionable, evidence-based results that support business decisions. Using a single platform (for correlation, aggregation, normalization, analysis, and distribution) or a centralized environment, CTI analyzes data and uncovers the essential patterns of threats – any piece of data that has the *capability*, the *intent*, and the *opportunity* to compromise a system.

CTI consolidates an organization's existing tools and platforms, integrates different data sources, and uses machine learning and automation techniques to define context regarding **indicators of compromise** (**IoCs**) and the **TTPs** of adversaries. Intelligence analysts and security professionals rely on IoCs to detect threat actors' activities. Therefore, the types of indicators that are selected are critical during intelligence execution. This is because they determine the pain it can cause adversaries or threat actors when IoCs access is denied. This is known as the *pyramid of pain* and provides correlations between indicator types and pain levels. This pyramid is shown in the following diagram:

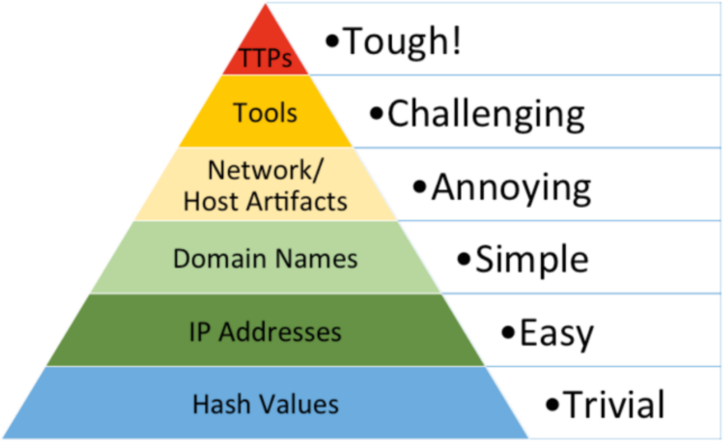


Figure 1.3 – ISC2 job concerns among cybersecurity professionals

Hash algorithms provide unique ways to obfuscate information. Hash indicators can be used to detect unique threats (such as malware) and their variants since a change in information results in a complete change in hash. Therefore, it is easy for adversaries to change malware hash values, for example. IP addresses are one of the popular indicators used to detect threats. An analyst can spot malicious activities using IP addresses. However, they can be changed easily.

An adversary can use proxy and TOR services to modify the IP addresses constantly. Domain names are also prevalent indicators as they can be used to spot malicious domain names. However, changing domain names requires a bit of effort (registration, payment, and hosting). Because there are many free hosting domains, adversaries can simply change a domain.

Changing domains takes a while. Hence, it is not as easy as changing IP addresses. Network and host artifacts are also important indicator types. Once professional security changes the network and host information, adversaries are forced to review and reconstruct their attacks (most attack networks and hosts). Hence, changing the host and network artifacts annoys the adversary.

The next indicator type is tools, and they detect the kind of tools that adversaries use to orchestrate attacks. When the intelligence analyst can detect threat actors' tools and their artifacts, this means the adversaries in question have no other option than to change the tool or create a new one completely (this takes time and money for the adversaries). Hence, making changes to tools challenges the adversary enormously.

At the top of the pyramid is TTP. At this level, any detection from the analyst results in a complete reinvention from the adversaries because, at this level, the intelligence analysts operate on the behavior, not just the tool – the higher the operating level of intelligence, the more difficult it is for adversaries to compromise the system. More details on IoCs will be provided in *Chapter 13*, *Threat Intelligence Metrics, Indicators of Compromise, and the Pyramid of Pain*.

CTI helps organizations protect revenue and measure the efficiency of the entire security infrastructure. By integrating CTI in the business processes, organizations can create a positive return on investment in the short term. Data breaches can be costly in terms of financial implications, brand reputations, and business situations. Hence, CTI is an essential aspect of revenue protection and generation.

Threat intelligence is considered an intricate domain of exclusive analysts. However, threat intelligence analysts conduct CTI projects for others – to secure other people's infrastructures. Hence, it adds value to the functions of any organization. From small businesses to large corporations, governments, and threat actors, everyone is a benefactor of threat intelligence. CTI should not be considered a separate entity of the security components, but it should be a central element of every existing security function, as we will see in the coming chapters. The main reason for this is that the CTI project's output should be shareable and accessible across all the organization's security functions.

By now, every organization or individual should be able to do the following:

- Define threat intelligence and identify real threats by focusing on their characteristics.
- Enumerate and identify the challenges related to data security and threat intelligence.
- Understand the reason to integrate CTI as an essential business component.

Now that we have understood and mastered what CTI is all about, it is vital to understand and master the cyclic process of CTI and how business functions fit each step.

Planning, objectives, and direction

The planning step is the most critical step of a CTI project's integration. It is the main ingredient of the success or failure of a CTI project. If planning is not done properly and the objectives are not set reasonably, a threat intelligence project will likely fail. The planning and direction step can be segmented into two main objectives and three fundamental phases.

CTI main objectives

Any organization or individual who wants to implement threat intelligence must start by asking the right question: *why do I want a CTI team?* Planning a CTI program comes down to the objectives and goals of the CTI project. The answer to this question will define the purposes of the threat intelligence team. According to the *SANS FOR578*, a CTI team's primary function in an organization involves providing threat preventive measures, incident response, and strategic support:

- **Preventive measures**: Threat intelligence analysts who are part of a team can provide tremendous support to the **security operations centers** (**SOCs**). The SOC teams deal with frequent threat monitoring systems and are flagged continuously with alerts and issues. Because many processes are done manually in the legacy security system, it can be cumbersome for the SOC team to prioritize alerts or manage critical adversaries.

Because threat intelligence is based on a centralized approach, a CTI team adds more value to the organization's SOC by filtering and prioritizing alerts, expanding and enriching **indicators of compromise** (**IoC**), and extracting the correct information that's used to assess the system's efficacity.

- **Incident response unit**: In many organizations, the SOC team is separated from the incident response team. Threat intelligence can help the IR team respond to threats, consolidate the information, and share and benchmark threats against what is happening in other organizations. CTI is also about sharing information – the existence of security blogs, newspapers, and so on. By knowing what happened in the past in other organizations, threat analysts can improve the IR team's efficiency when dealing with known or unknown adversaries.
- **Strategic support unit**: At a strategic level, threat intelligence supports stakeholders' business decisions based on evidence and actionable facts or events. Strategic intelligence is the best way to keep an organization informed of the current and prospect threats landscape and their potential impact on the business. CTI also exposes the current resource situation of an organization to the stakeholders. For example, it can advise on the types of people that need to be acquired for the threat intelligence team or the best training or skills required to mitigate specific threats.

Another goal of the first process is to position the threat intelligence team within the organization, which will be detailed in the next chapter. Nevertheless, it is essential to know how the CTI team will work with other security functions such as SOC, incident response, malware analysis, and risk assessment. Threat intelligence has to work with all security functions to facilitate the unit's analysis process and information sharing.

The CTI team's objectives must be set in such a way that they match the organization's core business or values. And they must be set to reduce the time to respond or mitigate threats and minimize the negative impact on business operations while maximizing profit.

CTI planning and direction – key phases

When planning and setting a CTI team's direction, it is also crucial to look at its operational plan. There are three main operational planning phases in threat intelligence implementation: intelligence requirements collection, threat modeling, and intelligence framework selection. Including these three phases in the first step increases the chances to succeed in the threat intelligence implementation.

Each of these phases will be discussed as separate chapters in this book:

- **Intelligence requirements collection**: In this phase, the CTI team collects the requirements from each business function to create a database of requests and pain points that need to be addressed. This phase can be achieved through a set of single facts or activities. It is necessary to avoid open-ended questions as the CTI results need to be specific and evidence-based. The requirements need to be collected at each business level: strategic, operational, and tactical.
- **Threat modeling**: When planning for a CTI project or implementing an intelligence team, it is essential to evaluate all the assets that an adversary will target. Threat modeling involves identifying the organization's principal assets and performing a reconnaissance of the adversary. Using past information can help model threats using functional activities such as financial data, personal information, and intellectual property data.
- **Intelligence framework selection**: To effectively produce intelligence, threat analysts need to collect the data, process it, and deliver the output transparently. It is essential to project how data will be used to provide the desired answers. Intelligence framework selection is a critical parameter when producing intelligence. It gives insight into the different data sources (internal and external) and how the data is exploited to produce intelligence. An intelligence framework should fulfill a certain number of criteria, which will be detailed in *Chapter 3*, *Cyber Threat Intelligence* Frameworks. However, the main tip is to select a framework that provides an end-to-end view of the available data (external and internal).

Now let's take a look at the consumers of the results.

Determining the consumers of the results

During the planning phase, the threat analysts should also determine the consumers of the end products. Although CTI is beneficial to all, identifying the major players will help determine which area to focus on. For example, will the intelligence product be sent to the cybersecurity analysts (more technical and hands-on professionals), or will it be sent to the executives who focus on a global overview of the organization's security status to justify the investment in the project or the team?

The planning and direction of threat intelligence is summarized in the following diagram:

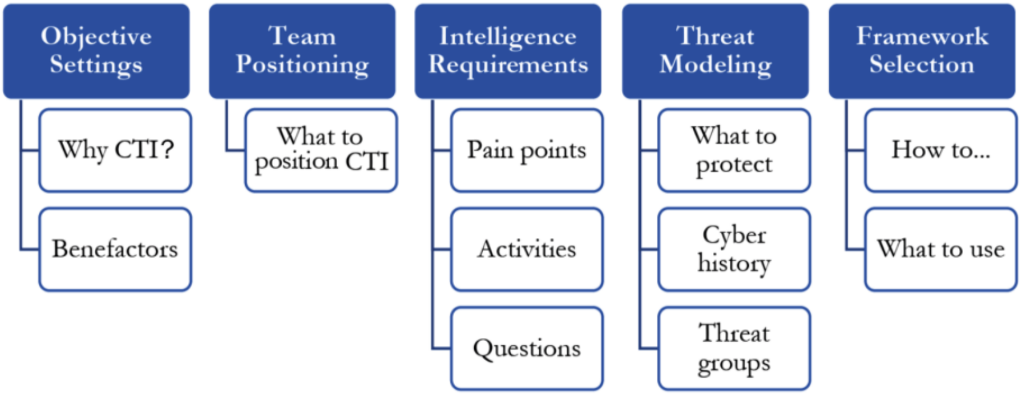


Figure 1.4 – Threat intelligence planning and direction summary

The CTI team and the organization security teams must use the layout shown in the preceding diagram to conduct the planning and direction phase. The output of this will drive the data collection phase. If we know the organization's security weaknesses, the assets to protect, and the possible threats to the security system, we will be able to acquire the correct intelligence data.

Intelligence data collection

There is no intelligence without data. After carefully planning and directing the intelligence team, the next step is to access the data. Data is collected to fulfill the requirements that have been assembled in the planning phase. It is recommended to collect data from different sources to have a rich arsenal of information and an effective intelligence product. Intelligence data sources can be divided into internal and external sources (detailed in *Chapter 7, Threat Intelligence Data Sources*):

- **Internal sources**: Internal sources constitute, or should constitute, the foundation of the data. It is essential to have an idea of the internal information first before looking at external sources. This data source includes network element logs and records of past incident responses. The most common internal data source collection could consist of intrusion analysis data by using the Lockheed Martin Kill Chain, such as internal malware analysis data (one of the most valuable data sources of threat intelligence), domain information, and TLS/SSL certificates.

- **External sources**: External sources are mandatory data collection points as they bring new visibility to threats. Those sources include external malware analysis and online sandbox tools, technical blogs and magazines, the dark web, and other resourceful sources such as open source and counterintelligence data. Malware zoos are also an essential part of external sources. By using and accessing an online sandbox system or using a malware analysis tool, intelligence analysts can collect useful information about adversaries' signatures to enrich the intelligence database.

As we will see in *Chapter 7*, *Threat Intelligence Data Sources*, collected data is placed into lists of **indicators of compromise** (**IOC**). Those indicators include, but are not limited to, domain information, IP addresses, SSL/TLS certificate information, file hashes, network scanning information, vulnerability assessment information, malware analysis results, packet inspection information, social media news (in raw format), email addresses, email senders, email links, and attachments. The more data that's collected, the richer the intelligence's repository and the more effective the intelligence product.

Suppose an attacker sends an email to a person in the organization who downloads and opens an attachment. A trojan is installed on the system and creates a communication link with an adversary. The relevant data needs to be available to detect and react to such an incident. For example, the threat intelligence analyst can use the network, domain, and certain protocol information to detect and prevent the trojan from infecting the system.

Therefore, collecting the right data is critical. We can directly create a link to the first step. If the intelligence framework's choice was poorly conducted, it would take time and a lot of effort to react to such a threat (adversary). Therefore, when selecting a framework, a CTI analyst should project the amount of data sources they intend to integrate into the system. They must also choose a platform that can accommodate big data.

Intelligence data processing

Raw data holds no meaning until it is converted into useful information that the organization can use. Data is seen as the new oil, which means every organization collects a fair amount of data in various forms. Security companies collect big data in terms of logs, scans, assessments, and statistics. This step aims to process and format the big, collected data into a readable or easy-to-understand arrangement. However, it is difficult, if not nearly impossible, for an analyst to manually or singlehandedly mine the data that's been collected to build intelligence effectively. Therefore, processing the collected data needs to be automated by using intelligence platforms. This will be covered in detail in *Chapter 5*, *Goals Setting, Procedures for the CTI Strategy, and Practical Use Cases*.

There are several intelligence frameworks and structured models that can be used to process intelligence data dynamically. During the processing task, the analyst uses one or more frameworks or structures to organize the data into different buckets or storage units. Imagine a bank being targeted by several adversaries simultaneously; it is unlikely for threat analysts to detect and prevent all those threats manually. Structured models and frameworks help identify patterns in the data and identify intersection points between the different sources to understand how the adversaries operate effectively.

Security information and event management (**SIEM**) tools are mostly used to facilitate intelligence data processing and exploration. SIEM will be studied in detail in *Chapter 12*, *SIEM Solutions and Intelligence-Driven SOCs*. These tools provide a holistic view of the entire security system by correlating data from different sources. They are a great starting point for data processing and transformation. However, intelligence platforms and frameworks also allow us to perform intelligence data processing and exploration, especially when dealing with unstructured data from different sources or different vendors. Currently, some platforms support machine learning to identify threats in the data. Frameworks such as MITRE ATT&CK, Diamond model, and Kill Chain can all be used to process intelligence data smartly.

Using the Diamond model and the example provided in the previous section, a cyber threat intelligence SIEM can model the described threat in terms of four components: the adversary (the threat creator), the victim of the trojan (the employee and the system where it is implanted), the tactics and techniques used by the adversary to compromise the system, and the way the threat accessed the system (through an email attachment). The model correlates these four pieces and extracts commonalities to profile the adversary and initiate the appropriate actions.

The MITRE ATT&CK framework would focus more on the adversary's tactics and techniques and identify the threat's impact on the system. The most typical components that the framework extracts include the method used by the malware to access the system (in our case, an email, also known as phishing), the execution method (through double-clicking), the capabilities of the threat (privilege escalation, persistence nature, credentials theft, and so on), its direct impact on the system, and more.

In both cases, we can notice that both frameworks correlate different data to gain structured, meaningful information. For example, to understand that the initial access was done through phishing, it is vital to have email-related data (links, sender, attachments, receiver, attached IP address, domain, and so on), which can help the organization pivot through different data sources to analyze the threat. A link can already be established between data collection (what data is available or being collected) and processing.

The processing phase also addresses the storage problem. Since a lake of raw intelligence data is created in step 2 (*intelligence data collection*), a warehouse of processed data needs to be built in step 3 (*intelligence data processing*). The CTI team should be able to store the data effectively so that information can be accessed and retrieved easily as required. Specific CTI platforms, as we will see in *Chapter 3*, *Cyber Threat Intelligence Frameworks*, provide fast storage capabilities. Depending on the objectives and set requirements, an organization can choose to store processed intelligence information in the cloud or on-premises. It is crucial to evaluate and select the right approach from the early phases (step 1, *planning and direction*).

Another important feature to consider when selecting a CTI framework is the capability to process data in different languages. This can be a deciding point when setting and integrating an intelligence project. It allows the CTI team or analyst to go beyond the language barrier.

In this step, the CTI team or analyst must set up the tools, frameworks, and platforms that efficiently process raw intelligence data and store the information in an easy-to-access and easy-to-retrieve repository (considering the capabilities of the underlying tools).

Analysis and production

Analysis and production can be thought of as the interpretation step where the processed data is converted into indicators of compromise, alerts, and alarms, with the capability to notify all the relevant parties of any potential threats. The results should be presented in perfect harmony with the objectives and requirements that were collected in the first phase (planning and direction). There is no one specific output format for presenting the analysis of an intelligence project. It is essential to understand the consumers before providing the results. This step is the livelihood of the intelligence project; that is, the main reason for its existence. Hence, the analyst or CTI team needs to pay attention to it.

Although collecting and processing intelligence data is automated, interpreting the results requires human expertise. And this is where human errors cause disruptions. This is known as *bias* and needs to be avoided when analyzing the processed data. Bias is causally linked to personal views, opinions, and interpretation of the intelligence result. CTI is an evidence-based product and process. Hence, every analysis should be supported by clear evidence – for example, an analyst who supports a specific theory without evidence based on experience or their gut feeling. The analyst then looks for evidence that supports the idea and rejects any other evidence that doesn't support the theory. This kind of analysis will result in a higher bias toward supportive facts.

One of the most commonly used methods is **structured analytic techniques** (**SAT**), created by the United States Government. It is used to implement an unbiased solution and improve intelligence analysis. SAT will be covered in detail in *Chapter 3*, *Cyber Threat Intelligence Frameworks*, as a form of tradecraft. SAT is used by several private sectors and intelligence analysts, including the CIA. Its primary objective is to minimize judgment and control uncertainties that can happen during analysis. This method uses three different techniques, grouped by their purpose:

- **Diagnostic techniques**: These techniques focus on transparency. As approached by SATs, diagnostic techniques use arguments and assumptions to support decisions or threat analysis output. The idea behind this method is to ensure that intelligence analysts do not discard any relevant hypotheses. Some of the techniques in this category are as follows:

  a. **Quality of information check**: This is where the comprehensiveness of the data that analysis is or needs to be performed on is benchmarked. This category provides grounds for confidence in the analytic evaluation and results in a precise assessment of what is provided by the intelligence platform.

  b. **Indicators of change**: While exploring and analyzing the intelligence output, it is imperative to observe indicators regarding sudden data changes. This method is useful when the CTI team or an analyst wants to track activities specific to a target or an adversary. This method avoids bias by adding credibility to the analytics result.

  c. **Analysis of competing hypothesis**: Suppose that the CTI team collected and processed a large amount of data. In this method, every CTI analyst provides an interpretation of the analysis. Cross-evaluation is then done in the form of a challenge, where hypotheses are compared based on their efficacity and the evidence that supports them. The best approach to using the competing hypothesis is to create a matrix of analysis.

- **Contrarian techniques**: These techniques challenge a specific hypothesis. The idea is to eliminate bias through contradiction. The analysts contradict even the most founded intelligence analysis interpretation to collect more evidence to support it. Some of the popular methods that are used in this category of techniques include the following:

  a. **The devil's advocate**: As the name implies, this method challenges a strong interpretation of the result by developing and supporting alternative interpretations. Suppose that after intelligence analysis is performed, indicators showing threats from Chinese IP addresses emerge. The entire team concludes that Chinese IP addresses are trying to communicate with a certain system application.

Using the devil's advocate, a brave analyst challenges this conclusion by saying that those IP addresses belong to another country and that proxychains and VPNs were used to mask the adversary's real origin. Now, the team uses the contradicting hypothesis to prove that the threats originate from China. This method removes bias by showing how confident the team is in their interpretation.

b. **AB team**: This is one of the most prominent methods. The manager or the CTI team leader divides the group into two teams: A and B. The two teams challenge each other by competing when it comes to interpreting the intelligence result. Moreover, it is essential to draw a line between the AB team and the devil's advocate approach. The former is used when there is more than one interpretation of the same analysis. The objective should remain the same: discussing how to eradicate everyone's bias mindset by making them defend an interpretation they do not agree upon.

c. **What-if analysis**: In the example provided for the devil's advocate, instead of confirming the team's opposing thoughts, an analyst should ask, *what if the IP addresses are not from China?* The focus is on *how is it possible to have China's IP addresses as a threat?* The team can then focus on parameters that might have enabled the presence of Chinese IP addresses in the system.

- **Creative thinking techniques**: These techniques produce new interpretations or insights regarding the analysis. This allows analysts to create further analysis angles and produce alternative results to the primarily completed study. Imaginative thinking includes several popular methods, such as the following:

a. **Brainstorming**: Brainstorming involves generating new concepts, ideas, theories, and hypotheses around the analysis results. The CTI team must use brainstorming to promote creativity and push analysts to think outside the box. It is used to reduce bias as analysts are likely to step away from their clouded opinions to develop fresh new ideas – every concept matters. The CTI team leader should consider all analysts' views and understand the triggering points of those ideas.

b. **Red team analysis**: The most technical approach to intelligence analysis is when the analyst wears the adversary's dress. In red team analysis, the CTI analyst tries to replicate the adversary's threat method (how an adversary attacks, how they think, and so on). When performing threat intelligence analysis, it is vital to take a red team approach because it assumes the worst scenario, and it also helps the team prepare a defense mechanism that can resist the most potent of threats. The analyst becomes a white adversary. Note that this kind of analysis is complicated, time-consuming, and resource-intensive. This is because an exceptional team of analysts needs to be implemented to simulate the adversary.

c. **Outside-in thinking**: The CTI team must always look at the external factors that can easily influence the analysis. The intelligence analyst should be able to identify the forces that impact the analysis. For example, what are the key elements that might push China to be a cyber threat? Factors such as politics, socioeconomics, and technology should be considered when doing critical thinking regarding an analyzed threat.

In most cases, the CTI team uses the three techniques described here to perform an approximate complete and unbiased analysis. Each technique has several key components that need to be checked to validate their application (more details will be covered in *Chapter 3*, *Cyber Threat Intelligence Frameworks*).

The analyst should also establish or identify relationships between different threats and adversaries during the analysis step. This helps with finding a correlation, patterns, or unique characteristics between different threat actors (for example, a current threat might have the same properties as a past threat). The diamond model is one of the universally used models for clustering and correlating threats and adversaries.

With that, we have explained what needs to be done during the analysis and exploration step, as well as what methodologies a CTI team can use to yield a useful analysis and interpretation. More details on how this can be done, along with examples, will be provided later in this book. We will also include a short overview of the biases that can mislead a threat intelligence operation.

Threat intelligence dissemination

A successful intelligence project should not be kept to yourself – it should be shared with others. Threat intelligence is performed to secure others. Hence, the CTI team or the analyst needs to distribute the intelligence product to the consumers. An organization only initiates actions if the result has reached the relevant personnel.

The dissemination step must be tracked to ensure continuity between intelligence cycles in a project. This sharing must be done in a transparent way using ticketing systems, for example. Let's assume that an intelligence request has been logged in the system. A ticket should be created, reviewed, updated, answered, and shared with the relevant parties. However, the CTI team must know how to share the output with different audiences by considering their backgrounds. Therefore, understanding the consumers of the product is capital. The consumers are the ones that define the dissemination process. What differentiates the consumers is parameters such as the intelligence background, the intelligence needs, the team in question, and how the results will be presented.

At the operational level, the intelligence output can be presented technically (we will detail *why* in the next chapter). The target audience in this group includes cybersecurity analysts, malware analysts, SOC analysts, and others. At the strategic level, the intelligence output should be less technical and focus on business-level indicators. At the tactical level, the outcome must clearly show the tactics and techniques of adversaries. The format's technicality must be profound at this level as it includes professionals such as incident response engineers, network defense engineers, and others. It is essential to know the consumer or the target audience and tailor the output accordingly. Intelligence dissemination must match the requirements and objectives that were set in the planning and direction phase.

The dissemination phase overlooks the reporting phase because the intelligence result is distributed and shared in the form of reports, blogs, news, and so on. The CTI team or analyst must write valuable reports that convey an honest message with the appropriate metrics and indicators to support the output (or the conclusion that was made). Reporting and intelligence documentation will be covered in *Chapter 14, Threat Intelligence Reporting and Dissemination*. However, it is essential to outline the findings clearly and concisely. Interesting topics must always be covered first to give the audience the desire to continue reading. Should there be actions to take, they should be highlighted at the beginning of the report. The CTI analyst must also be able to assess the entire process and the presented result. They must always be confident enough to defend everything included in the intelligence report using evidence and by quoting the different sources that were used. We will provide a template for documentation and reporting in *Chapter 14*, *Threat Intelligence Reporting and Dissemination*.

Threat intelligence feedback

The final step is a bridge between the dissemination and the initial phases. The benefactors, consumers, or target audience of the intelligence product evaluate and assess the project and mark it as successful or not. Their perspective determines the satisfaction index of the project as a whole. Only after or during the feedback step are actionable or business decisions made.

The intelligence authors' feedback and reviews can come in the form of acceptance criteria that are ticked as *OK* or *NOK*, in correlation with the input requirements. This feedback is then used as the initial objectives for the next CTI cycle's planning and direction phase. This is enriched with new requirements (probably new data sources), and then the project continues with its cyclic operation. *Chapter 14*, *Threat Intelligence Reporting and Dissemination*, provides a deep dive into feedback examples and how those examples can be converted into new requirements.

Summary

From this chapter, we can conclude that threat intelligence is not only a finished product but a seven-step process that needs to be understood and mastered to ensure the success of the CTI project. Intelligence must be conducted to support the consumer's vision. Hence, any organization that intends to integrate CTI as part of the business must carefully work through the intelligence life cycle and collaborate with the CTI team at each operation phase. Evidence must accompany each phase's decisions. Because CTI is a continuous process, the next intelligence cycle must primarily use the current cycle's feedback. The first step in planning and directing a threat intelligence project involves generating requirements and implementing an effective CTI team. The next chapter will tackle how to create intelligence requirements and position a team.

2
Requirements and Intelligence Team Implementation

The most critical parts of intelligence integration's first step (planning and direction) is the requirements and positioning of a competent, diverse, and multi-skilled team to perform different project functions. To minimize security risks, the CTI project team must focus on what the organization's needs are and prioritize them accordingly. An organization's security needs fundamentally involve protecting sensitive information (personal information), intellectual properties, assets, and any other information that, if released, would result in financial losses and brand reputation damage. Collecting and generating information must be tackled on all levels: strategic (strategic security requirements), operational (operational security requirements), and tactical (tactical security requirements).

This chapter focuses on the task mentioned previously – generating the requirements and building a CTI team. We will detail the methods and ways to generate intelligence requirements that are used to drive the project. This chapter also highlights the prerequisites for a threat intelligence program's creation by positioning a competent team and structuring their operations.

By the end of this chapter, you should be able to do the following:

- Generate intelligence requirements and prioritize tasks.
- Develop intelligence requirements for a specific cyber project using an advanced method adapted from the military intelligence approach.
- Understand the CTI team's layout and the required skill set to build a reliable intelligence team.
- Position the intelligence team in the security stack to maximize the intelligence program's value.

In this chapter, we are going to cover the following main topics:

- Threat intelligence requirements and prioritization
- Requirements development
- Intelligence team layout and prerequisites
- Intelligence team implementation

Technical requirements

For this chapter, no special technical requirements have been highlighted. Most of the use cases will make use of web applications if necessary.

Threat intelligence requirements and prioritization

When planning a CTI project, it is vital to define metrics, identify factors, and gather questions that need to be answered during the project. A CTI analyst or the threat intelligence team leader needs to collect the correct intelligence requirements from each business function to create a substantial project.

In the CTI scope, a requirement relates to any business area that needs cybersecurity monitoring or upon which intelligence should be applied. Requirements must relate to the various pain points of the organization or the information that needs protection. Hence, they can come from multiple sources, such as previous attacks, past data breaches, or peer organizations of the same nature (organizations in the same business line as yours or containing the same data). Hence, organizations need to join cybersecurity **Information Sharing and Analysis Centers** (**ISACs**) to benefit from their peer's experience. For example, when collecting intelligent requirements for a bank's CTI project, the CTI team might want to look at other banks' cyber history, breaches, and exposed or leaked information to consolidate the requirements document (understanding the security landscape). Let's look at some of the points that can drive the requirement phase:

- **Past threats and attacks**: If the organization was attacked in the past or experienced some kind of threat, it is vital to use this as an intelligence requirement. The security team should detail the types of threats or attacks that happened. The CTI team uses this information to build a requirement table. Typical questions that could be looked at include the following:
    - Have attacks been attempted on the organization?
    - How did the attacks happen? Did the attacker exploit system vulnerabilities? Or was another method such as phishing used?
    - How did the organization detect or prevent the attack?
    - What useful information did the organization extract from the threat or attack?

- **Actual system hacks**: The main action here is to know whether there has been any real hack or information leaks in the organization. The CTI project is well justified and holds a higher percentage of approval when an organization has been a victim of an actual hack or espionage. However, this does not mean that CTI is not justified if no actual hack has occurred as an industry risk profile can be used to justify the program. The CTI team (or analyst) works with the organization's security teams to answer the following main questions:

    - Has the organization been hacked before?
    - How did it happen?
    - What information was targeted?
    - Who was the main actor or the adversary in the CTI scope? Was the attack automated or manually executed?

  The internal security team must provide such information to the CTI team to tailor the intelligence project.

- **Existing breaches**: Prevention is better than a cure, so they say, and that is true. The CTI analyst (or team) needs to know and understand breaches (that have occurred or are occurring) in the industry. The security manager might want to be aware of the potential vulnerabilities that could impact the organization as well – this includes the vulnerabilities and threats that the organization has no defense mechanism against. This requirement approach leans toward proactive threat intelligence. The CTI team must progress the project by answering the following questions:

    - What vulnerabilities are currently being exploited globally and industry-specific (industry threat landscape)?
    - Have there been breaches that are globally and industry-specific? How recent are the breaches and to what extent?
    - What vulnerabilities and breaches can the organization defend against or detect using the current status of security?
    - What prospective threats and vulnerabilities are currently under research? It is also important to understand the vulnerabilities that are being looked at by cybersecurity researchers to stay ahead of adversaries. This includes reports from academic and professional security research lab.

- **Possible indicators**: When generating the requirements, the CTI team needs to understand the organization's current state of security. For example, for breaches that happened in the past, it is crucial to evaluate the existence or absence of any indicator (or mechanism) that could have prevented or detected the incident. Also, summarize the organization's available security indicators. The CTI analyst and the internal security team can use the following questions to drive the requirements:
    - What indicators are available in the organization's security system?
    - Can those indicators prevent the existing common threats or past breaches?
    - Is there a need for more indicators to strengthen the current system's security?
- **Security measures**: This is a separate but continuous requirement parameter used to evaluate the current state of security. The CTI analyst must work with the organization's security team to identify, understand, and assess the existing security protocol (incident response, risk assessment, system audit, malware analysis, and so on). Once the security protocol and measures have been considered, the CTI team must correlate the steps with past (or existing industry) breaches. The CTI analyst (or group) and the organization's security team must then answer the following questions:
    - Was the organization's security protocol effective at detecting or preventing past attacks?
    - Was the protocol accurately followed to mitigate the attack or respond to past incidents?
    - Were there security measures that were not followed during the incident?

The global questions mentioned here act as the main drivers for the first step of the intelligence project life cycle. They also define the kinds of data collection that will be needed in the next chapters. The following table provides an example of an intelligence requirements global spectrum to help define the intelligence project. It also shows how the intelligence requirements can be answered and used to shape the cycle's data collection step. The CTI team and the internal team should use this template to collect global and specific intelligence requirements. The method facilitates assigning tasks to the team:

CTI requirements (in the form of a question)	**Prospective answer**	**Collection requirements (example for future steps)**
Have attempted attacks happened in the organization?	Yes or no.	Check past security, networks, intrusion detection logs, and so on.
How did the organization detect or prevent the attack?	Firewall policies, deep packet inspection, intrusion detection and prevention, and so on.	Collect the relevant logs to understand the policies, rules, and so on.
What useful information was extracted from the attack?	Adversary details: origin (region), IP addresses, domains, attack model, and so on.	Collect the relevant logs.
Which vulnerabilities are being exploited globally?	Password brute forcing, phishing (social engineering), ransomware, and so on.	Collaborate with other organizations or other CTI analysts. Refer to online platforms to get information on those vulnerabilities, and so on.
How the organization been hacked before? How did it happen?	Yes or no. Through phishing. An HR executive opened an attachment from a malicious email who pretended to be an employee.	Refer to malware analysis, opensource feeds of malicious web links, emails, and so on.
What prospective vulnerabilities and threats are under research?	Crypto security, identity theft, high-level espionage, and so on.	Refer to online forums, the dark web, and so on.

Table 2.1 – CTI requirements – main questions

Extracting the right requirements can be challenging as several organizations are still reluctant to embrace threat intelligence technology. However, working with the organizations' management teams or decision-makers is key to an intelligence project's success as they know the business. Therefore, they should help prioritize the requirements. It is essential to follow previously discussed protocol (involve the organizations' relevant parties). In cases where the prerequisites have been defined by the CTI team only, the chance of failure augments. The intelligence requirements' primary objective should be to ensure that no discrepancy exists between the program's end product and the organization's security needs.

Important Note

A persuasive first draft of intelligence requirements must always start with closed-ended questions. Open-ended questions can be used to justify or sustain a closed-ended one. For example, it is essential to start with a question such as *Have the company been attacked before?* Rather than *What system resource has been attacked in the past?* The second question should be a supporting argument for the first: the more closed-ended questions, the better.

In this subsection, we have learned how intelligence requirements can be formulated in questions and why it is vital to have them in place. The answers to these requirements questions constitute the initial steps to be taken in any threat intelligence project.

Prioritizing intelligence requirements

Prioritizing intelligence requirements is as important as gathering (or collecting) them. Understanding the most critical questions to be answered by the CTI project helps structure the operations. There are several methods we can use to prioritize the requirements, but they should all be based on common ground – critical asset and sensitive data protection. After developing the base questions, the CTI team must create a list of short-, mid-, and long-term requirements that must be addressed accordingly.

Short-term requirements

Short-term requirements need an immediate lookout and should be tackled in the most minimal time possible. A typical example would be identifying threat actors directly targeting the organization's main assets. This type of requirement should be a high priority and looked at immediately. Short-term requirements include asking questions such as, *Is there a group planning to attack the ABC insurance company after the recent protest against the new policies?* Or *Has there been a group that attacked the ABC insurance company after demonstrations against a specific policy?* Such questions should be a high priority if the organization senses danger in the matter.

Could a group of unhappy people be a threat to the organization? Let's analyze to what extent this can be categorized as a threat:

- **The intent**: Do they have an intent? The answer is *yes*. After the company's debatable policy, the group has a *purpose*. The confidence level to classify such an action as the intent is *high*.
- **The capability**: Do they have the capability to compromise the organization? This capability can be acquired. Hence, the answer is *yes*. However, we must take into consideration the required budget to outsource capabilities. Therefore, the confidence level of classification ranges from *medium* to *high*, depending on their resources.
- **The opportunity**: Do they have the opportunity? The answer is *yes*. Since there is a complaint against the company, it is enough motive to orchestrate a cyber attack. The confidence level is *high* as the actions can be justified.

After the preceding analysis, the group can be considered a threat to the ABC insurance company. The CTI team must directly identify and select indicators to facilitate the monitoring of such a threat (or threat actor or adversary). We will see how threat intelligence frameworks (such as the MITRE ATT&CK or Cyber Kill Chain) can be used for such purposes in *Chapter 4*, *Cyber Threat Intelligence Tradecraft and Standards*, and *Chapter 5*, *Goals Setting, Procedures for CTI Strategies, and Practical Use Cases*. And finally, use the requirements and the indicators to implement an action plan, thereby improving the security protection, or ask for help from law enforcement if there's a lack of adequate resources to single-handedly deal with the threat. The concept is known as **Prioritized Intelligence Requirements** (**PIRs**). This example can be modeled, as shown in the following diagram:

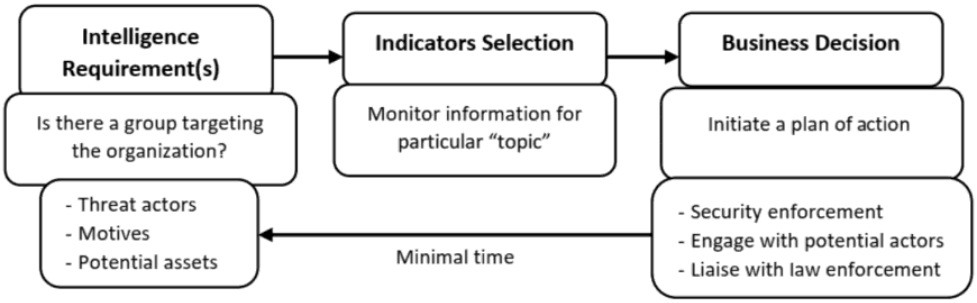

Intelligence Requirement(s)
Is there a group targeting the organization?
- Threat actors
- Motives
- Potential assets
Indicators Selection
Monitor information for particular "topic"
Business Decision
Initiate a plan of action
- Security enforcement
- Engage with potential actors
- Liaise with law enforcement
Minimal time

Figure 2.1 – Prioritized intelligence requirements

PIRs are characterized by the top priority tag as it helps the management team and other strategic units to understand the severity of threats in a simple way. Now, let's look at mid-term intelligence requirements.

Mid-term requirements

Mid-term requirements are intelligence requirements that are not currently critical but can be a security concern in the near future. Not being critical does not make mid-term requirements less necessary. However, a CTI analyst needs to categorize these requirements. For example, the ABC insurance company has effectively contained the critical threat and has not been a victim of such adversary harassment for some time. After a while the adversary has been reported to have changed their **tactics, techniques, and procedures** (**TTPs**). To avoid any security surprises, ABC insurance's CTI team should continuously identify such requirements, set the appropriate indicators to monitor potential changes in the TTPs, and then initiate a plan of action. This concept is referred to as **specific intelligence requirements** (**SIRs**) and is illustrated in the following diagram. These requirements can wear a *major* or *medium* tag on the priority scale:

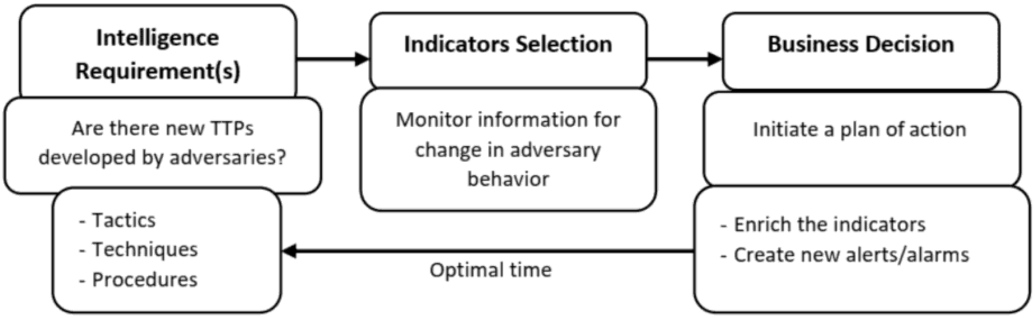

Intelligence Requirement(s)
Are there new TTPs developed by adversaries?
- Tactics
- Techniques
- Procedures
Indicators Selection
Monitor information for change in adversary behavior
Business Decision
Initiate a plan of action
- Enrich the indicators
- Create new alerts/alarms
Optimal time

Figure 2.2 – Specific intelligence requirements as a mid-term goal

Mid-term requirements also answer the future questions of process automation, **Indicator of Compromise** (**IOC**) handling, enrichment, and integrating new data sources to ensure that the threat intelligence program is up to date. Mid-term requirements are essential in keeping and developing a solid intelligence team.

Important Note

In cases where SIPs are used to break down a PIR, it automatically changes to a critical priority. We will look at how SIP supports PIR in the next section. It is vital to understand the impact of a requirement before classifying it.

Therefore, major or medium tags characterize SIPs, and they must always align with PIRs. Now, let's look at the long-term intelligence requirements.

Long-term requirements

Long-term requirements are used to ensure far-future protection. CTI is conducted for the organization, not for the analyst or CTI team itself. Hence, it is essential to look beyond the current horizon and project threats and security risks into the extended future. The priority of long-term requirements depends on the CTI team and the internal security teams. These requirements are more general to the organization's environment. Although they are used in a lower priority category, they are the foundation of PIRs and SIRs. These requirements answer the following general questions:

- Will there be a threat to the organization we should know about (perhaps after a future business expansion)?
- Are there internal threats targeting the organization?
- Are there known threats targeting the related industries?

Such threats target insurance companies in general. We can directly see that the question that was asked regarding short-term requirements or PIRs is directly linked to the general requirements' first question.

In this subsection, we have learned about the importance of prioritization in intelligence projects. We mentioned that prioritization allows us to tackle security based on its direct impact on the organization. Another popular method of prioritizing intelligence requirements is ranking the requirements using the *high*, *medium*, and *low* priority scales.

In this section, we have learned how to generate global questions that drive the intelligence requirements step. This section has also summarized the effective methods we can use to prioritize intelligence tasks by introducing general, prioritized, and specific requirements. Throughout this section, we have highlighted the collaboration between the CTI analyst (or team) and the organization security teams (more details will be provided in the *Intelligence team implementation* section, later in this chapter).

Requirements development

This section tackles how to develop the intelligence requirements that are overlooked by the industry's CTI matured corporations and training providers – including SANS, IBM, and so on. It relates to the US military's approaches to intelligence planning direction, and requirements generation. Intelligence requirements questions must target all three CTI integration levels (strategic, operational, and tactical) with a single potential problem. A question such as *What organization functions are at the forefront of cyber attacks?* needs to be addressed at the strategic level of intelligence, requiring the full collaboration of the organization's decision and policymakers. However, a question such as *What are the active threat actors in the business industry?* is more of a technical problem that needs to be addressed at the operational level of intelligence and also requires the technical team's collaboration. Finally, a question such as *What adversary tactics are likely to compromise the organization?* is a type of question that involves security tactics, requiring the tactical team's collaboration.

Any organization's team in the security scope should contribute to the intelligence requirements as the organization is the primary consumer of the intelligence product. The requirements are developed using the **Intelligence Preparation of the Operational Environment** (**IPOE**). The IPOE is a four-step process used by organizations to analyze potential threats and other malicious behaviors toward them, as shown in the following diagram:

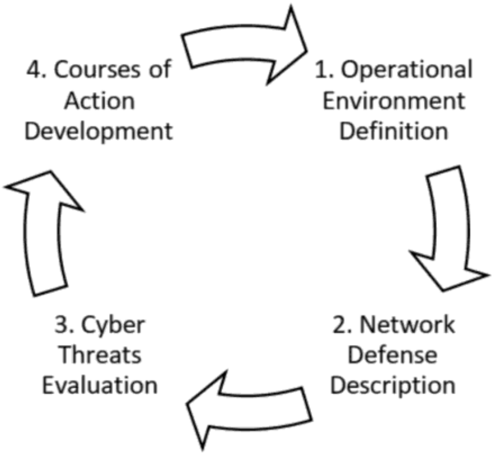

4. Courses of Action Development
1. Operational Environment Definition
3. Cyber Threats Evaluation
2. Network Defense Description

Figure 2.3 – The intelligence preparation process (IPOE)

The internal security team must use this process to sustain the intelligence project – the latter sits on top of the current security infrastructure. The process provides a full landscape of the security infrastructure. Hence, its presence is crucial for developing an intelligence product. One of the process's key outputs is **PIRs** and data collection planning. In the upcoming sections, we will look at each of these steps in detail, as well as how they are used to prepare intelligence requirements.

Operational environment definition

Threat intelligence is built on top of the existing IT infrastructure. The CTI team needs to work with the internal team to define the security operation's span, particularly the executives or the decision-makers. Understanding the operational environment is critical to building intelligence and identifying the system characteristics that can impact the organization's defense system.

After completing the first step of the preparation phase, the CTI should have a clear and concise physical and logical definition of the system to defend (also known as the *area of operation*) and the different parts of the system that are used by adversaries to orchestrate malicious actions (known as *area of interest*). The area of interest includes the company's assets, relevant features, and threats that directly impact the defense structure. Operational controls for the secure information infrastructure are provided by standard frameworks such as NIST 800-53 (`https://bit.ly/3wtMtVV`), ISO 27002 (`https://bit.ly/3un6s6O`), and NIST CSF (`https://www.nist.gov/cyberframework`). The area of operation and the area of interest generate a certain number of characteristics that influence the business, highlighting the gaps in the current security systems.

The deduced characteristics and the identified gap will be translated into intelligence requirements, facilitating the intelligence cycle's planning and direction step. At this stage, the CTI team estimates the preparation efforts and pinpoints the area of interest that could provide the best sources of information to construct the intelligence requirements. For example, by identifying the area of operation and interest, an intelligence analyst should know the following:

- The information (such as logs or open-source data) that's used by the security team to detect, assess, and analyze threats
- The organization's resources (processes, tools, and people) that are destined for security improvement
- The gap in the security infrastructure
- Where to find any information in the organization's security landscape

The expected operational environment information template is illustrated in the following table:

Physical	**Logical**	**Regulatory**	**Natural**
Business model and scope	Offices connections	Regulations and policies	Natural catastrophes
Business and risk priorities	VPNs and VPN providers	Standards and tradecrafts	
Expansion plan	Domains owned		
	Cloud services (private and public)		
	Third-party systems		
	Internet service providers		

Table 2.2 – Operational environment preparation information

The CTI analyst must ensure that the organization's strategic team defines the information shown in *Table 2.2*. At the physical level, the executive board must determine the business model (answering the question, *What kind of business is the organization involved in?*). The entire business landscape must be defined to prepare the operational environment information properly. In conjunction with the technical team, they must also provide a risk priority scope (by answering the question, *What is the most prominent business risk?*). If there is an expansion plan, it must be defined and shared with the CTI analyst (or team). At the logical level, the executive team must define factors such as offices/branch connectivity (*How are the business parts logically connected?*). They must tell us whether the organization uses a VPN and name the service providers. They must define the scope of owned domains, the use of private or public cloud services, and any third-party company used in the security scope.

The regulatory and natural characteristics that directly impact the security system must be identified as well. The CTI analyst must correlate the intelligence product to the regulations and catastrophic obstacles. A typical example is defining the state's position or standards in cyberspace, as well as specifying the organization's geographic constraints (an earthquake region or rugged terrain). These characteristics influence the organization's defense system.

The CTI team will have a full landscape of how the business operates, and they can identify new security gaps and create an efficient requirement priority list.

Network defense impact description

The next step of preparing the operational environment involves understanding the network topology. The network topology is a significant parameter of the network's defense system. The intelligence analyst must analyze the network topology to understand how the defined characteristics in step 1 (*operational environment definition*) impact the business operation. This step aims to obtain the network topology, the network's key nodes, the network's key information, the potential threats' paths, and the detection points. A defense mechanism must protect a system against all types of threats, regardless of whether they're internal, external, or natural. While several organizations focus on external threats, internal and natural ones can be the most dangerous (in the sense that recovering from them could be difficult or even impossible). Let's examine the following scenarios:

- Imagine that an employee or a contractor who has access to the organization's sensitive data intentionally attacks the system. The defense system can become powerless in such a scenario. The attack success rate will be higher than a cybercriminal trying to attack the system remotely.
- Imagine a software engineer who unintentionally releases an application with security flows – sometimes due to poor coding skills. Such cases reduce the system's defense strength.
- Imagine that fire has started inside a data center, where servers contain the company's critical business data, or an earthquake has destroyed the entire data center. This is another scenario that renders the defense system powerless.

Examples are legion, but by referring to the preceding three scenarios, we can see that internal and natural threats should not be taken lightly. In most cases, external threats are global but efficient since skilled cybercriminals orchestrate them with different and diverse motives. The defense must take precautions against external threats such as the competitor's espionage, hacktivists, extortionists, and so on. The analyst drafts a simple threat description table, as shown in the following table. This table provides a simple template that describes the different threats that influence the defense mechanism.

> **Important Note**
>
> The template information in *Table 2.3* is non-exhaustive. The CTI and the internal team must generate a comprehensive, exhaustive list of threats. If this step is well executed, the threat modelling phase will be smooth.

The CTI analyst must collaborate with the technical team to create a threat description. This is based on past threat history, industry threat news, or open-source intelligence. The threat description table is one of the principal inputs in threat modeling (covered in *Chapter 6*, *Cyber Threat Modeling and Adversary Analysis*):

Threat type	Threat name	Description	Outlook
Internal	Malicious insider	**Opportunity**: anytime since he/she has access **Capability**: uses internal tools (same access as admin, for example)	**Intent**: angry at the company or a manager
	Unintentional insider	**Opportunity**: anytime since he/she is part of the organization. **Capability**: lack of skills or attention opens the door to outside attacks	**Intent**: no direct intent but might not use security practice methods – which is considered as intent to harm the organization
External	Corporate espionage	**Opportunity**: any opened door will be an opportunity. **Capability**: very skilled or outsource the skills	**Intent**: to steal business secrets and strategies. Access IPRs, and so on.
	Foreign espionage	**Opportunity**: any opened door will be an opportunity. **Capability**: very skilled, and resourced, or outsource the skills	**Intent**: to steal business secrets, sensitive information, and sell them to third parties or competitors.
	Hacktivists	**Opportunity**: any opened door will be an opportunity (they can be anywhere) **Capability**: they are skilled but may be unstructured.	**Intent**: to deliver a message or get back to someone or an organization.
Natural	Earthquake/fire	**Opportunity**: anytime based on nature **Capability**: physically destroy the infrastructure	**Intent**: no direct intent. But indirect natural phenomena

Table 2.3 – Threat description table (non-exhaustive list)

The CTI analyst must also request a physical map of the entire system that displays the network's main components. The objective is to analyze the network's defensive features from the topology – including, but not limited to, networking devices and management tools, system devices (end-user stations), software, and critical information. The most critical parts of the network topology that the analyst must look at are as follows:

- Components that filter, allow, deny, degrade, stop, or quarantine system traffic from reaching a destination – elements such as firewalls, IDSes, IPSes, ACLs, web proxies, and so on. These components are also referred to as *network obstacles*.
- Routes to the destination; that is, paths that traffic follows from a specific source to a particular destination. Highlighting these traffic routes will help the analyst understand and predict a potential threat's mode of action. It is known as the **avenues to approach** (**AA**).

- Network components with the capability to manage the traffic flow, inspect packets, and detect anomalies in the network traffic – elements such as domain controllers, deep packet inspectors, and central log servers.
- Critical information, that is, the data that needs to be protected at all costs. This includes trade secrets, IPRs, business plans, and strategies – information that criminals want (also known as *key information*).

By evaluating the network topology, the CTI team will assess the network obstacles' position and their impact on the traffic paths to get a deep understanding of the security landscape and possible points of threat detection. A network's typical high-level topology or architecture is shown in the following diagram:

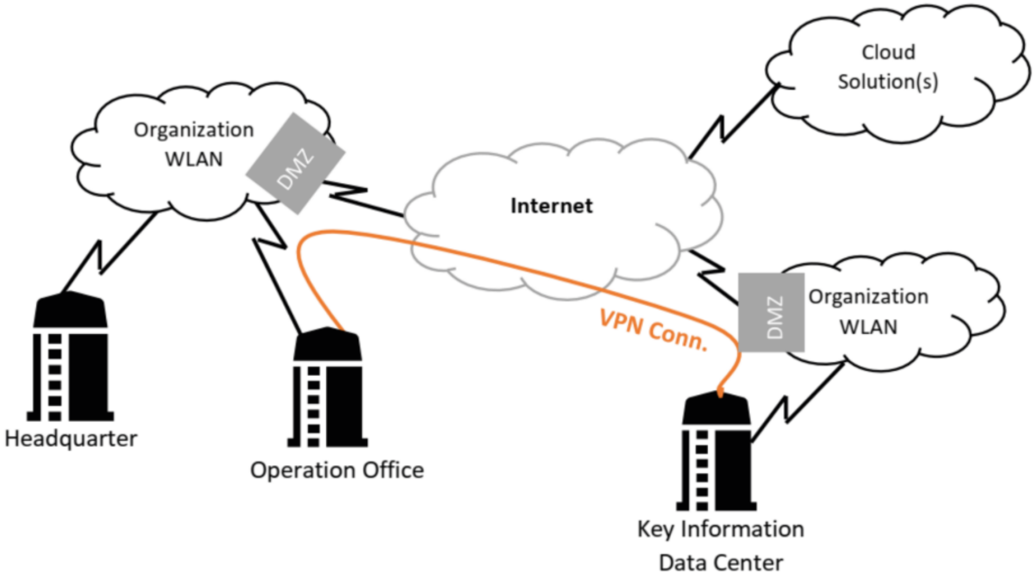


Figure 2.4 – High-level network topology

This topology shows how the organization's functions interact with each other and with the internet. If there are cloud services, it also shows the connection to them. Another important task in understanding network defense is to acquire a high-level security obstacle architecture and the key nodes that are protected, as shown in the following diagram. This is built on top of a high-level architecture:

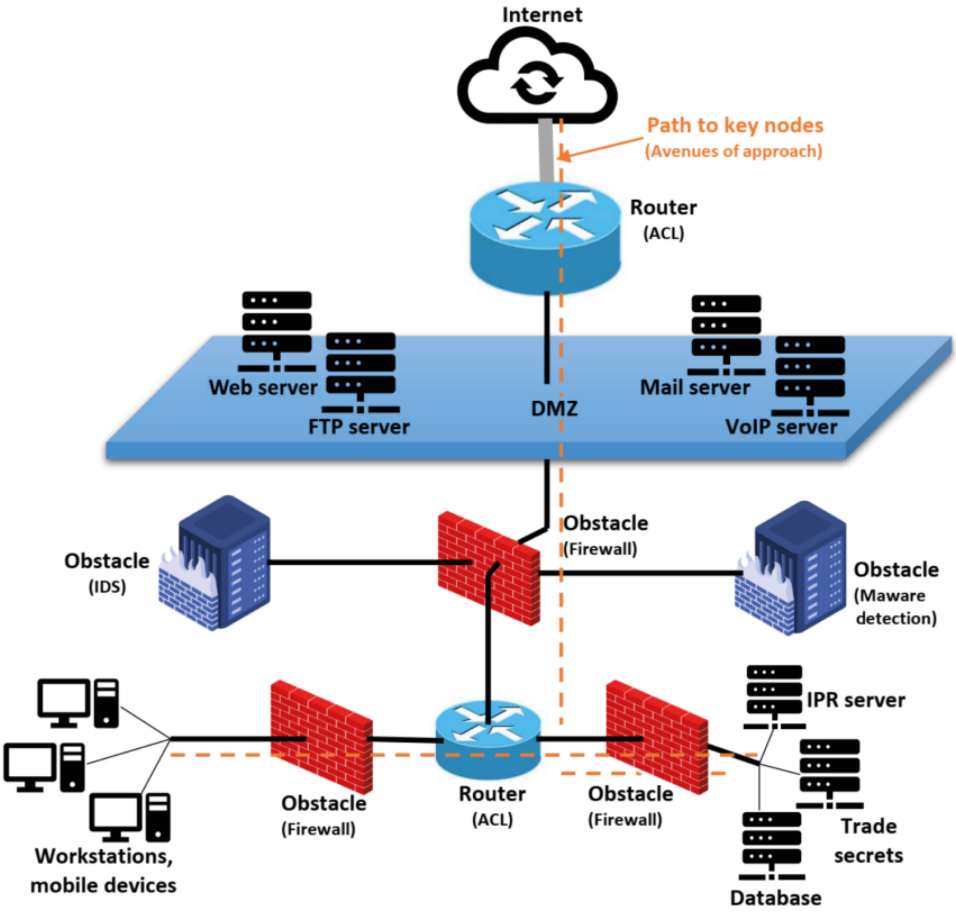


Figure 2.5 – Security obstacle architecture

The security obstacle architecture allows the analyst to overview what is protected, which obstacles are used to protect the key nodes that contain key information, and understand the path that a potential threat will take to compromise the defense system and access the key nodes. The internal team must provide information such as how often the key nodes' software is patched, as well as which **operating systems** (**OSes**) are used on key nodes, to help build intelligence on the specific OS threat.

While many accents have been put on the network components, the analyst needs to understand the impact that users, employees, and contractors have on the security defense system. The analyst must assess the cybersecurity education level of the personnel; for example, developing an Excel template of the security users and their level of education. This data will be used to plan and direct intelligence – particularly when monitoring user behavior.

In this subsection, we described the influence network defense has on security. We detailed the different information that an analyst or the CTI team must possess to develop intelligence requirements.

Current cyber threats – evaluation

The next step in the preparation process involves evaluating threats. In this step, the analyst, along with the internal team, uncovers the different TTPs used by threats to attack the system. Critical threats should be evaluated to determine the extent of the compromise. This step aims to simulate the operations of past cyber threats and their mode of propagation. If the internal security team possesses past threat models, they must share those with the CTI team (or analyst) so that they can use them during the project's intelligence threat modeling phase. The CTI team extracts the characteristics of the threats to help develop the action plan. More details are provided in *Chapter 6*, *Cyber Threat Modeling and Adversary Analysis*.

Past threats and historical data should be classified based on their capability to attack the defense system. A summary of threat capabilities is shown in the following table:

Threat capability	Capability category	Category classification
Attack: threats that attack and compromise one of the CIA	• **Deny**: threats that compromise the system availability	• **Destroy**: threats that compromise the availability entirely. • **Degrade**: threats that compromise the availability to a certain extent (showing the system) • **Disrupt**: threats that compromise the proper running of the system.
	• **Manipulate**: threats that compromise the system integrity	
Collect information: Threats that steal personal and sensitive information	**Credential harvesters**: threats that access and collect sensitive information	• **Insider collector**: threats that steal information by intruding the target system. For example, social engineering • **Outsider collector**: threats that steal information without intruding on the network. For example, open source intelligence.

Table 2.4 – Threat capabilities

The malware analysis result is essential in this step for evaluating and understanding past threats. This subsection has briefly described the information needed to set up proper intelligence requirements through threat evaluation.

Developing a course of action

The last step of preparing the operational environment includes the threats' span of behaviors that directly impact the organization's security system. There are several expectations from the current stage. One of the most essential is the event matrix, which generates security statements for the intelligence requirements. To develop a practical threat course of action, the analyst must understand its characteristics (detailed in the previous steps) and the related network topology.

Once the threats' courses of action have been developed, the analyst and the internal team can prioritize these threats, insert them into the event matrix, and then use this as input to the intelligence requirements and prioritization task.

At the end of this step, the analyst and the internal team will have an understanding of the security landscape and how threats are likely to compromise the system. Given a threat and its characteristics, the analyst should be able to overlay the network topology and anticipate the extent to which it can impact the system and its defense mechanism. For example, a polymorphic threat can assess and exploit vulnerabilities in the database's configuration, harvest credentials, achieve persistence in the target system, or use the harvested credentials to log into unauthorized subdomains or networks. Once the analyst determines all the courses of action for such a threat, they can prioritize the methods of action, such as sensitive information access (*critical*), database injection (*critical*), persistence (*major* or *medium*), and so on.

Intelligence preparation for intelligence requirements

At this stage, we assume that the security team and the CTI analyst have adequately prepared the operational environment, have understood the security landscape, and all the necessary details to position any threat in the defense system. They can then develop the intelligence requirements and select indicators required to build the CTI product. The preparation process simplifies the requirements into two tasks: *validating* or *denying* a threat's course of action. The intelligence requirements must be backed up by the four previous steps' output (operational environment preparation, network defense impact description, current threat evaluation, and courses of action development) as it is submitted to the strategic team for approval. The event matrix and the developed intelligence requirements templates are shown in the following tables:

Detention points (need to know the network topology)	**Indicators (selected from the characteristics of the threat)**	**Course of action**
Enter the detection point as per the network topology	Specify the indicators: For example, IDS alerts, antivirus alerts, HTTP requests to malicious destinations, malware signatures	Detail the courses of action

Table 2.5 – Event matrix example

The analyst and the internal team use *Table 2.5* and *Table 2.6* to fill all the requirements in the form of questions. They must include all the aspects of the security landscape, as approached in the preparation phase – software and hardware questions, network changes, vulnerabilities, TTPs, groups, people (internal and external), and other industry threat questions:

Intelligence requirements	**Prioritized intelligence requirements**	**Specific intelligence requirements**
Are these groups or threats that can attack the organization?	Who are the groups (threats, adversaries) that are likely to attack the organization?	Are there internal or external threats that have attempted to access prohibited business sectors?
		Are there emails coming from suspicious sources to the internal domain? What are those threats?
		Are there people on social media talking about attacking the organization? What are those threats?
Do the groups targeting the organization have TTPs or capabilities to compromise the organization?	What are the capabilities and TTPs used by threats or groups targeting the organization?	Are there known TTPs that may be used against the organization? What are they?
		Are there malicious domains mirroring the organization? What are they?

Table 2.6 – Detailed intelligence requirements

In conclusion, this section has tackled the first step of the planning and direction phase of the CTI cycle. The section has described how to develop intelligence requirements using the operational environment's preparation effectively, a method used and introduced by the US army to plan and direct intelligence on the battlefield. This process has been adapted and adopted to cyberspace by several organizations.

Intelligence team layout and prerequisites

The CTI team is responsible for the intelligence project or product implementation. It supports internal security functions for analyzing and collecting massive network data. Hence, a CTI team must be made up of professionals who can collect, analyze, and make sense of threat data to produce actionable intelligence at the strategic, technical, and tactical levels. The following are the essential prerequisites for the CTI team, based on what we learned earlier and the industry's intelligence analyst requirements:

- *A CTI analyst must know all the intelligence types*; that is, strategic, operational, and tactical. Although we mentioned these in the previous sections, the next section provides a summary of each intelligence type.
- *A CTI analyst must be familiar with most of the industry-leading intelligence tools, platforms, and methodologies*. It is practically impossible to know all the vendor-specific intelligence platforms by heart. However, a CTI analyst must possess those platforms' global functioning principles because intelligence platforms function in a similar fashion, including, but not limited to, data collection and support, processing and analysis, reporting tools, statistical and malware analysis tools, threat sharing platforms, and so on. Platforms will be covered in the next chapter.
- *A CTI analyst must know where to find intelligence data and be able to collect it*. An analyst must be familiar with tools such as Google Hacking, Shodan Engine, DNS querying, web crawling, and a few counterintelligence skills. Therefore, they must have good data acquisition and collection capabilities. We will cover this in *Chapter 7*, *Threat Intelligence Data Sources*.
- *A CTI team must analyze internal and external data and produce useful intelligence to help the organization make business decisions*. Therefore, CTI analysts need to have a strong analytical background. They should know the industry-leading threat analysis platforms as well.
- *A CTI analyst must be able to convey intelligence through transparent and professional reports*. Therefore, they must have good writing capabilities.
- *A CTI analyst must be able to inform the organization of any threats* – including current, prospect, and zero-day – that the company could be vulnerable to and how to protect themselves against them. Therefore, they must have a good sense of research and be able to work independently.

One of the key prerequisites of a CTI team is *diversity*. CTI projects require different views, opinions, or interpretations of intel to have a reliable product. Analysts must be able to bring new ideas to the team. Hence, it is crucial to not only focus on technical abilities but also cognitive, innovative, and thinking-outside-the-box abilities. Diversity is essential in eliminating bias in product interpretation. When planning and forming a CTI team, it is imperative to consider the analyst's practical and hands-on aspects. An analyst should have a strong theoretical background and a sufficient practical education, as shown in the following diagram:

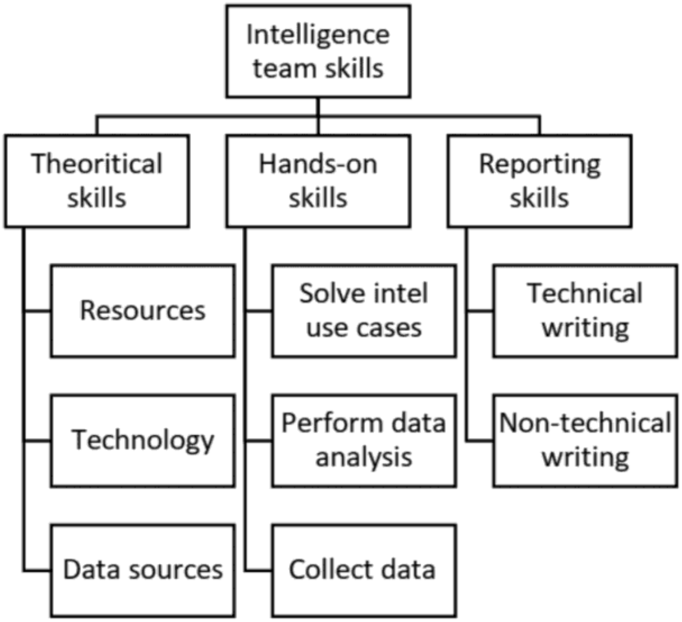


Figure 2.6 – Intelligence team skills layout

This section has described the global prerequisites for constructing a CTI team. We have detailed the essential skill set required to acquire proficient intelligence analysts for a CTI project. Note that the CTI project manager can add any other relevant skills or capabilities.

Intelligence team implementation

Setting up a robust intelligence team is critical for the CTI program success. But positioning the team facilitates the direction of the entire program As mentioned earlier, threat intelligence is built on the existing security system. After understanding its operation, the area of interest, and generating the intelligence requirements, the CTI manager must identify which security function the intelligence team will support the most. In this section, we will look at two things: how to structure (position) the intelligence team and what types of intelligence the organization envisioned.

Intelligence team structuring

The CTI team's position in how the organization functions will determine the scope of its application. Because CTI analysts have profound and diverse security knowledge, it is essential to place the team in the security system's heart. This is to ensure that every function extracts value from CTI. The following points can justify the team's security system position:

- *The CTI team will work with the incident response team* to analyze, prioritize, and enrich indicators to control and contain threats. An intelligence analyst benchmarks the indicators against the requirements and can propose new indicators to strengthen the incident response platform.
- They facilitate the distribution of threat data in the organization. CTI can be a public process as well. Therefore, *the intelligence analyst can help share the data externally and collaborate with other analysts outside the organization*. We must emphasize the importance of joining threat intelligence sharing centers or **ISACs**.
- The executive team uses intelligence analyst products or outputs to make business decisions, such as optimizing the system's infrastructure and reducing security costs. Hence, *the CTI team must also be closer to the organization's strategic function*.
- *The team works with the SOC team to identify risks and vulnerabilities that are critical to the business and monitor the security system's behavior*. During CTI product (project) development, good threat modeling equips the SOC team with threat information that they did not have before.
- Because the CTI team provides in-depth intel on threats, as well as current and prospective malware trends, *malware analysis is one of the functions that benefit the intelligence team*.

- *The CTI team supports network forensics and threat management units to help identify, collect, and prioritize cyber evidence that can be used for different purposes.* Because CTI has a broader span of threat knowledge, the forensics function can use the intel product to create a proactive test method.

The following diagram shows the structure and position of the intelligence team in the organization security unit (risk management and vulnerability management can also be separated into two different teams):

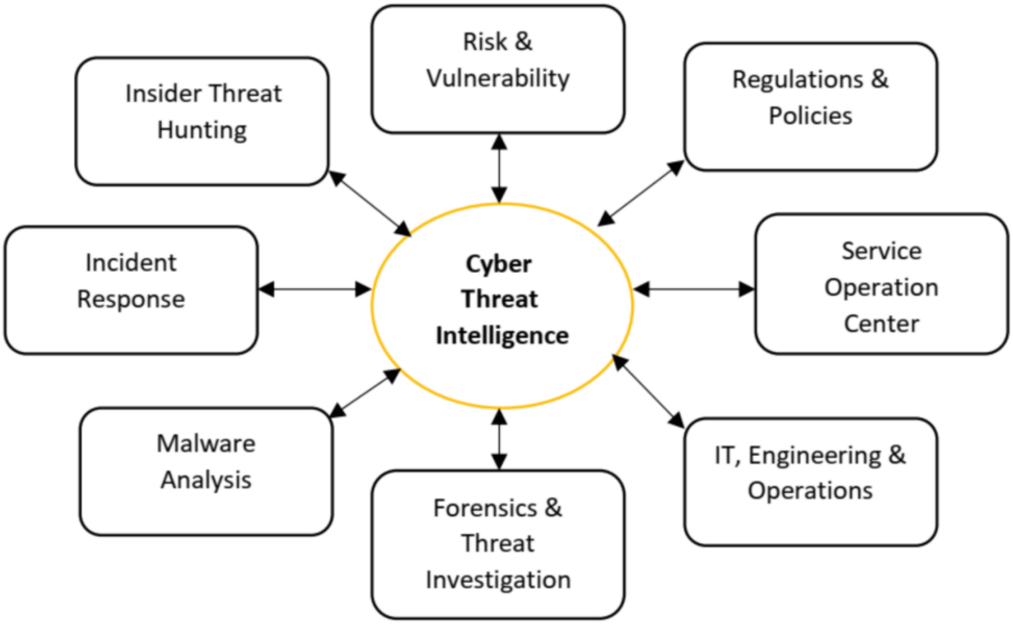


Figure 2.7 – Recommended threat intelligence position in the security landscape

The *central position* is recommended for reasons mentioned earlier, but depending on the executive's intelligence vision, the team can lean toward any security functions. In that case, it will work closely with that specific function to provide intelligence and improve the security stance.

Intelligence team application areas

There are three application areas in which intelligence can operate in a business. These are also known as types of intelligence or intelligence levels: tactical, operational, and strategic. A few characteristics of these three areas have been mentioned in previous developments:

- **Strategic intelligence**: Strategic intelligence is the intelligence that focuses on high-level, non-technical decisions. A strategic intelligence analyst works directly with the executive team of organizations. Therefore, they must have a global understanding of the security and threat trends, adversaries, and their impact on defensive systems. The analyst then uses that knowledge to influence business decisions. Hence, the strategic intelligence's main stakeholders include the executive board, the CTO, the CISO, and the CIO. These are the owners of the intelligence product. They make every decision.
- **Operational intelligence**: Operational intelligence is the intelligence that focuses on adversaries and cyber attacks. It is an action-based type of intelligence that concentrates on understanding, replicating, and analyzing adversaries, threats, and actual attacks. Therefore, an operational intelligence analyst must be able to isolate threats and attacks, detail their courses of action, and orchestrate prioritized and targeted operations. An operational intel analyst's activity scope includes threat hunting, vulnerability and risk assessment, incident response, and so on. This type of analyst is considered the front driver of intelligence.
- **Tactical intelligence**: Tactical intelligence is the intelligence that looks at the TTPs of selected threats and adversaries and their relevant **IOCs**. Activities such as malware analysis and indicator enrichment are part of tactical intelligence. The tactical intelligence analyst must ingest threats' behavioral data and indicators to defend the system properly. Some main components and stakeholders for tactical intelligence include SOC analysts, **Security Information and Event Management** (**SIEM**), IDS/IPS, endpoints, firewalls, and so on. Tactical intelligence should also use the pyramid of pain to visualize the types of indicators to be used for adversary activity monitoring and evaluating the pain that the latter need to confront to keep up with the defense system.

> **Important Note**
>
> Some CTI course providers and researchers break tactical intelligence into tactical and technical intelligence, where the TTPs and their relevant scope are assigned to tactical intelligence and indicators and their applicable scope are assigned to technical intelligence. You should not be confused if another manuscript defines four intelligence areas or categories.

From the preceding explanation, we can anticipate that a complete CTI team must have the skill sets of these three areas – they must have one or more tactical intelligence analysts, one or more operational intelligence analysts, and one or more strategic intelligence analysts. Now, we can conclude with the following:

- **A tactical intel analyst must possess one or more tactical security skills**:

  They must have good knowledge of the SOC and SIEM. They must understand the operations of network obstacles (firewalls, IDSes, and IPSes) and end-user stations. SOC analysts, network security engineers, network defenders, and defensive security professionals (generally) are examples of tactical intelligence profiles.

- **An operational intel analyst must possess one or more operational security skills**:

  They must know how to conduct threat hunting and penetration testing. They must know how to respond to security breaches and other incidents and must be able to track adversaries both internally and externally. Penetration testers, hackers, forensics investigators, SOC analysts, and offensive security professionals are examples of operational intelligence profiles.

- **A strategic intel analyst must think like a strategic stakeholder (or an executive)**:

  They must have a global vision of everything. They must, for example, understand the global threat market (through reports, magazines, and so on) and the cost of a data breach (this is essential for the intelligence project as it indicates the possible causes and consequences of different data breaches). An information security officer is an example of a strategic intelligence profile.

Summary

This chapter covered threat intelligence requirements and their prioritization. It also detailed the most effective methods for developing intelligence requirements using a military approach known as the IPOE. Lastly, we tackled how to construct an intelligence team by laying out the required skills and structuring the organization's security system by selecting the right profile for the CTI team.

The second crucial step in the planning and direction phase of the intelligence cycle is selecting the platforms and tools for the intelligence project. Therefore, the next chapter covers various intelligence frameworks, how they can be used to produce an intelligence product, and how to select the appropriate framework for the tasks that have been defined.

3
Cyber Threat Intelligence Frameworks

Organizations are filled with security tools from different vendors for different tasks. You will likely find one tool that performs vulnerability assessment, another that serves malware analysis, and an additional tool for fraud detection and data monitoring. Even an average organization has a good arsenal of security tools because most of the time, the strategic team acquires new tools as the needs manifest. However, if they're not integrated appropriately, those tools can create a complex ecosystem that makes security tracking difficult. Such resource chaos not only slows the response effectiveness to threats; it also makes it difficult to justify the **Return On Investment** (**ROI**) of the entire system.

This chapter focuses on common threat intelligence frameworks, selecting the appropriate one for the CTI project, and how they can be used to build intelligence. We will expand on how each component or step of the traditional intelligence life cycle interacts with the whole project.

At the end of this chapter, you should be able to do the following:

- Understand the importance of intelligence frameworks in a CTI program.
- Explain and discuss the three most popular threat intelligence frameworks.
- Select the frameworks of choice when conducting an intelligence project.
- Integrate the framework in the security ecosystem.

In this chapter, we are going to cover the following main topics:

- Intelligence frameworks – overview
- Lockheed Martin's Cyber Kill Chain framework
- MITRE's ATTA&CK knowledge-based framework
- Diamond model of intrusion analysis framework

Technical requirements

For this chapter, no special technical requirements have been highlighted. Most of the use cases will make use of web applications if necessary.

Intelligence frameworks – overview

Cyber threat intelligence revolves around how the adversaries operate and what they are doing and can do, as well as understanding their **Tactics, Techniques, and Procedures** (**TTPs**) to help develop a reliable defense system. That information is then used to make objective business decisions to defend the system. CTI is not an isolated field; to defend against global threats, analysts and organizations mostly share the intelligence product. A standard framework is needed to create a collaborative cyber defense environment. The cyber threat framework can be defined as the universal language of threat intelligence and defense. The United States government developed it to facilitate the characterization and categorization of threat activities and identify trends and changes in adversaries' behaviors (`https://bit.ly/35K9RTi`). Hence, any organization that invests in cybersecurity should use the cyber threat framework to integrate these capabilities and produce intelligence. The following section highlights the benefits of intelligence frameworks.

Why cyber threat frameworks?

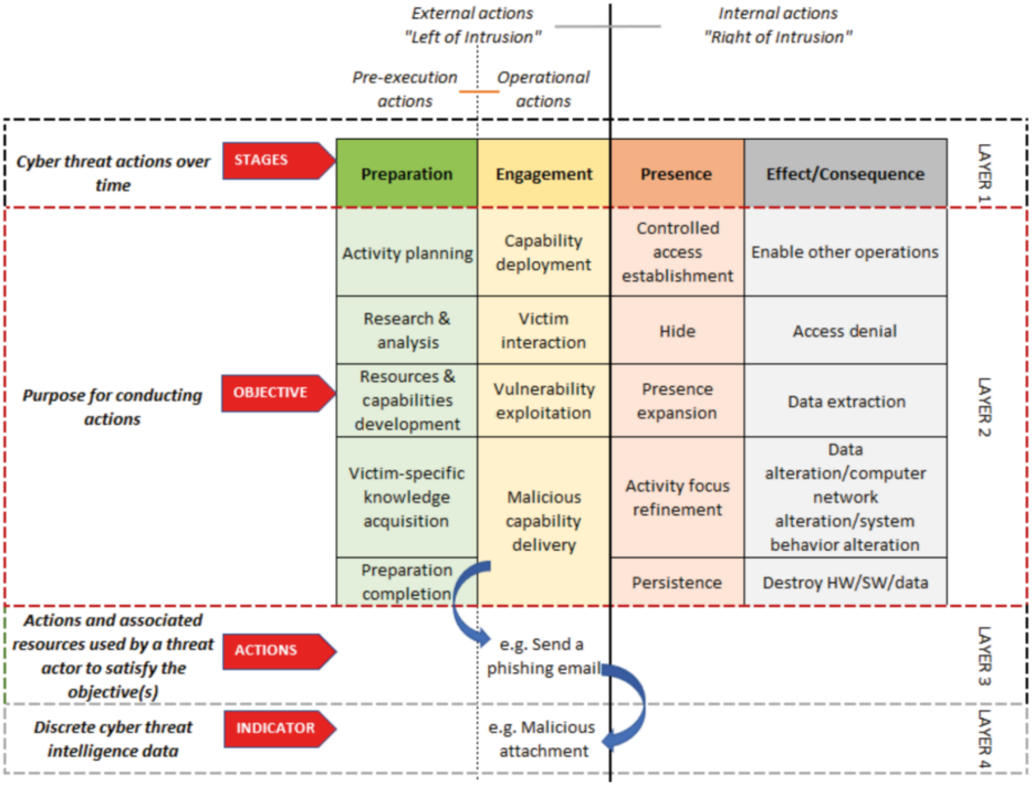
Cyber threat frameworks provide several universal benefits, including but not limited to the following:

- **Common language**: Cyber threat frameworks provide a universal way of communicating and describing threat information. By using a framework, two or more organizations can share intelligence products. For example, a threat intelligence task that uses MITRE ATT&CK follows a certain number of steps that are identical to all analysts using it.
- **Consistency**: Using a cyber threat framework allows the team to analyze threats consistently, facilitating both internal and external results. The strategic, tactical, and technical intelligence units can then use these results to support decisions and interpret the threat intelligence program output.
- **End-to-end threat analysis**: Cyber threat frameworks allow us to monitor and capture adversaries' activities (life cycles), from preparation to attack identification.
- When analysts use frameworks, they can discover threats earlier – even when the adversaries are just performing reconnaissance or non-intrusive activities. It allows them to have an end-to-end view of the adversary's movement and behavior (track changes in an adversary's TTPs and facilitate threat hunting). Since threat actors invest in discovering new methods to compromise systems, it is essential to have a view of how their TTPs evolved.
- **System integration**: Organizations invest in a lot of security tools and resources. However, those tools sometimes increase the security ecosystem's complexity, resulting in scheme chaos and loss of visibility on threats. Frameworks allow us to integrate the entire security ecosystem to provide values across multiple domains and platforms. They also combine internal and external data for better intelligence.
- **Iteration and continuity**: CTI is an iterative and continuous process. Therefore, threat intelligence frameworks provide a simplistic way to continuously learn and track variables that can impact the defense system. It helps us monitor adversaries' behavior and their modes of action unceasingly.

Threat intelligence frameworks are essential in developing and implementing an intelligence program. In the next subsection, we look at the cyber threat framework architecture and operating model.

Cyber threat framework architecture and operating model

As described by the US government, the general cyber threat framework model aims to simplify the cyber process by incorporating a layered perspective (that looks at cyber details), employing structured and documented categories, and focusing on evidence to support decisions. It must accommodate various data sources, threat actors, and tasks. The cyber threat framework architecture is shown in the following diagram:


External actions
"Left of Intrusion"
Internal actions
"Right of Intrusion"
Pre-execution actions
Operational actions
Cyber threat actions over time
STAGES
LAYER 1
Purpose for conducting actions
OBJECTIVE
LAYER 2
Actions and associated resources used by a threat actor to satisfy the objective(s)
ACTIONS
e.g. Send a phishing email
LAYER 3
Discrete cyber threat intelligence data
INDICATOR
e.g. Malicious attachment
LAYER 4

Preparation	Engagement	Presence	Effect/Consequence
Activity planning	Capability deployment	Controlled access establishment	Enable other operations
Research & analysis	Victim interaction	Hide	Access denial
Resources & capabilities development	Vulnerability exploitation	Presence expansion	Data extraction
Victim-specific knowledge acquisition	Malicious capability delivery	Activity focus refinement	Data alteration/computer network alteration/system behavior alteration
Preparation completion		Persistence	Destroy HW/SW/data

Figure 3.1 – Cyber threat framework by the US government (`https://bit.ly/35K9RTi`)

The framework uses a four-step process to capture the adversary's life cycle, from preparing the necessary capabilities to creating threat consequences. The four steps include preparation, engagement, presence, and consequence. Each step possesses a certain number of objectives and tasks to be executed. Let's look at some short descriptions of each step and understand how adversaries operate:

- **Preparation**: Preparation is the first step in the adversary life cycle. This is where the adversary collects all the relevant information about the target and plans the attack (an effective reconnaissance). To launch an attack, adversaries conduct in-depth research of the target system using active (network mapping and enumeration) and passive methods – such as open-source intelligence or dark web research. Based on the gathered information the adversaries prepare resources and develop the capabilities needed to move to the next step (engagement). They complete this preparation by ensuring that all the required knowledge and information about the target organization has been acquired.
- **Engagement**: After preparation, the adversary is ready to engage with the target system, which can be your organization. They interact with the target by exploiting vulnerabilities that have been collected in the preparation phase. This interaction is mostly achieved by implanting malicious software or files in the target using various modes of action (social engineering; that is, spear phishing or brute-forcing the system). Once the attack has been engaged and successful, the adversary gains full or partial control of the target, which is the next step.
- **Presence**: In this phase, the adversary performs tasks to fully control the system and cover their tracks (hiding his/her/their existence). They can perform privilege escalation to have high-level access to the system and compromise more. And if needed for a future entry, they are likely to establish persistence in the target system. Now, they are ready to compromise the system.
- **Consequence/effect**: Effect or consequence is the last phase of the adversary life cycle and is where the real actions are performed on the target. Depending on the objectives that were set in the preparation phase, the adversary can deny access (perform a DoS attack – availability), steal information and access sensitive data (confidentiality), and modify information to their will (integrity). They can even shut down the system.

The framework should be able to trace threats at each point of the adversary life cycle. The CTI analyst or team must map threats to the framework model to locate where the threats are. Let's look at the following examples:

> *"Using the threat detector, the security team of the ABC organization suspects cyber activity from a specific country. They have found that by using open source intelligence and the dark web, a lot of searches about the organization were made from that country in the last 3 days."*
>
> *"The malware analysis team has discovered the presence of a malicious DLL file in a third-party application being used by the organization. The DLL connects to IP addresses from a specific part of the country."*
>
> *"The ABC company was hit by ransomware named Xyz, which blocked all access to the ABC system for 24 hours until a sum of R 1M was paid to the adversary."*

The preceding three examples are real-life scenarios that can happen to any organization. Each instance can come from a different source. Assuming that these three scenarios come from different sources, it is difficult to correlate the events and build intelligence – although actions can be taken on the spot. By using an intelligence framework model, a threat analyst can map the preceding examples to the framework being used, as shown in the following diagram. They can also engage in the correct actions to prevent or address the threat directly:

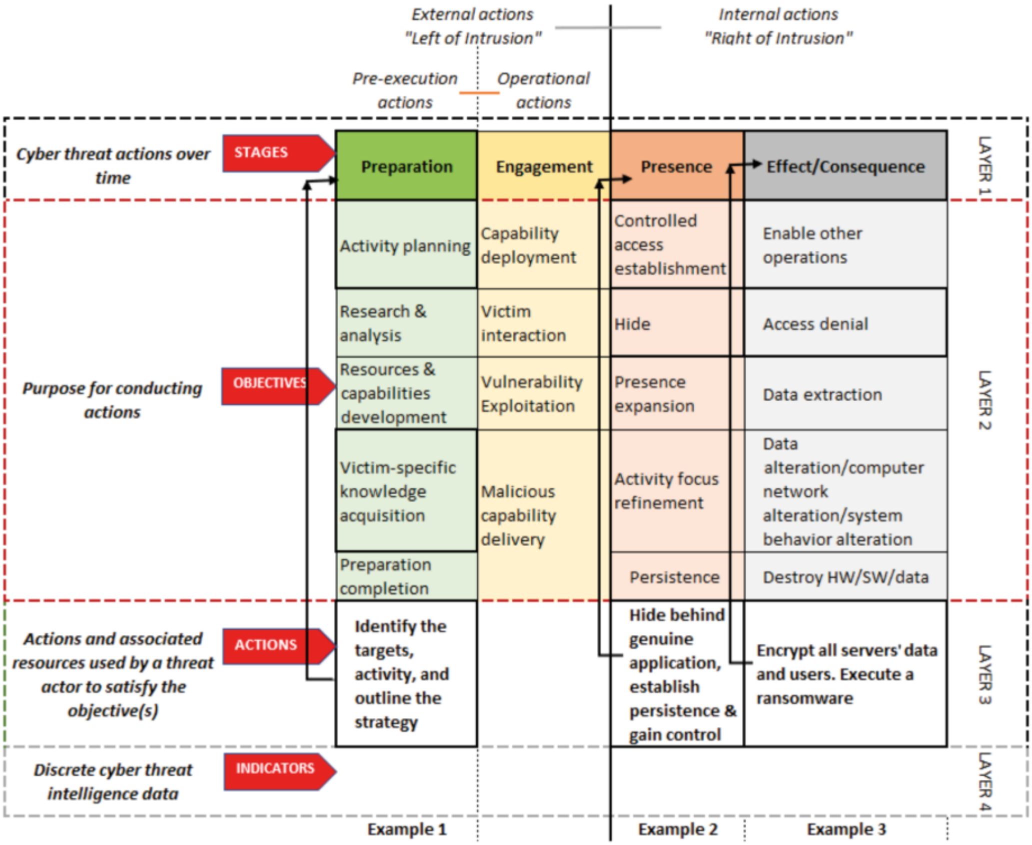

External actions
"Left of Intrusion"
Internal actions
"Right of Intrusion"
Pre-execution actions
Operational actions
Cyber threat actions over time
STAGES
Preparation
Engagement
Presence
Effect/Consequence
LAYER 1
Purpose for conducting actions
OBJECTIVES
Activity planning
Capability deployment
Controlled access establishment
Enable other operations
Research & analysis
Victim interaction
Hide
Access denial
Resources & capabilities development
Vulnerability Exploitation
Presence expansion
Data extraction
Victim-specific knowledge acquisition
Malicious capability delivery
Activity focus refinement
Data alteration/computer network alteration/system behavior alteration
Preparation completion
Persistence
Destroy HW/SW/data
LAYER 2
Actions and associated resources used by a threat actor to satisfy the objective(s)
ACTIONS
Identify the targets, activity, and outline the strategy
Hide behind genuine application, establish persistence & gain control
Encrypt all servers' data and users. Execute a ransomware
LAYER 3
Discrete cyber threat intelligence data
INDICATORS
LAYER 4
Example 1
Example 2
Example 3

Figure 3.2 – Cyber threat framework by the US government (`https://bit.ly/35K9RTi`) with our examples mapped to layers 1, 2, and 3

On layer 1, the cyber analyst maps the cyber events to the specific adversary life cycle step. Examples 1, 2, and 3 are directly mapped to the preparation, presence, and consequence stages, respectively.

On layer 2, the cyber analyst maps the cyber events to their specific objectives. Example 1 is detected at an early stage. The adversary is still planning the attack and acquiring knowledge about the organization. In example 2, the adversary has their presence in the system. Hiding and gaining control of the system are the adversary's aims at this stage (because access has been granted). Example 3 is a success story to the adversary. They now have to make the organization dance to their music – an expression to say they can engage in any course of action. That is the objective. In this context, denial of access to the service is provided.

On layer 3, the cyber analyst describes the actions that adversaries have used or can use to meet the objectives. In example 1, the adversary is likely to establish a strategy after 3 days of collecting information. With this, they have identified the ABC organization as a target. In example 3, the adversary's possible action is to execute the ransomware and demand payment.

On layer 4, the cyber analyst highlights the intelligence data that has been used or can be used by the adversary to act. In example 1, the indicators could be the Maltego intelligence tool or dark web data. In example 3, the data could be customizing a well-known piece of ransomware software.

The objective is to map every event to a framework process, and a useful CTI project must be able to achieve that. The cyber threat framework is not and should not replace an organization's existing security tools, methods, and models. However, this consolidates data across the multiple existing platforms and maps it to its structure. It provides a centralized point of cyber monitoring and data exchange. In the following sections, we look at the most popular frameworks used in the threat arena.

Lockheed Martin's Cyber Kill Chain framework

Lockheed Martin's Cyber Kill Chain is a popular intelligence framework used by analysts to understand and analyze adversary actions. It was developed in 2011 by Lockheed Martin. The Cyber Kill Chain maps the cyber attacks, breaches, and **Advanced Persistent Threats** (**APTs**) to the intelligence framework's structure. It takes its root from the military approach by describing methods used in warfare to attack and destroy enemies. Its military essence makes it a brutal and effective framework for correctly identifying threat actors, stopping them, and catching them rapidly. Hence, it is essential for intelligence analysts to fully comprehend this framework if they wish to build a robust defense system. The Cyber Kill Chain answers the question of, *What do adversaries really do to reach their cyber goals?*. The answer to this question is a set of TTPs commonly used by adversaries.

Adversaries orchestrate attacks using processes (steps) organized in a chain. This chain has linked nodes. To achieve their goals, threat actors should complete the tasks as planned in a chain structure (or in chronological order). Therefore, the cybersecurity or intelligence *analyst must break the chain by stopping the attack at any point in the process*. As viewed by the framework, an attack's success is determined by successfully exploiting all the adversary life cycle attack's phases. The Cyber Kill Chain uses a seven-step process to model an adversary's behavior. It maps any (or all) cyber threats and attacks to the seven steps or phases. Hence, any attack vector can be identified and analyzed using the framework. Let's look at the seven stages/phases of the model, as illustrated in the following diagram:

- **Reconnaissance**: Reconnaissance is always the first stage in every cyber attack. Nobody attacks what they do not know. Adversaries plan the attack by doing in-depth research on the target. They ensure that they collect relevant information to achieve their goals. In the reconnaissance phase, adversaries' techniques include using **open source intelligence** (**OSINT**) to get IP address ranges, domain information, email addresses, employees' information, press information, website information, and to uncover public-facing servers. The intelligence team must attempt to detect reconnaissance activities at their early phase to build intelligence and extract the adversaries' potential *intent*. However, stopping reconnaissance activities is not easy as such activities are often performed outside of the organization's defense systems and controls.

- **Weaponization**: The second stage in the Cyber Kill Chain is the weaponization stage. After successfully gathering information, adversaries use the collected data to prepare the attack. Depending on the objectives and methods that have been employed, they are likely to weaponize legitimate documents, create malware, and develop undetectable trojans. The *capability* is expected to be there since well-engineered malware, payloads, and exploit creation tools to carry advanced system attacks are available. *Only a few skilled adversaries can program their weapons to compromise systems*. However, with *Threat-as-a-Service*, even less skilled attackers can purchase state-of-the-art weapons and launch devastating attacks. The intelligence team, along with the internal security, must have clear visibility of this phase and implement methodologies to detect weaponized resources (including methods such as malware analysis and scanning, intrusion detection, and so on).

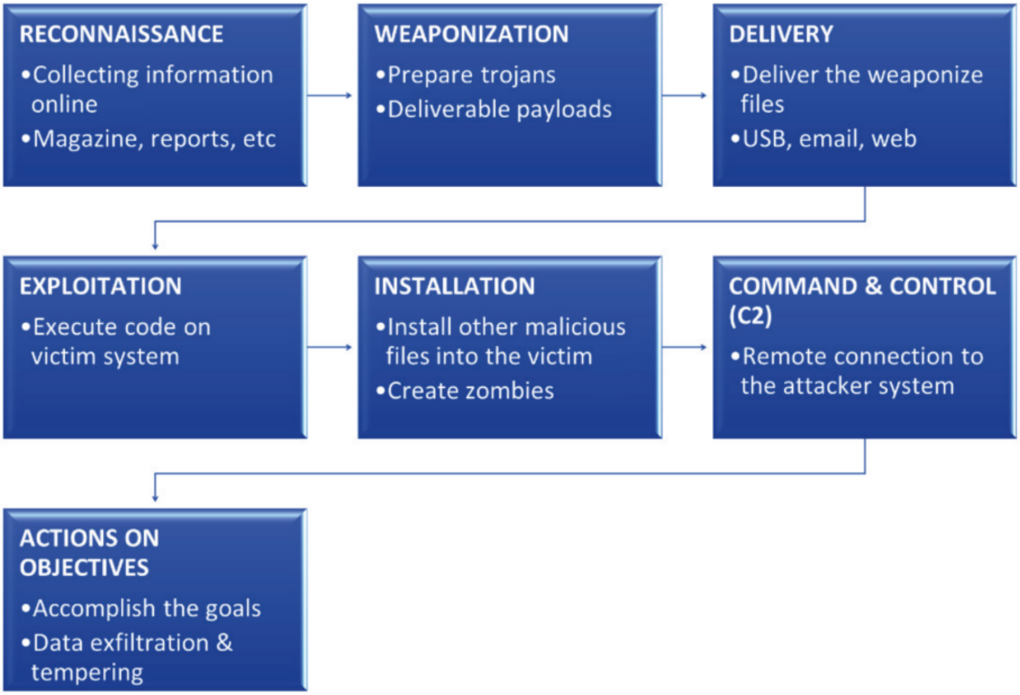


Figure 3.3 – Lockheed Martin's Cyber Kill Chain (`https://lmt.co/3iHGjLl`)

- **Delivery**: The adversary is ready to attack. The delivery stage involves techniques used to convey the malicious file(s) to the target. The framework breaks the delivery stage into two styles: adversary-controlled delivery (where the adversary manages the delivery; for example, using public-facing servers) and adversary-released delivery (which includes practices such as phishing, planting USB sticks, and so on).

The intelligence team develops ways to block intrusions. This is an essential step of the chain. If an adversary passes this stage, they are likely to affect the target system operation, even if they are detected in later stages.

- **Exploitation**: The exploitation phase is where the adversary gains access to the victim. They take advantage of system vulnerabilities to get into the system. The techniques used at this stage include exploiting vulnerabilities in software, hardware, and humans (social engineering). They can also use *zero-day exploits* or leverage *unpatched vulnerabilities* to gain access. Other methods involve opening malicious attachments or navigating malicious web links. The security team must develop countermeasures to prevent or stop the attack.
- **Installation**: Unless the operation is a one-off task, adversaries are likely to install persistent backdoors for future intrusions. This helps them maintain access for as long as they want in the victim system. The intelligence team must develop ways to detect backdoors (using a methodology such as endpoint instrumentation). Some techniques used by the adversaries at this stage include changing the registry, adding environment variables, or modifying legitimate processes to achieve persistence.
- **C2**: Once a backdoor has been planted in the victim, an adversary finds techniques to communicate with it and take control. The Cyber Kill Chain describes techniques that threat actors use to create communication with backdoors. Hence, the defense team can use countermeasures to block the attack. C2 is the last stage where the intelligence team and the defense system can take action – after this, only tears remain.
- **Actions**: At this stage, the adversary can execute any action on the target system, from collecting sensitive information to denying services to the users. The framework enumerates some of the most used adversarial actions, including privilege escalation, lateral movement, internal reconnaissance, collecting and exfiltrating data, system destruction, system modification, and data corruption. At this stage, the defender's objective is to detect the action rapidly to avoid further damage. Forensics methods are used at this stage to gather pieces of evidence on the breach (incident response).

The Cyber Kill Chain model uses a comparative method of the adversary tactic and the possible defensive stand. For each stage, it provides techniques to defend against the corresponding adversarial movement.

Use case – Lockheed Martin's Cyber Kill Chain model mapping

Scenario and objective: A group of hackers has decided to take down the ABC insurance company after voting for and passing policies that customers are unhappy with. Their sole objective is to take down the business for as long as they want in order to push the company to remove the policies.

The group harvests email addresses, domain information, IP ranges, and SSL certificate information from the public internet. They come across the email address of Vanessa, the IT admin, on LinkedIn and her life routine on Instagram. They also discover the company router that faces the internet and the company's website, where users can register for insurance, contact the company, and leave comments.

- Cyber Kill Chain mapping: *Reconnaissance*.

  Countermeasure: Continuously collect website access logs for search activities, collect traffic analytics from web administrators, and detect unique and suspicious recurrent browsing behavior.

  The group selects the **Metasploit Framework** (**MSF**) as their tool to generate a set of malware embedded in a document to send to Vanessa.

- Cyber Kill Chain mapping: *Weaponization*.

  Countermeasure: Know the most used malware generation platforms, perform malware analysis, and identify and detect malware payload types and their origins.

  The group is ready to use two techniques to compromise the system. They send an email to Vanessa and also prepare a USB stick with the prepared weapon that will physically be installed on Vanessa's personal computer.

- Cyber Kill Chain mapping: *Delivery*.

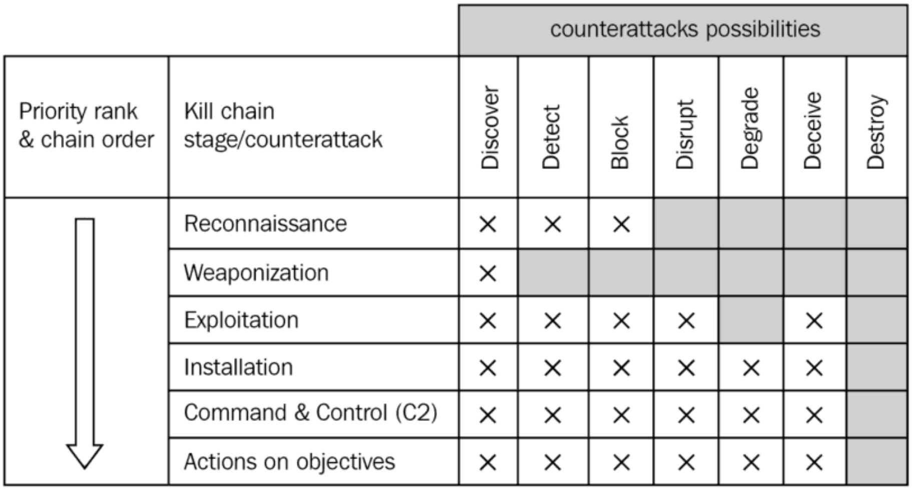
  Countermeasure: Understand the upstream infrastructure, understand the people and their roles, understand what information can be accessed by which user, and frequently perform forensics reconstruction.

  Paul is a member of the group. He befriended Vanessa a month before and has been able to visit her at her place. One of the ways to deliver malicious code is for Paul to convince Vanessa to open the document on the USB stick. Alternatively, Paul can send an email with the attachment to Vanessa and she will open it.

Integrating the Cyber Kill Chain model into an intelligence project

A cyber threat intelligence model such as the Cyber Kill Chain is not an independent component of security but a model that needs to be integrated into an intelligence framework to build a resilient defense system. In this subsection, we will look at how the model can be applied to an intelligence project:

- **SIEM enrichment and prioritization**: Most organizations have a SIEM system to manage security events. A CTI project collects data from different sources and creates alerts and indicators. Mapping alerts and indicators to each stage of the Cyber Kill Chain helps the intelligence team prioritize security tasks and identify missing components to build a resilient defense. The higher the location where an event is mapped in the kill chain, the higher the priority. For example, an intrusion detection system alert and a malware presence alert cannot be treated the same way as they map to different kill chain phases. The highest priority events must be responded to quickly.
- **Escalation control**: When a cyber attack happens, it creates a different atmosphere in the organization. The security and intelligence teams need to determine how to handle the escalation of cyber threats. The Cyber Kill Chain at each phase, assesses the level of impact an attack has and can guide the CTI team in reporting and escalating cyber events. For example, an attack that has been mapped to stage seven of the kill chain must wear a critical priority hat and must be escalated to the strategic team (as the intruder might have interrupted the business already). An event that's been mapped to the delivery stage doesn't need to be escalated to a strategic level but can be handled at the tactical and technical levels.
- **Identify gaps in the security defense and prioritize investment**: Using the Cyber Kill Chain model, the intelligence team can map all organization tools and their functions to the model's stages. The analysis team defines a matrix of potential adversarial actions against each step of the kill chain by specifying whether the organization possesses tools and resources to defend against such actions. An example of a gap matrix using the Cyber Kill Chain is shown in the following diagram with the seven Ds, explained in *Chapter 13*, *Threat Intelligence Metrics, Indicators of Compromise, and the Pyramid of Pain*:



		counterattacks possibilities						
Priority rank & chain order	Kill chain stage/counterattack	Discover	Detect	Block	Disrupt	Degrade	Deceive	Destroy
	Reconnaissance	×	×	×	▨	▨	▨	▨
	Weaponization	×	▨	▨	▨	▨	▨	▨
	Exploitation	×	×	×	×	▨	×	▨
	Installation	×	×	×	×	×	×	▨
	Command & Control (C2)	×	×	×	×	×	×	▨
	Actions on objectives	×	×	×	×	×	×	▨

Figure 3.4 – Intelligence gap matrix using the Cyber Kill Chain

The intelligence gap based on the Cyber Kill Chain will display the security defense areas that might need reinforcement, thereby helping in security investment (what tools are missing from the arsenal to ensure a resilient defense system?).

- **Assess the system's effectiveness and resilience**: An analyst needs to document threat events and insert marks (in the intelligence platform of choice) at each stage where attacks are detected, prevented, or disrupted. The earlier an attack is spotted, the better the chance of mitigating it and counter-attacking. Over time, the team can evaluate at which stage of the kill chain the system mostly detects, blocks, or disrupts cyber attacks This is known as *effectiveness*. We can use trends or any graphical visualization to evaluate a system's effectiveness using the Cyber Kill Chain

  Another important point to address in any intelligence and defense project is the *resilience* of the system. Can an attack still be detected if the adversary changes techniques, attack signatures, or strategies to achieve the same objectives? An intelligence analyst must always project the possibility of a strategy change from the adversary. If the system can still detect, stop, or disrupt the attack at any stage of the kill chain after the attack changes, the system is *resilient*.

Apart from the Enterprise Matrix of adversary behaviors, the ATT&CK framework also describes the Mobile Matrix, which includes most of the preceding tactics and their relevant techniques. For each tactic and technique, the framework provides a detailed description and how to mitigate such an attack. The matrix navigation architecture is shown in the following diagram:

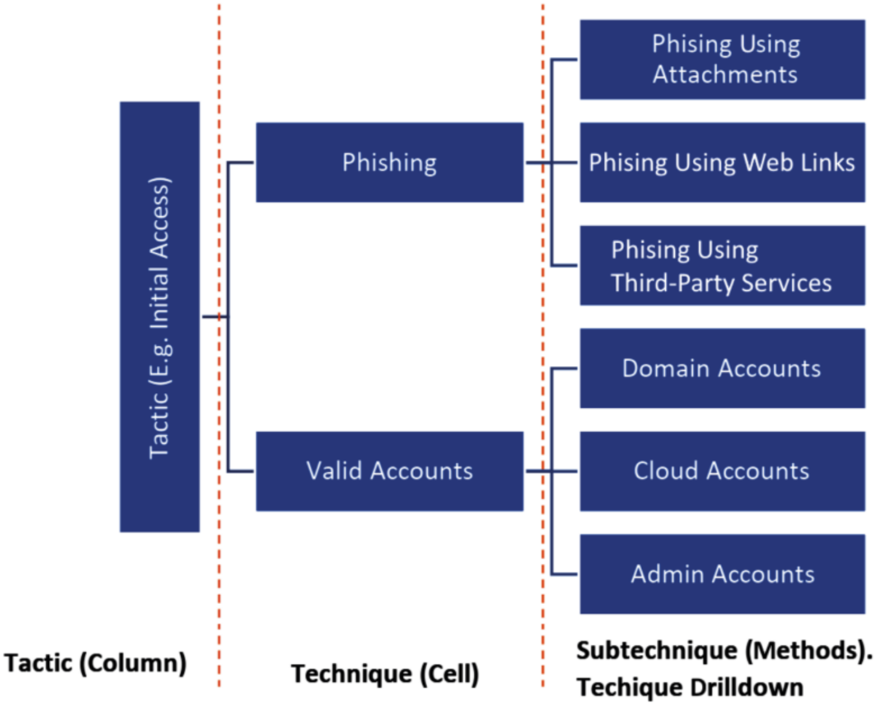

Tactic (E.g. Initial Access)
Phishing
Valid Accounts
Phising Using Attachments
Phising Using Web Links
Phising Using Third-Party Services
Domain Accounts
Cloud Accounts
Admin Accounts
Tactic (Column)
Technique (Cell)
Subtechnique (Methods). Techique Drilldown

Figure 3.6 – ATT&CK matrix navigation architecture

To join the theoretical overview of the framework described here to a practical use case, we will look at a model that can be mapped to a real cyber attack scenario.

How to mitigate such an attack

The framework provides mitigation practices for such attacks. Mitigation includes installing antivirus software (to quarantine or remove malicious files) and intrusion prevention devices (to block suspicious activities). It also includes web-based content restriction (blocking some extensions and scanning the attached compressed files) and user training (training the users to detect suspicious email attachments and links). If Joe had paid attention, he would have noticed the scam.

The preceding use case shows how the ATT&CK framework maps the adversary activities to the tactics and techniques and provides ways to deal with each tactic and technique. By looking at the mitigation and detection step, the target organization can assess and strengthen its defense system. Now, let's look at how analysts and the security team can use the ATT&CK matrix to build intelligence.

Integrating the MITRE ATT&CK framework

The MITRE ATT&CK framework is rich in terms of adversary behaviors and can support organizations' security infrastructures in many ways. By adopting the framework, the organization can do the following:

- **Emulate adversary behavior**: They can use threat intelligence to understand the adversary's behavior and check the security system's consistency. They can also map each threat to the tactics and techniques described in the framework.
- **Perform red team operations**: Even though the organization has not or has never been attacked, a preventive security system can be put in place by ethically hacking the organization and assessing the impact of each ATT&CK tactic and technique on the security infrastructure. This is the best way to test the defense system's strength.
- **Perform analytics**: It is essential to keep track of threat activities and visualize threats insights using analytics. An organization can use the ATT&CK framework to analyze, group, and uncover suspicious activity patterns.
- **Assess the gap in the defense line**: By using the ATT&CK framework, intelligence analysts can identify the holes in the security system. This can be achieved by looking at how many and which tactics can easily penetrate the organization's defense system. ATT&CK can also help in evaluating the available security resources in the arsenal.
- **Evaluate the SOC system**: The ATT&CK system exposes the defense's weaknesses. Using the tactics and techniques available in the framework, analysts can rapidly assess the SOC's effectiveness. How fast can the SOC system detect threats and respond to breaches?

- **Enrich the intelligence project**: MITRE's ATT&CK framework is continuously updated. Hence, new tactics and techniques are added to the framework quickly, helping organizations have new indicators and improving security monitoring.

MITRE's ATT&CK framework can be integrated into the security system in two ways: *manual* and *automatic*. It can also be integrated into SIEM systems. Data from different sources is collected and analyzed to detect potential threats, and it is mapped to the ATT&CK framework to help us understand the adversary's behavior. It can also be integrated into endpoint detection and response systems to locate at which phase of the attack an adversary is situated. By knowing such information, the analyst can project the impact of the attack on the defense system. It can also be integrated into cloud security systems. Now that we know how to use MITRE's ATT&CK framework, let's look at some of its benefits.

Benefits of the ATT&CK framework

MITRE's ATT&CK framework provides many benefits to an organization and the global security world in general from a technical and non-technical perspective. The following are some of the benefits of using this framework:

- The framework is rich in terms of adversary tactics, making it one of the most used security frameworks in cyberspace.
- ATT&CK is used not only for intelligence projects but for cross-IT department operations as well. It means that every security function can independently use the framework to map, analyze, and respond to threats.
- ATT&CK is an open-source framework and is maintained by the security community. It maintains a library of common information about adversary groups and cyber campaigns that have been conducted.
- It provides a centralized environment to help create, collect, share, and manage information.
- Anyone and any organization can use it.

MITRE's ATT&CK is widely used in the cybersecurity space, and it has built a strong reputation in the CTI environment because of its comprehensive and continuously updated adversaries' behavior libraries. It is essential as an intelligence analyst must know the advantages of the ATT&CK framework. Next, we will look at the Diamond model of Intrusion Analysis.

- It is compatible with popular IOC sharing formats such as STIX, TAXII, and **Cyber Observable Expression** (**CyBox**). Analysts can use YARA to scan the system for malware intrusion.
- It can be installed on Unix (Linux and OS X) and Windows stations and support terminal execution.
- Its rules are easy to write and share.

An example of a YARA rule is shown in the following snippet (`https://bit.ly/3eOE8V4`). YARA has a similar structure to the C programming language:

```
/*
    A YARA mutli-line comment
*/
rule ExampleRule //An example rule to show YARA structure
{
    strings:
        $my_text_string = "text here"
        $my_hex_string = { E2 34 A1 C8 23 FB }
        $my_regex_str = /md5: [0-9a-zA-Z]{32}/
    condition:
        ($my_text_string or $my_hex_string) and $my_regex_str
}
```

The structure of the syntax can be described as follows:

- The `rule` identifier: This is the name of the `rule`. It acts as a function in programming. It starts every YARA. The rule comprises two parts (`strings` and `condition`) and an optional component for the metadata. The metadata is used to add descriptions, titles, and other descriptive messages.
- The `strings` section: This defines the strings to be searched. Strings can be used as *text* (in double quotes) or *hexadecimal* (in curly braces). Each string variable starts with a `$` character. Hexadecimal characters are separated by spaces. There are three YARA strings' types: (*1*) *hexadecimal* strings that can have wildcards for unmatched bytes; (*2*) case-sensitive *text* strings – using `nocase` at the end of the string makes it case-insensitive; and (*3*) regular expressions to match any character string. They must be enclosed inside forward slashes.
- The `condition` section: This is required by every YARA rule. It indicates when the rule must alert us using Boolean expressions and arithmetic. Additionally, it holds the rule's logic.

A string can be an IP address, a domain name, or a specific hash value. A regular expression (regex) can be a URL or a mutex pattern. You can count the number of times a string variable appears in the file.

Understanding the essential components of a YARA rule is fundamental for writing and interpreting them. However, more complex rules can be created (including global and private rules and modules). Once a YARA rule has been created, it can be uploaded to the security tools for IOCs and malware scanning.

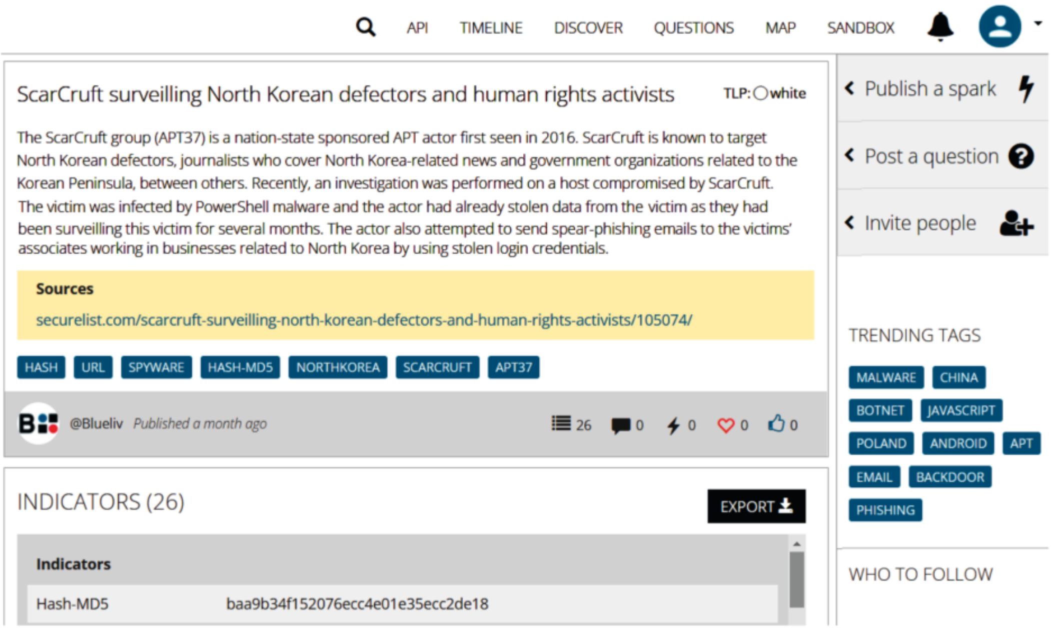
> **Important Note: YARA for a CTI Analyst**
>
> YARA is essential for incident response analysts and malware analysts. A CTI analyst does not have to be an expert in writing YARA rules. However, they must be able to write simple rules and understand complex rules for system integration.

Chapter 15, Threat Intelligence Sharing and Cyber Activity Attribution - Practical Use Cases, covers a practical use case for malware detection and IOC creation using YARA rules. For more information about YARA, please visit the official documentation that can be found on the website (`https://yara.readthedocs.io/en/v3.5.0/index.html`).

Other popular threat intelligence sharing formats include the following:

- **Structured Threat Information eXpression (STIX)**: This is an open source language for threat intelligence exchange (`https://bit.ly/3eOODYs`). STIX is covered in *Chapter 4*, *Cyber Threat Intelligence Tradecraft and Standards*. Another helpful use case is covered in *Chapter 15*, *Threat Intelligence Sharing and Cyber Activity Attribution - Practical Use Cases.*
- **Trusted Automated eXchange of Indicator Information (TAXII)**: This is a communication protocol that uses HTTPS for cyber threat information (CTI information in STIX format). TAXII is also covered in *Chapter 4*, *Cyber Threat Intelligence Tradecraft and Standards*.
- **Cyber Observable eXpression (CybOX)**: This is a structured language for sharing and communicating cyber observables (`https://cyboxproject.github.io/`). Note that CyBox is integrated into STIX 2.0.

- **Blueliv Threat Exchange Network** (`https://community.blueliv.com/`): This is a web platform that is used for sharing IOCs for threat protection. It contains a cyber threat map, a malware sandbox, an API for integration with internal systems, and a timeline that provides a threat actor's activities and profiles. An example is shown in the following screenshot:



ScarCruft surveilling North Korean defectors and human rights activists TLP: ○white

The ScarCruft group (APT37) is a nation-state sponsored APT actor first seen in 2016. ScarCruft is known to target North Korean defectors, journalists who cover North Korea-related news and government organizations related to the Korean Peninsula, between others. Recently, an investigation was performed on a host compromised by ScarCruft. The victim was infected by PowerShell malware and the actor had already stolen data from the victim as they had been surveilling this victim for several months. The actor also attempted to send spear-phishing emails to the victims' associates working in businesses related to North Korea by using stolen login credentials.

Sources

securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/

INDICATORS (26)

Indicators	
Hash-MD5	baa9b34f152076ecc4e01e35ecc2de18

Figure 14.12 – The Blueliv Threat Exchange Network timeline

The system is open source. Hence, you can register and explore the features of the threat exchange platform.

- **Anomali STAXX** (`https://www.anomali.com/resources/staxx`): This is a tool that provides easy access to the STIX/TAXII data feeds. STAXX can be downloaded from Anomali's official website and set up in five simple steps: (*1*) Download the STAXX `OVA` file and import it into the virtual machine environment. (*2*) Set STAXX using the configuration wizard. (*3*) Configure the STIX/TAXII feed using the tool's wizard. (*4*) Select the intelligence feeds. (*5*) Set the schedule for the intelligence data update, and the tool is ready to be used.
- **Cyware Threat Intelligence eXchange** (`https://cyware.com/ctix-stix-taxii-cyber-threat-intelligence-exchange`): This is a client-server TIP with ingestion, analysis, enrichment, and sharing capabilities. It supports all the known intelligence sharing formats, including STIX (1.0 and 2.0), MISP, CybOX, MAEC, YARA, PDF, email, and text-based formats.

Index