A Guide to Cyber Threat Intelligence

Oscar Rosengren ⋮ 15-19 minutes

1. Introduction

Cyber threat intelligence (CTI) is a process and a product which provides a valuable tool for identifying and mitigating offensive capabilities of hostile actors in cyberspace. By following best practices for conducting effective CTI, organisations can better understand the threat landscape, identify emerging threats, and develop strategies for mitigating them. Efficient CTI will help organisations reduce the risk of a successful attack and minimise the impact of any breaches that do occur.

2. What is Cyber Threat Intelligence?

CTI is a product and process. CTI as a product is the result of the process when cyber threat information has been collected, evaluated in the context of its source and reliability, and analysed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information. When describing CTI as a process, it identifies and analyses cyber threats. Like all intelligence, cyber threat intelligence provides a value-add to cyber threat information, which reduces uncertainty for the consumer while aiding the consumer in identifying threats and opportunities. Analysts must identify similarities and differences in vast quantities of data and detect deceptions to produce accurate, timely, and relevant intelligence (source).

Moreover, often confused with threat information, a list of possible threats, the CTI shows the bigger picture by interrogating the data and the broader context to construct a narrative that can inform decision-making. Hence, CTI must be actionable rather than information of possible threats. CTI is timely, provides context, and is presented in a manner in which it is understood by decision-makers (source).

CTI can be understood from three categories –tactical, operational, and strategic.

2.1. Strategic Level

Strategic CTI refers to the high-level analysis designed for non-technical audiences – for example, the board of a company or organisation. It covers cybersecurity topics that may impact broader business decisions and look at overall trends and motivations. Strategic threat intelligence is often based on open sources – which means anyone can access them – such as media reports, white papers, and research.

2.2. Operational Level

Operational CTI is designed to answer questions about the ‘who’, ‘why’, and ‘how’ behind a hostile cyber operation. By studying past cyber-attacks, operational CTI focuses on concluding intent, timing, and sophistication. Since cyber attackers can’t change their tactics, techniques, and procedures (TTPs) as quickly as they can change their tools – such as a specific type of malware, the operational CTI often requires more resources than tactical intelligence, but its value has a longer lifespan.

2.3. Tactical Level

Tactical CTI is focused on the immediate future and is designed for a more technically proficient audience. It identifies simple indicators of compromise (IOCs) to allow IT teams to search for and eliminate specific threats within a network. IOCs include:

- Lousy IP addresses.
- Known malicious domain names.
- Unusual traffic.
- Log-inincrease i.
- Andownload requests.

Tactical CTI is the most straightforward form of intelligence to generate and is usually automated. However, it can often have a short lifespan as many IOCs quickly become outdated.

3. Why is Cyber Threat Intelligence Important?

CTI is essential because cyber threats are constantly evolving, and organisations must be proactive in their approach to enhance security. CTI provides organisations with valuable insights into emerging threats and helps them develop strategies for mitigating them before they can cause damage. The benefits of CTI include:

- Improved threat detection and response.
- Reduced risk of a successful attack.
- A better understanding of the threat landscape.

CTI can also help organisations identify weaknesses in their security posture and develop strategies for strengthening it. CTI enables organisations to make faster and more informed security decisions. Furthermore, it encourages proactive rather than reactive behaviours in the fight against cyber-attacks. The importance of CTI is illustrated in its several benefits, which include:

Reduced risks

Hackers are always looking for new ways to penetrate enterprise networks. CTI allows businesses to identify new vulnerabilities as they emerge, reducing the risk of data loss or disruption to day-to-day operations.

Avoiding data breaches

A comprehensive CTI system should help to avoid data breaches. It monitors suspicious domains or IP addresses trying to communicate with an organisation's systems. A sound CTI system will block suspicious IP addresses from the network, which could otherwise steal data.

Reduced costs

Data breaches are expensive. In 2021, the global average data breach cost was $4.24 million (source). These costs include elements like legal fees and fines plus post-incident reinstatement costs. By reducing the risk of data breaches, cyber threat intelligence can help save money.

Essentially, CTI helps an organisation to understand cyber risks and what steps are needed to mitigate those risks. Hence, CTI is a crucial part of any cybersecurity ecosystem.

4. How to Conduct Cyber Threat Intelligence

Rather than being developed in an end-to-end process, intelligence development is a circular process called the intelligence cycle. The cycle is a structure to ensure that data collection is planned, implemented, and evaluated; the results are analysed to produce intelligence; and the resulting intelligence is disseminated and re-evaluated in the context of new information and consumer

feedback. The cycle's analysis portion differentiates intelligence from information gathering and dissemination.

Intelligence analysis relies on a rigorous way of thinking using structured analytical techniques to identify and manage biases, mindsets, and uncertainties. Instead of just reaching conclusions about difficult questions, intelligence analysts evaluate how they reach conclusions. This extra step ensures that, to the extent feasible, the analysts' mindsets and biases are accounted for and minimised or incorporated as necessary.

The process is a cycle because it identifies intelligence gaps, and unanswered questions, which prompt new collection requirements, thus restarting the intelligence cycle. Intelligence analysts identify intelligence gaps during the analysis phase. Intelligence analysts and consumers determine intelligence gaps during the dissemination and re-evaluation phase (source).

5. The Cyber Threat Intelligence Life Cycle

A typical example of a cyber threat lifecycle would involve direction, collection, processing, analysis, dissemination, and feedback.

5.1. Phase 1: Direction

This phase focuses on setting goals for the threat intelligence program. It might include:

- Enhanced understanding of which aspects of the organisation require protection, which allows for a priority order.
- Identifying what CTI capabilities the organisation needs and what products are crucial to protect assets and respond to threats.
- Understanding the organisational impact in relation to the risks of a cyber breach.

5.2. Phase 2: Collection

This phase is about gathering data to support the goals and objectives set in Phase 1. Data quantity and quality are crucial to enhance the capability to avoid severe threat events or being misled by false narratives. In this phase, organisations need to identify their data sources which include:

- Metadata from internal networks and security devices
- Threat data feeds from credible cyber security organisations
- Interviews with informed stakeholders

5.3. Phase 3: Processing

All the collected data needs to be turned usable. Different data collection methods will require various means of processing. For example, data from human interviews may need to be fact-checked and cross-checked against other data.

5.4. Phase 4: Analysis

Once the data has been processed into a usable format, it needs to be analysed. The analysis is turning information into intelligence that can guide decision-making.

5.5. Phase 5: Dissemination

Once the analysis has been carried out, the key recommendations and conclusions need to be circulated to relevant stakeholders within the organisation. Different teams within the organisation will have different needs. To disseminate intelligence effectively, questions must be answered of the

actor's intelligence needs. For example, what format is suitable for the intelligence products to remain actionable.

5.6. Phase 6: Feedback

Feedback from stakeholders will help improve the CTI program, ensuring that it reflects the requirements and objectives of the entity. The term' lifecycle' indicates that CTI is not a linear process. Instead, organisations must use a circular and iterative process for continuous improvement.

6. Tips and Tricks on Cyber Threat Intelligence

Even though there are several tips and tricks when conducting CTI, below are some extra valuable points:

- Define objectives and scope.
- Identify desirable data sources.
- Establish processes for the collection, analysis, and dissemination of data.
- Establish partnerships and information sharing with relevant actors.

Overall, CTI is an essential practice for organisations looking to stay ahead of emerging cyber threats and protect their networks and data. By understanding the critical components of a CTI program and the resources and tricks needed to implement it, organisations can develop effective strategies for mitigating cyber threats and minimising the impact of any security incidents.

7. Common Mistakes to Avoid when Conducting Cyber Threat Intelligence

Several common things could commonly be improved when conducting CTI. There are several mistakes at the organisational level. Among them are:

- An inability to define objectives and scope.
- Over-reliance on automated tools, which are perceived to outplay the human elements when conducting analysis.
- A lack of context where the CTI as a product is not put in relation to the reality of the organisation.
- A failure to share the information which harms the capability to detect and respond to emerging trends and threats. The Internet does not recognise physical boundaries such as state borders. Hence, effective methods of cooperation may offer crucial opportunities for a force multiplier when facing different threat actors in cyberspace.

As an individual seeking a career within CTI, at least two mistakes are common. These are:

- To mistake information with intelligence, i.e., the difference between open-source information and open-source intelligence.
- To underestimate your capabilities.

8. Tools and resources for Cyber Threat Intelligence

Cyber threat intelligence (CTI) requires various tools and resources to gather, process, and analyse data from various sources. Some of the tools and resources commonly used in CTI are:

Threat Intelligence Platforms (TIPs): These are platforms designed to aggregate and correlate data from multiple sources and provide a central repository for storing, managing, and analysing threat intelligence. TIPs can help automate data processing and analysis, making it easier for analysts to identify and respond to threats.

Open-Source Intelligence (OSINT) Tools: These are publicly available tools to gather information about threat actors and their TTPs. OSINT tools include:

- Search engines.
- Social media monitoring tools.
- Websites that aggregate information about known threat actors and campaigns.

Security Information and Event Management (SIEM) Tools: These are tools that aggregate and analyse log data from various sources, such as firewalls, intrusion detection systems, and other security devices. SIEM tools can help identify patterns and anomalies in network activity that could indicate a potential threat.

Malware Analysis Tools: These tools can be used to analyse and understand the behaviour of malware. Malware analysis tools can help identify the source of a malware infection, its capabilities, and its potential impact on an organisation.

CTI Sharing Platforms: These are platforms that facilitate the sharing of threat intelligence data among organisations, industry groups, and government agencies. Sharing platforms can help organisations identify emerging threats and coordinate responses to cyber attacks.

Overall, the tools and resources used in CTI can vary depending on an organisation's specific needs and capabilities. The key is to have a comprehensive approach to gathering and analysing data from various sources, so organisations can stay ahead of emerging threats and protect their networks and data from cyber-attacks.

9. Frequently Asked Questions about Cyber Threat Intelligence

9.1. Why is CTI important?

Learning about current and developing cyberattacks enables your business to defend your valuable assets and contribute to overall resilience on national and international levels.

It is imperative to understand the threat landscape and your organisation's role in it to address vulnerabilities and develop adequate security measures in proportion to your valuable assets. The interdependent relationship between actors in cyberspace requires such knowledge and does not allow for half-measures. The primary motivation for developing adequate cybersecurity measures is often two-fold. First, your organisation is kept safer from harm. Also, it is a matter of responsibility and trust-building signals to clients.

9.2. What are the benefits of CTI?

CTI benefits any organisation. Processing threat data to understand attackers better, respond faster to incidents, and proactively get ahead of a threat actor's next move is crucial to maintain business.

9.3. What data sources are used in CTI?

CTI often comes from external sources, such as open-source information sharing or communications between relevant actors. However, it can also come from internal information sources, such as an organisation's SIEM or log management tools.

9.4. What skills are needed for CTI?

What skills are needed to conduct CTI varies based on the level of CTI. However, operational CTI usually requires experience in data analysis, information technology, security, incident response, vulnerability management, penetration testing, and ethical hacking.

Strategic CTI usually requires more geopolitical and geostrategic knowledge and analytical skills. Such skills are precious when identifying the motives of certain threat actors and how the general security situation on national or international levels may affect the behaviour of named actors.

9.5. How can organisations get started with CTI?

No standard answer exists to how one develops CTI capabilities within an organisation. The capabilities must match the specific needs of the organisation in question. However, CTI is either a capability developed in-house, usually within the company's security department, or by external consulting. An excellent first step is to get in contact with a cybersecurity firm for guidance.

10. Conclusion

Cyber threats are an ever-present risk to organisations, and the threat landscape is constantly evolving. Therefore, organisations need to be proactive in their approach to cybersecurity to stay ahead of emerging threats and protect their computer systems, networks, and data. CTI is a product and process. As a process, it must follow a methodology which clearly defines the objectives and scope based on the organisation's needs. Moreover, the sources, i.e. tools, to conduct efficient CTI must be put in place as well as processes for the collection, analysis, and dissemination of data. As a product, it is critical that CTI remains actionable rather than just a process of information-gathering of possible threats. CTI as a product is timely, provides context, and is understood by decision-makers.