Cyber Threat Intelligence – Challenges and Problems

Today in the landscape of online threats there is an increasingly rapid, organized and harmful evolution of cyber threats and, consequently, addressing them is a process that becomes tough and complex.

Cyber criminals are more skilled, organized and have more funds than before. Cyber Threat Intelligence (CTI) has become a very current topic and currently, many organizations are considering it for countering the increase in cyber attacks.

Taking a look at today's situation, it is clear that it is extremely difficult to prevent attacks and security breaches due to the ability of hackers to target vulnerabilities not only in technology but also in the people and processes. Cyber criminals have improved their tactics, techniques and procedures (TTPs) to the point that it is nearly impossible to detect them, investigate their activities and undo the damage they cause. Their TTPs are less predictable, more persistent, more ingenious, better funded, sharply organized and aimed at making money. Multiple organizations are targeted by cyber criminals who use ransomware to force them to pay to unlock essential data and systems for their business.

In recent years, the CTI has received considerable media coverage and has been identified as one of the solutions to counter the rise and complexity of online security incidents. Businesses have chosen to subscribe to various threat intelligence services from both open-source and commercial sources.

It is important to fully understand the basic concept in order to define the CTI and its origin. Below we will cover three important terms in this field: **cyber attack, cyber threat, and intelligence**.

1. Cyber Threats And Cyber Attacks

There are multiple definitions to clarify the concepts of cyberattack and cyber threat, as both terms are the topics most addressed by the major media. In 2013, the US government defined the cyber threat as an extensive range of malicious activities that can occur in cyber space. Such threats include **website defacement, espionage, intellectual property theft, denial of service attacks, and destructive malware**. In contrast to the explanation proposed by the US government, the Oxford English Dictionary defines cyber threats as "malicious attempts to damage or disrupt a network or computer system". While the cyber attack is defined as "an attempt by hackers to damage or destroy a network or a computer system".

2. Information And Data Intelligence

There is a huge difference between noisy data, data threats, information and intelligence. Understanding this is essential to getting the most out of threat intelligence platforms. The data consists of basic, raw and generally unfiltered information, which usually appears in the form of symbol and sign readings. Information, on the other hand, is data that is processed, aggregated and sorted in a format that is more understandable to humans that provides more context and is useful for conducting certain forms of analysis.

To summarize, it can be said that **the data collected by the operating environment is processed and refined to produce information**. Then, this information is analyzed and translated into usable formats that constitute intelligence.

3. Use Cases Of Cyber Threat Intelligence

In recent years, CTI has increasingly become a critical topic in cybersecurity, but the lack of resources for clarifying the concept and presence of companies that tend to use their own definition to distinguish their product can lead to some misunderstanding.

Despite of how ambiguous it may be, CTI can be defined as **evidence-based knowledge that encompasses context, mechanisms, indicators, implications, and actionable advice regarding an existing or emerging threat that can be used to make informed decisions about the response of the subject at that given threat or danger.**

CTI adoption measures are still in an early stage and research and development are needed to exploit its full potential. An organization can implement an **online threat sharing platform to manage a large volume of threat feeds** and **hire a qualified data analyst to analyze, process, and transform that threat data into actionable intelligence**.