UDC 501

Basic concepts, approaches and fundamentals of cyber threat intelligence

Maryna Makovska [1], Oleh Kozlenko[1]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" ,
Physics and Engineering Institute*

Abstract

This article is designed to introduce readers to Cyber Threat Intelligence (CTI). Various Threat Hunting (TH) techniques and sources of information about threats were mentioned. Commercial tools and open source software for cyber threat hunting are also described.

Keywords: search for cyber threats, CTI, Threat Hunting, MISP, OpenCTI

Introduction

Cyber Threat Intelligence (CTI) is a proactive discipline in the field of cyber security, both in relation to hosts and in relation to networks, and is an analogue of classical intelligence in military affairs. The main function is data collection and information analysis to assess the situation regarding threats to the organization's information system. The result of CTI activities is accurate, up-to-date information. The interaction of cybercriminals, sales and purchases of malicious software, and variety of attacks on businesses currently require collaboration between cybersecurity specialists and, first of all, information dissemination and acquisition about new vulnerabilities and attacks. Presentation of CTI basics, approaches and software projects is the main goal of this article.

1. CTI Levels

Like intelligence in other types of affairs, CTI can be divided into three classes depending on the information and activities of the organization [1]:

1) Strategic level - result of this level's CTI is intended for the understanding for the top management of the organization regarding the main properties of threats and the motivation of attackers who may try to carry out an attack.

2) Operational level – result of this level's CTI is intended for persons who determine the main priorities and allocate resources for the normal functioning of the organization's information system.

3) Tactical level – result of this level's CTI is intended for people who need most detailed and technical information about the behavior of criminals.

Usually, cybercrime, cyberterrorism, hacktivism, cyberespionage are the most interesting areas of malicious activity for CTI. Some targets are representatives of APT groups - the largest professional groups of cybercriminals with high levels of compromise.

Sources of threat information can be many objects:

- use of OSINT tools to obtain publicly available information;
- use of honeypots to obtain information about how attackers will try to compromise the information system;
- use of public and private IOCs, which were obtained in public access or detected in the system;
- use of malware analysis and sandboxing to study behavior of malicious software;

The received information from threat sources should also be classified to create a further strategy for the protection of the information system or to modify an already existing strategy.

2. Threat hunting types

Threat Hunting is also one of the foundations of special type of threat hunting - Intel-Driven Threat Hunting (IDTH). Targeted Hunting Integrating Threat Intelligence (TaHiTI) is one of the main methodologies for IDTH [1]. Its main feature is the integration of CTI in all phases of methodology implementation. Threat intelligence begins with information about an adversary or cybercriminal that has been obtained through CTI sources, then conceptualizing this information in terms of found artifacts or TTPs, and then iteratively using this information to detalied search. The main initiator to start implementation of the methodology are triggers in the information system. TaHiTI consists of the following phases and points [1]:

1) Initiation – receiving the trigger and starting the threat hunting activity. The trigger can be information about cyber threats, as well as monitoring data or indicators of compromise.

2) Search – the process of detailing the situation regarding the trigger that was the initiator in the first phase. The received details of the trigger can lead to a new trigger and, accordingly, to the details of new information.

3) Finalization – the process of documenting the obtained results of the first and second phases and obtaining a general conclusion on the trigger. The result of the third phase is common to the staff and can be studied by interested analysts.

Cyber threat intelligence also includes a set of issues that need to be addressed during the life cycle:

1) The value of information in determining its relevance and value. The complexity of this problem lies in the dynamics of information in terms of its usefulness and depends on the goals of using this information in further actions. Examples of relevant information are:

- analysis of a specific threat;
- additional information about an existing threat (even contrary to the initial analysis);
- threat analysis after or during the incident;

2) Threat analysis i primarily related to the decision of how to present information to the final beneficiary cyber threat intelligence result.

3) Information classification. One of the key factors in the success of cyber threat intelligence is how to disseminate information in detail and how to apply it. For this, the classification of the results plays an important role in the use of the general conclusion.

4) Determination of the degree of confidence in the analysis. Cyber threat intelligence reports often lack information about the likelihood of a threat to an organization or individual system. This raises the question of how to work with information that indicates a low probability of the threat's realization, or whether to spread information about the threat in general or not.

5) Updates to reports/analysis. During the life cycle of cyber threat intelligence, it is necessary to update information about threats that have already been detected.

There is another type of threat hunting - Technique-Driven Threat Hunting (TDTH). It is based on a certain technique of data analysis, which is chosen depending on a number of factors, for example, the environment in which the search is carried out or the volume of data [1]. The most common techniques are:

1) Volume analysis – considers the volume of certain data sets. This can be useful when analyzing the network to detect anomalies. For example, which systems have the most antivirus warnings or which endpoint sent the most data;

2) Frequency analysis – studies the frequency of events. Most often, this method is applied to traffic at the network and application levels, to detect anomalies in malware agents. Frequency analysis is usually combined with volume analysis for a more detailed study;

3) Cluster analysis is a technique based on unsupervised machine learning that finds connections and patterns in large data sets that at first glance are not related at all. Apache Spark, GraphFrames and Jupyter Notebooks can be used for this technique;

4) Stacking – checking similar or identical values in order to find statistical extremes. Sometimes it is possible to detect a noticeable difference in values, which completely goes beyond the specified range. This allows us to speculate on the reason that could have caused this result.

3. Threat hunting tools

Hunting ELK (HELK) [3] is widely used in Threat Hunting. It is an open source platform that includes a large number of analytical capabilities such as graphing, machine learning through Jupyter, Apache Spark notebooks, using an interactive SQL interface for streaming on

Kafka (KSQL) without the need to write code in a third-party programming language. There is also a built-in ElastAlert framework, which notifies about anomalies, high jumps or other interesting changes based on the data in Elasticsearch.

With the help of Sigma, you can describe the developed methods and share them with other people. HELK primarily works with datasets, one of most popular is MORDOR [4] for example. MORDOR provides access to previously encountered security incidents generated as JavaScript Object Notation (JSON) files for convenient access from a web browser. The use of MORDOR data allows you to reproduce a certain threat, investigate it, share the received information with others or use the analytics of previous reports.

OpenCTI is a free open source platform that allows you to structure, store, organize and visualize technical and non-technical information about cyber threats [5]. Main features:

- automatically draws logical conclusions, reveals implicit facts and associations in real time ;
- open architecture provides easy integration with other tools such as MISP, TheHIVE, SIEMonster or MITER ATT&CK;
- user can visualize hyper-objects, hyper-relations, nested relationships for highly accurate threat predictions;
- displays operational and strategic information using a single data model based on STIX2 standards;
- widget development for comparing attack scenarios;

MISP is an open source software platform that allows structured storage and exchange of information about malicious software samples, incidents, detected threats, and visualization of received data [6]. This project includes 40 repositories on Github, for example, a repository of integration modules with other platforms for CTI, a REST API library. This platform integrates with many external sources through developed plugins.

LookingGlass Cyber Solutions is a free, open-source threat analysis platform that provides unified protection against complex cyber-attacks for enterprises and government institutions through operational analysis [7]. It main feature if Threat Indicator Confidence (TIC) - its own data repository. This program combines structured and unstructured data from more than 87 channels.

Anomali ThreatStream is a commercial product that helps to collect, compare and exchange global data and to investigate the infrastructure of attackers [8]. This project collects data from hundreds of sources and combines them into a single set. It has interactive panels with tactical, technical, operational and strategic information about cyber threats. Enables automatic correlation of indicators with TTP in MITER ATT&CK.

Conclusions

The main goal of the article is to familiarize readers with the process of cyber threat intelligence and popular software projects. The main elements of CTI, the main problems that arise when searching for and interacting with information about cyber threats were analyzed in this article. Different approaches, such as IDTH and TDTH, have their advantages and disadvantages, and appropriate designs depend on the chosen approach. Open source software (OpenCTI, MISP, HELK) are the most widely used projects for cyber threat intelligence, but require special approach and administration. Commercial software is ready for integration "out-of-the-box" and does not require technical skills from users.

References

[1]. V. Palacin. Practical Threat Intelligence and Data - Driven Threat Hunting. — 2021.
[2]. MITRE ATT&CK. — Access mode: https://attack.mitre.org/.
[3]. The HELK. — Access mode: https://thehelk.com/intro.html.
[4]. Mordor. — Access mode: https://github.com/UraSecTeam/mordor.
[5]. OpenCTI. — Access mode: https://www.opencti.io/en/.
[6]. MISP Threat Sharing. — Access mode: https://www.misp-project.org/.
[7]. LookingGlass. — Access mode: https://lookingglasscyber.com/.
[8]. Anomali ThreatStream. — Access mode: https://www.anomali.com/products/threatstream.