CTI Challenges and Perspectives as a Comprehensive Approach to Cyber Resilience

Rasim Alguliyev
Institute of Information Technology
Baku, Azerbaijan
r.alguliev@gmail.com

Babak Nabiyev
Institute of Information Technology
Baku, Azerbaijan
babek.nabiyev@gmail.com

Konul Dashdamirova
Institute of Information Technology
Baku, Azerbaijan
konulahmed@gmail.com

2023 5th International Conference on Problems of Cybernetics and Informatics (PCI) | 979-8-3503-1906-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/PCI60110.2023.10325971

***Abstract*—The significant growth in the number, variety, and sophistication of cyber threats in recent years makes traditional approaches ineffective against new generation cyber threats. More effective mechanisms against cyber threats and attacks require intelligent analysis of the threats themselves. Cyber Threat Intelligence (CTI) is a new approach based on artificial intelligence technologies aimed at collecting, analyzing and resolving current and potential attacks that threaten the security of an organization or its assets. This thesis explores CTI technologies and considers problems and advantages in this area.**

Keywords—CTI, cyber security, cyber threat, artificial intelligence

I. Introduction

Currently, information technologies have become one of the most important factors affecting people's lifestyle, education, work, society formation, and also the government's interaction with society. The sharp increase in the number of Internet users every year leads to an increase in the volume of information sharing and the generation of "Big Data". The abundance of information in cyberspace, the ability to influence any IT structure, individual and mass psychology make cyberspace attractive to criminals. Threats that can affect the interests of individuals, society and states are increasing rapidly. Criminals create cyber threats and carry out cyber attacks using various methods and tools. Organized cybercrime has become a global problem and relevant for all countries of the world. But organizations, as well as individuals, stubbornly do not believe that they can become victims of such criminal activity. The fact is that behind all digital data on the Internet, various kinds of cyber threats can be hidden. In most cases, the danger is offensive and harmful in nature. While using various platforms, users can fall prey to malicious actors, lose their intellectual property, expose their online bank accounts, or unintentionally spread malware to other computers on their network. Depending on the targets of the criminals, at a higher level, confidential business information can be stolen and even critical national infrastructures of the country can be damaged.

In 2022, the damage caused by cybercrime at the global level was approximately 8.4 trillion USD. The average cost of data loss was 3.86 million USD in 2020 and 4.24 million USD in 2021. In 2023, the damage caused by illegal activities on the Internet is predicted to exceed 11 trillion USD [1]. Moreover, there is a serious shortage of personnel in the field of cyber security. As of April 2022, there are more than 700,000 cybersecurity job openings in the United States [2].

In such circumstances, multiple security methods are used to detect and prevent cyber attacks. However, the significant increase in the number, variety, and complexity of malware samples in recent years renders traditional security approaches ineffective in the face of new generation cyberattacks.

Cyber-attacks are more effective when actors cooperate with each other and use various tools and services, as well as share experiences on certain platforms. In such circumstances, obtaining information about malicious behavior and the methods used are very important both to prevent them and to fight against them.

Cyber Threat Intelligence (CTI) is a field of cyber security formed on the basis of artificial intelligence technologies aimed at collecting, analyzing and solving information about current and potential attacks that threaten the security of an organization or its assets [3]. CTI is a new approach that enables organizations to learn the goals, tactics and tools of threat actors, to build an effective strategy to protect against cyber attacks, and to collect and evaluate information about current threats and cybercriminal groups. Companies can collect cyber threat information themselves or order it from third-party providers.

II. Cyber Threat Intelligence (CTI)

CTI studies cybersecurity threats, cybersecurity actors, malware, vulnerabilities, data and communications collection, threat assessment, enforcement, and more. Currently, many cyber security companies such as Symantec, McAfee, Trend Micro, FireEye, Cyveillance, Sophos and Kaspersky have developed intelligent analysis of cyber threats and become leading companies in providing this service to government and commercial organizations [4]. Many companies also create their own internal CTI units and collect information about cyber threats themselves.

For CTI to be effective, reliable data sources are required. Regardless of the companies, data is collected from various sources, i.e., network traffic logs, database access logs, configuration change logs, Intrusion Detection System, Intrusion Prevention System, login and access logs, antivirus logs, etc. To support the security community, European Network and Information Security Agency (ENISA) has developed a powerful cyber security detection system called Open Cyber Situational Awareness Machine (Open-CSAM). This tool uses artificial intelligence, natural language processing (NLP), machine learning (ML) technologies to continuously monitor CTI sources and generate reports. The first instance of Open-CSAM was developed in 2018. This was the first step in creating a tool that produces cybersecurity awareness reports [5].

Data for CTI can be collected in structured and unstructured format. Once unstructured data is collected, it is

structured either manually or automatically so that it can be used. Structured Threat Information eXpression (STIX) is an XML programming language designed to translate information about cyber security threats into a language understandable by humans and security technologies. STIX is considered to be a reliable source and the structured data obtained from it conforms to standards. Unstructured data such as reports, websites, or community forums can be problematic to use and require manual data analysis [5].

CTI traditionally analyzes attacks after they occur, leading to countermeasures [4]. Therefore, the analysis of cyber threats should be a continuous and cyclical process. All stages require feedback and analysis to confirm and ensure that useful information is obtained. This process creates a CTI cycle (fig. 1). The data structuring and the specification of their relationships are illustrated in the CTI cycle:

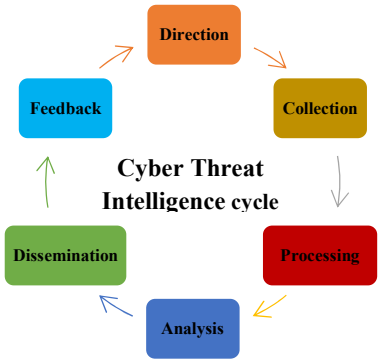


Fig. 1. Cyber Threat Intelligence cycle

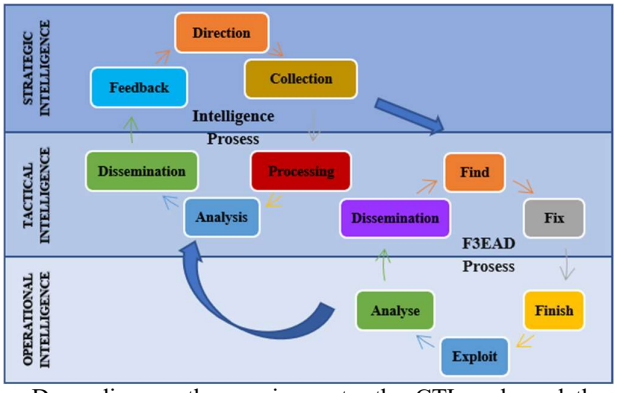
- Direction – the first step is to determine what information is needed to make informed decisions in the shortest possible time.
- Collection - collection of data consisting of digital and physical evidence depending on cyber threats.
- Processing - the process of cleaning the collected data and transforming it into understandable form for user - the process of data structuring is carried out.
- Analysis – following the data structuring, suspicious behaviors and threats are identified using various analysis methods to get detailed information about threats.
- Dissemination – reports from the analysis phase are sent to decision makers.
- Feedback – feedback should be established between the relevant groups of the organization and the CTI team to reanalyze the organization's cyber security.

A threat analysis organization can use a threat taxonomy to assess the likelihood of threat-related actions.

Another approach to threat intelligence analysis is the F3EAD cycle [6]. The F3EAD cycle (Find, Fix, Finish, Exploit, Analyze and Disseminate) is an alternative reconnaissance cycle used by western military forces, with deadly consequences for drone strikes or special forces. The concept of the F3EAD cycle is applied to the field of information security, implementing the practice of "find, delete and move on", which is the basis of the F3EAD cycle (fig. 2). This approach combines practical and intellectual process. A basic summary of the cycle stages is as follows:

- Find – answers to the questions "who, what, when, where, why" are sought at this stage to identify a potential target.
- Fix – checking of the target(s) defined in the previous step is performed.
- Finish – the process of destroying the target is carried out based on the evidence obtained from the previous two stages.
- Exploit – at this stage, the evidence obtained is deconstructed.
- Analyze – the results are analyzed.
- Dissemination – the results of the study are sent to key stakeholders.

Fig. 2. F3EAD cycle



Depending on the requirements, the CTI cycle and the F3EAD cycle can be used closely together to conduct both tactical and strategic analysis [11].

David Bianco presented a new approach to detect and respond to cyberthreats [5]. A graphical representation of the CTI application was developed. The "Pyramid of Pain" shows the hierarchical relationship between the types of indicators used to detect the actions of entities and "how much damage they will do if you deny these indicators" (fig. 3). The higher the pyramid, the longer indicators will be available.

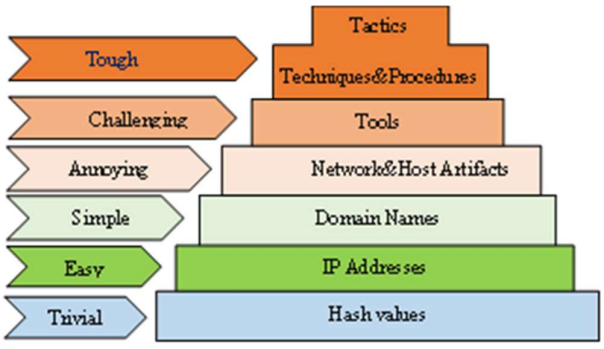


Fig. 3. Pyramid of Pain

Attention should be paid to a higher level IoC (Indicator of Compromise). IoC - in the field of computer security, an object (or activity) observed in a network or on a certain device indicates, with a high probability, unauthorized access to the system. Such indicators are used to detect malicious activity initially and block known threats.

IoC collected from all levels of the pyramid can be investigated and remedied by Security Information and Event Management (SIEM).

III. CTI and Artificial Intelligence Technologies

As cyberthreats become more complex, stealthy, and traditional security systems become ineffective in combating flexible and ever-changing cyberattacks, new advanced approaches based on artificial intelligence technologies are required to fight cybercrime. Currently, in the field of cyber security, there is a great need for artificial intelligence technologies to improve the protection of information systems. Artificial intelligence with powerful automation and data analysis capabilities can be used to analyze large volumes of data efficiently, accurately and quickly. Cyber security solutions based on artificial intelligence can provide the latest information about global and man-made threats.

AI methods can be applied to a number of cybersecurity challenges:

- Detection of spam and phishing pages;
- Malware detection and identification;
- Detection of DoS and DDoS attacks;
- Anomaly detection;
- Biometric recognition;
- Social media analytics;
- Detection of data leakage;
- Detection of advanced persistent threats;
- Detection of vulnerabilities in software, etc. [7].

Artificial intelligence has a number of advantages in the field of cyber security in the following aspects [8, 9]:

- Artificial intelligence can detect new complex changes in previously recorded incidents.

Traditional technologies focus on the past and are mainly based on known attacks and allow threats that are not similar to previous threats to enter the system without paying attention to the vulnerabilities in the protection of the information system. Deficiencies in old digital information security systems are now being overcome with the help of intelligent technologies. AI solutions can be used to detect advanced cyberthreats faster and more accurately by remembering previously recorded threats. This is especially true as cyber attacks become more sophisticated, and hackers develop new and innovative approaches.

- Identification of emerging threats;

Artificial intelligence can be used to identify cyber risks and potentially dangerous activities. Since traditional software systems cannot deal with the large volume of new viruses emerging every week, AI can be effective in this area. Artificial intelligence systems can be used to predict cyber attacks and detect malware before it enters the system using complex algorithms. Artificial intelligence gathers material for itself by scanning articles, news and more, and provides better predictive information through computer linguistics. It can provide information on emerging anomalies, cyber attacks and countermeasures.

- Attack Bots;

Bots now make up a significant portion of internet traffic, and they can be dangerous. Bots can be a real threat, from account takeovers using stolen passwords to fake account creation and data theft. Automated threats cannot be defeated with manual responses alone. Artificial intelligence and machine learning methods help analyze data about website traffic and distinguish good bots (e.g., search engines) from malicious bots.

- Predicting an unauthorized system risk access;

Artificial intelligence technologies help define IT asset inventory, a complete and accurate list of all devices, users, and applications that have varying degrees of access to systems. AI-based solutions can predict how and when a system will be hacked. Reports from AI-based analysis help improve policies and procedures aimed at strengthening overall cyber resilience.

- Protection of remotely connected devices;

The number of devices connected remotely to the network is increasing rapidly, and each of them can be secured through artificial intelligence solutions. Antivirus programs and secure virtual private networks (VPNs) can help protect against malware and virus attacks; however, this approach is not reliable due to the lack of updating of the antivirus solution by the user or, in some cases, insufficient knowledge of the software developers. Artificial intelligence uses a new approach based on a repeated learning procedure to protect remotely connected devices.

- Large volumes of data can be managed through artificial intelligence technologies.

AI can create autonomous security systems to detect attacks and respond to breaches to improve network security. The number of security alerts received daily can be overwhelming for security teams. Automated threat detection and response can help reduce the workload of experts and detect threats faster than other methods. With large amounts of security data being generated and transmitted over the network every day, network security professionals are challenged to track and identify attack agents quickly and reliably. Artificial intelligence can help monitor and detect suspicious behavior. This will help network security personnel to quickly respond to situations they have not encountered before.

Machine learning algorithms are used to detect and respond to cyber attacks. ML can analyze large volumes of data collected about security incidents to identify patterns of malicious activity.

IV. AI Applications for Cyber Security

Currently, a number of IT applications are applied in the field of cyber security. They may include [10]:

EDR (Endpoint Detection and Response) is a class of solutions for detecting and analyzing malicious activity on remotely connected devices: networked workstations, servers, IoT devices, etc. The collected data is analyzed using machine learning technologies. Their IoC are compared to data on other sophisticated threats available. If the EDR system detects an incident with cyber incident signs, it notifies the security staff about it. Artificial intelligence makes decisions based on a

common knowledge base gathered by collecting data from multiple devices.

NDR (Network Detection and Response) - devices and analytical platforms that detect attacks at the network level and allow to quickly respond to them. NDR uses both artificial intelligence and machine learning methods to detect network anomalies. The system first creates a base for the daily operation of the network. It then continuously monitors the network to detect deviations from the baseline (networked attacks).

UEBA (User and Entity Behavioral Analytics) - systems aimed at finding and identifying anomalies in the behavior of users and various systems. Since many different data collection systems are used in companies to ensure information security, the class of Behavioral analysis systems was created. At the same time, employees cannot always review all available information and respond to potential incidents in time. UEBA systems increase efficiency by profiling and ensure timely response to potential data breaches.

TIP (Threat Intelligence Platform) is a platform that helps to analyze potential threats and, accordingly, the measures to be taken to eliminate them. Threat intelligence platforms can be formed in the form of SaaS or local solutions. With the help of such platforms, four main functions are performed:

A. collection of information from several sources;

B. data structuring, enrichment and risk assessment;

C. integration with existing security systems;

D. data analysis and sharing about threats.

SOAR (Security Orchestration, Automation, and Response) refers to a set of software solutions and tools that enable organizations to optimize security operations in three key areas: threat and vulnerability management, incident response, and automation of security operations.

Application Security – tools aimed at protecting software products from threats.

Antifraud is a system that analyzes purchases made on websites to detect fraudulent transactions. It collects data about user behavior. It compares them with suspicious samples to confirm or reject the order. Thus, it adds an additional layer of security to the business process to prevent fraud. Fraud protection systems use artificial intelligence technologies to identify deviations from established business processes, thereby helping to quickly respond to possible financial crimes 6].

V. Current Problems in CTI

In addition to CTI being a new approach, there are also a number of actual problems [11]:

- The fewer updates, the less attention is paid to security. This is an inherently dangerous approach to cyber risk management.
- A functioning cyber security system does not necessarily mean preventive behavior/measures.
- In addition to ensuring safety, efforts should be made to increase the efficiency of existing technologies.
- Determining the attack vector;
- Attack indicator detection;
- Determination of corporate security priorities;
- Employee cyber security, as well as critical intellectual property and corporate data must be protected.

VI. A New Method Based on CTI Levels

Depending on the initial requirements, data sources, objectives and scope, CTI is mainly implemented at four levels: strategic, tactical, technological and operational [12]. Each of the four levels is necessary for a comprehensive threat assessment.

The strategic level - is a generalized analysis of potential cyber-attacks and their possible consequences for decision-makers. It is presented in the form of official documents, reports and presentations and based on a detailed analysis of emerging risks and trends from around the world. It is used to create a high-level view of an organization's cybersecurity landscape.

Tactical level - provides information about tactics, technological procedures used by threat actors. It is designed for professionals directly involved in the protection of IT and information resources. It provides detailed information on how an organization can be attacked, based on the best ways to protect against or mitigate the effects of the latest attacks in use.

Technological level - focuses on the signs that indicate the beginning of a cyber attack, whether it is phishing, social engineering, etc. At the technical level, it plays an important role in preventing social engineering attacks. Applied technologies must adapt to the new reality as corporations update their tactics to exploit new loopholes and tricks.

Operational level - is based on the data collection from various sources, including operating systems, network, logs, etc. It is used to predict the nature and timing of future attacks. Data mining and machine learning methods are often used to automate the processing of hundreds of thousands of data in several languages.

The thesis proposes a new approach for the intelligent analysis of threats, i.e., a supersystem (fig. 4). A detailed analysis of the levels of the supersystem is given below:

At the operational level, information about incidents from various sources is collected, monitored and aggregated, the threats are detected by analyzing collected log files. CERT and CSIRT perform this activity at the corporate, national, regional and global levels. However, considering the requirements of the modern era, the intensity of events, the multitude of generated information sources, the heterogeneity of systems and the variety of log files slow down the process of threats' identification and do not provide operational efficiency. CERT based on artificial intelligence technologies should be established in order to collect only appropriate data from the large volume of data to be collected and according to the specified indicators. It is important to establish the CERT.AI model for collecting information in a short time, monitoring and prompt identification of threats.

Detected incidents are explored at the technological level. At the operational level, detected security incidents are analyzed in real time, types of cyber threats, goals and targets, causes of cyber incidents, and hazard rate are determined. The measures to be taken to prevent this type of cyber threats in

the future are determined. The security of information, telecommunications and other critical resources is evaluated operationally. The main goal is to analyze incoming log files from various sources and prepare solutions and recommendations for preventing emerging threats. Currently, SIEM performs these functions. Intelligent SIEM can detect new variants of previously known threats by learning the characteristics of security events, and respond to security events in real time. When the intensity of cyber-attacks is increasing and transformation is undergoing, it is necessary to establish SIEM.AI based on new artificial intelligence technologies for faster detection and prevention of cyber-threats.

At the tactical level, the cyber security strategy of the system should be determined, the cyber security policy should be established, and the priorities should be determined. In order to manage the entire process, the roles within the system should be defined, registers should be created, and instructions should be prepared in accordance with events and threats. Currently, this function is performed by the SOC. SOC analysts monitor an organization's network 24/7 and explore potential security incidents.

There are certain intersections in duties and functions between CERT/CSIRT, SIEM and SOC systems. Methods should be developed to determine the exact distribution of roles and responsibilities on the above-mentioned levels of the system.

Fig. 4. A new method based on CTI levels

We must take into account that in corporate environments, a company may have a department in the national, regional and global framework, and each department should be managed under a unified system. In this regard, following the establishment of intelligent CERT, SIEM, SOC at all levels, a supersystem that can control the whole process will be required. Intelligent CERT/CSIRT, SIEM, SOC created at the strategic level will be integrated into a single supersystem under an umbrella of CTI. Data obtained from CERT.AI, SIEM.AI and SOC.AI levels will be processed through Cyberthreat Intelligence (CTI) and reports will be prepared to support decision-makers.

VII. Conclusion

In conclusion, integrating an aggregator artificial intelligence (AI) supersystem within CTI processes for CERT, SIEM and SOC brings significant benefits. By applying artificial intelligence methods, organizations can efficiently collect, process and analyze various monitoring data from various sources. This increases the accuracy of threat detection and response and real-time intelligence. The AI supersystem's capacity to learn threats, adapt and automate the process improves the overall security posture and enables proactive countermeasures against evolving cyberthreats. Full feedback between AI and human analysts is critical to ensure accurate decision-making.

References

[1] Estimated cost of cybercrime globally 2016-2027 https://www.statista.com/statistics/1280009/cost-cybercrime-

[2] White House Pushes to Fill 700,000 Cybersecurity Jobs in U.S. https://www.dice.com/career-advice/white-house-pushes-to-fill-700000-cybersecurity-jobs-in-u-s

[3] Trifonov R., Nakov O., Mladenov V. Artificial intelligence in cyber threats intelligence // 2018 international conference on intelligent and innovative computing applications (ICONIC), IEEE, 2018, pp.1-4.

[4] Samtani S. et al. Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence // Journal of Management Information Systems, 2017, T. 34, №. 4, pp.1023-1053.

[5] Tatam M. et al. A review of threat modelling approaches for APT-style attacks // Heliyon, 2021, T. 7, №. 1, pp.05969.

[6] Methods and Methodology. https://www.first.org/global/sigs/cti/curriculum/methods-methodology

[7] Thomas T., Vijayaraghavan A. P., Emmanuel S. Machine learning approaches in cyber security analytics, Singapore: Springer, 2020, pp.37-200.

[8] Mohammed I. A. Artificial intelligence for cybersecurity: A systematic mapping of literature // Artificial Intelligence, 2020, T. 7, №. 9, pp.172-176

[9] Truong T. C. et al. Artificial intelligence and cybersecurity: Past, presence, and future // Artificial intelligence and evolutionary computations in engineering systems, Springer Singapore, 2020, pp.351-363.

[10] Skrypnikov A.V. et al. Solving problems of information security with the use of artificial intelligence, 2021, №. 6-2, pp.277-281.

[11] Conti M., Dargahi T., Dehghantanha A. Cyber threat intelligence: challenges and opportunities, Springer International Publishing, 2018, pp.1-6.

[12] Wagner T.D. et al. Cyber threat intelligence sharing: Survey and research directions //Computers & Security. 2019, T. 87, pp.101589.