http://doi.org/10.35784/iapgos.2822

APPLICATION OF THE THREAT INTELLIGENCE PLATFORM TO INCREASE THE SECURITY OF GOVERNMENT INFORMATION RESOURCES

Bohdan Nikolaienko[1], **Serhii Vasylenko**[2]

[1]Institute for Special Communication and Information Protection of the National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Department of Telecommunication Systems, Kyiv Ukraine, [2]Institute for Special Communication and Information Protection of the National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Research Center, Kyiv, Ukraine

Abstract. *With the development of information technology, the need to solve the problem of information security has increased, as it has become the most important strategic resource. At the same time, the vulnerability of the modern information society to unreliable information, untimely receipt of information, industrial espionage, computer crime, etc. is increasing. In this case, the speed of threat detection, in the context of obtaining systemic information about attackers and possible techniques and tools for cyberattacks in order to describe them and respond to them quickly is one of the urgent tasks. In particular, there is a challenge in the application of new systems for collecting information about cyberevents, responding to them, storing and exchanging this information, as well as on its basis methods and means of finding attackers using integrated systems or platforms. To solve this type of problem, the promising direction of Threat Intelligence as a new mechanism for acquiring knowledge about cyberattacks is studied. Threat Intelligence in cybersecurity tasks is defined. The analysis of cyberattack indicators and tools for obtaining them is carried out. The standards of description of compromise indicators and platforms of their processing are compared. The technique of Threat Intelligence in tasks of operative detection and blocking of cyberthreats to the state information resources is developed. This technique makes it possible to improve the productivity of cybersecurity analysts and increase the security of resources and information systems.*

Keywords: Threat Intelligence, cybersecurity, cyberdefense

ZASTOSOWANIE PLATFORM THREAT INTELLIGENCE DO ZWIĘKSZENIA OCHRONY ZASOBÓW INFORMACJI PUBLICZNEJ

Streszczenie. *Wraz z rozwojem technologii informacyjnych wzrosła potrzeba rozwiązania problemu bezpieczeństwa informacji, gdyż stała się ona najważniejszym zasobem strategicznym. Jednocześnie wzrasta podatność współczesnego społeczeństwa informacyjnego na nierzetelną informację, nieterminowe otrzymywanie informacji, szpiegostwo przemysłowe, przestępczość komputerową itp. W związku z tym, jednym z ważniejszych zadań jest szybkie wykrywania zagrożeń, w kontekście pozyskiwania informacji o napastnikach, możliwych technikach i narzędziach cyberataków, wraz z metodami ich opisu i szybkiego reagowania na nie. W szczególności wyzwaniem jest zastosowanie nowych systemów zbierania informacji o cyberzagrożeniach, reagowania na nie, przechowywanie i wymiana tych informacji, a także, na ich podstawie, metod i środków znajdowanie napastników z wykorzystaniem zintegrowanych systemów lub platform. W celu rozwiązania tego typu problemów badany jest obiecujący kierunek Threat Intelligence jako nowy mechanizm pozyskiwania wiedzy o cyberatakach. Zdefiniowano Threat Intelligence w problemach cyberbezpieczeństwa. Dokonano analizy wskaźników cyberataków i narzędzi ich pozyskiwania. Porównywano standardy opisu wskaźników kompromisów oraz platformy ich przetwarzania. Opracowano technikę Threat Intelligence w zadaniach operacyjnego wykrywania i blokowania cyberzagrożeń dla zasobów informacyjnych państwa. Technika ta pozwala na zwiększenie produktywności analityków cyberbezpieczeństwa oraz zwiększenie bezpieczeństwa zasobów i systemów informatycznych.*

Słowa kluczowe: Threat Intelligence, ceberbezpieczeństwo, cyberochrona

Introduction

Several years ago, the main vectors of cyberthreats that cybersecurity experts worked with were mass cyberattacks. Today, these attacks are seen as secondary threats that simply create "noise" in the network. For the most part, organizations and institutions successfully protect themselves from them by analyzing the first cases of cyberattacks, forming their indicators of compromise (IoC) and rapidly disseminating these indicators. The most serious violations of cybersecurity are due to well-planned, complex attacks targeting specific companies or industries. Well-funded attackers make it difficult to detect their attacks by using social engineering techniques that cannot be identified by simple indicators of compromise or blocked by traditional means of protection.

In addition, the number of cyberthreats themselves is growing rapidly. Attacks and, as a result, compromise computer networks can take minutes, and the process of detecting, responding to, and eliminating the effects of an attack takes days, weeks, and even months. Most often, detection occurs after the state information resources are compromised. According to Cisco's annual information security report [13], security professionals are able to process only 56% of incoming threat messages during their business day, and only one in two (i.e. 28%) is considered valid. Thus, 44% of incidents go completely unnoticed. At the same time, organizations critically lack not only resources to handle all incidents, but also a common system that would make it possible to respond to them at an early stage - ideally before operation, as well as to accumulate distributed knowledge about threats, share data. To investigate the causes of threats and respond to them immediately. Data from a variety of sources should be used to gather information about potential threats more quickly. It is important that this information is standardized, i.e. standards and protocols for data transmission and provision must be defined in advance for all players. One of the most important functions of effective protection of the organization's information system is threat tracking. Threat Intelligence (TI) is used to mitigate adverse events in cyberspace [10]. The TI system allows you to detect threats and attacks before they can affect the system. In the event that an incident does occur, TI allows you to analyze and, based on the investigation, expand your knowledge base with context, mechanisms, indicators of compromise, and threat analysis.

At the same time, it is not necessary to translate the concept of Threat Intelligence verbatim and understand it as the investigation of threats in cyberspace in the sense specified in [7]. The word "Intelligence" in English, in addition to the meaning of "intelligence", in the sense of a military unit or the process of obtaining hidden information about countries, companies, etc., also means "the ability to understand, study, form judgments and opinions based on facts." Therefore, along with the definition of Threat Intelligence as threat intelligence, it is advisable to use analogues – the acquisition of knowledge about threats, or knowledge about threats in general. It is in this context that Threat Intelligence is one of the processes of cybersecurity.

1. Analysis of recent research and publications

In [19] provides information on the limitations that arise when exchanging information about cyberthreats within TI platforms, as well as ways to address these limitations and options for using TI platforms. The best practices for the use of TI, trends in this regard and the main definitions in the field of TI are given in [5].

The question of the relationship between the tasks of Threat Intelligence and Threat Hunting in the investigation of cyberattacks, reproduction of tactics of attackers according to the model MITER ATT & CK and tools that can be used in this case are given in [2]. At the same time, the issue of increasing the security of state information resources through the use of the TI platform directly in the tasks of rapid detection and blocking of cyberthreats in the known literature was not considered.

Therefore, the purpose of this article is to consider the possibility of increasing the security of public information resources through the use of Threat Intelligence in the tasks of operational detection and blocking of cyberattacks and cyberthreats.

2. Presenting main material

Threat intelligence, the acquisition of knowledge about threats (Threat Intelligence) is defined as a set of knowledge that is built on observations, and includes indicators of compromise, mechanisms and context of attacks, as well as practical recommendations for eliminating identified and potential threats. Cyberintelligence services combine cybermonitoring infrastructure with the findings of specialists from the centers of investigation and response to incidents. Data for the nfrastructure comes from a distributed monitoring network, Honeypot-traps, the results of botnet analysis, various conferences, private groups on social networks, as well as the exchange of information between associations to combat cyberthreats [14].

An important component of effective protection against threats is information about them, which allows you to anticipate attacks and prepare for them in advance, rather than dealing with costly and long-term elimination of their consequences. By processing and analyzing data from hundreds of sources, you can get personalized, verified and meaningful information about current threats.

The information obtained during TI is diverse – from network artifacts and indicators of compromise to the identification of the attacker. Moreover, for example, for technicians to configure the means of protection is more important information about the indicators of compromise. Therefore, there is a need to separate certain levels of TI and information that is extracted and processed at these levels. Currently, there is no generalized distribution of TI levels, so, based on the analysis of existing representations of TI levels by different organizations [15, 16, 18], TI levels and source information processed at these levels in specific organizations have been generalized (Table 1).

As we see in table 1, these sources define 3 (tactical, operational, strategic), or 4 (tactical, technical, operational, strategic) levels of TI. The definition of such levels is due to the different nature of the data extracted and processed during TI. The same data are assigned to different specialists. For example, a national activity report cannot be compared to an IP address, and cannot be applied in the same way. Summarizing the information obtained during the analysis of TI levels and data on these levels, taking into account the existing levels of martial arts in Threat Intelligence, we distinguish three separate levels (strategic, operational and tactical) and consider them in more detail.

At the strategic level, high-level information is processed, on the basis of which specific management decisions are made to counter the threat. The purpose of the TI strategic level is to help strategists understand current and probable risks, obtain the attributes of attackers, identify them, define their strategies and goals. Intelligence materials are often presented in the form of reports describing the geopolitical situation, the activity of ART groups in the direction of the organization, trends in cyberattacks, high-level risks, the likelihood of their implementation and ways to address these risks. This information is obtained from open source intelligence (OSINT), obtained from reports of analytical organizations, from computer incident response teams (CERT) and cybersecurity companies in the form of "feeds" [17]. It should be noted that from these sources it is possible to obtain relevant information for the operational and tactical levels of TI. Threat hunting technologies and network forensic analysis are also used to obtain information that is assessed at the strategic level. This information provides analysts with a strategic level of understanding of the threat landscape in their infrastructure.

At the operational level, information is obtained about possible attacks on the organization, their possible tactics, as well as techniques and procedures that have already taken place. This information is obtained by analyzing events detected by network security tools (firewalls, Honeypots and Honeynets network lures), end device security tools. These protections typically act as data sources for the SIEM network event and message management system, through which professionals can aggregate, correlate, and process detected events to identify tactics, techniques, and procedures for attacks that have already taken place. At the same time, information obtained from open sources or "feeds" on possible complex ART attacks is used to configure these protections.

At the tactical level, during threat detection, based on data from intrusion detection and prevention systems (IDS/IPS), network sensors, server log file data, end devices, specialized security tools (eg, Security E-mail Gateway), network artifacts and identifiers of computer network compromise and the hypothesis of attack tools. The use of a network scanner and a vulnerability scanner provides information about existing vulnerabilities in computer network components. OSINT also provides information on vulnerabilities and compromise identifiers that are specific to an organization's computer network. Based on the data obtained, network administrators or information security specialists can respond to a cyberattack, configure and adjust the rules for detecting attacks in computer network security systems. The described levels of TI are summarized in table 2.

Table 1. TI-levels and source information processed at these levels in specific organizations

Organizations	TI levels	Source information
National Center for Cyber Security of the United Kingdom (NCSC)	1. Tactical	methodologies, tools and tactics, actions and more about attackers
	2. Technical	indicators of certain malware
	3. Operational	details of a specific incoming attack, assessment of the organization's ability to identify future cyberthreats
	4. Strategic	high-level risk reduction information (strategic shifts) - senior management assesses threat assessments
Threat Connect	1. Technical	indicators of compromise, detection of signatures
	2. Tactical	methodologies, tools and tactics
	3. Operational	compromise indicators
	4. Strategic	risk reduction due to threat models, capabilities of attackers
National Institute of Standards and Technology (NIST)	1. Tactical	security alerts, signature detection, and in advanced cases, some form of kill chain analysis based on information about attackers or network behavior
	2. Operational	identification of botnets, malware, phishing, etc.
	3. Strategic	determining the intentions and capabilities of attackers
Fortinet	1. Operational	structured data, indicators of compromise
	2. Tactical	low-level reports or structured data, understanding of attackers' tactics, techniques and procedures
	3. Strategic	high-level reports, models of attackers, their intentions, motivation, plans

The analyzed sources and generalized levels of TI provide an understanding only of what information is extracted, processed and used at each of these levels. This corresponds to the approaches to building an organizational and technical model of cybersecurity, given in [3]. Of course, the ultimate goal of both TE and cyberattack investigation is to identify the perpetrator and his intentions. To achieve this goal, we use formalized models to detect intruders in cyberspace, which directly operate on the information obtained during TI on the basis of Q- and Diamond models [6]. Consider these models in terms of their application in TI.

The Q-model is designed as a map of the attribution process: it allows, not having sufficient technical base, to implement a detailed attribution of a cyberattack (Fig. 1) [4].

Table 2. TI-levels

	Levels	Source information
Threat Intelligence	Strategic	Identification of the enemy, his possible names, pseudonyms, e-mail addresses, etc. Defining intentions and opportunities, reducing risks by studying threat models
	Operative	Understanding the tactics, techniques and procedures of the enemy, responding to attacks, writing rules for defense mechanisms
	Tactical (technical)	Tools, network artifacts, compromise indicators

The use of the Q-model allows scientists, as well as politicians or managers, to increase significant technical detail and communicate meaningfully with technicians. The model also allows forensic experts to assess the strategic and political context. The model itself has three levels (strategic, operational, tactical) and is divided into three stages (conceptual, empirical, communicative). The first stage is conceptual: it presents attribution as a process of discussing the model in general terms, introducing several critical differences and dynamics. During this stage, specialists must answer the questions of how (tactical level), who (operational), why (strategic level) carried out the attack, what was his goal, strength and means. The empirical level raises clarifying, specific questions to the conceptual level, providing answers to which it is possible to find indicators of compromise for a more accurate attribution of the attacker. The communication stage determines the completeness of information and the subjects to whom it is transmitted during the exchange of research results, as well as the order of this exchange. The ultimate goal of attribution in the Q-model is to define an organization or government, not individuals. But through labeling, unification, and geotagging, individual indicators can be powerful evidence links between artifacts and specific organizations.

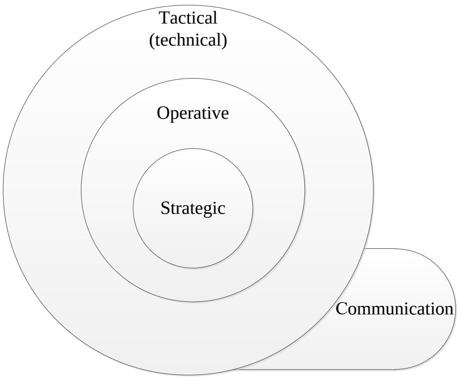

Fig. 1. Q-model

The diamond model describes a cyberattack as part of four main functions: attacker, infrastructure, capability, and victim [11]. These features are associated with the vertices, which represent their main relationship and are located in the shape of a diamond (Fig. 2).

This model also defines additional functions to support higher-level constructs, such as combining events together in activity streams and their subsequent integration. The model establishes a formal method that applies scientific principles to intrusion analysis, including measurement, testing, and repeatability. This scientific approach and simplicity can improve analytical efficiency and accuracy. Finally, this model provides the ability to integrate real-time threat intelligence to protect the network, automatically correlate and classify events. In its simplest form (Fig. 2), the model describes the enemy's ability to attack the victim's infrastructure. These elements are called events and are filled in by the analyst in case they are detected during threat investigation or cyberattack investigation. The vertices are connected by edges and distinguish connections between functions. Going along the edges and vertices, analysts find more information about the operations of the attacker and discover new capabilities (capabilities), infrastructure and victims. The event determines only one step in the series that the opponent must perform to achieve his goal.

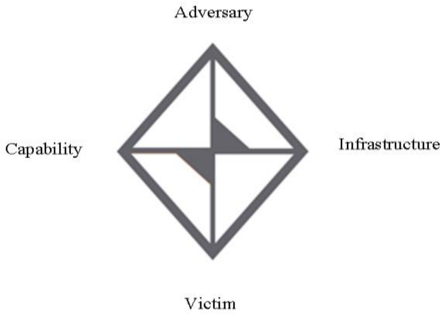

Fig. 2. Diamond model

In addition to the Q- and Diamond models, which directly describe the process of conducting TI, it should be noted the existence of such models as Kill Chain and MITER ATT & CK, which describe the behavior of the attacker during a cyberattack. Thus, the Kill Chain model determines the typical course of action of the attacker to achieve the goals [1]. To succeed, an attacker must usually go through all eight stages (intelligence, weapons, delivery, infection, installation, management, action, destruction of traces). The MITER ATT & CK matrix is a structured list of known behaviors of attackers, divided into tactics, techniques and procedures, expressed in the form of tables (matrices). Matrices for different situations and types of attackers are published on the MITER website [3]. The ATT & CK matrix can be useful for cyberintelligence because it allows you to standardize and describe the behavior of attackers.

As mentioned above, the information obtained during the TI, the identified indicators of compromise and threats, the order and format of the exchange of messages and reports need to be standardized. There are the following standards of description [8]:

- low level data (PCAP, CEF);
- indicators of compromise (MAEC, MMDEF, Snort rule, CybOX);
- enumeration (CVE, CWE, CPE);
- quantitative description of threats (CVSS, XCCDF);
- report formats (CVRF, IODF, STIX).

By using one of the standard formats, an organization can minimize the ambiguity of information, as well as use tools that support the exchange of these standards. However, there are other important technical considerations for the exchange of information, in particular the transport mechanisms used to request and transmit data. In addition, when using non-standard data formats, the choice of sorting method can have significant implications for overall performance and ease of integration with existing tools. Table 3 presents the standards, their levels, the ability to present information and an example of programs that use them.

Table 3. Standards and tools for information exchange and processing

Standard level	The name of the standard	Ability to present information	Programs that use the standard
Low level data	PCAP	packet taken from the network	Tcpdump, Wireshark
	CEF	event logging by hardware	ArcSight SIEM
Indicators of compromise	MAEC	characteristics of SPZ and their actions	Anubis, ThreatExpert, Cuckoo Sandbox
	MMDEF	file names, hash files, SPZ behavior	Cuckoo Sandbox
	Snort rules	IP addresses, ports, protocol, destination, HTTP request and response parameters	Snort, Suricata
	CybOX	network streams, network artifacts, files, SMS, images, emails	python-cybox
Enumeration	CVE	description of threats	STIX, VERIS
	CWE	a description of frequently used threats	IODEF-SC
	CPE	names of operating systems, software packages, classes of hardware devices	MAEC, CybOX
Quantitative description of threats	CVSS	threat assessment from 0 to 10	IODEF-SC, Cuckoo Sandbox
	XCCDF	full description and environment in which the threat is realized	SCAP
Report formats	CVRF	describes the entire lifecycle of vulnerability processing	Used within supplier communications
	IODEF	XML format, incident information exchange	ArcSight
	STIX	a full description of events by one of the above standards	CRITs, Microsoft Interflow

Currently, there is a critical lack not only of resources to handle all cybersecurity incidents, but also of common systems to respond to them in the early stages of cyberattacks, as well as to extract and accumulate distributed knowledge about threats, share data, investigate causes of attacks, respond to them and find perpetrators. Therefore, the main cyberintelligence platforms (Threat Intelligence Platform – TIR) that perform these tasks were considered, as well as a table on the capabilities of these platforms according to TI levels (table 4). The capabilities, functions and purpose of each platform are covered in detail in the public domain.

Thus, the threat intelligence platform can be deployed as software as a service to facilitate cyberintelligence management, accumulation and exchange of information about objects such as attackers, companies, incidents, vulnerabilities and TTP [12]. This is determined by its ability to perform four key functions: aggregation of intelligence from multiple sources; adjustment, normalization, enrichment and risk assessment; integration with existing security systems; analysis and exchange of information on threats. At the same time, not all TIRs can collect, process and exchange information at all levels of TIs, nor are general methods of the TI process known. Therefore, the following TI technique is proposed in the tasks of operative detection and blocking of cyberthreats to state information resources (Fig. 3).

Table 4. Comparison of major intelligence platforms according to TI-levels

Platform	Type	Levels		
		Tactical	Operational	Strategic
MISP	open	+	+	-
CRITs	open	+	+	-
TheHeroic	open	+	+	+
YETI	open	+	+	-
GOSINT Framework	open	+	+	+
R-Vision	open	+	+	+
ThreatStream	commercial	+	+	+
IBM QRadar Security TI	commercial	+	+	-

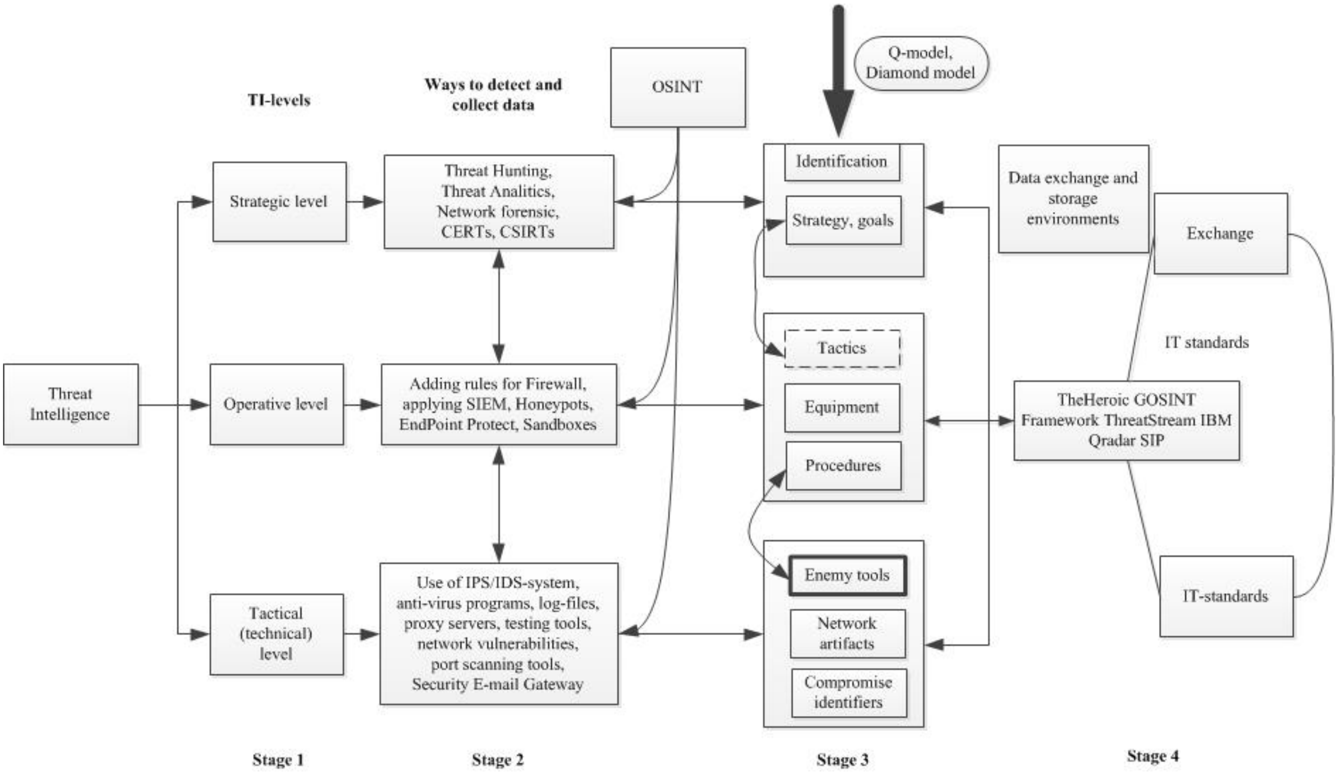
TI-levels
Ways to detect and collect data
OSINT
Q-model, Diamond model
Strategic level
Threat Hunting, Threat Analitics, Network forensic, CERTs, CSIRTs
Identification
Strategy, goals
Data exchange and storage environments
Exchange
IT standards
Threat Intelligence
Operative level
Adding rules for Firewall, applying SIEM, Honeypots, EndPoint Protect, Sandboxes
Tactics
Equipment
Procedures
TheHeroic GOSINT Framework ThreatStream IBM Qradar SIP
Tactical (technical) level
Use of IPS/IDS-system, anti-virus programs, log-files, proxy servers, testing tools, network vulnerabilities, port scanning tools, Security E-mail Gateway
Enemy tools
Network artifacts
Compromise identifiers
IT-standards
Stage 1
Stage 2
Stage 3
Stage 4

Fig. 3. TI methodology

The proposed TI technique (Fig. 3) is divided into four stages:

In the first stage, it is proposed to divide threat intelligence into three levels: tactical (technical), operational and strategic, according to which the tools for detection and data collection are determined (stage 2).

In the second stage, the analysis of attacks is performed using tools to detect and collect data. Stage 2, according to the model of the sequence of actions of the enemy's attack, has three sub-stages, namely: collection of attack data, processing, response and definition of strategies and goals of the attacker.

Attack data collection involves the use of IPS / IDS, SIEM, anti-virus programs, log files, proxy servers, network vulnerability testing tools, port scanning tools, Security E-mail Gateway and others.

After collecting all possible data on the cyberattack, they are processed and responded to incidents. This is possible by adding rules for Firewall, using SIEM, Honeypots, Honeynets, EndPoint Protect, Sandboxes, etc.

The last step of stage 2 is to determine possible data about the enemy, his strategies and goals . To do this, TI analysts use Threat Hunting methods, conduct network investigations using OSINT tools. OSINT tools can also be used during the third step to search for enemy data and possible threats.

In the third stage, threat attributes are identified and standardized according to TI levels. As malefactors have various motives, the purposes, ways, tools, for their identification it is necessary:

- collect and characterize all evidence using threat description standards (compromise indicators, network data and enemy tools);
- on the basis of the collected data and tools of cyberattack to define tactics, techniques and procedures according to which malefactors realize the purposes and to take measures for reaction to incidents;
- show the purpose of the attackers and how they will achieve the desired result, try to identify the attacker or group of attackers.

To perform these tasks, different models of detection and response to intrusion (Q- and Diamond models) should be used.

The final stage involves defining the storage environment and sharing the attributes of threats collected in the previous phase. Formalization of the exchange of such data is provided by special standards, which are considered in Table 3.

3. Conclusions

Built complex information security system, information security systems and information security management system on the objects of information activities, which process state information resources, the binding nature of which is defined in [20] require increasing their efficiency through the use of computerized methods and tools. Such tools allow automating the processes of data collection, detection and processing of new threats, their blocking and further study in order to develop general recommendations for protection against them.

The paper considers the essence of TI as a new type of intelligence, defines the levels of intelligence and their representation by different organizations, analyzes the main models for detecting intruders, based on the ontological approach shows the features of the offender's tactics, techniques and procedures for targeted cyberattacks. Provide a description and formalization of the exchange of indicators of compromising cyberattacks, as well as determine the purpose of the most well-known cyberintelligence platforms and the possibility of their work.

Based on the analysis, the TI methodology was developed for the tasks of rapid detection and blocking of threats to public information resources, which will improve the efficiency of cybersecurity analysts, as well as increase the security of public information resources and systems.

References

[1] Hutchins E. M. et al.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2010.

[2] Palacín V.: Practical Threat Intelligence and Data-Driven Threat Hunting. Packt Publishing Ltd., 2021.

[3] Potiy O. et al.: Conceptual principles of implementation of organizational and technical model of cyber defense of Ukraine. Information protection 23(1), 2021.

[4] Rid T. et al.: Attributing Cyber Attacks. The Journal of Strategic Studies 38(1-2), 2015, 4–37.

[5] Shackleford D.: Who's Using Cyberthreat Intelligence and How? SANS Institute 2015.

[6] Zhylin M. et al.: Functional model of cybersecurity situation center. Information Technology and Security 6(2), 2018, 51–67 [http://doi.org/10.20535/2411-031.2018.6.2.153490].

[7] Exploring the opportunities and limitations of current Threat Intelligence Platforms. Public version 1.0, ENISA, December 2017.

[8] Standards and tools for exchange and processing of actionable information. European Union Agency for Network and Information Security, 2017.

[9] https://attack.mitre.org

[10] https://rvision.pro/blog-posts/chto-takoe-threat-intelligence-iv-chem-ego-tsennost

[11] https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/

[12] https://www.anomali.com/resources/what-is-a-tip

[13] https://www.cisco.com/c/uk_ua/products/security/security-reports.html

[14] https://www.forcepoint.com/cyber-edu/threat-intelligence

[15] https://www.fortinet.com/ru

[16] https://www.ncsc.gov.uk

[17] https://www.ncsc.gov.uk/content//files/protected_files/guidance_files//MWR_Threat_Intelligence_whitepaper-2015.pdf

[18] https://www.nist.gov

[19] https://zakon.rada.gov.ua/laws/show/2163-19#Text

[20] https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

Ph.D. Bohdan Nikolaienko
e-mail: nikolaenko_iszzi@ukr.net

Nikolaenko Bohdan Anatoliyovych, Candidate of Technical Sciences, Senior Lecturer at the Special Department No. 3 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Kyiv, Ukraine.

http://orcid.org/0000-0002-6888-5947

Ph.D. Serhii Vasylenko
e-mail: vasylenko.phd@gmail.com

Vasylenko Serhii Viktorovych, Candidate of Technical Sciences, Head of the Research Laboratory of the Research Center of the Institute of Special Communications and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Kyiv, Ukraine.

http://orcid.org/0000-0001-6779-8246

otrzymano/received: 15.11.2021 *przyjęto do druku/accepted: 15.12.2021*