STUDIA INFORMATICA
Nr 1 (28) Systems and information technology 2023

Andrzej BARCZAK[1],
ORCID: 0000-0002-3473-4585

Michał BARCZAK[2]
ORCID: 0009-0005-8628-1791

[1] Siedlce University of Natural Sciences and Humanities
Faculty of Exact and Natural Sciences
Institute of Computer Science
ul. 3 Maja 54, 08-110 Siedlce, Poland

[2] Mettler Toledo
ul. Poleczki 21d, 02-822 Warszawa, Poland

Selected issues of threat management in cyberspace

DOI: 10.34739/si.2023.28.01

Abstract. The paper describes the cyber threat management system. Three essential components of such a system are presented. With reference to such documents as ISO 2700, the NIST Cyber Security Framework, U.S. presidential executive orders, European Union regulations or STIX and TAXIS standards, norms, legal and standards regulations for managing cyber threats are described. The cyber threat management model is presented. Kill Chain and MITRE ATT&CK threat description methods are presented. A toolkit to support various stages of the cyber threat management process is also described.

Keywords. cybersecurity, threat management, cyber threat intelligence

1. Introduction

Modern societies function in a manner characteristic of the development of successive phases of the information revolution. The dimension, content, and essence of their functioning are determined primarily by the systemic informatization of social and economic processes on an individual, local and global basis, the widespread use of the Internet, including the Internet of things, the general use of artificial intelligence systems, and the rapidly increasing use of global software and hardware infrastructure resources and computer networks. All of these determine the modern space of life and the functioning of societies to acquire the character and features of cyberspace. Efficient, effective, and free of any tragic consequences, the functioning of cyberspace so understood takes on a special character in the modern world. The complexity and global nature of various types of cyber threats determines the scope, nature, and methods of defense activities. The scale of the phenomenon has created the need for transnational efforts to develop legal regulations and effective models, methods, procedures, and detailed, highly specialized techniques and software tools that will support the activities of decision-makers at various levels in the defense and threat management process in cyberspace.

The paper attempts to elaborate on a cyber threat management system. All three of its components were characterized. The scope, nature, and content of standardization recommendations on the process and procedures of cyber threat management were described. First of all, reference was made to recommendations developed by the White House and such international organizations as the European Union and the National Institute for Standardization, as well as standards for sharing cyber threat information such as Trusted Automated Exchange of Intelligence Information (TAXII) and Structured Threat Information Expression (STIX). A threat management model based mainly on the Cyber Threat Intelligence (CTI) process is presented. The various phases of the CTI process are described in detail, from defining a course of action through data collection, processing, and analysis to presenting the results and gathering feedback. Leading tools to facilitate threat management are also presented. Kiwi Syslog Server, Maltego, MISP, Azure Sentinel, and Rapid 7 Nexpose software are described, emphasizing their specificity and functionality.

2. Cyberspace threat management norms and standards

Undoubtedly, the scale of cybersecurity threats far exceeds the analytical capabilities of individual corporations or organizations. Therefore, in order to effectively counter cyber threats, cooperation between many actors is necessary. *The Executive Order on Improving the Nation's Cybersecurity*, issued by the President of the United States, Joe Biden, is an attempt

to respond to this challenge. As part of this legal act, issued on May 12, 2021, IT system providers are required to cooperate closely with U.S. government agencies in detecting and analyzing cyber threats. An essential aspect of this cooperation is to remove legal and procedural barriers to the exchange of information on cyber threats. The regulation requires the exchange of information in formats recognized by the various industries. Undoubtedly, this is associated with the need for standardization in the field of cyberspace threat management [8]. It is, therefore, necessary that suppliers use similar standards, procedures, and methodologies for exchanging threat information. As early as 2016, the National Institute of Standards and Technology published a special publication number 800-150, entitled *Guide to Cyber Threat Information Sharing*, describing the methodology for sharing information about cyber threats. It defines the types of threat information. According to this document, the following types of information are distinguished:

- **Indicators** to detect an attack related to a specific threat;
- **Tactics, Techniques, and Procedures (TTP)** to determine how a potential attack is performed. Tactics describe the attacker's behavior at a high level. Techniques refer in more detail to tactics, while procedures contain exact, often technical information related to attack vectors, e.g., software used, scripts, or specific exploit;
- **Security alerts,** also known as security recommendations, i. e. short information about existing threats, usually written in commonly understood language;
- **Recommendations** for tool configuration;
- **CTI reports** systematizing knowledge about threats. Typically, they specify both TTPs and security actors. These reports may also include information about vulnerable systems [8].

The Guide to Cyber threat Information Sharing also identifies the benefits of exchanging information on cyber threats. Undoubtedly, they can include the popularization of knowledge about the threats. Through the involvement of multiple parties, it is possible to better counter threats and build a common knowledge base on cybersecurity [16]. The document also defines the challenges of sharing this information. These include problems related to the automation of the information exchange process, building a system of universal trust between information-sharing organisations, and aspects related to the protection of sensitive information. An important issue addressed in the “Guide to Cyber threat Information Sharing” is the description of building relationships between entities exchanging information about threats. This process requires defining the objectives of information exchange, identifying internal sources of information on threats, defining the scope and rules of information exchange [29]. The

publication 800-150 also describes how to join the cyber threat information sharing community and how to operate within such a community.

Another vital document released by NIST is the 2018 NIST Cybersecurity Framework. Based on existing norms and standards, it is a set of high-level cybersecurity rules. The NIST Cybersecurity Framework defines the following cybersecurity activities:

- **Identification;**
- **Protection;**
- **Detection;**
- **Responding;**
- **Recovery.**

Identification activities are key to managing cyber threats, as they allow to better situate organizations in the cyber world around it and to specify the associated threats. As part of the identification, we can also find processes related to risk management, asset management, and business environment determination. In terms of identification of cybersecurity Framework refers to more detailed regulations such as ISO 27001 or NIST Special Publication number 800-53.

Protective measures are intended to mitigate the effects of the occurrence of the risks specified in the identification process. This is achieved through appropriate protective measures, counteracting the risks associated with particular risks. Despite all efforts, more than protective measures may be required to protect organizations against cyber threats fully [9]. **The detection activity** category refers to the situation of detection of a cybersecurity event. The NIST Cybersecurity Framework specifies that cybersecurity anomalies should be monitored and detected. Another group of actions are those related to the **response to the incident**. An action plan plays an essential role in the response to the incident. There must be procedures and action plans within the organization in the event of a cyber threat. The last categories of activities are those that relate to restoring the system to function after the occurrence of a cyberattack. **Recovery activities** must be coordinated and carried out in accordance with a pre-established recovery plan and appropriate procedures [9]. As part of the corrective processes, the NIST Cybersecurity Framework also specifies actions related to the company's image. According to the document described, public relations activities should be controlled, and the company's reputation after the event should be repaired.

The NIST Cybersecurity Framework also outlines how to apply and implement the rules it contains within an organization. It as well defines the levels of implementation of the directive [20]. It should be mentioned that the NIST Cybersecurity Framework is currently being updated.

Topics related to cyber threats and the exchange of threat information are also addressed in the *Directive of the European Parliament and of the Council (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, also known as the Network and Information Systems (NIS) Directive*. Issued in April 2017, the directive can be considered the first attempt to codify issues related to cyber threats inside the entire European Union [28]. This act obliges European Union member states to establish computer emergency response teams (CERTs) and exchange incident information between such teams [7]. Another important EU document related to cybersecurity is *Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).* According to the mentioned directive, one of ENISA's tasks is to promote the exchange of information on cyber threats [32]. The act also defines the scope and form of operational cooperation on cybersecurity within the European Union. Further *Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* has also affected the process of sharing information about cyber threats. It strictly regulates all aspects of personal data, and the activities of the threat management process must meet its requirements [31].

The ISO 2700 family of standards is also a widely respected international standard for cybersecurity. In the context of threat management, ISO 27001 and ISO 27002 (Information Security Management System) are relevant. They provide a set of principles and rules for information security and risk management [36]. The company can apply for paid certification in meeting the ISO 2700 family of standards. However, this is different from the NIST Cybersecurity Framework. Access to resources related to the NIST Cybersecurity Framework is free, while access to ISO standards comes at a cost. As a result, many organizations are starting to build a cybersecurity management program by implementing the recommendations of the NIST Cybersecurity Framework. As they reach an appropriate level of maturity on cybersecurity issues, they are applying for ISO certification. It is worth noting that many of the guidelines in the NIST Cybersecurity Framework are consistent with those in ISO 27001. An organization can use both regulations simultaneously. Of importance in the context of this article is the fact that in the latest versions of the ISO 27001 and ISO 27002 standards, issued in 2022, one of the control mechanisms described is the management of cyber threats (Threat Intelligence). This mechanism was not included in previous versions of the standards. According to the standards described above, an organization must collect information on cybersecurity threats to create a cyber threat management process. Adding this control

mechanism to the aforementioned standards highlights the growing importance of cyber threat information gathering processes.

It should also be emphasized that there are nowadays attempts to standardize protocols for exchanging data on cyber threats. The most popular standard in this regard is Structured Threat Information Expression (STIX). It is an open-sourced format, which in its latest version was based on the JSON format [30]. The basic structure of a JSON object is simple. It contains such fields as data type, identifier, specification versions, date of creation and modification of the message, its name, and description. Depending on the type of message, this object may contain additional fields like a reference to an external source. An example of a basic STIX message can be seen in Listing 1.

```
{
   "type": "campaign",
   "id": "campaign— 15972459-4799-4612-a723-231092612723 ",
   "spec_version": "2.1",
   "created": "2023-01-02T20:03:00.000Z",
   "modified": "2023-01-02T20:03:23.000Z",
   "name": "Malicious emails campain ",
   "description": "Campaign by ME Group sending malicious emals."
}
```

Listing 1. Example STIX object. Źródło: Source: own elaboration

The TAXII (Trusted Automated Exchange of Intelligence Information) protocol is also relevant in the context of cyber threat information exchange. It is used for the secure exchange of cyber threat information [30]. TAXII defines an API that allows information exchange in a client-server architecture. Data exchange between the client and the TAXII server can be done in channel or collection mode. Channel mode allows information to be subscribed to from a particular server, and the server distributes the information to all subscribing client applications. This allows information to be retrieved from multiple sources at once. The collection mode allows data to be exchanged between client and server in a request-response form [15].

The scale and complexity of cyber threat issues have necessitated standardization and codification in cyber threat management. A number of standards and regulations of both local and global scope have emerged. Decision-makers in both the European Union and the United States have issued legislation (*Executive Order on Improving the Nation's Cybersecurity and Directive (EU) 2016/1148 of the European Parliament and of the Council*) imposing threat management obligations on information system providers. According to *Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA*, one of the roles of the European Union Agency for Cybersecurity is to support the management of cyber threats and facilitate the exchange of information on such threats. A number of standards have also been created to describe cybersecurity management within organizations. NIST publication 800-150, titled *Guide to Cyber threat Information Sharing*, attempts to standardize the process of sharing information about cyber threats. The importance of this process in the secure operation of a company in the cyber world is also indicated by more general standards such as the globally recognized ISO 2700 and the NIST-issued Cybersecurity Framework. Both of these standards are similar in their recommendations. NIST Cybersecurity, based on and referring to existing standards, is a set of best practices for cybersecurity. Both ISO 2701 and NIST Cybersecurity Framework standards emphasize the leading role of an organization's management in cyber threat management processes. This is a role in both decision-making and reporting. For a company's management to make the right decisions, it must receive accurate data regarding cyber threats. There are also standards describing the format for exchanging information on cyber threats as well as protocols for exchanging information (STIX and TAXIS). None of the described standards and regulations clearly and fully define how the process of obtaining knowledge about cyber threats and exchanging such knowledge should look like. We think standardizing these processes should be the next step toward regulating and standardizing the cyber threat management process.

3. Cyber threat management model

Defining and managing cyber threats is one of the key aspects of how organizations can operate safely and effectively in today's cyber world. [19] [24]. An essential element of this process is the acquisition of threat intelligence. These activities are called Cyber Threat Intelligence (CTI) [17]. The word Intelligence may be associated with espionage activities. However, in this context, it should be understood only as a knowledge acquisition process. So what is knowledge acquisition and knowledge itself? Knowledge acquisition involves analyzing the information produced by processing available data according to defined rules.

The result of such a process is knowledge, which can be used when making decisions about the organization's budget for cybersecurity or methods of preventing threats. Unlike knowledge, data are facts that do not contribute much to solving a specific problem. Preliminary analysis of processed data allows us to obtain information and give it proper meaning. Knowledge, i.e., facts and rules of use, are obtained after further information analysis. This knowledge is created by combining many different pieces of information and giving them appropriate weights. To speak of knowledge, information must be verified and proven. Clearly, the possession or lack of knowledge can be of colossal importance in decision making at the highest levels of both corporate and government. Figure 1 shows the process of turning data into knowledge.

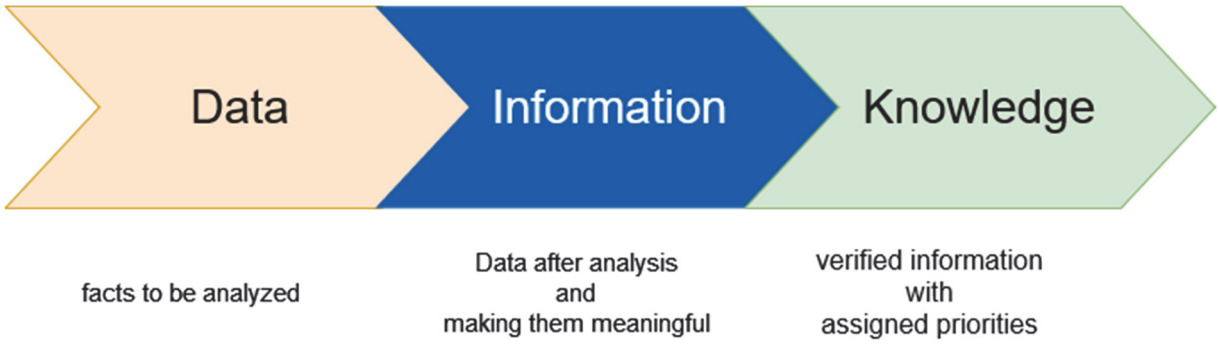

Figure 1. The process of knowledge acquisition. Source: Own elaboration

We divide the CTI process into six stages: defining a course of action, data collection, data processing in which normalization occurs, analysis, knowledge dissemination, and feedback collection [6]. CTI activities are continuous activities. Feedback gathered in one iteration serves as a basis for defining requirements for the next iteration. Figure 2 shows the life cycle of cyber threat knowledge management processes.

Figure 2. CTI lifecycle.Source: [6]

During the stage of **determining the course of action**, requirements are defined for the results of the entire CTI process. These requirements are made by the end consumers of the knowledge obtained. These are usually various levels of managers who will make cybersecurity decisions based on the results presented to them. These requirements are called Intelligence Requirements (IR) or Priority Intelligence Requirements (PIR). Good requirements definition has a not inconsiderable impact on the entire CTI process. Requirements form the basis for creating a set of questions that decision makers want to know the answers to [35]. Let us think what knowledge about what events and processes the organization wants to acquire during the CTI processes. During the tasks of describing threats and expanding knowledge about them, it is important to answer several essential questions.

We think that a key and significant one is to know the source of the threat. In this context, it is relevant to distinguish the type of cybercriminals. We can specify a number of types of cybercriminals, ranging from inexperienced amateur crackers whose actions can be classified rather as hooligan acts, or so-called scripts kiddies, through crackers organized into groups lined with an ideology called hacktivists, and organized criminal groups to perfectly organized and very often highly skilled and financially well-funded hacking groups sponsored by various governments called Advanced Persistent Threats (APT). It is usually easier to defend against threats from script kiddies than sophisticated attacks or attack campaigns perpetrated

by APT groups. The range of activities commonly used by APT groups is much wider than those used by script kiddies. It includes, among other things, elements related to a thorough analysis of infrastructure and target personnel, increasing the scope of the attack, or covering their traces [29] [11].

No less important issue is defining the tactics, techniques, and procedures (TTPs) used by attackers to breach security and launch an attack. Also important is how to detect the threat and defend against it. In terms of describing tactics, techniques, and procedures, the Kill Chain and MITRE ATT&CK models can be helpful. The Kill Chanin model is a military model developed by the Lockheed Martin Corporation, adapted to cybersecurity issues.

The cyber threats modeled with it will allow us to determine how to break through security. Using Kill Chain, we try to impersonate the attacker and analyze the steps performed during the attack [14]. Seven phases of attack are defined in the Kill Chain model. These are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and accomplishing mission objectives. [29].

Another useful model is the MITRE ATT&CK. It is a comprehensive collection of tactics, techniques, and procedures used by attackers. It was created by a non-profit organization called MITRE [17]. The MITRE ATT&CK model defines fourteen tactics. Techniques that can be divided into more detailed sub-techniques are associated with each tactic. Associated with the techniques are ways to detect the threat and ways to mitigate it. Within the MITRE ATT&CK database, we can also find information on attacker groups [33] [23]. Tactics in the described model are defined as the goals of the attacker's actions. They can be identified with the phases of attack known from the Kill Chain model. The so-called pain pyramid is associated with the MITRE ATT&CK model (Figure 3).

This is a graphical representation of an attacker's effort to change the attack's distinguishing features. The IT security team should therefore focus on detecting activity in the highest possible layers of the pyramid. Some attack parameters like IP addresses and hashes are relatively easy to change or spoof. Securing these layers is simple enough, but it is not an effective defense against more complex attacks.

As we can observe, it is the hardest for attackers to change tactics, techniques, and procedures. This shows the importance of threat intelligence gathering processes. Good TTP analysis is undoubtedly a very complex, time-consuming process that requires a high level of competence from the cybersecurity team. It also often involves large financial outlays. However, the level of security that can be achieved using such analysis is very high [44].

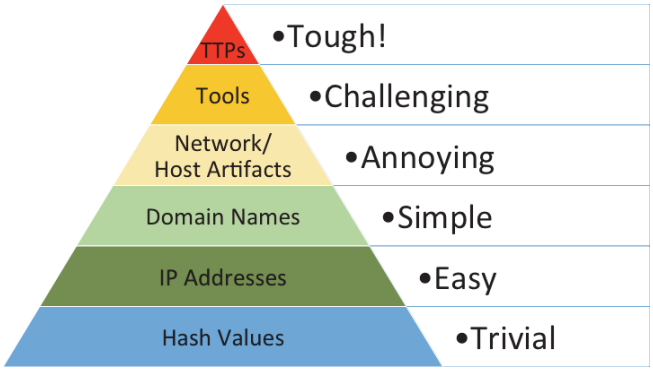

Figure 3. MITRE paine pyramid. Source: [42]

The next important issue that should be defined at the stage of defining the course of action is determining the data source for the CTI process. Undoubtedly, an initial in-depth analysis of the type of data and how it is described is useful in selecting a data source. Due to the overwhelming amount of data in the cyber world, identifying good data sources is not easy.

A good data source should be objective and have a high level of credibility and reliability. When selecting a data source, it is important to remember that it has a not insignificant impact on the entire CTI process. Poor selection of data sources can result in information noise or perception of false data, resulting in flawed analysis of such data and false information and knowledge presented. Based on false information, it will not be possible to make effective decisions what can bring measurable damage to the organization.

We can divide data sources for the CTI process into internal and external. Internal sources are the resources of the organization while external are services provided by vendors. Data sources can be both technical and human resources. Technical sources help to collect data on security breach attempts and detected system intrusions or malicious events in the systems [39]. Once the requirements for the threat intelligence process are defined, the actual collection of data occurs. It is crucial that a common repository is defined to allow all stakeholders in the CTI process to access the data easily.

The following step in cyber threat knowledge management is **data processing** [6]. It has a key impact on the entire CTI process. Once the data is processed, it must be understood by analysts. In this phase, data is converted into information.

The information obtained in the data processing phase is subjected to **analysis**. Undoubtedly, this is a time-consuming and complex process, requiring analysts to be both immensely knowledgeable in the field of cybersecurity and meticulous and accurate in analyzing all acquired information. Very often, this process is supported by automated tools. The result of the analysis processes are **reports** that meet the requirements set in the phase of

defining the course of action and thus provide answers to the questions asked at the initial stage. The reports present knowledge about cyber threats. The final reports can have different levels of detail depending on the type of CTI. We distinguish between strategic, operational, tactical, and technical CTI. **Strategic reports** present high-level knowledge of cyber threats and are intended for decision-makers in the organization who usually do not have technical knowledge [42]. As the name implies, a strategic report should enable senior management to make strategic decisions critical to the operation of the entire organization.

Operational report is designed for managers of defensive security teams and contain information about specific threats present in the cyber world and possible assets at risk [42]. It should not be characterized by excessive detail, and the language used in it must be understandable to the audience.

Definitely more precise and detailed is the **tactical report**. It is written in technical language and should include knowledge of techniques, tactics, and procedures used by adversaries. The purpose of a tactical report is to outline how an organization can be attacked, how a potential attack can be detected, and what measures should be taken to defend against particular threats. Recipients of such a report are technical managers of operational and offensive security teams and teams responsible for maintaining the organization's network infrastructure.

The **technical report** is designed for technical network and security teams. It contains very detailed, low-level technical knowledge of the technical resources held by attackers. Technical reports lose their relevance quickly due to the high dynamics of changes in the types and forms of attacks and the adaptation of attackers to the defensive measures used. The diversity of audiences and the varying scope of knowledge contained in each report show how critical the processes involved in gaining knowledge about cyber threats are for organizations [35].

The final phase of the CTI process is **collecting feedback and evaluating a given iteration of the process [**6]. During this phase, it is verified whether the previously stated requirements have been met. The feedback has a crucial impact on determining the requirements for the next iteration. Thus, it can be said that cyber threat knowledge acquisition processes are a continuous improvement of the organization in defining, detecting, and defending against cyber threats.

Managing threats in accordance with the CTI process undoubtedly brings tangible benefits to an organization. Well-conducted cyber threat knowledge acquisition activities allow an organization to prepare for various cyberattacks [2]. The costs of activities aimed at

increasing knowledge about threats are often high. This is primarily due to the need for an expert team to analyze threat data. Of course, there are also tools to facilitate data collection and analysis, but still, many activities are performed by analysts from security teams in a traditional way.

4. Tools to support the cyber threat management process

There are a number of tools that support the process of threat knowledge management at various stages, from data collection to data processing analysis and reporting to the vulnerability scanning. We will try to briefly characterize the different types of tools with examples such as SolarWinds Kiwi, Maltego, MISP Threat Sharing, Microsoft Sentinel, and Rapid 7 Nexpose. The first of the tools described is the **Kiwi Syslog Server** software developed by SolarWinds. It is a popular syslog protocol server allowing administrators to collect logs from multiple devices [37]. The free version of Kiwi Syslog Server allows the collection of logs from five sources, while the paid version has no such limitation. An unquestionable advantage of Kiwi Syslog Server software is the ability to set rules to facilitate the analysis of a large number of logs.

These rules make it possible to define, depending on the content of the Syslog messages, different types of actions, such as sending a mail with a notification, running a script, or triggering a sound signal [34]. Received messages are analyzed to ensure that all rules are met one by one. If a message is received, the server checks whether it meets the filters defined in the first rule. If all conditions are met, the actions described in the rule are executed. When any of the filter conditions are not met, the server analyzes whether the message meets the conditions defined in the following rules [10].

Another helpful tool during the threat management process is **Maltego**. This is software used during open-source intelligence (OSINT). It allows, based on generally available information on the web, to build profiles of both individuals and organizations [4]. Knowing basic data about the aggressors like for example a domain address, we can get such useful information as email addresses associated with that domain, IP address pools, or server addresses. Maltego allows us to build graphs of companies' connections to their resources, both human and technical. The knowledge gained in this way enables better system security and is an excellent data source for technical reports of CTI processes. The tool's graphical interface is self-explanatory and allows the collected data to be presented in the form of a linkage graph. Figure 4 shows an example of a generated linkage graph based on an email address.

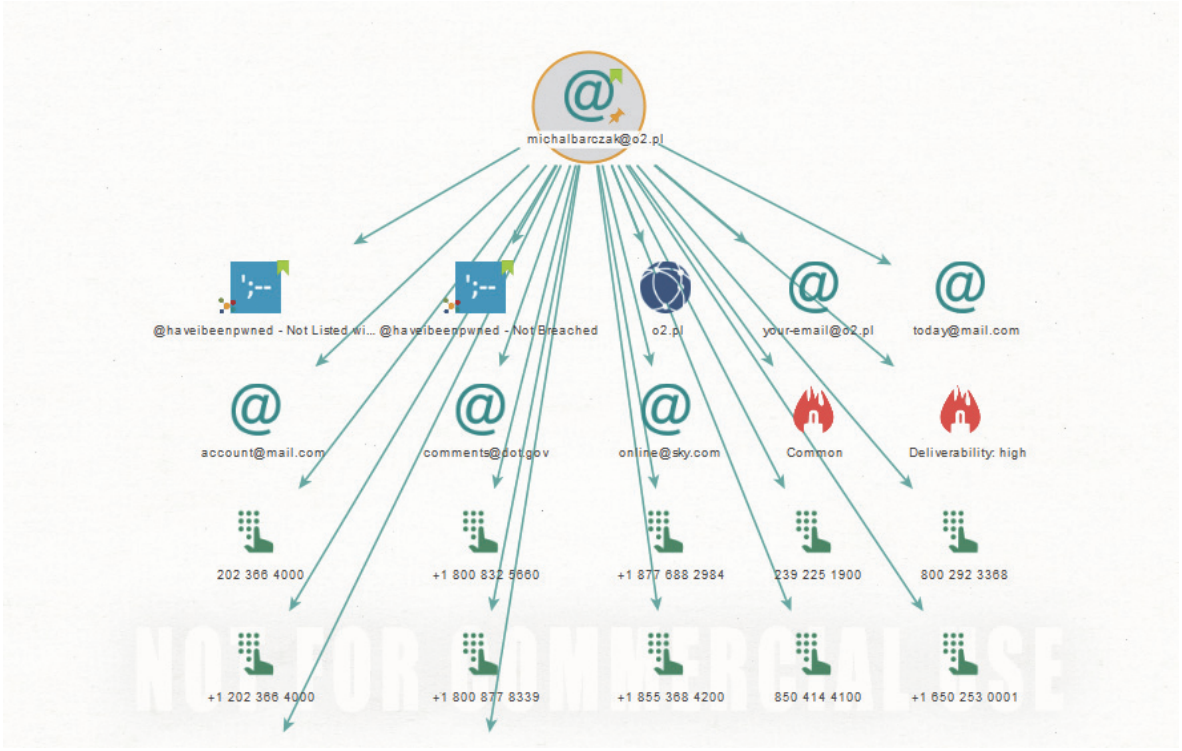

Figure 4. Generated graph based on email address. Source: own elaboration

As we can see from the figure, only by analyzing email address we can tell what domain the address belongs to. After further analysis of the domain, we are able to obtain more detailed information, like the pool of IP addresses associated with the domain. All the information presented is gained by exploring publicly available data on the Internet, and thus the use of Maltego software is fully legal. The Maltego tool uses multiple transformations to retrieve information. Some of the transformations, like domain analysis, can be built into the tool itself, and some are related to external tools. The free version of the tool has a limit of results per transformation [5]. Maltego tool can be used as well to analyze the information available about an organization. It allows the security team to verify what data about the company is publicly available and what information potential attackers have access to. Such analysis helps to focus on securing resources about which information is easily obtained [40].

Another valuable tool in the threat management process is **MISP**. It is a free tool for sharing information about threats both within the organization and with partners. The MISP application is an extensive service that includes a database. The MISP application is accessed through a convenient-to-use and user-friendly graphical interface provided in the form of a web page. The software can be a database of attack information or a tool for sharing knowledge about threats in a uniform and formalized way [21]. The MISP application, through integration with various types of security systems such as IPS systems, SIEM, or host scanners, allows a precise description of disturbing network events and the correlation of the collected information with

the MITRE ATT&CK model. The main advantage of MISP software is the functionality of synchronizing and sharing threat data with other organizations. There are two ways to synchronize data. It is possible to retrieve information from connected servers of so-called MISP instances or from publicly available MISP communities run by external organizations [22]. Once the data is synchronized, the threat information can be seen in the Events tab of the administration panel (Figure 5)

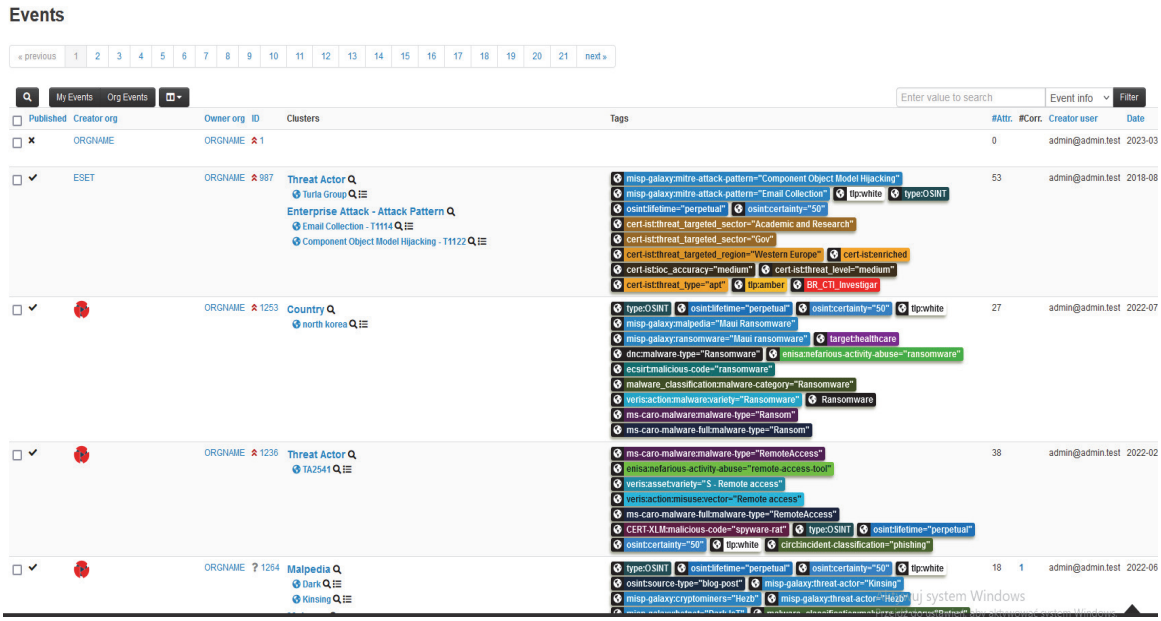

Figure 5. Threat information on the Events list. Source: own elaboration

Noteworthy, the information presented in the MISP tool can cover many aspects of cyber threats. Among other things, the system presents data on attacks, groups of attackers, techniques, tactics, or tools used in the attack. Most of the records have assigned tags, allowing faster search and filtering of the list. It is important that the records are linked to each other so that when analyzing a specific threat, the security team is able to quickly extract all available knowledge about the threat [21].

Users can view many details of a record. A useful feature is the presentation in the form of a graph of correlations between records. Users have as well the possibility to edit records. While editing the record, we can change parameters like the phase of the threat analysis or the threat level. Saving the changes, we can determine the scope of publication of the changes. MISP software provides the functionality of publishing changes only within a specific organization, within the community that published the record, within the publishing community and the combined communities, and globally.

The security team also has the ability to add new records to the MISP database. Undoubtedly, this functionality allows for building a personalized source of threat intelligence

available within the organization. MISP enables easy filtering event lists to present only data from within organization.

The MISP system is very useful tool in the threat management process. The data it contains can be the source of information for all reports in the CTI process. Information on threats specific to the industry the organization deals with is a critical element of the strategic report. Based on high-level cyber threat information, an operational report is constructed. More precise data in terms of tactics, techniques, processes, and resources used by cybercriminals form the basis for both technical and tactical reports.

In the era of cloud systems, security and threat management issues for cloud infrastructure have become very prominent. The complexity of cloud security aspects can arise from many aspects. One primary concern is the distribution of the system across multiple locations. Access to system logs by administrators can also be difficult [1]. Thus, the need for security systems aimed specifically at the cloud has arisen.

One such tool is **Microsoft Azure Sentinel**. It is a cloud-dedicated Azure module that performs two complementary functions. It provides the functionality of a threat and security information management system (SIEM-class system) and the centralization and automation of security tools to eliminate threats [43]. A significant advantage of the Azure Sentinel environment is the built-in algorithm, based on artificial intelligence, responsible for finding potentially dangerous activities in the system. With a large number of built-in connectors, Azure Sentinel allows for the connection of multiple data sources.

In addition to connectors to Microsoft software such as Windows Firewall, Microsoft Defender, and Microsoft Pureview, Azure Sentinel has connectors to systems from other vendors, for example, Cisco, Croudstrike, and Kaspersky. Also in favor of the Azure Sentinel environment is the integration functionality with other cloud platform providers, including Amazon Web Services and Google Cloud.

Not without significance is the ability to connect an organization's own on-premise infrastructure to Azure Sentinel as well. Due to a large number of potential data sources, we dare say that Azure Sentinel has an overview of the entire environment and makes it possible to detect threats and attacks and respond to them effectively. Figure 6 shows the architecture of an example of an organization's IT system monitored using Azure Sentinel.

The Azure Sentinel solution is based on detection rules that allow the administrator to be notified of a potential threat [43]. The user has the opportunity to use predefined rules or create their own. A beneficial functionality when defining security rules is the ability to verify rule coverage of threats described in the MITRE ATT&CK model [38].

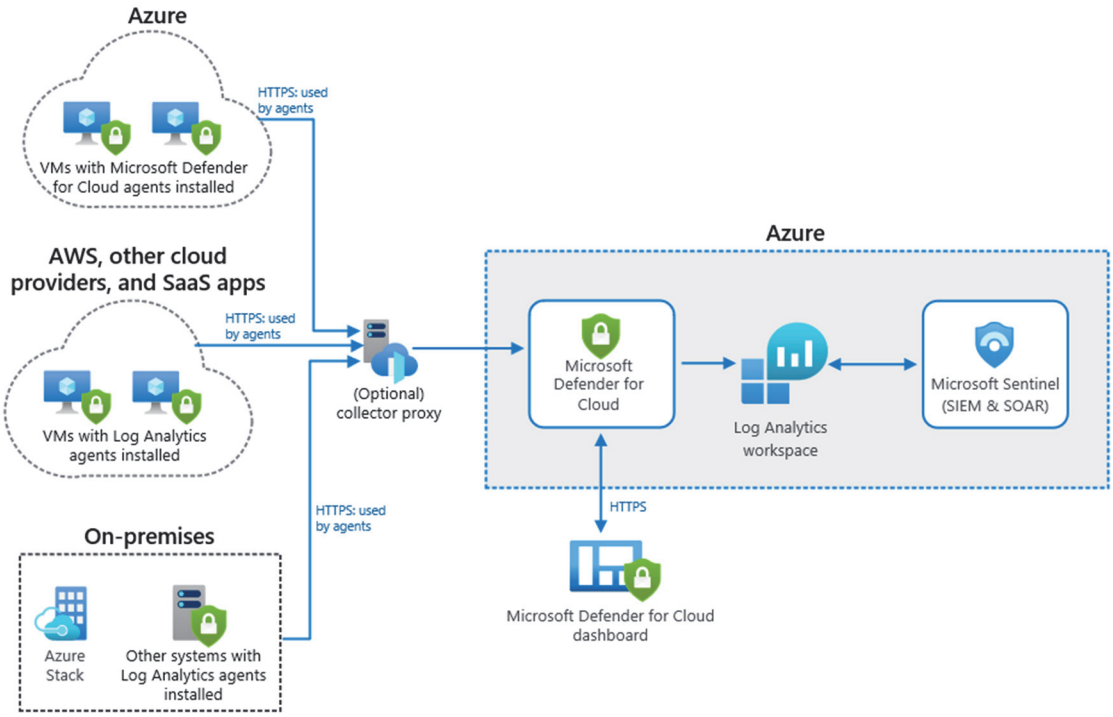

Figure 6. Architecture of a monitoring system using Azure Sentinel. Source: [12]

Using the integration of the Azure Sentinel tool with the Azure Logic App, the administrator is able to perform automatic actions in response to a security event. Azure Logic App has connectors to many environments, including Azure Active Directory, ServiceNow, and Jira. Azure Sentinel also has the functionality to present the scope and source of the threat in the form of a graph, making it much easier to analyze the incident. An example of such a graph can be seen in Figure 7.

Figure 7. Azure Sentinel threat graph. Source: [13]

Azure Sentinel, through a suitable data connector, also allows integration with STIX/TAXII threat knowledge data sources.

The last tool covered is **Rapid 7 Nexpose**. It is a vulnerability scanner that allows penetration testing within an organization. Without contradiction, analyzing the present vulnerabilities expands the knowledge of cyber threats [26]. It enables verification of an organization's security features and is a primary source of data for designing new security systems [3] [18]. Regular testing of the security of systems can be as well driven by general or federal regulatory requirements.

Rapid 7 Nexpose is one of the most popular vulnerability scanners due to its substantial capabilities. It allows detailed scanning of large networks. We can distinguish three types of vulnerability tests white box, black box, and gray box. During white box testing, the tester has complete knowledge of the network structure and software used by organizations. In black-box testing, the tester must breach the organization's security to analyze the network structure and detect the software. Grey box testing assumes the analyst has partial knowledge of the organization's infrastructure.

Rapid Nexpose is perfect for white box tests. It allows generating a test report, presenting both the detected vulnerabilities and proposed solutions to eliminate them [25]. Vulnerability scanning with Rapid Nexpose is based on the concept of a site. A site is a group of devices that are scanned together [41]. The division into sites is often done based on subnets or types of devices. When defining a site, the user can specify groups of devices. A single IP address, an IP address range, or the device's network name can describe these devices. An important task during scanning processes is to correctly define the authentication of the scanner. It is imperative that the scanning tool has access to all necessary resources. When creating a new site, we are also able to optionally indicate the account that will be used for scanning [27]. The use of a service account requires setting high-level permissions for that account. This can prove to be difficult or even a security vulnerability.

Another method of configuring access to resources is through firewall-level settings and system settings on resources. Configuring remotely scanned resources and rules on the firewall itself is a challenging task and requires careful analysis by the security team [26]. The Rapid 7 Nexpose vulnerability scanner allows scanning using a local scanning engine or a remote one. The computer on which the Rapid 7 Nexpose Security console is installed has the local scanning engine automatically installed. On the rest of the devices, the analyst needs to install and configure client software that allows remote scanning.

After defining the site and assigning it the appropriate scanning engine, it is possible to scan the devices grouped in the site. When running a scan, the administrator has several built-in scan templates at his disposal. A list of all available scanning templates, along with their descriptions, is available on the manufacturer's website. Once the scanning is started, the detection of the end devices to be scanned and the scan itself takes place. The advantage of the Rapid 7 Nexpose tool is that it can scan extensive computer networks [25] [26]. The result of the scan is a report presenting its results. An example report is presented in Figure 8.

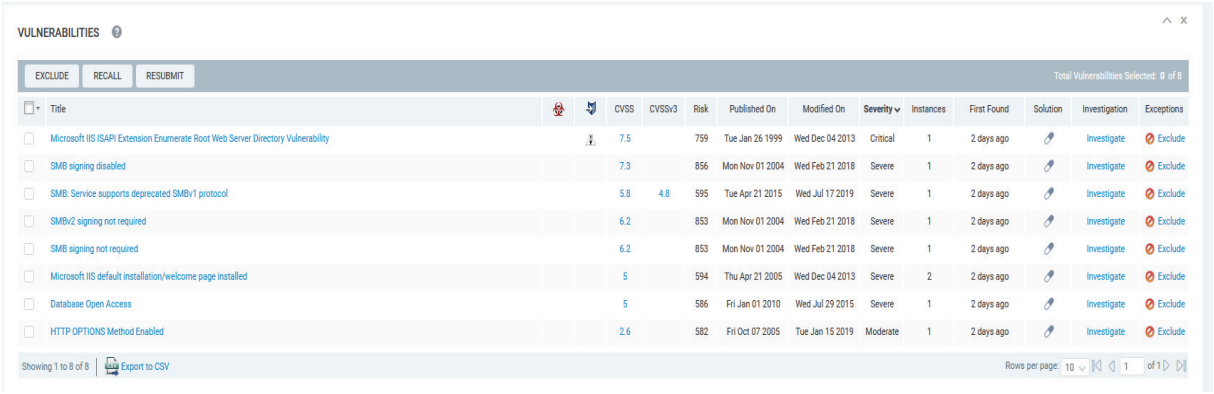

Figure 8. Scanning report. Source: own elaboration

The report, in addition to the vulnerabilities found, presents methods for removing them. Administrators have the option to export the final report to pdf format. Vulnerability scanning, like the entire threat management process, is a continuous and iterative process. As a result of the scanning iteration, actions should be taken to eliminate vulnerabilities. In the next step, through re-scanning, it should be ensured that vulnerabilities have been removed. Scanning reports can be an excellent source of knowledge about cyber threats and, in particular, the level of protection against threats in an organization.

We think we have succeeded in presenting a collection of valuable tools in various phases of the threat management process. From Kiwi Syslog Server serving as a repository for system logs, the Maltego open-source intelligence tool, MISP threat intelligence sharing software, and Azure Sentinel integrated security system to Rapid 7 Nexpose vulnerability scanner, the software described undoubtedly supports threat management.

5. Conclusion

The paper presents a cyber threat management system. All three of its components were characterized. The scope, nature, and content of standardization recommendations for the process and procedures of cyber threat management are described. A model for the threat

management process was proposed. Existing applications and information systems supporting decision-makers at various levels in all phases of the cyber threat management process were characterized.

A detailed analysis of existing and proposed solutions in each of the three components of the threat management system allows us to make recommendations for further research, legislation, design, and programming work. We believe that work should be undertaken that defines the sources of information about threats and the detailed way of exchanging this information between decision-makers very precisely. The solutions that currently exist in this area do not always accurately describe these issues. We think that a single standard for the exchange of information on cyber threats, for example, the STIX standard, should be applied and used.

Analysis of the scope and content of all phases of the cyber threat management process allows us to conclude that the presented management model is complete. The tools currently used to support decision-makers in the process of cyber threat management are very often autonomous and domain-specific. We believe there is a need to undertake design work on an integrated information system with significantly expanded functionality, generating final reports for decision-makers at all levels and phases of the threat management process.

References

1. Barczak A., Barczak M., Bazy danych w chmurze obliczeniowej, pages 25-27, Wydawnictwo Naukowe UPH, Siedlce, 2022.

2. Borges D., Adversial Tradecraft in Cybersecurity: pages 211-224, Packt Publishing, Birmingham, 2021.

3. Bravo C., Mastering Defensive Security, Packt Publishing, Birmingham, pp. 353-369, 2022.

4. Brotherson L., Berlin A., Defensive Security Handbook, O'Reilly Media, Sebastopol California, pages 185-221, 2017.

5. Customize your Maltego solution according to your investigative needs, https://www .maltego.com/pricing-plans [accessed: 01.03.2023].

6. Cyber threat Intelligence: How to Stay Ahead of Threats, https://www.agari.com /blog/what-is-cyber-threat-intelligence [accessed: 12.02.2023].

7. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=BG [accessed: 10.03.2023].

8. Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse .gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the -nations-cybersecurity/ [accessed: 10.03.2023].

9. Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs .nist.gov /nistpubs/CSWP/NIST.CSWP.04162018.pdf [accessed: 10.03.2023].

10. How Kiwi Syslog Server rules work, https://documentation.solarwinds.com/en/ success _center /kss/content/kss_gsg_about_rules.htm [accessed: 20.03.2023].

11. How an APT is carried out, https://accedian.com/blog/what-are-advanced-persistent-threats/ [accessed: 12.02.2023].

12. https://learn.microsoft.com/en-us/azure/architecture/hybrid/images/hybrid-security-monitoring.png [accessed: 20.03.2023].

13. https://learn.microsoft.com/en-us/azure/sentinel/media/investigate-cases/map-timeline .png [accessed: 20.03.2023].

14. Hutchins E. M., Cloppert M. J., Amin R. M., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2011.

15. Introduction to TAXII, https://oasis-open.github.io/cti-documentation/taxii/intro.html [accessed: 12.03.2023].

16. Johnson C., Badger M., Waltermire D., Snyder J., Skorupka C., Guide to Cyber threat Information Sharing, https://csrc.nist.gov/publications/detail/sp/800-150/final, 2016 [accessed: 20.03.2023].

17. Kaiser F., Muff J. Schultmann F., Wiens M., Attack Forecast and Prediction C&ESAR 21 - Computers & Electronics Security Applications Rendez-vous, 2021

18. Kim P., The hacker playbook, pages 23-50, Createspace Independent Publishing Platform, South California 2014

19. Kohnfelder L., Designing Secure Software, No Starch Press Inc., San Francisco, pages 49-70, 2022.

20. McCarhy B., Cyberjutsu, No Starch Press, San Francisco, pp.15-31, 2021.

21. MISP https://github.com/MISP/MISP [accessed: 20.03.2023].

22. MISP Sharing https://www.circl.lu/doc/misp/sharing/ [accessed: 20.03.2023].

23. MITRE Att&Ck https://attack.mitre.org/ [accessed: 12.02.2023].

24. Muliński T., ICT security in revenue administration – incidents, security incidents – detection, response, resolve, Studia Informatica Systems and Information Technology No 2, Vol. 27, pp. 75-94, 2022.

25. Muliński T., ICT security in tax administation –Rapid7 Nexpose vulnerabiliy analysis, Studia Informatica. Systems and Information Technology. No 1-2, Vol. 25, pp. 101-121, 2021.

26. Muliński T., Rapid Nexpose Vulnerability DetectionSolution, Inteligent Systems and information Technologies. [in:] Theory and Application of Artificial Inteligence Methods, [ed.: J. Tchórzewski, P. Świtalski], Wydawnictwo Naukowe UPH, Siedlce, pages 147-171, 2022.

27. Nexpose Quick Start Guide, https://docs.rapid7.com/nexpose/ [accessed: 01.04.2023].

28. Nweke L.O, Wolthusen S., Legal Issues Related to Cyber threat Information Sharing Among Private Entities for Critical Infrastructure Protection, 12th International Conference on Cyber Conflict, 2020.

29. Olejnik Ł. Kirasiński A., Filozofia cyberbezpieczeństwa, Wydawnictwo Naukowe PWN SA, Warszawa, pages 32-42 2022.

30. Ramsdale A., Shiaeles S., Kolokotronis N., A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages, Electronics, 2020.

31. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1679292943633 [accessed: 10.03.2023].

32. REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/eli/reg/2019/881/oj [accessed: 10.03.2023].

33. Rehberger J., Cybersecurity Attacks – Red Team Strategies, pages 137-142, Packt Publishing, Birmingham, 2021.

34. Rule Actions https://documentation.solarwinds.com/en/success_center/kss/content/kss_adminguide_add_action.htm [accessed: 20.03.2023].

35. Sakellariou G., Fouliras P., Mavridis I., Sarigiannidis P., A Reference Model for Cyber threat Intelligence (CTI) Systems, Electronics, 2022.

36. Tamimi M., SECURITY REVIEW BASED ON ISO 27000/ ISO 27001/ ISO 27002 STANDARDS:A CASE STUDY RESEARCH, International Journal of Management and Applied Science, 2019.

37. Tanner N.H, Cybersecurity Blue Team Toolkit, pages 139-150, John Wiley & Sos Inc., Indianapolis, 2021.

38. Understand security coverage by the MITRE ATT&CK® Framework, https://learn.microsoft.com /en-us/azure/sentinel/mitre-coverage [accessed: 22.03.2023].

39. Venkatesh V., Design of Cybersecurity Risk Assessment Tool for Small and Medium Sized Businesses using the NIST Cybersecurity Framework, KSU Proceedings on Cybersecurity Education, Research and Practice, 2018.

40. Weidman G., Penetration Testing, No Starch Press, San Francico, pp. 159-166, 2014.

41. What is a site?, https://docs.rapid7.com/nexpose/what-is-a-site [accessed: 01.04.2023].

42. What is Cyber threat Intelligence, https://www.cisecurity.org/insights/blog/what-is-cyber-threat-intelligence [accessed: 12.02.2023].

43. What is Microsoft Sentinel?, https://learn.microsoft.com/en-us/azure/sentinel/overview [accessed: 22.03.2023].

44. What is the Pyramid of Pain? https://www.attackiq.com/glossary/pyramid-of-pain/ [accessed: 12.02.2023].