Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 3, pp. 1872–1881, DOI 10.12694/scpe.v25i3.2779

RESEARCH AND DESIGN OF AN AUTOMATED SECURITY EVENT ANALYSIS AND HANDLING FRAMEWORK BASED ON THREAT INTELLIGENCE

LINJIANG XIE, ZHOUYUAN LIAO*, AND HANRUO LI

Abstract. In order to deeply explore and utilize the value of threat intelligence, strengthen research on attack organizations, and grasp the correlation between attack organizations, the author proposes the research and design of an automated security event analysis and handling framework based on threat intelligence. The author extracts the behavioral characteristics of the attack organization based on known APT attacks, and uses the machine learning framework Light GBM to establish a multi classification model to complete the analysis of unknown APT attack organizations. Through the study of multi-dimensional analysis of multi-source threat intelligence, attack organization correlation and judgment, an attack organization correlation and judgment system has been designed and implemented. The system includes six modules: threat intelligence collection module, threat intelligence multi-dimensional analysis module, attack organization fingerprint library module, attack organization correlation module, attack organization analysis module, and user module, providing attack organization correlation and judgment services for network security. The test results show that the intelligence reading and search query function can achieve the reading of various information of attack organizations, and achieve visual display of threat intelligence. The intelligence management function can achieve operations such as adding, deleting, and updating intelligence. The user management function of the system can achieve the management of administrator users and ordinary users. After testing, all functions of the system have been implemented and meet expectations.

Key words: Threat intelligence; Security incidents; Judgment and disposal; Design; APT attack

1. Introduction. With the rise of big data and the development of "Internet plus", the collection scope of threat intelligence has been greatly expanded. Threat intelligence describes existing or imminent threats or dangers to assets, and can notify the subject to make some response to the relevant threats or dangers [1]. The modern information technology represented by the Internet, especially mobile payments, cloud computing, social networks, and search engines, has had a fundamental impact on human financial models, accompanied by increasing external risks. How to strengthen the information security management of banks and form a scientific and effective information security management system to prevent financial information risks has become a major issue currently facing the financial industry. Organization and scale are increasingly becoming the most prominent characteristics of network attacks, and each attack is carried out with premeditation. Planned and often with political objectives, more and more national dreams and the construction of attack organizations and the implementation of attack behaviors have increased the difficulty of network defense due to the background of national cyber attacks.

At present, the implementation of relevant security technologies does not receive legal protection, such as extracting P message information. Monitoring device status and other issues are all related to personal privacy, and these issues cannot be solved solely through technological means. They rely more on the updating and improvement of network security laws and regulations. In order to better maintain cyberspace security and respond to APT attacks, threat intelligence has emerged. Threat intelligence is seen as a "visible" tool for quickly and effectively resisting attacks and maintaining cyberspace security Ability. From a personal perspective, threat intelligence can serve as an important defense indicator, and attackers also need threat intelligence to update technical means and achieve the goal of hiding their true identity through attack information forgery and intelligence. From the perspective of enterprises, different security companies can exchange different threat intelligence, such as vulnerability information[2]. P reputation information, license list. White list, etc., to achieve an integrated network of internal and external resources, thereby achieving collaborative street prevention, and forming products such as vulnerability detection, threat detection, etc. to generate

*Information Security Operation and Maintenance Center of Information Center of Yunnan Power Grid Co., LTD, Kunming, Yunnan, China, 650011 (Corresponding author, bgzzzy@126.com)

commercial profits.

For a country, threat intelligence is crucial for maintaining national security and safeguarding national interests. Safeguarding the legitimate rights and interests of citizens is of great significance, and even includes attackers. Attacking organizational information plays a strategic role in diplomacy and national defense. At present, research on threat intelligence mainly focuses on the productization of security vendors, with a general direction of providing traditional security products such as PS (Intrusion Prevention System) and information exchange modes. However, the value of threat intelligence is not as simple as productization, as it contains a large amount of attack organization information such as attack methods and tools. Attack behavior patterns, attack intentions, etc. can be correlated and judged through in-depth analysis of threat intelligence and value mining. Network attack and defense is essentially a major game and competition between attackers and defenders using the network as the battlefield. The analysis, research, and tracing of attack organizations can help develop targeted defense strategies to achieve effective defense and precise strikes. Therefore, the importance of threat intelligence analysis and research for attacking organizations in network defense cannot be ignored. Attackers use various techniques such as forging IP addresses, springboards, and anonymous networks to hide their identities and evade tracing, which undoubtedly poses a huge challenge to the tracing of attack organizations. However, it is precisely due to the existence of various tracing and forensics technologies such as host IP tracing, malicious code analysis, and packet logging that tracing tracing becomes possible, it is precisely the analysis results of these technologies that provide content support and technical possibilities for the association and analysis of attack organizations. At present, research on attack organizations around the world still presents fragmented characteristics, and there is no real system that can complete the analysis functions of various attack organizations. Therefore, the author's research on the correlation and judgment of attack organizations based on multidimensional analysis of threat intelligence and its method implementation have important research and application value [3,4].

2. Methods. The attack tactics and objectives of different APT organizations are different. The attack time, attack tactics, attack objectives, IOC, etc. of the attack organization are saved as threat intelligence, which includes the characteristic information of the attack organization. By extracting these features, an attack organization fingerprint library can be formed. By using the attack organization features, an association of existing attack organizations can be established. At the same time, When the network is attacked again, the attack organization can be determined by comparing the attack traces with the attack organization fingerprint database [5]. As shown in Figure 2.1. Based on the above research ideas, the following steps are required:

Acquisition of multi-source threat intelligence: Selecting multiple sources to obtain a large amount of threat intelligence and establishing a threat request intelligence base is the foundation and prerequisite of this study.

Multidimensional analysis of threat intelligence: Based on basic theories and analysis models, conduct multidimensional analysis of threat intelligence, extract feature indicators from each dimension, and establish a threat intelligence feature library;

Establishment of attacker organization fingerprint database: Analyze and process the collected threat intelligence to establish an attack organization fingerprint database [6];

Attack organization homology determination: Attack organization homology refers to the similarity between two attack organizations. By using this similarity analysis to determine whether two attacking organizations are unified or have associations, it can be achieved through similarity analysis between different organizations;

Consistency determination of attacking organizations: Research and judgment of attacking organizations. Comparing recently captured attack events with known attack organizations to determine the category of their attack organizations can be achieved through machine learning.

2.1. Acquisition of multi-source threat intelligence. At present, there are roughly four sources of threat intelligence for security teams: Public sources, commercial sources, open source intelligence sources, and internal data. The credibility of threat intelligence sources is often measured by the authority of the intelligence source. As shown in Equation 2.1, Au represents the credibility of different sources, where S is the intelligence

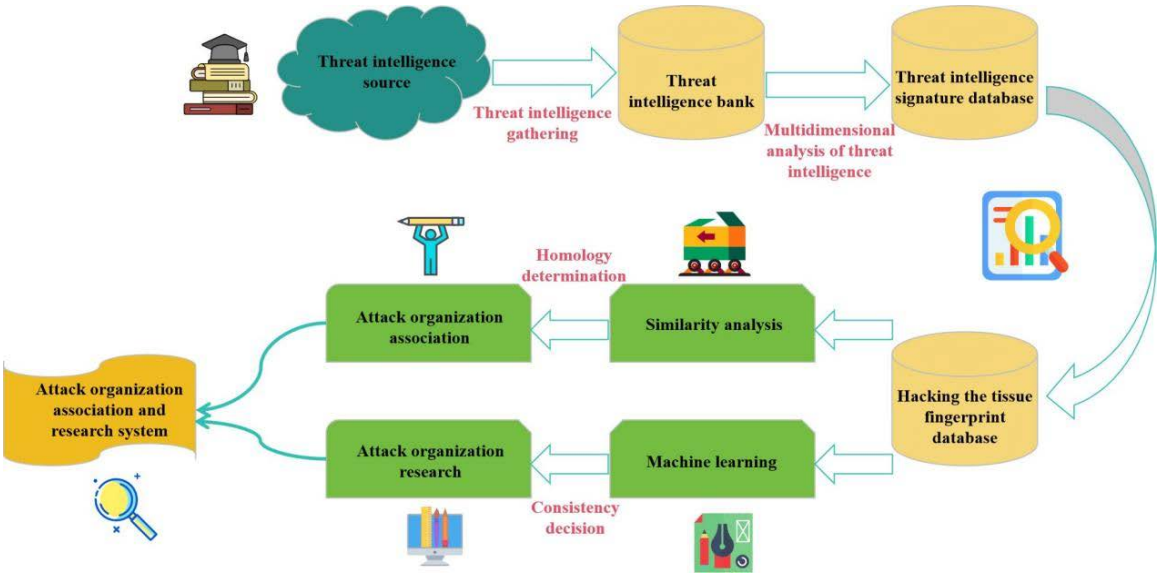

Fig. 2.1: Research ideas on attack organization association and judgment based on multi-dimensional analysis of threat intelligence

source and r is the Alexa ranking of the source site [7,8].

$$Au = \begin{cases} 0, & S\epsilon unknown \\ 0.2, & S\epsilon \text{Independent source station, blog} \\ 0.4, & S\epsilon site \quad \& \quad r < 10^6 \\ 0.6, & S\epsilon site \quad \& \quad r\epsilon[10^4, 10^6] \\ 0.8, & S\epsilon site \quad \& \quad r > 10^4 \\ 1, & S\epsilon \text{A well-known organization or institution} \end{cases} \tag{2.1}$$

The author's research is based on credible threat intelligence, and the credibility of threat intelligence from different sources also varies. Therefore, in order to ensure the credibility of threat intelligence, the author's sources of threat intelligence include public threat intelligence sources, open-source threat intelligence sources, and internal data, mainly including threat intelligence based on APT reports, shared intelligence on threat intelligence platforms, and accumulated data in practice (internal data) [9]. Research reports publicly released by national security departments, renowned security vendors or organizations, etc., on APT analysis intelligence. They rely on their own devices and platforms to mine various elements in APT attack events, then trace their sources, complete attack scenario reconstruction, and form analysis reports, which include specific analysis processes and results, as well as complete intelligence information such as attack tools, targets, and events. APT reports, as intelligence with rich knowledge content, have extremely high utilization value and are the highest level of threat intelligence. However, due to the wide distribution and large quantity of APT reports, it is difficult to collect them. At the same time, even with APT reports, accurately extracting threat intelligence from them also requires a lot of time. Therefore, this part of the workload is huge and difficult, which requires a lot of time and effort.

The publicly recognized machine readable intelligence provided by various threat intelligence sharing platforms is a clue to a network threat that has been analyzed and discovered at a certain time, and many platforms provide API interfaces, some of which require payment. At the same time, the data structure and information content of each shared platform are different, and not all threat intelligence is related to the attack organization, requiring screening and judgment.

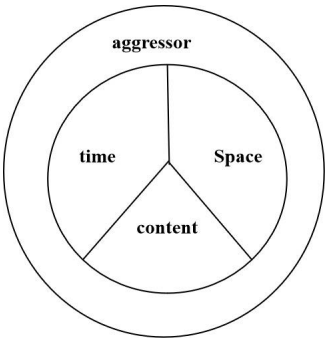

Fig. 2.2: Multidimensional Model of Threat Intelligence

2.2. Threat Intelligence Multidimensional Analysis Model. The research on attack organization involves a wide and complex range of technical means, including packet tracking, attack trace retention technology, malicious sample analysis, etc. These technologies obtain clue information of the attack organization through technical analysis of the attack process, which to some extent characterizes its characteristics [10]. The author focuses on the research of attack organizations, starting with threat intelligence, learning from the threat intelligence pyramid model, attack chain model, and diamond model, as well as different threat intelligence standards. With the ultimate requirement of attack organization association and judgment, the author integrates tactical intelligence, operational intelligence, and strategic intelligence. Through threat intelligence analysis and research, a multi-dimensional threat intelligence model guided by attack organization association and judgment is proposed. As shown in Figure 2.2, the model includes three dimensions: time dimension, spatial dimension, and content dimension, and proposes different feature indicators based on each dimension to establish a multidimensional analysis of threat intelligence. The proposal and establishment of this model mainly aims to deeply mine higher value threat intelligence information related to attack organizations through multidimensional analysis of threat intelligence, and use this model to achieve association and analysis of attack organizations.

(1) Characteristic indicators based on time dimension. Each attack is accompanied by a time characteristic, which is an inherent important characteristic of threat intelligence. Although IOC has timeliness and its role in the defense process may be reduced or even lost, for attacking organizations, each attack will last for a long time. Early threat intelligence can be used for early warning and defense in the later stage [11,12]. The time at which each attack organization initiates an attack varies, and the identity information of the attack organization can be inferred from the time. It can also be distinguished from other attack organizations. For example, APT28 (Fantasy Bear) is considered to have a Russian background, partly because during attack analysis, security engineers found that over 96% of the malware samples were compiled between Monday and Friday, and over 89% were in the UTC+4 time zone, Compiled between 8am and 6pm, similar to the working hours in Moscow and St. Petersburg, and judged to have a Russian background based on other information. At the same time, the attack time of different attackers varies over a long period of time. In order to clarify the relationship between attackers and attack time and support the time differentiation between different attack organizations, the author selected APT32 and BITTER as examples for analysis. Figure 2.3 shows the temporal distribution of all threat intelligence of APT32 and BITTER attack organizations from 2017 to 2022, with the horizontal axis representing time, the vertical axis represents the proportion of time distribution in all IOC within that time period.

From the above analysis, it can be seen that when an attacking organization initiates an attack, time clues are left behind. These time clues are also important content of threat intelligence. We can obtain the time dimension characteristics of the attacking organization by analyzing the time distribution of threat intelligence, which can be used as a classification basis for different attacking organizations. In summary, there is a certain correlation between time and attack events and attack organizations, which can be used as one of the specific indicators for classifying and judging attack organizations. Therefore, the characteristic indicator of the time

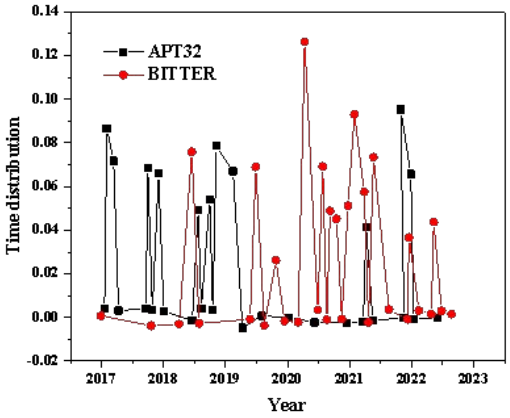

Fig. 2.3: Time distribution of APT32 and BITTER attacks

dimension of threat intelligence is the occurrence time of the attack event. Specifically, assuming that a threat intelligence is represented by "T", its time dimension is represented by "Tt", and the attack time is "T":

$$T_t = [t] \tag{2.2}$$

(2) Feature indicators based on content dimension. The collection of threat intelligence is a long and arduous process. Due to inadequate sharing mechanisms, the description of the same threat intelligence obtained through different sources and methods often does not have significant deviation, and there is a problem of one-sided content description [13]. Therefore, on the basis of analyzing the obtained threat intelligence, the author also comprehensively analyzed the intelligence content of multiple threat intelligence sharing platforms. In response to the main problem of the attack organization studied by the author, several characteristics with obvious directionality for the attack organization were abstracted from the multi-source threat intelligence. The main indicators include: attack target, attack purpose, attack event, code features IOC (URL, Hash, Domain, P, Emai1), Intelligence Description.

Specifically, assuming that "T" represents a threat intelligence information with a content dimension of "Tc". "C1" represents the "attack target" of "T", "c2" represents the "attack purpose" of "T", "c3" represents the "attack event" of "T", and "c4" represents the "code feature" of "T", If "c5" represents the "URL" of "T", "c6" represents the "Hash" of "T", "c7" represents the "Domain" of "T", "c8" represents the "IP" of "T", "c9" represents the "Eamil" of "T", and "c10" represents the "intelligence description" of "T", then the content dimension Tc of threat intelligence "T" can be expressed as:

$$T_c = [c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}] \tag{2.3}$$

(3) Feature indicators based on spatial dimensions. According to the diamond model of threat intelligence, infrastructure describes the physical or logical structures used by attackers to deliver capabilities, such as IP addresses, domain names, email addresses, etc. Due to the limitations of attack costs, the infrastructure chosen by attackers is often concentrated in a certain space, so security analysts often believe that some location information of the infrastructure is to some extent related to the attack organization or can be used to distinguish different attack organizations [14]. The "geographic location" information contained in threat intelligence can analyze the infrastructure status of attacking organizations, determine their possible locations, and distinguish different attacking organizations, therefore it is considered as one of the indicators of the spatial dimension of threat intelligence. In addition, each attacking organization has many purposes for implementing network attacks, and is currently increasingly politicized, including the influence of "geopolitical" factors. In

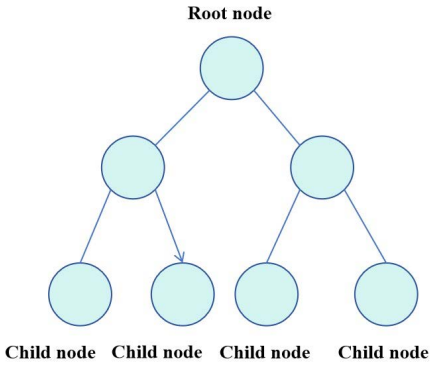

Fig. 2.4: Schematic diagram of tree structure

other words, the geographical location of the victims pointed to in these threat intelligence is also an important indicator for determining the attack organization. Therefore, the geographical location of the victim included in the threat intelligence is also considered as one of the characteristics of the spatial dimension.

In summary, the spatial dimension of threat intelligence includes two characteristic indicators, one is the distribution of address locations where the attack organization's infrastructure is located, and the other is the distribution of victim location information. Specifically, assuming that a threat intelligence information is represented by "T", its spatial dimension is represented by "T1", its home location is "l1", and the attacked country or region is "l2", then the spatial dimension T1 of threat intelligence "T" can be expressed as:

$$T_l = [l_1, l_2] \tag{2.4}$$

2.3. Attack Organization Analysis Based on LightGBM Model. The analysis of attack organizations is the determination of attack organizations for APT attacks that have already occurred, which is the consistency determination of attack organizations. It is based on the characteristics of attack organizations that have already occurred to define the initiator of new attack events. Ultimately, it is essentially a multi classification problem. There are two methods for this, one is to use the idea of attack organization similarity. Every time a new APT attack occurs, the similarity between the event and each attack organization in the attack organization fingerprint database is calculated to determine the direction of analysis. It is obvious that the time complexity of this method is linearly related to the number of known APT organizations in the fingerprint database. When the number of known APT organizations is too large, it will lead to excessive computational complexity. A more efficient method is to train multiple classification models through machine learning to complete the analysis of attack organizations.

(1) Fundamentals of Classification Models. The structure composed of nodes and edges is called a tree, as shown in Figure 2.4. The root node splits into child nodes, and the byte point splits into new child nodes by re serving as the parent node. Decision Tree, as the name suggests, utilizes a tree structure for decision-making, using each non leaf node (i.e. the connecting line in the graph) as a judgment condition and each leaf node (i.e. the circle in the graph) as a conclusion. Starting from the root node, draw a conclusion through multiple judgments. LightGBM is a gradient boosting framework based on decision tree learning algorithms. LightGBM chooses a decision tree algorithm based on histogram, which first divides accurately continuous values into discrete "bin" and then accumulates statistics in the histogram with "bin" as the index, then, based on the discrete values of the histogram, traverse to find the optimal segmentation point. This can simplify data expression, reduce memory usage, and avoid overfitting.

Unlike GBDT, LightGB uses a Leaf wise leaf growth strategy with depth constraints. Compared to Level wise, Leaf wise is more efficient, can reduce errors, and has higher accuracy. Level-wise splits one layer of leaves at a time, resulting in unnecessary overhead due to its indistinguishable nature. However, the Leaf-wise strategy first searches for the leaf with the highest splitting gain from all the current leaves before splitting,

which has the disadvantage of overfitting, therefore, LightGBM has added a maximum depth limit on this basis to avoid overfitting.

Category features are often used in machine learning processes, and most machine learning tools require the transformation of category features into multidimensional one hot encoded features. LightGBM directly supports category features without the need for additional one hot encoding, which reduces spatial and temporal efficiency. Compared to other frameworks, LightGBM has better performance, with advantages such as high training efficiency, low memory usage, and high accuracy.

(2) LightGBM model based on attack organization features. In this project, we will transform attack organization analysis into a multi classification problem solution. The specific classification algorithm process is as follows:

Step 1: Feature Engineering. A multi-dimensional model based on threat intelligence. By analyzing the attack organization, we establish a feature library for the attack organization. The characteristics of the attack organization include attack tactics, attack population, attack purpose, attack target, etc. Extract 51 feature dimensions from 99 attack organizations.

Step 2: Input. Encode the attack sample according to each feature, with 1 for the feature included and 0 for the feature not included, and map it to the vector space. And mark each vector category with the name of the attack organization, representing the 99 types of attack organizations as 99 dimensional vectors. Assuming that a sample x belongs to attack organization 2 (the attack organization has already been encoded in advance), then the sample is classified as category [0,1,0,0...]. By analogy, label all samples with attack organization categories;

Step 3: Training. In fact, a classification tree is trained for each possible category of the sample. There are a total of 99 attack organization categories in this round, which means that each sample includes 99 trees during each training round. For example, the first tree is for the first category of sample x, with the input being $(x, 0)$, and the second tree is for the second category of sample x, with the input being $(x, 1)$… Ultimately, the predicted values $f1(x)$, $f2(x)$ for each tree for sample x can be solved… Then, using softmax to generate probability, the probability of belonging to a certain attack organization n is:

$$p_n = \frac{exp(f_n(x))}{\sum_{k=1}^{99} exp(f_k(x))} \tag{2.5}$$

Step 4: Iteration. Calculate the residuals $f11(x) = 0 - p1(x)$, $f22(x) = 1 - p2(x)$, $f33(x) = 0 - p3(x)$ for each attack organization categor. Then use $(x, f11(x))$, $(x, f22(x))$, $(x, f33(x))$… As input for each category, iterate through M rounds, constructing 99 trees for each sample in each round. After training, we obtain a decision model labeled n for each category:

$$F_{nM} = \sum_{m=1}^{M} \hat{C}_{nm} I(x \epsilon R_{nm}) \tag{2.6}$$

Step 5: Determine. When an unknown attack occurs, it can be used as sample input to determine the type of attack organization. Assuming the sample to be tested is y, the probability that y belongs to a certain category c can be obtained by inputting the trained decision model as follows:

$$p_c = \frac{exp(f_c(x))}{\sum_{k=1}^{99} exp(f_k(x))} \tag{2.7}$$

We will use all attack samples from 99 attack organizations containing these features as training samples, and then use the Light GBM framework to train a model that can be used for attack organization classification [15]. In this process, our main focus is on parameter tuning. Light GBM through num leaves, learning rate, max depth, feature_fraction, objective, num_Several main parameters of class are used to control and optimize the algorithm, among which max_depth, feature_fraction, bagging, and fraction can all control or assist in controlling overfitting phenomena.

2.4. Overall Design of Attack Organization Association and Analysis System.

(1) Design concept of the system. The implementation of this system is based on the analysis of threat intelligence. The first problem to be solved is the acquisition of threat intelligence, which integrates multiple sources such as threat intelligence platform intelligence data, APT reports, and internal data to collect threat intelligence and form a threat intelligence library; Process the collected multi-source heterogeneous threat intelligence data to solve the problems of low credibility and high error rate, and form a threat intelligence feature library based on a multi-dimensional threat intelligence model, thereby forming an attack organization fingerprint library; Then, use similarity algorithms with different dimensions to calculate the association of attack organizations and determine their homology; Utilize the LightGBM framework to achieve consistency determination of attack organizations and output analysis results. Finally, the attack organization association and analysis system will be implemented.

(2) System architecture. Based on the above requirements analysis, the overall architecture of the prototype system includes six modules, namely threat intelligence collection module, threat intelligence multi-dimensional analysis module, attack organization fingerprint library module, attack organization association module, attack organization analysis module, and user module. Each module has different functional designs [16].

The acquisition of threat intelligence is the foundation and support of this study. This topic selected multiple threat intelligence sources to collect data, including obtaining APT reports through crawler technology and extracting threat intelligence. This includes collecting various intelligence data from multiple threat intelligence platforms, including intelligence data accumulated in practice, and enriching intelligence by comprehensively collecting relevant information from multiple threat intelligence sources. At the same time, the sources of threat intelligence are diverse and the structure is relatively complex. In order to facilitate subsequent analysis and processing, it is necessary to screen and process the collected intelligence data, eliminate threat intelligence with low credibility or errors, and correct errors that occur during the collection process. Based on the multi-dimensional analysis module of threat intelligence, deep analysis of threat intelligence is achieved, extracting feature indicators and attack organization information from time, space, and content dimensions. Organize threat intelligence with attack organizations as the core, and form a fingerprint database of attack organizations that can be used for association and analysis of attack organizations. Based on the multi-dimensional analysis module of threat intelligence and the fingerprint database module of attack organizations, the similarity calculation is used to determine the homology of attack organizations and establish the correlation relationship between attack organizations. Using the attack organization (event) to be detected as input, consistency is determined using the LightGBM model, and the analysis results are output. User module: Implement the management of user information and permissions.

(3) The hierarchical design of the system structure. Based on the analysis of market demand and the functional positioning of the system, as well as the usage scenarios of this association and analysis system, the author designed and implemented an attack organization association and analysis system using BS architecture, which combines a three-layer architecture and MVC using a hierarchical pattern for structural design. Through request and response data operations between layers, communication between layers is achieved [17]. Within each layer, modular development is carried out according to the overall system architecture of the system. Layering modules can achieve high cohesion and low coupling, and reduce development complexity by improving code reusability. When users use the system, they initiate requests through a browser and do not directly operate background programs, ensuring the security and stability of the system. The structural hierarchy of the system is designed from top to bottom as the presentation layer, application layer, and data layer. The content of each level is introduced as follows:

Presentation layer: Refers to the human-machine interaction interface provided by the system service, including visual display and system interface. It presents data in a user-friendly manner on the page with a user orientation, and is simple and clear, in line with user habits, and convenient for user operation. On the graphical system interface, users can perform operations such as querying.

Application layer: The application layer is the center of the system's business logic processing and calculation, mainly including threat intelligence collection module, threat intelligence multi-dimensional analysis module, attack organization fingerprint library module, attack organization association module, and attack organization analysis module. It is located in the middle layer of the entire structure and serves

Table 3.1: Display of Analysis Output Function

ID	Test file name	Output Results
1	test sample	78-Urpage-52.48%

Table 3.2: User Management Function

ID	Login Name	Joined on	Is it enabled
1	admin	2021-1-1-11:11	Enabled
2	yeshun	2021-1-1-11:11	deactivated

as a connection between the presentation layer and the data layer.

Data layer: The data layer is the bottom layer of the entire structure, playing the role of the "database" decision-making and serving as the database resources of the entire system, mainly including threat intelligence data, threat intelligence dimension features, attack organization data, and user data.

3. Results and Analysis.

3.1. Testing Environment. The attack organization association and analysis system developed in this project is a WEB system with a B/S architecture, and users need to request access through a web browser when using the system [18]. The testing environment for this system is different browsers for different operating systems, such as IE browser on Windows and Google browser on Mac. From the browser side testing verification, all the service functions provided by the system backend are normal.

3.2. System functional testing. The system has been tested for functionality in the Chrome browser on Windows 10 as follows. The intelligence reading and search query function can achieve the reading of various information about attacking organizations, and achieve intuitive display of threat intelligence. The intelligence management function can achieve operations such as adding, deleting, and updating intelligence. The association analysis function can clearly display the association relationship of attack organizations after calculating the similarity of each dimension. In this section, the similarity threshold setting and attack organization input are specially designed. By outputting the name of the attack organization to be queried and the lowest similarity, the association relationship graph related to it with a similarity greater than the threshold is analyzed and output. The results can serve as the basis for determining the homology of attack organizations. Table 3.1 shows the analysis output function, where the input is the attack samples to be detected and the output is the analysis results of the attack organization. Table 3.2 shows the user management function of the system, which enables the management of administrator users and ordinary users. After testing, all functions of the system have been implemented and meet expectations [19,20].

4. Conclusion. In recent years, an increasing number of APT attacks have threatened China's cyberspace security, bringing heavy pressure to cybersecurity defense. As the saying goes, "Knowing oneself and the enemy is invincible in a hundred battles." In order to occupy a favorable position in the game of network attack and defense and make breakthroughs in deep tracing, it is essential to study and master attack organizations. The author has conducted research on the association and analysis of attack organizations based on threat intelligence, and designed and implemented a system for the association and analysis of attack organizations. The attack organization association and analysis system developed in this project is a WEB system with B/S architecture, and users need to request access through a web browser when using the system. The testing environment for this system is different browsers for different operating systems, such as IE browser on Windows and Google browser on Mac. From the browser side testing verification, all the service functions provided by the system backend are normal. At present, the analysis technology of threat intelligence is rapidly developing, and research on APT is also receiving increasing attention from domestic and foreign researchers. The author proposes a multi-dimensional analysis based on threat intelligence to study the correlation and judgment methods of attack organizations, and designs and implements an attack organization correlation and judgment system,

which to some extent solves the problem of determining the homology and consistency of attack organizations, and can provide research ideas and guidance for security analysts. However, there are still some issues worth further research in future learning. Although certain achievements have been made in multi-dimensional analysis based on threat intelligence, the characteristics of each dimension are still not detailed enough, and there are still some features that cannot be obtained. How to obtain more detailed content and detailed dimensional features of threat intelligence needs to be further deepened in the analysis of threat reports.

REFERENCES

[1] Hou, H. , Cao, G. , Ding, H. , Zhao, C. , & Wang, A. . (2021). Research on automatic detection system of encoder accuracy based on pid algorithm. Journal of Physics: Conference Series, 1754(1), 012233-.

[2] Onyema, E. M. , Dalal, S. , Romero, Carlos Andrés Tavera, Seth, B. , Young, P. , & Wajid, M. A. . (2022). Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities. Journal of Cloud Computing, 11(1), 1-20.

[3] Olukoya, O. . (2021). Distilling blockchain requirements for digital investigation platforms. Journal of Information Security and Applications, 62(1), 102969.

[4] Liu, Y. , Hou, Z. , Cui, J. , & You, K. . (2021). Design and research of automatic fishing machine based on acoustic adjustment. Journal of Physics: Conference Series, 1802(2), 022052 (6pp).

[5] Liu, X. , Zhu, S. , Yang, F. , & Liang, S. . (2022). Research on unsupervised anomaly data detection method based on improved automatic encoder and gaussian mixture model. Journal of Cloud Computing, 11(1), 1-16.

[6] Li, G. , Zhai, J. , Luo, C. , & Li, A. . (2021). Retraction note: research and application of automatic monitoring system for tunnel-surrounding rock measurement based on gis. Arabian Journal of Geosciences, 14(24), 1-1.

[7] Lin, S. . (2021). Research on automatic inspection system of printed circuit board based on computer vision. Journal of Physics Conference Series, 1861(1), 012093.

[8] Zhang, L. H. , Liang, Y. , Tang, Y. , Wang, S. , Tang, C. , & Liu, C. . (2021). Research on unknown threat detection method of information system based on deep learning. Journal of Physics: Conference Series, 1883(1), 012107 (6pp).

[9] Gao, W. , Tang, J. , & Wang, T. . (2021). An object detection research method based on carla simulation. Journal of Physics: Conference Series, 1948(1), 012163-.

[10] Dang, L. . (2021). Research on landscape design assistant system based on artificial intelligence and information technology. Journal of Physics Conference Series, 1744(2), 022103.

[11] Bagga, P. J. , Makhesana, M. A. , Bhavsar, D. L. , Joshi, J. , Jain, K. , & Patel, K. M. , et al. (2022). Experimental investigation of different nn approaches for tool wear prediction based on vision system in turning of aisi 1045 steel. International Journal on Interactive Design and Manufacturing (IJIDeM), 17(5), 2565-2582.

[12] Zheng, S. , Li, J. , Chen, S. , Liang, Y. , & Lin, J. . (2021). Research on breakpoint area detection of computer communication network transmission data based on cloud framework. Journal of Physics: Conference Series, 2083(4), 042045-.

[13] Pan, A. , & Wang, N. . (2021). Design and implementation of crop automatic diagnosis and treatment system based on internet of things. Journal of Physics: Conference Series, 1883(1), 012062 (6pp).

[14] Zong, Y. , Zhao, X. , & Ba, Z. . (2021). Design and research on the fatigue detection system of ship bridge duty based on image processing. Journal of Physics: Conference Series, 2131(3), 032119-.

[15] Liao, X. , & Xie, J. . (2021). Research on network intrusion detection method based on deep learning algorithm. Journal of Physics: Conference Series, 1982(1), 012121-.

[16] Belousov, K. I. , Bashirov, R. K. , Zelianskaia, N. L. , Labutin, I. A. , Ryabinin, K. V. , & Chumakov, R. V. . (2023). Profiling of conceptual systems based on a complex of methods of psychosemantics and machine learning. Automatic Documentation and Mathematical Linguistics, 57(4), 193-205.

[17] Li, Y. , Li, F. , & Song, J. . (2021). The research of random forest intrusion detection model based on optimization in internet of vehicles. Journal of Physics Conference Series, 1757(1), 012149.

[18] Luo, M. , Ke, Q. , & Li, J. . (2021). Research on automatic braking and traction control of high-speed train based on neural network. Journal of Physics: Conference Series, 1952(3), 032048-.

[19] Zhang, B. , Bai, L. , & Chen, X. . (2021). Research on the design of fire alarm and pre-treatment robot system. Journal of Physics: Conference Series, 1865(4), 042106-.

[20] Lin, T. , Zhao, Y. , Zhang, H. , Li, G. , & Zhang, J. . (2021). Research on information security system of ship platform based on cloud computing. Journal of Physics: Conference Series, 1802(4), 042032 (7pp).

Edited by: Zhigao Zheng
Special issue on: Graph Powered Big Aerospace Data Processing
Received: Nov 1, 2023
Accepted: Nov 8, 2023