Security Situation Awareness Analysis of Mobile Power Business Based on Artificial Intelligence

Liang Yuan, Yubin Du*, Xinrui Ju, Mengyuan Li

Yubin Du:duyubin1221@163.com*, Liang Yuan:henbeirongd5@163.com,
Xinrui Ju:zengkongogq1@163.com,Mengyuan Li:zongrhr4078@163.com

State Grid Huitongjincai (Beijing) Information Technology CO., LTD (Beijing ,100089,China)

Abstract. Service bearer network is an important support for information communication in various jobs. The traditional security construction with numerous chimneys is difficult to form synergistic benefits and difficult to operate and maintain. The outbreak of malicious codes such as APT attacks and ransomware, and the access of new units all bring great risks and challenges to the safe operation of the network. Establish a system for statistical analysis and multi-form visual presentation of all kinds of security situation information, and realize the normal monitoring of cyberspace situation by compiling and integrating the security situation of each network. The test shows that the system supports equipment log collection, asset detection, security event feature extraction and correlation analysis, which can help network operators to grasp the security situation of cyberspace at any time and improve the overall security protection ability of the network.

Keywords: network security; Data acquisition; Situation awareness; data analysis.

1 Introduction

In recent years, there are more and more cyber attacks with national and organizational backgrounds, and the special roles of government, military, finance and large enterprises often face more threats from outside. For example, "Stuxnet virus" attacking Bushehr nuclear power plant in Iran, "Aurora attack" against Google mail server, "BlackEnergy" attack against Ukrainian power grid, etc. Although the information security personnel of the enterprise have deployed a large number of security devices in the network, some attacks will still bypass all protective measures and go straight to the enterprise, resulting in the leakage, damage or tampering of important data assets[1]. Therefore, it is necessary to find the threats hidden in the network in time through technical means, quickly find the malicious behaviors in the threats as soon as possible, accurately locate the target and the source of the attack, and judge and trace the intrusion path and attacker background, so as to solve the security threats in the enterprise network from the source and reduce the losses caused by the security threats to the enterprise as much as possible[2].

2 System design

In terms of system architecture design, the system is designed according to the overall architecture of three levels: security data access and convergence, security data processing and

MSIEID 2023, December 08-10, Guangzhou, People's Republic of China

DOI 10.4108/eai.8-12-2023.2344481

analysis, and security situation presentation. Security data is collected through mirror traffic, syslog and GCB010-2015 standard interface, data is preprocessed and stored by using big data technology, and network threats are intelligently analyzed in combination with Internet threat intelligence big data, and the analysis results are presented in a timely manner. At the same time, security incidents are handled automatically or in combination with security operation and maintenance personnel, forming security incident monitoring and monitoring[3]. The functional design of each level and module is relatively independent, and the information exchange is carried out by using industry common interface and military standard interface, so that the whole system has high expansibility. At the same time, relying on the multi-dimensional security measures such as physical security, host security, application security, data security, network security and so on, the security of the mobile office service bearing network is realized[4]. At the same time, it can discover key threats in advance, continuously perceive the network security situation, warn the network security incidents, and support the network security emergency response work. The overall architecture design of the system is shown in Figure 1.

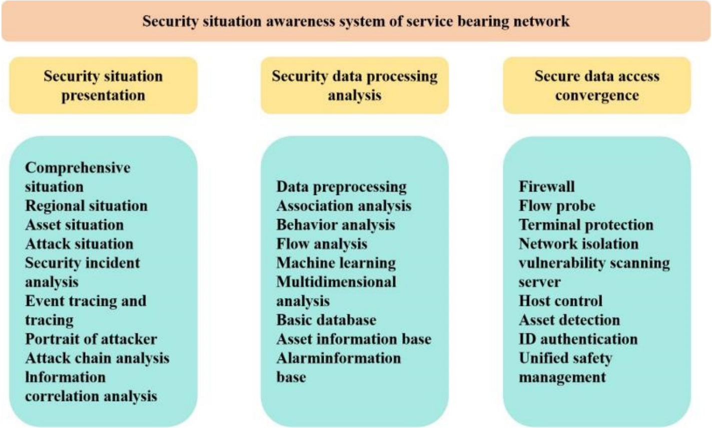

Figure. 1. System architecture design

The structure of artificial intelligence information security network perception system is shown in Table 1.

Table 1. Structure of Artificial Intelligence Information Security Network Perception System

Situation awareness	This module uses artificial intelligence algorithm to predict, understand and identify the situation to complete the situation awareness.
Information fusion	The collected security situation data generally come from network devices such as switches and routers, as well as security devices such as IDS/IPS and firewalls, as well as applications, services and databases, so the system needs to input these data from different sources. Line integration, so as to improve the accuracy of situation awareness.
Information extraction	This module belongs to the foundation of security

	awareness situation. Security situation data are basically obtained from network equipment, security equipment, applications and service systems. Information extraction mainly obtains information from these modules, revises and standardizes the information, and expands the basic characteristics of time.
Situation assessment	This module mainly analyzes the situation and relevance. According to the situation, the results are evaluated, a comprehensive network situation map is established, and the situation report is analyzed, thus providing decision-making basis for managers.
Information preprocessing	Situation awareness mainly uses multiple sensors to collect data, so there will be a lot of noise in the process of collection, and there may be data missing, which requires data denoising. At the same time, it can also realize the preprocessing of incomplete data, such as filtering impurities and handling user distribution.

2.1 Secure data access convergence

Security data access convergence is the system input of the whole network security situational awareness, and it is the premise and foundation of network security data analysis and situational awareness presentation. The security data convergence access layer collects data through traffic collectors, log collectors, asset detectors and other devices. Data collection according to unified planning and unified standards to obtain the key network traffic, logs and alarm information and asset data of the mobile power business carrying network, to ensure that the safety data input by the system is comprehensive, sufficient, detailed and accurate, and to lay a foundation for safety analysis and mastering the overall security situation[5].

The traffic collector is deployed at the core switch of each node in the form of network bypass, and the traffic is restored and analyzed after collecting the mirror traffic of the key network to generate traffic logs and traffic alarm information. Among them, the traffic log mainly records the time, IP address, port and protocol information of the data packet; Traffic alarm is to compare the traffic data with virus database and feature database after reduction, and analyze the threat to form alarm information. Through the full-factor and fine-grained records of network metadata, network transmission data, load behavior data and other information, the ability to find and trace targeted attacks and advanced threats is improved, so as to achieve the continuous detection effect of potential threats and unknown threats.

The log collector collects log and alarm information. Log information collection collects log and alarm information from terminal hosts (terminal protection software), network devices, security protection devices, and vulnerability scanning devices, including mobile power service servers, mobile power service terminals, routers, switches, firewalls, traffic probes, network isolation devices, security management systems, and vulnerability scanning devices. The data collection of the terminal host computer collects all kinds of security data from computers and various terminal assets in the mobile power service network through the existing terminal client software such as terminal security management and control software and antivirus software, and collects all the data generated by the terminal, including violation log data, patch information data, terminal poisoning situation, terminal log data, etc. The data acquisition of network equipment mainly collects log information and status information; The data collection of safety protection equipment mainly collects access strategy log, alarm log, operation log and status information, etc. The data collection of vulnerability scanning equipment mainly collects vulnerability information.

The asset detector periodically scans, detects and identifies all terminals, networks and security protection devices in the network by active detection, and obtains information such as asset types, IP addresses, operating systems, software versions, protocols, services and open ports, and the information is reported to the secure data bus by API calling[6].

2.2 Security data processing analysis

Security data processing and analysis is an important guarantee for the accurate perception and presentation of security situation. Under the guidance of the security system and the standard system, the system creates a comprehensive big data processing and analysis by building data access, data processing, data organization, data analysis, data governance and information sharing services.

The data access part is responsible for efficient and flexible access and distribution of heterogeneous data.

Data processing uses the results of data governance and the knowledge of models and rules in the knowledge base to complete the construction of original database, resource database, subject database and mobile electricity business database in data organization, generate data related information, realize data fusion and enhance data value.

By managing information such as data resource catalogue, metadata, classification and consanguinity, data governance defines the expected effect of data convergence, standardizes data organization forms, controls data quality, and ensures the operation of data throughout its life cycle through operation and maintenance means.

Table 2. Data Organization Category

Name	Function	Content
Primitive library	Data from different sources are stored according to the original data format, and all data types are supported.	Traffic log, terminal log, security log, equipment log, missed scan log, terminal alarm, equipment alarm, user behavior, etc.
resource library	Comprehensive various basic data resources are refined and processed to form a public data set.	Domain name database, security incident database, log database, alarm database, asset database, threat database, IP address database,etc.
Subject library	Organize data in a multi-dimensional and theme-oriented way to form a data set for business support or decision analysis support,provide basic data, temporary data, analysis data, mining data,etc. for business activities, and record the knowledge summarized and discovered in the business	Attack weapon library, attack means library,attacker information library, victim information library, monitoring information library, network behavior library, etc.

	process.	
knowledge base	Collection of characteristic knowledge data, rules and methods related to network security or network security professional field.	lP library, malicious city name library, algorithm library, model library, vulnerability library, label rule seal, etc.

Data organization standardizes the organization and presentation of data in the process of gradually increasing data value. The data organization categories are shown in Table 2.

2.3Network Security Situation Estimation

The impact of access to a security target is often associated with time and space. For the freedom of, its attack attack attack and the related resources will change after being attacked. For the whole network, the distribution of attacks will also change after attacks [7]. As time goes by, some event notifications will be released from the event timeout slowly and filled with new event notifications.The frequency of an alarm indicates the level of network access. The security risk level of the network node after calculating the fusion time is mainly related to the alarm confidence c, the alarm level v and the related h. The alarm confidence level is established by the auto translation and the fusion calculation. Resources relate to network configuration and services. In addition to the above analysis, it is also necessary to consider the node protection degree en and the alarm return sn. The security index of the independent node can be obtained by (1).

$$Z_n(t) = \sum c_i v_i h_i / e_n s_n \tag{1}$$

The risk value of network security can be calculated according to the following criteria (2).

$$Z_N(t) = \sum \omega_n Z_n(t) \tag{2}$$

However, in practical application, a complete safety problem is also needed to evaluate the operation level of the entrants. The formula is described as follows:

$$Q_n(t) = \sum c_i v_i \tag{3}$$

Through the above analysis, we can get the change curve of the network security evaluation value with time, and realize the prediction of network security based on the prediction value of network security state, thus realizes the realization of network security state.

3 Results and Analysis

The data sources that the system needs to collect include: network traffic image data, log data, security intelligence and support data. Among them, the log data is relatively standard[8]. You can export syslog log, web service log, firewall log, NetFlow log, etc. by configuring the logs of relevant devices and servers. At present, there is no unified standard for security intelligence and support data. We normalize the security intelligence data into the intelligence data that the system can identify and use. At the same time, we regularly update the intelligence base by synchronizing the cloud server or upgrade package, and store all kinds of intelligence and support data in the system for system processing and analysis.

The large-scale data acquisition and processing platform must have the ability of multi-point data acquisition and fault tolerance, especially for the large-scale data acquisition and processing center. The system preprocesses the original image traffic, uses multi-core parallel processing means to analyze, restore and analyze the original network data with large traffic, and then forms a unified traffic log format and uploads it to the big data platform for storage. The architecture of flow acquisition probe is shown in Figure 2:

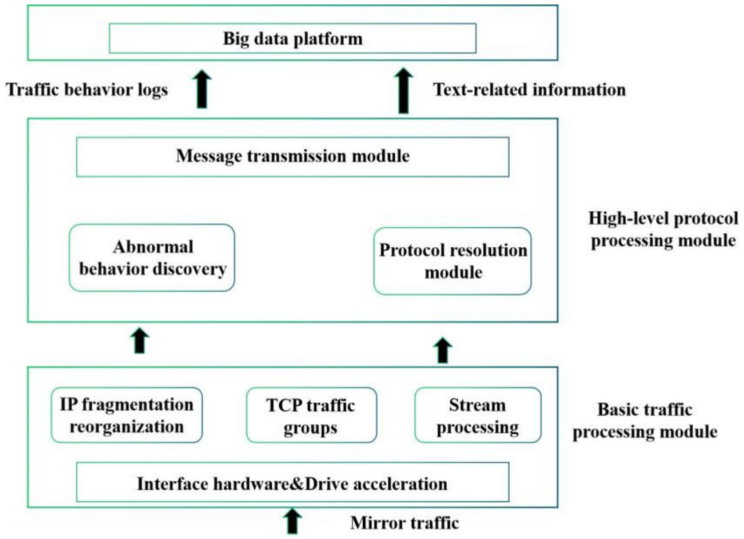
Big data platform
Traffic behavior logs
Text-related information
Message transmission module
High-level protocol processing module
Abnormal behavior discovery
Protocol resolution module
IP fragmentation reorganization
TCP traffic groups
Stream processing
Basic traffic processing module
Interface hardware&Drive acceleration
Mirror traffic

Figure .2. Traffic collection architecture diagram

One of the characteristics of the data layer of the attack characteristic event map is that a single attack characteristic event is a weakly connected branch of the whole attack characteristic event map. If E represents the attack characteristic event map and G (where i ∈ N + and ≤i≤ M, M is the number of weakly connected branches) represents a single attack characteristic event, the following relationship is shown in formula (4-6):

$$G= 1Gi \tag{4}$$

$$Gi \cap Gi=\varnothing(1 \leq i<j \leq M) \tag{5}$$

$$E= G. \tag{6}$$

From the perspective of set, E represents the complete set, and G is a division of the complete set E. This design can facilitate the system to traverse each weakly connected branch of the attack characteristic event map when discovering the attack behavior in the later stage[9].

The traffic collection probe is mainly divided into two modules. The basic traffic processing module is responsible for preprocessing the original traffic, including basic packet reorganization and traffic reorganization, and can analyze the information of traffic transmission layer and network layer; The high-level protocol processing module is also divided into abnormal behavior discovery, protocol resolution and message transmission modules. The protocol resolution module is responsible for in-depth resolution of application layer protocols, analyzing the information of application layer protocols such as HTTP, DNS and SMTP, and extracting key information to the message transmission module. At the same time, restore the files contained in HTTP, SMTP and other protocols, and send the restored information to the big data platform for saving; The abnormal behavior discovery module discovers the possible behaviors such as worms, port scanning and Trojans in the traffic. All information is standardized through the message transmission module, and then sent to the big data platform for storage. After continuous testing and optimization, we finally realized the real-time collection and processing of the full network traffic through the data restoration technology under the 10 Gigabit Network and IPv4 / IPv6 network environment. This technology mainly adopts the optical splitter image or network port image technology to export the traffic in the network, and then input it to the analysis platform for correlation analysis. Traffic restoration and data analysis can perform high-performance analysis on mainstream protocols such as HTTP and SMTP / POP3 in IPv4 / IPv6 network environment, and restore the files transmitted by mainstream P2SP software through fragment file detection and P2SP reorganization[10].

(1) Port matching: in the process of network protocol development, a series of standard protocol specifications have been formed, which stipulate the ports used by different protocols. Although some other widely used applications do not have standardized ports, they have formed de facto standard ports. Port matching is to use TCP / UDP ports to identify behaviors according to the corresponding relationship between standards or factual standards. This method has the advantages of high detection efficiency, but it is easy to be forged. Therefore, on the basis of port detection, it is necessary to add the judgment and analysis of feature detection to further analyze the data.

(2) Traffic feature detection: there are two kinds of traffic feature detection. One is the identification of standard protocol traffic. The standard protocol stipulates a unique message, command and state migration mechanism. These traffic can be accurately and reliably identified by analyzing the proprietary fields and states of the application layer in the traffic packet; The other is the identification of undisclosed protocol traffic. Generally, it is necessary to analyze the protocol mechanism through reverse engineering and identify the communication traffic directly or through the characteristic field of message flow after decryption.

(3) Automatic connection and association: with the development of Internet applications, more and more data are transmitted on the Internet, and the mode of single connection to complete all tasks gradually begins to appear bottlenecks. Therefore, many protocols use the way of dynamic negotiation port for data transmission. In order to identify these data, it is necessary to automatically associate them with the data transmission link and restore them according to the message information on the control link.

4 Conclusion

To sum up, the structure of the information network security situation awareness system based on artificial intelligence at this stage mainly includes information extraction, information preprocessing, information fusion, situation awareness and situation assessment. In the process of system operation, basic operation index, network vulnerability index and network threat index are key indicators, which provide data support for the operation of situational awareness system. The appearance of this technology is helpful to improve the security of information network, and it also integrates many technologies such as data mining, data fusion and pattern recognition, so that some information network security problems can be effectively solved in the early stage, which plays an important role in promoting the safe and reliable operation of power system and providing sufficient power for social production and people's daily life.

References

[1]Bai, J. , Zhang, Z. , & Shen, B. . (2022). Internet of vehicles security situation awareness based on intrusion detection protection systems. Journal of computational methods in sciences and engineering,85(1), 22.

[2] Yuan, Q. , Pi, Y. , Kou, L. , Zhang, F. , & Ye, B. . (2022). Quantitative method for security situation of the power information network based on the evolutionary neural network. arXiv e-prints,47(8),63-69.

[3] Zhan, K. . (2021). Design of computer network security defense system based on artificial intelligence and neural network. Journal of Intelligent and Fuzzy Systems,85(7), 1-13.

[4] Xia, Y. , Zhang, X. , Ge, H. , Hao, S. , & Zou, W. . (2021). Optimal dispatching technology of distributed power generation based on situation awareness. American Journal of Electrical and Electronic Engineering, 9(1), 7-11.

[5] Xiaoyu G S .(2023).A fuzzy group decision-making framework for computer network security evaluation with probabilistic linguistic information.International Journal of Knowledge-based and Intelligent Engineering Systems(3),355-365.

[6] Zhang, Z. , Miao, Y. , & Peng, X. . (2021). Analysis of research situation of domestic tomato irrigation and fertilization based on artificial intelligence technology. Journal of Physics: Conference Series, 1852(3), 032048 (9pp).

[7] Zhang, H. , Kang, K. , & Bai, W. . (2023). Hierarchical network security situation awareness data fusion method in cloud computing environment. Journal of computational methods in sciences and engineering,36(7),58-62.

[8] Choudhury, A. , & Asan, O. . (2023). Impact of cognitive workload and situation awareness on clinicians' willingness to use an artificial intelligence system in clinical practice. IISE transactions on healthcare systems engineering,69(74),12-16.

[9] Fahima K R S S I .(2023).A new method of image encryption using advanced encryption Standard (AES) for network security.Physica Scripta(12), 1744(3), 032024 (7pp).

[10] Cui, L. . (2021). A preliminary study on the management strategy of university personnel files based on artificial intelligence technology. Journal of Electronic Research and Application: JERA,857(2), 5.