УДК 681.3 http://doi.org/10.15407/pp2022.03-04.403

DEVELOPMENT OF DECISION SUPPORT SYSTEM USING OLAP-TECHNOLOGIES FOR INFORMATION SECURITY MONITORING SYSTEMS

Konul Dashdamirova

У статті висвітлено необхідність постійного моніторингу комп'ютерних мереж з метою забезпечення інформаційної безпеки та проаналізовано джерела даних для моніторингу інформаційної безпеки. Досліджено методи збору даних з різних джерел, досліджено категорії систем моніторингу інформаційної безпеки. Запропоновано архітектурно-технологічну модель системи підтримки прийняття рішень на основі OLAP (Online Analytical Processing) і сховища даних для швидкого реагування на інциденти безпеки та виявлені інциденти в системах моніторингу інформаційної безпеки.

Ключові слова: інформаційна безпека, моніторинг інформаційної безпеки, SIEM, UBA, OLAP, сховище даних

The article highlighted the need for continuous monitoring of the computer networks (CN) for information security and analyzed the sources of data for information security monitoring (ISM). Methods of data collection from various sources have been investigated, and categories of ISM systems have been studied. The architectural-technological model of the system supporting decision-making based on OLAP (Online Analytical Processing) and data warehouse has been proposed for quick response to security-related incidents and detected incidents in ISM systems.

Keywords: Information Security, Information Security Monitoring, SIEM, UBA, OLAP, Data warehouse

Introduction

The rapid development of the global Internet network and Information Communication Technology (ICT) has led to the formation of an information environment that affects all spheres of human activity. The emergence of local and global CNs facilitated the rapid dissemination of information and created new opportunities for information exchange. New technologies increase the efficiency of production processes and contribute to the expansion of business relations. However, despite the intensive development of ICT, the vulnerability of modern information systems and the CN does not decrease, and the dependence of the information technologies used by society on the degree of security is increasing. Modern methods of processing, transmission and collection of information lead to the emergence of threats related to the loss, distortion and disclosure of information. The CN is constantly exposed to various types of cyber threats. These threats can be hacker attacks, malicious programs, outdated or faulty network equipment and operating systems, mobile and public cloud computing, third-party service providers, and so on [1]. In an environment where cyber threats are widespread and unavoidable, rapid detection of cyber threats and rapid response to possible incidents are of great importance to ensure the uninterrupted and reliable operation of the CN. The need for continuous monitoring of the information security of the CN becomes urgent. ISM is the process of collecting, systematizing and analyzing information about the status of the network and the behavior of its users [2]. Modern ISM systems operate in a continuous, automatic mode, allowing timely detection of threats and the preparation of appropriate notifications. Serves to prevent security risks promptly.

Analysis of sources on which ISM systems are based

Information security is monitored by the process of checking all security incidents obtained from various sources. The source of incidents can be CERTs, antivirus systems located in the infrastructure of various organizations, operating system logs, scanners for security analysis of information infrastructure, network equipment, and other sources (Fig. 1.) [3].

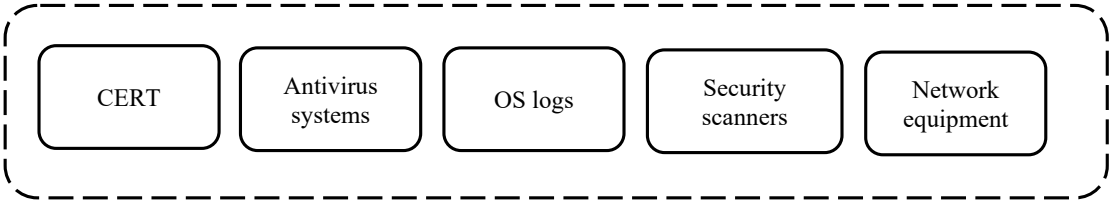

Fig. 1. Sources for information security monitoring

CERT (Computer Emergency Response Team) is a group of computer security experts involved in collecting, monitoring, classifying, and neutralizing incident information. The main purpose of CERT is to analyze incidents sent

by users (phishing, social engineering), suspicious files, viruses, as well as network traffic sessions, to respond quickly to new threats, inform users and develop security recommendations [4].

The first CERT group was formed at Carnegie Mellon University in 1988 after thousands of servers were infected with the Morris worm. The group currently has the status of a CERT coordination center and licenses and coordinates the activities of information security incident response centers around the world. National, regional or industrial CERTs can be established in coordination with Carnegie Mellon University. Currently, many companies around the world also create CERTs, but not all of them receive official status [5]. In total, there exist currently about 250 CERT teams in various countries around the world. Analysis of data collected in CERTs can allow for the timely detection and prevention of cyber threats and the assessment of the level of information security within a country to ensure the social security of society.

Today, computer viruses and malware are a real source of danger for any enterprise, organization, and others that use information technology in their activities. The widespread use of these global networks can be explained by the insufficient attention to network security issues in a large number of local computer networks. Computers are increasingly infected with malicious software when working with Internet resources or through email messages. The target of viruses can be any user's computer, global or local computer networks. The damage can lead to the failure of the computer and all computer networks in general, the violation of data integrity, accessibility, and confidentiality.

Every year, the creation of new types of viruses that can bypass traditional protection methods raises the issue of protecting computer networks from malware. An important way to fight computer viruses is to prevent them in time. Timely detection of infected files or disks, and complete destruction of detected viruses on each computer help to prevent the spread of the virus epidemic to other computers and computer networks. Antivirus software is a special program that is used to detect computer viruses, as well as undesirable (considered harmful) programs, recover infected (modified) files by these programs, and prevent infection (modification) of files or operating systems with malicious code. Network antivirus programs carry out monitoring of servers, network computers, and installed software, allow you to monitor e-mail, data of allowed network protocols (HTTP, FTP), file servers, external carriers (floppy disks, flashcards, CDs, DVDs), as well as all channels through which computer viruses and malicious programs can penetrate [6].

The essence of the antivirus monitoring method is that the antivirus program is constantly in the computer's memory and monitors all suspicious actions performed by other programs. Antivirus monitoring allows you to check all running programs, created, opened, and saved documents, programs, and files received via the Internet. The antivirus monitor will inform the user if any program tries to perform potentially dangerous actions.

Log files found in the logs of operating systems or web servers contain system information about the operation of the server or computer and information about the user behavior. The purpose of log files is to record all operations performed on the webserver or computer for monitoring by the administrator. This information is of great importance in the event of security incidents. Regular monitoring of logs and analysis of log files allows to identify errors in the operation of a particular system or site, diagnose malicious activity, identify threats, threats, collect information about user behavior, as well as evaluate according to various criteria [7].

Weaknesses in information systems, infrastructure nodes, and elements of the information security complex create great problems for information security. To identify vulnerabilities, companies need to analyze the security of their information infrastructure. As a rule, vulnerability scanners are used for security analysis from automatic instruments operating in static and dynamic scanning modes. At present, this class of tools allows you to solve a wide range of problems. A vulnerability scanner is a program that identifies and creates a registry of all systems connected to the network (servers, computers, virtual machines, containers, firewalls, switches, and printers). The program allows you to identify each device, the operating system and installed programs on this device, as well as other attributes such as open ports and user accounts and passwords, as well as track other elements that pose a potential threat to information security [8].

Faults in the hardware or software of the CN, slowing down or stopping the operation of important network services can lead to unpleasant consequences. A modern network equipment monitoring system is a complex information system that monitors servers, hosting, processes, and services on users' computers, as well as files, folders, and databases. It consists of the following components.

- network device indicators (CPU, temperature, device availability, packet loss, interface errors, available throughput, etc.) are critical parameters that need to be monitored;
- monitoring – the process of collecting, assembling, and analyzing indicators to improve the understanding of the characteristics and behavior of the components of the system. The data collected as a result of the monitoring can be visualized and drawn in the form of various graphs, diagrams, and histograms.
- the warning system is an important component that takes action when changes occur in the values of the observed indicators. When the critical value is reached, the metric value can try to solve the problem itself according to the developed scenario or send an alert to the responsible person using SMS, email, and so on [1, 2].

The network equipment monitoring system allows receiving timely information about the fault, controlling the situation, to eliminate the fault with minimal time loss [10]. During ISM, the monitoring information can be collected from various sources using both automated and non-automated tools. Primary data collection is used to analyze the state of information security and conduct various types of assessments. The following methods can be applied to obtain primary data during the use of automated monitoring tools (Fig. 2):

- agent-based data collection (agents for security incident monitoring);
- data collection without agent;
- questionnaires (forms);
- software.

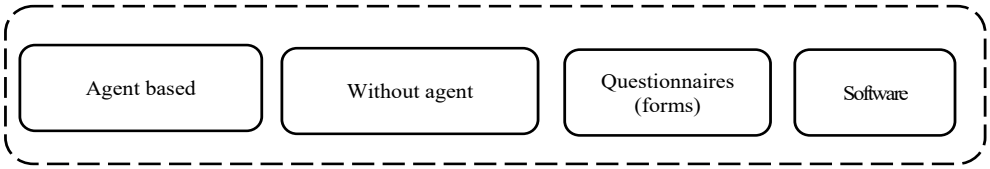

Fig. 2. Methods for collecting information from different sources

A security monitoring agent is software installed on information infrastructure components and information system nodes to gather the necessary information directly from a source. Monitoring agents can be used to collect information on security incidents, software effectiveness, user behavior, and other information.

The method of collecting data without agents involves the receipt of data from sources over the network without installing additional software for monitoring. Non-Agent data collection methods include:

- Read data directly from security log files or databases;
- Receiving information from sources using standard protocols for transmitting information about security events;
- Data collection by connecting to the program interface or the web service of the data source.

By the usage of agent-free data collection method, data collection can be carried out about security incidents, the operability of the software, and other information that the source can provide.

The collection of data on security incidents using questionnaires (forms) is carried out by filling in special electronic (paper) forms and then transferring them to information security monitoring personnel.

Data collection method using software includes information management systems on information security threats, security control systems, inventory means of software and technical means, software and information protection tools, and so on [10].

Categories of ISM systems

All currently established and used ISM Systems can fall into one of the following categories.

SIEM (Security Information and Event Management) is a system that allows analyzing data obtained from various sources in real-time. SIEM is a combination of Information Security Management and security event management systems into a single security management system. The results of the analysis carried out by SIEM are presented in a single interface, accessible to security analysts. This also facilitates the study of the corresponding characteristic features of security events and allows analyzing the events that occur in order to respond to security threats in real-time (Fig. 3). Sources of information for SIEM systems can be antivirus programs, authorization and authentication systems, network screens, security walls, logs of network equipment, servers and workstations, intrusion detection and prevention systems (IDS / IPS), information leakage prevention systems (DLP) and other programs [11].

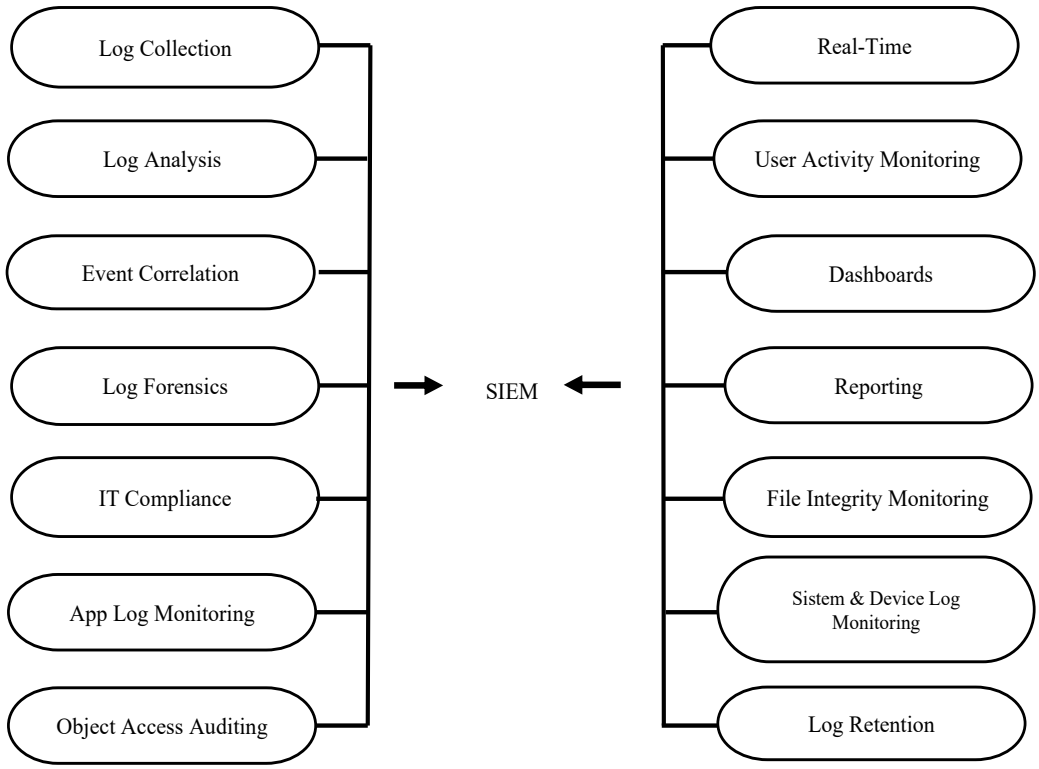

Fig. 3. Security Information and Event Management

UBA (User Behavioral Analytics) – systems that collect and analyze all behaviors, including managed data, used to manage fraudulent activities at the expense of financial threats with internal threats [12].

UEBA (User and Entity Behavioral Analytics) – systems aimed at searching for and detecting anomalies in the behavior of users and various systems. A class of behavioral analysis systems has been established because companies use many different data collection systems to ensure information security. At the same time, employees are not always able to review all the information received and respond to potential events in a timely manner. UEBA systems increase efficiency by compiling profiles and ensuring timely response to possible data leaks [13].

Employee monitoring and time recording systems are systems that allow the organization to analyze the activities of employees and monitor the use of working time in the workplace, as well as control business processes, solve several tasks related to confidential information leaks, and further investigate of incidents [14].

Different types of attack detection and detection systems are aimed at improving the overall protection of the corporate network [14].

The architecture of the decision support system in information security monitoring systems

To ensure the efficiency of decision-making is necessary in order to quickly respond to security breaches and incidents in information security monitoring systems. In order to support decision-makers and improve analytical activities in this area, the development of a system that supports decision-making in information security monitoring systems is proposed.

A decision support system is a computer system that allows decision-makers to make more reasonable and correct decisions based on analytical recommendations provided to them. The decision support system can be created on the basis of various technologies, including OLAP (Online Analytical Processing) and Data Warehouse (DW) (Fig. 4.) [15]. The OLAP concept was described in 1993 by Edgar Codd, a well-known database researcher and author of the relational data model. OLAP is a key component of the database. This is a technology that collects, stores, and analyzes multidimensional data. Performs multidimensional, operational, and analytical data processing in real-time. For the preparation of reports, the construction of forecast scenarios, and statistical calculations based on large information systems with a complex structure are intended [16]. Through OLAP technology, the original data is converted into information that can be used for decision-making. We can visualize the results of the analysis and present the data in the form of graphs.

A warehouse is a place where all analytical information is collected for decision-making. ETL (Extract, Transform, Load) is a three-step process called extraction, conversion, and loading that collects data from multiple sources in a single parent repository.

- Extraction - extraction of data from external sources in an understandable format;
- Transformation - the conversion of primary data into suitable structures for the establishment of an analytical system;
- Loading - uploading data to the warehouse.ETL processing is usually done by software, but can also be done manually by system operators. Unnecessary data is cleaned up on the basis of statistical or expert methods [17].

Figure 4 presents the architectural-technological model of the system that supports decision-making for IMS.

At the first level, data sources are identified for ISM. The source of the data can be CERTs created within an organization, a region, a country, network antiviruses, OS logs, security scanners, network equipment, and so on.

At the second level, the process of collecting primary data from various sources should be carried out for the ISM system. Data can be collected from sources within an organization, a region, or a country. Data collection can be done with agent programs, without agents, questionnaires (paper or electronic), or software. To ensure the high quality of the data before it falls into a single Database, this may be necessary to clean it and delete unnecessary data. Therefore, in the intermediate stage, during the transition to the third level, the data enters the field of data purification, and the ETL process is carried out as an intermediate stage.

Depending on the issue set at the third level, data on security incidents collected from sources within an organization, region, or country by means of data collection methods (one or some of them may be) is collected in the form of a separate database (DB) in one DW. Based on the data collected in each DB, reports are prepared for analysis using OLAP technology.

On the fourth level, reports prepared for analysis on the basis of a separate database are collected in DW. OLAP technology prepares reports for analysis by decision-makers on surveys sent to the data warehouse. Analysis of security incidents collected from different sources within one organization, one region, or one country allow to determine and assess the state of information security within an organization, one region, or one country, and to identify the sources of threats.

Conclusion and Future Scope

The rapid development of the global Internet and ICT, and the impact on all areas of human activity, raises the information security problem in CNs. The article analyzes ISM systems rapidly to detect cyber threats and respond quickly to possible incidents for CNs to operate smoothly and reliably. Sources of primary data for ISM systems were investigated, and categories of ISM systems were analyzed. As a result of the analysis, to en-

sure the speed of decision-making for rapid response to security breaches and incidents was determined. In order to support decision-makers and improve analytical activities in this area, a system has been developed to support OLAP and data warehouse decision-making in ISM systems.

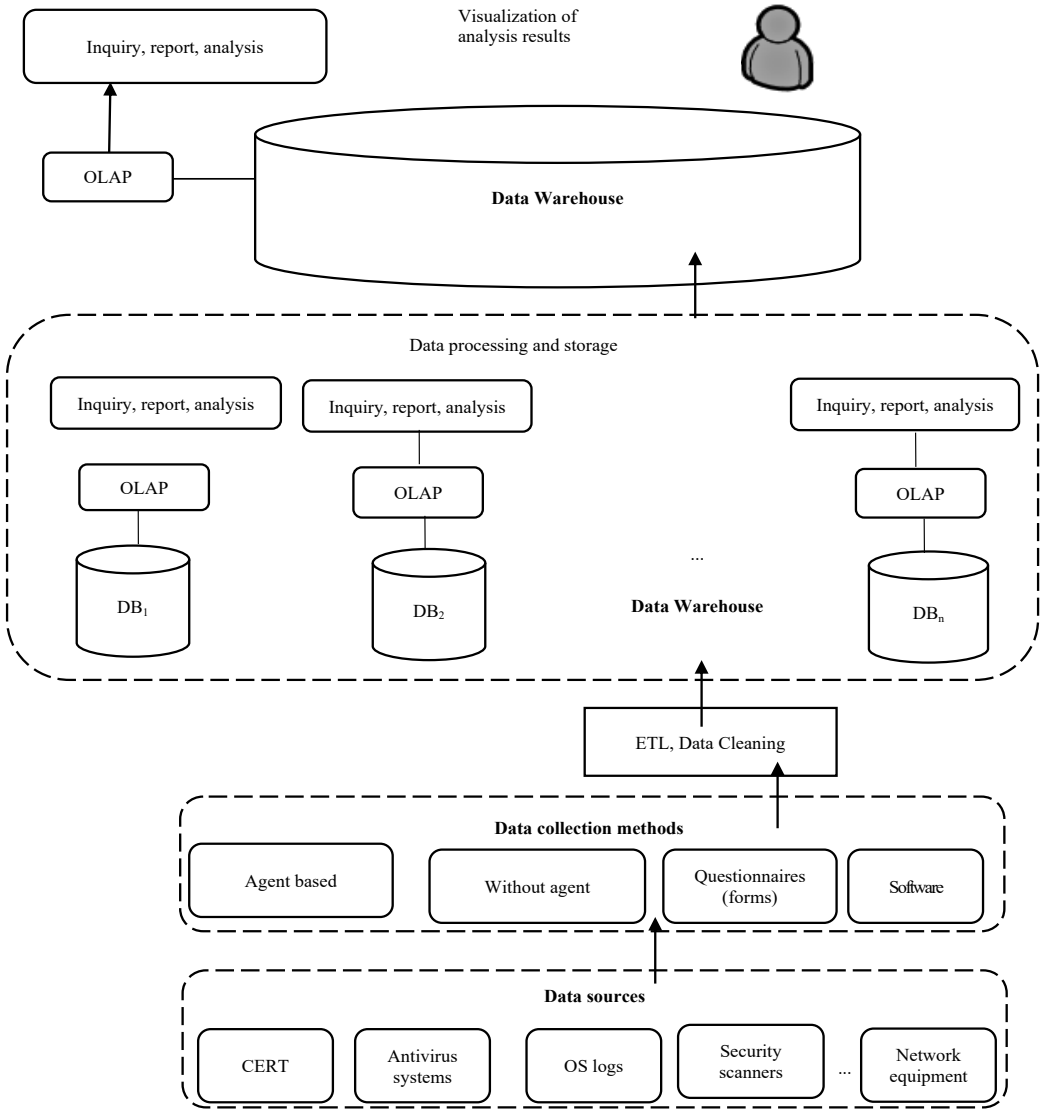

Fig. 4. Architectural-technological model of Decision Support System for ISM systems

References

1. GRAHAM D. (2010). Cyber threats and the law of war. J. Nat'l Sec. L. & Pol'y T. 4. P. 87.
2. ALGULIEV R. et al. (2014). Analysis of methods for network security monitoring. Problems of Information Technology. P. 60-68.
3. MUZALEVSKIY F. Information security monitoring. (in Russian). Available from: https://rtmtech.ru/articles/monitoring-informatsionnoj-bezopasnosti. [Accessed 14/04/2022].
4. LITTLEWORT G. et al. (2011). The computer expression recognition toolbox (CERT). IEEE International Conference on Automatic Face & Gesture Recognition (FG). IEEE. P. 298-305.
5. Software Engineering Institute. Available from: https://www.sei.cmu.edu/about/divisions/cert/index.cfm [Accessed 04/03/2020].
6. YAZOV YU. K. & SOLOVYOV S. V. (2015). Protection of information in information systems from unauthorized access. Kvarta. P. 357-440. (in Russian)
7. BARRINGER H. et al. (2010). Formal analysis of log files. Journal of aerospace computing, information, and communication. T. 7. No. 11. P. 365-390.
8. HOLM H. (2012). Performance of automated network vulnerability scanning at remediating security issues. Computers & Security. T. 3. No. 2. P. 164-175.
9. CôRTES H. & SANTOS P. & DA SILVA. & FILHO J. I. (2022). Monitoring electrical systems data-network equipment by means of Fuzzy and Paraconsistent Annotated Logic. Expert Systems with Applications. P. 115865.
10. LETHBRIDGE T. C. & SIM S. E. & Singer J. (2005). Studying software engineers: Data collection techniques for software field studies. Empirical software engineering. T. 10. No. 3. P. 311-341.
11. KARLZEN H. (2009). An Analysis of Security Information and Event Management Systems: The Use of SIEMs for Log Collection. Management. and Analysis. P. 45
12. BERNASCHINA C. et al. A big data analysis framework for model-based web user behavior analytics. International Conference on Web Engineering. Springer. Cham. P. 98-114.
13. SHASHANKA M. & SHEN M. Y. & WANG J. (2016). User and entity behavior analytics for enterprise security. IEEE International Conference on Big Data (Big Data). IEEE. P. 1867-1874.

14. KUFEL L. (2012). Security event monitoring in a distributed systems environment. IEEE security & privacy. T. 11. No. 1. P. 36-43.
15. CODD E. F. & CODD S. B. & SALLEY C. T. (1993). Providing Olap. On-line Analytical Processing to User-Analists: An IT Mandate. Associates. T. 19.
16. KRZYSZTOF. J. CIOS. (2007). Data Mining: A Knowledge Discovery Approach. Springer. P. 123.
17. NABIBAYOVA G. (2011). About an application of OLAP-technology in decision making support systems. 5th International Conference on Application of Information and Communication Technologies (AICT). IEEE. P. 1-4.

Received 17.07.2022

About the authors:

Dashdamirova Konul Qadim
PhD student and senior researcher
Institute of Information Technologies
Azerbaijan National Academy of Science
senior research associate.
Publications in foreign journals – 4
http://orcid.org/0000-0003-0365-6139

Place of work:

Institute of Information Technologies
Azerbaijan National Academy of Science
Azerbaijan Republic, Baku, B.Vahabzade str., 9A
Phone: (994 12) 539 01 67
E-mail: konulahmed@gmail.com

Прізвища та ініціали авторів і назва доповіді англійською мовою:
K.Q. Dashdamirova
Development of decision support system using
OLAP-technologies for information security
monitoring systems

Прізвища та ініціали авторів і назва доповіді українською мовою:
К.К. Дашдамірова
Розвиток системи підтримки рішень з використанням
OLAP-технологій для системи моніторингу інформаційної безпеки