Methodology of Rational Choice of Security Incident Management System for Building Operational Security Center

© Igor Subach[0000-0002-9344-713X], © Volodymyr Kubrak[0000-0001-8877-5289] and © Artem Mykytiuk[0000-0002-8307-9978]

Institute of Special Communications and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Ukraine
igor_subach@ukr.net

Abstract. This article discusses the purpose, tasks and composition of the Operational Security Center (SOC). The basic technological tools which should include modern effective SOC are indicated. The focus is on the key role of the Information Security Incident Management System (SIEM) in the SOC. The purpose of SIEM and the main tasks that it should solve are reviewed. The peculiarities of solving the problem of choosing of SIEM are analyzed. The groups of indicators that characterize the degree of fulfillment of the requirements to SIEM are highlighted. The application of fuzzy set theory for processing expert information on qualitative indicators characterizing SIEM is proposed. The formulation of the SIEM selection problem is done and the main stages of its solution are proposed: preparation of initial data; choosing the method of solving the multicriteria problem; algorithm development. The method of normalization of SIEM quantitative indicators and the method of paired comparison based on the rank estimates for processing of SIEM qualitative indicators are proposed. It is proposed to use the 9-point Saaty scale to derive functions of SIEM qualitative values based on the processing of expert assessments. The algorithm of the considered method is implemented. Methods for solving multicriteria problems are analyzed and the use of a lexographic method is proposed for solving the SIEM solution for the Security Center (SOC). An algorithm for its implementation has been developed. To illustrate the operation of the proposed algorithm, we give an example of how to apply it to choose a rational SIEM option. Recommendations for application of the results obtained are offered.

Keywords: cybersecurity, Information Security Incident Management System, Operational Security Center, lexographic method, fuzzy sets theory.

1 Introduction

It is impossible to counteract the modern cyber threats without the use of modern cybersecurity technologies that enable monitoring, collection, collation and processing of information in order to identify existing and predict future threats. Important role is

given to the special units that deal with information and cyber security issues at the organizational and technical level – the Security Operation Centers (SOC).

Modern SOC solves the following tasks [1]:

taking immediate actions to protect against cyberattacks and minimize their damage;

identification of system security vulnerabilities and taking actions to eliminate them;

centralized security management of various devices in the system;

continuous monitoring of system threats status;

technical support for cyber security of the system and others.

Structurally, the SOC has three main components: personnel – skilled professionals using modern cybersecurity technologies with teamwork and management competencies; processes – business processes, technological processes, operational and analytical processes; technologies – tools for detecting, counteracting and preventing cyber threats.

Effective SOC should include the following modern technological tools to ensure cyber security [2]: Next Generation Firewall, Intrusion Prevention System (IPS), Web Application Firewall (WAF), Database Protection, Email Security, Endpoint Detection and Response, Vulnerability Scanners, Data Loss Prevention, Forensics, Network Access Control and others.

However, the basis for building an effective SOC is the use of the SIEM system (Security Information and Event Management) – a system for managing information and security events. The use of SIEM in protection system enables proactive management of cyber incidents. That is, to predict future events that will occur in the system by applying automated mechanisms that use information about events that have already occurred in the system, as well as to adapt the protection settings of the system to its current state, thereby implementing preventive measures even before the situation in the system becomes critical [2]. In accordance with this, SIEM system should solve a range of tasks which include [3]:

collection, processing and analysis of security events coming from a variety of heterogeneous distributed sources;

detection of real-time or close cyber attacks and violations of security policies;

investigation of cyber incidents;

developing effective solutions for cyber security;

generation of reporting documents and visualization of system status and others.

In order to solve these problems, the SIEM-system, on the basis of the initial data collected from the log files which accumulate information about the events that occur in the system, selects those events that may be a sign of cyber attacks or other undesirable actions in the system.

The main feature of the solution to the problem of choosing a SIEM-system for building SOC is a large number of indicators that characterize the degree of fulfillment the requirements for systems of this type which can be both quantitative and qualitative. Qualitative indicators, first of all, include those that characterize how effectively the

SIEM system can be used to solve the functional tasks entrusted to it by the SOC; what will be the cost of purchasing and using the system; how reliable it is and easy to operate, etc.

Analysis of recent publications [4-11] showed that these figures can be represented as follows:

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}\},$$

where x_1 – event source support;

x_2 – event collection;

x_3 – correlation;

x_4 – search and analytics;

x_5 – visualization and reporting;

x_6 – prioritization and notification;

x_7 – general settings and installed;

x_8 – scalability, fault tolerance, storing;

x_9 – system component monitoring and internal audit;

x_{10} – ease of use;

x_{11} – availability of state certificates of conformity;

x_{12} – additional system modules;

x_{13} – cost.

Therefore, the problem of rational selection of SIEM-system for building the SOC is characterized by multicriteria and the need to consider a large number of qualitative and quantitative indicators.

In its turn, the first characteristic requires the use of an effective method of solving multicriteria problems, and the second – the application of fuzzy set theory for the processing of expert information on qualitative indicators [12, 13].

2 The problem of rational choice of SIEM

The general statement of the problem of rational choice of SIEM-system can be described as follows.

It is necessary to find

$$S_0 = \arg \underset{s \in S}{opt} W\left(\overline{X}(s)\right), \quad (1)$$

where W – some generalized indicator of system quality;

S – a set of possible system choices;

$\overline{X}(s)=|x_1(s),x_2(s),\ldots,x_k(s),x_{k+1}(s),\ldots,x_n(s)|$ – vector of SIEM quality indicators, besides first k ($i=\overline{1,k}$) requirements are quantitative, and the other n-k $k=\overline{k+1,n}$ – qualitative.

The value of the partial indicator i, which characterizes the degree of fulfillment the SIEM requirement i, is determined by its approximation to the optimal value.

The main stages in solving the task (1) are: preparing initial data; choosing a method for solving a multicriteria problem; algorithm development.

3 The method of solving the problem

It is advisable to use normalized values to estimate the degree of proximity of the quantitative indicator i to the optimal value for j variant of the SIEM. $x_{ij}, i=\overline{1,k}; j=\overline{1,k}; 0\le x_{ij}\le 1.$

Normalization of the value of a quantitative indicator can be made as follows:

$$x_{ij}=\frac{x_{ij}-x_{ij}^{*}}{x_{ij}^{**}-x_{ij}^{*}}, \tag{2}$$

where x_{ij} – the value of indicator i for j variant of the system;

x_{ij}^{*}, x_{ij}^{**} – the worst and the best indicator value.

Accordingly, the degree of proximity of the quality indicator i to the optimal value for the j variant of the SIEM can be determined using the membership function $\mu_S(x_i)$. To build a membership function $\mu_S(x_i)$ it is advisable to use a rank-based method or pairwise ranking method [14, 15].

In this case, the rank of an element $x_i \in X$ refers to a number $r_s(x_i)$ that characterizes its importance in the formation of the SIEM property which is described by a fuzzy term S. Suppose that the greater the rank of an indicator, the greater the value of its membership function.

If you introduce the following figures

$$r_S(x_i)=r_i, \mu_S(x_i)=\mu_i; i=\overline{1,n},$$

then the distribution of membership degrees can be represented as follows:

$$\frac{\mu_1}{r_1}=\frac{\mu_2}{r_2}=\ldots\frac{\mu_n}{r_n}, \tag{3}$$

in case of normalization:

$$\mu_1 + \mu_2 + \ldots + \mu_n = 1. \tag{4}$$

On the basis of (3), the membership degree of all elements of the set is determined by the membership degree of the so-called supporting member.

For supporting member $x_1 \in X$ that has a membership function μ_1:

$$\mu_2 = \frac{r_2}{r_1} \cdot \mu_1;\ \mu_3 = \frac{r_3}{r_1} \cdot \mu_1;\ \ldots;\ \mu_n = \frac{r_n}{r_1} \cdot \mu_1; \tag{5}$$

For supporting member $x_2 \in X$ that has a membership function μ_2:

$$\mu_2 = \frac{r_1}{r_2} \cdot \mu_2;\ \mu_3 = \frac{r_3}{r_2} \cdot \mu_2;\ \ldots;\ \mu_n = \frac{r_n}{r_2} \cdot \mu_2; \tag{6}$$

Accordingly, for supporting member $x_n \in X$, that has a membership function μ_n:

$$\mu_n = \frac{r_1}{r_n} \cdot \mu_n;\ \mu_2 = \frac{r_2}{r_n} \cdot \mu_n;\ \ldots;\ \mu_{n-1} = \frac{r_{n-1}}{r_n} \cdot \mu_n; \tag{7}$$

From (5-7) and in case of normalization (4) we obtain:

$$\begin{cases} \mu_1 = \left(1 + \frac{r_2}{r_1} + \frac{r_3}{r_1} + \ldots + \frac{r_n}{r_1}\right)^{-1} \\ \mu_2 = \left(\frac{r_1}{r_2} + 1 + \frac{r_3}{r_2} + \ldots + \frac{r_n}{r_2}\right)^{-1} \\ \ldots \\ \mu_n = \left(\frac{r_1}{r_n} + \frac{r_2}{r_n} + \frac{r_3}{r_n} + \ldots + 1\right)^{-1} \end{cases} \tag{8}$$

On the basis of (8), it is possible to calculate the membership degrees $\mu_s(x_i)$ on the relative estimates of the ranks $\frac{r_i}{r_j} = \xi_{ij}, i, j = \overline{1,n},$ which create the following matrix:

$$\Xi = \begin{bmatrix} 1 & \frac{r_2}{r_1} & \frac{r_3}{r_1} & \cdots & \frac{r_n}{r_1} \\ \frac{r_1}{r_2} & 1 & \frac{r_3}{r_2} & \cdots & \frac{r_n}{r_2} \\ \cdots & \cdots & \cdots & \cdots & \vdots \\ \frac{r_1}{r_n} & \frac{r_2}{r_n} & \frac{r_3}{r_n} & \cdots & 1 \end{bmatrix} \quad (9)$$

It is easy to see that the properties of the matrix (9) are the following: it is diagonal, transitive, and elements of the matrix that are symmetric about the main diagonal are connected by dependence relation: $\xi_{ij} = 1/\xi_{ji}$.

Since matrix (9) is a matrix of paired comparison of the element ranks, a 9-point Saaty scale can be used for expert evaluation of its elements: $\xi_{ij} = r_i / r_j$ (Table 1).

Table 1. Relative Importance Scale

Intensity of relative importance	Definition
1	Equal importance of compared requirements
3	Weak importance of one over another
5	Strong importance
7	Demonstrated importance
9	Absolute importance
2,4,6,8	Intermediate values between the two adjacent judgments

Thus, using (8), the expert data on element ranks (their paired comparison) are transformed into a fuzzy term membership function.

The algorithm for constructing the membership function includes the following steps.

1. Set a linguistic variable (qualitative characteristic of SIEM).
2. Determine the universal set on which the linguistic variable is set (the value of the qualitative characteristic of SIEM).
3. Set a variety of fuzzy terms $\{S_1, S_2, \ldots, S_n\}$ that are used to evaluate the variable set in the first step.
4. Form a matrix (9) for each term $S_j, j = \overline{1,m}$.
5. Using the formulas (8) calculate the membership functions of the elements (SIEM characteristics) for each fuzzy term.
6. The procedure for the normalization of the received membership functions should be carried out by dividing them by the largest value of the membership function.

The most common methods for solving a multicriteria problem (1) are the following [16]: the principal indicator method, generalized additive/multiplicative indicator method, generalized minimax indicator method and lexographic method. The analysis shows that they all have their pros and cons, and the choice of a method is largely determined by the completeness and credibility of the expert knowledge of the importance and degree of interrelation of partial quality indicators. Since lexographic method is the least demanding for expert information about the degree of preference for partial indicators, it is advisable to choose the lexographic method in order to solve the problem of rational choice of SIEM-system for building the SOC. The essence of use of this method is the following.

At the previous stage of solving the task it is possible to find a set of "good solutions" (Pareto-optimal solutions) by consistently comparing possible SIEM options for all quality indicators. [17, 18, 19].

Further, all the partial indicators are ordered by importance. Then the set of alternatives with the best score by the most important indicator is outlined. When such an alternative is the only one it is considered to be the best. Otherwise, when several alternatives are obtained, they are distinguished by those that have a better rating on another indicator and so on. Thus, the algorithm for implementing the lexographic method for solving the problem of rational choice of the system consists of the following steps.

1. Partial quality indicators are ranked by importance:

$$x_1(s) > x_2(s) > \ldots > x_n(s)$$

2. For each indicator the value of permissible concession is determined $\Delta x_i, i = \overline{1,n},$ within which the compared SIEM variants are considered to be equivalent;

3. For the first indicator $x_1(s)$ a set Ψ_1 of equivalent SIEM variants is formed which meets the following condition:

$$\max\left(x_{1j} - x_{1k}\right) \le \Delta x_1, j = \overline{1,m}\,; k = \overline{1,m}; k \ne j. \tag{10}$$

4. If the set contains only one variant, it is considered to be the best. Otherwise, when it contains more than one alternative, you need consider all variants of the set by indicator $x_2(s)$.

5. For the second indicator $x_2(s)$, from a set of variants Ψ_1, a set of variants Ψ_2 is formed which meet the condition:

$$\max\left(x_{2j} - x_{2k}\right) \le \Delta x_2, i \in \Psi_1\,; k \in \Psi_1\,; k \ne j. \tag{11}$$

6. If the set Ψ_2 contains one variant, it is considered to be the best. Otherwise, found variants are considered by indicator $x_3(s)$ and so on.

7. In the case where all indicators are consistently reviewed and a set $\Psi = \Psi_1 \times \Psi_2 \times \ldots \times \Psi_n,$ containing more than one alternative is obtained, there are two options: reduce the value of the permissible concession $\Delta x_i, i = \overline{1,n},$ from the first most important indicator and repeat the algorithm from the beginning or allow the decision maker to choose the best option.

To illustrate the proposed algorithm in work we give an example of its application to the selection of a rational variant of the SIEM system.

To select a SIEM system, we use four partial indicators: $x_1(s)$ – cost and $x_2(s)$ – event source support which are quantitative indicators, as well as $\mu_{x_3}(s)$ – scalability and $\mu_{x_4}(s)$ – ease to use which are qualitative indicators.

Five options for choosing a SIEM system $s_j, j = \overline{1,5}$ have been selected for consideration.

As a result of the calculations and expert assessments, the following data were obtained characterizing the degree of SIEM compliance with the specified requirements:

$$x_1 = \left\{ \frac{0,8}{s_1}; \frac{0,8}{s_2}; \frac{0,7}{s_3}; \frac{0,5}{s_4}; \frac{0,6}{s_5} \right\};$$

$$x_2 = \left\{ \frac{0,7}{s_1}; \frac{0,8}{s_2}; \frac{0,6}{s_3}; \frac{0,7}{s_4}; \frac{0,8}{s_5} \right\};$$

$$x_3 = \left\{ \frac{0,4}{s_1}; \frac{0,6}{s_2}; \frac{0,7}{s_3}; \frac{0,8}{s_4}; \frac{0,7}{s_5} \right\};$$

$$x_4 = \left\{ \frac{0,5}{s_1}; \frac{0,6}{s_2}; \frac{0,5}{s_3}; \frac{0,6}{s_4}; \frac{0,3}{s_5} \right\}.$$

1. Indicators are ranked by importance as follows:

$$x_1 > x_2 > \mu_S(x_3) > \mu_s(x_4).$$

2. The value of permissible concession $\Delta x_i = 0,1,\ i = \overline{1,4}.$

3. With the maximum value of the first indicator $x_1 = 0,8$ and the value of permissible concession $\Delta x_1 = 0,1$ to the set Ψ_1 of equal variants for SIEM, which meet the condition (2) the following variants are included:

$$\Psi_1 = \{S_1, S_2, S_3\}.$$

4. Of the set Ψ_1, by the second indicator x_2 meeting the condition (3): $x_2 = 0{,}8$ and $\Delta x_2 = 0{,}1$ to the set Ψ_2 the following variants are included:

$$\Psi_2 = \{S_1, S_2\}.$$

5. Of the set of variants: $\Psi = \Psi_1 \times \Psi_2$ for the third indicator x_3 meeting the condition (3) $x_3 = 0{,}6$ and $\Delta x_3 = 0{,}1$ to the set Ψ_3 the following variants are included:

$$\Psi_3 = \{S_2\}.$$

A rational choice of SIEM for building a SOC is the second option.

4 Conclusion

The conducted research shows that the lexographic method is an effective method for solving the multicriteria problem of SIEM selection for SOC. Groups of quantitative and qualitative indicators characterizing the requirements for SIEM in the SOC are formulated. Methods of processing quantitative and qualitative indicators of SIEM are offered. The expedience of applying the procedure for rationing quantitative indicators of SIEM and applying the method of paired comparison based on rank evaluations for processing its qualitative indicators is justified. The formulation of the SIEM selection problem is done and the main stages of its solution are outlined. An algorithm for the implementation of the lexographic method is developed and brought to practical implementation.

The results obtained can be used in practice to solve the problems of creating SOC and rational choice of its software such as SIEM.

References

1. KG, Vogel Business Media GmbH & Co. Was ist ein Security Operations Center (SOC)? – https://www.security-insider.de/was-ist-ein-security-operations-center-soc-a-617980/, , last accessed 22.06.19.
2. Laskin S. How to build a competent, scalable and effective information security management center / LAN Network Solutions Magazine. – https://www.osp.ru/lan/2017/04/13051902/, last accessed 28.03.2019.

3. Kotenko I.V., Voroncov V.V., Chechulin A.A., Ulanov A.V.: Proactive security mechanisms against network worms: approach, implementation and results of the experiments. Information Technology. Vol. 1, pp. 37-42. (2009).
4. Kotenko I., Saenko I., Polubelova O., Chechulin A.: Application of security information and event management technology for information security in critical infrastructures / SPIIRAS Proceeding, ISSN: 2078-9181. Issue 1(20). pp. 27–56. (2012).
5. Paley L. Comparison of SIEM systems. Part 1. – https://www.anti-alware.ru/compare/SIEM-systems, last accessed 07/04/2018.
6. Paley L. Comparison of SIEM systems. Part 2. – https://www.anti-alware.ru/compare/SIEM-systems-part2, 1/16, last accessed 08/05/2019.
7. Niyazov T. Comparison of SIEM solutions for building SOC, https://www.jetinfo.ru/stati/sravnenie-siem-reshenij-dlya-postroeniya-soc, last accessed 08/05/2019.
8. Comparison of SIEM systems, https://www.siem.su/compare_SIEM_systems.php, last accessed 08/05/2019.
9. Donskoy K.A., Levin L.S., Trushin V.A.: SIEM overview on the Russian market / Collection of scientific works of NSTU. No. 3 (89). pp. 124–132. (2017).
10. SIEM product comparison – https://comminity.softwaregrp.com/dcvta86296, last accessed 10/18/2019.
11. SIEM competitive comparision – https://www.securonix.com/products/competitive-comparison, last accessed 10/18/2019.
12. Boehm B., Brown J., Caspar H. et al.: Characteristics of software quality / [Translated from English]. – Moscow: Mir. – 208 p. (1981).
13. Borisov A.N., Krumberg O.A., Fedorov I.P.: Decision making based on fuzzy models: examples of use / Riga: Zinatne. 184 p. (1990).
14. Zaichenko Y.P.: Operations Research: Fuzzy Optimization. – Kiev: High school. 191 p. (1991).
15. Rothstein A.P.: Intelligent identification technologies: fuzzy sets, genetic algorithms, neural networks. – Vinnytsia: UNIVERSUM. – 320 p. (1999).
16. Gerasimov B.M., Divizinyuk M.M., Subach I.Y.: Decision support systems: design, application, performance evaluation / Monograph. – Sevastopol: Publishing Center SNIYE and P. – 320 p. (2004).
17. Tutkin L.S.: Optimization of electronic devices according to a set of quality indicators / Moscow: Radio and communications,. – 367 p. (1975).
18. Podinovsky V.V., Gavrilov V.M.: Optimization according to successively applied criteria / Moscow: Soviet Radio,. – 234 p. (1975).
19. Podinovsky V.V., Nogin V.D.: Pareto-optimal solutions to multicriteria problems / Moscow: Science, Main edition of the physical and mathematical literature, – 256 p. (1982).