A Multi-Attribute Approach for Cyber Threat Intelligence Product and Services Selection

Adrian Victor VEVERA, Carmen Elena CÎRNU, Constanta Zoie RADULESCU*

National Institute for Research and Development in Informatics – ICI Bucharest,
8-10 Mareşal Averescu Avenue, 011455, Bucharest, Romania
victor.vevera@ici.ro, carmen.cirnu@ici.ro, zoie.radulescu@ici.ro (**Corresponding author*)

Abstract: Cyber Threat Intelligence (CTI) is a significant field in Cyber Security research. It enables organizations to share threat data and allow a proactive defence against sophisticated intrusion attempts. The wide variety in the CTI products and services offered by different providers from the market, makes it difficult for the security experts to decide which CTI provider is the most suitable according to their security program requirements. CTI products and services provider selection is a complex decision-making problem that involves multiple criteria. The aim of the present paper is to propose a multi-attribute approach based on the VIKOR method for CTI providers ranking and selection, according to a set of criteria. A case study based on the users' evaluations reviews about the security threats intelligence providers is studied. The impact of the VIKOR user parameter variation on the CTI providers ranking is analysed. The proposed approach is a support tool for the security program leaders faced with the decision of selecting the CTI providers. It also helps the CTI service providers to improve the quality of their products and services.

Keywords: Cyber Threat Intelligence, Threats, Multi-attribute approach, VIKOR method, Security threat intelligence providers, CTI providers selection.

1. Introduction

The evolution of digital technologies and their use is radically transforming our lives. In an age of interconnected societies "security issues" call for attention to new forms of threats induced by computer networks. Cyber threats continue to evolve rapidly around the world, with the frequency and intensity of cyber scams, crimes and the number of data breaches increasing every year. This situation caused huge losses for businesses, public institutions etc. A risk-based security report found that in the first nine months of 2019 about 7.9 billion pieces of data were exposed to cyber-attacks. These figures represent more than double (112%) the amount of data exposed during the same period in 2018 (Risk based Security, 2021).

In 2020 the global cyber security market size was valued at USD 167.13 billion. In the period from 2021 to 2028 it is expected to grow from USD 180.33 billion in 2021 to USD 372.04 billion by 2028, recording a Compound Annual Growth Rate (CAGR) of 10.9% (MarketResearch, 2021). The growth of the market can be attributed to the growing sophistication of cyberattacks. Businesses worldwide had increased the spending on advanced information security technologies in order to improve their in-house security infrastructure.

Cyber Threat Report CEE report stated that Romania's region has a dynamic market for cybersecurity products and services that is much stronger than the rest of Europe (Kosciuszko Institute, 2018; Vevera, Georgescu & Cirnu, 2021). Romania is on the 24th place in the world according to National Cyber Security Index, 62th according to Global Cybersecurity Index, 58th according to ICT Development Index and 49th according to Networked Readiness Index (e-Governance Academy, 2021).

Due to the Covid-19 pandemic, a growing attention has been paid to health and the economic challenges posed by the new global conjuncture. During the Covid-19 pandemic the number of cyber-attacks has increased. This made companies to face new security threats. As a result, new cyber-security solutions are needed.

Any valuable information that can be used to identify, characterize or assist organizations in the response to cyber threats is commonly referred to as Cyber Threat Information. The analysis of this type of information can produce intelligence that may be used to inform companies about threats to their system. The market growth was stimulated by the increasing adoption by companies of threat intelligence security services and products to detect cyber threats and future vulnerabilities that might occur in their cyber systems.

In the market there are several cyber-security providers that are offering a large variety of CTI services and capabilities to their customers. The wide variety in the CTI service offered by different providers makes it difficult for the security experts to decide which service provider is the most suitable according to their security program requirements. The CTI customers have different cyber threats

https://doi.org/10.24846/v31i1y202202

profiles that belong to various domains: financial industry, healthcare, defence agencies, etc.

CTI products and services providers ranking and selection is a complex decision-making problem that involves multiple criteria. Thus, this problem is a multi-criteria one. When the number of alternatives is finite, the multi-criteria problem becomes a multi-attribute problem.

The aim of the present paper is to provide a multi-attribute approach for CTI services and products providers, ranking and selection. This approach is based on the VIKOR decision making method. An introduction to the field of CTI is made in the second section. In the third section a brief CTI literature review is presented. The fourth section is dedicated to the presentation of the multi-attribute approach based on VIKOR method for CTI providers selection. An implementation of this approach is realized for 17 CTI services and products providers, in the fifth section. An analysis on the rankings for variation of the VIKOR user parameter is performed. The paper ends with the conclusion section.

2. Cyber Threat Intelligence

Last decades witnessed an exponential rise in the number and sophistication of cyber-attacks.

In the last decade, CTI has become a hot topic in Information Security (IS). It is a discipline related to cyber security. The field of CTI is continuing to grow at a fast rate. Several works have been dedicated to the CTI field. They include whitepapers, advisories and scientific papers written by experts from cyber security companies, academic circles and professional bodies.

There are many different definitions that try to explain the term CTI. A simple definition of the CTI term is that it denotes the information gathered from a set of sources about current or potential attacks against an organization. The information is analysed, refined and organized and then used to minimize and mitigate cyber security risks.

A more complex definition is given in (Qiang et al., 2016): “CTI denotes the evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging threat that can be used to inform decisions regarding the subject’s response to that menace or hazard”. From the previous definition it follows that organizations can decide their action at the strategic, operational and tactical levels by using the collection of information that contain the details of current and emerging threat.

CTI enables organizations to share threat data and allow a proactive defence against sophisticated intrusion attempts. Some examples of cyber threats according to Open Threat Taxonomy and European Union Agency for Network and Information Security (ENISA) are cf. (Noor et al., 2020): Malware, Web Based Attacks, Phishing, Spam, Data Breaches, Ransomware, Advanced Persistent Threat, Manipulation /damage /theft / loss, Denial of Service, Botnets, Exploit Kits, Insider Threat, Information Leakage and Web Application Attacks.

Current approaches for ranking CTI service providers are based on a limited set of Key Performance Indicators (KPI) and do not take into account the customer’s security program relevance and requirements.

The use of CTI requires the collection of a massive amount of data. That is why in order to effectively use the cyber threats information new automated systems were developed. These systems have the ability to manage a vast amount of data, analyse, evaluate and classify the information, provide sophisticated defence capabilities and respond to incidents in real-time. They were commonly referred to as Threat Intelligence (TI) platforms. According to (Shin & Lowry, 2020) these platforms should include automatic processes of data transformation and intelligence production in order to ensure an efficient, proactive and timely defence model.

3. CTI – Literature Review

A very good survey about CTI can be found in (Abu et al., 2018).

In (Noor et al., 2020), an extensive set of KPI is defined. Based on the customer’s requirements a set of weights is assigned to KPIs. This allows to obtain a ranking of CTI service providers. The presented framework helps the security program leaders in decision making for CTI service provider selection. As a result, the QoS (Quality of Service) offerings is improved and a correct competition among CTI service providers is promoted.

In (van Niekerk, Ramluckan & Duvenage, 2019) an analysis of a number of publicly available

cyber intelligence and CTI documents (in the form of advisories and whitepapers) was made by using text mining, content analysis, and thematic analysis. These techniques were employed for assessing similarities amongst the documents, identifying common themes and categories and identifying gaps common to these documents.

The paper (Cirnu et al., 2018) proposes measures to mitigate cyber security risks and vulnerabilities in Service-Oriented Architecture (SOA) at business level. Open-source solutions are proposed as tools for enhanced security in SOA.

An exploratory study of software vendors and sharing perspectives was presented in (Sauerwein et al., 2017). After performing a broad literature review the authors of the paper identified 22 threat intelligence sharing platforms, protocols and methods used for sharing CTI.

A comprehensive evaluation methodology of threat intelligence standards and cyber threats intelligence platforms are provided in (de Melo e Silva et al., 2020). In state-of-the-art of the paper the CTI ecosystem and Threat Intelligence standards and platforms were analysed.

The paper (Huang et al., 2020) presents a new approach for detecting APTs (Advanced Persistent Threats) and presents two instances of this approach, implemented in ADONIS (Automating the ATT & CKTM-based Detection Of Novel Network Intrusions System) and CAAPT (Cognitive Agent for APT detection). The approach can reduce the operating costs of cybersecurity operation centers and improves APT detection performance.

In (Saxena & Gayathri, 2021) a Collaborative Cyber Threat Information Exchange system based on artificial intelligence is proposed.

CTI sharing plays an important role in an organization′s cyber security defence. Cyber threats are shared by tools that meet standards such as TAXI and STIX. The paper (Ramsdale, Shiaeles & Kolokotronis, 2020) analyses available standard and public available threat sources and how these standards (formats) are implemented. The analysis concludes that many standards have a low degree of adoption and implementation.

CTI platforms have been widely adopted to protect against cyber-attacks. But the performances of these CTI platforms should be measured in terms of success and efficiency. Theoretical and practical measurements differ with respect to the factors that influence the success of CTI platforms. In the paper (Zibak, Sauerwein & Simpson, 2021) the DeLone and McLean model is applied for sharing information about threats. Factors that are important for the efficiency of a CTI platform have been identified.

A mixed integer programming approach is proposed in (Sawik, 2013), for making decisions on the optimal selection of countermeasures in IT security planning, in order to prevent or mitigate cyber threats. Within a limited budget, the user must decide what countermeasures to implement to minimize potential losses due to cyber-attacks and to mitigate the impact of disruptions caused by IT security incidents. In order to control the risk of large losses due to operational interruptions, the author applies a conditional value at risk approach combined with scenario-based analysis.

The paper (Bhol, Mohanty & Pattnaik, 2021) aims to provide the classification of cyber security metrics. The authors use Multi-Criteria Decision-Making methods for ranking.

To select the “best” set of cyber security measures, the paper (Llansó, McNeil & Noteboom, 2019) analyses the selection based on a set of weighted criteria. The definition of criteria was based on the priorities and restrictions in the organization.

The paper (Neto & dos Santos, 2020) introduced concepts for threat modelling and knowledge discovery in databases focused on high-level threat hunting. The discovered knowledge was used in an experiment in which the efficiency of machine learning and decision-making algorithms for prioritizing hypotheses in the screening phase was evaluated.

4. A Multi-Attribute Approach for CTI Providers Selection

4.1 A Multi-Attribute Approach

For the CTI providers ranking and selection, according to a set of criteria, a multi-attribute approach based on VIKOR method is proposed.

Some examples of multi-attribute methods frequently used in practice are: SAW, TOPSIS, AHP, PROMETHEE and ELECTRE III. Comparing with these methods, the VIKOR multi-criteria method has the avantage of taking into consideration the

compromise between the overall benefit and the maximum individual deviation.

The profile and user requirements are specified. Depending on the profile and user requirements, the set of CTI services and products providers is chosen. This will be the set of alternatives.

There are several specialized platforms with CTI products and services providers on the internet. Some examples of this platforms are Top Threat Intelligence Platforms for 2021 (eSecurityPlanet, 2021), Threat Intelligence Platforms (Trust Radius, 2021), Best Threat Intelligence Services Providers (G2 Deals, 2021), Security Threat Intelligence Products and Services Reviews and Ratings (Gartner, 2021), Top 10 Threat Intelligence Platforms (Enterprise Management 360, 2021), etc. Starting from these platforms, the data collection is built.

The set of evaluation criteria for CTI services and products providers is established. For each criterion the maximum/minimum type, quantitative/qualitative and measure scale is chosen. When a weighting of the criteria is desired, it can be done directly by an expert or a team of experts or it can be done with the help of a weighting method chosen from a set of weighting methods (Radulescu & Radulescu, 2018; Radulescu et al., 2022). In the proposed approach, equal weights for criteria will be considered.

The problem of selecting a set of alternatives according to a set of criteria is a multi-criteria problem (Zavadskas et al., 2019; Zavadskas et al., 2020).

CTI services and products providers are evaluated according to the selected criteria. In order to obtain a ranking of CTI providers, the VIKOR method was chosen. Note that the VIKOR method has proven its efficiency in many fields. By applying this method, a ranking of CTI providers was obtained. Based on this ranking, the decision maker or group of decision makers can make an informed decision to choose the best CTI provider.

4.2 VIKOR Method

VIKOR method is a well-known compromise MADM (Multi-attribute decision making) method developed by Opricovic and Tzeng (Opricovic,1998; Opricovic & Tzeng, 2002). Its name in English is Compromise Ranking Method. The name VIKOR comes from an abbreviation of its Serbian name (Vlse Kriterijumska Optimizacija I Kompromisno Resenje).

The most important difference between VIKOR other MCDM methods like TOPSIS and SAW is the presence of the user parameter θ, called utility weight. The value of θ can be adjusted according the decision-makers preferences.

The method introduces a multicriteria ordering index based on a particular measure of "approximation" to the "ideal" solution. The method considers a set of alternatives and a set of criteria. Each alternative is evaluated according to each criterion. Compromise ordering is achieved by comparing the approximation measure with the ideal alternative. The multicriteria measure for compromise ordering is developed from the L_p metric using an aggregation value (Yu, 1973; Zeleny, 1982).

Applications of the VIKOR method were made in several domains. A systematic review of the VIKOR method applications areas is presented in the paper (Mardani et al., 2016). The important application areas are: Performance Evaluation, Risk and Financial Management, Service Quality, Material Selection, Operation Management, Manufacturing, Construction management, Health-care, Supply Chain, Sustainability and Renewable Energy, Tourism Management, Marketing, Water Resources Planning, Human Resource Management and Other application areas. In a recent paper (Alidrisi, 2021) the VIKOR important application areas are: manufacturing, materiality assessment, construction engineering and management, sustainability, finance, marketing, performance evaluation, and HRM.

Input data in the VIKOR method are:

1. V - the set of m alternatives where $V=\{V_1, V_2,...,V_m\}$, $|V|=m$.

2. C - the set of n criteria where $C=\{C_1,C_2,\ldots C_n\}$, $|C|=n$. A criterion C_i from set C is measured using a measure unit and can be max (benefit) or min (cost) criterion. A weight can be associated for each criterion. The n-dimensional vector of weights is denoted by $\mathbf{w}=(w_j)$. The weights usually have a numerical value in the range (0,1) and $\sum_{j=1}^{n} w_j = 1$. The weight w_j shows the importance of the criterion j.

3. E - is the evaluation matrix where $E=(e_{ij})$, $i=1,2,...,m$; $j=1,2,...,n$. e_{ij} are real numbers and denote the assessment of the i alternative for j criterion.

4. $\theta \in [0.1]$ is a parameter that shows the decision-making strategy between the subjective involvement of experts and the objective evaluation. If $\theta>0.5$ then is "Voting by majority rule". If $\theta=0.5$ then is "by consensus" and if $\theta<0.5$ then is "with a veto".

Below is presented the algorithm of the VIKOR method in following steps (Opricovic & Tzeng, 2002):

Step 1. The following indicators are calculated:

$$e_j^{\max} = \begin{cases} \max\limits_i e_{ij} \text{ if } C_j \text{ is a max criterion} \\ \min\limits_i e_{ij} \text{ if } C_j \text{ is a min criterion} \end{cases} \quad (1)$$

$$e_j^{\min} = \begin{cases} \min\limits_i e_{ij} \text{ if } C_j \text{ is a max criterion} \\ \max\limits_i e_{ij} \text{ if } C_j \text{ is a min criterion} \end{cases} \quad (2)$$

Step 2. The weighted normalized matrix $\overline{E} = \left(\overline{e}_{ij}\right)$ is calculated. Weighted normalization entries of the matrix $\overline{E}$ are computed as follows:

$$\overline{e}_{ij} = w_j \left(e_j^{\max} - e_{ij}\right) / \left(e_j^{\max} - e_j^{\min}\right) \quad (3)$$

Step 3. The L_p metric is:

$$L_{p,i} = \left\{ \sum_{j=1}^{n} \left[\overline{e}_{ij} \right]^p \right\}^{1/p}; 1 \le p \le \infty; i = 1,2,...,m \quad (4)$$

VIKOR method is used for ranking $L_{1,i}$ and $L_{\infty,i}$. The entries of the vectors $S=(S_i)$ and $R=(R_i)$ are calculated as follows:

$$S_i = L_{1,i} = \sum_{j=1}^{n} \left[\overline{e}_{ij} \right], i = 1,2,...,m \quad (5)$$

$$R_i = L_{\infty,i} = \max_{1 \le j \le n} \left\{ \overline{e}_{ij} \right\}, i = 1,2,...,m \quad (6)$$

$L_{1,i}$ represents the overall group benefit and $L_{\infty,i}$ the individual deviation.

Step 4. The following indicators are calculated:

$$S^{\min} = \min_i S_i \; ; S^{\max} = \max_i S_i \quad (7)$$

$$R^{\min} = \min_i R_i \; ; R^{\max} = \max_i R_i \; ; i = 1,2,...,m \quad (8)$$

Step 5. The entries of the vector $Q=(Q_i)$ are calculated as follows:

$$Q_i = \theta \frac{S_i - S^{\min}}{S^{\max} - S^{\min}} + (1-\theta) \frac{R_i - R^{\min}}{R^{\max} - R^{\min}} \quad (9)$$

The choice of parameter $\theta \in [0.1]$ shows the balance between the overall benefit and the maximum individual deviation. Larger values of θ emphasize the group gain, while smaller values of θ emphasize individual deviations.

Step 6. Alternatives ranking. The entries of vectors S, R and Q are ordered in ascending order.

Let α, β, γ be permutations of the set $\{1,2,\ldots,m\}$ such that:

$$Q_{\alpha(1)} \le Q_{\alpha(2)} \le ... \le Q_{\alpha(m)}$$

$$S_{\beta(1)} \le S_{\beta(2)} \le ... \le S_{\beta(m)}$$

$$R_{\gamma(1)} \le R_{\gamma(2)} \le ... \le R_{\gamma(m)}$$

Step 7. The alternative $\alpha(1)$ is the best ranked (corresponds to the minimum value of the entries of vector Q) in the VIKOR method if the following two conditions are fulfilled:

Condition 1. "Acceptable Advantage":

$Q_{\alpha(2)} - Q_{\alpha(1)} \ge \frac{1}{m-1}$ where: the alternative $\alpha(2)$ is the second-best ranked alternative in the arrays of vector Q ranking list.

Condition 2. "Acceptable stability in decision making":

The alternative $\alpha(1)$ must also be the best ranked in the list of arrays of vector S or R, that is

$\alpha(1) = \beta(1)$ or $\alpha(1) = \gamma(1)$.

If one of the above conditions is not satisfied, then a set of compromise solutions is proposed:

- Alternatives $\alpha(1)$ and $\alpha(2)$ are the best if only Condition 2 is not satisfied, or
- Alternatives $\alpha(1), \alpha(2), ..., \alpha(k)$ are the best, if the Condition 1 is not satisfied, and $Q_{\alpha(i)} - Q_{\alpha(1)} \le \frac{1}{m-1}$ for every $i=1,2,...,k$ and $Q_{\alpha(k+1)} - Q_{\alpha(1)} > \frac{1}{m-1}$.

5. Case Study

In the present case study, a set of Security Threat Intelligence Products and Services is considered. The intention is to obtain a ranking of the product and services from the above set with the help of the Multi-Attribute approach based on VIKOR method.

The source of information for building the data collection, for this case study, was the Security Threat Intelligence Products and Services Reviews and Ratings platform (Gartner, 2021). 17 products and services, related to Security Threat Intelligence with more than 10 user reviews, mostly from Europe, were selected.

A classification by the areas involved in the study is presented in Figure 1.

The set V of alternatives has 17 Security Threat Intelligence Products and Services (m=17):

The set C of criteria considered in the evaluation are:

- Number of reviews (C1),
- Number of stars in assessment (C2),
- Evaluation & Contracting (C3),
- Planning & Transition (C4),
- Delivery & Execution (C5).

The measure scale for C2, C3, C4 and C5 is qualitative from 0 to 5. Criteria C1 is quantitative and all criteria are benefit criteria.

The criteria and sub-criteria are presented in Figure 2.

All the criteria weights are considered to be equal, that is:

w=(0.2, 0.2, 0.2, 0.2, 0.2).

The evaluation matrix E with 17 alternatives and 5 criteria is displayed in Table 1.

The vectors $S=(S_i)$ and $R=(R_i)$ are calculated based on equations (5) and (6). Then the ranks of the arrays of vectors R and S are calculated. Based on equations (7), (8) and (9) the vector Q is calculated. The parameter θ is taken to be equal to 0.5. This corresponds to the "consensus" case. The ranks of arrays of vector Q are calculated.

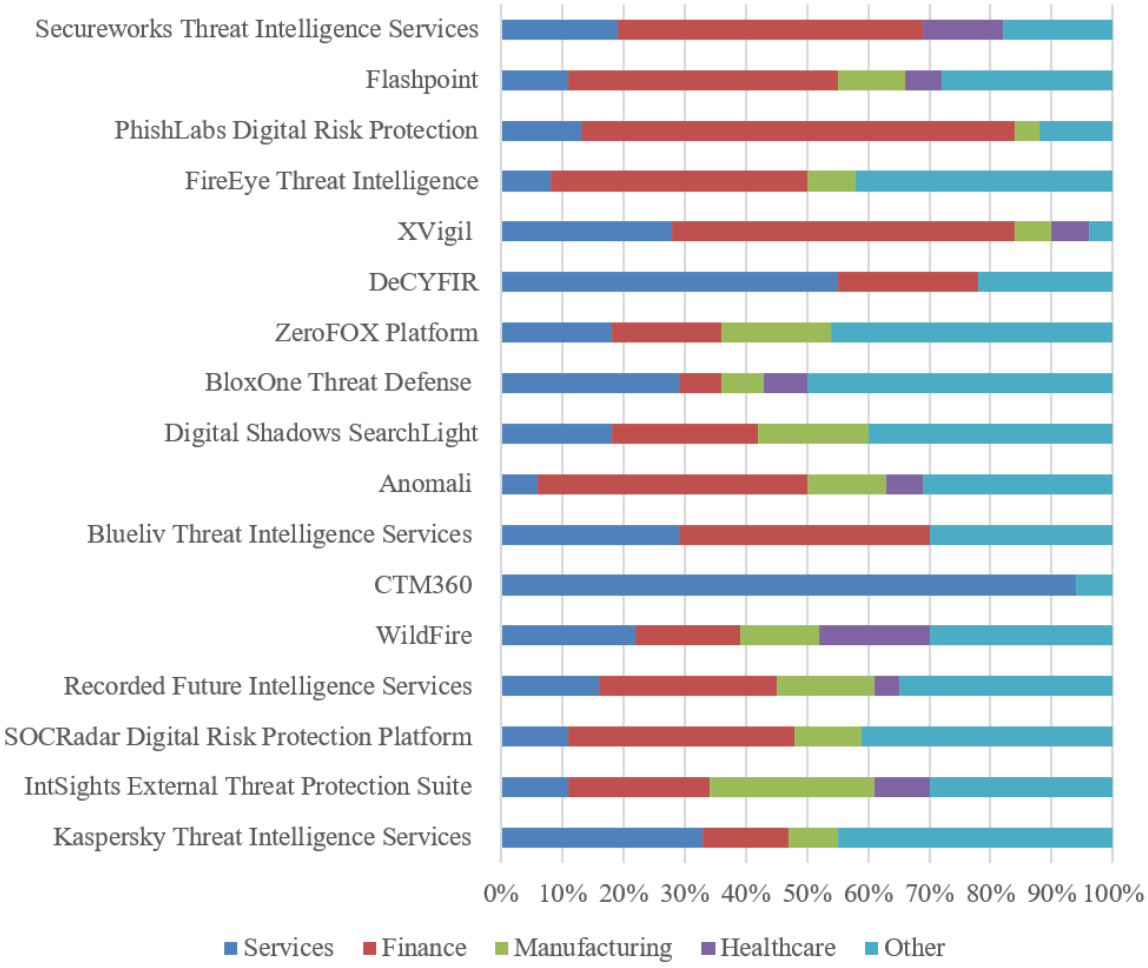

Figure 1. Classification according to the fields participating in the study

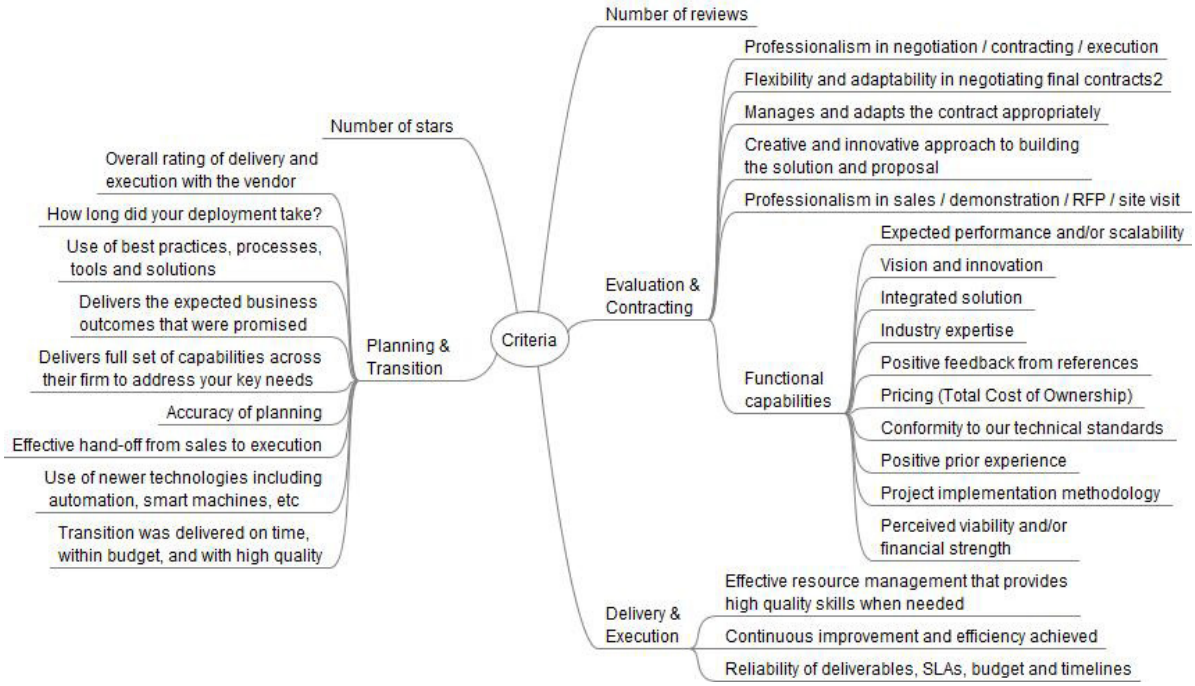

Figure 2. The criteria and sub-criteria

Table 1. The evaluation matrix E

Security Threat Intelligence Products and Services	Symbol	Reviews	Stars	Evaluation & Contracting	Planning & Transition	Delivery & Execution
Kaspersky Threat Intelligence Services	V1	49	4.9	4.8	4.9	4.9
IntSights External Threat Protection Suite	V2	44	4.8	4.8	4.8	4.8
SOCRadar Digital Risk Protection Platform	V3	19	5	5	4.9	4.9
Recorded Future Intelligence Services	V4	69	4.8	4.6	4.8	4.8
WildFire	V5	54	4.7	4.6	4.6	4.7
CTM360	V6	18	4.9	4.9	4.9	4.8
Blueliv Threat Intelligence Services	V7	17	4.7	4.5	4.7	4.7
Anomali	V8	16	4.6	4.5	4.6	4.5
Digital Shadows SearchLight	V9	17	4.4	4.4	4.6	4.4
BloxOne Threat Defense	V10	14	4.5	4.2	4.5	4.3
ZeroFOX Platform	V11	11	4.8	4.8	4.6	4.8
DeCYFIR	V12	22	4.8	4.9	5	5
XVigil	V13	18	4.6	4.8	4.8	4.7
FireEye Threat Intelligence	V14	12	4.6	4.5	4.4	4.7
PhishLabs Digital Risk Protection	V15	24	4.8	4.8	4.8	4.7
Flashpoint	V16	18	4.8	4.7	4.8	4.7
Secureworks Threat Intelligence Services	V17	16	4.2	4.4	4.1	4.4

The arrays of vectors R, S, Q and their ranks are displayed in Table 2.

Alternative V1 "Kaspersky Threat Intelligence Services" is the best alternative in the VIKOR method since the following two conditions are fulfilled:

Condition 1 is met: Note that

$$Q_{\alpha(2)} - Q_{\alpha(1)} = 0.131 - 0 = 0.131$$

and

$$\frac{1}{m-1} = \frac{1}{17-1} = 0.0625$$

hence $Q_{\alpha(2)} - Q_{\alpha(1)} \geq \frac{1}{m-1}$.

Table 2. The vectors *R, S* and *Q* and the ranks of their arrays

Alternatives Symbols	*R*	*R* ranks	*S*	*S* ranks	*Q*	*Q* ranks
V1	0	1	0	1	0	1
V2	0.132	2	0.131	5	0.131	2
V3	0.789	7	0.040	2	0.415	6
V4	0.237	3	0.080	4	0.158	3
V5	0.237	3	0.291	8	0.264	4
V6	0.816	8	0.156	6	0.486	8
V7	0.842	11	0.475	12	0.659	11
V8	0.868	13	0.627	13	0.748	13
V9	0.842	11	0.768	15	0.805	15
V10	1.000	15	0.889	16	0.945	16
V11	1.000	15	0.354	10	0.677	12
V12	0.711	6	0.060	3	0.385	5
V13	0.816	8	0.368	11	0.592	10
V14	0.974	14	0.628	14	0.801	14
V15	0.658	5	0.269	7	0.463	7
V16	0.816	8	0.333	9	0.574	9
V17	1.000	15	1.000	17	1.000	17

Condition 2 is met:

0.131-0>0.0625 (for *R*)

or

0.040<0.0625 (for S).

The best Security Threat Intelligence Product and service, in relation to the considered criteria, is Kaspersky Threat Intelligence Services. It is followed by the IntSights External Threat Protection Suite. The last is Secureworks Threat Intelligence Services.

In order to analyze the influence of the parameter θ on the obtained solution, the parameter θ will be varied in the interval (0,1) with step 0.1.

For each value of the parameter θ, a solution will be obtained by applying the VIKOR method.

The ranks of each alternative for various values of parameter θ are displayed in Table 3.

If $\theta = 0.6$, $\theta = 0.7$, $\theta = 0.8$ and $\theta = 0.9$ then the ranking is made by "voting by majority rule".

Table 3. The ranks of each alternative obtained by applying the VIKOR method and varying the values of parameter θ

Symbol	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	Max	Min	Difference
V1	1	1	1	1	1	1	1	1	1	1	1	0
V2	2	2	2	2	2	2	3	3	5	5	2	3
V3	7	7	7	6	6	6	5	5	3	7	3	4
V4	3	3	3	3	3	3	2	2	2	3	2	1
V5	4	4	4	4	4	4	6	6	7	7	4	3
V6	8	8	8	8	8	7	7	7	6	8	6	2
V7	11	11	11	11	11	12	12	12	12	12	11	1
V8	13	12	12	13	13	13	13	13	13	13	12	1
V9	12	13	14	14	15	15	15	15	15	15	12	3
V10	16	16	16	16	16	16	16	16	16	16	16	0
V11	14	14	13	12	12	11	11	11	11	14	11	3
V12	6	6	5	5	5	5	4	4	4	6	4	2
V13	10	10	10	10	10	10	10	10	10	10	10	0
V14	15	15	15	15	14	14	14	14	14	15	14	1
V15	5	5	6	7	7	8	8	8	8	8	5	3
V16	9	9	9	9	9	9	9	9	9	9	9	0
V17	17	17	17	17	17	17	17	17	17	17	17	0

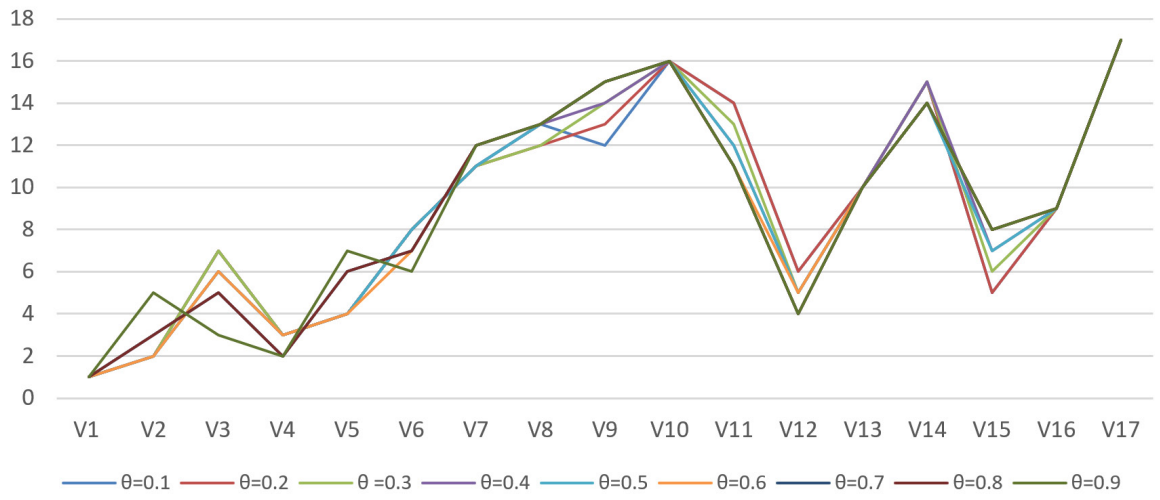

Figure 3. The differences in the ranks for various values of parameter θ

If $\theta = 0.5$ then the ranking is made "by consensus rule" and if $\theta = 0.1$, $\theta = 0.2$, $\theta = 0.3$ and $\theta = 0.4$ then the ranking is made "by the veto rule".

The order of the first two alternatives is the same up to the value 0.7 of the parameter θ.

The order of the alternatives placed on positions 1 (alternative V1 "Kaspersky Threat Intelligence Services"), 10 (alternative V13 "XVigil"), 16 (alternative V10 "BloxOne Threat Defense") and 17 (alternative V17 "Secureworks Threat Intelligence Services") does not change with the variation of the parameter θ. The biggest difference between the ranks is for alternative V3.

In equation (9) larger values of θ emphasize group gain, while smaller values of θ emphasize individual deviations.

The differences in the ranks for different values of parameter θ are displayed in Figure 3.

6. Conclusion

In the last decade, the increasing frequency and violence of cyber-attacks has determined the cyber-security community to elaborate advanced and intelligent solutions based on CTI. CTI is a rapidly growing field. However, it still suffers from being poorly defined.

In the market there are several CTI products and services providers. In this paper the VIKOR multi-attribute decision making method is used for obtaining a ranking of CTI services and products providers according to a set of given criteria. The proposed approach is implemented in a case study. The source of information for building the data collection, in the case study, is Security Threat Intelligence internet platform.

In VIKOR method, by varying the θ parameter several sets of CTI services and products rankings are obtained. The impact of the θ parameter values on the alternatives ranks is analysed.

The proposed approach helps the security program leaders in decision making for CTI products and services provider selection.

Acknowledgements

The research reported in this paper was supported by projects: PN 19 37 01 01 "Research on advanced policies and solutions for securing critical infrastructure against cyber-attacks" and PN 19 37 01 02 "Cyber polygon for industrial control systems (ROCYRAN)", funded by the Romanian Core Program of the Ministry of Research and Innovation (MCI), 2019-2022.

REFERENCES

Abu, M. S., Selamat, S. R., Ariffin, A. & Yusof, R. (2018). Cyber threat intelligence–issue and challenges, *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371-379.

Alidrisi, H. (2021). An Innovative Job Evaluation Approach Using the VIKOR Algorithm, *Journal of Risk and Financial Management*, *14*(6), 271.

Bhol, S. G., Mohanty, J. R. & Pattnaik, P. K. (2021). Taxonomy of cyber security metrics to measure strength of cyber security, *Materials Today: Proceedings.* Available at: <https://doi.org/10.1016 /j.matpr. 2021.06.228>, last accessed: 13th September 2021.

Cirnu, C. E., Rotună, C. I., Vevera, A. V. & Boncea, R. (2018). Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture, *Studies in Informatics and Control*, *27*(3), 359-368. DOI: 10.24846/v27i3y201811

de Melo e Silva, A., Costa Gondim, J. J., de Oliveira Albuquerque, R. & García Villalba, L. J. (2020). A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence, *Future Internet*, *12*(6), 108.

e-Governance Academy. (2021). *National Cyber Security Index*. Available at: <https://ncsi.ega. ee/ country/ro/>, last accessed: 14th September 2021.

e-Governance Academy. (2021). *National Cyber Security Index*. Available at: <https://ncsi.ega. ee/ country/ro/>, last accessed: 14th September 2021.

Enterprise Management 360. (2021). *Top 10 Threat Intelligence Platforms*. Available at: <https:// em360tech.com/top-10/top-10-threat-intelligence-platforms>, last accessed: 14th October 2021.

eSecurityPlanet. (2021). *Top Threat Intelligence Platforms for 2021*. Available at: <https://www. esecurityplanet.com/products/threat-intelligence-platforms/>, last accessed: 14th October 2021.

G2 Deals. (2021). *Best Threat Intelligence Services Providers*. Available at: <https://www.g2.com/ categories/threat-intelligence-services>, last accessed: 14th September 2021.

Gartner. (2021). *Security Threat Intelligence Products and Services Reviews and Ratings*. Available at: <https://www.gartner.com/reviews/market/security-threat-intelligence-services>, last accessed: 14th September 2021.

Huang, J., An, Z., Meckl, S., Tecuci, G. & Marcu, D. (2020). Complementary Approaches to Instructable Agents for Advanced Persistent Threats Detection, *Studies in Informatics and Control*, *29*(3), 269-282. DOI: 10.24846/v29i3y202001

Kosciuszko Institute (2018). *Cyber Threat Report CEE*. Available at: <https://cybermadeinpoland.pl/ wp-content/uploads/2020/06/Cyber-Threat-CEE-500-CYBERSEC-HUB-report.pdf>, last accessed: 13th September 2021.

Llansó, T., McNeil, M. & Noteboom, C. (2019). Multi-criteria selection of capability-based cybersecurity solutions. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 7322-7330).

Mardani, A., Zavadskas, E. K., Govindan, K., Amat Senin, A. & Jusoh, A. (2016). VIKOR technique: A systematic review of the state-of-the-art literature on methodologies and applications, *Sustainability*, *8*(1), 37.

MarketResearch (2021). *Cyber Security Market Size, Share & Trends Analysis Report By Component, By Security Type, By Solution, By Services, By Deployment, By Organization, By Application, By Region, And Segment Forecasts, 2021 – 2028.* Grand View Research. Available at: <https://www. marketresearch.com/Grand-View-Research-v4060/ Cyber-Security-Size-Share-Trends-14553577/>, last accessed: 13th September 2021.

Neto, A. J. H. & dos Santos, A. F. P. (2020). Cyber Threat Hunting Through Automated Hypothesis and Multi-Criteria Decision Making. In *IEEE International Conference on Big Data* (pp. 1823-1830).

Noor, U., Anwar, Z., Altmann, J. & Rashid, Z. (2020). Customer-oriented ranking of cyber threat intelligence service providers, *Electronic Commerce Research and Applications*, *41*, 1-20. Article: 100976.

Opricovic, S. (1998). *Multicriteria Optimization of Civil Engineering Systems*, 302 pp. PhD Thesis, Faculty of Civil Engineering, Belgrade.

Opricovic, S. & Tzeng, G. H. (2002). Multicriteria planning of post-earthquake sustainable reconstruction, *Computer-Aided Civil and Infrastructure Engineering*, *17*(3), 211-220.

Qiang, L., Zeming, Y., Baoxu, L., Zhengwei, J. & Jian, Y. (2016). Framework of cyber-attack attribution based on threat intelligence. In Mitton, N., Chaouchi, H., Noel, T., Watteyne, T., Gabillon, A. & Capolsini, P. (eds.), *Interoperability, Interoperability, Safety and Security in IoT*, 92–103. Springer: Cham, Switzerland.

Radulescu, C. Z. & Radulescu, M. (2018). Group decision support approach for cloud quality of service criteria weighting, *Studies in Informatics and Control*, *27*(3), 275-284. DOI: 10.24846/v27i3y201803

Radulescu, C. Z., Radulescu, M., Zbaganu, G. & Boncea, R. (2022). A Group Multi-Criteria approach

for development of a country COVID-19 indicator, *Procedia Computer Science, 199*, 149-156. Elsevier.

Ramsdale, A., Shiaeles, S. & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages, *Electronics*, *9*(5), 824.

Risk based Security. (2021). *Q3 2019 Data Breach QuickView Report*. Available at: <https:// www. riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/>, last accessed: 13th September 2021.

Sauerwein, C., Sillaber, C., Mussmann, A. & Breu, R. (2017). *Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives*. Semantic scholar. Available at: <https:// www.semanticscholar.org/paper/Threat-Intelligence-Sharing-Platforms%3A-An-Study-of-Sauerwein-Sillaber/0b9b00a2dbf6ae467395fac917e0 f7b73cc3e7aa>, last accessed: 13th September 2021.

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning, *Decision Support Systems*, *55*(1), 156-164.

Saxena, R. & Gayathri, E. (2021). Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution, *Materials Today: Proceedings*. Available at: <https://doi. org/10.1016/ j.matpr.2021. 06.204>, last accessed: 14th September 2021.

Shin, B. & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished, *Computer Security*, *92*. Article: 101761.

Trust Radius. (2021). *Threat Intelligence Platforms*. Available at: <https://www.trustradius.com/threat-intelligence-platforms>, last accessed: 14th October 2021.

van Niekerk, B., Ramluckan, T. & Duvenage, P. (2019). An analysis of selected cyber intelligence texts. In *Proceedings of the 18th European Conference on Cyber Warfare and Security* (pp. 554-559).

Vevera V., Georgescu A. & Cîrnu C. E. (2021). Opportunities for Cybersecurity Research in the New European Context, *Romanian Cyber Security Journal*, *1*(3), 79-88.

Yu, P. L. (1973). A class of solutions for group decision problems, *Management Science*, *19*(8), 936–946.

Zavadskas, E. K., Stevic, Ž., Turskis, Z. & Tomašević, M. (2019). A Novel Extended EDAS in Minkowski Space (EDAS-M) Method for Evaluating Autonomous Vehicles, *Studies in Informatics and Control*, *28*(3), 255-264. DOI: 10.24846/v28i3y201902

Zavadskas E. K., Bausys, R., Lescauskiene, I. & Omran, J. (2020). M-generalised q-neutrosophic MULTIMOORA for Decision Making, *Studies in Informatics and Control*, *29*(4), 389-398. DOI: 10.24846/v29i4y202001

Zeleny, M. (1982). High technology management, *Human Systems Management*, *3*(2), 57-59.

Zibak, A., Sauerwein, C. & Simpson, A. (2021). A Success Model for Cyber Threat Intelligence Management Platforms, *Computers & Security*, *111*(1). Article: 102466.