

The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 2026

Volume 41, Pages 101-110

ICRETS 2026: International Conference on Research in Engineering, Technology and Science

Multi-Criteria Decision-Making Application in Human Resource Management: The Case of a Cyber Security Specialist

Rabia Yumusak

Sivas Cumhuriyet University

Abstract: Information security is of vital importance for individuals, organizations, and societies to sustain their existence in the digital age. However, information security management processes constitute a complex structure that requires the simultaneous coordination of the fundamental objectives of confidentiality, integrity, and availability. In addition, information security policies differ at the individual, organizational, and societal levels. While individuals implement their own policies to ensure their personal information security, organizations rely on cybersecurity specialists. This is because the protection of organizational assets is of great importance in terms of sustainability. As a matter of fact, an organization that fails to ensure information security may experience not only financial losses but also reputational damage. This situation poses a significant risk to the sustainability of the organization. In order to minimize these risks, organizations need to select the most suitable cybersecurity specialist. To address this problem faced by organizations, a two-stage solution is proposed in the literature. First, the criteria affecting the selection and their relative importance levels must be determined. The second stage involves the evaluation of alternatives. In this study, the first stage is addressed. The criteria affecting the recruitment process of cybersecurity specialists are identified and their importance levels are calculated. In total, 5 main criteria and 24 sub-criteria are considered in the study. The inclusion of the “inclination toward artificial intelligence” criterion reflects the innovative aspect of the study. Due to the hierarchical structure of the problem, one of the multi-criteria decision-making methods, the Analytic Hierarchy Process (AHP), is employed for evaluation. As a result of the evaluation, experience and certifications emerge as the most prominent main criteria. In addition, the inclination toward artificial intelligence also holds a significant place in the selection of cybersecurity specialists.

Keywords: Information security, Selecting a cybersecurity expert, Multi-criteria decision making, Analytic hierarchy process

Introduction

With the rapid advancement of technology, although significant improvements have been achieved in cybersecurity and its supporting infrastructure, cyberspace is still far from being completely secure (Shiva et al., 2010). This situation compels cybersecurity service providers to continuously monitor emerging technological developments and adapt their personnel accordingly. In today's rapidly evolving technological environment, cybersecurity companies must place particular emphasis on human resource management processes to deliver their products effectively and ensure their sustainable use. This is because all cybersecurity products and services are ultimately created through the integration of employees' knowledge and skills with technology.

Furthermore, it is difficult to recruit qualified cybersecurity professionals. Therefore, for organizations, it is crucial to effectively manage every stage of the human resource process, beginning with personnel selection and extending to employee training, performance evaluation, and promotion (Furnell et al., 2017). The first stage of human resource management is personnel selection, and all subsequent human resource activities depend on this initial step. This highlights the critical importance of the personnel selection process. Selecting an unsuitable candidate may negatively affect subsequent processes, including employee training, organizational commitment,

- This is an Open Access article distributed under the terms of the Creative Commons Attribution-Noncommercial 4.0 Unported License, permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

- Selection and peer-review under responsibility of the Organizing Committee of the Conference

© 2026 Published by ISRES Publishing: www.isres.org

and overall job performance. Moreover, considering that cybersecurity is a mission-critical function responsible for protecting organizational information assets, the importance of selecting the right personnel becomes even more significant.

Personnel management, one of the core business processes of organizations, encompasses numerous decision-making activities. Following the identification of staffing needs, personnel selection represents one of the most critical decision-making stages within the human resource management process because organizations make substantial investments in newly hired employees. An inappropriate hiring decision may result not only in financial losses but also in wasted time, reduced organizational efficiency, and even reputational damage. Consequently, the personnel selection process is of strategic importance (Danişan et al., 2022).

Motivated by the importance of this problem, the present study addresses the selection of a cybersecurity specialist for employment in a financial institution. The personnel selection problem has been extensively investigated in the literature across various sectors, including the food industry (Chuang et al., 2020), textile industry (Danişan et al., 2022), logistics (Nong & Ha, 2021), security services (Kose et al., 2013), tourism (Urosevic et al., 2017), service systems (Uslu et al., 2021), and information technology, which is closely related to the application domain of the present study (Raj Mishra et al., 2020). Multi-Criteria Decision-Making (MCDM) methods are widely employed to solve personnel selection problems in these sectors. Pandey et al. (2026) provided a comprehensive literature review summarizing these studies.

A review of personnel selection studies in the field of information technology reveals the application of several MCDM techniques, including the Analytic Hierarchy Process (AHP) (Erdem, 2016), Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) (Samanlioglu et al., 2018), Additive Ratio Assessment (ARAS) (Raj Mishra et al., 2020), Evaluation Based on Distance from Average Solution (EDAS) (Karabasevic et al., 2018), and Step-wise Weight Assessment Ratio Analysis (SWARA) (Heidary Dahooie et al., 2018).

A review of the literature specifically addressing cybersecurity specialist selection indicates that only one related study exists. Yumusak and Eren (2022) calculated the weights of the criteria affecting cybersecurity specialist selection using the AHP method and subsequently ranked candidate alternatives using the PROMETHEE method. Although personnel selection has been extensively investigated within the information technology domain, research focusing specifically on cybersecurity specialist selection remains very limited. In the present study, the criteria affecting the selection of a cybersecurity specialist for a financial institution are evaluated using the AHP method. Furthermore, the set of 24 evaluation criteria employed in this study has, to the best of the authors' knowledge, not previously been considered together in the existing literature.

The remainder of this paper is organized as follows. Section 2 introduces the Analytic Hierarchy Process (AHP). Section 3 presents the proposed solution model for the cybersecurity specialist selection problem and describes the application steps in detail. Finally, Section 4 discusses the findings and presents the conclusions of the study.

Method

In this study, the Analytic Hierarchy Process (AHP) was employed because the decision problem exhibits a hierarchical structure.

Analytic Hierarchy Process (AHP)

The Analytic Hierarchy Process (AHP) is a multi-criteria decision-making (MCDM) method first developed by Thomas L. Saaty in 1980 to solve complex decision problems involving multiple criteria (Saaty, 1980). The method enables decision-makers to incorporate both objective and subjective judgments into the decision-making process. Owing to its flexibility and ease of application, AHP has been widely utilized in various decision-making problems across different disciplines. One of the primary reasons for its widespread adoption is that its methodology is intuitive and easily understood by decision-makers. The application steps of the AHP method are presented below.

Step 1: Construction of the Hierarchical Structure

In the first step, a hierarchical decision structure is established for the problem under consideration. This hierarchy generally consists of the overall goal at the top level, the evaluation criteria and sub-criteria at the intermediate levels, and the decision alternatives at the lowest level.

Step 2: Pairwise Comparison of the Criteria

Based on the hierarchical structure established in Step 1, pairwise comparison matrices are constructed. At this stage, the criteria are compared with one another, and the alternatives are evaluated with respect to each criterion through pairwise comparisons. These comparison matrices are developed using the fundamental importance scale proposed by Saaty (1980). The Saaty importance scale is presented in Table 1.

Table 1. Saaty importance scale	
Important Values	Value Definitions
1	Equally important
3	Somewhat important
5	Very important
7	Extremely important
9	Absolutely important
2, 4, 6, 8	Intermediate values

Step 3: Obtaining the Normalized Matrices and Relative Importance Weights.

For each criterion, the normalization process is performed using Equation (1), and the importance weights are calculated using Equation (2).

$$b_{ij} = \frac{a_{ij}}{\sum_{i=1}^n a_{ij}} \quad (1)$$

$$w_i = \frac{\sum_{i=1}^n b_{ij}}{n} \quad (2)$$

Step 4: Calculating and Verifying Consistency Ratios for Comparison Matrices.

The consistency index (CI) and the consistency ratio (CR) are calculated to determine the consistency of the comparisons. The formulas used to calculate the CI and CR are given in Equation (3) and Equation (4).

$$CI = \frac{\lambda_{maks} - n}{n - 1} \quad (3)$$

$$CR = \frac{CI}{RI} \quad (4)$$

CR values less than 0.1 are considered consistent. The RI values are given in Table 2.

Table 2. RI values (Saaty, 1980)														
n	1 ve 2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0	0,58	0,9	1,12	1,2	1,32	1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,59

Step 5: Identifying and Selecting the Best Alternative.

Based on the results of the AHP method, the alternative with the highest importance weight is selected as the best alternative.

Case Study

With the advent of Industry 4.0, ensuring information security for rapidly digitizing companies has become of great importance. As the importance of information security grows day by day and demand for solutions to these problems increases, the need for a qualified workforce has also risen. In this context, this study examines the recruitment process at a financial company providing services in the field of cybersecurity. The company in question identified a need for cybersecurity specialists, and this study aimed to optimize this recruitment process. The study was conducted in three main phases: first, problem definition; second, the identification of criteria influencing the selection process; and finally, the evaluation of these criteria using the AHP method.

Problem Definition

Cybersecurity is of critical importance for banks, insurance companies, investment firms, and fintech companies to conduct their operations securely. This sector is one of the primary targets of cyberattacks due to the high volume of financial transactions it handles and the sensitive customer data it processes. Therefore, selecting the right cybersecurity specialist plays a decisive role in protecting the organization's information assets. For this reason, this study addresses the problem of selecting a cybersecurity expert to work in the financial sector. The criteria influencing personnel selection were identified and prioritized. The study examined five main criteria and 24 sub-criteria.

Determining the Criteria

In determining the criteria to be considered during the selection process for a cybersecurity specialist to be employed in the financial sector, we drew upon current studies in the literature and expert opinions. There is one study in the literature that addresses the selection of cybersecurity specialists. However, there are no studies specifically focused on the selection of cybersecurity specialists for the financial sector. By combining the studies in literature and expert opinions, the criteria presented in Table 3 were established.

Table 3. Criteria influencing the selection of cyber security specialists

Main criteria	Sub-criteria
1. Education Level (C1)	1. Associate's degree (C1.1)
	2. Bachelor's degree (C1.2)
	3. Master's degree (C1.3)
	4. Doctorate (C1.4)
2. Professional Certifications (C2)	1. CISSP (C2.1)
	2. CEH (C2.2)
	3. CompTIA Security+ (C2.3)
	4. OSCP (C2.4)
	5. CISM (C2.5)
3. Analytical and Cognitive Competencies (C3)	1. Analytical thinking (C3.1)
	2. Crisis management (C3.2)
	3. Research skills (C3.3)
	4. Ability to learn quickly (C3.4)
4. Communication and Social Skills (C4)	1. Ability to work in a team (C4.1)
	2. Written and oral communication (C4.2)
	3. Leadership (C4.3)
	4. Time management (C4.4)
	5. Ability to work under pressure (C4.5)
5. Technical Knowledge and Competencies (C5)	1. Knowledge of network security (C5.1)
	2. Knowledge of operating systems (C5.2)
	3. Software security (C5.3)
	4. Malware analysis (C5.4)
	5. Penetration testing experience (C5.5)
	6. Proficiency in artificial intelligence (C5.6)

Level of Education

The level of education is a key criterion in selecting a cybersecurity specialist, as it reflects the candidate's theoretical foundation, analytical thinking skills, research abilities, and aptitude for professional development. Cybersecurity is a complex field comprising a combination of many disciplines, such as computer networks, operating systems, cryptography, software development, risk management, and information security. Therefore, the quality and level of a candidate's education can directly impact their ability to understand and solve security problems.

Professional Certifications

Professional certifications are nationally or internationally recognized documents that demonstrate that cybersecurity specialists possess specific knowledge, skills, and practical competencies. Due to the constantly evolving nature of technologies and threats in the field of cybersecurity, certifications are considered an important indicator that an individual possesses up-to-date knowledge and meets specific professional standards. For this reason, they are one of the key criteria evaluated alongside technical knowledge and experience in personnel selection processes.

Analytical and Cognitive Competencies

These competencies are of fundamental importance for cybersecurity experts to analyze complex security problems, accurately assess threats, and develop effective solutions. Attacks encountered in the field of cybersecurity are often multi-stage, dynamic, and involve a degree of uncertainty. Therefore, it is not enough for experts to possess only technical knowledge; they must also have strong analytical thinking, problem-solving, critical thinking, and decision-making skills.

Communication and Social Skills

Communication and social skills are of great importance not only for cybersecurity experts to solve technical problems but also to establish effective collaboration with various stakeholders, raise security awareness, and ensure proper coordination during crises. Today, cybersecurity has evolved beyond a purely technical activity; it has become a strategic discipline requiring collaboration among information technology, senior management, legal, human resources, and other business units. Therefore, strong communication skills are just as essential as technical knowledge among the core characteristics of a successful cybersecurity specialist.

Technical Knowledge and Competencies

Technical knowledge and competencies are among the most important criteria in selecting a cybersecurity specialist. This is because cybersecurity specialists are responsible for protecting an organization's information assets, detecting attacks, addressing security vulnerabilities, and responding quickly to potential threats. Effectively carrying out these tasks requires strong technical knowledge and practical skills.

Prioritization of Criteria Using the AHP Method

In the first step of the application, a hierarchical structure was established. The objective is to select a cybersecurity specialist. In line with this objective, five main criteria and 24 sub-criteria are presented in Figure 1. After the hierarchical structure was established, the pairwise comparison matrix for the main criteria was created using Table 1. Table 4 presents the pairwise comparison matrix for the main criteria. The normalized decision matrix was constructed by applying Equation 1 to the matrix shown in Table 4. The normalized decision matrix for the main criteria is presented in Table 5.

The weights of the main criteria were calculated by applying Equation 2 to the data in Table 5. The weights of the main criteria are shown in Figure 2. The most important main criterion was "Technical Knowledge and Competencies." When Equations 3 and 4 were applied, the consistency ratio was found to be 0.004. Since this value is less than 0.10, the result is consistent.

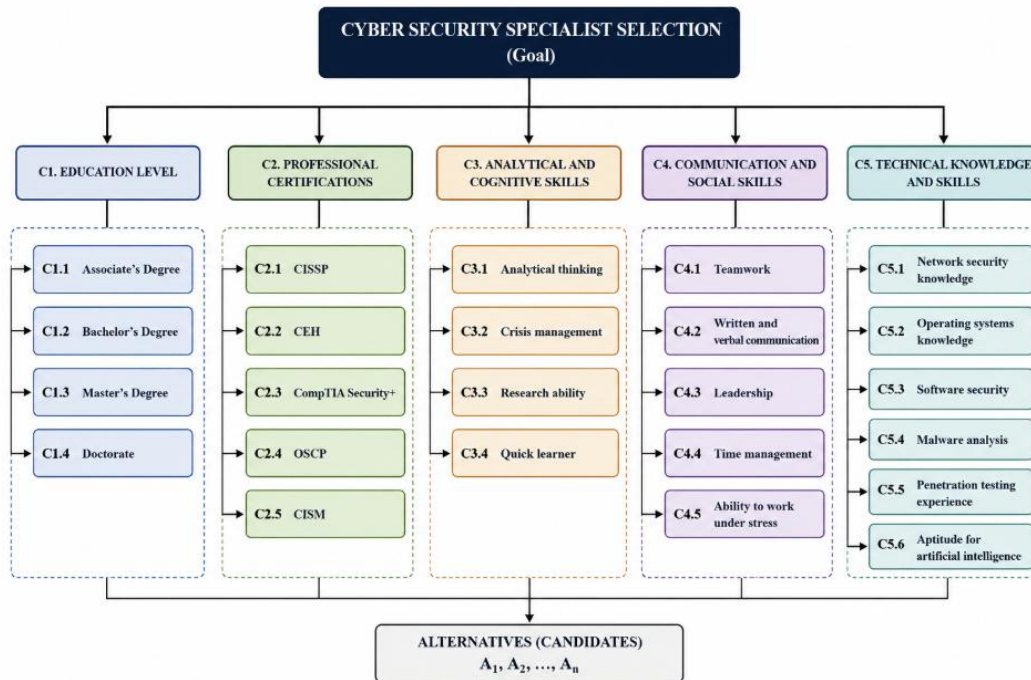


Figure 1. Hierarchical structure

Table 4. Pairwise comparison matrix of the main criteria

	C1	C2	C3	C4	C5
C1	1	0,500	0,200	0,250	0,143
C2	2	1	0,333	0,2	0,200
C3	5	3	1	2	0,500
C4	4	3	0,5	1	0,333
C5	7	5	2	3	1

Table 5. Normalized decision matrix for the main criteria

	C1	C2	C3	C4	C5
C1	0,053	0,040	0,050	0,039	0,066
C2	0,105	0,080	0,083	0,031	0,092
C3	0,263	0,240	0,248	0,310	0,230
C4	0,211	0,240	0,124	0,155	0,153
C5	0,368	0,400	0,496	0,465	0,460

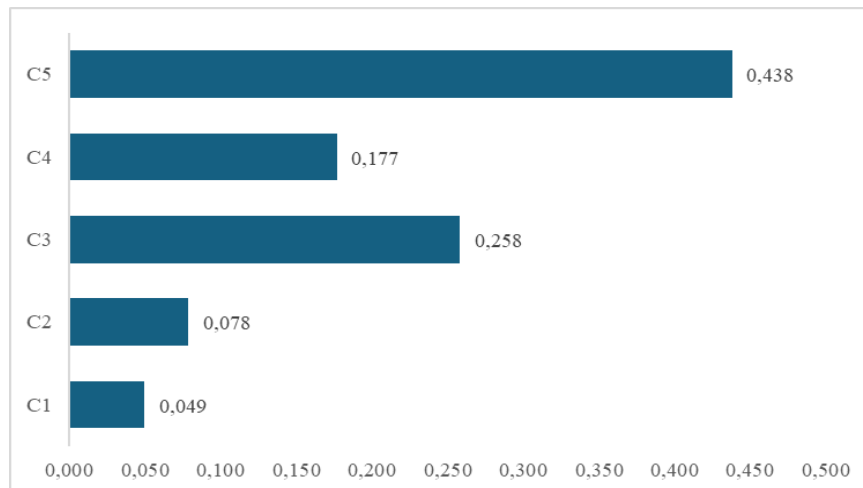


Figure 2. Main criterion weights

After the weights of the main criteria were calculated, the subcriteria for each main criterion were evaluated. The data related to the evaluation are presented in Table 6.

Table 6. AHP data for subcriteria

	C1.1	C1.2	C1.3	C1.4	local criteria weights		
C1.1	1	0,500	0,200	0,167		0,068	
C1.2	2	1	0,333	0,2		0,113	
C1.3	5	3	1	0,333		0,282	
C1.4	6	4	3	1		0,537	
	C2.1	C2.2	C2.3	C2.4	C2.5		
C2.1	1	5,000	3,000	0,500	6,000	0,304	
C2.2	0,2	1	0,250	0,2	3,000	0,079	
C2.3	0,333	4	1	0,333	3,000	0,157	
C2.4	2	5	3	1	7,000	0,414	
C2.5	0,167	0,333	0,333	0,143	1	0,045	
	C3.1	C3.2	C3.3	C3.4			
C3.1	1	4	7	9		0,597	
C3.2	0,250	1	5	7		0,270	
C3.3	0,143	0,2	1	3		0,089	
C3.4	0,111	0,143	0,333	1		0,044	
	C4.1	C4.2	C4.3	C4.4	C4.5		
C4.1	1	0,500	5,000	0,167	0,200	0,104	
C4.2	2	1	3,000	0,5	0,250	0,133	
C4.3	0,2	0,333	1	0,25	0,143	0,048	
C4.4	6	2	4	1	0,500	0,274	
C4.5	5	4	7	2	1	0,440	
	C5.1	C5.2	C5.3	C5.4	C5.5	C5.6	
C5.1	1	0,500	3	5	2	6	0,254
C5.2	2	1	4	6	3	8	0,390
C5.3	0,333	0,250	1	2	0,500	4	0,102
C5.4	0,2	0,167	0,5	1	0,333	3	0,063
C5.5	0,5	0,333	2	3	1	5	0,158
C5.6	0,167	0,125	0,25	0,333	0,2	1	0,033

Table 7. Sub-criterion weights

Main criteria	Sub-criteria	Weights
1. Level of Education (C1)	Associate's Degree	0.003
	Bachelor's Degree	0.006
	Master's Degree	0.014
	Doctorate	0.027
	CISSP	0.024
2. Professional Certifications (C2)	CEH	0.006
	CompTIA Security+	0.012
	OSCP	0.032
	CISM	0.004
	Analytical thinking	0.154
3. Analytical and Cognitive Competencies (C3)	Crisis management	0.070
	Research ability	0.023
	Quick learner	0.011
	Teamwork	0.018
	Written and verbal communication	0.024
4. Communication and Social Skills (C4)	Leadership	0.008
	Time management	0.048
	Ability to work under stress	0.078
	Network security knowledge	0.111
	Operating systems knowledge	0.171
5. Technical Knowledge and Competencies (C5)	Software security	0.045
	Malware analysis	0.028
	Penetration testing experience	0.069
	Aptitude for artificial intelligence	0.015

Finally, the global subcriterion weights were calculated by multiplying the local subcriterion weights by the main criterion weights. The subcriterion weights are presented in Table 7.

Results and Discussion

The problem of selecting a cyber security specialist at a financial company was addressed using the AHP method. The criteria in the problem were prioritized, and the results are presented in Figure 3. According to the analysis results, the sub-criterion with the highest weight is Operating System Knowledge (C5.2), with a weight of 0.171. This result indicates that it is considered a critical requirement for a cybersecurity specialist working in the financial sector to possess advanced knowledge of the security, configuration, and management of Windows, Linux, and Unix-based systems. Analytical Thinking (C3.1) ranks second, with a weight of 0.154. It is clear that analytical thinking skills play a major role in analyzing cyberattacks, incident response, threat hunting, and solving complex security problems. Network Security Knowledge (C5.1) (0.111) ranks third. Given the financial sector's high exposure to network-based attacks, proficiency in secure network architecture, firewalls, IDS/IPS systems, and network protocols emerge as a critical competency.

When the resulting global weights are evaluated together, it becomes evident that technical knowledge and experience are the most decisive factors in selecting cybersecurity specialists in the financial sector. In particular, knowledge of operating systems, analytical thinking, and network security emerged as the three most critical sub-criteria in the decision-making process. In contrast, educational level and certain professional certifications carry lower weights and are not decisive factors on their own in selecting a candidate. This situation demonstrates that the financial sector places greater emphasis on practical technical competencies, problem-solving skills, and qualities that can ensure operational success, rather than theoretical knowledge. These findings reflect the sector's need for experts with strong practical skills, analytical thinking, and the ability to make effective decisions in critical situations, given the rapidly evolving cyber threat landscape.

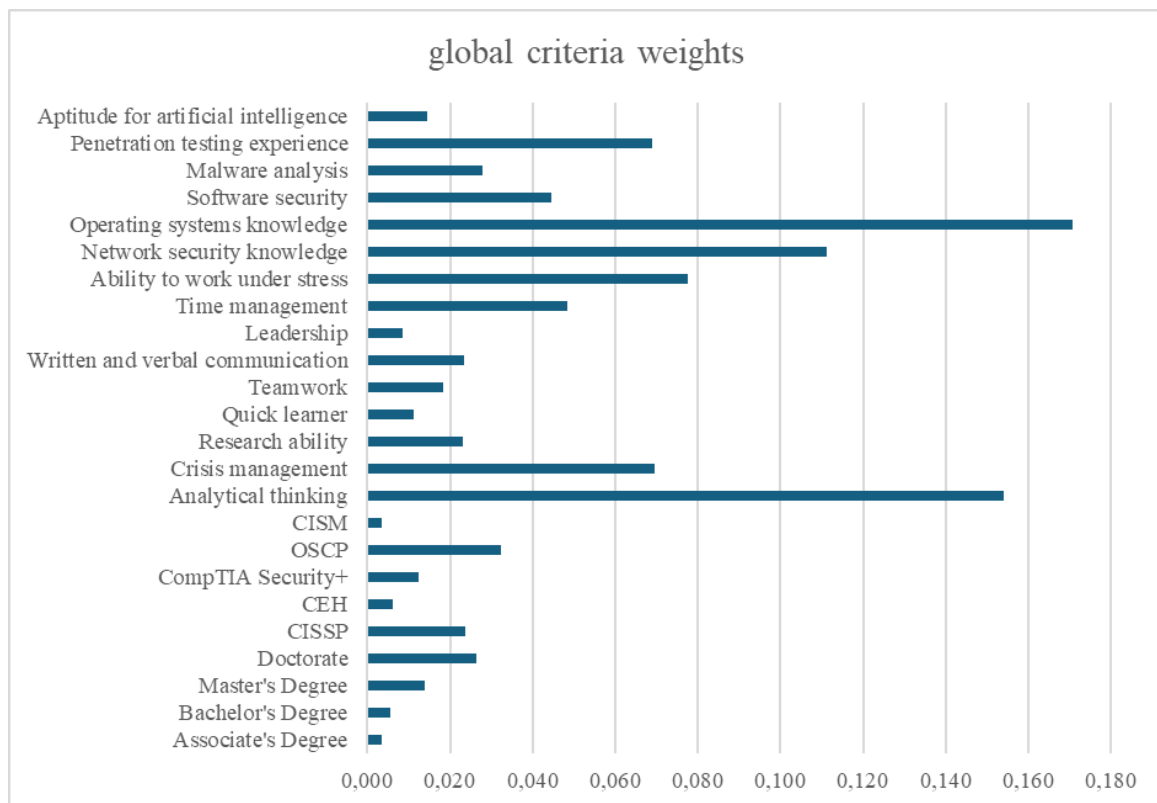


Figure 3. AHP results

Conclusion

In this study, which addresses personnel selection, the Analytic Hierarchy Process (AHP)—one of the multi-criteria decision-making methods—was used. The consistency indices obtained upon verification of the results

are presented in Table 8. Upon evaluation of the consistency indices, it was concluded that the results are consistent, as all values were less than 0.10.

Table 8. Consistency rates

Evaluation Criteria	Consistency Rate
Main Criteria	0,040
Education Level (C1)	0,017
Professional Certifications (C2)	0,060
Analytical and Cognitive Competencies (C3)	0,089
Communication and Social Competencies (C4)	0,088
Technical Knowledge and Competencies (C5)	0,024

This study, which addresses the problem of selecting cybersecurity specialists in financial companies, contributes to the literature in terms of its scope of application and the criteria used. While there is one study in the literature on the selection of cybersecurity specialists, there are no studies specifically addressing the financial sector. When evaluating the criteria, a maximum of 18 criteria were considered, including criteria such as certifications and aptitude for artificial intelligence, which are addressed for the first time in the literature. In this study, 24 sub-criteria were evaluated. From this perspective, it is a comprehensive study.

Recommendations

This study addresses the problem of selecting a cybersecurity specialist at a financial company. The problem consists of two stages. The first stage involves determining and weighting the criteria. In the second stage, the alternatives are evaluated based on these criteria. This study does not include the second stage. This stage, in which the alternatives are evaluated, could be added to the study. The study could be examined using fuzzy multi-criteria decision-making methods. Finally, a more comprehensive study could be conducted by identifying artificial intelligence tools for the “suitability for artificial intelligence” criterion.

Scientific Ethics Declaration

* The author declares that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the author.

Conflict of Interest

* The author declares that there is no conflict of interest.

Funding

* There is no funding available for this study

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Research in Engineering, Technology and Science (www.icrets.net) held in Batumi/Georgia on July 09-12, 2026.

References

- Chuang, Y. C., Hu, S. K., Liou, J. J. H., & Tzeng, G.-H. (2020). A data-driven MADM model for personnel selection and improvement. *Technological and Economic Development of Economy*, 26(4), 751–784.
- Danişan, T., Özcan, E., & Eren, T. (2022). Personnel selection with multi-criteria decision making methods in the ready-to-wear sector. *Tehnički Vjesnik*, 29(4), 1339–1347.

- Erdem, M. B. (2016). A fuzzy analytical hierarchy process application in personnel selection in IT companies: A case study in a spin-off company. *Acta Physica Polonica A*, 130(1), 331–334.
- Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, 2017(2), 5–10.
- Heidary Dahooie, J., Beheshti Jazan Abadi, E., Vanaki, A. S., & Firoozfar, H. R. (2018). Competency-based IT personnel selection using a hybrid SWARA and ARAS-G methodology. *Human Factors and Ergonomics in Manufacturing & Service Industries*, 28(1), 5–16.
- Karabasevic, D., Zavadskas, E. K., Stanujkic, D., Popovic, G., & Brzakovic, M. (2018). An approach to personnel selection in the IT industry based on the EDAS method. *Transformations in Business & Economics*, 17(2), 54–65.
- Kose, E., Kabak, M., & Aplak, H. S. (2013). Grey theory based MCDM procedure for sniper selection problem. *Grey Systems: Theory and Application*, 3(1), 35–45.
- Nong, N.-M. T., & Ha, D.-S. (2021). Application of MCDM methods to qualified personnel selection in distribution science: Case of logistics companies. *Journal of Distribution Science*, 19(8), 25–35.
- Pandey, N., Dash, S. P., & Kaur, P. (2026). A systematic review of multi-criteria decision-making (MCDM) methods applied to personnel selection: Trends, models, and effectiveness. *OPSEARCH*. Advance online publication.
- Raj Mishra, A., Sisodia, G., Raj Pardasani, K., & Sharma, K. (2020). Multi-criteria IT personnel selection on intuitionistic fuzzy information measures and ARAS methodology. *Iranian Journal of Fuzzy Systems*, 17(4), 55–68.
- Saaty, T. L. (1980). *The analytic hierarchy process: Planning, priority setting, resource allocation*. New York, NY: McGraw-Hill.
- Samanlioglu, F., Taskaya, Y. E., Gulen, U. C., & Cokcan, O. (2018). A fuzzy AHP–TOPSIS-based group decision-making approach to IT personnel selection. *International Journal of Fuzzy Systems*, 20(5), 1576–1591.
- Shiva, S., Roy, S., & Dasgupta, D. (2010). Game theory for cyber security. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research* (Article 34). New York, NY: ACM.
- Urosevic, S., Karabasevic, D., Stanujkic, D., & Maksimovic, M. (2017). An approach to personnel selection in the tourism industry based on the SWARA and the WASPAS methods. *Economic Computation and Economic Cybernetics Studies and Research*, 51(1), 75–88.
- Yumuşak, R., & Eren, T. (2022). Selecting a cyber security specialist with multi-criteria decision-making methods. *International Journal of Management Information Systems and Computer Science*, 6(2), 117–130.

Author(s) Information

Rabia Yumusak

Cumhuriyet University, Department of Database, Network
Design and Management, Cumhuriyet Vocational School of
Social Sciences, Sivas, Türkiye
ORCID iD: <https://orcid.org/0000-0002-0257-939X>

*Contact e-mail: rabiayumusak@cumhuriyet.edu.tr

*Corresponding author(s) contact email

To cite this article:

Yumusak, R. (2026). Multi-criteria decision-making application in human resource management: The case of a cyber security specialist. *The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM)*, 41, 101-110.