Combined Method for Prioritizing Information Security Risks

Assel Nurusheva *, Nikolaj Goranin, Dina Satybaldina, Askhat Amrenov *

Posted Date: 22 January 2025

doi: 10.20944/preprints202501.1561.v1

Keywords: information system; DLP system; information security; risk assessment; CSIRT

Article

Combined Method for Prioritizing Information Security Risks

Assel Nurusheva [1], Nikolaj Goranin [2],Dina Satybaldina [1] and Askhat Amrenov [1,*]

[1] Department of Information Security, Faculty of Information Technology, L.N.Gumilyev Eurasian National University, Astana, Kazakhstan

[2] Department of Information Systems, Vilnius Gediminas Technical University (VilniusTech), Vilnius, Lithunia

* Correspondence: askhat.amrenov@gmail.com

Abstract: This article proposes a combined method for managing information system security risks based on expert assessments and risk-oriented patterns. The scores were obtained by conducting a questionnaire (expert assessment), as well as using the Common Vulnerability Scoring System (CVSS). CVSS was used to calculate vulnerability level and threat likelihood metrics after taking countermeasures. This method can be used to prioritize information security risks, as well as to determine information security requirements. Attacks on information leak prevention systems are simulated. The priorities of the risks associated with these attacks have been identified. Such systems can be used in SOC and CERT work. Therefore, the method can be used when building business processes related to SOC and CSIRT.

Keywords: information system; DLP system; information security; risk assessment; CSIRT

1. Introduction

Ensuring information security is an important task in the modern world. The main functions of the SOC and CSIRT teams are timely response to information security incidents and their prevention, as well as timely detection of vulnerabilities, threats, and risks in the system and their processing.

CSIRT teams face certain difficulties when performing information system (IS) risk assessments. First, at the stage of planning and building certs and related processes, it is difficult to take into account all the risks associated with the IS in which they will work. Secondly, there is no time- and cost-efficient risk assessment method. The team needs to assess the risks of an ongoing attack or identified vulnerability as soon as possible and make quick decisions on how to mitigate the risks.

Third, explaining to other departments involved in CSIRT processes the criticality of a particular vulnerability and the need to take countermeasures to minimize the risks is a challenge. Because it can be difficult for legal, administrative, and security departments to understand technical risk analysis reports due to the lack of a standardized way of presenting this information. The challenge is that management does not always understand complex technical risk reports, and there is no appropriate method to communicate infrastructure risk information clearly and visually to senior management.

This paper discusses information security risks associated with the use of Data Leakage Prevention (DLP). We propose a combined risk assessment method to efficiently and quickly assess risks when new vulnerabilities are discovered in IS in an environment in which information security incident response teams are operating. This can enable the prioritization of risks and the order in which certs should notify customers of a discovered vulnerability. The stage at which categorization, criticality level determination, and assessment take place. CSIRT teams also deal with targeting IS attacks. Unfortunately, it is not always possible to incorporate these attacks into threat models due to their unpredictability and complexity. That is, the teams lack methods that would allow them to

 doi:10.20944/preprints202501.1561.v1

effectively determine the level of risk associated with advanced, targeted attacks. To solve this issue, a method based on expert assessments using risk-oriented patterns is proposed. Moreover, security teams need to conduct risk assessments within their IS and infrastructure to eliminate possible cybersecurity threats.

This will help identify information security risks associated with using technical means before the commissioning of informationization facilities. Moreover, this method may be suitable for business process modeling specialists, who can assess information security risks in advance to identify potential vulnerabilities and determine priority. Information security risk-oriented patterns are the best way to convey the necessary information clearly and easily, for example, the technical aspects of an information system, to all interested parties who are in any way connected with this IS. Business process modeling experts have limited experience in the information security area.

A literature review was conducted for our research. Article [1] examines automation in security operations centers (SOCs) and its impact on analysts. The authors highlight issues such as automation bias and complacency that arise as analysts become increasingly dependent on automated tools.

Research [2] proposes an adaptive risk management approach to counter privacy attacks in Fog-IoT environment. The authors highlight the importance of integrating edge computing (fog computing) into IoT to reduce latency, increase geographic distribution, and local data processing. [3] discusses a security assessment framework that combines two different multi-criteria models with the goal of finding interconnections between security criteria with further prioritization. Paper [4] describes the improvement of the threat modeling technique with the involvement of a number of master's students with the goal of evaluating the completeness and correctness of the results analysis.

The objective of research [5] is to determine the security conditions of e-banking applications and analyze the risks and threats that can happen to customers.

Work [6] examines the problem of insider threats in the healthcare industry using text mining techniques to identify and prevent potential risks. The authors emphasize the importance of protecting patients' confidential information and propose using text mining to monitor and detect abnormal employee actions that may pose a threat to data security.

Many research papers have been written about risk determination, security, and reliability by implementing multi-criteria methods in different practical spheres [7–10]. In [11]–14], the problems of information security and reliability were researched, methods providing security and reliability for identification and mitigating security risks at the initial phase of IS construction were suggested, and a suitable software system was constructed on the basis of the suggested methods.

In [15], a method for automatic sorting, containment, and escalation for SOC is proposed.

2. Materials and Methods

Sorting in the context of information security refers to the process of prioritizing incident resolution based on the severity of a security breach or compromise. Triage in the context of information security incident response is the primary processing and screening of cybersecurity incidents. The proposed method can help CSIRT and SOC in these two processes (triage and sorting) to handle cybersecurity incidents and make further analyses for the determination of security risks connected to cybersecurity incidents. In this article, according to the method, assessments are made partially by experts and partially using the CVSS method. This method involves using security risk-based BPMN to identify system and business assets, security threats related to IS components, and countermeasures for them with further risk assessment by means of expert interviews. The use of risk-oriented model BPMN visually helps to identify, sort, and assess risks. Our method helps prioritize vulnerabilities without resorting to complex technical tools. CSIRT may provide a new service to check ensurance of the security and reliability of information systems by applying risk assessment according to the proposed method. This method can be applied to prioritization of information security risks and determining information security requirements.

Let’s consider the next scenario: when the CSIRT or SOC receives several security incidents at once, it is crucial to determine the order of response to them since it is not always possible to handle

 doi:10.20944/preprints202501.1561.v1

incidents in parallel. In this way, the method can be applied at the initial stage of incident processing - identify the assets involved in the incident, determine the vulnerabilities that the attacker exploited, and come up with a way to eliminate the threat. And, of course, it is best to visualize each step using BPMN. Next, in order to prioritize incident response, it is necessary to assess the risks that these IS incidents may pose.

The next way how the proposed method can be used is to implement it at the stage of building processes and information and communication infrastructure of CSIRT or SOC. That is determination using risk-based BPMN of system and business assets of future information and communication infrastructure, possible vulnerabilities and threats to information security of assets that may arise, and how to counteract the emerging cyber threats. Further, according to the method - to assess the risks that may occur after the construction of CSIRT and SOC, and if necessary - to eliminate them depending on the level of criticality of the risk.

According to the method, the first step is to describe the organization's assets that need protection and determine the security criteria with the goal of security risk assessment. At this stage, business assets and system assets are allocated, and security goals are determined. Metrics such as value and security requirements are defined. Business assets mean events, tasks, and data objects. System assets mean data storage, containers - independent units of the process, and organizational units (for example database, program, and IS components).

Let's consider the application of the risk assessment method in the example of DLP-related infrastructure. DLP system is a tool that CSIRTs often use as part of their core business. Therefore, the risk assessment will help to identify the main gaps, weaknesses in the security of this DLP system and prevent possible information security incidents related to various vulnerabilities.

Figure 1 shows business assets, system assets, and IS assets. It describes the authorization process of an administrator in the DLP system. The DLP system processes the username and password entered by the user. If the password and username match, it grants administrator privileges and gives this user a specific session identifier.

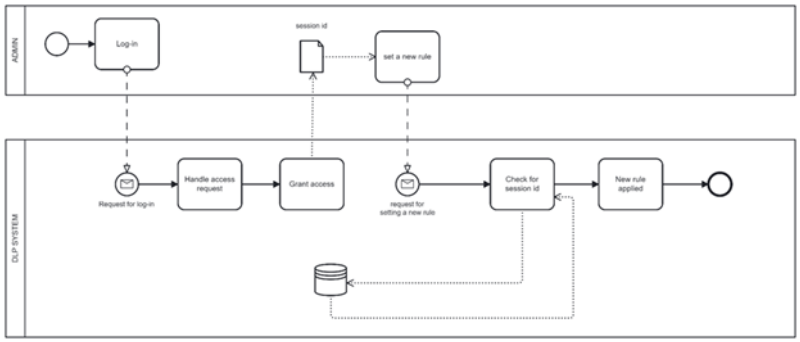


Figure 1. Context and asset model in risk-oriented BPMN.

Next, concepts related to information security risks are used to identify these risks and their components. Risk-based BPMN is utilized to show the violator's actions, vulnerabilities in the system, and other activities that aim to achieve desired results. The risk value is determined with the help of the risk level metric. It is important to map the details of the risk as closely as possible so that experts can understand what the risk is about, how it occurs, what consequences and threats the risk may carry, and more accurately assess metrics such as risk level, impact level, potentiality and probability of risk. The CVE vulnerability database was used to describe the risks.

Thus, Figure 2 shows the risk associated with a vulnerability in the DLP, which can occur due to improper session management. An attacker can use this vulnerability to gain the privileges of the DLP system administrator and gain further access to confidential documents. The figure shows that an attacker can use a brute force attack to select a session ID and act on behalf of the administrator due to a vulnerability in the DLP system.

 doi:10.20944/preprints202501.1561.v1

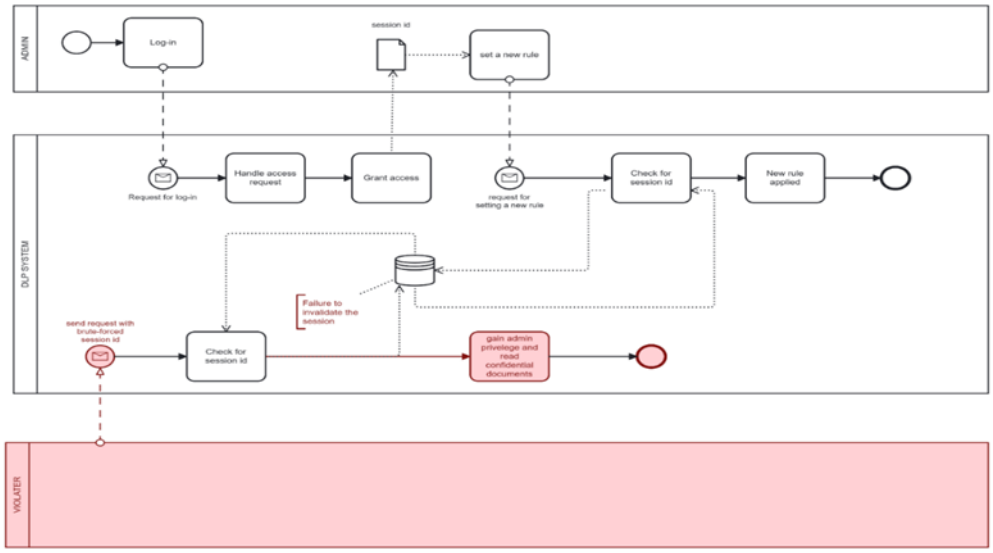


Figure 2. Security risk model in risk-oriented BPMN.

Figure 3 shows the method of applying countermeasures to the actions of the violator described above. These countermeasures reduce the risk. To ensure that the session on the server is terminated when the user logs out, it is proposed to implement an "inactivity timeout" for each session.

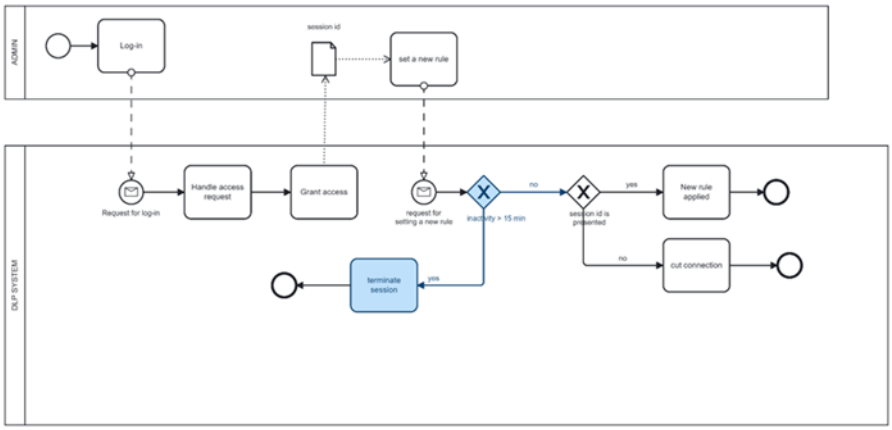


Figure 3. A model of countermeasures in a risk-oriented BPMN.

Further, risk assessment and analysis take place after determining the risks.

Risk assessment is conducted by experts. Experts are invited to review the questionnaire, which presents questions that will help them obtain certain scores for a particular metric and ultimately help to assess each risk and conduct further analysis. As a result assessments of security need, cost, value, threat likelihood and vulnerability level were obtained.

Some of the questions from the questionnaire that were given to the experts:

- What score will you set for the value parameter for this asset?;
- Evaluate the impact on the confidentiality metric for the session ID asset;
- Evaluate the impact on the integrity metric for the session ID asset;
- Evaluate the impact on the availability metric for the asset session ID;
- Evaluate the vulnerability level metric;
- Rate the threat likelihood metric.;
- Evaluate the cost metric (the cost of implementing these countermeasures);
- How much do you think it will cost to implement these countermeasures?;

The average values of expert estimates were calculated for value, security need, threat likelihood, cost, and vulnerability level.

 doi:10.20944/preprints202501.1561.v1

As a result, experts evaluated only seven metrics. The other two metrics were automatically received using the CVSS method. The rest of the metrics were calculated based on previously assessed metrics.

And now about how the points were assigned. The questionnaire asked each BPMN diagram to be scored for specific metrics. For example, under the diagram depicting the model of context and asset, it was proposed to assign points for the value of assets from 1 to 5 and also to assign points for 3 metrics of security need, namely, confidentiality, availability, and integrity, in the range from 1 to 3. Under the diagram of the security risk model in the questionnaire, experts were asked to give points for the metrics vulnerability level from 1 to 10 and for the metric probability of threat to give points from 1 to 10. Below the countermeasures model diagram, experts were asked to score the cost of countermeasures metric from 1 to 10.

The event potentiality metric was calculated as probability plus vulnerability level minus one. The impact metric was obtained through the security need metrics by finding the maximum of the three metrics. The risk level metric is calculated based on the other two metrics by multiplying event potentiality by the impact.

The risk reduction level is obtained as risk level 1 (risk level before countermeasures) minus risk level 2 (risk level after countermeasures). CVSS was used to calculate vulnerability level and threat likelihood metrics after taking countermeasures. Thus, the assessment method is combined and consists of two methods – expert and CVSS.

Metrics such as vulnerability level after treatment and threat likelihood after treatment are assessed using the program method CVSS. This method makes assessment of estimated metrics much easier and more precise. It's hard to completely convey and depict all the nuances of IS using risk-oriented models. Therefore, an assessment made using a risk-oriented BPMN can sometimes turn out to be rough. Assessing countermeasures requires knowledge of the specifications and peculiarities of IS and how IS can behave after security risk decreases, especially in the planning stage. Companies can't provide detailed IS diagrams for some considerations. For this reason, it will be a little bit hard for external experts who are involved in other departments or organizations to assess it precisely. It is suggested to use the CVSS method together with expert assessment, which can help assess security risks more precisely, save time and increase efficiency.

For our combined method of security risk assessment, we used the base score metric and exploitability subscore metrics from the CVSS framework.

3. Results

Table 1 presents other risk-based models for the remaining risks for convenience. These models are determined analogically by the method described above.

Table 1. Description of risk-oriented models.

Risk id	Description of Context and Asset Model	Description of Risk model	Description of Countermeasure Model
2	The process of sending an alert notification about an Information security event by the dlp client to the dlp server. Information about the event is parsed and sent to the database. Next, the system generates a	A vulnerability in the DLP system is an SQL injection vulnerability that can be exploited by an intruder to execute remote code on the server and obtain administrator privileges to further gain access to data. In this case, the attacker sends a query with SQL injection, which	Implementing input verification and using parameterized queries is proposed.

 doi:10.20944/preprints202501.1561.v1

	report and sends it to the administrator console.	is processed by the database, allowing the attacker to execute commands.	
3	Data entry is the process by which the administrator in the DLP subsystem responsible for case management enters data. IS confirms the received data and accepts it for further work. The DLP administrator can already view the cases on his console, considering the updated information.	A vulnerability in the DLP system is an XSS–injection vulnerability that can allow an attacker to obtain session cookies from the DLP system administrator. In this case, it is shown that due to the vulnerability, an attacker introduces a malicious link using XSS injection into the DLP case management framework. Next, the dlp admin sees this link and clicks it. The browser executes the script and sends information about the administrator session to the attacker. This may allow you to log in to the system as an administrator.	Implementing data entry verification and filtering is proposed.
4	The process of registering a new user of the DLP system. When registering, the new user sends his username and password to the DLP system. The password and login are confirmed by the DLP system and sent to the database.	Vulnerability of unsecured storage of credentials, namely, credentials are stored in the usual form – in the form of text. This may allow an attacker connected locally to read the data stored in the logging files in plain text format in the database, gain access to all logins and passwords, i.e. credentials, and then connect to a password-protected resource.	It is proposed that cryptographic password hashes be stored as an alternative to plaintext storage. It is also possible to try to solve the password management problem by hiding the password using the encoding function.

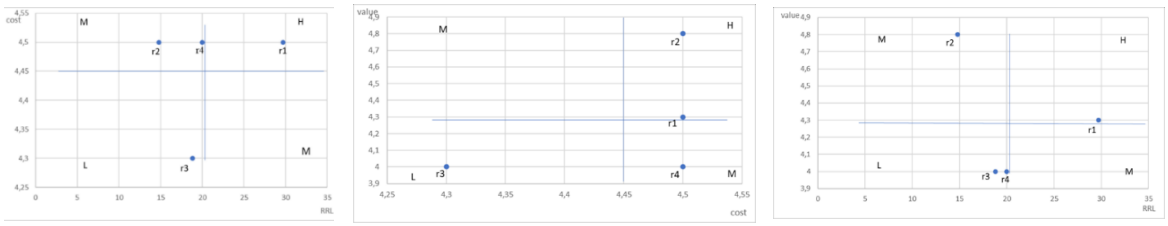
After calculating all the metrics, an analysis based on the data was carried out to identify the risk with the highest priority.

The priority of response to incidents connected with discovered vulnerabilities, i.e., security risks, has very important meaning for computer emergency response teams. Thus, it is necessary to understand which risk should be reflected first. For these goals, the trade-off analysis is conducted using the risk reduction level (RRL), countermeasure's cost, and business asset value obtained from expert assessment.

Utilizing these metrics, three graphs were accomplished (see Figure 4(a), 4(b), and 4(c)) incorporating data on cost and RRL, value and cost, value and RRL. The graphs are divided into four quadrants, and the priority for each quadrant is identified by labels low (L), medium (M), and high (H) on each quadrant. From an incident response perspective, the cost of countermeasures refers to the amount of human and programmatic resources that must be used to eliminate an attack or incident. By the value of the cost, it is possible to conclude the magnitude and severity of the risk. A high value of an asset implies that a lot of work will have to be done to eliminate the incident if the

 doi:10.20944/preprints202501.1561.v1

risk is realized, from which we can conclude that the risk is critical. Its elimination becomes a higher priority than a risk with a lower value. From the Incident Response point of view, the value of the Risk Reduction Level can be used to infer the criticality of the risk and the appropriateness of the response to the incident. The higher the value, the greater the effect of responding to the incident and, thus, the more appropriate it is to respond to the security incident in the first place. This makes the risk a higher priority for incident response teams. Of course, the higher the asset's value, the more the CSIRT or SOC prioritizes it when responding to incidents. Figure 4(a) presents a graph of the cost against the level of risk reduction.



(a) (b) (c)

Figure 4. (a)Dependence of cost on RRL; (b) Dependence of value on cost;(c) Dependence of value on RRL.

According to the graph, Risk 1 (r1) is high priority, Risk 2 (r2) and Risk 4 (r4) are middle priority, and Risk 3 (r3) is low priority.

Figure 4(b) is about the business asset value against the cost of countermeasure. According to the graph, Risk 2 (r2) and Risk 1 (r1) are a high priority, and Risk 4 (r4) has a low priority.

Figure 4(c) is about the asset value against the risk reduction level. According to the graph, Risk 1 (r1) is a high-priority risk, Risk 2 (r2) is a middle-priority risk, Risk 3(r3) and Risk 4(r4) are low-priority risks.

Then, according to the diagrams, the total score for each risk was calculated. If the risk falls into area H, then 3 points are awarded, if it falls into area M, then it gets 2 points, if it falls into area L, then 1 point is awarded. As a result, after calculations, it turned out that risk 1 has the highest priority, risks 2 and 4 have medium priority, and risk 2 has the lowest priority.

4. Discussion

In this article, a combined method of IS security risk management is proposed, which is based on expert assessments. This method can be applied to prioritize information security risks at the stage of sorting information security incidents, and to determine information security requirements when modeling IS processes. Sorting in the context of information security refers to the process of prioritizing incident resolution based on the severity of a security breach or compromise. The response teams sort through the incidents that have already occurred. This article proposes a method based on expert assessments using risk-oriented patterns to manage IS security risks. Information security risk-oriented patterns are the best way to convey the necessary information clearly and easily, for example, the technical aspects of an IS, to all interested parties who are in any way connected with this IS. Using this method can visually help identify, sort, assess risks, and prioritize vulnerabilities without the use of technical means.

The proposed method is considered when modeling attacks on information security systems against leaks. The priorities of the risks associated with these attacks have been identified. Such systems can be used in SOC and CERT work. Therefore, the method can be applied when building business processes related to SOC and CERT.

 doi:10.20944/preprints202501.1561.v1

Abbreviations

The following abbreviations are used in this manuscript:

SOC	Security Operations Center
CSIRT	Computer security incident response team
DLP	Data Loss Prevention

References

1. Tilbury, J.; Flowerday, S. Automation Bias and Complacency in Security Operation Centers. Computers 2024, 13, 165. https://doi.org/10.3390/computers13070165.
2. Selvan, S.; Mahinderjit Singh, M. Adaptive Contextual Risk-Based Model to Tackle Confidentiality-Based Attacks in Fog-IoT Paradigm. Computers 2022, 11, 16. https://doi.org/10.3390/computers11020016
3. K. C. Park and D.-H. Shin, "Security assessment framework for iot service," Telecomm. Systems, vol. 64, no. 1, pp. 193-209, Jan. 2017, doi: 10.1007/s11235-016-0168-0.
4. R. Scandariato, K. Wuyts, W. Joosen, "A descriptive study of Microsoft's threat modeling technique," Requir. Eng., vol. 20, no. 2, pp. 163–180, June 2015, doi: 10.1007/s00766-013-0195-2.
5. G. Mogos and N. S. Mohd Jamail, "Study on security risks of e-banking system," Indones. J. Electr. Eng. Comput. Sci., vol. 21, no. 2, pp. 1065–1072, Feb. 2020, doi: 10.11591/ijeecs.v21.i2.pp1065-1072.
6. Lee, I. Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach. Information 2022, 13, 404. https://doi.org/10.3390/info13090404
7. Collen, A.; Szanto, I.-C.; Benyahya, M.; Genge, B.; Nijdam, N.A. Integrating Human Factors in the Visualisation of Usable Transparency for Dynamic Risk Assessment. Information 2022, 13, 340. https://doi.org/10.3390/info13070340.
8. Khan, A.N.; Bryans, J.; Sabaliauskaite, G.; Jadidbonab, H. Integrated Attack Tree in Residual Risk Management Framework. Information 2023, 14, 639. https://doi.org/10.3390/info14120639.
9. Alsafwani, N.; Fazea, Y.; Alnajjar, F. Strategic Approaches in Network Communication and Information Security Risk Assessment. Information 2024, 15, 353. https://doi.org/10.3390/info15060353.
10. A.M AbdelMouty, A. Abdel-Monem, "Neutrosophic MCDM Methodology for Assessment Risks of Cyber Security in Power Management," Neutrosoph. Systems Appl., vol. 3, pp. 53-61, Mar. 2023, doi: 10.61356/j.nswa.2023.18.
11. Villegas-Ch., W.; Ortiz-Garces, I.; Sánchez-Viteri, S. Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. Computers 2021, 10, 102. https://doi.org/10.3390/computers10080102
12. Portase, R.M.; Colesa, A.; Sebestyen, G. SpecRep: Adversary Emulation Based on Attack Objective Specification in Heterogeneous Infrastructures. Sensors 2024, 24, 5601. https://doi.org/10.3390/s24175601.
13. Metin, B.; Duran, S.; Telli, E.; Mutlutürk, M.; Wynn, M. IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture. Information 2024, 15, 55. https://doi.org/10.3390/info15010055
14. Kim, I.; Park, M.; Lee, H.-J.; Jang, J.; Lee, S.; Shin, D. A Study on the Multi-Cyber Range Application of Mission-Based Cybersecurity Testing and Evaluation in Association with the Risk Management Framework. Information 2024, 15, 18. https://doi.org/10.3390/info15010018
15. P. Danquah, "Security Operations Center: A Framework for Automated Triage, Containment and Escalation," J. Inf. Sec., vol. 11, no. 4, pp. 225-240. 2020, doi: 10.4236/jis.2020.114015.