electronics

MDPI

Article

The Method for Identifying the Scope of Cyberattack Stages in Relation to Their Impact on Cyber-Sustainability Control over a System

Šarūnas Grigaliūnas, Rasa Brūzgienė and Algimantas Venčkauskas *

Department of Computer Sciences, Kaunas University of Technology, Studentu Str. 50, 51368 Kaunas, Lithuania
* Correspondence: algimantas.venckauskas@ktu.lt

Abstract: Industry X.0 is the new age of digitization, when information and communication systems are strongly linked to other systems and processes and are accessed remotely from anywhere at any time. The existing information systems' security methods are ineffective because they should focus on and assess a broader range of factors in physical and digital spaces, especially because tactics of cybercrimes are always evolving and attackers are getting more inventive in searching for holes that might be exploited. To fight it, it is a need to be one step ahead of the attacker, including understanding the nature, stages and scope of the upcoming cyberattack. The objective of our research is to identify the impact of the scope of a cyberattack's stages on the cyber resilience of an information and communication system, assessing the level of cybersecurity based on existing technical and operational measures. The research methodology includes a numerical simulation, an analytical comparison and experimental validation. The achieved results allow for the identification of up to 18 attack stages based on the aggregation of technical and organizational security metrics and detection sources. The analytical comparison proved the proposed method to be 13% more effective in identifying the stage of a cyberattack and its scope. Based on this research, the extensive scoping flexibility of the proposed method will enable additional control measures and methods that would reduce the impact of an attack on the robustness while increasing the cyber-sustainability of a system.

Keywords: stages of cyberattack; cyberattack prediction; cyber-sustainability; cybersecurity; TechSec; OpSec

Citation: Grigaliūnas, Š.; Brūzgienė, R.; Venčkauskas, A. The Method for Identifying the Scope of Cyberattack Stages in Relation to Their Impact on Cyber-Sustainability Control over a System. *Electronics* **2023**, *12*, 591. https://doi.org/10.3390/electronics12030591

Academic Editors: Jianyi Liu and Ru Zhang

Received: 29 December 2022
Revised: 17 January 2023
Accepted: 23 January 2023
Published: 25 January 2023

1. Introduction

A successful progression of existing cyberattacks targeting information and communication (ICT) and industrial control systems (ICS) might result in a loss of control over irreversible processes, whether physical or digital in nature, which can have catastrophic repercussions [1], particularly if such systems are implemented in the industrial sector known as Industry X.0 [2]. As a result, the challenge of ensuring cybersecurity for complex systems was recast as the challenge of ensuring cyber-sustainability.

Cyber-sustainability is defined as a system's ability to maintain proper operation in the face of destructive cyber impacts, also known as cyberattacks. Theoretically, cyber-sustainability refers to the continuity and stability of ICT systems in response to negative influences [3–5]. It is stated "theoretically" because the cyber-sustainability of the system is directly dependent on the existing security solutions implemented in the system, the evolving technology-driven system's architecture and its complexity, technical and operational security control measures, outsourcing of services, required human resources, etc. Therefore, at its core, cyber-sustainability means focusing time, effort and resources on mitigating cyber risks and potential loss and damage, both now and in the future.

The interaction of the essential factors—people, processes and technologies—in the context of cybersecurity is required for the proper realization of cyber-sustainability. Engaged employees are the first line of defense for sustainable cybersecurity. As more people

realize the importance of cybersecurity, the practice of finding and blocking activities that pose a likely cyberthreat should become commonplace and spread to other people. Adaptive security awareness education alters the understanding and preventive actions in response to evolving attacks while addressing old ones in novel ways, which can keep ICT system users more interested and involved [6]. In turn, users become a sustainable part of long-term cybersecurity as active first defenders.

On the other hand, if human participation is still required in the automated operations, it might lead to cybersecurity sustainability issues (i.e., the recovering of the user account). That is one of the examples of wasteful ways that requires a lot of resources (human, time, energy, etc.) without necessarily reducing the cyber risk. The functioning of a modern, technologically based society must also be safeguarded by a sustainable computing ecosystem [7], where processes and technologies evolve in terms of the people, methods and technologies used to confront and mitigate cybersecurity risks. That is the whole idea of cyber-sustainability from a cybersecurity perspective: to implement, use, control, manage or maintain security methods and techniques that do not degrade or deplete over time due to anything that influences the security of an ICT system. Pursuing this line of thought, the management of a sustainable approach to cybersecurity depends on (Figure 1) the existing security implemented in ICT systems as well as the available resources for its improvement; well-gathered information about the ICT infrastructure; security design and building; strategies and policies; etc.

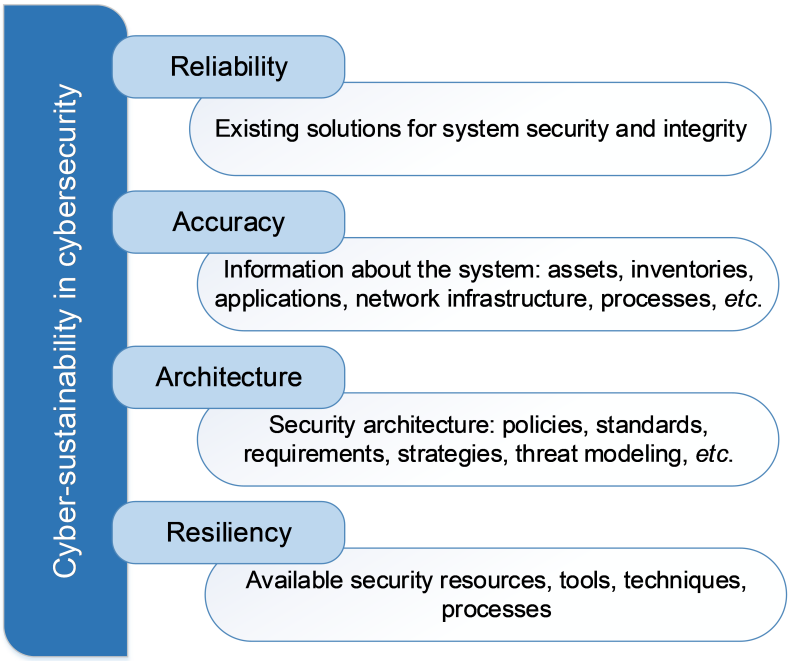

Figure 1. Management of cyber-sustainability in the context of cybersecurity (based on [8]).

Present-day circumstances preclude the existence of a true fault-tolerant system that is not linked with system security. In this context, if the system's security is compromised, this will have repercussions on its reliability, and vice versa. On the other hand, the quality of security can be affected if the information about the ICT system is not accurate. Protection is difficult if there is missing information. In order to secure the assets, for instance, the precise inventory and asset information is required. This might include the whole on-premises and cloud presence, all internally managed or externally outsourced assets (apps, network infrastructure, mobile and endpoints) or assets from a third-party vendor. Security architecture guarantees that fundamental security defenses are always correctly aligned and integrated with security standards, policies, functional and nonfunctional requirements, strategic planning and road maps. It is most likely the sole item that connects people, processes and technology with the other three principles: accuracy, reliability and

resiliency. A properly designed security architecture must allow the modeling of potential cyberthreats as well as the assessment of the nature and scope of cyberattacks on the ICT system. Resilience is reached through a variety of integration strategies, starting with the strong and dynamic management of the changing cyberthreat environment, which may or may not disrupt the company and its operations. This will help the company handle such disruptions, if they happen, with minimal or no impact on the functioning of the ICT systems or on the overall infrastructure. With the capacity to completely predict the danger scenario and keep one step ahead of the attackers, it can withstand any unanticipated interruption. The most crucial aspect of resiliency is the ability to completely recover, or return to the greatest possible peak capability, as soon as possible after any interruption or adverse event. This includes assessing the risks, mitigating the threat, reacting to the interruption and recovering quickly.

Unfortunately, the management of cyber-sustainability in terms of cybersecurity is challenging due to the fact that cyberthreats are evolving and their patterns of operation are becoming more complex and dangerous. For the modern security specialist, it is no longer enough to detect a potential cyberattack and prevent it. It is necessary to identify and analyze what malicious activity the detected cyberattack has performed or is still performing, at what stage it is, what is the scope of that activity and what are the possible further vulnerabilities it can cause. If this is not done, the penetration and further movements of a cyberattack can bring down both the systems and the entire organization. Therefore, the continuous monitoring, analysis and assessment of the vulnerability of an organization's ICT infrastructure to cyberattacks becomes a challenging process toward a cyber-sustainable ICT system.

In this paper, the authors undertake a thorough analysis of the research issue regarding the connectedness between the identification and overlapping of a cyberattack's stages and the ability to predict the attack's movement, the progression and the potential risk to the information and communication systems. The objective of this research work is to identify the impact of the scope of a cyberattack's stages on the cyber resilience of an information and communication system, assessing the level of cybersecurity based on the existing technical and operational measures. The main contributions of this research work are the following:

- Through a thorough evaluation of the current state of cybersecurity in the primary target areas of the ICT system and the simultaneous synthesis of this information with the potential impact of a cyberattack on the system's resources, it is possible to accurately identify the stage of the attack and its scope. This comprehensive analysis allows for a comprehensive understanding of the attack scope and the potential risks to the system, enabling the development of effective countermeasures and strategies for protecting against and mitigating potential cyberattacks.
- The proposed method for identifying the scope of cyberattack stages involves the compilation, gathering and association of existing technical and operational measures within the system, the security incident triggers and the attack attributes as well malicious activities at each stage of the attack.

The remainder of this paper is organized as follows. Section 2 reviews the scientific works related to the modeling, forecasting of cyberattacks and assessment of the security holes over the system as well as an analysis of the cyber risks. Section 3 introduces the concept of the proposed method for the identification of the scope of cyberattack stages and its modeling results. Section 4 outlines the method validation in an experimental test case. Section 5 presents the results of the proposed method's effectiveness in comparison to the other authors' published cyberattack scoring model. The discussion in Section 6 reviews the importance, capabilities and limitations of the proposed method. Finally, Section 7 concludes the presented work by outlining the achieved results and future works.

2. Related Works

The cyberattacks, which are evolving nowadays, have been labeled as cyberwar and researchers worldwide have made preliminary recommendations for future cyberspace defense. To prevent further attacks, the defense mechanism focuses on understanding the system as well as the network itself and the attacker's nature, motivation, attack strategy and security flaws in the system. With this in mind, this review of the scientific works includes works related to the modeling of cyberattacks, prediction of cyberthreats, estimation of the systems' or network's vulnerability and evaluation of the cyber risks.

Understanding the nature of a cyberassault requires modeling it in advance in order to strengthen the ICT system's security, which may be tailored to the requirements of the organization. Knowing the system's vulnerabilities is essential for detecting or responding to cyberattacks. The stressed importance of cyberattack modeling and its analysis with an explanation on how dangers can be modeled to lessen cyberattacks in any organization was discussed in [9]. Automated [10–12], formal based on mathematical models [13,14], graphical based on attack trees [15–17] and attack graphs [18], defense graphs or tables characterize the many approaches to cyberattack modeling. Modeling methodologies such as the OWASP threat model, OWASP treat dragon, Kill Chain, MITTRE ATT&CK, Open Weakness and Vulnerability Modeler (OVVL) [19], etc., are the examples of the modeling methodologies used to analyze cyberattacks. Attack modeling approaches are necessary to understand, research and confirm security holes in the ICT infrastructure.

In an effort to predict adversary behavior, tactical methods and systematic harmful acts, the scientific community has focused on modeling cybersecurity attack patterns and strategies based on reported occurrences and their in-depth examination [20,21]. A study of prediction and forecasting techniques used in cybersecurity was provided by the authors [22]. The authors focused on projecting the attacker's next action or purpose, recognizing when an intrusion has occurred and predicting the state of the cybersecurity throughout the whole system. They identified it as the core features covered in attack projection and intention recognition. In [23], the authors proposed a methodology for quantifying cyberattacks by identifying each element of the offensive cybersecurity used in those cyberattacks. They calculated the cyberattack score based on the Open-Source Intelligence (OSINT) method and matrix it along with the stages of the cyberattacks based on Kill Chain (Figure 2). However,the proposed methodology cannot be applied to real malware.

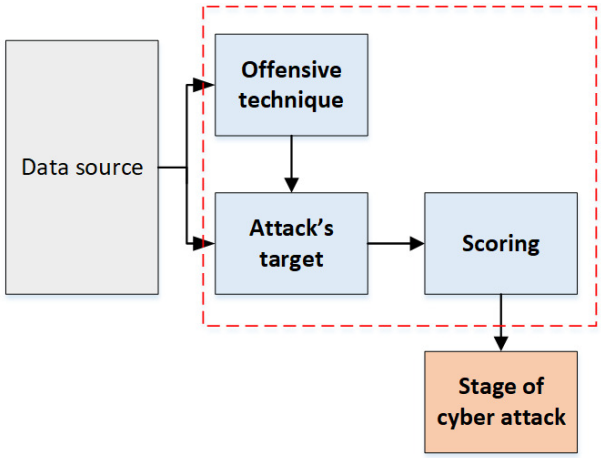

Figure 2. Identification of stages of cyberattack by scoring offensive techniques to attack's target (based on [23]).

On the other hand, the methods that can quickly identify strange things in a network can be used to find the appearance of abnormal cyberactivity [24]. Analyzing and identifying the nature of cyberthreats, its appearance on ICT systems may benefit from both continuous model-based approaches [25], such as time series and grey models, and discrete

model-based approaches, such as attack graphs, Bayesian networks and Markov models [26]. Techniques such as machine learning [27] and data mining [28], which have lately attracted a significant amount of attention and seem promising in a setting as dynamic as cybersecurity, may also be employed. The detection of each stage of the cyberattacks by sorting cyberattacks in stages was discussed in [29]. The authors suggest a method for anticipating the prediction on how the attacks are proceeding over the system using Bayesian networks. However, the suggested solution does not account for the possibility of an attacker returning inside a certain stage.

The cybersecurity team of the institution also needs to comprehend the attacker's motivation, the potential target data and the circumstances surrounding the attack [30]. Careful planning is required in order to combat the cyberattacks. Companies are investing a substantial amount of time and money in the development of effective countermeasures against cyberattacks, i.e., social engineering attacks [31]. However, the current detection techniques have significant flaws, and countermeasures are ineffective in dealing with the rise in social engineering attacks. The subjectivity of people imposes restrictions on techniques that depend on humans. Likewise, technologically dependent methods may be subject to specific constraints [32] because they may be vulnerable to an attack. In the work by [33], the primary defensive vulnerabilities against realistic adversary attacks over the ICT system were identified. The modeling of such cyberattacks against machine learning-based network intrusion detection systems revealed that poisoning attacks during the training phase are possible, provided the attacker has access to the training data (through write access). It is important to mention that the cyberattacks continue to evolve as their authors get stronger and more intelligent. Because of this, we are in dire need of improved methods not only to detect these attacks but to identify its stages over the ICT system and halt or mitigate their impacts.

It is crucial to evaluate the cyberimpacts and dangers of an assault. It can be performed by analyzing the stages of the cyberattack. The authors in [34] have concentrated on theoretical and practical issues linked to risk management and cybersecurity based on Lockheed Martin's cyber kill chain concept. The suggested way of integrating cyber risk management with the cyber kill chain is innovative and has never been documented before. The basis of the proposed method is the offered risk management process, which comprises identifying, analyzing, evaluating, assessing and ultimately reacting to cyberthreats and monitoring risks at each stage of the cyber kill chain. It may be used by companies implementing security measures to comply with regulatory requirements or to reduce cyber risks to a level that is tolerable. The approach identified each attack stage by performing a causal analysis of the attack occurrence, followed by a scenario appraisal based on the attack phases. The last steps of another suggested technique [35] enable detecting the attack goal of the subsequent stage to anticipate the network security settings based on successful attack stages matched with the vulnerability and network connection.

Putting it all together, the ICT systems experience cyberattacks every day from all over the world. The attacks involve a number of impacts that may affect the systems over a short or long period of time. The industry lacks tools that can help in identifying and tracking the progress of a cyberattack over the system, as well as mitigating the impact of them.

3. Proposed Method for Identifying the Scope of Cyberattack Stages

It is important for cybersecurity experts to identify the stages of an attack at the physical, network and application layers of an information system in order to comprehend the link between the execution and the scope of a cyberattack and the malevolent intent behind its execution. The UKC (Unified Kill Chain) model [36] gives insights and definitions for the scope of an attack through the orderly arrangement of stages of cyberattacks, including different attack vectors. It also combines and improves the CKC [37] and MITRE ATT& CK [21] frameworks that are already out there. During the operation of a cyberattack, the behavior of a malicious person basically includes eight main stages (Figure 3):

- Preparing for the execution of the attack;
- Searching for access opportunities to the environment of the target being attacked and determining the methods;
- Executing the initiation of penetration;
- Avoiding the detection of the attack;
- Distributing the malicious activity;
- Spreading and strengthening the harmful actions in the target environment;
- Implementing malicious goals;
- Having a negative impact on the target.

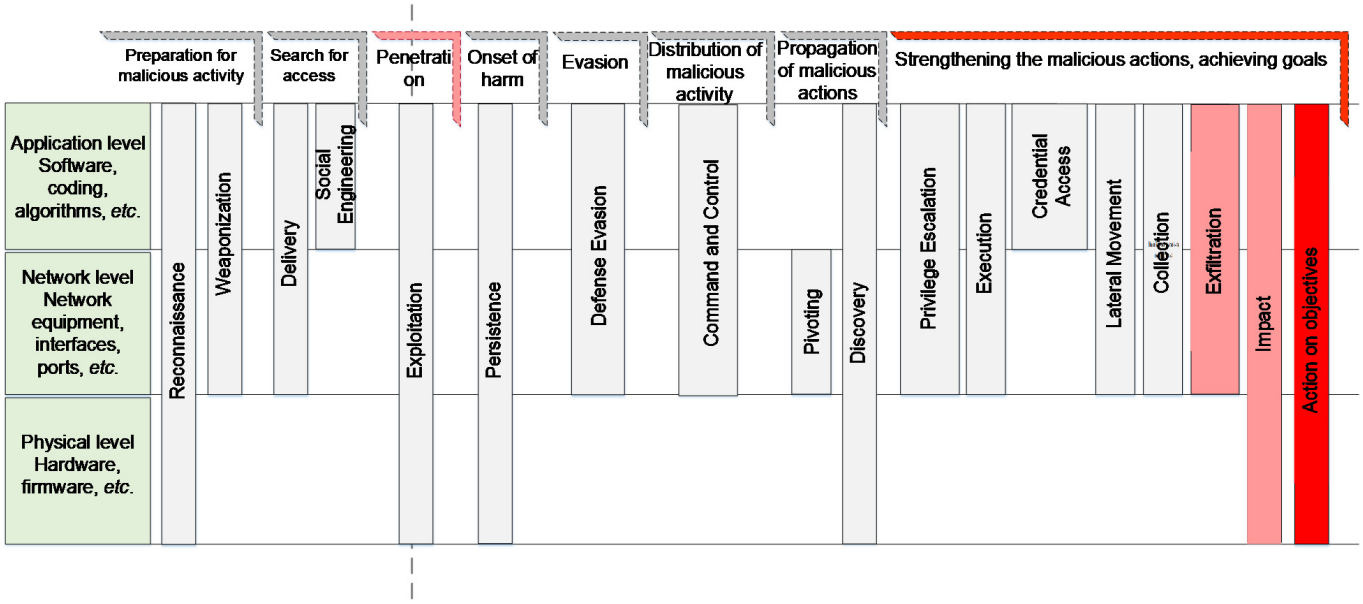

Figure 3. Link between stages of a cyberattack and malevolent intents on application–network–physical levels.

A malicious cybercriminal's preparation begins with gathering information or intelligence and selecting an attack method in the early stages of a cyberattack. During access to the target's information system, a person, organization or group with malicious goals uses both social engineering threats and other cyberthreats, which ensure that the attacker will have the opportunity to deliver malicious software or other malicious tools. The infiltration process serves as a pivotal point in the overall attack execution process. This means that even before the attacker has penetrated the system, their activities, i.e., the execution of the attack, can be stopped during each of the initial stages. However, if the attack moves to the penetration stage and beyond, it will be extremely difficult to stop such an attack.

In general, the transition to the further stages of the attack already results in a negative impact on the institution's or organization's information systems, communication networks, hardware and/or software, etc. In this case, the only difference is the scope of the negative effect during each stage of the cyberattack. The further a cyberattack spreads, the stronger the negative impact on its target will be.

In the following, the authors assume that the identification of the scope of an attack on an ICT system can be conducted through the stages it has reached. However, identifying the specific stage as well as the scope of the cyberattack continues to be a challenge for researchers all over the world. In response to this, the authors hypothesized that by assessing the current level of cybersecurity in the main target areas of the system and at the same time performing its synthesis with the impact of the attack on the system's resources, it is possible to determine the stage of the attack and its scope.

Figure 4 presents the proposed method for the identification of the stage of a cyberattack as well as its scope on a target system. The institution's ICT system's cybersecurity is based on the availability to detect malicious activities on time. The selection rules,

known as sr_i, for detecting malicious activity include information such as cybersecurity indicators, signs and attributes of a cyberthreat, compromised and vulnerable hosts, data sharing ecosystem, active network traffic flows, DNS, etc., from various public and organizations private databases. Malicious behavior during a cyberattack can basically target 4 essential areas of cybersecurity in an organization's infrastructure: network domain (i.e., IP addresses, subnet mask, network topology, domain names, etc.), host domain (i.e., user names, group names, architecture type, operating system family, version, TCP/UDP services and versions, etc.), private domain (i.e., home address, telephone no., frequent hangouts, computer knowledge, dark secrets, etc.) and security architecture (i.e., password complexity requirements, password change frequency, expired/disabled account retention, physical security factors, firewalls, IDS, etc.). The series of cybersecurity techniques used for finding adequate solutions to address the risk of technical failure or mitigation hacking activities over network and host domains refer to the technical security, called TechSec. Methods and approaches enable risk management by examining operations, security strategy on the ICT infrastructure cover the private domain and security architecture. It is called OpSec or Operation Security. Consequently, in the concept of the proposed method, security incident trigger, which refers to an event that indicates the signs of a cyberthreat, is represented for network domain as sr_1, for host domain as sr_2 and, respectively, for private domain—sr_3, security architecture—sr_4.

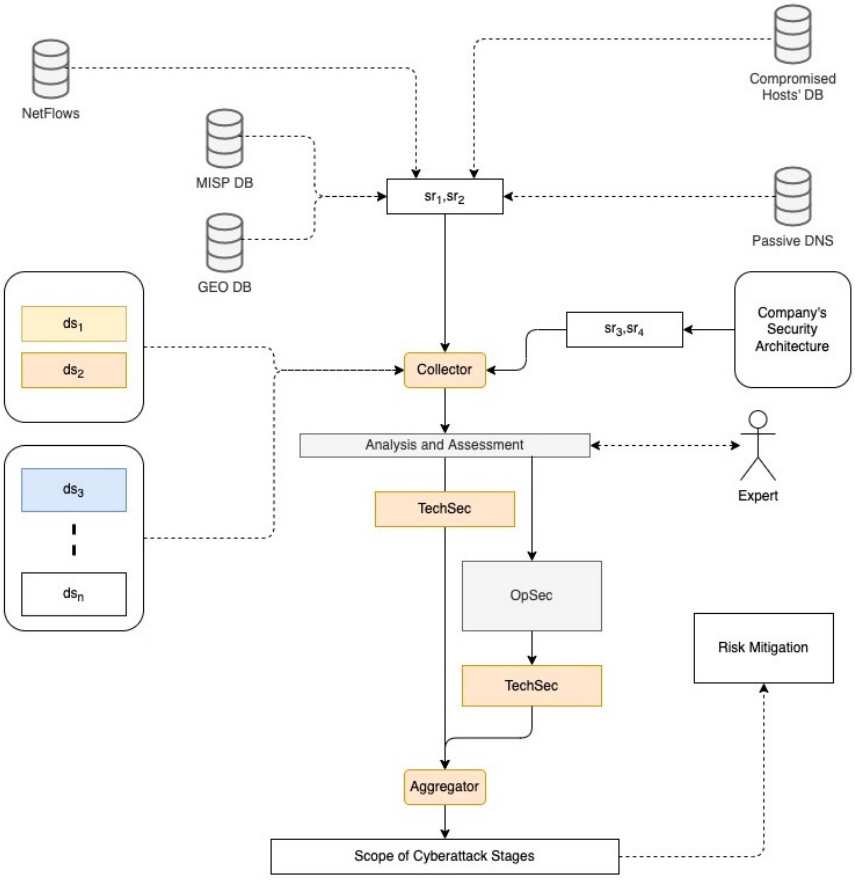

Figure 4. Proposed method for identifying the scope of cyberattack stages.

These incident triggers along with detection sources *ds* are collected for further automated and expert-driven analysis and assessment. Detection source refers to the various information subjects/topics that may be gathered by ICT system's objects or logs. It also includes data components, which indicate certain properties/values of a detection source that are useful to identifying a given malevolent approach or sub-technique. During this process, the aggregation of TechSec and OpSec security measures with appropriate detec-

tion sources is performed. Finally, it results in identification of the scope of cyberattack stage and highlights the ways for cyber risk mitigation.

One of the data sources sr_2 supports NetFlow (https://www.rfc-editor.org/rfc/rfc3954, accessed on 2 December 2022) network monitoring via integration with network traffic-analyzed attributions. It can act as a collector of NetFlow messages as well as raw packets inspector. We are analyzing network traffic in real time according to criteria, such as host, interfaces and flows with 5 min period. It extracts metadata from captured packets and uses this information to identify who/what (application protocols) are generating the flows in the network and how much bandwidth is being consumed. Among various security threats that have evolved lately, cyberattack (type ex., Dos, Flood) is the most destructive according to the security experts. A cyberattack is a method of blocking or owning a service from its intended users. A characteristic-based cyberattacks identification approach to detect subtle threats from NetFlow records.

For the experimental activities, artificial datasets were used from dataset.litnet.lt (https://dataset.litnet.lt, accessed on 2 December 2022) repository and from Cyber Shield 2022 exercises, where over 100 organizations test their cybersecurity skills and expertise to respond to various types of cyberthreats on virtual platform. The data that will serve as input for method aggregation were stored in their native formats in MISP (https://www.misp-project.org/, accessed on 2 December 2022) data method. The size of generated data is expected to be in the order of hundreds of records while the size of input data is expected to be in order of thousands or millions of records.

During the aggregation process, the identification of the stage of the cyberattack and its scope is based on the compilation, gathering and association between technical and operational security measures, security incident triggers, detection of attack attributes and malicious activities in each of the attack stages. As a result, the scope of the attack stage is equal to the outcome of cyber-sustainability control, which is based on the suitability of technical and operational security measures at the application, network and physical levels, as well as their impact found in detection sources (see Equation (1)). The expert layer has several components: data sharing, a protocol for synchronization between instances and a selection mechanism that allows defining which records to import from other instances. In the context of expert input, a unification process is defining and applying to the set of use cases related to identify cyberstage considered at organization.

The expert layer of the data flow includes a feedback loop in which cybersecurity or context experts (e.g., cyberstage) consume the data provided by the method, process it and feed new information back into the method. This is a representation of the threats to which a certain target is exposed or that exist in a certain scenario, like the cyberattack moment prediction. A threat analysis, which is made by experts, is a process that allows identifying such threats in this sense, including both a vulnerability and an attack vector that allows exploiting it.

$$S_s = M(TOS)_{ds} \cup F(TOS)_{ds}, \tag{1}$$

where S_s = scope (stage); M = mitigation; ds = detection source; TOS = technical and operation security.

The construction function for the security incident trigger f_{sr_i} can be defined as:

$$f_{sr_i} = M \cup F_i, \tag{2}$$

where F_i is a set of information system files or folders on the specific domain. The item of F_i is f and p is a set of TOS.

The construction functions f_{sr_i} for the security incident triggers are described as $\{sr_1, sr_2, \ldots, sr_n\}$, the variants of technical and/or operation security $TOS\{p_1, p_i, \ldots, p_n\}$, and variants of detection sources $ds\{ds_1, ds_i, \ldots, ds_n\}$.

After all the sequence function in the first stage of a cyberattack, known as reconnaissance, can be written as set of (Equations (3)–(13)):

$$\{f_{11}\} excludes \{f_{sr_2}, f_{sr_3}, f_{sr_4}\} \tag{3}$$

$$\{f_{11}\} requires\_any\_of \{f_{sr_1}\} \tag{4}$$

$$\{f_{21}\} excludes \{f_{sr_1}, f_{sr_3}, f_{sr_4}\} \tag{5}$$

$$\{f_{21}\} requires\_any\_of \{f_{sr_2}\} \tag{6}$$

$$\{p_1\} requires\_any\_of \{ds_1, \ldots, ds_i, \ldots, ds_n\} \tag{7}$$

$$\{p_2\} requires\_any\_of \{ds_3, \ldots, ds_i, \ldots, ds_n\} \tag{8}$$

$$\{f_{sr_1}\} requires\_any\_of \{p_1\} \tag{9}$$

$$\{f_{sr_1}, f_{sr_2}\} requires\_any\_of \{p_1\} \tag{10}$$

$$\{f_{sr_3}, f_{sr_4}\} requires\_any\_of \{p_2\} \tag{11}$$

$$f_i \rightarrow f_{sr} \rightarrow p_i \rightarrow ds_i \tag{12}$$

$$f_{11} \rightarrow f_{sr_1} \rightarrow p_1 \rightarrow ds_1; f_{33} \rightarrow f_{sr3} \rightarrow p_2 \rightarrow ds_3 \tag{13}$$

This is an example of how the aggregation of security measures, detection sources, incident triggers, security domains, threat signs can be conducted for the reconnaissance stage. All the dependencies, which characterize the stage 1 of a cyberattack, can be matrixed into Table 1 in this manner.

The process of gathering information or gaining reconnaissance consists of methods used by malicious actors to actively and/or passively gather information that will be used in later stages of the attack. Such information may include detailed information about the target organization, institution, personnel, or personal data of employees. The collected information basically helps the attacker activate the execution of the attack, moving from one stage of the attack to another.

As can be seen, four detection sources are used to identify the scope of the first stage. It is worth mentioning that mitigation methods along with appropriate detection sources are matrixed in relation to the threat models and methodologies, provided by [38]. First detection source refers to data sent over a network that is either summarized (e.g., NetFlow) or recorded in an analyzable manner as raw data. Information gathered about many sorts of Internet-connected services and servers, often by active network traffic probes or site crawling, is outlined as second detection source. Events gathered by third-party services such as mail servers, web apps and other devices are recognized as detection source ds_3. Pre-compromise mitigation method is dependent on actions conducted beyond the purview of enterprise defenses and controls; hence, detection source ds_4 shows detection attempts centered on other stages of adversary life cycle.

Weaponization (Table 2) is accomplished through methods in which an attacker creates, purchases, compromises or misappropriates capabilities that are purposefully exploited to launch a cyberattack. User accounts for access to IT systems, domains, IT infrastructure, and its structural elements (hardware, software, communication network equipment,

equipment for the institution's functions or activities (e.g., printers, scanners, electrical devices, etc.) are examples of such resources.

Table 1. Stage 1: Reconnaissance.

		Areas of Cybersecurity			
		TechSec p_1		**OpSec p_2**	
Mitigation Method M	**Detection Source ds**	**Network Domain F1**	**Host Domain F2**	**Private Domain F3**	**Security Architecture F4**
Pre-compromise M1	Network traffic ds_1	f_{11}	f_{21}		
	Internet scan ds_2	f_{12}	f_{22}		
	Application log ds_3	f_{13}	f_{23}	f_{33}	
	Related stages of the adversary life cycle ds_4	f_{14}			
Software configuration M2	Network traffic ds_1	f_{11}	f_{21}		
User training M3	Application log ds_3		f_{23}	f_{33}	f_{43}

Table 2. Stage 2: Weaponization.

		Areas of Cybersecurity			
		TechSec p_1		**OpSec p_2**	
Mitigation Method M	**Detection Source ds**	**Network Domain F1**	**Host Domain F2**	**Private Domain F3**	**Security Architecture F4**
Pre-compromise M1	Domain name ds_5	f_{15}			
	Internet scan ds_2	f_{12}	f_{22}	f_{32}	f_{42}
	Network traffic ds_1	f_{11}	f_{21}		
	Persona ds_6			f_{36}	
	Malware repository ds_7	f_{17}	f_{27}		f_{47}
	Certificate ds_8	f_{18}			f_{48}

Delivery (Table 3) actions involve the attacker's ability to deliver and activate malware on the target's IT infrastructure. In this stage of the attack, the attacker exploits techniques that allow the malware to run on the target's information system or IT infrastructure, either locally or remotely. The methods of performing malicious actions are usually combined with the methods of all other stages of the attack in order to achieve wider malicious goals, for example, exploring the topology of the communication network or leaking information.

Table 3. Stage 3: Delivery.

		Areas of Cybersecurity			
		TechSec p_1		**OpSec p_2**	
Mitigation Method M	**Detection Source ds**	**Network Domain F1**	**Host Domain F2**	**Private Domain F3**	**Security Architecture F4**
Application isolation, sandboxing	Network traffic ds_1	f_{11}	f_{21}	f_{31}	
Exploit protection	Process ds_9	f_{19}	f_{29}	f_{39}	
Restrict web-based content	Application log ds_3	f_{13}		f_{33}	
	File ds_{10}	f_{110}		f_{310}	
Update software	Process ds_9	f_{19}	f_{29}		f_{49}

Tables 4 and 5 provide aggregated information to stage 4 (social engineering) and stage 5 (exploitation).

During the social engineering stage (Table 4), the attacker tries to penetrate the institution's IT infrastructure, information system or communication network. This stage uses techniques based on the operation of various entry vectors to achieve the primary goal of the attack, which is to enter the target's environment. Methods include spearphishing, targeted phishing emails, exploiting vulnerabilities in public web servers, etc. The state of resilience gained during the social engineering access allows the attacker to continue further, deeper penetration into the target's environment. For example, using the institution's user accounts for the embezzlement of higher-level access, remote access to information systems, etc.

Table 4. Stage 4: Social Engineering.

		Areas of Cybersecurity			
		TechSec p_1		**OpSec p_2**	
Mitigation Method M	**Detection Source ds**	**Network Domain F1**	**Host Domain F2**	**Private Domain F3**	**Security Architecture F4**
Building a security culture	Penetration tests ds_{11}	f_{111}	f_{211}	f_{311}	f_{411}
Spreading awareness about the psychological triggers	Social engineering tests ds_{12}		f_{212}	f_{312}	f_{412}
Audit and policy	Audit logs ds_{13}	f_{113}	f_{213}		
Biometrics	Logon session ds_{14}	f_{114}	f_{214}	f_{314}	
Sensors	Sensor health ds_{15}		f_{215}	f_{315}	
Artificial intelligence	Process ds_9	f_{19}	f_{29}		f_{49}
Social honeypot	User account ds_{16}		f_{216}	f_{316}	f_{416}

Table 5. Stage 5: Exploitation.

		Areas of Cybersecurity			
		TechSec p_1		**OpSec p_2**	
Mitigation Method M	**Detection Source ds**	**Network Domain F1**	**Host Domain F2**	**Private Domain F3**	**Security Architecture F4**
Multi-factor authentication	User account ds_{16}	f_{116}	f_{216}	f_{316}	f_{416}
Network segmentation	Command ds_{17}	f_{117}	f_{217}		
Operating system configuration	Process ds_9		f_{29}		f_{49}
Privileged account management	User account ds_{16}		f_{216}	f_{316}	f_{416}
Limit software installation	Windows registry ds_{19}		f_{219}		f_{419}
Update software	Network traffic ds_1	f_{11}	f_{21}		
User account control	Command ds_{17}		f_{217}	f_{317}	f_{417}
Restrict file and directory permissions	Active directory ds_{18}		f_{218}		f_{418}
Execution prevention	Process ds_9	f_{19}	f_{29}		

During the exploitation stage (Table 5), the adversary exploits the disclosed vulnerability for their own reasons. If the vulnerability is genuine, the typical infrastructure breach

scenario will occur. Once an attacker has located a hole in the system, they exploit it and launch their assault. Once an attacker has acquired a footing inside the network, they will often download further tools, try privilege escalation, extract password hashes, etc. Nevertheless, if the vulnerability is a trap, its efficacy will be precisely proportional to the realism of the honeypot. This is the first stage in which data become accessible for forensic investigation for both stealth and non-stealth deception.

It is feasible to describe all 18 stages of a cyberattack (see Table 6) in accordance with the UKC model by making use of the notion of the method that was proposed in this paper.

The application of the proposed method to characterize the stages of a cyberattack highlights that the further along the cyberattack is, the greater the quantity of detection sources required when constructing the function describing the incident trigger. Moreover, to identify the scope of the attack stage, the right selection rules for security incident triggers in each security domain need to be chosen.

Matlab R2022a programming and computing software was used to model the proposed method in order to identify the scope of the stages of the cyberattack. The results of the modeling are presented in Figure 5.

The given example of the first five stages of a cyberattack that was provided demonstrates that the level of sophistication of the attack has already increased in proportion to the number of security incident triggers that have occurred and the extent to which they have impacted detection sources. For example, the scope of the first stage is defined by 10 security incident triggers detected from four sources.

Table 6. Synthesis of TechSec and OpSec in data sources at different stages of cyberattack.

ds	S1	S2	S3	S4	S5	S6	S7	S8	S9
Network traffic ds_1	f(sr1,sr2)	f(sr1,sr2)	f(sr1,sr2,sr3)		f(sr1,sr2)	f(sr1,sr2, sr4)	f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)
Internet scan ds_2	f(sr1,sr2)	f(sr1,sr2, sr3,sr4)							
Application log ds_3	f(sr1,sr2, sr3,sr4)		f(sr1,sr3)			f(sr1,sr2)	f(sr1,sr2)		f(sr1,sr2, sr4)
Related stages of the adversary life cycle ds_4	f(sr1)								
Domain name ds_5		f(sr1)							
Persona ds_6		f(sr3)							
Malware repository ds_7		f(sr1,sr2,sr4)							
Certificate ds_8		f(sr1,sr4)							
Process ds_9			f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)
File ds_{10}			f(sr1,sr3)			f(sr1,sr2, sr4)	f(sr2,sr3,sr4)		f(sr2,sr4)
Penetration tests ds_{11}				f(sr1,sr2, sr3,sr4)					f(sr1,sr2, sr3,sr4)
Social engineering tests ds_{12}				f(sr2,sr3,sr4)					
Audit logs ds_{13}				f(sr1,sr2)		f(sr1,sr2)			
Logon session ds_{14}				f(sr1,sr2,sr3)			f(sr2,sr3,sr4)		f(sr2,sr3, sr4)
Sensor health ds_{15}				f(sr2,sr3)					
User account ds_{16}				f(sr2,sr3, sr4)	f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr3,sr4)			
Command ds_{17}					f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr3,sr4)		
Active directory ds_{18}					f(sr2,sr4)	f(sr2,sr4)			
Windows registry ds_{19}					f(sr2,sr4)	f(sr1,sr2, sr4)	f(sr1,sr2)		
Firmware ds_{21}						f(sr2,sr4)			
Service ds_{22}							f(sr1,sr2, sr3,sr4)		
Script ds_{23}							f(sr1,sr2,sr4)		
Module ds_{24}							f(sr1,sr2, sr4)	f(sr2,sr4)	

Table 6. *Cont.*

ds	S10	S11	S12	S13	S14	S15	S16	S17	S18
Network traffic ds_1	f(sr1,sr2,sr4)		f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr4)	f(sr1,sr2,sr4)	
Application log ds_3			f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr4)	f(sr1,sr2,sr4)				
Process ds_9	f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	f(sr1,sr2)	f(sr2,sr4)	f(sr1,sr2,sr4)	
File ds_{10}	f(sr2,sr4)	f(sr2,sr4)	f(sr2,sr4)	f(sr2,sr4)	f(sr2,sr4)			f(sr2,sr4)	
Logon session ds_{14}	f(sr2,sr3, sr4)	f(sr2,sr3, sr4)		f(sr1,sr2, sr4)	f(sr1,sr2, sr3,sr4)	f(sr1,sr2,sr4)			
User account ds_{16}		f(sr1,sr2, sr3,sr4)		f(sr1,sr2, sr3,sr4)					
Command ds_{17}		f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr3,sr4) f(sr2)		f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	f(sr1,sr2, sr4)	
Active directory ds_{18}									
Windows registry ds_{19}		f(sr1,sr2,sr4)						f(sr2,sr4)	
Driver ds_{20}		f(sr1,sr2,sr4)							
Firmware ds_{21}								f(sr1,sr2,sr4)	
Service ds_{22}		f(sr1,sr2)							
Script ds_{23}			f(sr1,sr2,sr4)						
Module ds_{24}	f(sr2,sr4)	f(sr1,sr2)	f(sr1,sr2,sr4)	f(sr2)					
Cloud storage ds_{25}	f(sr1,sr2, sr3,sr4)					f(sr1,sr2, sr3,sr4)	f(sr1,sr2, sr3,sr4)		
Container ds_{26}		f(sr1,sr2)							
Scheduled job ds_{27}			f(sr2)						
Web credentials ds_{28}				f(sr1,sr2)					
Drive ds_{29}					f(sr1,sr2,sr4)				
ISMS document log ds_{30}									f(sr1,sr2, sr3,sr4)
Security event management tools ds_{31}									f(sr1,sr2, sr3,sr4)

Security experts should already consider the increase in the number of security incident triggers up to 37 in eight detection sources as the second stage of a cyberattack. Transitions between stages of a cyberattack can be defined as the moment of time between gaining possession in a particular stage and going on the further actions to impact target right away. Due to this, the transition to the third stage of the attack occurs when the number of detection sources in the ICT system increases in response to malicious signs. During the fourth stage, TOS security metrics, malicious signs and security incident triggers are unevenly distributed, making the shift between the fourth and fifth stages more abrupt than in previous stages. As a result, there is a great probability that a malicious person who is engaged in social engineering would abruptly transition to exploiting system vulnerabilities.

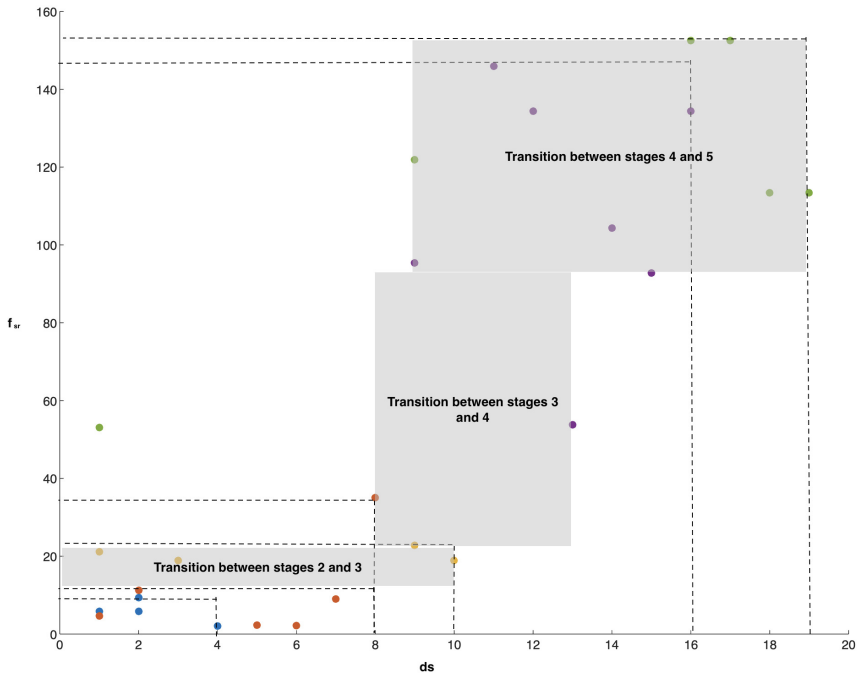

Figure 5. Modeling of the identification of the scope of cyberattack stages.

The validation of the proposed method suitability to control the cyber-sustainability over the experimental ICT system is presented in the section below.

4. Experimental Test Case for Method Validation

The proposed approach was tested experimentally in an analyzed typical medium-to-small business model organization. The main stakeholders of the organization are national universities and research institutes, as well as relevant ministries in charge of education, research and e-infrastructures. The organization was first founded by the Ministry of Education in 1949 with a few employees.

A new management system for organization programs was approved: institutional program committee groups of study fields were formed to assist in mobilizing the potential of all units; a mentoring program was developed; and a new structure for teams was developed and approved, taking into account the traditions, their recognition in the national and international environment, economic efficiency and continuity of activities. In the first year of the organization renewal program, the implementation of over three joint projects began: the management of programs, quality improvement of science, internationalization, human resource development, infrastructure management and optimization and marketing and communication development. The organization is in the European Union and therefore subject to EU legislation and regulation.

The organization is governed by a five-member representative board and has employees providing 40 full-time equivalents (FTE). There is one CEO and one CTO. The CEO is in charge of finance and human resources. Management tasks include member relations, data protection, information security, safety, business continuity and project management. Figure 6 depicts the overall architecture of the described organization's ICT system.

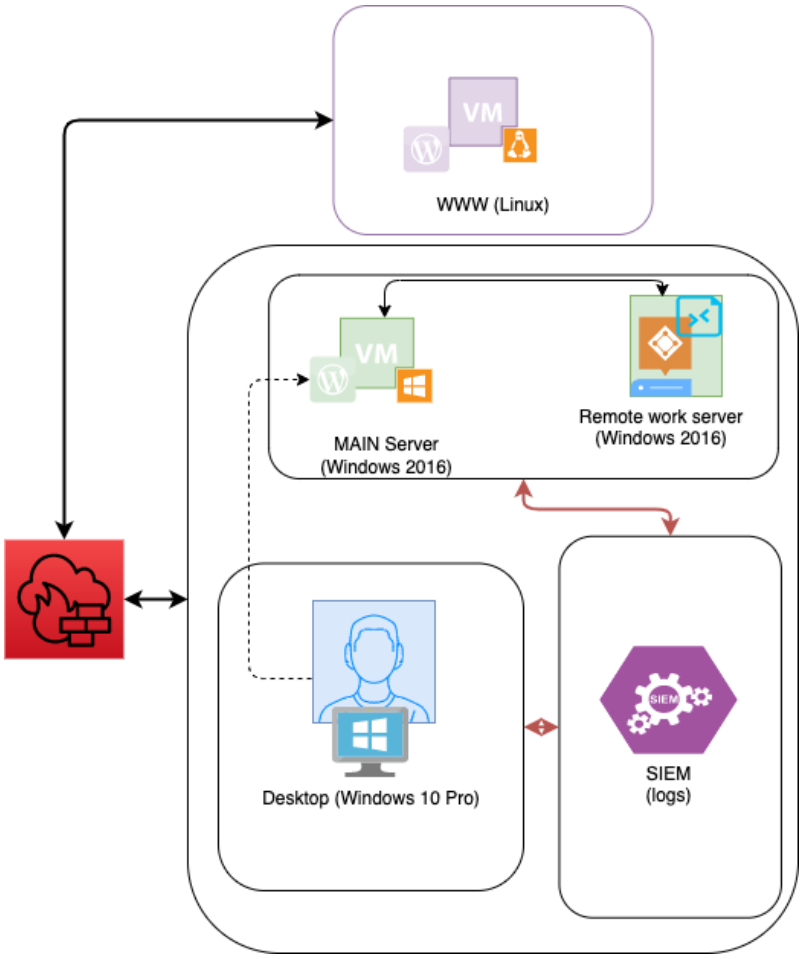

Figure 6. Architecture of organization's ICT system.

A detailed description of the identification of the stage of a cyberattack and its transition to a further stage, including the scenario and sequence of events, how the ICT infrastructure of a typical organization was hacked and compromised and the methods used to do so, is described following. The experimental testing and validation were carried out for the five-stage attack process, for which the methodology of identifying the stages and its numerical analysis are described in Section 3.

At the beginning of the cyberattack, information is available from the service station (this is the first stage of a cyberattack). The organization's standard ICT infrastructure is given in Figure 6. Afterward, a cyberattack was conducted (in a testing scenario—phishing (see Figure 7)).

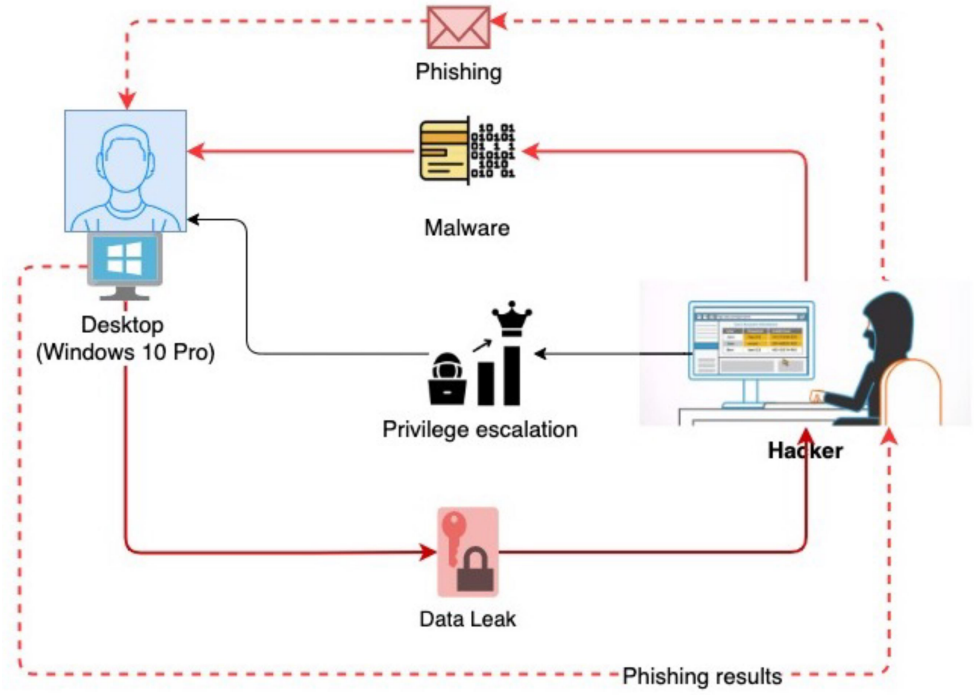

Figure 7. Phishing cyberattack.

Stage one (corresponds to modeling results in blue colour, see Figure 5). Noise is detected—active port scanning, an automated comment-writing bot is activated, which occurs every 15 s in our chosen current news. It writes a comment. There are 1000 IP addresses from which the scanning of IP packets directed to the organization's web page is performed. At this stage, information is received from these detection sources: network traffic, web service (Apache), Wordpress logs (application logs), SIEM and internet scans. The triggering related to the transition from the first stage to the second comes from the automated comments, as it seems like unauthorized access.

Stage two (corresponds to modeling results in orange colour, see Figure 5). Attempted to brute-force the user by guessing the password. From log file */var/log/apache2/access.log*, a real IP and domain name address are not shown but stored to SIEM. The number of comments leads an expert to create a prediction for recognizing the persona profile.

```
AA.171.XX.217--[17/Oct/2022:14:35:32 +0000]"POST/wp-login.php HTTP/1.1"200
2881 "-" "python-requests/2.21.0"
AA.171.XX.217--[17/Oct/2022:14:35:32 +0000]"POST/wp-login.php HTTP/1.1"200
2881 "-" "python-requests/2.21.0"
```

User "admin" attempted to guess the password. While viewing the web page, the attacker noticed that the news was written in the name of "admin".

```
2022-10-17 09:24:10 158.129.5.135 POST /wp-login.php- 8080-AA.171.XX.217
python-requests/2.21.0 - 200 0 0 109
2022-10-17 09:24:10 158.129.5.135 POST /wp-login.php -8080-AA.171.XX.217
python-requests/2.21.0 - 200 0 0 111
```

The brute-forcing of the passwords as well as other security incident triggers shows the transition to the third stage of a cyberattack, when access to the ICT system can be owned by an attacker.

Stage three (corresponds to modeling results in yellow colour, see Figure 5). It is known that a vulnerability of "TheCartPress 1.5.3.6" may be exploited by establishing a new account with administrator privileges. The intruder checks the server's IP address using "*nmap*" or comparable software. A TCP 80 connection is determined to be open at HTTP Apache log: access.log service.

```
AA.171.XX.217 - - [17/Oct/2022:14:38:38 +0000] "POST
/wp-admin/admin-ajax.php?action=tcp_register_and_login_ajax HTTP/1.1"
200 541 "-" "python-requests/2.21.0"
AA.171.XX.217 - - [17/Oct/2022:14:37:31 +0000] "HEAD
/wp-config.php.uk HTTP/1.1" 404 342 "http://BBB.129.C.147:8000"
"WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
```

The type of malware that was downloaded is known.

```
{POST /wp-admin/admin-ajax.php?action=tcp_register_and_login_ajax
HTTP/1.1" 200 541 "-" "python-requests/2.21.0"}
```

At this stage, the services show an additional type of scan directed at the application-level wpscan (https://wpscan.com/wordpress-security-scanner, accessed on 2 December 2022), with the aim of finding weaknesses and vulnerabilities in the system. From the SIEM system record, we can see that the POST method was performed to initialize the session. The expert assumes that the system was compromised by exploiting the vulnerability "TheCartPress 1.5.3.6", gained access and is ready for the next stage. A malicious file upload was identified.

Stage four (corresponds to modeling results in purple colour, see Figure 5). Instructions with a malicious attachment giving access to the workstation. Local privileges are being elevated to administrator status. The theft of important data; evidence of social engineering. An IT administrator planning to leave a workplace is approached by a representative of an unfriendly country with offers of additional income. The IT administrator contacts his head of division or department and informs him that he has received a suspicious email and has opened the file provided in the instructions. Publicly released files (e.g., a staff holiday schedule, a housing or car repair bill, and an invitation to a child's birthday party). Media contacting the organization for comment.

Recruited user: A meeting in the city was added to the calendar, just before the cyberattack started. A user of the ICT system receives an e-mail at 09:08 on 2022-10-17 09:08 from an email sender, named forallists, to the receiver email (IT admin) with a link to the malicious-driven instructions.

General statistics gathered from the email server by using the SMTP (https://www.rfc-editor.org/rfc/rfc5321, accessed on 2 December 2022) service: about 56 thousand email addresses were targeted by the social engineering attack, of which 2.6 thousand responded by clicking a malicious link and 4.5 thousand of them clicked on a link and provided profile credentials (login: company email and password). The audit logs show that the attack was successful for around 8.1% of the total company employees.

Stage five (corresponds to modeling results in green colour, see Figure 5). After setting the plugin version and name, searching the CVE and EDB vulnerability databases is

performed. Vulnerability: EDB-ID: 50378 (https://www.exploit-db.com/exploits/50378, accessed on 2 December 2022). The intruder performs a scan of possible HTTP directories with "dirb" script to find out more about the service version. WordPress plugins are discovered to be running after the scan is completed. The intruder attempts to brute-force the WP administrator's password (no password is found).

```
84.15.180.141 - - [17/Oct/2022:14:42:58 +0000]
"POST /wp-login.php HTTP/1.1" 302 1161
"http://BBB.129.C.147:8000/wp-login.php?redirect_to=
http%3A%2F%2F158.129.5.147%3A8000%2Fwp-admin%2F&reauth=1"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/102.0.0.0 Safari/537.36"

84.15.180.141 - - [17/Oct/2022:14:45:48 +0000] "POST
/wp-admin/admin-ajax.php HTTP/1.1" 200 530
"http://BBB.129.C.147:8000/wp-admin/admin.php?page=
wp-dbmanager%2Fdatabase-manage.php" "Mozilla/5.0
(Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/102.0.0.0 Safari/537.36"
```

Another detection source, available log entries from the Windows station, provides information about the forged email with an offer to cooperate. After connecting to the content management system, the attacker made a copy of the database and downloaded it. The malicious person downloaded *secret.zip* file containing copies of ID cards and a file, named "salary summary.xlsx".

```
2022-10-17 09:32:42 BBB.129.C.135 GET /secret.zip - 8080 - AA.171.XX.217
Wget/1.20.1+(linux-gnu) - 200 0 0 70
```

```
In the information message you can see a link from where to get the
information file. Downloaded, read the letter: 09:15
09:21-09:24 (session succeeded) - the start time of the attack.
09:30 Used volume created
09:45 Network scan in progress. The scan files are saved in the
C:\ directory.
10:08 data archive created
10:18 fetching file aarchivas.zip archive.zip (detected big d
ata scout in network image)
10:23 User volume - this user is connected via RDP access
```

Security information and event management tools (SIEM) can search for RDP connections (Remote Desktop Protocol) from the internet by destination port 3389. This rule detects network events that may indicate that RDP traffic from the internet is being used. The RDP is typically used by system administrators (in this case, the employee and the attacker) to remotely control the system for maintenance purposes or to access shared resources. Attack on logins (port: 8081, date: 17 October 2022, time since: 09:21).

After successfully executing the phishing attack and clicking on the link, a reverse shell to the Windows workstation was obtained. By extracting the Windows registry log, the expert concludes that the user account has been taken over and new processes have been initiated on workstations and DMZ (DeMilitarized Zone) servers. This shows that the attack does not really stop at this stage as there is an opportunity to affect the company's active directory (AD). From all the collected security incident triggers, the expert assumes

that the workstations are occupied and the attacker could attempt to occupy the active directory and move to the sixth stage. This allows the expert to initiate active preventive actions by hardening the cybersecurity of the servers and workstations, as well as changing the active directory security policy.

5. Results

In order to analyze and verify the effectiveness of the proposed method, a comparison was made with another author's proposed method for scoring the stage of a cyberattack using Open-Source Intelligence (OSINT) [23]. The proposed method can be applied to identify the scope of 18 stages of a cyberattack according to the UKC model.

Table 6 presented that identification can be performed using 31 detection sources (*ds*) in these stages. Following the evaluation principle, proposed by [23], the total sum of 31 detection sources equals to 100. In this case, one detection source is equal to a score of 3.22. The total score for 31 detection sources in 18 stages of a cyberattack is equal to 1796.76.

The table below (see Table 7) shows a comparison of five stages in a row. The first column (S_i) outlines the proposed method. The solution, proposed by other researchers, is marked as S_iO. This table also shows the number of elements (in the proposed method known as *ds*) and a total score per one detection source in all stages. The authors of the comparative solution indicated their attack stage and scope detection effectiveness equal to 20 for each of the elements. In their case, the total score is equal to 700. In our case, it stands for a 57.96 score per one detection source in 18 stages of a cyberattack.

The amount of salt and how it is obtained determines the effectiveness of the identification of the attack stage, and the samples were taken, on average, twice as accurately. The elements number of detection sources (*ds*) and how they are obtained determine the accuracy of identifying the attack stage and scope, which is on average twice as accurate.

Table 7. Evaluation of the proposed method effectiveness.

Stage	S_1	S_1O	S_2	S_2O	S_3	S_3O	S_4	S_4O	S_5	S_5O
Elements	4	2	6	3	4	3	7	3	6	3
Score	57.96	20	57.96	20	57.96	20	57.96	20	57.96	20
Effecti-veness	**0.13**	0.06	**0.19**	0.09	**0.13**	0.09	**0.23**	0.09	**0.19**	0.09

When evaluating the identification efficiency of the scope of a cyberattack stage per detection source, the weight values that are obtained are 0.032 for the method that was presented and 0.029 for the method that was compared. As a direct result of this, it provides identification that is about 13% more effective on the scope and stage of the cyberattack.

6. Discussion

All current computer systems have the capacity to monitor the behavior of cyberattacks that are aimed at a particular firm by using a variety of information sources. It might be messages received at the application level or on the network that were created as a result of previously established sets of rules (IDS, firewalls, NetFlows, etc.). The authors of this paper propose increasing the organization's resilience to cyberthreats by adopting a more expansive perspective, specifically by identifying the scope of the cyberattack stages. If an organization deals with and manages individual occurrences, it will put itself in a position where it must constantly put up a defense and will always be one step behind the person or group launching the attack. By using the proposed method together with the already-known Unified Kill Chain model, it is easy to understand which stage of the attack the organization is at.

Precisely identifying the stage of an attack in the ICT system requires a combination of technical expertise and knowledge of cybersecurity best practices, as well as the ability to gather and analyze data from various detection sources. This includes both internal and external detection sources, such as network traffic, system logs and threat intelligence feeds.

Security incident triggers also provide important information for identifying the stage of an attack. For example, an intrusion detection system (IDS) alert may indicate that an attacker is attempting to exploit a known vulnerability, while a security information and event management (SIEM) alert may indicate that an attacker has successfully gained access to a system. This means that a detection source, known as security event management tools, provides useful information regarding the malevolent approach on an ICT system.

Detection sources such as network traffic and system logs as well as threat intelligence feeds can be associated and synthesized with security incident triggers, which can provide additional context and information for identifying the stage of an attack. For example, a network traffic analysis can reveal the specific attack vector used by an attacker, while threat intelligence feeds can provide information about the tactics, techniques and procedures used by a specific threat actor.

Automation and orchestration helps to integrate and correlate data from various detection sources, which can speed up the incident identification and response. This includes the use of security orchestration and automation and response platforms, which can automate incident response processes by integrating with multiple detection sources and security tools. Overall, security incident triggers and detection sources play an important role in identifying the stage of an attack as they provide valuable information for incident response teams to make informed decisions and take appropriate actions against cyberattacks.

The method proposed by the authors allows for identifying the stages of a cyberattack and predicting its further expansion in the ICT system. Moreover, using it, it is possible to fully supplement and expand the digital forensics. Identifying the stage of a cyberattack can supplement digital forensics by providing valuable information about the scope and nature of the attack, as well as the objectives and methods of the attackers. By identifying the different stages of the attack, investigators can gain a better understanding of the entire attack process, including how the attackers gained access to the system, what information was stolen or compromised and how the attackers covered their tracks. Moreover, it can help to identify the attackers by understanding the methods and techniques used in each stage of the attack. Investigators can identify vulnerabilities in the system that the attackers exploited and prioritize their response and recovery efforts to focus on the most critical areas of the system that were compromised. By identifying the stage of the attack, investigators can document the chain of custody of the evidence and provide a clear picture of the attack from start to finish.

However, the method also has limitations. It is possible for an attack to switch from an 18-stage process to an 11-stage process or shorter. During the experimental testing of the proposed method, the incident security triggers generally were based on TechSec. Due to this, the precision to identify the stage of the cyberattack was very high and gained detection sources from service and audit logs, network traffic flows, packet capture or PCAP (also known as libpcap), SIEM, etc. However, the further an attack moves on an ICT system, the more challenges appear in relation to the existing security policies and rules on the ICT system, which come from OpSec. In general, attackers may adjust their tactics and strategies in response to changes in the security of a system or network or in response to countermeasures taken by defenders. The use of the proposed method allows for the identification of the transition between stages in a horizontal vector of the cyberattack. It is still challenging to identify the stages in the switching backward of a cyberattack. It requires the implementation of the advanced threat detection technologies, security risk management and regular security assessments to detect the transition-backward process of the attacks quickly and effectively, regardless of the attackers' tactics and objectives.

7. Conclusions and Future Challenges

Based on the aggregation of technical and organizational security metrics and detection sources, the authors proposed identifying up to eighteen attack stages in order for the organization to grasp the scope of the attack directed at it. It was also proven in the coverage of the five stages of the attack how, with a sufficient number of detection sources

and security event triggers, it is feasible to foresee the future steps of a cyberattack. When the suggested approach was compared to the findings of other researchers, it was shown to be 13% more effective in identifying the stage of a cyberattack and its scope.

Future work will involve the development of risk management and organizational readiness strategies to defend against cyberattacks at the appropriate stage. Comprehensive risk management should handle all components of an organization's ICT systems, including people, processes and technology. Moreover, risk management is a crucial aspect of cyber-sustainability. It entails detecting, evaluating and reducing possible risks to an organization's ICT systems and data in a sustainable manner. This entails forecasting and planning for future risks in addition to resolving current challenges. A cyber-sustainable risk management should adopt a comprehensive approach that tackles not just the technical components of cybersecurity but also the organizational and social factors, with a focus on the organization's ICT systems' long-term sustainability and resilience. A proposed method that could include comprehensive and adaptive risk management and incident response strategies would be very useful for auditors and researchers when they need to compare, use as a benchmark or predict how an attack will progress or can be stopped.

Author Contributions: Conceptualization, Š.G. and R.B.; methodology, R.B.; software, Š.G.; validation, Š.G., R.B. and A.V.; formal analysis, Š.G.; investigation, Š.G. and R.B.; resources, Š.G.; data curation, Š.G.; writing—original draft preparation, Š.G. and R.B.; writing—review and editing, A.V.; visualization, Š.G. and R.B.; supervision, A.V.; project administration, A.V.; funding acquisition, A.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this paper are available on request from the corresponding author. The data are not publicly available due to the project not being completed.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Firoozjaei, M.D.; Mahmoudyar, N.; Baseri, Y.; Ghorbani, A.A. An evaluation framework for industrial control system cyber incidents. *Int. J. Crit. Infrastruct. Prot.* **2022**, *36*, 100487. [CrossRef]
2. Van Den Dool, F.; Widdershoven, G.; Haughton, A. Cyber Resilience for Industry X.0 in Europe. 2019. Available online: https://www.accenture.com/_acnmedia/pdf-92/accenture-cyber-resilience-busindx-europe.pdf (accessed on 18 November 2022).
3. Lavrova, D.S. Maintaining cyber sustainability in industrial systems based on the concept of molecular-genetic control systems. *Autom. Control Comput. Sci.* **2019**, *53*, 1026–1028. [CrossRef]
4. Zegzhda, D.P. Convergent Evolution of IT Security Paradigm: From Access Control to Cyber-Defense. In *The Economics of Digital Transformation*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 143–155.
5. Bei, H. Problems of cybersecurity in the context of becoming and development of the new economy. In Proceedings of the Competitivitate şi Inovare în Economia Cunoaşterii, ASEM, Chişinău, Republica Moldova, 27–28 of September, 2019; pp. 454–464.
6. Khando, K.; Gao, S.; Islam, S.M.; Salman, A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Comput. Secur.* **2021**, *106*, 102267. [CrossRef]
7. Gomes, C.; Dietterich, T.; Barrett, C.; Conrad, J.; Dilkina, B.; Ermon, S.; Fang, F.; Farnsworth, A.; Fern, A.; Fern, X.; et al. Computational sustainability: Computing for a better world and a sustainable future. *Commun. ACM* **2019**, *62*, 56–65. [CrossRef]
8. Chanda, D. Principles of Sustainable Cybersecurity. Available online: https://www.bankinfosecurity.com/blogs/principles-sustainable-cybersecurity-p-3127 (accessed on 7 November 2022).
9. Al-Mohannadi, H.; Mirza, Q.; Namanya, A.; Awan, I.; Cullen, A.; Disso, J. Cyber-attack modeling analysis techniques: An overview. In Proceedings of the 2016 IEEE 4th iNternational Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 69–76.
10. Musman, S.; Turner, A.J. A game oriented approach to minimizing cybersecurity risk. *Int. J. Saf. Secur. Eng.* **2018**, *8*, 212–222. [CrossRef]
11. Stojanović, B.; Hofer-Schmitz, K.; Kleb, U. APT datasets and attack modeling for automated detection methods: A review. *Comput. Secur.* **2020**, *92*, 101734.
12. Enoch, S.Y.; Huang, Z.; Moon, C.Y.; Lee, D.; Ahn, M.K.; Kim, D.S. HARMer: Cyber-attacks automation and evaluation. *IEEE Access* **2020**, *8*, 129397–129414. [CrossRef]

13. Fu, Y.; O'Neill, Z.; Yang, Z.; Adetola, V.; Wen, J.; Ren, L.; Wagner, T.; Zhu, Q.; Wu, T. Modeling and evaluation of cyber-attacks on grid-interactive efficient buildings. *Appl. Energy* **2021**, *303*, 117639. [CrossRef]
14. Goncharov, V.; Goncharov, A.; Shavrin, S.; Shishova, N. The Cyber Attack on the Corporate Network Models Theoretical Aspects. In Proceedings of the 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 16–18 March 2021; pp. 1–4.
15. Ahmadi, A.; Nabipour, M.; Taheri, S.; Mohammadi-Ivatloo, B.; Vahidinasab, V. A New False Data Injection Attack Detection Model for Cyberattack Resilient Energy Forecasting. *IEEE Trans. Ind. Inform.* **2022**, *19*, 371–381. [CrossRef]
16. Stellios, I.; Kotzanikolaou, P.; Grigoriadis, C. Assessing IoT enabled cyber-physical attack paths against critical systems. *Comput. Secur.* **2021**, *107*, 102316. [CrossRef]
17. Tatam, M.; Shanmugam, B.; Azam, S.; Kannoorpatti, K. A review of threat modelling approaches for APT-style attacks. *Heliyon* **2021**, *7*, e05969. [CrossRef]
18. Stergiopoulos, G.; Dedousis, P.; Gritzalis, D. Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in Industry 4.0. *Int. J. Inf. Secur.* **2022**, *21*, 37–59. [CrossRef]
19. Shi, Z.; Graffi, K.; Starobinski, D.; Matyunin, N. Threat Modeling Tools: A Taxonomy. *IEEE Secur. Priv.* **2021**, *1*, 2–13. [CrossRef]
20. Straub, J. Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks. In Proceedings of the 2020 IEEE International Conference on Smart Cloud (SmartCloud), Washington DC, WA, USA, 6–8 November 2020; pp. 148–153.
21. Xiong, W.; Legrand, E.; Åberg, O.; Lagerström, R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Softw. Syst. Model.* **2022**, *21*, 157–177.
22. Husák, M.; Komárková, J.; Bou-Harb, E.; Čeleda, P. Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Commun. Surv. Tutorials* **2018**, *21*, 640–660. [CrossRef]
23. Kim, K.; Alfouzan, F.A.; Kim, H. Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework. *Appl. Sci.* **2021**, *11*, 7738. [CrossRef]
24. Kotenko, I.; Saenko, I.; Lauta, O.; Kribel, A. An approach to detecting cyber attacks against smart power grids based on the analysis of network traffic self-similarity. *Energies* **2020**, *13*, 5031. [CrossRef]
25. Biroon, R.A.; Biron, Z.A.; Pisu, P. False data injection attack in a platoon of CACC: Real-time detection and isolation with a PDE approach. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 8692–8703. [CrossRef]
26. Muhati, E.; Rawat, D.B. Hidden markov model enabled prediction and visualization of cyber agility in iot era. *IEEE Internet Things J.* **2021**, *9*, 9117–9127. [CrossRef]
27. Khan, F.A.; Gumaei, A.; Derhab, A.; Hussain, A. A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access* **2019**, *7*, 30373–30385. [CrossRef]
28. Rahman, M.A.; Al-Saggaf, Y.; Zia, T. A data mining framework to predict cyber attack for cyber security. In Proceedings of the 2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA), Kristiansand, Norway, 9–13 November 2020; pp. 207–212.
29. Pivarníková, M.; Sokol, P.; Bajtoš, T. Early-stage detection of cyber attacks. *Information* **2020**, *11*, 560. [CrossRef]
30. MITRE. CALDERA: A Scalable, Automated Adversary Emulation Platform. 2021. Available online: https://caldera.mitre.org/ (accessed on 30 September 2022).
31. Siddiqi, M.A.; Pak, W.; Siddiqi, M.A. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Appl. Sci.* **2022**, *12*, 6042. [CrossRef]
32. Conteh, N.Y.; Schmick, P.J. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *Int. J. Adv. Comput. Res.* **2016**, *6*, 31. [CrossRef]
33. Apruzzese, G.; Andreolini, M.; Ferretti, L.; Marchetti, M.; Colajanni, M. Modeling realistic adversarial attacks against network intrusion detection systems. *Digit. Threat. Res. Pract. (DTRAP)* **2022**, *3*, 1–19. [CrossRef]
34. Hoffmann, R.; Napiórkowski, J.; Protasowicki, T.; Stanik, J. Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manuf.* **2020**, *44*, 655–662. [CrossRef]
35. Kun, W.; Hui, Q.; Haopu, Y.; Di, H. Network security situation evaluation method based on attack intention recognition. In Proceedings of the 2015 4th International Conference on Computer Science and Network Technology (ICCSNT), Harbin, China, 19–20 December 2015; Volume 1, pp. 919–924.
36. Pols, P.; van den Berg, J. *The Unified Kill Chain*; CSA Thesis: Hague, The Netherlands, 2017; pp. 1–104.
37. Ahmed, Y.; Taufiq, A.; Md Arafatur, R. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. *Comput. Mater. Contin.* **2021**, *67*, 2497–2513. [CrossRef]
38. MITRE. ATT&CK. 2022. Available online: https://attack.mitre.org/ (accessed on 10 July 2022).